A structured, systemic methodology to improve maritime fire safety in machinery spaces

James McNay

Submitted for the

Degree of Doctor of Philosophy,

Maritime Safety Research Centre, Department of Naval Architecture, Ocean & Marine Engineering, University of Strathclyde.

October 2020

Abstract

The primary cause of machinery space fires is cited as the release of flammable oil mist contacting unprotected hot surfaces. With this being common knowledge why do we continue to see this type of incident reoccurring on ships carrying thousands of passengers to precarious destinations? Anecdotal evidence suggests that the prime focus of maritime fire safety falls on risk mitigation, as opposed to its prevention. It also appears technological safety barriers are placed in an 'install and forget' mentality through lack of appreciation of the overall system of safety control. This belief is explained by referring to risk reduction of adding a 'layer of protection' or by supposedly higher cost-effectiveness of accident mitigation measures. The significance of this belief goes beyond the accurate understanding of the state-of-the-art of maritime safety. If it turns to be wrong, at best it can misplace precious resources aimed at safety improvements, at worst it can result in an almost inevitable drift towards a machinery space fire with neglect of the control of fire free operation.

The current approach to fires in machinery spaces is hypothesised to be reactive in nature, primarily focusing on detection of already materialised hazards with little or no regard to the systemic nature of hazard occurrence. My research analyses the focus to verify the hypothesis. I then determine if an alternative method can be applied to improve fire safety.

With the initial hypothesis proven correct, the societal implication could be significant. Everyday life in the 21st century involves the interactions between humans, machines and the environment, and this trend is only increasing. If safety fails to account for such factors adequately, safety related accidents may continue to occur at a consistent, if not increased, rate. Conversely with the application of the methodology developed in this research, which accounts for systemic factors using established state of the art hazard analysis techniques to a new application and in a novel manner (directly incorporating design and operation), society may see the elimination of accidents it has grown to accept as unavoidable.

This thesis adopts an alternative method and process (STPA) to apply a structured approach to systemic fire hazard identification and analysis, as an input to safety barrier identification and improvement techniques (e.g. Dynamic Barrier Management [DBM], real time risk representation, etc.). Barrier identification and improvement techniques are only useful if relevant hazards and causal factors are being evaluated alongside the interactions between humans, technology, and the environment. The approach also only has success if applied into the facility lifecycle during the operational phase. The novelty of applying a structured systemic approach to achieving fire safety during HAZID with a direct link to safety auditing is therefore fundamental to the impact of this thesis.

Within the research I apply this technique in a case study and audit on an operational cruise ship where it is demonstrated that the approach has unearthed otherwise dormant safety concerns. These gaps would have been difficult to discover through the application of an unstructured/ traditional approach to fire safety design and auditing. The findings from the case study provide a critical input to the improvement of the leak prevention barrier of fire safety and demonstrate the novelty and usefulness of such an approach in striving for fire free operations.

Where safety barriers are required or can be improved (i.e. if the same events occur at a consistent frequency from seemingly the same causal factors), the research introduces the Systemic HAZID and Operational Risk Evaluation (SHORE) methodology which presents an easy to follow process (for those not familiar with STPA) leading to the informed selection of specific sensor inputs, for example, which are safety critical and either not installed, or ineffective where they have been installed. The methodology also allows for easy and direct incorporation into the Safety Management System (SMS) of the ship through auditing for continued operational safety evaluation.

Acknowledgements

I wish to acknowledge and thank the contributions made towards this research from the University of Strathclyde's Maritime Safety Research Centre (MSRC) and the technical contribution and support from the MSRC sponsors DNVGL and RCCL. Without the academic knowledgebase within MSRC and the operational wealth of knowledge and experience from both DNVGL and RCCL this thesis would not have been possible.

Special thanks go to Dr Romanas Puisa and Professor Dracos Vassalos for providing continual support during my research, and for going well above and beyond the call of duty. Their guidance and passion for the subject helped me through every stage in the research. My trips to Glasgow were always a great source of inspiration for both this thesis, but also in life.

The contribution from the team I collaborated with on the SEAMAN project is also greatly valued, the findings of which helped to mould the direction of travel of this thesis and were critical through the validation process of the SHORE methodology.

Table of Contents

Contents

Table of Figures

List of Tables

1 Introduction and Motivation

1.1 Problem Definition, Innovation and Impact

1.1.1 The Problem

Fire is widely accepted as a significant hazard in the maritime industry (1), particularly in machinery spaces (2, 3). With the societal shift towards safer operations and fire safety being singled out by cruise ship and RoPax operators as a primary focus (4, 5), why therefore do we continually see fires occurring at a consistent frequency (6)? Why also are machinery space fires seemingly a result of the same causal factors, namely the release of flammable material coming into contact with an exposed hot surface (7, 8)?

The problem is presented to us: maritime machinery spaces regularly have fires from, seemingly, the same causal factors. This research aims to first determine why this is the case, and evaluate if there is an opportunity for strengthening fire safety through alternative methods or through modification of the existing means of applying fire safety in these spaces.

1.1.2 The Innovation

If one adopts the notion of hazard control, fires continually occur because the control is inadequate at certain critical moments. These moments may occur at the sharp end within the machinery space, or they may occur far from that location, for example through managerial decision making onshore. To control a hazard, there is a hierarchical structure in place, from engineers and equipment (implementing the SMS for example), to the company (who design, updates and enforce the SMS), and beyond to regulators and designers (who verify and impose constraints on the SMS). Ultimately, therefore, there must be something wrong in this system if it cannot achieve its purpose of fire free operation. The innovation presented in this thesis aims to address the systemic nature of accidents for the previously mentioned application, identifying the requirements of safety barriers and analysing existing gaps to verify utility. The subsequent methodology presented, will apply the state of the art in hazard

identification and analysis to the problem. This aims to efficiently identify such gaps by practitioners during design and operation with increased emphasis on prevention. Novelty is presented in achieving both design and operational systemic hazard prevention within the same methodology.

1.1.3 The Impact

Within the maritime industry, it is credible that a novel structured systemic approach, which accounts for goal-based fire safety with added focus on preventative measures, can be used to demonstrate an alternative design arrangement of equivalent safety from traditional prescriptive/ reactionary approaches. This will assist fire safety measures in further encompassing the preventative region and move towards a systems-based, holistic analysis. When applied specifically within the Maritime industry, the approach will provide operators with a methodology to address systemic causal factors, increasing fire safety and resilience while being easily incorporated within the current SOLAS and SMS frameworks. Resilience in this context refers to “an organisation’s ability to detect, prevent, respond to, and recover and learn from operational and technological failures which may impact the delivery of critical business and economic functions or underlying business services” (9). The approach will also be attractive to Class societies as this presents a methodology which, if applied, assists in demonstrating design and operational safety is an active process within the shipping operator, and can also become a service offering.

With respect to the immediate impact of the research, it has resulted in the newly developed Systemic HAZID and Operational Risk Evaluation (SHORE) methodology, and has been applied as part of a global research project with a world leader in operating cruises and an industry leading class society.

Connected with this impact is the development of the methodology which has scope for commercialisation and application into the wider safety community. This methodology allows the application of the approach higher in the safety control hierarchy in addition to the sharp

end, which opens up an interesting area of further study, to investigate the findings when the approach extends to the upper echelons of control in the maritime, or any other, industry.

This academic novelty and impact is demonstrated when considering the use within virtually any field which requires hazard prevention, where a control structure is present encompassing humans, technology and the environment, with hazard prevention measures implemented in design and operation. Such fields include, but are not limited to, the aviation, business and finance sectors. The academic contribution is presented in demonstrating that the combination of: a focus on prevention; a structured decomposition of the system of control; and the direct connection between ‘design’ and ‘operations’, can result in any ‘event’ becoming preventable through adequate systemic control. One such example is the potential application of SHORE by governments in addressing societal issues such as violent crime, as discussed in Chapter 9. When the prevention of a problem is treated as an issue of systemic control, opportunities to address previously unrealised causal factors emerge, showing a wide application potential of the approach.

1.2 Philosophy of Fire Safety

It is often suggested that the prime focus of maritime safety falls on accident mitigation, as opposed to prevention. This can be seen in the development and integration of mitigation-based technologies in machinery spaces including oil mist detection, CCTV based smoke detection etc. over the last decade. This belief is frequently explained by referring to supposedly higher cost-effectiveness of accident mitigation measures. This implies that a rational strategy would be to start with improving mitigating measures (e.g., fire detection and suppression), and only then improve preventive barriers (e.g., detection of fire precursors). Therefore, while both prevention and mitigation are clearly present, one must analyse the overall philosophy of fire safety and how these facets of fire safety interact to provide safe operation.

Supporting references are given from the offshore oil and gas industry, where the mitigating barriers are indeed the prime focus (10, p. 49). The significance of this proposition goes beyond the accurate understanding of the state-of-the-art on maritime safety. If it turns out to be wrong, it can misplace precious resources aimed at safety improvements. Therefore, the initial stages of this thesis must examine if this belief is justified.

The reference to cost-effectiveness usually refers to the criteria applied during a Formal Safety Assessment (FSA), the instrument for rule-making at the IMO (11), which is to be further examined in the critical review. There can, however, also be subjective or experiential judgment leading to this belief. It can, for instance, be stimulated by the perception that the complexity of modern designs and operations makes incidents inevitable. Indeed, in complex systems design, errors are frequent and procedures are often underspecified (12). Hence, improving the response through higher robustness of passive systems and resilience of active ones should take precedence over, arguably, contingent effort on prevention. For instance, fire protection in machinery spaces has recently been transformed by high pressure water mist systems (13-15) and new generations of fire alarm systems that use intelligent sensors (16). This is also demonstrated in flooding protection, which is conventionally achieved by maintaining the ship's watertight integrity by passive and active measures, being prominent at the centre of maritime safety (17). A recent advancement in this area is the new, much stricter damage stability regulation, SOLAS 2020 (18). Efforts on improving effectiveness of the ultimate mitigating barrier, evacuation, have also, however, been significant (19, 20).

Regardless of how much work is done on accident mitigation, whether for flooding or fire safety, it only underlines the importance of this second barrier being dependent upon failure of the first barrier: prevention. Importantly, from the cost-effectiveness perspective, the main effort may actually need to be directed to prevention. It is commonly known that preventing a hazard from materialising is more preferable than fighting its consequences (21-23). If prevention succeeds, the event is only a near-miss, (or potentially not even registered as a near miss if the drift towards failure is detected and prevented early enough) and it will not

normally disturb the ship's primary function (delivery of payload). Eliminating the hazard from the system has to be the best strategy, provided the ship's prime function and its performance requirements (desired speed, fuel consumption, payload capacity, etc.) remain undisturbed. By eliminating a hazard (e.g., flammable oil mist cannot be formed at all), a myriad of opportunities for various incidents are singularly eliminated. If a hazard cannot be eliminated (e.g., because the ship's primary function is disturbed), the minimisation of likelihood of its materialisation into specific incidents by some control actions would still be more effective than the alleviation of incident damages. Additionally, the cost of implementing preventive strategies has been shown to be generally lower than the cost of reliance on mitigation barriers (24-26).

Accentuating the incident avoidance also aligns well with the business perspective in the maritime sector. The occurrence of accidents, i.e. incidents resulting in fatalities, can bring irreparable damage to reputation of a shipping company. It can dissuade people from choosing the operator, reduce market share, company value, and introduce new safety regulations with additional financial repercussions. Moreover, even an incident with no serious consequences, perhaps apart from a few scratches on the hull, is already a dramatic experience for passengers. The contemporary society holds high expectations for safety and service quality, which is essentially how leisure and business services are marketed today. Hence, poor incident avoidance, which would lead to frequent disappointments on the part of customers, is clearly damaging for the business. Notably, the rail industry nearly exclusively focuses on collision avoidance, i.e. on preventive barriers (10, p. 49).

In the top causes of loss where this results in a maritime claim, fire ranks second on the list by the number of claims at 16%, and also second in value of claim (3). As previously mentioned, fire in machinery spaces, has been singled out by cruise ship and roll-on/ roll-off (RoPax) operators as a primary focus, singularly or collectively striving to contain this risk (4, 5). Between August 2011 and January 2018, amongst 112 'serious' and 'very serious' fire incidents (as defined by EMSA), 57 were in the machinery spaces (27). More than a decade

ago, a study by Det Norske Veritas (DNV) reported that about half of fires that occurred in machinery spaces resulted from the contact between combustible oil mist and high temperature surfaces (7). Little has changed since then, for this very scenario remains rife today (28).

The approach to fire safety is intended to reflect knowledge of how fires happen and develop, and, therefore, implement methods whereby fires shall be prevented or at least controlled. Prevention and control (or mitigation) are often considered complementary and could be viewed as two sequential processes of protection, providing redundancy in safety against fire development. In fact, idealistically these could be classed as independent. If the design can, for example eliminate the flammable material entirely, there could be no need for a fire detection and suppression system. While this is idealistic, it is critical in the argument for cost effectiveness when we consider prevention and mitigation are closely related and trade-offs can therefore be struck.

The notion of prevention vs mitigation shall be further developed and interrogated by analysing specifically what the current approach is and whether this is effective. These issues shall be required to be addressed in reviewing why we see fires from seemingly the same causal factors. This will provide the basis of analysis into whether fire safety can be improved through alternative methods, or through modification of the existing means.

Existing methods are informed by experience, fire safety tradition, technological and programmatic constraints, as well as the input from accident investigation. The latter plays a special role, for it arguably creates new knowledge by explaining what happened and how this can be avoided next time (Figure 1). Although maritime accident investigation recommendations are aimed at shipping companies, they often also have a ripple effect across the whole industry, affecting safety rules and their implementation, offered technology, design and operational decisions, and the course of research. A notorious example is the fire on passenger ferry Scandinavian Star in 1990, which triggered a comprehensive revision of the

International Code for Fire Safety Systems in 1992 and affected the approach to fire protection and evacuation (29).

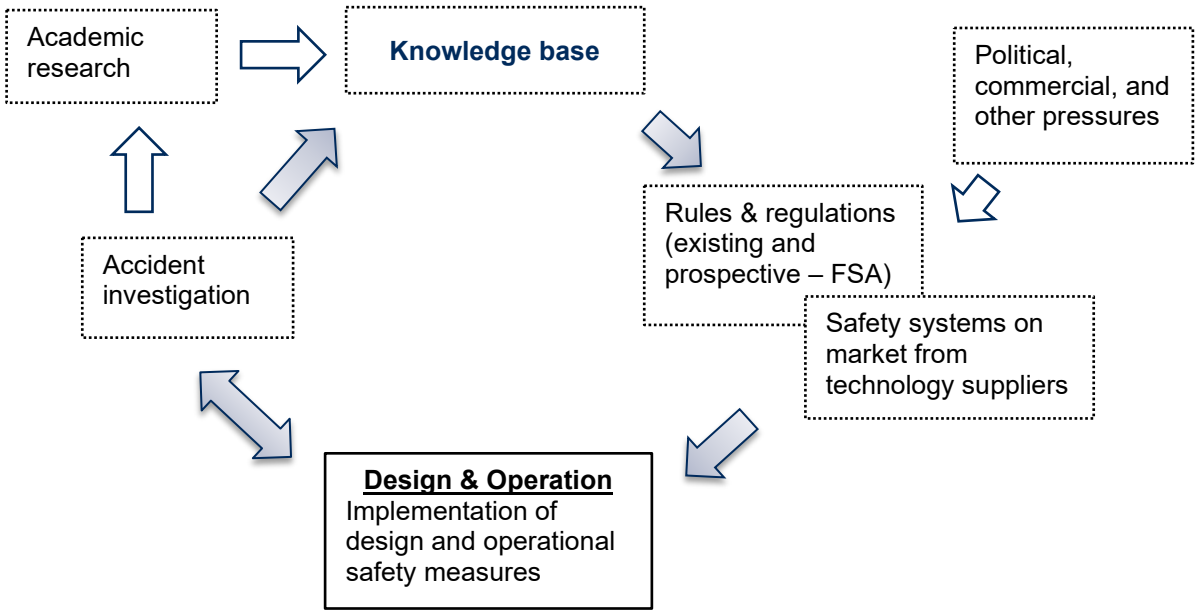


Figure 1: Evolutionary process to safety (30)

Accident investigations begin with prior assumptions at hand, i.e., an accident model - the understanding of how fires, and accidents in general, occur. The prior assumptions prompt what to look for and what will, therefore, be found (31). Subsequently, what is found, is recommended to be fixed. The problem is that these assumptions can be flawed on some fundamental aspects, leading to ineffective safety rules, regulations, good practices, and, in part, safety systems. This results in inadequate hazard control and, therefore, incidents. On the other hand, ineffectiveness may also be unwittingly introduced by political, commercial and other pressures (Figure 1). Statutory safety rules, in particular, are a result of a consensus between rule givers (i.e. regulators) and rules takers (i.e. operators, designers) (32). Thus, in the strict sense, safety rules cannot be said to set either a minimal or average safety level, but merely an agreed safety level.

Flaws in prior assumptions about how incidents occur, and hence how they can be prevented, has attracted much attention over the last few decades. Pre-ignition events take time to

develop. Conditions (e.g., wrong design assumptions, presence of design limitations) would lead to events or other conditions (e.g., ill-informed management, training, and O&M procedures), which in turn lead to other events and conditions and so on. The metaphors like “incubation period” and “drifting into failure” are used to explain the dormant, latent conditions in a system that, with time, insidiously degrade the system to the point when an incident becomes imminent (33, 34). This degradation or drift is systematic (not random) and fuelled by natural phenomena of adaptation to new circumstances (endogenous and exogenous) and optimisation of resources (35); it is also explained as the inexorable manifestation of entropy. A helpful property of this dynamic is its relative slowness and determinism, which means that the drift is detectable and preventable (26, 36). On the other hand, this natural system dynamic undermines the utility of accident investigation results that inevitably reflect the past circumstances, which may not remain relevant (37). It also shows the importance of maintaining relevance of safety measures and barriers throughout the lifecycle of a facility.

The important realisation is that the underlying system behaviour cannot be changed by merely looking for or reacting to its events, or by analysing components of the system in isolation (38). Therefore, increasing the layers of protection does not necessarily lead to safety in socio-technical systems because additional safety barriers and protection can be defeated by psychological reactions (39). The reason being that a socio-technical system is more than the sum of its components (35). Thus, the cause of an incident and accident is the inadequate design of the system as a whole, rather than specific scenarios in isolation. Such inadequacies, e.g. flawed links, can exist for a brief moment in time in the correct context, yet distant to each other in a different time and context. This can, however, be enough to cause an effect that is nonlinear, such as small events or conditions which can cause serious consequences (40); the reverse is also true. Therefore, the modern paradigm of systems thinking may be more appropriate. The systems approach accentuates the importance of nonlinear interactions between system components and the system structure and mental models that determine it (41).

This paradigm is taken up by safety research in the maritime industry. It is observed that such research points towards further appreciation of the organisation, inter-organisational, and human aspect of the problem (42-45), and all factors which are hypothesised may not be accounted for in the current approach. Such research also points to the importance of not analysing barriers in isolation, but rather applying an appreciation of the entire system, and the interactions between its components, being of critical importance when analysing the emergence of ‘safety’ as a condition. While this wider safety research does not directly relate to fire safety in machinery spaces, its tailored application to fire safety would be novel and may provide holistic improvements in fire safety on ships. This systemic approach to accident prevention should not be at the expense, however, of analysis of individual features of fire prevention. These can be noted in the literature covering human and organisational factors, historical causal factors of fires in maritime transportation, calculation of fire probability (8, 46, 47), along with fire impact analysis research focusing on mitigating the outbreak of fire (48-61).

With the above in mind, the question is whether the prior assumptions that guide accident analysis, safety rules and regulations, etc. are indeed flawed. If so, we should not expect effective prevention or/and mitigation of fire events. In fact, as systems include an increased human, environment, and technological interaction, should we expect fire incidents to increase if the approach to fire safety does not also evolve? To answer this question, this research will analyse the current approach to fire safety, identifying its focus along the line of accident development. The thesis specifically examines the current rules and regulations and their development biases, as well as biases in accident analysis and safety systems offered on the market. I will then discuss the implications and the significance of these biases in view of the defined problem.

The issues highlighted in this introductory section looking at the philosophy behind fire safety shows the direction of investigation to be taken in this research. Can the continual referral to the same causal factors be the result of a ‘tunnel vision’ approach through the facets of fire

safety, which influence design (accident investigation, previous experience etc.), coupled with an inability to review systemic failures and real time drift into failure to subsequently take necessary action during operation?

2 Hypothesis, Aims and Objectives

2.1 Research Hypothesis & Methodology

Maritime machinery spaces regularly have fires from, seemingly, the same causal factors. 1) why is this the case, and 2) can the fire safety strategy be improved to eliminate these recurring fires?

The current approach to fires in machinery spaces is postulated to be reactive in nature, primarily focusing on detection of already materialised hazards (including leaks and hot surfaces (62) at the point it may be too little too late), ignition or explosion itself. It is also postulated there is a primary focus on dealing with individual safety barriers in isolation at the sharp end with little consideration to the overall system of safety control including the interactions between humans, technology, and the environment.

It is hypothesised these fires continually occur through systemic failures (particularly in the preventative aspect of fire safety) not being addressed in design and operation. This hypothesis portrays systemic uncertainty/ causal factors may not be fully addressed when applying traditional methods of Hazard Identification (HAZID) and operational auditing which has led to fire remaining a prominent risk to maritime operations.

To test this hypothesis, it is predicted that if a structured fire safety approach is implemented which accounts for interaction between humans, technology and the environment across the entire prevention and mitigation spectrum, opportunities for improvement in machinery space fire safety will present themselves. These improvements may take the form of strengthening existing safety barriers by addressing factors not considered when such barriers are placed in isolation with no consideration of context, or perhaps new/ alternative barriers will be discovered which will improve fire safety.

Should the hypothesis be proven valid, the societal implication could be significant. Everyday life in the 21st century involves the interactions between humans, machines and the

environment, and this trend is only increasing. Against all odds, if society can do the unthinkable by eliminating fires in engine rooms (ERs) by analysis of the system, accounting for such human/ machine/ environmental interactions, while structurally removing the potential systemic routes to failure, there is no limit to previously perceived unavoidable hazards being removed from society in our everyday lives/ business ventures where we continually live with ‘acceptable risk’, which could in the future become ‘unacceptable’. Such industries which could benefit from such an approach include but are not limited to aviation, finance, medicine, and business. Let us use business as an example.

It has been observed in business innovation that where a company has an idea, develops this idea, and brings it to market in isolation, they can find there is no market for the resultant product. This could be comparable to placement of oil mist detectors in engine rooms, as oil mist is a precursor to fire. While this will (hopefully) detect the oil mist, it does not address the fundamental functional requirement of preventing the leak in the first place.

Companies with more structured approaches to innovation, who start with a customer segment and analyse the ‘pains’ and requirements of those working in that segment (in their specific context), reap the rewards (63, 64). This would lend itself to an approach of focusing on the problem of fire philosophically to develop solutions which prevent the systemic precursors to fire in the specific context of that environment and control structure.

While business may not realise it, this is a systematic approach to business growth. Such approaches may not explicitly call out control and feedback loops, contexts, environmental influencers etc. but it is a structured approach to solving a problem using functional requirements to propose a barrier (or product) to help the customer achieve success. To be successful in its application, tools are developed to guide the business through its application. It is therefore the intention of this research to develop a methodology to allow facility operators which contain a fire hazard to be able to apply a structured systemic approach to fire safety barrier implementation and management, with impact in the application of this State of the Art

(SOTA) in HAZID to a new application, and academic/ industrial novelty in directly linking the systemic HAZID to the operational phase of the lifecycle.

To fulfil the requirement of the method proposed in demonstrating the hypothesis and testing it, a series of research objectives are set.

2.2 Research Objectives

The research aims to reduce the epistemic uncertainty through a structured approach to hazard analysis of the wider socio-technical system responsible for the fire hazard and its precursors. Epistemic refers to the presence of knowledge. Uncertainty with respect to knowledge refers to the lack of accurate or adequate feedback, which will subsequently lead to inaccurate or inadequate control actions, and progress towards a failure. Improved certainty surrounding causal scenarios will be used to enhance modern fire prevention technology from design to operation. Should the method applied provide a benefit and expand on the SOTA in fire safety, the methodology will be developed and presented to allow the approach to be applied in a wider environment during design, operation, and crucially to provide a bridge between the two.

To achieve this aim, the following research objectives are set:

- Objective 1: Investigate the extent and nature of fires in machinery spaces
- Objective 2: Present a review of the current approach and SOTA in fire safety in ship machinery spaces to establish a potential area for improvement
- Objective 3: Present a methodology of structured analysis of the system and subsequent safety barriers (or the absence of such barriers) and their performance requirements which could be a significant influence on systemic fire safety, with a view to strengthening such barriers in design and operation

- Objective 4: Develop the methodology, allowing access to the structured systemic approach in the specific area of interest and also to a wider audience
- Objective 5: Validate the method can be used to provide effective improvements in systemic fire safety through barrier analysis
- Objective 6: Consider any improvements or future opportunities using the method

The following table shows the chapter outline with a confirmation of the objectives which are addressed within that chapter.

Table 1: Research objectives

Chapter	**Objectives**					
	1	**2**	**3**	**4**	**5**	**6**
Chapter 1: Introduction and Motivation	X					
Chapter 2: Hypothesis, Aims and Objectives	N/A					
Chapter 3: Critical Review	X	X				
Chapter 4: STPA: A Novel Structured Approach to Fire Safety			X			
Chapter 5: Application of STPA on a Cruise Ship Engine Room			X	X		
Chapter 6: Validation of the STPA and Proposed Approach			X	X	X	
Chapter 7: Systemic HAZID and Operational Risk Evaluation (SHORE) Application				X		
Chapter 8: Conclusions and Future Works						X
Chapter 9: Wider Academic Contribution						X
Chapter 10: Limitations	N/A					

2.3 Approach to Define the Current Method

The research must first determine the focus of the current method of achieving fire safety, the approach of which is detailed in this chapter. The research will identify the bias, if any, of the primary facets of fire safety, specifically:

- Current safety rules and regulations (IMO1, Classification Societies, Administrations).
- Studies of formal safety assessment (FSA), i.e. recommendations for new safety rules.
- Accident investigation (sample of recommendations from recent investigations).
- Technology currently aimed at fire safety, Dynamic Barrier Management (DBM)

The biases are determined by classifying the safety strategies within each constituent of fire safety in sub-categories of prevention and mitigation, as shown in Table 2 and Figure 2. It is important to note that while the analysis focuses on fire safety onboard, fires in machinery spaces is of special interest due to the volume and repeatability of fire incidents here.

Omitted from the analysis is an examination of the current 'best practices' which may be applied by individual companies which are used in conjunction with the rules applied from regulatory or governing bodies. Also excluded from the analysis are underlying factors which may still have an impact on fire safety, for example the effect of political pressures, global economy, any assumptions behind FSA implementation or results etc.

2.4 Classification

Prevention and mitigation form the two primary strategies associated with loss prevention, but they can be subdivided into more specific, and hence useful, sub-categories. It is important in the context of this research that the commonly used terms of 'accident' and 'incident' are defined. An accident is defined as an unforeseen event that develops to result in serious consequences/ losses (property damage, injury, fatalities). An incident is an unforeseen event resulting in minor consequences, but which could escalate to an accident (65).

In developing a method of categorisation for safety barriers in the following critical review, I look to the literature. Hollnagel provides five possible strategies for loss prevention (65),

[1] International Maritime Organisation (IMO)

namely replacement (failed component, subsystem etc.), prevention, facilitation (e.g., simplification or redesign of a task), protection (as means of mitigation or recovery), and elimination. Leveson et al. go one step further and propose the impact scale for hazard mitigation strategies (42). They suggested similar categories for safety strategies: elimination (impact level 4), prevention (level 3), control (level 2), and damage reduction (level 1). By "control", the authors refer to reduction in the likelihood that the hazard results in an accident, i.e. the incident develops into an accident. Damage reduction would be mitigation of the consequences when the accident (ignition) occurs. The assignment of the impact level reflects the logic described earlier in the introduction, e.g. the elimination has the biggest impact because it removes all opportunities for damage. Thus, the bigger the impact with respect to loss prevention, the greater the strategy's effectiveness. This approach has been applied in other recent work (25) and is adopted in this method of categorisation to provide a guide to the effectiveness of the current approach once it is established.

For the analysis to be more informative, I classify the prevention category into four sub-categories, focusing on eliminating a hazard, preventing systemic, contributing, and direct causal factors, as shown in Table 2. These subcategories correspond to Johnson's three-level model of accidents, which assumes that systemic causal factors give rise to contributing factors, which in turn, allow the direct factors (a.k.a., proximate or immediate events) to trigger an incident (66).

With respect to the level of effectiveness (E), we introduce the linear scale of effectiveness such that E can be reflected explicitly - as opposed to being used tacitly (25, 26) (Table 2). I assume basic increments of increased effectiveness ranging from 1-6, with the strategy for hazard elimination having the greatest effectiveness (E=6), ranging to the lowest effectiveness level of damage limitation (E=1), where consequences are difficult to predict, and we are in the so called 'last line of defence'. It is important to note, elimination may not always be possible (e.g., replacing flammable materials in the engine which requires combustion) but is included as a strategy for consistency.

It is noted there is a cost implication on the strategy developed and applied, however this is out with the scope of the initial analysis here. Some notes on perception around cost effectiveness are provided, however, in the critical analysis.

Table 2: Strategies for loss prevention

Focus	Strategy category	Safety function	Example barrier systems	Effectiveness level (priority scale) (E)
Prevention	1	Eliminate hazard	Decisions at concept and detailed design stages (based on risk assessment, tests, and other studies): substitution, simplification, decoupling, replacement, etc.	6
	2	Prevent systemic factors of incident	Strong safety culture, effective inter-organisational links, industrial best practices, robust safety assessment methodology, flawless standards and practices and regulatory oversight	5
	3	Prevent contributing factors of incident	Safety management system (SMS), clear communication and responsibilities and roles, crew training and supervision, adequate manning, fire drills	4
	4	Prevent direct factors of incident	Passive and active safety systems (thermal insulation, leak prevention, condition monitoring, etc.), and their inspection and maintenance actions	3
Mitigation	5	Control accident (stopping from propagating to loss)	Management decisions (training, staffing, preventive maintenance etc.), automatic detection and suppression systems, emergency shutdown, ventilation control system etc.	2
	6	Reduce damage (loss)	Management decisions (training, staffing etc.), containment (structural fire protection, fire doors etc.), automatic and manual firefighting equipment and preparedness, evacuation equipment and preparedness	1

In cases where a specific safety measure (e.g. a fire suppression system) fits into more than one safety category (e.g., fire safety technology, which applies to damage reduction and incident control), it will be assigned the effectiveness value of the most effective category, thus rewarding the benefit of an earlier approach.

Table 2, and hence the results, can also be mapped to a 'bowtie' diagram (67-69). The bowtie reflects the progress towards an incident and as this analysis of effectiveness directly applies to the timeline of when the controls are implemented, where the strategy sits on the bowtie provides a visual reflection of the effectiveness. While the bowtie can hide complexity as it does not contain information on barrier type or system (Physical, Functional, Symbolic, Incorporeal), or account for systemic factors (i.e the interactions between various system actors), the initial analysis here simply verifies where the focus sits and does not deal with specific barriers such as those presented by Saleh (70). The bowtie therefore serves as a means of communicating barrier categories along the timeline of events. This assists in this analysis, presenting where the focus lies with respect to fire safety. The accuracy of the bowtie as a risk analysis method is not in the scope of this research and is solely applied as a visual representation on where the categories from Table 2 would sit.

Figure 2 shows this generic representation of the bowtie, with preventative measures applied to the left of the centre and mitigating factors, post ignition, carried out to the right.

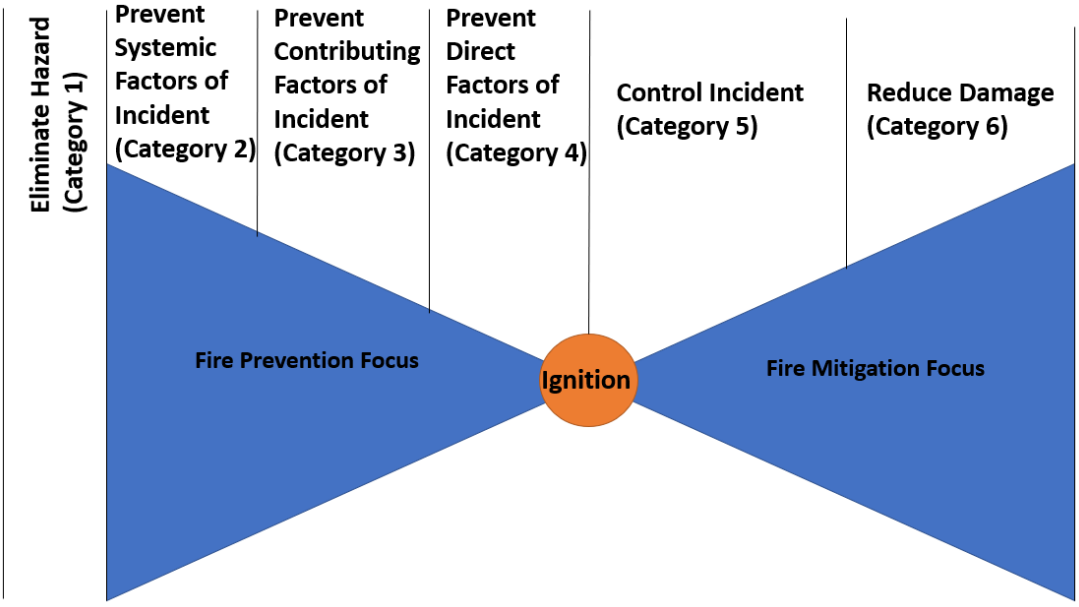


Figure 2: Focus on prevention/ mitigation

As I map the discrete category intervals from Table 2 onto the bowtie, I implicitly assume that the effectiveness is continuous and decreases linearly from the left to the right within each interval. Thus, improvements in safety barrier systems at the boundary between Category 4 and 5 (e.g., smoke detection and early fire suppression) would be more effective, and hence preferable, than those between Category 5 and 6 (e.g., emergency shutdown).

The following critical review will apply this method to categorise the background research in determining the current focus of fire safety and what SOTA looks like. This will allow the thesis to set out the hypothesis based on where the focus lies, where the gaps lie (if any), and subsequently set out the methodology in which to test this hypothesis. The critical review allows effectiveness to be evaluated against the hypothesis of current fire safety effectiveness and provides the platform for an alternative approach to be investigated if required based on any gaps which are discovered.

3 Critical Review

3.1 Introduction

The following review will analyse the current approach to fire safety in marine machinery spaces. Initially I present a brief overview of the current accident models and hazard analysis techniques, followed by how safety rules and regulations, Formal Safety Assessment (FSA), accident analysis and investigations, and fire safety systems all contribute to the current approach. An analysis of the effectiveness is then presented, with additional notes on perceptions around cost effectiveness between prevention and mitigation. The role of auditing in the operational phase as a tool of implementing design decisions is also presented. This will provide a snapshot of the SOTA regarding fire safety and identify the gaps which exist in fire safety to be addressed in this thesis.

3.2 Historical Accident Models

Before analysing each facet of fire safety, the various historical accident models will be reviewed, with a brief overview of traditional methods up to the SOTA in HAZID and risk analysis.

The two prevalent traditional methods of accident model are sequential (i.e. domino effect (71)) and epidemiological (i.e. swiss cheese (72)). Sequential models would treat the problem of incident occurrence as one failure leading to another, leading to another and so on, thus the analogy with the domino effect. Epidemiological models, however, would incorporate latent failures into the model. Epidemiological models maintain a similar ‘trajectory’ as sequential models, in the sense an arrow of direction and linearity remains present and fundamental in their application.

The epidemiological approach first put forward by Gordon in the 1940s suggests that accidents are caused by random interactions between the agent (energy), the environment and the host

(victim). While this was intended to look at disease, it was determined as pertinent in looking at accidents also. This, as with most other hazard analysis and identification techniques, applied a reactionary approach to risk.

Qureshi (43) concludes that neither of these models are adequate in the analysis of complex modern systems.

With respect to the design and review of safety systems, multiple risk/ accident models have historically been applied, with those previously discussed traditional models remaining prevalent in the marine industry. For example, in recent analysis by EMSA, which attempts to classify accident precursors, a traditional cause/ effect model is applied within its first Appendix (73). These models consist of sequential and epidemiological models (including LOPA/ swiss cheese models etc.). More recently, systemic based models have risen in prevalence in adjacent industries such as military and aerospace applications (43, 74), but are yet to be applied in mainstream marine based risk analysis. This is despite such an approach, using STPA for example, showing some evidence of higher effectiveness in reducing likelihood of an incident occurring (25). The following figure shows a representation of the traditional (sequential and epidemiological) and SOTA (systemic) risk analysis techniques.

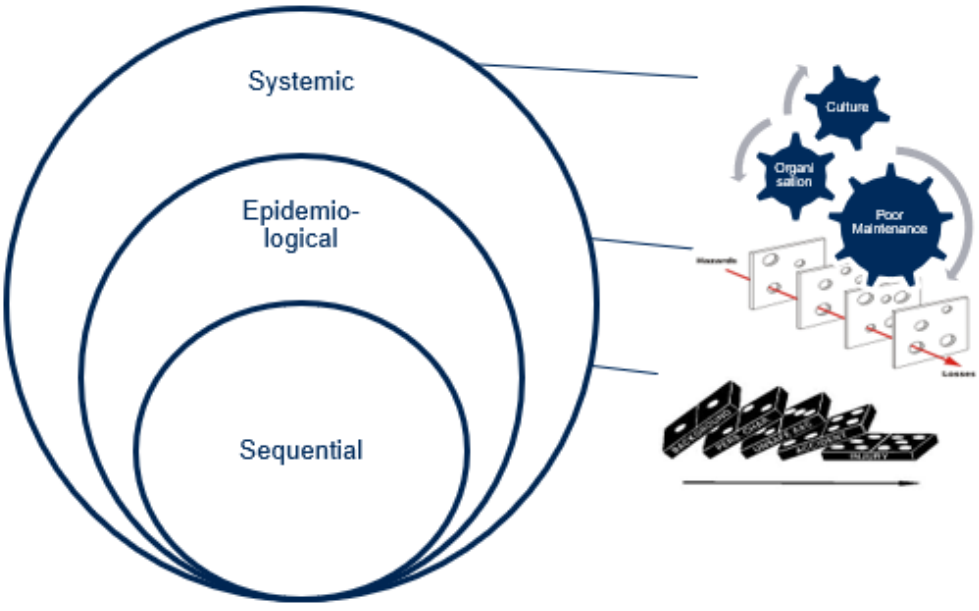


Figure 3: Historical risk models

When reviewing accident causation, it is important to consider the complexity in the context and factors which lead to an incident. For example, there may be eight causes of a hazard, and when all eight causes are present together, the hazard is realised. It may be the case, however, that cause 1 and 3 together will result in the same hazard as causes 2, 4 and 6 together. How can a hazard identification and analysis approach consider such combinations for a complex system accounting for the interactions between humans, technology, and the environment?

Consider a systemic causal factor where incident A may result in B, but incident B does not require A to occur. Vehicle accidents as a result of drink driving are a prime example of this. Driving while under the influence of alcohol does not always result in an accident, but it is a potential cause (75). It is therefore important that causal factors are considered for all unsafe control actions which may be taken. For a control action to be unsafe, the context must be relevant for that action to become unsafe. By understanding these contexts and actions, causal scenarios can be identified and eliminated.

When reviewing the cause and effect based analysis applied in traditional hazard analysis, evidence shows these analysis typically start from commonly known failures (76), as seen in the marine industry with failures such as a release of oil mist contacting a hot surface. Goerlandt and Montewka (77) state that calculations of probabilities typically come from observed frequencies. As these traditional models do not address the entire socio technical context, dealing with the interactions between humans, technology and the organisation, it is challenging for them to address lagging failures interacting with one another (78) which may occur further left on the bow tie, or higher up in the control hierarchy.

Qureshi (43) critiques historical risk assessment methods in not keeping up to speed with technological advances and the fact that the causes of modern disasters are different from historical events and therefore to prevent future events we need to develop a new method of risk assessment, such as the systemic techniques proposed by Leveson (79).

In reviewing the limitations of the traditional approach to safety, Schröder-Hinrichs et. al. (80) discuss the analysis of 41 accident investigations relating to fires/ explosions in machinery enclosures. The results show that considering the expectations of the IMO guidelines with respect to accident investigations, organisational factors were not adequately addressed. Their findings show that a large percentage of the stated accident causes related to technological failures and failed physical safety barriers. This critique highlights the limitations in looking at proximate events and fire propagation, and notes that failures further left in the bowtie may not be being highlighted using the current approach. The findings are further examined by Rollenhagen (81) who demonstrates there is a lack of attention to the organisational context in which an accident investigation is taking place.

With accident investigations and historical occurrence heavily influencing the traditional methods of risk analysis, the EMCIP platform, managed by EMSA is an important resource. This rests on the cognitive reliability and human error analysis method CREAM (82), whereas the casualty analysis methodology behind the EMPIC was developed under project CASMET (83), which integrated human and organisational errors in the accident analysis. The CREAM, however, is currently considered obsolete as it would focus solely on one ‘component’ of the system, i.e. the human, and be based on the theoretically vacuous concept of human error (84). Equally, the EMCIP aims to classify and tabulate the causes as discrete events arranged sequentially, i.e. with direct links between causes and effects, as assumed in sequential and epidemiological accident models (43). Consequently, the summary statistics on accident causes in the EMCIP is limited to proximate events such as “human erroneous actions”, followed by the “equipment failure” as the second direct cause behind the incidents and accidents (85). The recommendations would then be aimed at strengthening the failed safety barriers (65), i.e. by new or stricter procedures, failure prediction, detection and control systems, redundancy (failsafe) etc., which would subsequently influence the future fire safety designs using traditional sequential and epidemiological analysis.

As an additional point to note, in the report of their eighty seventh meeting (86), the maritime safety committee noted that novel designs with very little historical accident data in which experts could rely on, should use a first principles approach in FSA. This would infer that for applications where historical data is available, a first principles approach is not required, and yet similar accidents continue to occur. The problem has not been solved, but rather has been accepted. It would therefore be of benefit if a method of applying the SOTA approach in hazard identification and analysis could be applied retrospectively to increase safety, without a significant cost implication of altering the safety barriers already in place. The approach would simply strengthen the existing barriers, where traditional methods may neglect this operational criticality. One aim is that the work demonstrated in this thesis helps along this route.

Now, however, the thesis will analyse the current approach to fire safety in the marine industry by reviewing the primary facets of fire safety, starting with safety rules and regulations.

3.3 Safety Rules and Regulations

In 2001, the IMO released Guidelines on Alternative Design and Arrangements for Fire Safety (87, 88). This document lays out the method by which engineering analysis can be carried out in complying with the performance-based fire safety requirement of SOLAS Chapter II-2. The guide refers to examples such as the SFPE Engineering Guide to Performance Based Fire Protection Analysis and Design of Buildings (89). This guide discusses implementation of inherently safer design and verifies that building design will function as intended in the event of a fire, starting from the assumption of fire presence, rather than focusing on the prevention of a fire in the first instance. The focus is therefore more strongly placed in the mitigation phase of fire incident control (Categories 5 and 6), detecting fire early and protecting the ship against propagation of the event.

In 2009 the IMO produced a document intended to harmonise the design practices to reduce fire in high risk areas on ships in the Guidelines for Measures to Prevent Fires in Engine Rooms and Cargo Pump Rooms (62). Particular attention was given to the lifecycle of areas

which process flammable oils. The guidance aims to remove as far as possible the fuel from the fire triangle, providing recommendations like applying spray shields, applying jacketed piping systems where high-pressure streams exist etc. Also covered is the protection of hot surfaces where a flammable material may be present. The focus of this is clearly fire prevention, as the strategy focuses on preventing the propagation of precursors from developing into an accident. This would be classed as a prevention-based focus in Category 4 with respect to Table 2. These recommendations are also included in SOLAS Chapter 2, Regulation 4 (90), calling for the means to control leaks of flammable liquids, limit the accumulation of flammable vapours, restrict combustible materials, restrict ignition sources, separate ignition sources from materials which would ignite, and to eliminate an explosive atmosphere in the cargo tanks.

The IMO's Guidelines on implementation of the International Safety Management (ISM) Code (91) is intended to be an international standard on safe operation and management of ships. The code mandates a Safety Management System (SMS). The main, but not sole, focus of the Code is the control of hazards where possible, accounting for human factors, and the prevention of incidents through improved safety management and operations (Categories 2 and 3 respectively). The ISM code also covers emergency preparedness which can contribute from the moments of ignition through to damage limitation, which covers Categories 4-6. This shows a broad focus of the ISM Code from Category 2 - 6.

Regarding guidelines available in reference to specific technologies in relation to fire safety, the IMO Fire Safety Systems (FSS) Code (92) was put in place to advise on strategies of incorporating fire detection and protection systems. This is another indicator of where safety rules and regulations focus, specifically on detection at the right of centre of the bowtie. The document discusses application of technologies used in the mitigation of ignition, principally falling under Category 5.

Another document with a similar focus is ISO14520-1:2015 providing guidance on gaseous fire extinguishing properties and design (93). The intent of the document is to maintain a minimum standard of extinguishing practices and, therefore, shows the mitigation focus of the guidance. It is credible that such systems could be used to cool exposed hot surfaces and therefore be a preventative measure in cooling the hot surface (such that if flammable material is released it will not contact with an exposed high temperature surface causing the ignition), but this is not the primary intent of the guidance, therefore it is assigned as a Category 5 fire safety guide.

Functional safety guidance can be applied in preventative efforts for applications such as ship engine rooms, despite being primarily focused in the process sector (94). This guidance focuses primarily on the reliability and design of safety instrumented systems which can be used to detect accident precursors and prevent failures. This is of relevance in engine room fire prevention with machinery failures presenting a notable precursor to fire. This guidance focuses within Category 3, although does branch into probability of incident detection which moves into Category 4. The document also provides guidance on the elimination of systematic failures during design, and the importance of risk assessment in the elimination or control of hazards. This provides us guidance focused in Category 2.

The IMO (95) also provide guidelines on evacuation analysis on passenger ships which, although relating to a multitude of safety issues, presents a significant mitigation function in the case of a fire - the removal of humans who could be harmed. This guidance therefore falls within category 6, relating to the reduction of losses.

According to Lloyd's list (96), the top four shipping classification societies in 2017 were DNVGL, ClassNK, ABS and Lloyds Register. When analysing Class requirements, these societies shall be analysed with respect to the guidelines available from them (97-102).

The DNVGL rules and guidance provide a reference directly back to SOLAS Chapter 2. Fire prevention measures are limited to those covered under this SOLAS reference. Beyond this,

there are specific requirements with respect to preventing oil leakage and ignition from exposed hot surfaces, structural requirements, fire suppression/protection requirements and means of escape, clearly focused on Categories 4-6 from Table 2.

The guidance provided by ClassNK focuses very much on fire control. The guidance presented on integrated fire control systems focuses on detection of fire, and ventilation systems to control smoke - Category 5 recommendations. The document, however, does discuss countermeasures to prevent ignition from releases of flammable materials, falling under Category 4.

ClassNK also present guidance on fire protection systems, of which reference is provided to the IMO guidelines on the maintenance and inspection of fire protection systems and appliances (MSC.1/Circ.1432 and MSC.1/Circ.1516) which are stated as ClassNK's minimum guidelines. The document includes a chapter on probability of ignition, where control of hot surfaces and releases of flammable materials are discussed, providing Category 4 recommendations. This chapter is, however, followed by 21 chapters specifically related to mitigation measures including fire detection, suppression and means of escape - Category 5 and 6 recommendations. While focus exists on preventative measures, most of the class rules relate to mitigation measures related to fire falling under Category 5 and 6 guidance.

American Bureau of Shipping (ABS) presents guidance on the extinguishment of a fire and presents various classifications of fire for consideration when designing the overall protection system. The main bulk of the guidance focuses very much on fire suppression requirements including guidance on fixed gas, water and foam fire extinguishing systems, falling under Category 5 recommendations. The guidance does, however, contain additional fire protection requirements which could be classed as preventative, when it discusses the segregation of hot surfaces and flammable materials, separation of pressurised processes, material requirements to avoid ignition and insulation of hot surfaces which could present an ignition source - Category 4 recommendations.

The guidance provided by Lloyd's Register details fire safety related factors such as active fire protection systems, structural protection, emergency shutdown measures in the presence of fire, and fire response measures. The guidance provides focus on reviewing how fires will escalate and what barriers are adequate in fire containment and mitigation, falling under Categories 5 and 6.

From the analysis it is apparent that the regulations and class requirements guide towards both prevention (Category 2-4) and mitigation (Categories 5 and 6). It is notable, however, that the preventative attempts are those which are principally reacting to a failure which has already occurred in the most part, e.g. a release of flammable oil, as opposed to the prevention of such failures in the first place. In the case of machinery spaces, failing to account for earlier prevention of precursors to those incidents could explain most fires being caused by the same direct causal factors, which the regulations and class rules aim to prevent/ mitigate at the sharp end.

Guidance relating specifically to fire safety, as discussed in this section, is somewhat separate from inherently safer design of machinery (i.e. Categories 1-4), for example, which is in place to prevent some of the events which could lead to fire (i.e. break in containment). Documentation addressing loss prevention in machinery spaces, although not specifically specified for the marine industry, includes BS EN ISO 12100:2010 (103), which provides guidance in complying with the Machinery Directive 2006/42/EC of the European Parliament and Amending Directive 95/16/EC (104), within which seagoing vessels are excluded. The guidance and directive discuss factors that designs should take account of and have been known to contribute to fires in the past. As this is generally left to previous experience or knowledge of what has gone wrong before, this emphasises the importance of accident investigation during design, which will be addressed later in this review. It also highlights the potential importance of a move towards a systemic based hazard identification method which addresses the entire scope of prevention and mitigation.

3.4 Formal Safety Assessment (FSA)

In the aftermath of the Piper Alpha disaster in 1988, a review of the safety regime and practices was triggered towards a more systematic (scientific) and proactive approach for their development, in view of established practices—such as probabilistic safety assessment—in nuclear, aeronautic and other industries. In 1993 the UK Maritime and Coastguard Agency (MCA) submitted a five-step procedure for safety analysis called Formal Safety Assessment (FSA) (11), with the IMO adopting interim FSA guidelines and starting trials in 1997. FSA is generally accepted in the industry now. Initially intended for IMO committees and maritime administrations, it is now used by classification societies for development of classification rules (32).

The FSA guidelines outline a systematic process of assessing different risks and risk control options (RCOs) or safety barriers (67), and provide guidance on cost benefit analysis of RCOs (11, 105). The FSA process fundamentally implies the quantitative assessment of risks and safety barriers through the probabilistic framework. The quantification of risks is essential for cost benefit analysis, i.e. determining if a proposed RCO is cost effective with respect to a quantitative criterion. If this can be taken as the current method, as stated by Goerlandt (5, 77), its focus can be determined by reviewing its results, i.e. the proposed safety barriers in the context of fire safety in machinery spaces.

This thesis investigates the FSA carried out as part of the SAFEDOR project (106). The assessments focused on cruise ships and Ro-Ro passenger ships (107, 108). Another recent source where the FSA process has been applied is the FIRESAFE project (109). The project was aimed to develop safety barriers against fires on Ro-Ro passenger ships, with exclusive focus on vehicle decks. Although the focus was not on machinery spaces, I argue that the study is indicative of the current approach to fire safety and hence is useful for this analysis. This FIRESAFE project was followed up in 2018 with FIRESAFE II (110), the results of which are also presented.

The proposed RCOs across the three studies include the installation of oil mist detectors, monitoring of hot surfaces, electrical connection boxes, use of ship cables and adaptors, IR cameras etc. (Category 4 recommendations), along with Category 5 and 6 recommendations including rolling shutters, freshwater activation, CCTV systems and evacuation optimisation systems. The only preventative finding in categories 1-3 related to training, to increase awareness - a category 3 recommendation.

Table 3 highlights all RCOs recommended on Cruise Ship applications under SAFEDOR, and RoRo passenger ships under both FIRESAFE projects (FIRESAFE I and II RCOs are noted as FS). Titles of RCOs have been extracted directly from the reports, so any ambiguity of title is carried forward. Grouping has, however, been determined based on the RCO descriptions. Where RCOs are applicable to more than one category they are listed multiple times.

Table 3: Risk Control Options (RCOs) recommended (106) (109) (110)

Focus	Safety function	Risk Control Option (RCO)
Prevention	Eliminate hazard – Category 1	• -
	Prevent systemic factors of incident – Category 2	• -
	Prevent contributing factors of incident – Category 3	• Training for awareness (FS)
	Prevent direct factors of incident - – Category 4	• Installation of oil mist detectors • Temperature monitoring (of hot surfaces?) • Key-card system to turn on el-system in cabin • Mandatory FM-Class • Laundry exhaust ducts • Correct maintenance in Engine Room • Stricter smoking procedures • Robust connection boxes (FS) • Only ship cables (FS) • IR Camera (FS) • Only crew connections (FS) • Use of cable reeling drums (FS) • Correct maintenance in Engine Room

Mitigation	Control accident (stopping from propagating to loss) - Category 5	• Better emergency training of crew • Automatic shutdown of fryers • Open decks fire detection and suppression • Combustible material requirements* • Mandatory FM-Class • Combined heat & smoke detection (FS) • Remote control (FS) • Rolling shutters (FS) • Efficient activation routines (FS) • Fresh water activation/ flushing (FS) • CCTV (FS) • CCTV & remote release (FS) • Increased frequency fire patrols (FS) • Alarm System Design & Integration (FS) • Preconditions for Early Activation of Drencher System (FS) • Fire Monitors on weather deck (FS)
	Reduce damage (loss) - Category 6	• Better emergency training of crew • Self-illuminating lights • Evacuation notification system • Outdoor stairways • Regard sundeck as a public space • Distance to mustering area/ open deck • Ventilation systems in corridor • Combustible material requirements* • Ban / closure of side & end openings (FS) • Improved markings/signage for wayfinding and localization (FS) • Safe distance (FS)
*This has been placed in both mitigation categories as the combustible material requirement description is not fitting of preventing an ignition, but rather preventing spread of a fire throughout the ship and limiting the damage a developed fire can cause.		

Aside from analysing the focus of the current approach, to facilitate the debate around cost effectiveness comparisons between mitigation and prevention, the thesis also aims to adduce evidence against the belief that mitigation is currently the prime cost effective focus of safety

efforts. The evidence essentially summarises the-state-of-the-art in the development of risk control options (RCOs) and their assessment of cost-effectiveness. The thesis uses official FSA reports and other studies to source specific RCOs and their assessment results to compare the cost-effectiveness of proposed prevention and mitigation measures. Since the FSA process can be taken as the current method for identifying RCOs and determining their cost effectiveness (77), the result of FSA is important evidence of what category of RCOs tends to be more cost-effective based on the objective criteria.

On the subject of RCO cost effectiveness, two measures of cost-effectiveness (CE) can be applied: gross cost of averting a fatality (GCAF) and net cost of averting a fatality (NCAF). They can be expressed as the ratios of the cost (gross or net) incurred per ship lifetime after implementing an RCO to the corresponding reduction in the societal risk per ship lifetime. For an RCO to be cost-effective its GCAF and NCAF must be below some upper limit. NCAF values, however, should be used with care as they can fall below the limit even though the reduction in risk is negligible. This can happen when the benefits of implementing an RCO outweigh the costs; such RCOs should not generally be considered as risk reduction measures, but merely as design improvements. The upper limit is determined based on the willingness-to-pay to avert a fatality, past decisions and the costs involved, consideration of societal indicators such as the life quality index (LQI), and other aspects (111, 112). The limit is not static and might need to be updated before each use. For instance, it in 2007 the value was 3M USD (e.g., FSA MSC 83/21/1). Ten years later, the value was adjusted to 7M Euro (~7.7M USD) (5).

The application practice of FSA, however, has not been without difficulties (113-116). The raised issues are related to the overreliance on historical data and expert opinion, confusion of frequencies for probabilities, uncertainties in both risk and financial components, shallow assessment of interactions between combined RCOs and their effect on the joint cost-effectiveness. The diversity of the proposed preventive RCOs can be rather poor. As pointed out by Yang et al. “some consequences such as collisions and groundings have been

considered as initiating events in FSA studies, which results in the focus of RCOs shifting from risk prevention to risk mitigation. The development of ‘higher level’ events (i.e. root causes) leading to the occurrence of consequences should be emphasised in FSA studies, particularly in the establishment of casualty databases with more detailed root cause information” (113). In other words, the proposed RCOs were essentially limited to safeguard against proximate causal factors at the sharp end. There is, however, a wide array of prevention alternatives that could have been found when analysing the safety control system at the company level and beyond, e.g. (117). Sometimes, just ensuring adequate communication between ship designers and ship operators can be the easiest and most cost-effective alternative (118). A structured approach to analysing fire safety at all levels could present a solution to avoid such failings.

A notable critique, which is attributed to QRA in general, is the assumption of event independence of basic events in fault trees, e.g. (109). However, should this assumption turn out to be false, it would open the way for common-cause failures (119). A review of 609 aviation accidents found that at least 11% of them were caused by common-cause failures (120). There is no basis to assume a lower rate in the maritime sector, given lower levels of standardisation and much shorter development times. The assumption of independence can also lead to so-called Titanic coincidence (121), when many low probability events are multiplied to estimate the top event probability. This results in a negligible probability of the top event, which is then discarded as impossible or cost-ineffective to attend to.

It is also worth noting that the FSA guidelines suggest using the human reliability analysis to quantify human errors. A human action is typically classified as the human error in the aftermath of an accident when that action is found to have been in breach of safety procedures. However, many examples demonstrate that violating safety procedures was necessary to actually maintain safety (39). Consequently, such ‘violations’ would not be considered as errors should they avert an incident. In other words, human error is a product of the hindsight bias and is a psychological construct but not an objective or technical one (122, 123, p. xvii).

Hence, determining the frequency of human errors, as suggested by the FSA guidelines (11), becomes essentially useless. Further, people do their best, hardly behave randomly, and make decisions based on the circumstances they are in (124). This means that the same circumstances will make people consistently produce a similar output. Of course the chance to unwittingly deviate from the pattern exists (e.g., due to health issues), but it is negligible and can be ignored in most cases. Therefore, it is clear that assigning a probability to human errors is inappropriate, unless the context that directly affects human action is random. This therefore presents a problem in quantifying fire risk using probability models, as humans are highly likely to be involved at some stage in the ignition. A better approach therefore would seem to be accounting for the interaction between humans and their environment and technology and placing barriers which account for this interaction in the varying contexts which could result in a ‘human error’, rather than placing barriers and making assumptions based on probability to determine safety.

An analogous treatment is applicable to software, which is becoming ubiquitous on modern marine systems. Software failure is a misnomer, for software does not fail but does precisely as it is told in the specification (125). In other words, for the same input, the software will always produce the same output. Consequently, assigning a probability to this deterministic phenomenon is ill-advised. In contrast to human behaviour, software will never deviate from the specification. However, this often advantageous property can turn out to be hazardous when the specification appears to be wrong (126).

The above frailties of the FSA make the comparison of RCOs against any quantitative criteria precarious. The fact that confidence bands are not normally given in FSA results and generally in QRA studies (127) is unhelpful. Even when the corresponding analysis is undertaken (128), it is too simplistic to address the issues highlighted above. Therefore, the comparison should not be strictly based on obtained numbers, so to speak, but also consider wider, possibly unquantifiable, knowledge. To paraphrase Albert Einstein, what is important may not be measurable and what is measurable may not be important.

In addition to the aforementioned FIRESAFE and SAFEDOR projects, there are other FSA-based studies found in the academic literature. Thus, Akyildiz et al. presented FSAs on cargo ships and fishing vessels (129, 130). The authors deal with both flooding and fire risks, analysing many RCOs for prevention and mitigation. Lois et al. reported on an FSA of fires on cruise ships (131), offering nine preventive and seven mitigative measures. Guarin et al. studied the cost-effectiveness of two high-level RCOs against the risk of flooding (132). Goerlandt et al. looked into the risks of flooding and environmental damage by studying the effect of collision prevention measures (133). Wu et al. presented a selection method for safety control options for NUC (not under control) ships, focusing on collision avoidance (134). Kristiansen offers an example of FSA application to life-saving appliances such as lifeboats and individual immersion suits (32). Table 4 lists specific reports from where the pertinent results of cost-effectiveness analysis have been extracted. Specifically, from each data source the following information was obtained:

- A list of RCOs against flooding and/or fire risks.
- Categories of RCOs: preventive or mitigative.
- GCAF and NCAF values for each RCO.
- Used upper limits for GCAF/ NCAF.
- A final list of RCOs found to be cost-effective and/or recommended for consideration.

Table 4: Data sources

Source	Reference[2]	Reference in Figure 4 and Figure 5
FSA – Liquefied Natural Gas (LNG) carriers	MSC 83/21/1, 3 July 2007	R1
FSA – Container vessels	MSC 83/21/2, 3 July 2007	R2
FSA – Crude Oil Tankers	MEPC 58/17/2, 4 July 2008	R3
FSA – Cruise ships	MSC 85/17/1, 21 July 2008	R4
FSA – RoPax ships	MSC 85/17/2, 21 July 2008	R5
FSA – Large passenger ships	NAV 51/10, 4 March 2005	R6
FIRESAFE II Combined Assessment for RoPax ships. This report presents the results of the combined assessment of cost effectiveness based on the results from the different parts previously considered separately in FIRESAFE and FIRESAFE II. Six sub-groups of ships are considered.	Version 1.1, December 2018	R7.1 - R7.6 (or R7 when to all)

Table 5 shows the data gathered from R1 to represent the information obtained from all reports, along with the nature of the RCO (mitigative or preventative), the GCAF (in USD) and whether the RCO was recommended or not.

Table 5: List of proposed RCOs in data source one

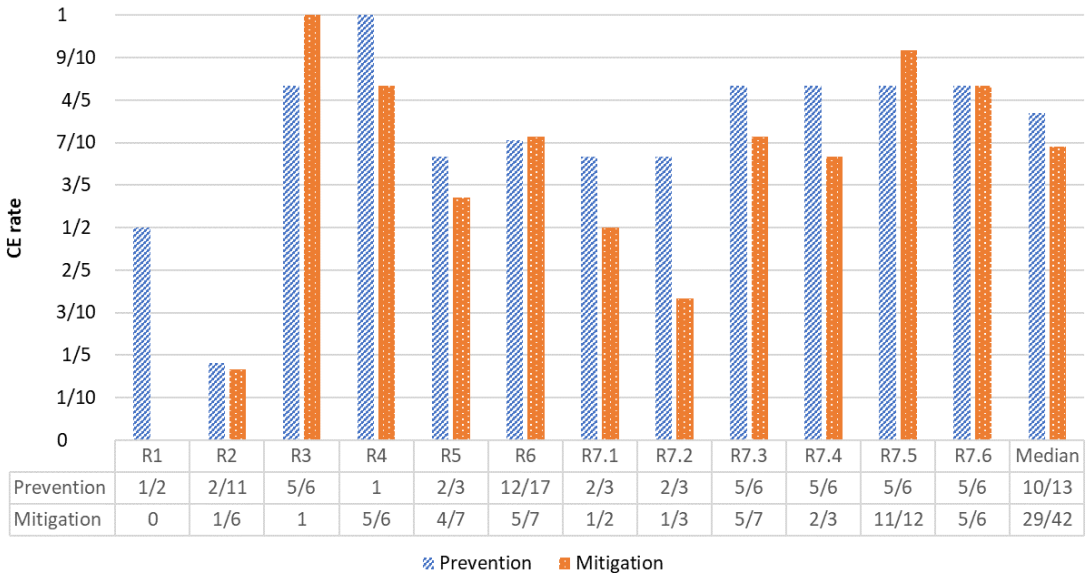
#	Risk control option	Mitigation/ Prevention *	GCAF** (10^6)	Recommended?
1	Implement risk-based maintenance of propulsion system	FLP	57.2	Y
2	Implement risk-based maintenance of steering system	FLP	7.4	Y
3	Implement risk-based maintenance of navigational system	FLP	2.21	Y
4	Implement risk-based maintenance of cargo handling system	FLP	159	
5	Implement a restriction on crew schedule to avoid fatigue of crew	FLP	159	
6	Increase use of simulator training	FLP	12	
7	Introduce a redundant propulsion system (two shaft line)	FLP	60.8	

[2] The reports can be found online (last accessed on 18/09/2019):
http://www.safedor.org/resources/index.htm
http://www.emsa.europa.eu/firesafe.html

8	Improve navigational safety: ECDIS	FLP	3.1	Y
9	Improve navigational safety: track control system	FLP	0.4	Y
10	Improve navigational safety: AIS integrated with radar	FLP	0.06	Y
11	Improve navigational safety: improved bridge design	FLP	2.3	Y
12	Increase double hull width	FLM	74.3	
13	Increase double bottom depth	FLM	59.5	
14	Increase hull strength	FLM	60	
15	Perform a periodic thermal image scanning of engine-room	FRP	28	
16	Use strain gauges for measuring stresses onboard	FRP	394.1	
17	Redundant radar sounding for filling level check	FRP	236	

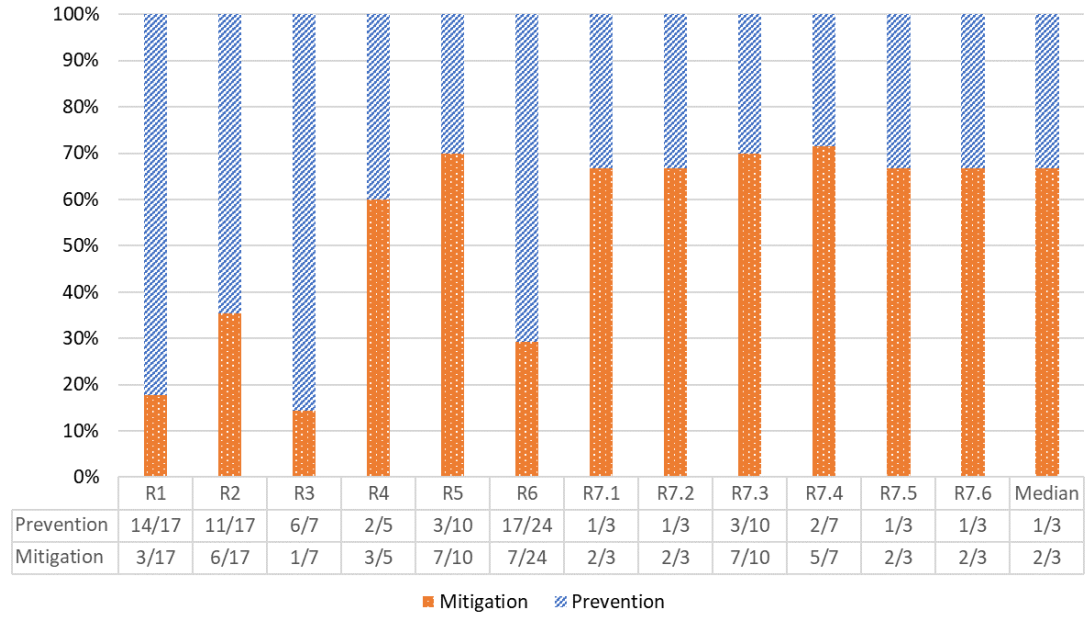
* FLP – flooding prevention, FLM – flooding mitigation, FRP – fire prevention, FRM – fire mitigation (unused in this table but present in other sources).
**GCAF units are cost (in USD) per fatality averted.

Figure 4 shows a bar chart of CE rates across all reports; the median value is also shown for guidance. The median CE rate indicates that preventive measures would “typically” be more cost-effective. However, the qualitative difference is what matters most. The proposed preventive measures tended to be more cost-effective than mitigative measures (e.g., in R1 none of mitigative RCOs were considered feasible), even though the number of mitigative RCOs considered across all reports was higher (Figure 5). Further, one can observe that in 10 out of 13 cases (including median value), preventive measures have higher or the same cost-effectiveness (Figure 4). In other words, the proposition that improving accident mitigation is more cost-effective, as opposed to incident prevention, is unwarranted, as far as this analysis is concerned. Further discussion on cost effectiveness is presented in Chapter 3.8.



	R1	R2	R3	R4	R5	R6	R7.1	R7.2	R7.3	R7.4	R7.5	R7.6	Median
Prevention	1/2	2/11	5/6	1	2/3	12/17	2/3	2/3	5/6	5/6	5/6	5/6	10/13
Mitigation	0	1/6	1	5/6	4/7	5/7	1/2	1/3	5/7	2/3	11/12	5/6	29/42

Figure 4: CE rate per data source



	R1	R2	R3	R4	R5	R6	R7.1	R7.2	R7.3	R7.4	R7.5	R7.6	Median
Prevention	14/17	11/17	6/7	2/5	3/10	17/24	1/3	1/3	3/10	2/7	1/3	1/3	1/3
Mitigation	3/17	6/17	1/7	3/5	7/10	7/24	2/3	2/3	7/10	5/7	2/3	2/3	2/3

Figure 5: Proportion of preventive and mitigative RCOs per data source

3.5 Accident Analysis and Recommendations

Accident investigation aims to understand accident causation and provides an important basis for changes in design and operational practices (8). Accident analysis, therefore, plays the key role in safety improvement. Here I and look at research into accident investigations,

followed by a small sample of recent fires in machinery spaces to provide a more detailed overview, while being admittedly a limited sample.

In analysing the current approach to safety, Schröder-Hinrichs et. al. (80) discuss the analysis of 41 accident investigations relating to fires/ explosions in machinery enclosures. The results of this study provide a broad view of where the recommendations focus. Schröder-Hinrichs et. al. conclude that, considering the expectations of the IMO guidelines with respect to accident investigations, organisational factors were not adequately addressed. Their findings show that a large percentage of the stated accident causes related to technological failures and failed physical safety barriers, focusing on causation linked to Category 4, but also failing to consider the relationship between these systems and the environment they are placed (and who may be tampering with them). The finding is further demonstrated by Rollenhagen (81) in that there is a lack of attention to the organisational context in which an accident investigation is taking place, demonstrating a lack of appreciation for Categories 2 and 3. Further evidence of a limited application of systemic causal factors in accident investigation is shown by Puisa (117, 118).

Highly populated databases such as the European Marine Casualty Information Platform (EMCIP) present causation statistics, but refers to accident causation in generic terms such as ‘Human Erroneous Action’ or ‘Equipment Failure’ (135). As these details are high level, extracting the recommendations from accident investigations from these statistics, despite having a vast number of accidents included, will not present data on the specific accident causes and subsequent recommendations which are detailed in the reports. To demonstrate the current focus of accident investigation, I therefore briefly review three recent fires in machinery spaces, highlighting the determined causes and the recommendations made.

Le Boreal

On 18th November 2015 a fire broke out in the engine compartment on board the Expedition-Cruiser Liner Le Boreal (136). The accident investigation concluded that a spray of oil

contacted a turbo blower exhaust elbow and ignited. The report presented that the release had been caused by an engineer replacing a clogged filter on a diesel generator duplex filter believed to be isolated. The recommendations included the alteration of maintenance procedures (Category 4), exploration of the value of segregating Heavy Fuel Oil (HFO) and Marine Diesel Oil (MDO) circuits feeding the engine to simplify maintenance (Category 3) and to review the effectiveness of radio communication during firefighting (Category 5/6). This shows a focus both on prevention and mitigation with Categories 3-6 featuring. However, the primary emphasis focuses on the proximate, direct causes and response.

MV Zenith

On 25th June 2013, the MV Zenith had a fire between the turbocharger and cylinder head in the engine room (137). The immediate cause of the fire was deemed to be a fracture of a low carbon steel pipe (a result of fatigue) which led to the release of flammable material spraying onto an exposed hot exhaust gas manifold.

The report recommended risk assessing machinery spaces to identify critical equipment, such that it could be implemented in the ship's maintenance routine (Category 4). As this risk assessment appears to focus on including equipment in the maintenance routine (prevention through planning), rather than eliminating a hazard, it has been included in Category 4 only. The recommendations focused on prevention of proximate events immediately before ignition.

Sea Gale

On 20 May 2014 the crew supply vessel Sea Gale experienced a fire at a carbon composite panel and insulation area above the main engine exhaust pipe (138). The investigation concluded that ignition likely occurred through overheating of the panel due to the radiating heat from the exhaust pipe, with contributing low ventilation conditions.

The report states that several 'preventive' measures are being placed including a review of manifold, exhaust pipe and funnel insulation (Category 4), along with better implementation of

emergency buttons and quick closing valves (Category 5). Some operational improvements are also highlighted, with a checklist for main engine start up to provide increased airflow prior to start up, with additional reporting requirements when this is complete, and amendments to procedures for supervision/approval of works going on at shipyards. These fall within Category 3 recommendations. Improvements in training to improve emergency response is also included, proving a Category 5 recommendation.

Analysis of these three sample fires shows that most recommendations are preventative, with some mitigation-based recommendations (Categories 3-6). The overall findings relating to prevention and mitigation are all, however, close to the centre of the bowtie. This is in line with the analysis of a large set of accident investigation reports of fires in machinery spaces (80).

3.6 Fire Safety Systems

When considering barriers to be implemented to increase safety, technology-based barriers are often a perceived quick and easy fix to increase safety (78, 139, 140). Such fire safety systems range from the application of instrumentation based technological safety systems, to passive structural measures designed into the ship (fire walls, blast walls etc.). To determine the focus of technology we must analyse the current technologies used in addressing fire safety in machinery spaces.

The drive towards improved fire detection began with traditional smoke/heat detection, providing fast response detection of fire to improve response in the event of a fire. Such technologies have evolved to detect more than just fire, with some being used to highlight the presence of fire precursors (i.e. hot surfaces) using temperature sensing cable products (141). In 2004 the first 5th generation fire alarm system was supplied to the shipping industry, using intelligent sensors, interconnected as an analogue addressable system (16). Such technologies reside within Categories 4 and 5 as per Table 2.

DNV stated that 63% of fires start in the engine room, primarily due to oil leaks (7). Oil mist detectors, available as either a point (142), open path (143), or aspirating device (144), have therefore risen in prevalence as potentially suitable technologies in detecting proximate events/ precursors of fires in engine rooms (Category 4). In 2003 the IMO released MSC/Circ.1086 (145), a code of practice for the application of oil mist detectors which further highlights their importance as a fire safety related technology. Such devices reside within Category 4.

Application of CCTV based imaging devices present a potential solution with respect to detection of flammable releases within the area of concern. Imaging devices may be applied to detect the release of flammable mists/ volumes of gas through Gas Cloud Imaging (146), in addition to elevated temperatures of specific high risk pieces of equipment (147). The focus of this technology is clearly on proximate precursors to fire in Category 4.

Instrumentation monitoring the internal flow, pressure, and temperature of equipment feed lines may present information on potential leaks and releases which could act as a precursor to a fire. Should these systems be installed in pre-determined high-risk pieces of equipment, they can provide alarms signalling precursors to loss of containment, a major precursor to fire (Category 4). Pressure, flow and temperature transmitters could be a credible solution to detecting and acting on fire precursors and are currently readily available. At the time of writing, however, there is little data to suggest the widespread application of these safety instrumented systems in engine rooms with automated protection actions in the context of fire prevention.

This analysis shows the focus of fire safety technologies related to prevention are focused on anomalies immediately left of ignition on the bowtie, falling under Category 4, with the mitigation-based technology carrying though Categories 5 and 6. Technologies exist which can detect further left of centre on the bow tie (such as the safety instrumentation previously discussed), but it is unclear if these are applied with a focus on fire prevention. As an additional

note, while detection and suppression are separate systems, both must operate as intended to achieve the required hazard control. When, for example, detection occurs, an action must be taken to mitigate the situation such as automated suppression, or mobilisation of the emergency response team. Both are independent, critical systems.

While this has demonstrated the focus of fire safety technology, Dynamic Barrier Management (DBM) is an emerging technique aimed at strengthening these barriers surrounding the centre of the bowtie. Through analysis of barrier health and overall risk to the system, DBM is generally applied before the incident, measuring performance at the sharp end of hardware (and perhaps software and people). There exists a limitation in how far left of the centre such a technique can be applied when there is a limitation on how safety facets (such as categories 2 and 3) can be ‘measured’, in real time. The data which can be directly measured can, however, be used to improve the interactions / decisions / assumptions to the far left of the bowtie. This emerging and important aspect of the system operating as a whole, addressing interactions from Category 2 through to 4, in addition to its place in the overall context of system safety may prove beneficial in an alternative structured approach to improving fire safety. Processes such as audits emerge as a critical factor in ‘measuring’ softer aspects of safety and could present an input to a holistic DBM system.

The following table summarises the focus of each available fire safety related technology applied in machinery spaces against the criteria of Table 2.

Table 6: Fire safety technology focus

Focus	Safety function	Fire Safety Technology
Prevention	Eliminate hazard	N/A
	Prevent systemic factors of incident	N/A
	Prevent contributing factors of incident	N/A
	Prevent direct factors of incident	• Process Instrumentation (pressure, temperature etc.). Unconfirmed if widely applied* • Oil mist detection • Temperature sensing cable • Gas cloud imaging • Infrared cameras
Mitigation	Control accident (stopping from propagating to loss)	• Traditional smoke/ heat detection • Optical flame detection • Suppression systems
	Reduce damage (loss)	• Evacuation systems** • Passive protection measures (structural arrangements)

**such systems may be applied for multiple reasons including equipment protection (to protect engine overspeed for example) as well as safety and may not specifically be applied under a 'fire safety' category.*

***Evacuation systems here refers to a multitude of systems including procedural systems (fire drills etc. as part of the SMS), and adequate signage, escape routes etc.*

3.7 Effectiveness of the Current Approach

This research first aims to analyse the current fire safety focus to verify the initial hypothesis that fires continually occur through systemic failures (particularly in the preventative region) not being addressed in design and operation, and that systemic uncertainty/ causal factors may not be fully addressed when applying traditional methods of HAZID and operational auditing which has led to fire remaining a prominent risk to maritime operations.

3.7.1 Results of Initial Analysis

As the facets of fire safety have been demonstrated, the research must now determine if any gaps exist in the SOTA in order to test the first part of the research hypothesis: *Is fire safety reactive in nature, primarily focusing on detection of already materialised hazards?*

Table 7 demonstrates the focus of the current approach with respect to fire safety. The values of effectiveness, as defined in Table 2, are shown under each constituent of safety control. The resultant effectiveness value (the maximum possible effectiveness relating to the approach) is shown for each constituent.

Table 7: Summary of the focus of the current approach to fire safety

Focus	Safety function	Safety rules and regulations	Formal safety assessment	Accident analysis and recommendations	Fire safety systems
Prevention	Eliminate hazard	x	x	x	x
	Prevent systemic factors of incident	✓	x	x	x
	Prevent contributing factors of incident	✓	✓	✓	x
	Prevent direct factors of incident	✓	✓	✓	✓
Mitigation	Control incident (stopping from propagating to accident/loss)	✓	✓	✓	✓
	Reduce damage (loss)	✓	✓	✓	✓
Effectiveness I Value		**5**	**4**	**4**	**3**

Key:

✓ = The constituent of safety control **does** consider fire safety in this region of the bowtie.

X = The constituent of safety control **does not** consider fire safety in this region of the bowtie.

Mapping the analysis in Table 7 onto the bowtie, we can visualise the focus of the analysed constituents of safety control of the current safety approach and where they lie in the prevention and mitigation regions. Note, however the limitation exists that where one constituent extensively covers one specific region, for example mitigating an incident, and only briefly touches on another, for example preventing direct causes of an incident, the distinction between these varying degrees of emphasis is not specifically measurable in all circumstances. Credit is therefore conservatively assigned to both, with no differentiation between the two.

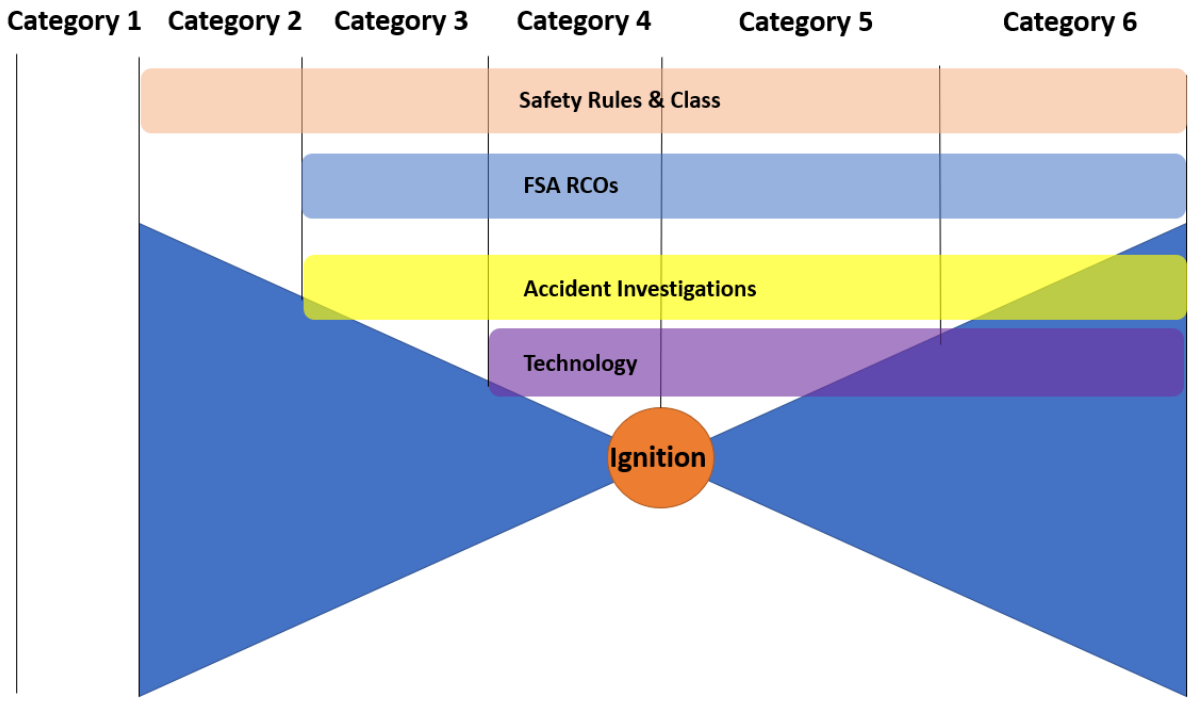


Figure 6: Bow tie of current fire safety focus

This figure demonstrates that FSA, accident investigation and technology present some scope to improve upon the preventative aspects and subsequently improve upon their inherent effectiveness, while safety rules and regulations cover the spectrum of prevention and mitigation from Categories 2-6.

With specific comment on FSA, the recommended RCOs with respect to machinery space fire safety relates to Categories 3-6. It is worth noting, however, that many of these preventative options relate to proximate precursors immediately before ignition (Category 4) and the focus appears predominantly towards a combination of Category 5-6 recommendations. It is also worth noting that only one out of 33 RCOs was left of Category 4, which provides an optimistically high effectiveness of 4.

With respect to accident analysis and recommendations, the investigation reports regularly present recommendations to address SMS deficiency (Category 3) and proximate precursors immediately left of the bowtie, including insulation of exposed high temperature surfaces (Category 4) and improvements in the actions of first responders (Categories 5 and 6) in machinery spaces. This highlights the potential for accident investigation to focus on a bigger causal picture, looking for systemic causal factors beyond proximate events. This echoes a general critique of accident analysis for its bias to look for and stop at “root causes”, which typically appear to be proximate individual failures (26).

When analysing the application of technology to fire safety in machinery spaces, Table 6 suggests that the use of preventative technologies is on par with mitigation aimed systems. This may be somewhat misleading, however, in addressing how far left these preventative technologies focus, shown in Figure 6. The guidance specifically relating to technology is weighted towards mitigation, with SOLAS Chapter 2, the class requirements, the FSS Code, ISO14520-1 etc. all focusing on application of mitigation focused systems. Where prevention is a focus, it is immediately before an ignition occurs, as is also reflected in the preventative technology guidance in SOLAS Chapter 2 regulation 4. The guidance which exists relating to preventative measures in the centre-left to far-left region of the bowtie (e.g., ISM Code) does not necessarily refer to technology. Concluding from this, there may be limiting factors in how far back in the bowtie technology can currently progress.

3.7.2 Discussion of the Analysis

The review has established the focus of the current approach to fire safety in machinery spaces focuses predominantly on direct causal factors and mitigation. Taking a closer look at incident prevention, the bias towards direct causal factors may be attributed to the widespread application of linear, event-based models to accident analysis. Namely, sequential and epidemiological models, known by the Domino (71) and Swiss Cheese (72) metaphors. These models represent the classic paradigm of linear representation of causation, where clear links between causes and effects must be known, and system safety is assumingly improved by independent treatment of individual components of the system. Hence, the system is assumed as essentially a sum of its individual components. Although this linear paradigm has its own merits, it is insufficient to achieve system safety as shown in the literature (25, 42, 43, 67, 74, 78, 139, 140). The linear thinking focuses on incident events and their patterns–which are the visible tip of the iceberg—but systematically fails to explain the underlying structure and mental models that give rise to those events—the invisible, underlying portion of the iceberg (148). The underlying system behaviour cannot be changed by merely reacting to its events, or by analysing components of the system in isolation (38). The reason being that a system is more than the sum of its components (35). Therefore, the modern paradigm of systems thinking must be addressed. In addition to contribution to causation of individual components, the systems approach accentuates the importance of nonlinear interactions between them and the system structure and mental models that determine it (41). As a result, the accident analysis will naturally seek to answer not only *what* happened but also *why* it happened. This finding presents a significant gap worth investigating, relating to the primary hypothesis of the research – that a more structured approach to fire safety, accounting for the entire system specifically further left on the bowtie, will present improvements. If plugging this gap by addressing the entire system including interactions between people, software, and systems (including the context they are placed in) will result in improved fire safety this will be investigated and demonstrated.

Such techniques do exist, including the SCAT chart – Systematic Cause Analysis Technique (149). This accident/ incident analysis technique attempts to address direct causes, as well as the basic/ underlying causes of events. Such an approach can however fall into the same trap of treating the failure as a linear series of events (150). There is little evidence in the recommendations from accident analysis that such a systematic technique is widely applied in practice during this process.

Another explanation of the bias towards proximate events lies in the final stages of accident investigation of machinery space fires, namely the development of recommendations. It is known that recommendations for remedial actions are often tailored to the existing capacity (of the shipping company) to implement them (151), and the focus on proximate events, such as recommending fixes to failed technical barriers, would be seen as the 'low-hanging fruit'.

To improve things further, the misconception of human error must be addressed. Human error at the sharp end is regularly cited as a cause of fire (152). It can be divided into two distinct categories of *slips* and *mistakes* (153, 154). A mistake is an error in the intention (the planning of an action), whereas a slip is an error in carrying out the intention. The machinery space fire on board Le Boreal was triggered by a slip (155), which are relatively easy to prevent, for example, by using different colour coding, warning signals, separation by distance, interlock, etc. Prevention of planning mistakes requires a more fundamental approach, for the errors are only seen as such in hindsight (26). It is suggested that the term human error should be replaced by instead considering such events as human-task mismatches (156). In general, human errors at the sharp and blunt ends are symptomatic of deeper underlying problems in the control of safety rather than the direct and sole cause of accidents (44). Thus, the systems based approach may again be beneficial (39). It is also critical that assumptions made during design regarding human interactions with technology and the environment remain valid in operation. This specific link between design and operation appeared to be lacking in discussion in all the investigated facets of fire safety.

The literature would tend to suggest the ISM code intended to address such factors, while in its relative infancy, is limited in its application (80). This may also be true of other strategies, as the events close to the centre of the bowtie are generally those which have a higher degree of certainty (i.e. rupture of a pipe combined with exposed ignition source). As Category 4 and 5 are those closest to the centre of the bowtie, it would therefore be understandable if these categories were the most commonly applied strategies with respect to fire safety designers and technology applied. This analysis has shown that every facet of fire safety addresses these two categories.

It has also been shown, that when it comes to safety automation and technology, there exists a limit in how far back one can currently go in the bow tie in preventing machinery space fires. The available precursor detection technology (e.g., temperature sensors) focus on proximate events because they are of relative ease to address in design and operation. Its effect on safety is also certain and observable, and hence such technology is easy to justify. However, dealing with more underlying causes such as contributing and systemic causes becomes problematic. The automation is not directly applicable to ‘measuring’ people, the organisation, procedures etc. Also, there is a general lack of knowledge about early, systemic fire precursors, a lack of a clear solution on how to deal with them, and difficulty in measuring performance of such safety barriers in place to prevent or mitigate such precursors. This gap in identifying the key causal factors, applying functional requirements to prevent them, and ensuring this is applied and continually measured in operation is critical and will be the contribution presented in this thesis.

The analysis of Dynamic Barrier Management (DBM) also shows us the importance of strengthening the technological barriers, but also the impact this can have elsewhere in the system, and the importance of addressing interactions throughout the entire left-hand side of the bowtie. The contribution of this thesis will provide a method to generate the relevant inputs to any future development of DBM.

To simplify this, applying DBM to the preventative technologies (i.e. oil mist detectors) does not move ‘Fire Safety Technology’ as a facet of fire safety any further left on the bowtie, but it can assist the barriers placed further left, therefore also strengthening them. DBM provides an improved operational feedback and control loop with respect to the sharp end barriers to the other controllers across and further up the system hierarchy. For DBM to be successful, however, the inputs must be relevant, useful and remain valid. An example of where this can be useful includes the application of a digital twin (DT), where a digital representation of a vessel or its part can have real time numerical assessments of a given situation carried out to assist with real time consequence analysis to improve systemic fire safety improvements. This is, however out with the scope of this research, which will focus on identifying and validating the inputs to potential DBM systems in the future.

Notable from Table 7 is the move right on the bowtie as we move from Safety Rules and Regulations, through FSA and accident investigations and technology (with the caveated discussion on technology above). One possible consideration for the marine industry is the integration and application of the current safety rules and regulations into all facets of fire safety. This could, in time, assist in reducing the consistent frequency in which fires in the machinery spaces continue to occur. If FSA and accident investigations can begin to account for the factors being advocated in the safety rules and regulations (along with improved feedback throughout the system through DBM), an improvement in holistic fire safety is certainly credible.

On reflection of the results and this discussion, the idea of treating the system as a whole may in fact provide an effectiveness metric itself. A gap emerges whereby the fire safety strategy is not structured and systemic in its application, accounting for people, the system and society, and is limited in how far back in the bowtie/ up in the control structure. Combining a structural approach with an appreciation of the whole control system may present some improvements in safety barrier application and management. In fact, this critical review has potentially fallen into the same trap as the current approach… treating each facet of fire safety individually by

splitting these into categories and assigning effectiveness. This may not adequately address the effectiveness of the system and its interacting components. While the objective of this initial review is to test the first part of the hypothesis (determine the focus of fire safety), investigation of the second part of the hypothesis must investigate the application of methods which focus on the entire system.

While mitigation (Categories 5 and 6) begins from the assumption of a fire being present (likelihood of 1.0), preventative categories do not work in this way. The traditional approach of assigning effectiveness differences between Categories 1-4 as we do with mitigation may not be an accurate method of analysis when compared to an analysis of the entire system effectiveness (i.e. the ability of the system to account for all four preventative categories rather than each in isolation).

This further demonstrates that in order to design and operate an effective system, a different approach may have to be applied. Mitigation, where cost benefit analysis and FSA can more easily be carried out (as per the current approach), along with technological capabilities which allow mitigation barrier health to be monitored, may continue to apply a quantitative risk approach in deciding what RCOs to apply. When it comes to prevention, however, such an approach may need to be supplemented with a systems-based approach which can only be effective when the entire left-hand side of the bowtie (for want of a graphical representation) is accounted for. This allows the operators to focus on the interactions between all of the actors in the system, rather than a reductionist view of safety being a sum of all the parts, leading to the criticised approach of adding more layers of barriers to ‘increase’ safety (38). The process under which FSA is conducted may therefore not be effective in improving fire prevention.

Applying a systemic approach is one in which the groundwork already exists, with SOLAS allowing for alternative design arrangements with respect to fire safety (90). With the ability to address alternative design arrangements, we move towards a goal-based approach which

requires designs to set functional requirements allowing designers the freedom to meet those requirements in any number of ways. With the move away from prescriptive guidance, this provides the scope for the marine based fire safety industry to expand from a focus as shown in Figure 6, towards addressing prevention more thoroughly and effectively as a complete system.

3.8 Cost Effectiveness: Prevention vs. Mitigation

Having reviewed the effectiveness of the current approach and demonstrated there is scope for improvement through focusing into the preventative region, and analysing the interactions between humans, technology and the environment, there must ultimately be a consideration of cost. It would be easy to suggest measures which would improve fire safety if financing was an unlimited factor, so the decisions to focus more closely on prevention or mitigation, for example, needs to consider the impact on cost. To continue the testing of the hypothesis that safety can be improved, a discussion of cost effectiveness between the preventative and mitigative regions is provided in this note.

While the focus of the current approach has been discussed, a connected discussion regularly appears regarding the difference in effectiveness between prevention and mitigation. Where should a ship or facility operator determine where to focus finite financial resources in the reduction of risk for that facility – in prevention or mitigation? It is therefore important to address this problem.

With regard to the previous analysis of recommended RCOs in FSA with respect to cost effectiveness between prevention and mitigation regions, it is noted that preventive measures relating to training, procedures and other ‘soft’ factors have considerably higher cost-effectiveness than so called ‘hard’ factors such as component redundancy and other significant changes to the ship. This is primarily due to lower cost of implementation, but not necessarily due to a higher potential in reducing risk.

From review of the RCOs analysed in Chapter 3.4 (albeit a limited sample), improving incident prevention, can be as cost-effective, if not more, than investing in accident mitigation. The two categories, however, are equally essential for implementing the principle of defence-in-depth (157). The principle is essentially deterministic, strictly demanding to have a barrier. In this case, both preventive and mitigative barriers are required, and weakness of one barrier cannot be compensated by making another one stronger (10). The rationale is that even the strongest barrier can fail under certain foreseeable (albeit unlikely or even reasonable) scenarios. This demonstrates the importance of treating the problem from a systemic perspective, and highlights the importance of verifying that soft, as well as hard, safety factors are being implemented in operation as assumed during design. This shows that regardless of the cost effectiveness argument, auditing/ operational processes of measurement will play a crucial role in systemic operational safety.

Figure 7 illustrates the primary focus in various industries (noting that the actual scope of risk control would cover, with varying degree of detail, both prevention and mitigation in all industries) on a bow-tie or barrier diagram (158). The illustration adds the safety scope of the merchant shipping to the original representation (10). It shows that both incident prevention and mitigation are important for risk control in the shipping industry. This echoes the earlier review of effectiveness of the current approach where I compared the prescribed and actual scopes of fire safety control.

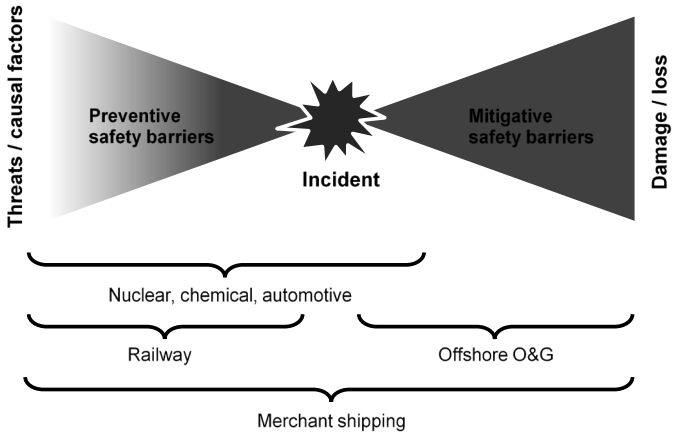


Figure 7: Illustrative scope of risk control in various industries (158)

It is also presented that prevention and mitigation essentially deal with different phenomena that require a different response. Pre-incident events take time to develop through systematic (not random) processes, with detectable warning signs and recognisable precursors (26). The metaphors like ‘incubation period’ and ‘drifting into failure’ are used to explain the insidious degradation of the system up to the point when an incident becomes imminent (33, 34). This degradation, or drift to failure, is a result of normal dynamics of systems, i.e. constant adaptation (adjustments) and optimisation of resources to daily circumstances (35, 159). Incidents happen when interactions between system components (hardware, software, people, and organisations) become dysfunctional, even though individual components have not failed (37). When such interactions are adequate, even sudden failures of individual components (e.g., power loss in stormy weather and in the vicinity to shore) would be effectively mitigated. Thus, incident prevention operates within a complex socio-technical system (117), and it relies on effective safety management. In contrast, mitigation is heavily reliant on technology, i.e. engineering controls. From the physical point of view, incidents develop to accidents when the response energy is unable to thwart the energy being released. Speed of response is decisive, for the damage energy is released rapidly (e.g., an explosion in the engine room with abrupt rise in temperature). Engineering controls, particularly passive ones, have proven to be effective in such abnormal, distress conditions. The role of people is critical, but they arguably would be unable to compensate for a bad design. This concept of causal factors throughout the system from early prevention to incident mitigation, with appropriate and specific functional requirements being implemented to provide safety is developed in the contribution of this thesis.

The review in this chapter has aimed to verify the credibility of the proposition that, in the maritime domain, accident mitigation is more cost-effective than its prevention.

One concludes that the proposition is unwarranted, as far as the presented analysis is concerned. The analysis has shown that improving incident prevention, can be as cost-effective, if not more, than investing in accident mitigation.

There exists, however, an issue in addressing the notion of holistic fire safety, accounting for fire prevention and mitigation in the same analysis. If prevention, for example, is included in the overall risk analysis as part of an event tree analysis, the overall risk reduction capability of mitigation measures can be diluted. Where likelihood of initiating events further left on the bow tie are accounted for, the likelihood of the central event (i.e. fire) is of such a low likelihood, that the risk benefit of mitigation measures are reduced to the point of potential omission from a cost benefit perspective. See also the previously referenced Titanic effect. Typically, in fire engineering, the likelihood of the central initiating event (i.e. fire) is taken as 1.0 to ensure sufficient mitigation measures are applied. While this may overestimate the cost effectiveness of mitigation, there is a risk in moving the other direction to include likelihood of the event to be considered in the mitigation cost effectiveness calculation resulting in a reduction in mitigation measures. This dilution of the risk reduction measures attributed to mitigation could be dangerous in reducing the emphasis on technology-based mitigation but may also be a more accurate reflection on the benefits assigned to the mitigation measures. This debate sits out with the scope of this thesis as the focus here is on systemically preventing fire and ensuring operational safety measures are effective in achieving the goals set out in design. It is, however, a connected area for study and an interesting route for further investigation.

While this critical review has illuminated the path forward with respect to integrating SOTA in design (as described in the SEAMAN project (160)), when discussing facets like DBM, and the systemic approach from a first principles standpoint, operational contexts become critical in analysing the effectiveness of existing barriers during operation. It therefore becomes apparent that a direct link between the decisions made in design and the operational phase must exist in addition to a systemic HAZID. As audits are the primary tool used in analysing the softer safety systems further from the sharp end, these will require review to determine the SOTA and investigate if improvements can be made when reviewing them from the systemic perspective, considering the current connection with the design phase.

3.9 Hazard Identification to Safety Auditing

In analysing the current approach, the approach to identifying hazards and the subsequent connection between design decisions and operational assumptions and verification appears to be critical in achieving fire free and safe operations. Before determining how to test the hypothesis that fire safety can be improved, that connection between design and operation is further reviewed as a potentially significant input to any proposed method for improvement.

3.9.1 Transitioning Safe Design to Operational Safety

Facility safety cases are examined by Wang (161). In such safety cases, accident scenarios can be determined, and it must be demonstrated that risks are reduced to ‘as low as reasonably practicable’ (ALARP). Safety cases are given the freedom to present the specific risks of the specific facility rather than being prescriptive in nature. The results are often, however, arrived at through event trees and other quantitative risk models which fall under the same shortcomings of those previously discussed. It is important to note, as highlighted by Wang (162), that where a sufficient level of data is available, quantitative methods are applied. It can be claimed that it is more appropriate in the absence of such data to apply the qualitative approach, rather than a quantitative approach with sweeping assumptions forming some of the primary inputs, simply for the sake of applying a quantitative approach. Such qualitative approaches may prove difficult, however, in application using traditional methods of risk analysis where a quantitative value is often used as the metric of adequacy.

It is shown that this approach to safety sets high level performance requirements for the system to fulfil (163). Wang states “It is clear that it would be possible to prevent marine accidents by good design, training, and operation in an appropriate systematic management system.” It therefore seems pertinent that the method used to arrive at those functional requirements, and the methods used during operation, apply a structured approach which also considers systemic issues to strengthen the approach. The combination of a structured and systemic approach appears novel in this particular field.

When we move to operation, when a quantitative value has been generated and classed as ‘safe enough’ in design, auditing may become focused on physical failures of the components or controller, rather than systemic failures of the system of control. I will therefore review the role of auditing and its relationship with the design process relating to safety to determine if gaps exist which can be filled to improve the relationship between design and operation.

Wang discusses risk assessment, and specifically reviews the use of the Formal Safety Assessment (FSA) approach (used as a rule making instrument by the IMO) which includes “a proactive approach, enabling hazards that have not yet given rise to accidents to be properly considered”, and “a rational basis for addressing new risks posed by ever-changing marine technology.” This should be fundamental in the underpinning methodology used in any proposed method aiming to address SOTA in safety design, and also shows the importance of continuous application and revalidation of the assumptions, as also indicated by DNVGL (164). This brings my analysis to now consider the importance of, and SOTA in, auditing.

3.9.2 Auditing of Safety

To assess the current application of auditing in safety, studies relating to auditing techniques are considered.

Tools such as the Severity and Outcome Assessment Tool (SOA) are used in the medical field in patient assessment allowing case selection, resource allocation and audit of treatments (165). A standardised tool was applied to audit treatments in orthodontics. To do this, standard measures were required to allow unbiased analysis of results to verify if treatments had been successful on a large scale.

Belgian radiotherapy clinics underwent a systematic audit of multiple facilities between 2011 and 2015 using the International Atomic Energy Agency QUATRO methodology, the results of which were subsequently critiqued (166). The systematic audit resulted in 381 recommendations ranging from process optimisation, protocol improvement, infrastructure quality etc. In the ensuing questionnaire on whether the audits were useful, 54% responded that the recommendations were very useful, with 42.7% claiming they were very relevant and

23.5% claiming they had an important impact. It would therefore appear that auditing has an important role to play in gathering operational information and status.

When considering the marine environment, however, it was found by Mitchell et al. (167) that existing fleet safety audit tools lacked an evidence based, standardised approach. She then proceeds to develop a new tool “to identify the extent to which fleet safety is managed in an organisation against best practice.” This tool is used primarily as a benchmarking tool for organisations. As with the previous audits discussed, this audit addresses a standardised approach to benchmark, rather than find specific shortcomings, and does not address HAZID or hazard analysis. While, therefore, it is presenting information on the safety context, it would not address the current state of any design assumptions which were made which are no longer applicable, for example, such that safety barriers can be maintained or strengthened. This also relates to the previously discussed factor that the ‘benchmark’ is simply a widely agreed consensus of acceptable risk, which is subject to fluctuation. This fluidity in acceptable risk would be classed as a precursor in a systemic risk analysis when reviewing the regulatory controllers in the system, whereas it is treated as a benchmark for auditing in the case of Mitchell. This is not a critique but simply a highlight of the oversight of systemic precursors.

Moving away from audits solely as a safety tool, the use of audits as an accounting governing mechanism is evaluated by Manita (168), specifically on the impact of digitalisation (big data, AI, analytics etc.) on the audit process. It is determined that digitalisation will improve audit relevance, allow firms to offer additional services, improve audit quality (through ease of data collection), and allow for a new profile of auditor to emerge, allowing for improved innovation. Such an auditor can pull trends from ‘big data’ to no longer rely on sampling, but rather apply global data. This means auditors can focus on data analysis rather than data collection. While the safety industry may not currently be in a position to gather such data, future research, methods (such as the proposed SHORE methodology in the latter sections of this thesis) and technology may provide the route for such an approach to emerge. The gathering and analysis of data relating not only to the sharp end of safety (on the ship in the engine room), but also the higher controllers such as class societies, regulators, ship owners, societal trends etc.

would allow DBM to be applied and audited across the entire socio technical context. This would present a useful area of research, extending from that analysed in this thesis.

Safety audits cannot analyse data received from such sensors/ networks if they do not exist. If such data collection devices/ techniques are not implemented in design, they cannot be analysed in audits. Likewise, if such sensors are placed during design, their functional requirement must be documented such that the audit can evaluate their effectiveness in achieving the original design intent. This shows there would be a benefit in linking the HAZID and audit portions to the facility design and lifecycle to allow the audit to be directly relevant and based on functional and physical requirements which are in place… or should be in place as specified during design.

Specifically putting this into a safety context, this could assist in evaluating accidents which have not yet happened where innovation can thrive. With financial auditing, the focus is historically on the past with little thought on the future. It is here that resilience against external risks becomes apparent. Increasingly, businesses are required to strengthen their operational resilience against external risks (9) with concern recently after a number of systemic failings resulting in successful cybersecurity attacks, for example. Such traditional thinking of what has come before, and reduced consideration of systemic risks and increased resilience can also be true of safety audits (31). It is important, therefore, that an audit process engages specific controllers in a system being audited on the critical safety factors with respect to operations, such that further update and innovation to the HAZID, hazard analysis and barrier implementation is accounted for.

As with traditional risk analysis techniques, audits can be impacted by historical biases based on an individual's previous experience or perception. Asante-Appiah (169) investigates the impact of a company's negative Environmental Social and Governance (ESG) perception on the quality of audits carried out. This shows a relationship between an open audit format and an external auditing party's perception of a company on the quality of the audit. While this refers primarily to financial auditing of firms, the fundamentals of external influencing factors affecting the quality of an audit is a credible concern. Any proposed method of improvement

would therefore be best served to be founded upon an existing document/ analysis generated during design/ separate from the audit itself, with the audit serving as a tool for updating those original assumptions. Where the structure of the audit is based directly from this, external influences of perception, for example, can be removed.

With respect to the state of the art in safety auditing, resilience emerges as a proxy to be addressed: resilience has been described as “an organisation’s ability to detect, prevent, respond to, and recover and learn from operational and technological failures which may impact the delivery of critical business and economic functions or underlying business services” (9). Businesses must begin to consider the extreme but plausible events, and create a flexible audit process which is comprehensive in addressing a business’s resilience, but can also be easily incorporated in operations (9).

Checklists are applied within the concept of operational resilience in the risk management arena, as shown by Stolker (170). Such checklists are used to address how a company performs for each of the attributes of resilience. Examples are given by Stolker as to the importance of resilience in a business’ success. One gap emerges when reviewing this auditing technique, when looking at the checklists proposed in measuring a company’s resilience. They remain at a high level in reviewing various levels of management. This is not necessarily always a limitation with respect to their objective, as this is the intention of the checklists. Such an approach, however, is not specific to the hazards identified and the engineering, design and operational assumptions put in place during design, for example, and therefore will not be beneficial in verifying if specific assumptions during design remain relevant across the system.

Stolker references McDonald (171) who states resilience probably needs to be seen as an aspect of the relationship between a particular socio technical system and the environment of that system, which shows the important link between HAZID (based on a systemic risk analysis) and the auditing of operational resilience.

The importance of resilience is directly linked to the company achieving its objectives. As such, unexpected but major events need to be addressed. It is not relevant specifically how such a

major event occurs, but that it may occur and therefore we must be resilient against such an event. Performance based functional requirement setting, is therefore useful in measuring resilience at all levels of an organisation's control structure.

On the topic of auditing process safety, Allford (172) discusses the perceived lack of effectiveness in auditing of safety management systems. In the questionnaire used in the study he finds the majority of those questioned state their company apply internal standards which the audits are performed against. They also dictate the form the audit will take. Having an approach which generates the hazards to be addressed by functional requirements, which then generates safety barriers which are subsequently certified by the class society, should provide the direct basis of the audits implemented in the SMS to address this issue. This gap is a critical one, and a potential solution is to be further investigated in this thesis through the introduction of the SHORE methodology.

Limitations in the current application of auditing are also highlighted by Wilkinson (173), such as the term 'audit' often simply meaning a checklist in the eyes of operators. This means that internal audits can become literal checkbox exercises with independence and impartiality lost. Wilkinson also discusses the issues around discretion of the auditor. If there is no industry wide standard for auditing, a high degree of freedom is available to the auditor and is in fact encouraged. A good auditor must strike a difficult balance between not being locked on the rails of an audit, while not applying so much discretion that the audit is not repeatable.

The issues surrounding audit effectiveness are highlighted further in the investigation into the Buncefield accident in 2005 (174). The investigation states "There should be effective auditing systems in place which test the quality of management systems and ensure that these systems are actually being used on the ground and are effective." The report concludes: "effective auditing systems were not in place. Auditing and monitoring arrangements focused on whether a system was in place; the audits did not test the quality of the systems and, most importantly, did not check whether they were being used or were effective."

This shows the clear importance of auditing not simply covering whether a barrier is in place, but rather whether the functional requirement of a particular facet of safety remains relevant

and effective. This may be achieved by reviewing specific barriers, but the focus of effective audits must be on the performance based functional level, rather than solely physical functionality. Audits which focus on checklist type analysis of specific barriers will not be effective (173). Blewett et al. (175) warns that auditing has become “a ritual rather than a means of improving workplace health and safety”. They also warn against common failure modes of audit including paperwork for the sake of the audit, confusion of audit criteria, and lack of auditor independence and skill.

A useful method of assessing health and safety management systems, applying the resilience engineering approach is presented by Costella et al. (176). The ‘method for assessing health and safety management systems’ (MAHS) approach looks specifically at auditing while incorporating the systemic approach (assessing the system prescribed), the operation situation (what is really happening) and the performance-based approach (what are the key performance indicators) to safety. The method is derived from the requirement to address health and safety management applying the socio technical context and to include provision for the degradation of barriers as the lifecycle progresses. The method proposed by Costella aims at developing an effective audit and applies the foundational principles built upon in this thesis with respect to auditing SOTA: a structural decomposition of the system to verify if the performance-based nature of safety is addressed in both design and operation.

Costella’s method generates topics to be audited including documentation and records, legal requirements, top management commitment etc. These are important areas to audit; however, it does not provide a direct link to the HAZID process or address the direct resulting functional requirements generated. Verification of production processes and hazard identification (on a traditional and organisational context) is included, but the verification is based on whether mechanisms are in place to account for them.

The core elements included in the method are critical in assessing safety from the resilience engineering perspective, however a direct and verifiable link to the HAZID stage is not provided in order to generate the effective and relevant questions to be asked during audit. Such questions are required to verify if specific barriers are in place and operating as

anticipated during design to meet the functional requirement, or to provide a critical input to a DBM system for example. Questioning directly and verifiably from the HAZID would ensure independence and impartiality in questioning and would ensure such questions are directly relevant to the design assumptions being verified. The application of SOTA in both HAZID and operational audits, as implemented later in this thesis, must account for these factors.

The questions posed in the MAHS approach are listed to allow the auditor to include them directly in the audit. These questions focus on the primary facets of safety – performance, structural or operational. The questions are posed for the auditee to present evidence of how the facet is addressed in the company. An example objective presented for the auditor to address in the MAHS method is “to check how workers and supervisors on the shop-floor have autonomy to take decisions which influence safety, such as to stop production should there be an imminent risk of accidents (flexibility).” These objective statements were subsequently updated to present questions to make the audit easier to implement and to address factors including the resilience engineering principles more systematically, guidance on developing an action plan as a result of the audit, improved ease of use, and improved score assignment procedures (177).

The method is an example of how to incorporate the systemic approach in an audit, and highlights that this is not commonly done, representing a significant gap in auditing. A further gap emerges, however, that the method does not allow for the approach to be applied as part of an ongoing SMS, directly linking to the HAZID process, and is intended as primarily a ‘benchmarking’ audit tool. Such gaps are to be addressed in this thesis.

3.9.3 Available Audit Tools

A review of safety auditing tools available online reveals many safety audit ‘checklists’. A selection of 15 safety audit checklists is easily accessible through ‘Safety Culture’ (178), however these show the limitation of being basic templates to drive directly into an audit. Tools like iAuditor from Safety Culture allow managers to verify in real time if certain operational actions/ inspections have been completed. This is useful to flag up real time gaps, but again

doesn’t account for drift into failure, control and feedback loops, or allow for annunciation of invalid assumptions which were correct on facility launch which require verification during a safety audit.

This will result in similar limitations of traditional safety barrier design (decisions taken based on previous biased experience). With this being implemented in the audit, we suffer from a similar lack of appreciation of the socio technical context and a structured approach to address the precursors to fire.

ROSPA (179) provides a selection tool questionnaire such that the most appropriate tool can be selected. While this will undoubtedly be useful for organisations starting out with safety audits, to fulfil the previously highlighted gap in auditing tools this research shall aim to be automatically relevant for the company and fire safety as a result of its origin as part of systemic hazard identification and analysis.

Safety Media also produce a safety audit module (180). Here, audits can be tailored to include risk and incident management factors prepopulated, distributed to managers, then auditors can attach documents and assign a pass/ fail criterion after their audit. Again, this does not carry out identification or analysis of hazards or derive directly from a performance based HAZID or hazard analysis process for a specific facility. This may be suitable for standard prescriptive applications like office workplace health and safety, but a hazardous application governed under performance-based design rules would benefit from a more detailed and specific safety audit process.

The QUATRO method of audit used in atomic energy (181) focuses on the entire radiography process, reviewing aspects including the organisation, infrastructure, clinical and physical elements in a department. Recommendations are classed based on 1) staffing, 2) infrastructure, 3) process and 4) organisational factors. Again, the audit is independent of any HAZID or analysis and is based on a general audit, the objectives of which are developed before carrying out the audit, and as with previous tools, checklists are used for the auditor review.

The QUATRO methodology is shown by Aude (166) to have a limitation in requiring to be structured specifically for the region and operating practices of that region. Note this is not necessarily a limitation as checklists which are too generic will not be able to include certain nuances/ details which mean the conclusions are not credible. A method/ tool applied in addressing the GAP in the current application of auditing will need to assist is in being specific, but from a common start point i.e. the basis of the audit emerges from the original design assumptions/ HAZID/ hazard analysis.

The “patient-oriented” character of the QUATRO audit brings advantages but resulted in the audits requiring to be stopped between 2015-16 to specifically review the Belgian context evolution. This resulted in a secondary tool being developed for the second wave of audits, B-QUATRO. While this can be true of all audits, that context is crucial, inherent within the management of the method proposed later in this thesis must be a review of the socio technical context at its core.

An auditing tool used in operations in the marine industry is the Marine Systematic Cause Analysis Technique (M-SCAT), by DNVGL. The tool is used in addressing systematic causes of incidents. The tool addresses barrier management through the traditional Swiss Cheese approach. This tool is useful in incident analysis; however, the gap exists in not being proactive as part of a continual barrier management process to ensure assumptions in design are accurate, and the control and feedback provisions in place have not deteriorated.

In light of DNVGL’s positional paper on Dynamic Risk Management (164), a safety tool which can be used in HAZID, hazard analysis and safety audits would be useful and could be expanded to also address the systemic causes of incidents by addressing the system wide factors.

Audit tools such as SOA, ROSPA etc. provide useful metrics for comparison between organisations or results in some way, but do not directly provide an analysis of what problems could occur and how to prevent them, while providing an avenue to continually validate design assumptions directly with the controller of a specific hazardous process. These tools focus on painting a picture of a snapshot in time and use generic templates in their application. They

assume that safety is what one has (static property), rather than what one does (dynamic process) (182).

As the marine industry applies performance-based design, audits should follow suit and be based upon such a goal-based design.

The method to be presented in this thesis aims to structurally decompose the system of control to find the failure routes and identify functional safety requirements to fulfil the overall objective of fire free operations, providing performance requirements for those barriers in a structured manner. The approach must also allow the results to be continually and verifiably validated as part of an effective SMS.

4 STPA: A Novel Structured and Systemic Approach to Fire Safety

4.1 The Method

This critical review has answered the question of where the current approach to fire safety in machinery spaces focuses, and whether it is effective. To answer it, I conducted an analysis of current industrial practices and academic interests concerning fire safety in the maritime sector. During the analysis, I used specific criteria for inferring the focus and subsequent effectiveness of analysed safety rules, regulations, recommendations, and technologies. The results show that the effectiveness of the current safety measures used in practice may be suboptimal, with the focus being placed on the detection of proximate events immediately prior to ignition, and on the mitigation of post ignition events.

As the critical review has verified the initial hypothesis that current fire safety efforts are concentrated at the sharp end of safety and inadequately address the systemic causal factors of fire, I must now determine if an alternative method can be applied to test the following hypothesis: *If a structured fire safety approach is implemented which accounts for interaction between humans, technology and the environment across the entire prevention and mitigation spectrum, opportunities for improvement in machinery space fire safety will present themselves.*

It must be stated that the current approach allows cost based analysis to be calculated by the application of event or fault tree type analysis (i.e. a value is assigned to risk which can either be classed as tolerable or intolerable). Whether this is adequate or not, companies and designers alike see benefit in employing this. It complies with the ‘so far as is reasonably practical’ approach to safety in balancing the equation with one side being safety barriers and the other being cost. It is clear this provides a degree of justification in decision making, which is verified as standard practice in Health and Safety law. It is important to note, however, that this is somewhat at odds with the ‘was this foreseeable?’ approach in the UK courts (183). If

prosecution can occur where a major accident hazard was ‘foreseeable’ but not addressed, and the traditional method of risk analysis allows for high consequence, low likelihood events to be discounted, how is the equation squared?

A traditional risk assessment during design may, for example, determine a specific failure frequency based on generic databases of equipment reliability. This would then be applied as a likelihood value for a given physical failure. In reality, site specific and accurate risk cannot be based on such generic and static values. Operational conditions should be considered when moving to a real time appreciation of risk and decision making based on the specific facility and conditions over time. Only then can verification be carried out that the functional requirements developed during design remain relevant and complied with. The assumptions during design may be perfectly robust, but these may lose accuracy once the facility goes into operation and the risk becomes dynamic. They may also prove inaccurate due to human interaction which would normally be a safe and appropriate action, but in a unique environmental context becomes unsafe. Therefore, despite the traditional approach allowing a value to be generated to address cost effectiveness, the shortcomings are clear and must be addressed. It is time for the safety community to embrace an alternative priority scale in decision making for design and operations. This is not to discount the important aspect of cost effectiveness, but simply to highlights that new methods need to be produced to allow cost effectiveness to be integrated in the SOTA in HAZID and operational safety.

To improve the effectiveness of the current approach to fire safety in machinery spaces, the author recommends investigation of the adoption of a novel systemic and structured approach to fire safety at sea with an expanded effort towards prevention further left in the bowtie, accounting for the entire left portion of the bowtie as a complete system. The current approach does not allow the system to be considered. When fire occurs, there has been a control failure in the system. If the control is adequate, the fire will not occur. The fire does, however, occur because the sharp end focus is too little too late.

It is proposed that adoption of the systemic approach to hazard identification will reduce the frequency of fire by identification of latent causal factors in the system by addressing the interactions between all components throughout the system at the blunt and sharp ends of safety. While this thesis will focus on a functional level looking at the increase of effectiveness as we move left on the bowtie, there is an acknowledgement to the current quantitative analysis capabilities with respect to barrier effectiveness from category 4-6, but highlights the requirement for a new method of analysis of Categories 1-3 (and possibly also integrating Category 4) to address the strengthening of preventative barriers. The approach is equally applicable to mitigation but as the gaps appear predominantly in prevention, this is where the focus will pertain to.

With a view to potential industry impact, it is credible that a novel structured systemic approach, which can account for goal-based fire safety with added focus on preventative measures can demonstrate an alternative design arrangement of equivalent safety. This would help fire safety measures increase their scope further left in the preventative region and towards a systems-based, holistic analysis.

With respect to expanding on this work, DBM provides scope for investigation and is linked to the ‘real time’ factors which influence the emergence of safety. The ability to monitor processes has become far more accessible in providing a snapshot of a given condition. While such an approach currently focuses on the prevention of incidents close to the point of ignition, and where available technologies can provide feedback (Category 4), the integration of DBM to assist and strengthen barriers relating to Categories 2 and 3, including procedural and organisational latent factors, is certainly of interest. It may also assist in the regulatory and research community’s promotion of increased focus on prevention by addressing the interaction of various barriers across all categories of fire safety. In order to have successful DBM, the inputs of what to measure are critical. Currently it appears these inputs are taken from historical experience using the traditional methods previously discussed. This may be sub optimal, and a structured systemic approach may result in providing rational, reasoned,

and impartial inputs to a DBM system. The approach may also reveal areas for innovation to be integrated into the DBM system, which would previously have remained undiscovered. Such an approach must also consider the life cycle of a facility if these measures are to be successful in the fluctuating operational environment.

4.2 Testing the Proposed Method

The analysis of this thesis will test if a systemic HAZID will provide additional benefit in presenting functional requirements which can influence new safety barriers or help strengthen existing barriers which would otherwise be overlooked. This will provide a critical input to any future success of DBM.

Furthermore, with risk having a relationship of likelihood and consequence, during design the risk assessment (i.e. QRA) will make assumptions such that the lifecycle of the asset can be accounted for. When this moves into the operational phase, these assumptions may become inaccurate and decision making in the moment can alter the assumptions made during the design.

As a result of this dynamic risk, a model for operational safety is required which validates the assumptions made during design, and continually verifies that confidence in asset safety is maintained. Hidden risks which emerge during operation should be flagged and addressed continually over the life of the asset. We must also have confidence in the results of this operational risk assessment as “confidence in results can be equally important as the results themselves” (164).

Essentially the focus must be on ensuring the operational degradation of safety barriers is detected. This becomes progressively difficult as we move away from the sharp end, relying more on operational audits, for example. It is therefore also critical in this thesis that I analyse how the findings of the systemic HAZID can be integrated as part of a system health check and overall SMS. It will be investigated if there is benefit in carrying out an operational audit

directly from the HAZID. It will then become clear if this line of questioning presents opportunities for improvement which could be linked to the SMS and DBM, which would otherwise not have been discovered applying traditional hazard identification, analysis, and audit techniques.

In summary, two important factors emerge during operation: 1) Are the assumptions of operational safety activities from the initial HAZID still applied, 2) Are the assumptions of operational safety activities from the initial HAZID still valid.

To test whether this approach can result in new systems of detection/ hazard monitoring, this thesis applies a tailored method of STPA (for both HAZID and audit) to specific hazards in an engine room of an operational cruise ship in the form of a case study. The aim is to determine causal factors (some of which may not have been considered before), rank these causal factors with respect to criticality and effectiveness, and determine if the functional requirement is in place, or if new technologies or strategies can be applied to address these causal factors and improve holistic fire safety on board passenger ships. I then validate the findings within a group of experts from within the marine industry (namely an operator, a class society and a system integrator). Such an approach is to be applied in a structured manner, decomposing the system which controls fire safety to find those contexts and actions which can result in a failure.

The primary rational behind the selection of STPA is derived from the requirement to address the system, not the individual components and their reliability (184). In keeping with the state of the art of HAZID and risk analysis and based on humanity's understanding of why accidents happen (as discussed in section 3.2), a systemic analysis technique is selected. Once the systemic method was selected, STPA has been designated as the most prevalent technique of applying systems theory for the purposes of HAZID.

The systemic method will apply to controllers both at the sharp and blunt ends. If the HAZID identifies causal factors linked with the interactions within the system which would otherwise

have been overlooked, this will demonstrate success of the method in its primary function. Analysis from the critical review also demonstrates that audits may not be optimal. If the operational audit phase (derived from the systemic HAZID) then presents findings which demonstrate specific safety barriers perceived to be in place are actually ineffective, this will demonstrate a benefit in directly linking a systemic HAZID to the operational audit which can be integrated into the SMS.

4.3 How does this Improve on SOTA?

The contribution of this research is intended to provide a method and process whereby the approach and findings are an input to any barrier improvement system, for example DBM. While this research and experiment may find specific areas of improvement, the important facet of the research is the method which has resulted in those findings. To that end, the specific recommendations for any proposed barrier improvement system will not be expanded in the research, but rather the analysis will show if the method discovers these gaps and if so, how the method has found those gaps.

Where safety barriers are required or need to be improved, it is proposed this thesis will present the new SHORE methodology and process (to allow personnel not fully experienced in STPA or fire engineering to obtain suitable findings) which leads to the pin pointing of specific inputs which are important and potentially failing in a system. The method results in the recommendation of functional requirements to be used in design and provides the inputs for an audit when a facility is in operation. The intention of the audit is to highlight poorly performing barriers, or barrier gaps which can then be addressed as part of a continuous improvement safety programme. In this case it is predicted that safety barriers at the sharp end can use sensor analysis and prognostics to detect failure or barrier degradation. The process can then be repeated to add in additional sensors, if required, to the leak prevention barrier. This can be applied to multiple barriers at multiple levels of a system, to multiple hazard types and to different industries.

4.4 Novelty in the Approach

In addition to the novelty of applying a structured systemic HAZID to fire safety in the maritime industry, there is also innovation in the particular type of structural approach being used - the use of a systemic accident model for hazard identification and analysis as a direct input to barrier selection and/or performance improvement, which is also directly integrated into the audit process. Unlike conventional methods (FMEA etc.), this method is better suited for analysis of the socio-technical context present in fire safety control of machinery spaces. This thesis presents the first example of how this can be used to comply with the performance-based method of fire safety design within SOLAS, and directly integrate into the SMS for application within the facility lifecycle.

Applying this structured systemic approach assists in solving the safety problem at hand. This contrasts with traditional approaches where safety barriers are added in a reactionary way, as is represented in the fix what you find approaches to accident investigation (31). Essentially, a reactive approach uses incidents/accident as evidence that a specific scenario is plausible (provided it is not unique to that specific operation / ship). While this can be incorporated into the criticality metric of a functional requirement, it is not a primary driver using the method presented. This can result in a hazard analysis, the results of which seem hard to accept. In safety engineering this is a common occurrence. The adage of “the past seems incredible, the future implausible” is particularly relevant in this respect (185). It is therefore critical to highlight the benefits of the systemic HAZID link to the SMS to assist in applying soft safety systems which are harder to measure (SMS etc.) and are currently neglected. To prove this does not need to be the case, the systemic approach can be applied to such barriers to analyse risk and improve/ develop new barriers on a system level. This direct and measurable link between HAZID and audit is to be tested to verify if 1) hazards are identified which are previously overlooked, and 2) the audit based directly from the HAZID presents findings which would otherwise have been overlooked.

5 Application of STPA on a Cruise Ship Engine Room

The following chapter will review the model applied for fire safety including the reason for model application, along with the steps included in the project. This analysis involved a definition of the hazards as a starting point. This is carried out to focus the analysis to a specific group of hazards which can lead to the incident or accident we aim to prevent (in this case fire). Once the hazards are defined, the analysis aims to determine the scenarios in which those hazards can occur. Once those hazardous scenarios are defined this allows the safety goals to be defined which would help to prevent the occurrence of the hazardous scenario (referred within this chapter as the functional requirements). Once the requirements have been developed, we can then decide on which barriers can be implemented to achieve those requirements. The requirements specification allows us to set specific and facility tailored performance requirements with respect to fire safety, rather than a generic prescriptive requirement. The barrier can therefore be tailored specifically to the application to increase the effectiveness of fire safety. This is, however, dependent on there being adequate signals in place to assist in ensuring such barriers remain robust in achieving their functional requirement.

Once this analysis is complete, a validation exercise, presented in Chapter 6, is crucial in determining if the analysis is applicable to a live facility, while also verifying if any additional safety measures can easily be incorporated into the field in the short term. From this validation exercise some recommendations can be made on the application of the analysis.

In the process of developing the method in this chapter and the audit in Chapter 6, the basis of the SHORE methodology is developed to carry out the HAZID, functional requirement specification and audit function for operational safety. This methodology is fully populated in Chapter 7.

5.1 Defining the Hazards

It is determined that philosophically, and practically, fire prevention is a function of risk control of hazardous processes. In this respect, in determining the risks to a ship from fire, we must determine what the potential causes of a fire could be, and specifically what the hazards are which we want to prevent. These causes, albeit only proximate, are well documented in the literature yet continue to occur at a consistent rate (1, 6, 186-190). For this reason, an alternative is proposed which treats the problem from a first principles hazardous process control approach. This method is Systems Theoretic Process Analysis (STPA), based on the Systems-Theoretic Accident Model and Processes (STAMP) methodology presented by Leveson. STAMP has been selected as it is cited as the most widely applied systems based method (191) and has a robust network of data available (Leveson 2012), and is often the most effective at representing a truly systems based approach (192), as previously discussed.

This approach focuses on finding the weak points in a system (the integration of humans, technology, and the organisation) which could present precursors to an accident. These can be in the moments before ignition (where the current approach is focused), or much further back in the bow tie. The bow tie is referred here as it is often used to determine the 'journey' towards an incident/ accident in risk assessments (193).

To apply the approach, there are several steps involved which are presented in this case study, with engine room ignition at the heart of it.

SOLAS contains guidance regarding the operational readiness and maintenance of the fire safety systems (194). The purpose of this regulation is to ensure that fire safety systems are fit for purpose and that the intended functional requirements are achieved. For this reason, it is crucial that the functional requirements are clear. Rokseth et al. (45), highlight that moving towards a 'functional abstraction' from a typical 'structural decomposition' would present some benefits in risk assessment. For example, the analysis of the potential route to failure by looking at individual failures as a chain of events (excessive vibration leading to fracture of

pipe leading to oil contacting an exposed hot surface) may not highlight all the potential flaws which could lead to failure. Viewing the safe transfer of flammable materials as a hazardous process to be controlled and reviewing the possible feedback and control loops which maintain the system in a safe state may flag gaps in the overall system (humans, technology and environment).

The first stage to be carried out in the STPA is the identification of potential losses of concern. Typically, in such a study, the losses refer to losses of life and health, damage to equipment / property, loss of ship (aka total loss), which can all be caused by a fire, but not in all cases. In this study, the primary loss to be reviewed is simply the fire. Traditionally the fire may be viewed as an incident which could lead to losses, however in this study there is no benefit in analysing losses which result from the fire, but rather the study will treat the fire as the loss. This maintains the focus on prevention/ mitigation of the hazards which can lead to fire.

The following defines the loss to be prevented in this STPA:

- Loss (L) = Fire

The second stage of the STPA identifies system level hazards which can directly lead to those losses previously defined, and importantly specifies the boundary of the model in which we review these system level hazards. Considering the fire triangle, we require the combination of three factors to cause fire: Oxygen, fuel, and an ignition source. Removal of Oxygen is not a credible approach therefore we focus on the removal of ignition sources, flammable materials, and elimination of the interaction of those two hazards. Figure 8 shows the boundary of the system to be reviewed along with the two sub systems (the system to control ignition sources, and the system to control flammable materials).

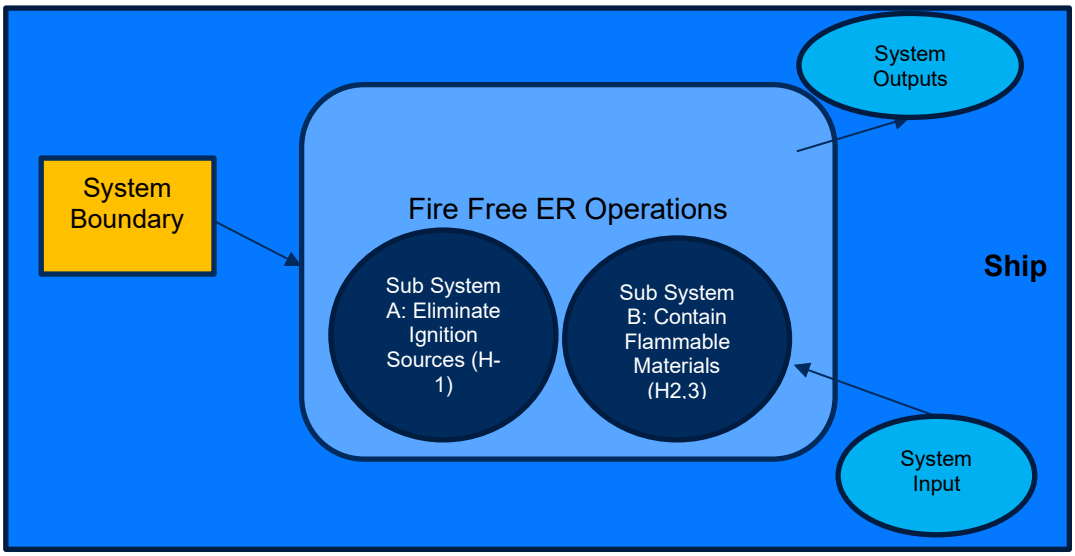


Figure 8: Definition of the System

In this case, the 'System' would be defined as the efforts towards a fire free engine room during operation, the 'Environment' could be represented as the ship itself (but can be expanded to include external influences including regulatory influences), and the 'System Boundary' contains all of the processes which allow for the ER to serve its function. Such processes do not necessarily have to be geographically within the room or ship. High-level factors including societal perceptions/ expectations of safety, for example, are also inputs to the fire free operation of the ER. For example, if a particular ship engine room has been built to the highest of standards and markets itself as 'the fire free engine room', this can lower the guard of maintenance engineers who now have a lower perception of the fire risk. This could result in actions which push the ER towards having a fire. Figure 9 represents the notion of unsafe acts and the relationship/ proximity of controllers (i.e. management, the company, regulators) with respect to a hazard being realised. The specific case study in this thesis will review aspects of the system from the Company/ Organisation to the ER itself.

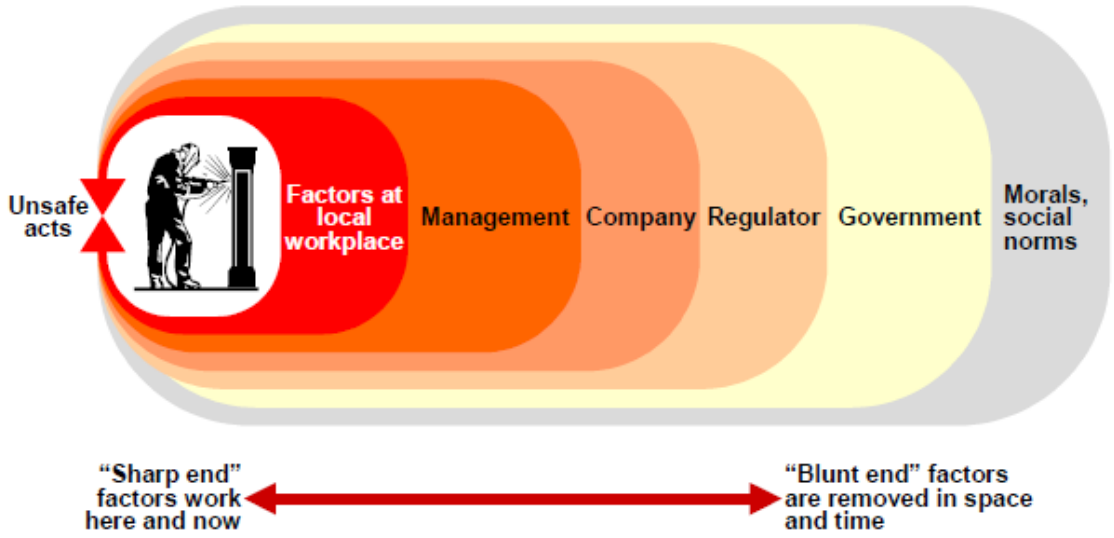


Figure 9: Relationship of sharp end/ blunt end factors in safety (Hollnagel, 2002)

SOLAS Ch II Regulation 4, Probability of Ignition (194) lists 6 functional requirements in the prevention of fire: 1) means shall be provided to control leaks of flammable liquids, 2) means shall be provided to limit the accumulation of flammable vapours, 3) the ignitability of combustible materials shall be restricted, 4) ignition sources shall be restricted, 5) ignition sources shall be separated from combustible materials and flammable liquids, 6) the atmosphere in cargo tanks shall be maintained out of the explosive range.

As the thesis will concentrate fully on the machinery spaces, requirement 6 is excluded. As a holistic functional requirement, we can also collate requirements 1-3 to the control of flammable/ combustible materials in the room and combine 4 and 5 as the elimination and control of ignition sources. During a workshop held in Miami (24-26 February 2019) between RCCL, DNVGL and the University of Strathclyde, while discussing the proposed approach to ensure hazards of relevance to an operator were applied, the following three hazards were presented to be analysed (195):

H-1: Hot surfaces (>220degC) in ER

H-2: Leak from pressurised oil systems

H-3: Failure to contain oil leak

Requirements from SOLAS Ch II, Reg 4 to meet the functional requirements include rules on the limitations and arrangements of fuels, design of piping systems, electrical appliances etc. These aspects of design cannot currently be directly monitored in the engine room/ on the ship and cannot be detected by proximate detection techniques. It was therefore important that an appropriate boundary is determined on the case study. As such, the case study focuses on the ship, and the control/ feedback loop between the ship and the company. This high-level control and feedback loop between the ship and the company is the extent to which the analysis extends.

Requirements present in Regulation 4 such as prevention of overpressure, protection of high temperature surfaces and ventilation in the space can be detected and actioned within the ER through physical, functional and symbolic barrier systems in place, which are presented in the Safety Control Diagram (Figure 10) and STPA sheets (Appendix A). Feedback and control should also be verified to ensure a safety system is put in place in design and adequate in operation. To look only at the factors in the room, however, ignores their interaction with the factors outside the room, consequently addressing the issue only in part. Leveson (26) highlights this issue, for example, when discussing the failures of the Challenger and Columbia space crafts. While the proximate precursors were vastly different, many of the systemic causes were similar. This case study will apply a systems-based approach to review if gaps exist in the system when we consider the interactions of the components within the organisation.

5.2 Defining the Hazardous Scenarios

For the purposes of this case study, this STPA will focus on the ER, other areas of the ship affected by/ which affect the ER, and the company. This is not to say, however, that the approach cannot be expanded to other areas of the ship, and further from the company with respect to the societal and regulatory context. Extending beyond the boundaries of the organisation is, however, an area of future research.

The following structure represents a summarised high-level control diagram of the areas within the scope of this STPA.

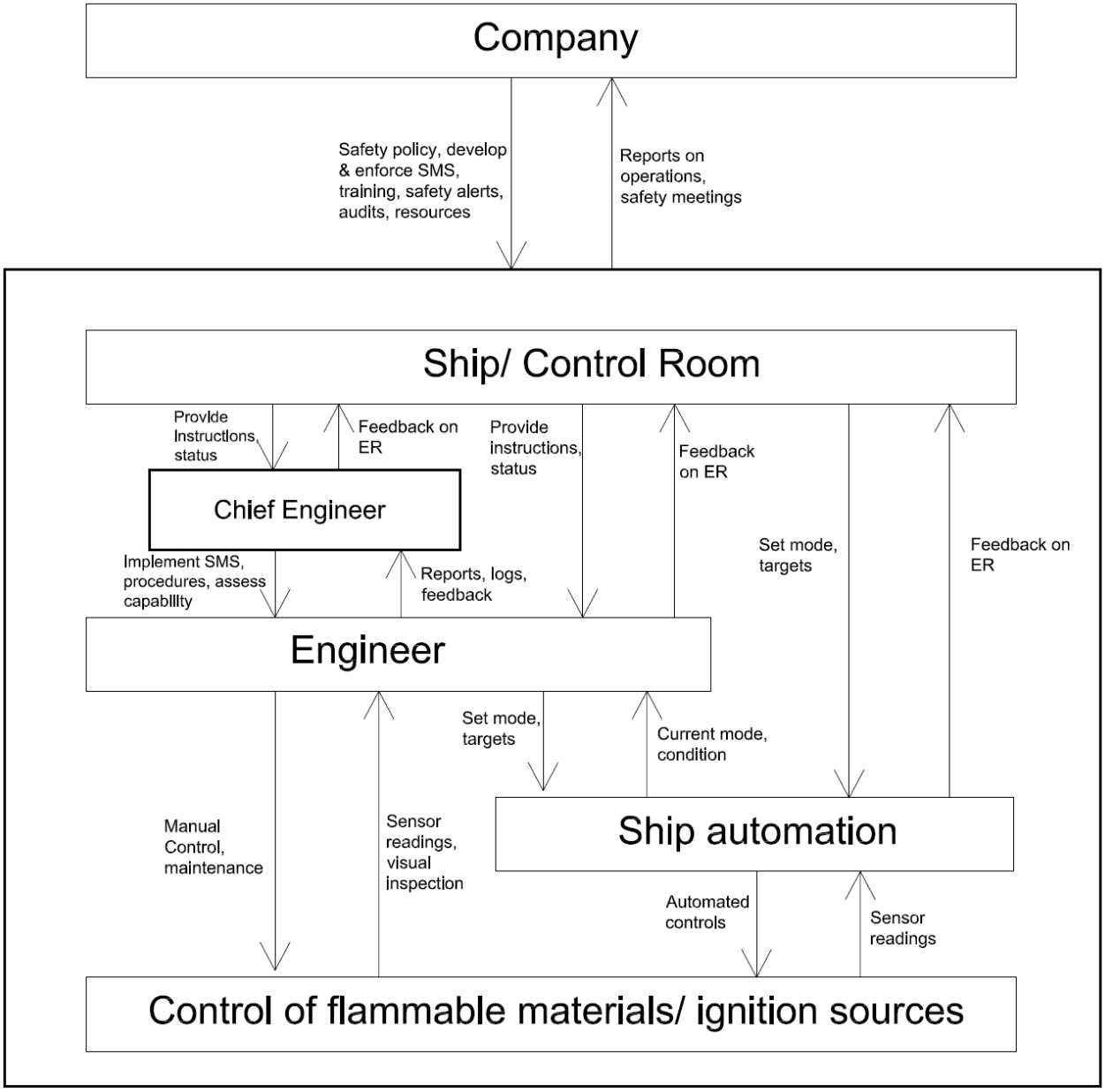


Figure 10: High level control structure of fire control

As shown in the control structure, the controllers can be seen above the hazardous process being controlled. These controllers include the ‘Ship Automation’, ‘Engineer’, ‘Chief Engineer’, ‘Ship/ Control Room’, and ‘Company’ (the only controller which technically resides off the ship, but can have a direct impact on operations and can occasionally have representation on board the ship). Each controller has a selection of control and feedback loops presented, and the

controller or process which those control and feedback loops pertain to. It is important to note that some controllers have generic terms applied to them i.e. ‘Engineer’. This term can apply to several different engineers on board i.e. the duty engineer, staff engineer. Ultimately the controller ‘Engineer’ encompasses those roles and the specific functional requirement would simply be validated against the specific responsible engineer in practice.

From the diagram’s control and feedback loops, the reviewer can begin to examine whether the controller may predominantly use a physical, functional, symbolic, or incorporeal barrier (or a mixture of all). The initial review reveals that controllers very close to the hazardous process (i.e. ship automation) are likely to implement barriers on the physical and functional level. As we move further away from the hazardous process, symbolic and incorporeal barriers (i.e. those which fall under a maintenance requirement which rely on individuals interpreting a degradation which would require action) creep into the analysis.

To progress from the determination of the controllers and the statement of the hazards intended to be reviewed, the following process is followed to present the hazardous scenarios. Examples for each stage are presented below pertaining to the ‘Engineer’ controller.

1) The objective/ responsibility of each controller is determined.

   To begin to present the controller inputs and outputs and position within the greater hazardous process control, the overall objective/ responsibility of that controller is presented in a high-level overview.

   Example objective: Maintain equipment within the ER, ensuring hot surfaces and breaks in containment do not occur.

2) Show the Input and Output of the controller

   To begin to understand the actions of a controller, the inputs to that controller should be considered, along with the expected outputs of that controller, again providing context to the position of that controller in the larger system.

Example controller input = Instruction from Chief Engineer/ ECR. Initiative while in the ER. Sensor readings.

Example controller output = Repair of equipment. Maintenance of equipment. Reports to Chief Engineer/ Company. Feedback to ECR. Manual process control when required.

3) Constraints of the controller

All controllers will have constraints which can prevent the controller from operating entirely effectively. Determining these high-level constraints at the beginning of the process provides some leading information in determining how their control actions may become unsafe.

Example constraints: Resources, Time, Instructions, Training, Autonomy

4) Identify control actions of each controller

Each controller in the system will have control actions which are carried out. These control actions are the primary output of the controller and are intended to be carried out to maintain avoidance of the primary hazards. The control actions are implemented based on input received by the controller (i.e. through instruction by a superior, or through their own personal intuition). The effectiveness of said control actions is therefore critically related to the relevancy and accuracy of the input, the internal process or mental model of the controller, and the environmental context of the action. It is important to note in the context of this research I do not have access to the assumptions made during the design of the Allure cruise ship where the case study is implemented. I have therefore treated the operational risk model as a generic appreciation of the risk and received continual verification with the ship operator and the class society DNVGL to ensure my assumptions are accurate. There may be some control actions which were included in the initial design which the analysis has omitted, and conversely there may be some control actions included in this analysis which were

not addressed in the initial risk assessment/ design. In isolation, even this shows a benefit to such an approach to the fire risk model being used during design and applied holistically during operations to maintain consistency, relevance, and reference to design assumptions.

It is not necessarily an indictment of the design if additional control actions are added to the operational risk model. This can be a function of the evolving and dynamic nature of the risk. Accounting for these during design, however, would likely result in an overall more robust and accurate operational risk model when the ship is put into service. Note all control actions for each controller are presented in Appendix A.

> *Example control actions:* Inspect Equipment; Report on integrity; Repair equipment; Shutdown Engine; Shutdown Fuel Supply; Release Water Mist

5) Identify unsafe control actions

With each control action assigned to the controller, there are potential circumstances in which the action can result in a hazardous situation. The context in which the action is carried out determines whether said action results in the intended outcome, or an unintended dangerous outcome. We therefore have to review the context in which the action is carried out. Analysing the effects of the action not being provided, being provided, providing the action too early or too late, stopping the action too soon, or applying the action too long all provide potential contexts in which the action could result in the unintended outcome. Note all unsafe control actions for each controller are presented in Appendix A.

> *Example unsafe control actions:* Engineer does not detect loss of integrity during inspection (H-2, H-3); Engineer repairs equipment but does not complete/ implement the repair correctly (H-1, H-2, H-3)

6) Identify Causal Factors i.e. hazardous scenarios

Once the unsafe control actions have been documented, the safety engineer shall determine the causal factors/ hazardous scenarios which could lead to those unsafe control actions. It is reasonable that each unsafe control action can have multiple causal factors. Typical scenarios which could produce a specific causal factor include an inadequate input, an inadequate control algorithm; an inconsistent process (or mental) model, design of an incomplete process (or mental) model, design of an incomplete process (mental) model, inadequate feedback, an inadequate control path, or an unruly controlled process. Note the causal factors for each unsafe control action are presented in Appendix A.

Example causal factors/ hazardous scenarios: Engineer is not aware of what to look for/ what the signs are of loss of integrity due to lack of skills/ knowledge; Engineer unaware of how to apply the manufacturer guidelines when checking equipment (i.e. bolts on the fuel supply pipework) due to a lack of qualification/ competence.

5.3 Functional Requirements

To flesh out the full analysis, the performance requirements and performance influencing factors will need to be determined. Once the causal factors/ hazardous scenarios are listed, one must specify the performance-based requirements which would be put in place to prevent the occurrence of the causal factor and subsequently the unsafe control action.

Examples of performance requirements already listed in MSC.1-Circ.1321 include “Temperature of thermal insulated surfaces must be below 220 °C”, “insulation should be non-combustible and so supported that it will not crack or deteriorate when subject to vibration”, and “hose assemblies should be inspected frequently and maintained in good order or replaced when there is evidence of distress likely to lead to failure”. The corresponding influencing factors include aging, vibration, irregular inspections and overhauls, and quality of materials.

Specifically looking at the analysis carried out in this project, and looking at the causal factors (CFs) listed previously, we can present some functional requirements (FRs) generated as part of the analysis (full analysis presented in Appendix A):

CF1) Engineer is not aware of what to look for/ what the signs are of loss of integrity due to lack of skills/ knowledge

FR1) Engineers shall be able to recognise hot box and fuel supply pipework/ engine loss of integrity which can lead to H2-3.

CF2) Engineer unaware of how to apply the manufacturer guidelines when checking equipment (i.e. bolts on the fuel supply pipework) due to a lack of qualification/ competence

FR2) Engineers shall be familiar with equipment on board where a risk of H1-3 exists and trained on all potential actions required to be made on that equipment.

As a result of over 600 functional requirements being developed to prevent H1-3, these have been categorised into Unsafe Control Action categories (i.e. inadequate detection/ inspection), and Causal Factor categories (i.e. inadequate knowledge [training/ competence]).

As can be seen from the functional requirements, these can be achieved in multiple different ways, which are based on the discretion of the operator, company, or designer. There are many different routes to meeting the requirements allowing freedom in applying adequate fire safety measures to the facility. How the company achieves compliance with the functional requirement is down to their own SMS.

By implementing this novel type of analysis, fire safety can be addressed accounting for the entire system, and the interactions between controllers in a manner in which traditional risk assessment could oversee glaring failure modes. It also allows holistic fire safety to be applied without following prescriptive rules which may not provide ‘safety’ to all ships in all contexts.

The functional requirement above (FR1), for example, could be achieved by implementing new or existing technology which can recognise loss of integrity, which would change the control action requirement of the engineer. Equally the requirement can be fulfilled through a training and competence program to ensure engineers are aware of the signs of loss of integrity, to strengthen the robust nature of the inspection. The novelty is expanded further by

the documentation of such requirements for use in continual auditing of FRs, incorporated into the SMS.

This introduces the observations of barriers integrity. This is important, as the functional requirements may be demonstrated as being achieved during design or upon commissioning, however in the field these functional requirements may no longer be met through degradation of the barrier put in place. For example, the technology in place to detect loss of integrity may degrade over time and therefore lose accuracy, or a process may simply be lost over time meaning the functional requirement is no longer achieved. The staff member trained in detecting loss of integrity, for example, may move to a different ship, introducing a less experienced engineer to the ship who cannot detect the loss of integrity. Such degradation of barriers is crucial to monitor in order to ensure operational safety is maintained at the desired level. Equally as important is the verification that FRs are still valid. For example, a new technology may be introduced which makes a historical manual process obsolete. Continual verification of the design assumptions of the system would therefore ensure cost effectiveness in ending the previous FR and updating to make the requirement more relevant during operation.

Many of the FRs presented in Appendix A would seem to be obvious, however this does not mean specific barriers are in place to ensure the requirement is achieved. A site visit is conducted to validate requirements generated in the STPA are in place. This validation is presented in Chapter 6, and also begins to show the criticality in creating a direct link between the generation of the FRs and the auditing process in checking they are implemented and remain valid and effective.

5.4 Barriers and Signals

As previously discussed, the application of suitable barriers which can prevent an incident or hinder an incident leading to an accident is the aim of the approach. For this to be effective,

the health of such barriers is important to monitor such that the following questions can be answered:

- Is the process currently in or approaching the hazardous condition?
- Is it hazardous to carry out action ‘x’/ hazardous to postpone action ‘y’?

Such an approach relies on prognosis (prediction of what will happen if actions are carried out) as well as diagnosis (what is the current situation) to monitor the system health.

Barriers can be implemented to achieve the goal based functional requirement. Assigned barriers can include physical i.e. a wall; functional i.e. where preconditions are required for action; symbolic i.e. barrier requiring interpretation - signs, warnings, alarms; and incorporeal i.e. organisational rules. (67). Dependent upon the controller, the control action, the context the action is taken, the causal factor, and the subsequent requirement, any number of barriers (and types of barrier) can be applied.

The following Figure 11 presents some generic barrier functions and sub functions to control flammable materials. These provide an example of the types of barriers which can be applied in a similar application to that analysed in the case study, with a more generic approach.

-

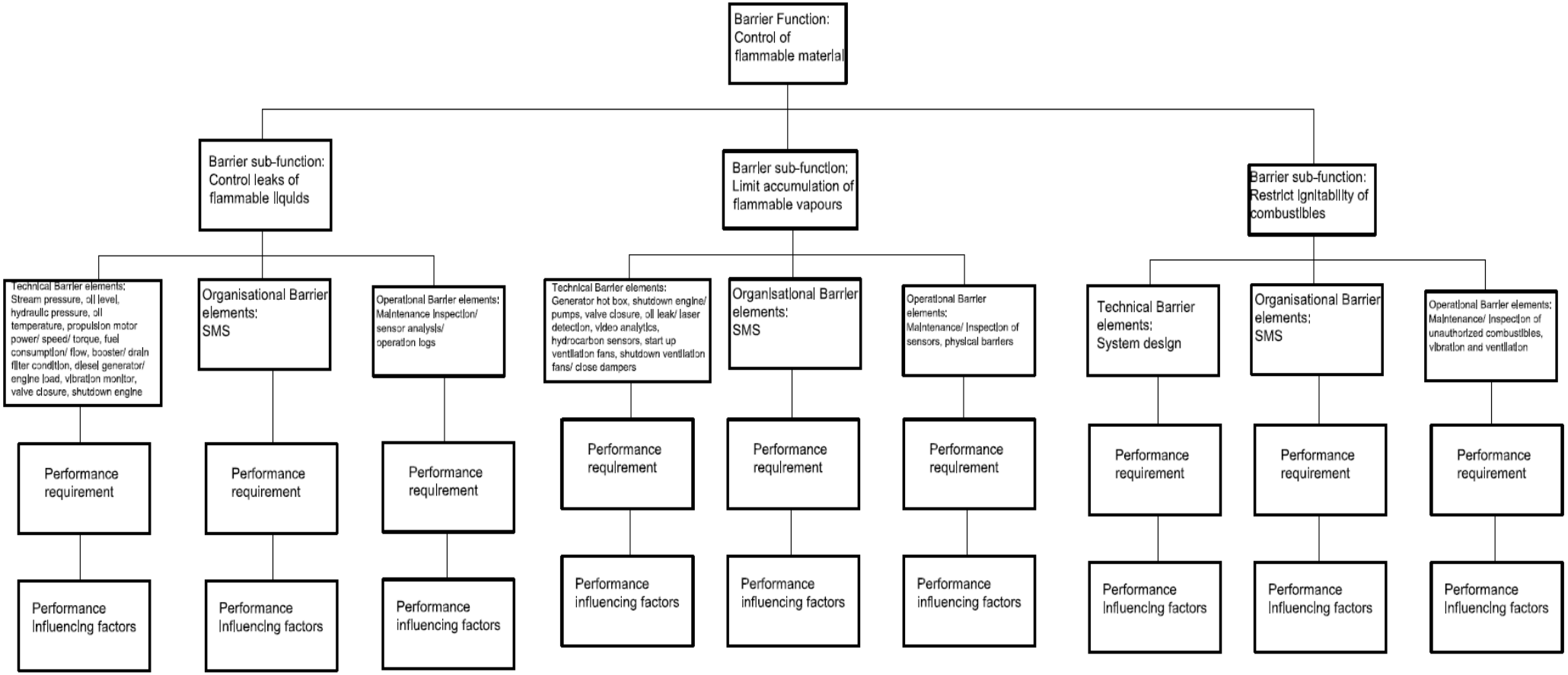


Figure 11: Generic functional requirements of the control of flammable/ combustible materials

Possible proposed barriers in the STPA which can be applied to comply with the functional requirements include a training and competency management system, adequate staffing and task allocation, tooling, and spares procedure etc. Example barriers are presented in the STPA to provide insight into possible routes to compliance with the functional requirement. These are not absolute requirements and would be beneficial to be tailored to the specific company and application.

With each barrier implemented, barrier degradation is a factor which must be monitored as discussed in the previous section. Sensors can be applied through technology, or through more procedural measures i.e. audits. Examples of signals to monitor barrier health presented in the STPA include an audit of procedural knowledge and compliance, audit of competence, indicator showing fault after a diagnostics test in a sensor etc. Monitoring the health of these barriers is critical in achieving a snapshot of 'real-time' risk. If the assumption during design with respect to the barriers in place is no longer valid, the holistic fire safety value will be changed. When the context of the ship changes and these barriers have degraded, this can lead to a potentially unacceptable level of risk.

5.4.1 Barrier Ranking

From the development of the barriers, it was determined that it could be useful to develop a ranking of the barriers from those which would provide a higher degree of risk reduction, versus the barriers which would only marginally improve safety. A method was therefore developed to rank barriers in order of effectiveness and criticality.

The proposed barriers (or if the barriers already exist, the measures to improve the barrier – from now on both cases will simply be referred to as the barrier) are required to be ranked to determine the greatest magnitude of risk reduction (MORR). It is therefore crucial to determine a metric for both effectiveness and criticality.

5.4.2 Barrier Effectiveness

The following table provides a review of different safety functions, with example barrier systems and an associated effectiveness level as developed earlier in this thesis and as

presented in Table 2 – shown again below in Table 8 for ease of reference. This definition is applied to rank the barriers in the SHORE methodology on a scale of 1-6.

Table 8: Research objectives effectiveness ranking of barrier systems (30)

Focus	Strategy category	Safety function	Example barrier systems	Effectiveness level (priority scale) (E)
Prevention	1	Eliminate hazard	Decisions at concept and detailed design stages (based on risk assessment, tests, and other studies): substitution, simplification, decoupling, replacement, etc.	6
	2	Prevent systemic factors of incident	Strong safety culture, effective inter-organisational links, industrial best practices, robust safety assessment methodology, flawless standards and practices and regulatory oversight	5
	3	Prevent contributing factors of incident	Safety management system (SMS), clear communication and responsibilities and roles, crew training and supervision, adequate manning, fire drills	4
	4	Prevent direct factors of incident	Passive and active safety systems (thermal insulation, leak prevention, condition monitoring, etc.), and their inspection and maintenance actions	3
Mitigation	5	Control accident (stopping from propagating to loss)	Management decisions (training, staffing, preventive maintenance etc.), automatic detection and suppression systems, emergency shutdown, ventilation control system etc.	2
	6	Reduce damage (loss)	Management decisions (training, staffing etc.), containment (structural fire protection, fire doors etc.), automatic and manual firefighting equipment and preparedness, evacuation equipment and preparedness	1

5.4.3 Barrier Criticality

Once the effectiveness is determined (how effective the barrier will be in controlling a hazardous situation early and maintaining control), the criticality of implementation of that barrier is reviewed. Within SHORE, the criticality focused on knowledge relating to historical occurrence of the causal factor to show how relevant the hazardous scenario was, how likely the hazardous situation is (i.e. even if it hasn't happened yet, could it?), whether barriers already exist to address the causal factor etc. Once these factors were assigned to the criticality metric, the following process was adopted to rate the criticality.

- Step One:

    - Low Priority: The causal factor is not currently known to have led to previous incidents. Go to Step 2.
    - High Priority (4): The causal factor led to previous incidents and is dealt with by existing barriers
    - Very High Priority (5): The causal factor led to previous incidents and is not dealt with by existing barriers.
- Step Two (for low priority):
    - Scenario is improbable and effective barriers are already in place - Very Low Priority (1)
    - Scenario is probable, but no record of incident in the past. Scenario is covered by existing barriers - Low Priority (2)
    - It is probable but not addressed/overlooked - Medium Priority (3)

It is important to note at this stage the importance of historical accident or near miss data in the criticality review stage. Should certain causal factors at the organisational level, for example, be omitted from the accident investigation, this could potentially result in an artificially low criticality metric for that causal factor. Consideration should be given to this in the analysis of the findings and future research into this field and that of accident investigation.

Near-miss investigations are also as important, as these can also demonstrate how successful the safety system was. For example, a fire almost occurred, but due to barrier ‘x’ or ‘y’ an accident was prevented. This can be a useful input to the STPA process in assigning barrier criticality.

5.4.4 Magnitude of risk reduction (MORR)

Once the effectiveness and criticality are determined, a standard risk matrix as depicted in Figure 12 is applied to show a magnitude of risk reduction for that functional requirement. In this matrix green represents a low priority as it is either covered already, is an unlikely event, or is an ineffective barrier. Conversely red is a high priority as it will be an effective barrier, is a likely event, or is not covered under the current application of fire safety.

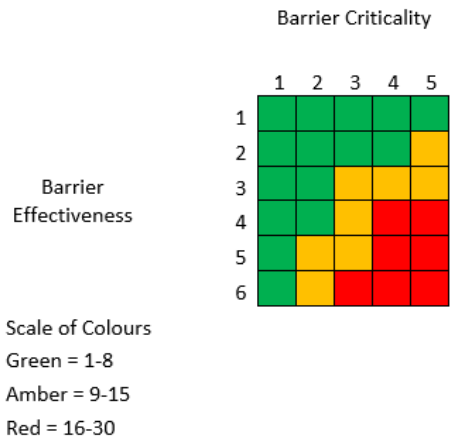


Figure 12: Risk matrix to determine magnitude of risk reduction (MORR)

Once the magnitude of risk reduction is determined, barriers can be applied to form the system which will demonstrate risk is ALARP. For example, a functional requirement with effectiveness of 5 and a criticality of 3 would be awarded the MORR of 15 (5x3=15). This functional requirement would therefore appear amber in the analysis, just short of appearing red. Application into a DBM system would then ensure these barriers will have continuous monitoring to show when a barrier has failed, is failing, or shows imminent failure, to allow a snapshot of risk to be determined. This will then influence behaviour through the organisation which will prevent further incidents, in this case fire. The specific magnitude of risk reduction which is lost by a barrier degrading can be analysed easily within SHORE and can provide a critical input to any future DBM system.

As the FRs were being ranked it became apparent that three trends were emerging in the analysis:

- The further the analysis gets from the process being controlled in the control diagram (physically), the fewer documented historical occurrences are presented of the specific failure, despite being noted as credible causal factors. This could show that they occur but are simply not recorded. If true, this will have a notable impact on the criticality value and also accident investigations.

- The further we get (physically) from the hazardous process in the control diagram, the higher the effectiveness value becomes.
- The further we get from the process (physically), the more the barriers/ signals become procedural/ organisational i.e. audit based.

5.4.5 Additional Considerations for Criticality – Ease of Implementation

In addition to the metrics applied in the analysis, an additional metric which will require practical consideration is the ease with which the barrier can be implemented. While these are not included in the initial fire safety model analysis, once specific barriers are determined these considerations can be taken into account to select the barriers which will be pursued, and those which would not provide a high cost effectiveness.

The following ease of implementation measures are noted for information only and can form an interesting route for future study in expanding on the SHORE process to also incorporate a cost effectiveness calculation. The scale applied is simplified to: 1 = easy to incorporate; 6 = difficult to incorporate.

1: Barrier exists and is currently audited (e.g. would simply need to be programmed into the real-time DBM monitoring)

2: Barrier already exists but is not audited (requires a new method of collecting the signals)

3: Barrier exists but is not used in fire prevention/ mitigation (requires a change in application and a method of collecting signals)

4: Barrier does not exist but could be put in place using known technology/ procedures

5: Barrier does not exist and would require new technology to implement

6: Barrier does not exist, and it is not known how such a barrier can be implemented (R&D required)

An example of a barrier falling within category one would be a verification of operational condition before breaking containment to ensure equipment is not interfered with while processing fuel oil at pressure for example. Conversely an example barrier which would fall under category 6 includes a vibration monitoring system which can detect strain across a

range of operating equipment (fuel transfer pipework, engines etc.) and pinpoint where the vibration exceeds a predetermined threshold where failure can occur.

This metric system was consciously applied when selecting the FRs to be audited in Chapter 6 to ensure barriers which could be incorporated/ strengthened with relative ease (i.e. should already be in place) were analysed. This led to some interesting findings on the pressure sensor network related to the oil transfer system. This is expanded in the findings and is a primary contribution in the verification of the hypothesis on fire safety improvements applying this method.

5.4.6 Additional Considerations for Criticality – Magnitude of Safety

The magnitude of safety element allows us to assess the requirements which are functional and instruct what to do, but not how to do it. If a specific requirement, when addressed and monitored therefore considered healthy, will eliminate many causal factors, the magnitude of safety for that requirement can be considered high, therefore favourable. This idea is represented in Figure 13, which is representative of the traditional fault tree type analysis:

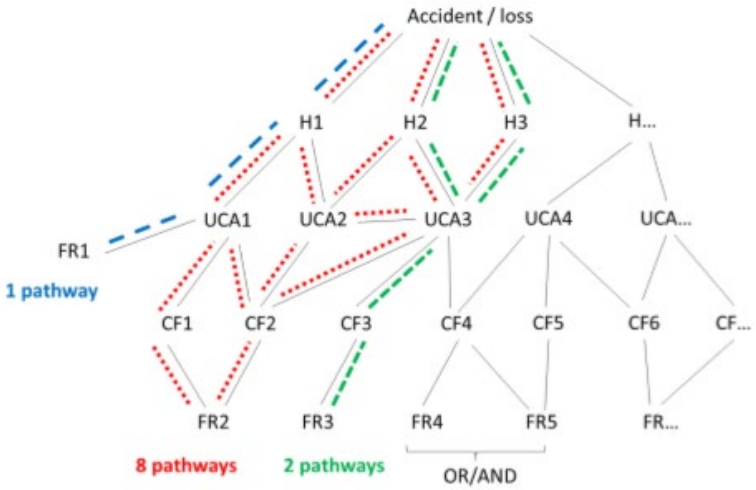


Figure 13: Pathways to an Accident/ Loss through varying causal factors and unsafe control actions (196)

Such an approach is not considered in the STPA for effectiveness or criticality as it can fall into the same failings as traditional fault tree analysis type causal factor analysis. The philosophy behind it can, however, assist along with the ease of implementation and cost benefit analysis of determining which barriers are to be implemented and monitored in practice

to demonstrate risk is ALARP, dependent upon the company's position on quantitative analysis of risk reduction etc. and traditional fault tree analysis.

Careful consideration shall be applied, however, as this will provide results highly focused on the designer's previous experiences. If the designer carrying out the STPA implements many slightly varying causal factors for why an engineer doesn't carry out an inspection as a result of their pre-set biases (for example taking too long a lunch break, sleeping in, forgetting to carry out the inspection) this can add priority to the functional requirement of ensuring staff have a task list which is fulfilled in a timely manner. If the designer considers only one causal factor for the engineer not being able to understand the maintenance requirement (for example it is in a different language), this would result in a low magnitude of safety for the functional requirement of ensuring maintenance instructions are clearly defined and easily understood. In reality the engineer may not understand the maintenance procedure because he/ she is not sufficiently trained, the maintenance procedure is not written in a clear way, the maintenance procedure is for a similar but different piece of machinery etc. The functional requirement would deal with all these causal factors, so it is not crucial to record them all, but as they were not all implemented in the analysis, the magnitude of safety is artificially low. It is important to note not all causal factors, with their subtle differences, can be captured and so the process shown in Figure 13 may not present the most robust way of assigning criticality or effectiveness to the functional requirements in every case. It is, however, useful in demonstrating the causal web towards incidents and accidents.

Additional points of note upon completion of the STPA for this specific application include the fact the higher we go in the control diagram (further from the sharp end), the greater the criticality factor reduces, while the effectiveness increases. This appears to be primarily due to the metrics which are applied – criticality is based on previous experience of the event, but as discussed earlier, documented evidence of the failures being caused this high up the hierarchy becomes difficult to source. This can likely lead to an under representation of criticality further from the sharp end, which is worthy of further review when applying the method in practice.

In the higher controllers (further from the sharp end), it is credible to surmise that this method and process has generated causal factors and functional requirements one would not consider when applying traditional hazard analysis techniques i.e. Casual Factor 5.2 in the 'Company' controller: "Company does not appreciate the time sensitive nature of the resource request in order to prevent fire on the ship". Such a hazardous scenario is not typical of traditional hazard identification techniques; therefore, it is reasonable to assume such a causal factor would not be addressed in the safety system of a traditional assessment. Equally as the original assumptions made during the design were not accessible during the case study shows the importance of documenting such assumptions which, even if they are accounted for within the traditional approach, are not documented. This shows a useful impact of the analysis which will be elaborated further with specific examples of the findings in Chapter 6. The method of HAZID and audit, and particularly the coupling of the two also demonstrate novelty in the approach, the basis of which is documented in Chapter 7 to be applied in similar applications, or even to be opened up to a far wider audience.

5.5 Next Steps

Once the HAZID and requirements specification as described in this section were completed using the initial stages of the SHORE methodology, an auditing template was generated for validation purposes of the STPA. This would also prove useful in investigating if there is benefit in having the HAZID, requirements specification and audit all directly connected within the methodology. The results of the validation are now discussed in Chapter 6, with the detailed discussion of SHORE, after being validated, presented in Chapter 7.

6 Validation of the STPA and Proposed Approach

6.1 Audit Process

To validate the results of the STPA, an on-board audit of the Allure was carried out. The initial purpose and proposition of the audit was to consider the following:

- Does the appreciation of importance generated in the STPA align with personnel on the ship for the following?
    - Effectiveness
    - Criticality
    - Magnitude of risk reduction
- Are the functional requirements being complied with?
- Is there a trend between the perceived important barriers (i.e. high magnitude of risk reduction) and compliance?
- Are there any functional requirements queried which the ship have not considered?
- What is the level of uncertainty regarding fire safety functional requirements? For example, answers of ‘Don’t Know’ demonstrate a high uncertainty, therefore possible greater risk
- Is there a benefit in the audit questions being derived directly from the HAZID in finding gaps?

The checklist applied in the audit is provided in Appendix B. The novelty and impact of basing the audit directly from the STPA was also subject to investigation after the audit was completed as part of developing the SHORE methodology. This analysis is critical as presented in Chapter 7.

The initial challenge facing the audit, however, was the volume of functional requirements developed during the STPA. With over 600 functional requirements developed it was not credible to audit them all a single audit. An approach was therefore developed to audit a

representative range of the developed functional requirements to fulfil the aims of the audit listed above.

A selection of functional requirements meeting the following rules were selected to provide a suitable spread:

- Audit only the ‘Ship/ Control Room’, ‘Engineer’ and ‘Ship Automation’ controllers
- Functional requirements from each of the three controllers were selected, covering a mix of the following:
    - High effectiveness, low criticality
    - Low effectiveness, high criticality
    - High magnitude of risk reduction (high effectiveness and criticality)
    - Low magnitude of risk reduction (low effectiveness and criticality)

The format in which the audit was to take place was also determined using the following approach:

- For each Functional Requirement, the checklist presents the Unsafe Control Action, Causal Factor and Functional Requirement to the auditee
- Auditee is then asked:
    - Is the functional requirement addressed: Yes; No; Don’t Know.
        - If yes provide evidence
        - If the answer is ‘No’ or ‘Don’t know’… Why?
    - Auditee is asked how they would rank the importance of the functional requirement for ‘effectiveness’ (scale of 1-6) and ‘criticality’ (scale of 1-5)
        - Definitions of effectiveness and criticality to be presented by the auditor

The audit was carried out by an experienced auditor from DNVGL who had been briefed on the SHORE methodology and the aims of this specific audit. Of the 7 personnel audited, the positions were made up of the chief electrical engineer, three duty engineers, the first

electrician, first engineer and staff chief. Personnel were only audited on those sections relating to their specific position. The duty engineer 3 and Staff Chief did not provide any effectiveness or criticality figures therefore these sheets have been omitted from the analysis. Once the format was set and the nature of the audit confirmed, the audit presented four objectives to fulfil the previously discussed aims:

1) Verify if there are gaps in compliance with the Functional Requirements (FRs) developed in the STPA
2) Validate the risk rankings (a-c) set within the STPA against the perceptions on the ship
    a) Magnitude of Risk Reduction (MORR)
    b) Effectiveness
    c) Criticality
3) Verify if the perceptions of FR presence & importance align between auditees on board the ship
4) Determine any benefit in finding gaps by deriving the audit directly from the HAZID

The first aim is important as it would provide the verification if potential fire safety measures were simply not implemented. This also allowed me to verify if there was a trend between an individual's perception of a MORR associated with a functional requirement, and whether they would state if it was complied with or not. This also allowed me to validate if individuals on board were in agreement of what safety systems are in place.

Prior to the audit, the ranking of the functional requirements was carried out in the STPA and validated with the workshop team of onshore based experts, so consensus was achieved on the assumptions and values used. The 2nd requirement of the audit was to verify if there was a consistency between the perceptions of those onshore and those on board the ship. This would provide a critical stage of validation as if these values presented discrepancies I could potentially see a hazard emerge through a variation in risk and hazard perception between

those who design/ specify/ manage the safety systems, and those who maintain/ respond to these systems in the field, at the sharp end.

The 3rd aim of the audit was also critical as if individuals on board have differing perceptions of the hazards with each other, this can lead to the same problems associated with the 2nd aim. If the hazard prevention strategy then becomes dependent on the specific individual dealing with a situation and what their specific perception of that hazard and the presence of the safety system is, this could present uncertainty and a break in the chain of successful fire prevention.

The final aim pertains to the novelty and potential impact of the SHORE methodology. Should there be a demonstrable benefit in directly linking the HAZID and operational risk evaluation this will show not only an industrial impact, but potential academic impact also.

Full results from the audit are provided in Appendix C.

6.2 Audit Results

The following shows the collated results of the auditee's perception of importance of a barrier, categorised by compliance or otherwise for that functional requirement. Auditees assigned values for MORR and stated whether the ship was in 'Compliance', 'Non-Compliance', or 'Don't Know'.

A Functional Requirement was determined as important if the MORR value was 9 or higher. This was taken from the agreed risk matrix within the STPA.

The graph shows the total number of FRs against whether they were in Compliance, Non-Compliance or Unknown, split between the auditee's perception of important or not important.

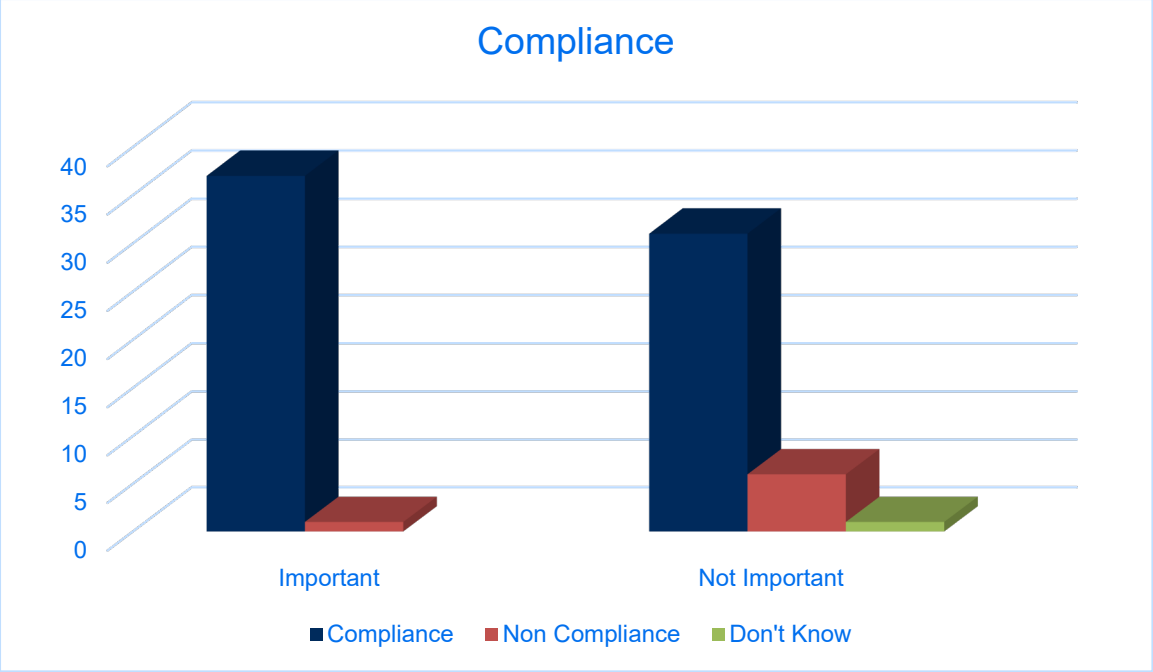


Figure 14: Comparison of perceived functional requirement compliance

It can be noted from this that there is no immediate correlation between MORR and compliance, however more perceived 'Important' FRs are complied with. It can also be noted the level of compliance is very high – only eight non compliances, only one of which was 'Important' (one of the non-compliances does not have an auditee assigned MORR and is therefore excluded from the chart). Equally as interesting is the finding that there was only one single response of 'Don't know'. This shows a relatively high degree of perceived certainty on which barriers are in place, and which barriers are not. This does not mean the barriers are in place as we will see, but simply that the auditees have a high degree of certainty in their position.

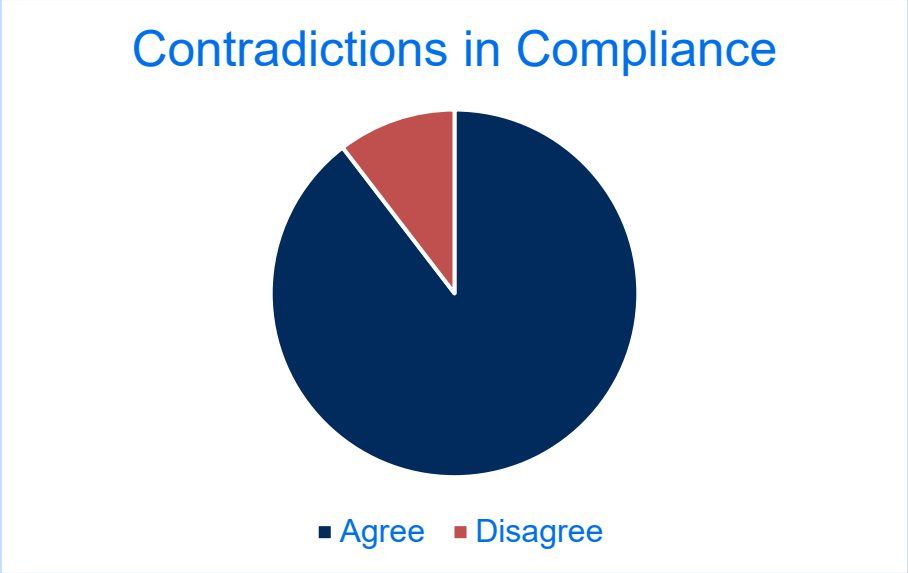


Figure 15: Contradictions in perceived functional requirement compliance

Of the 48 FRs included in the audit, only 5 resulted in a difference in opinion on whether the FR was complied with or not as shown in Figure 15. The two auditees who were questioned on the ECR controller both agreed that all FRs were complied with. In contrast, the two auditees who were questioned on the automation controller did not always agree on what barriers were in place.

The first auditee stated FRs 1, 5 & 6 were not complied with, whereas their counterpart stated they are were complied with. That same auditee also stated FRs 4, 12 & 16 were not complied with, whereas the first auditee stated they were all complied with (however FR 16 was left blank in the case of the first auditee).

This did demonstrate, however, that there are no corroborated non compliances. Where two auditees were questioned on the same controller, there were no corroborated statements of non-compliance.

In the entire audit there was only one FR which was regarded as important which was not complied with. This was the following:

- **Unsafe Control Action:** Ship automation does not alarm to pressure deviation in the oil systems (H2-3)

- **Causal Factor:** No feedback exists on stream pressure because no sensor is in place, resulting in no alarm signal on pressure deviation, resulting in pipework rupture
- **Functional Requirement:** Stream pressure shall be known to the process controller.
- **Explanation from Auditee:** No system to indicate high pressure. However, drop in pressure will result in an alarm

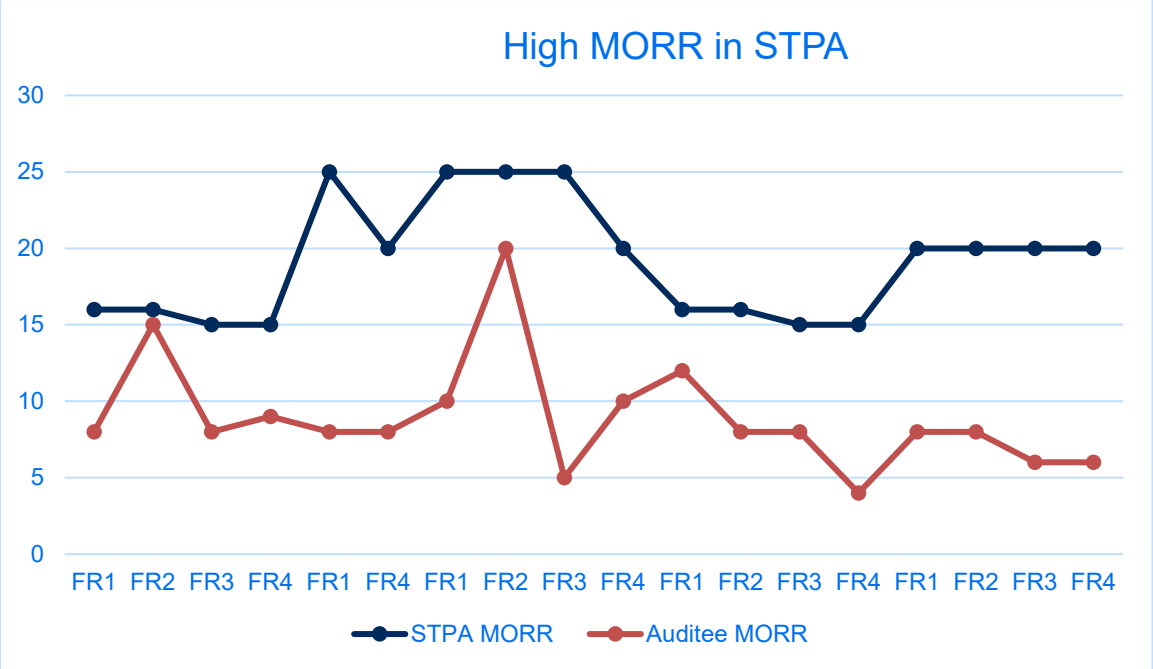
This same causal factor was stated as complied with by the other automation controller audited:

- **Explanation from Auditee:** Pressure sensors are fitted to detect high or low pressure

This deviation will be addressed further in the discussion surrounding non-compliances and alternative FR compliance but already shows impact from the novelty of deriving the audit directly from the HAZID. A potential non-compliance has been discovered which the onshore team believed was in place. Regardless of whether such a system is in place, the finding will have relevance in achieving systemic fire safety.

The next aim of the audit focused on perceptions of the risk and how these perceptions compared to those of the onshore working group, and how these compared between auditees. The following shows a summary of the comparisons of auditee perceptions of MORR and effectiveness/ criticality compared to the perceptions of the STPA as verified by the onshore working group.

These results show the comparison of perceived importance of the functional requirement within the STPA working groups the auditees



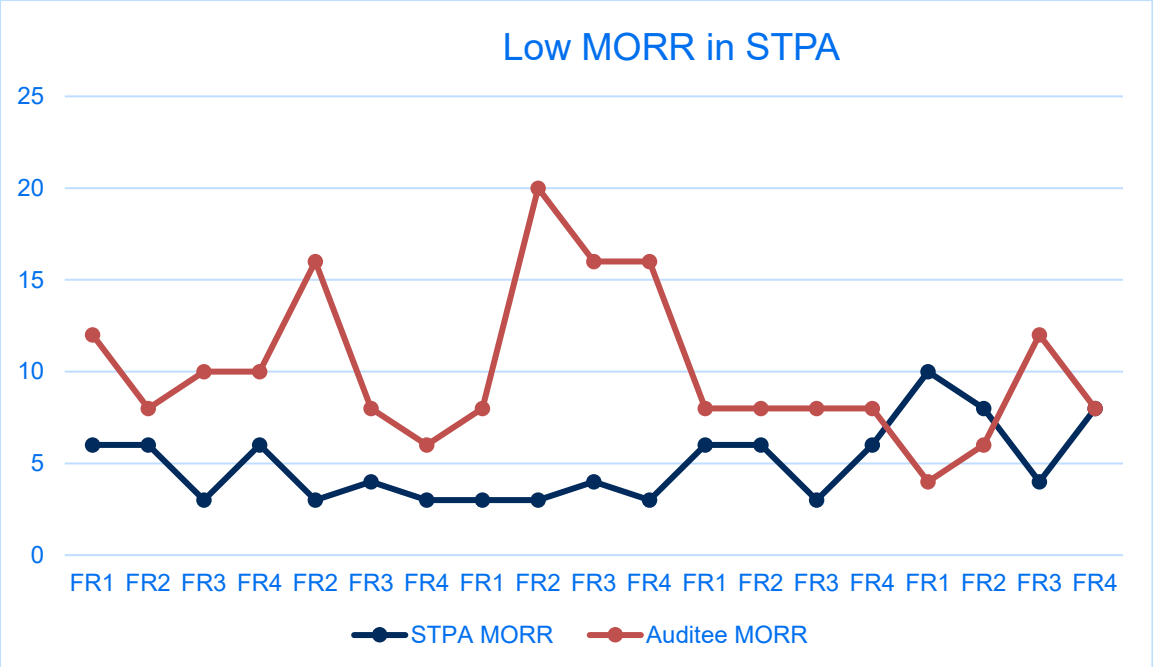
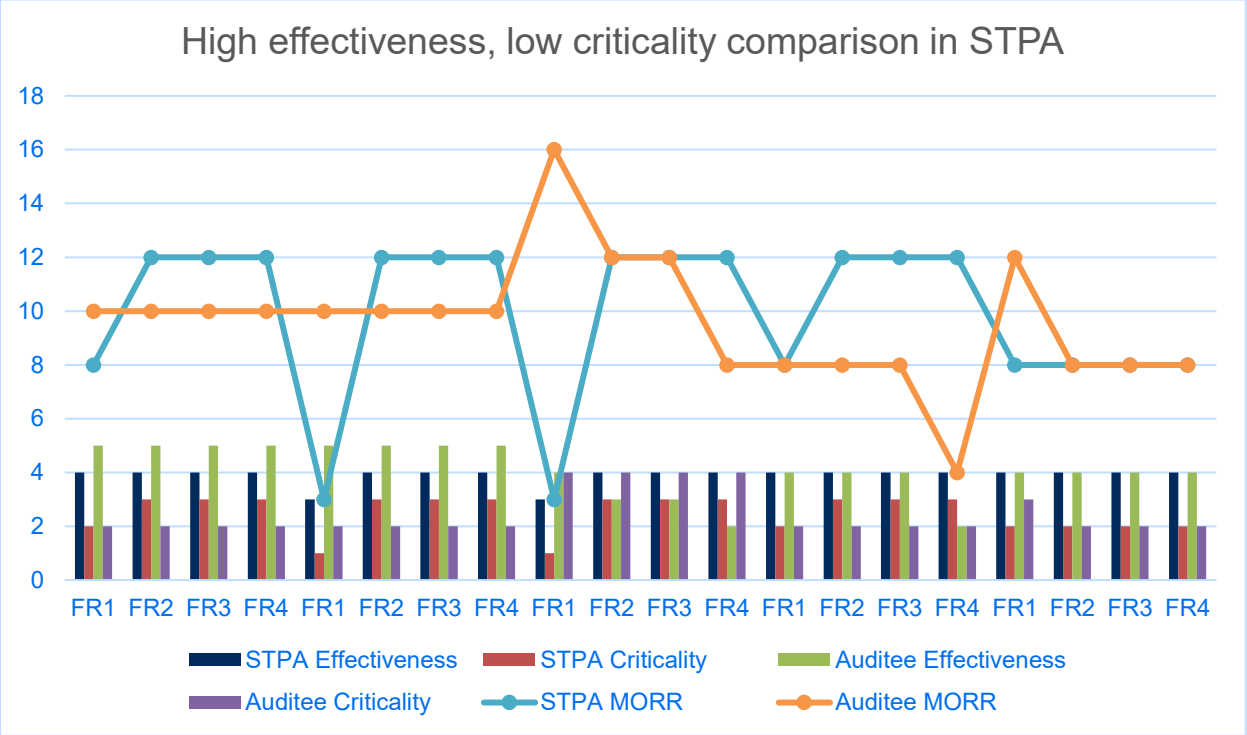


Figure 16: MORR comparisons between working group and auditee

From this comparison I note that where the STPA group viewed the FR as having a high MORR, the auditees perceived it to be of low MORR. Conversely where the STPA group viewed the FR as having a low MORR, the auditees perceived it to be of high MORR. This shows the first contradiction in hazard perception between the analysis in the STPA verified by the working group onshore vs. the staff on board the ship.

The following results show the comparison of perceived ‘effectiveness’ and ‘criticality’ of the functional requirements within the STPA working group vs. the auditees, overlain by the MORR value for reference.



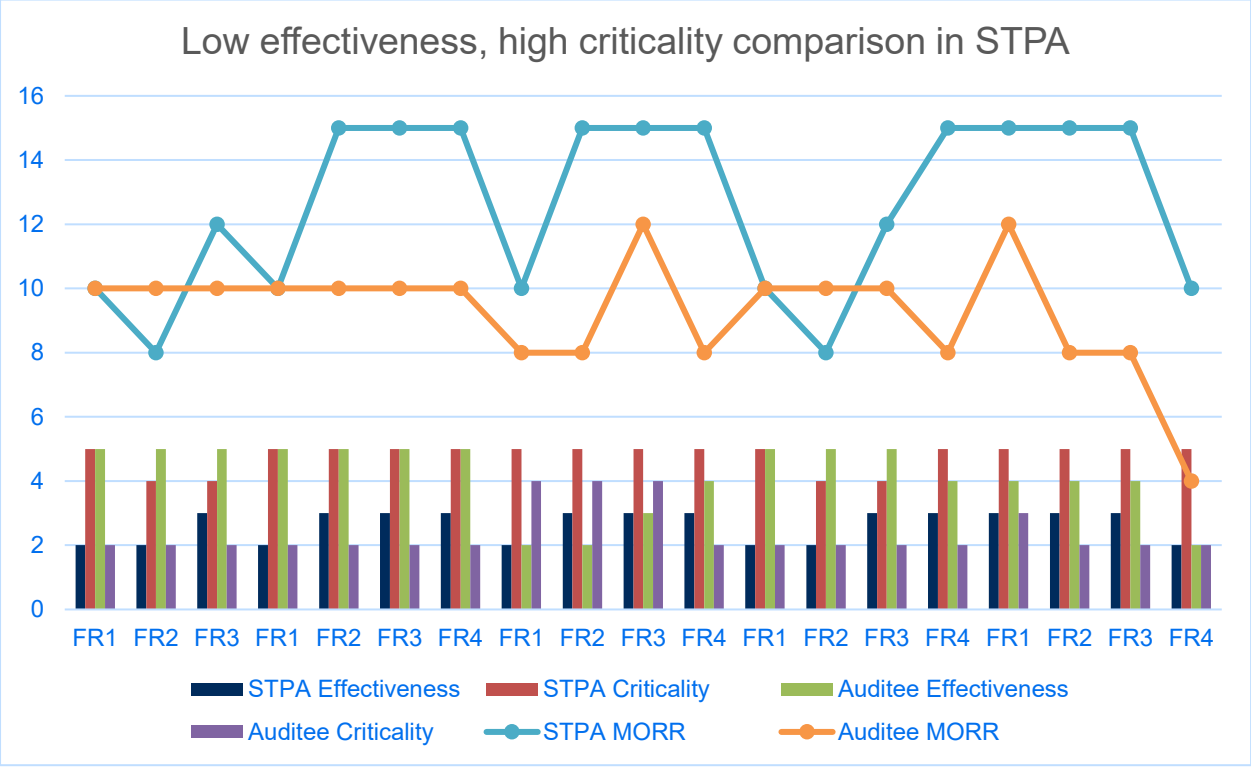
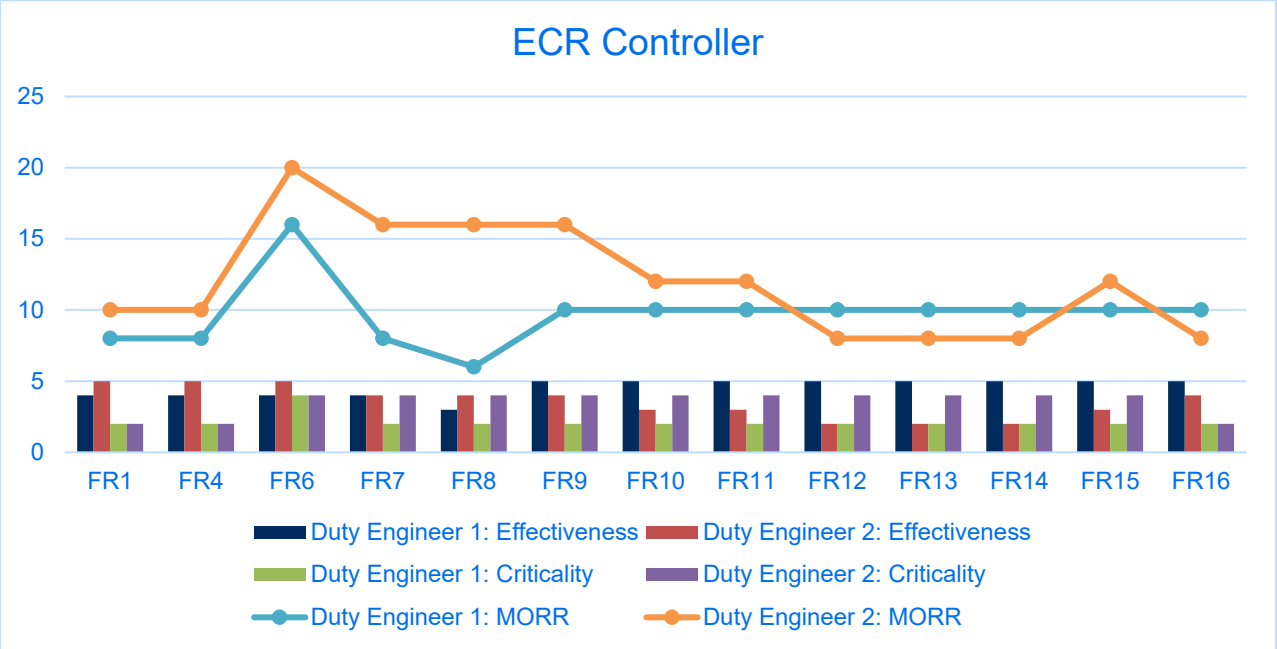


Figure 17: Criticality and Effectiveness comparisons between working group and auditee

From this comparison the author notes in the first graph of Figure 17, that STPA working group and auditee classification of effectiveness and criticality generally track with each other, with the auditee effectiveness grades being regularly higher than the criticality, as anticipated by the working group. This shows a relative corroboration between the working group and the staff on the ship but appears to be the only set of FRs where this happens.

The second graph returns to a deviation between ship and onshore and shows that the auditees class the effectiveness consistently higher than both the STPA working group's effectiveness, and also higher than their own criticality grade, showing a consistent discrepancy between the working group and the auditees perceptions of effectiveness and criticality for this set of FRs.

Of interest in the audit is also the spread of individual perceptions of effectiveness and criticality on board the ship. The following figures present a comparison between the two personnel audited on the ECR controller, and the two personnel audited on the Automation controller. Note as only one individual was audited on the engineer controller, no comparison can be made for this. Where an auditee did not provide a value for effectiveness or criticality this FR does not appear on the graphs.



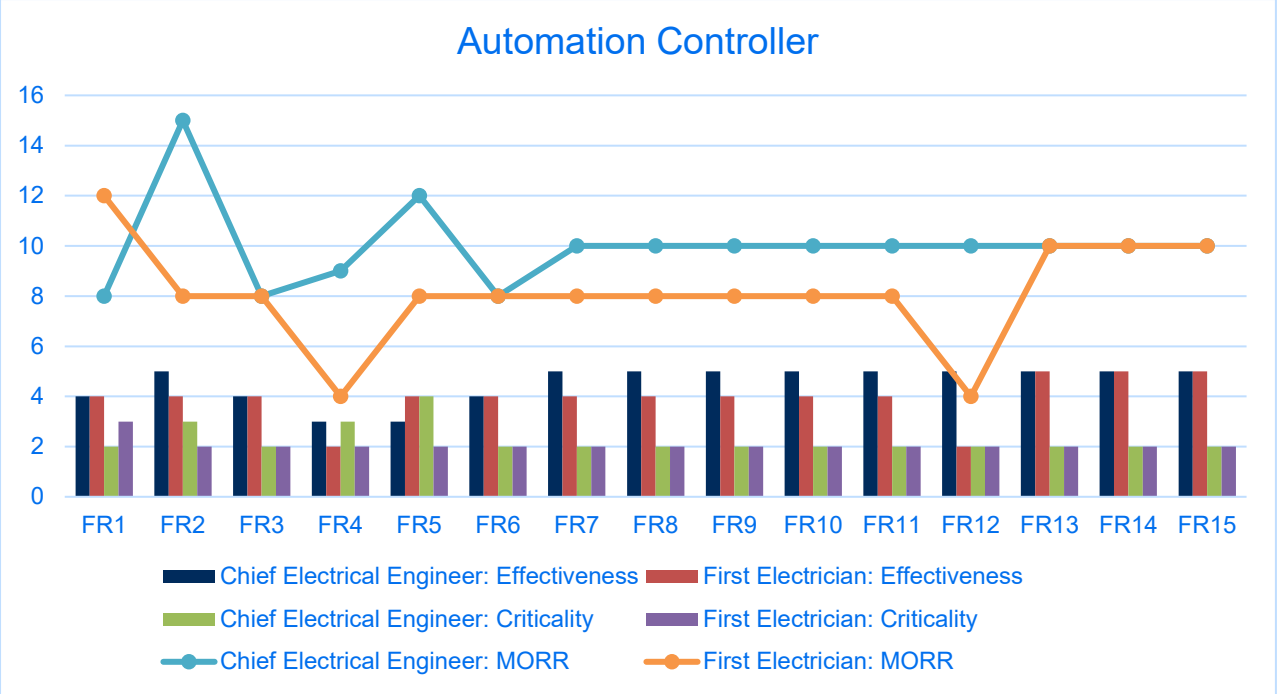


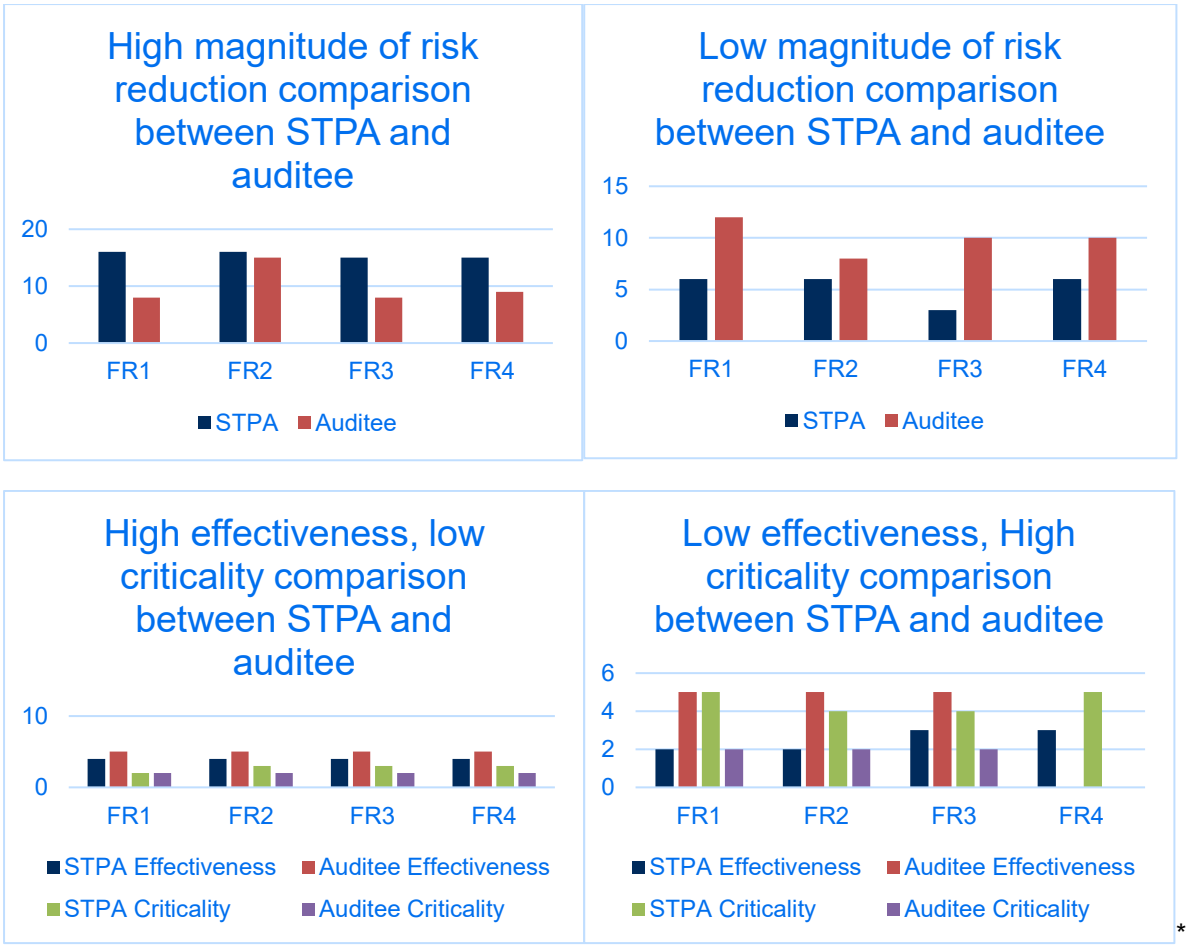
Figure 18: Effectiveness, criticality, and MORR comparisons between auditees

What we can see from the results is a general tracking of the individuals on board's perception of the magnitude of risk reduction, with a few individual outliers for each controller i.e. FR 7&8 on the ECR controller, and FR2, 4 & 12 of the automation controller. The automation auditees have a closer tracking on individual effectiveness and criticality metrics than those queried in the ECR.

The following details a description of the primary findings from each audited individual. For the avoidance of doubt, the results generated in the STPA and validated by the working group will simply be referred to as the results of the 'STPA'.

6.2.1 Chief Electrical Engineer (Automation Controller)

The following figures represent some of the extracted findings of the audit aimed at meeting the objectives discussed above.



*

Figure 19: Chief electrical engineer rankings

**Some values were not populated during the audit. These have been left blank.*

It is noted that the chief electrical engineer estimated the MORR of the functional requirements lower in the FRs which the STPA had ranked among the highest. By contrast in the FRs which the STPA ranked as insignificant, these were ranked significantly higher by the auditee.

For the high effectiveness, low criticality FRs, there is a trend of agreement between the auditee and the STPA, however with the low effectiveness, high criticality comparison, the auditee ranks the effectiveness much higher than the STPA, and the STPA ranks criticality much higher than the auditee for the same FRs.

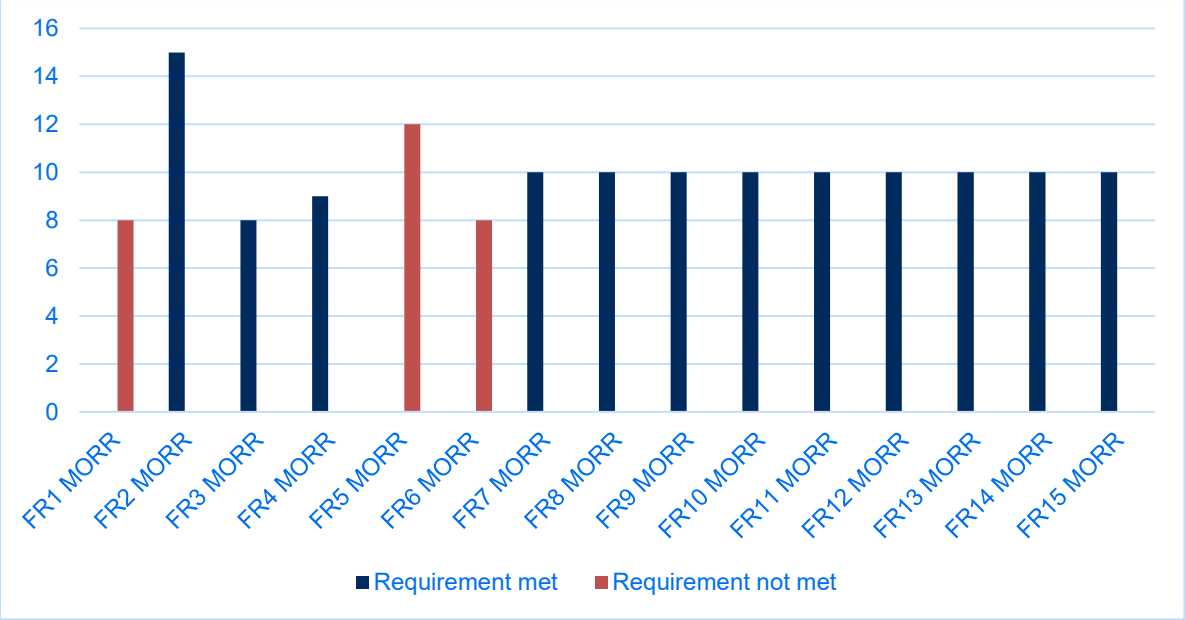


Figure 20: Chief electrical engineer statements of compliance

**FR16 was stated as not being complied with however values for Effectiveness and Criticality were not provided.*

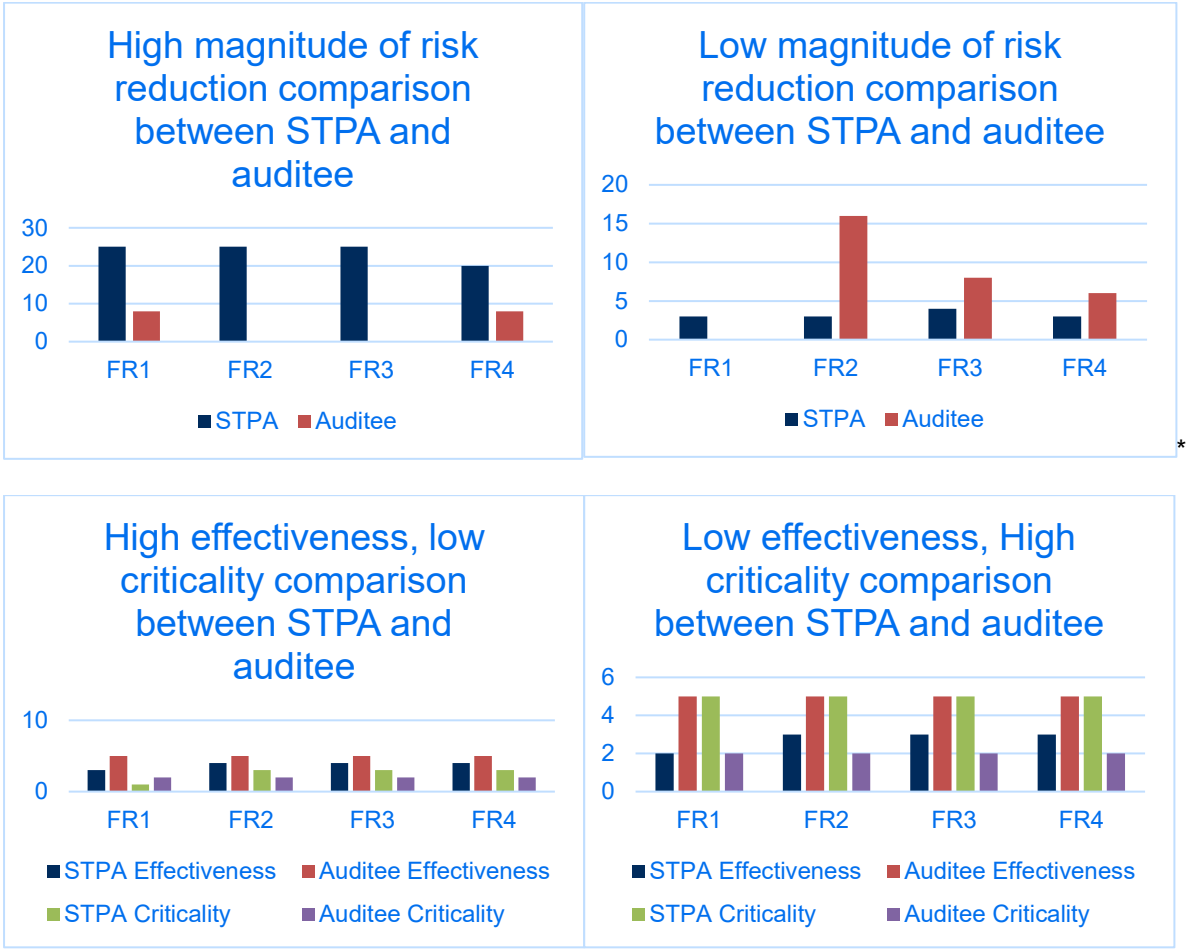
There appears to be no reasonable trend in the auditee's classification of MORR compared to whether the FR is complied with or not. This is shown by a consistent spread of risk reduction magnitude, and the lower value of risk reduction (8) resulting in one FR being complied with and one not.

Additional points of interest from the response by the chief electrical engineer are the following observations:

- No systems are in place to detect potential breach of the SOLAS requirement of eliminating exposed hot surfaces over 220°C.
- No high-pressure sensors in pipework which would indicate potential conditions for a break in containment, but low-pressure sensors are there to detect when a leak has occurred.
- Low pressure warnings are also present to prevent engine damage rather than as a fire safety measure.

6.2.2 Duty Engineer 1 (ECR Controller)

The following figures represent some of the extracted findings of the audit aimed at meeting the objectives discussed above for the Duty Engineer.



*

Figure 21: Duty engineer 1 rankings

**Some values were not populated during the audit. These have been left blank.*

It is noted that the duty engineer estimates of the MORR in a manner opposed of that shown in the STPA. Those FRs noted as high MORR in the STPA were found to be of low value to the duty engineer, whereas those viewed as least important by the STPA were viewed as highly important by the duty engineer.

This trend continued with the low effectiveness, high criticality comparison, with the auditee ranking in the opposite direction as the STPA. No discernible trend appeared in the high effectiveness, low criticality category.

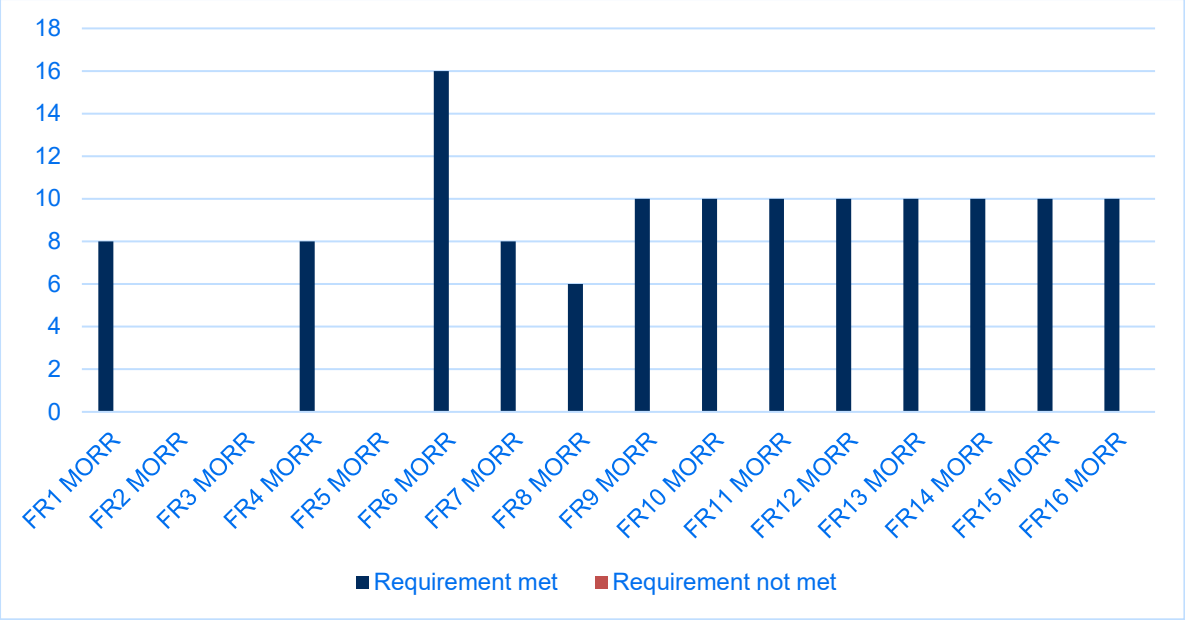


Figure 22: Duty engineer 1 statements of compliance

There appears to be no reasonable trend in the auditee's ranking of MORR compared to whether the FR is complied with or not. It was noted that every FR was responded as being complied with. In this respect, the ranking of MORR became redundant.

Additional points of interest from the response by duty engineer 1 include the following observations:

- One of the responses regarding hot surface detection referred to the Autronica flame detection system. This may highlight the issue of conflating prevention and mitigation, and potentially not being able to comply with the SOLAS requirement regarding exposed hot surface prevention.
- Some responses refer to a FR being complied with due to experience gained in previous company/ ship. This could highlight a perception of compliance based on previous experiences assumed to be relevant to the new position and ship.

6.2.3 Duty Engineer 2 (ECR Controller)

The following figures represent some of the extracted findings of the audit of the duty engineer 2.

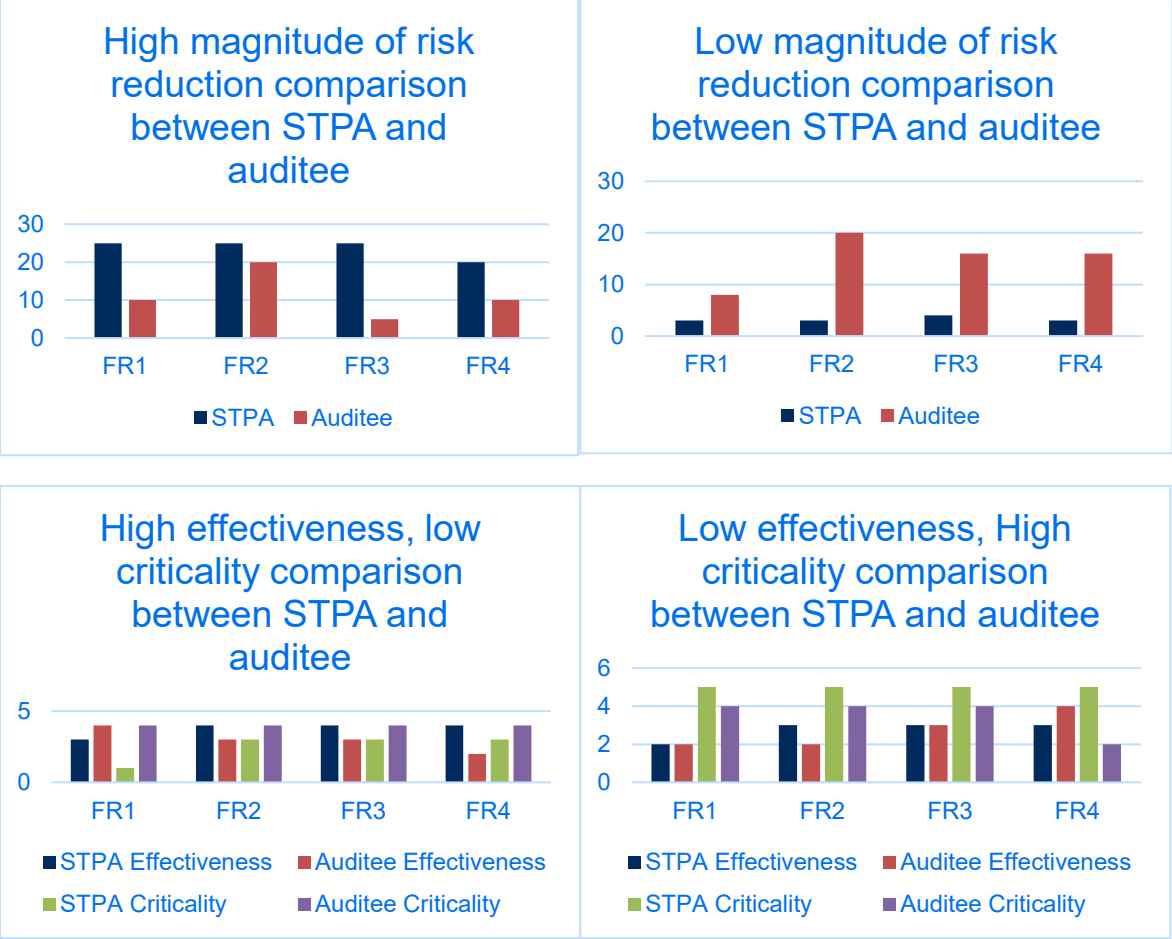


Figure 23: Duty engineer 2 rankings

For those FRs rated as high in MORR in the STPA, duty engineer 2 consistently estimated a lower value, while providing a much higher estimate of MORR for those rated lowest in the STPA.

Effectiveness and criticality values show very little trending between STPA and auditee. There are also a small number of FRs where there is a significant discrepancy (FR1 in 'High effectiveness, low criticality' and FR4 in low effectiveness, high criticality).

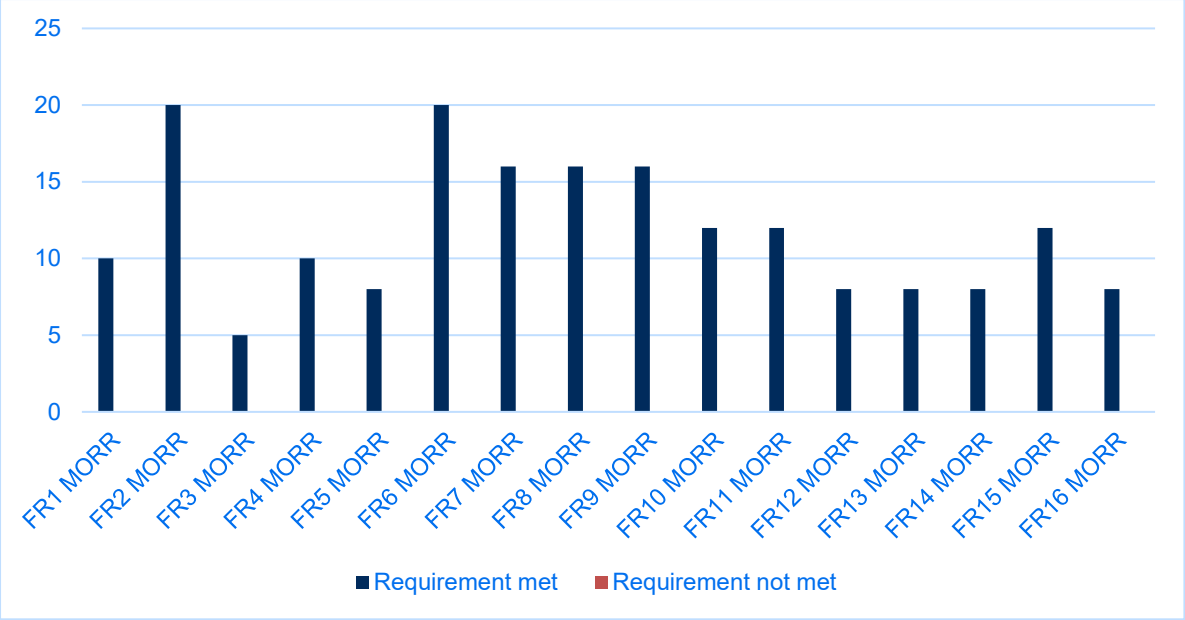


Figure 24: Duty engineer 2 statements of compliance

As with previous auditees, there appears to be no reasonable trend in the auditee's class of MORR compared to whether the FR is complied with or not as it is noted that every FR was responded as being complied with.

The following observation is also presented:

- As with the previous Duty Engineer, one of the responses regarding hot surface detection referred to the flame and smoke detection system. This could possibly highlight the issue of conflating prevention and mitigation, and potentially not being able to comply with the SOLAS requirement regarding hot surface detection.

6.2.4 First Electrician (Automation Controller)

The following figures represent some of the extracted findings of the audit of the first electrician.

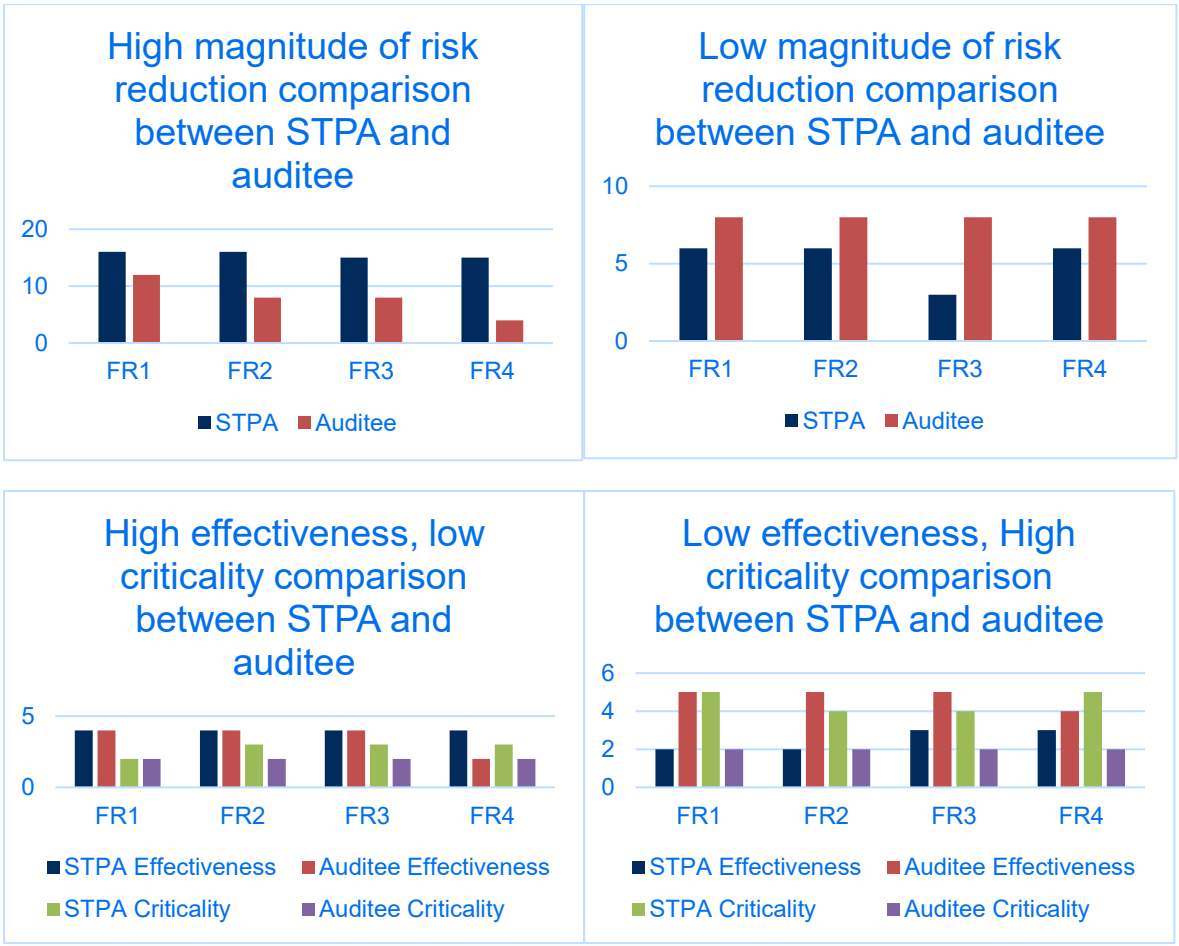


Figure 25: First electrician rankings

It is noted that the first electrician consistently estimated the MORR of the functional requirements lower in the FRs which the STPA had ranked among the highest, while in the FRs which the STPA ranked as insignificant, these were consistently ranked higher by the auditee.

For the high effectiveness, low criticality FRs, there is a general trend of agreement between the auditee and the STPA, however with the low effectiveness, high criticality comparison, the auditee ranks the effectiveness higher than the STPA, and the STPA ranks criticality higher than the auditee for the same FRs.

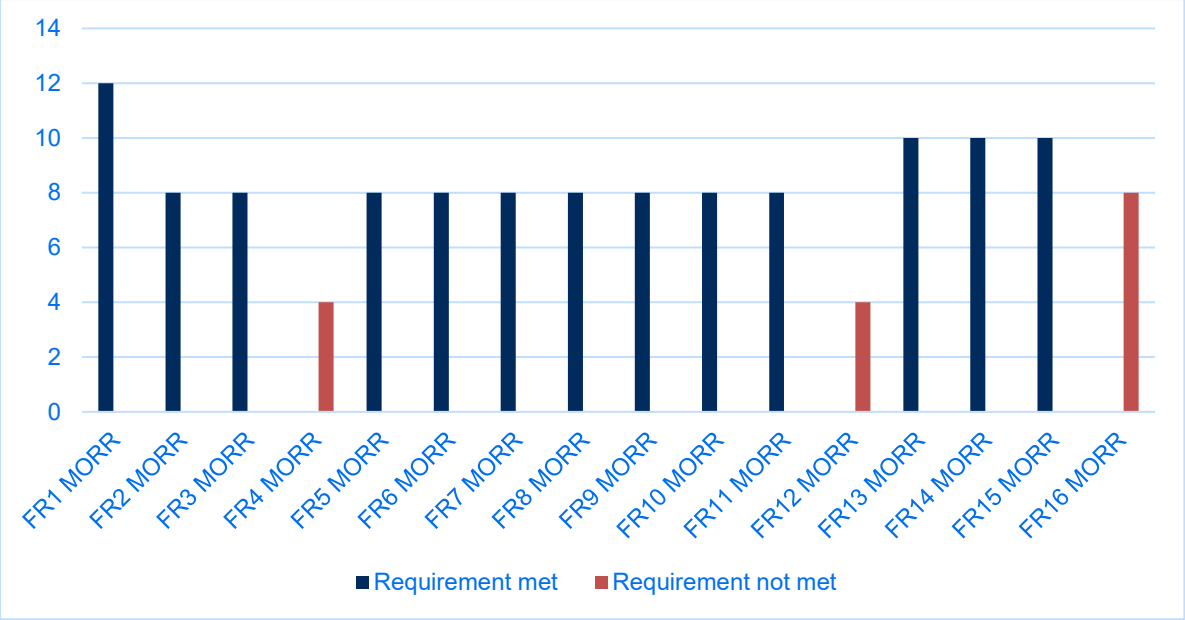


Figure 26: First Electrician statements of compliance

Regarding a link between the perceived MORR and whether the FR was complied with, the two FRs which the first electrician ranks as the lowest are not complied with, while those ranked with a value of 8 or higher, with one exception, are complied with.

Additional points of interest from the response by the first electrician are the following observations:

- It is stated there are no temperature sensors fitted to monitor for hot surfaces, in contradiction with other auditees (albeit reference is made elsewhere to smoke and heat detection). Whether there are sensors fitted or not, this contradiction could show a potential failure in the SMS.
    - 1) if sensors are fitted, this is not widespread information commonly known by all engineers, which could lead to a failure in the control/ feedback loop.
    - 2) If there are no sensors, some of the other engineers believe there are which could present a creep into failure based on perceived safety systems which do not exist.
- Many responses were of the form ‘this is checked regularly’ or ‘they are trained’ (paraphrased), without specific reference to a procedure, set timescale or minimum

training requirement. There could be gaps in what is perceived, and whether this is adequate as per the design assumptions.

6.2.5 First Engineer (Engineer Controller)

The following figures represent some of the extracted findings of the audit of the first engineer.

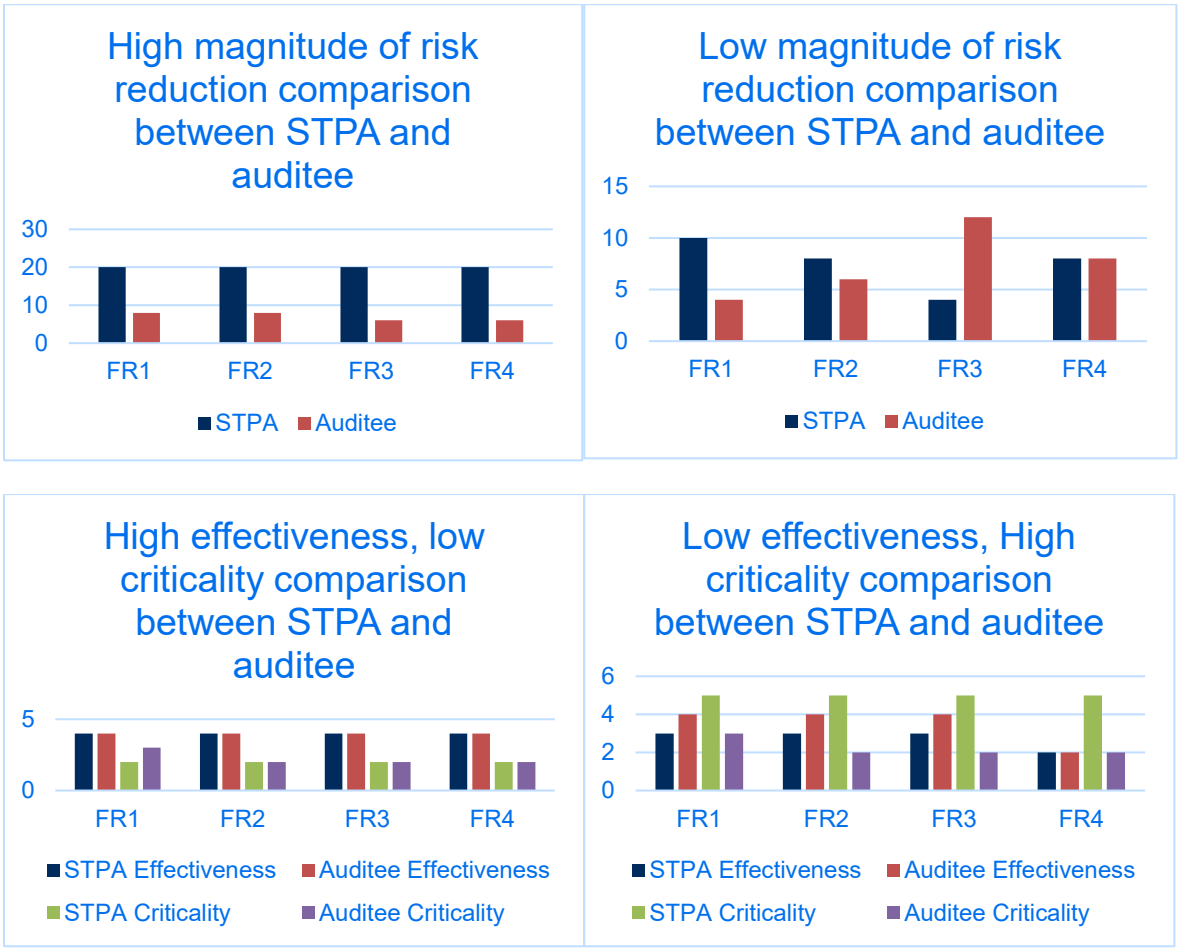


Figure 27: First engineer rankings

It is noted that the first engineer estimated the MORR consistently low when the STPA estimated it high. For the FRs which the STPA ranked as insignificant, there was more consistency between the STPA and the auditee, although these were only aligned in one instance.

For the high effectiveness, low criticality FRs, there is an almost matched agreement between the auditee and the STPA, however with the low effectiveness, high criticality comparison, the

auditee ranks the criticality consistently higher that the STPA. Effectiveness in this range is comparable.

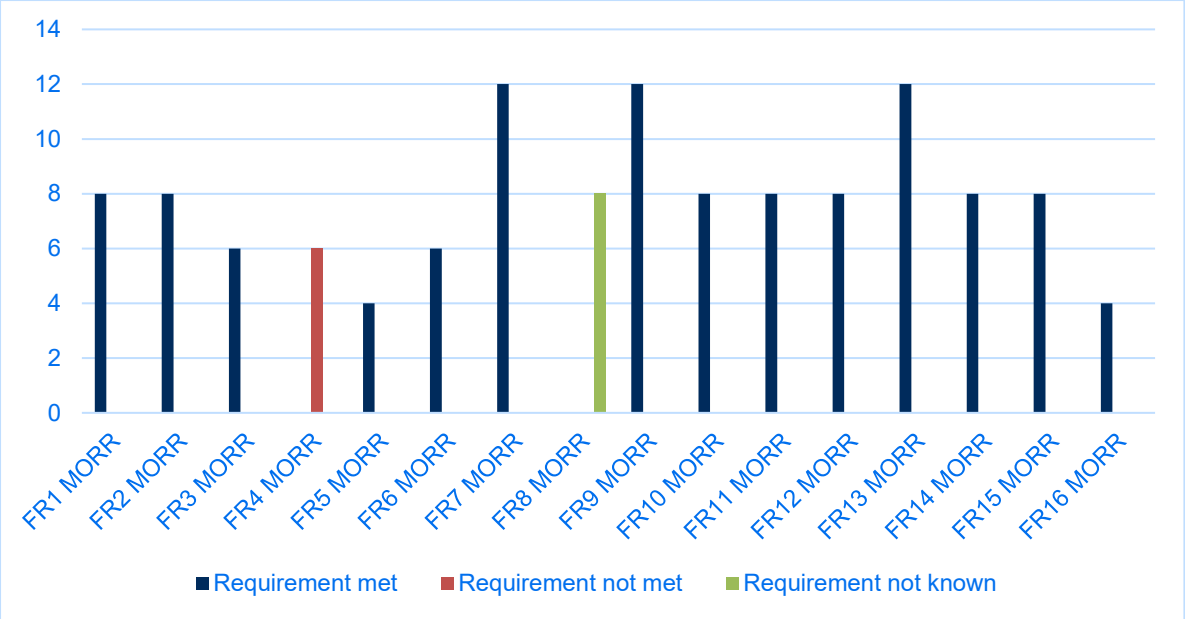


Figure 28: First engineer statements of compliance

The highest rated FRs with respect to MORR were complied with. The only FR which the auditee lists as not complied with is rated as being of relatively low importance.

Additional points of interest from the response by the chief electrical engineer are the following observations:

- The auditee listed uncertainty in whether one of the FRs was complied with.
- There was a common response that leaks have occurred but categorically not because of the causal factors listed. This could be a sign that there are perceived ‘causes’ of leaks and that possibly contributory factors to those causes could be overlooked. Such causes are not specified by the auditee and therefore cannot be verified against the other causal factors present in the complete STPA worksheets. This response can also be a signal that, perhaps unsurprisingly, previous experiences can be a greater influence on perceived risk of leak and causes rather than information presented which could theoretically lead to a leak.

This analysis of hazard perception, and perception around requirement effectiveness has been illuminating in understanding the focus of personnel on board the ship, and those generating potential requirements from a safety design perspective. Perhaps if FRs are a fundamental aspect of design, and audit is based directly from this with clear, documented and communicated justification of why the particular barrier is in place, it will move those on the ship towards a systemic approach to maintaining fire safety operations. Understanding the thought process behind FRs and their application, and to subsequently be audited on those specific factors can only be a benefit in hazard perceptions on board assisting to maintain fire free operations.

6.3 Collation of Auditees Results

Of interest in the audit is also the spread of individual perceptions of effectiveness and criticality on board the ship. The following figures present a comparison between the two personnel audited on the ECR controller, and the two personnel audited on the Automation controller. Note as only one individual was audited on the engineer controller, no comparison can be made for this. Also note that where an auditee did not provide a value for effectiveness and criticality this appears as a ‘0’ value.

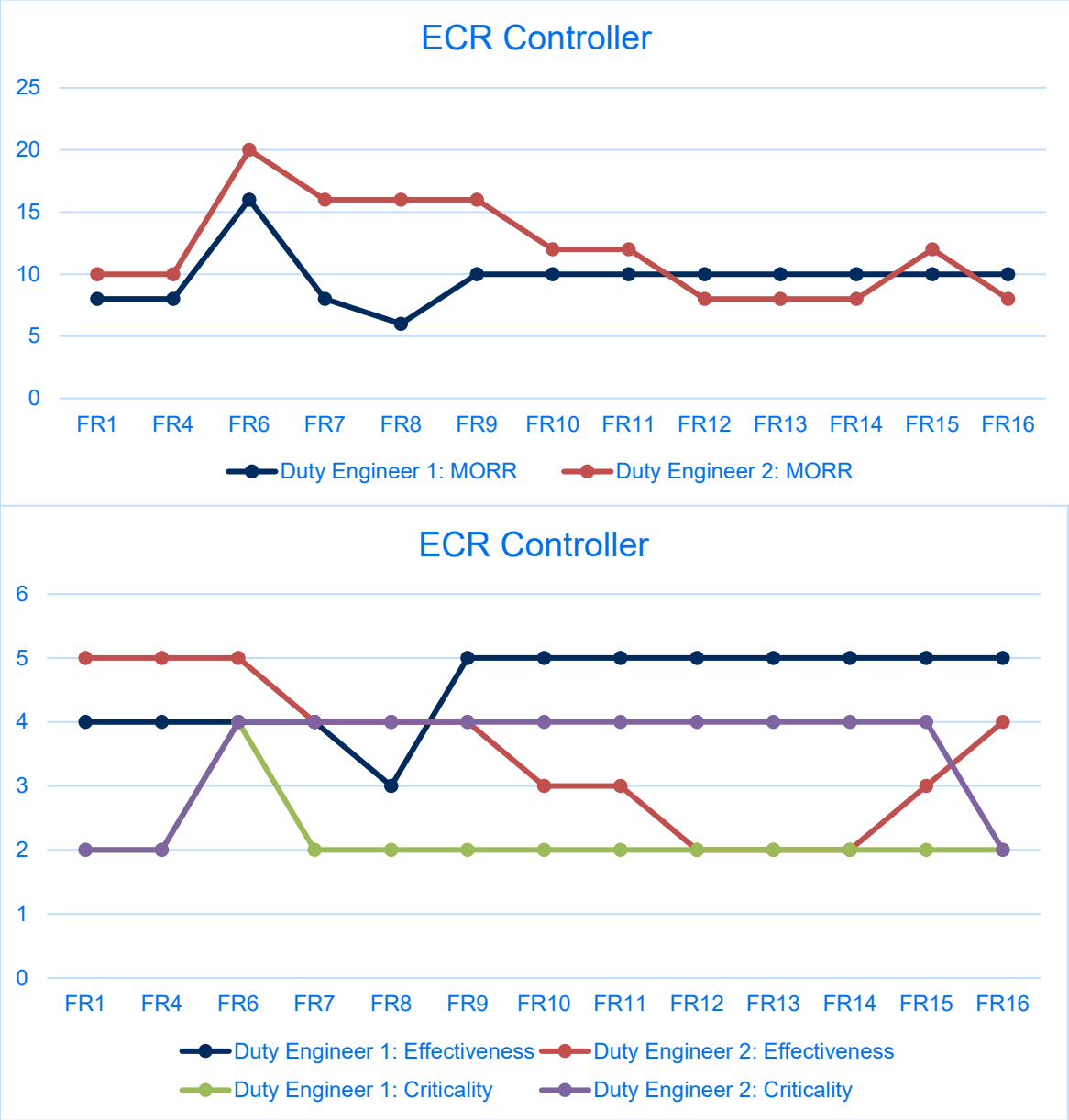


Figure 29: ECR auditees effectiveness and criticality comparison

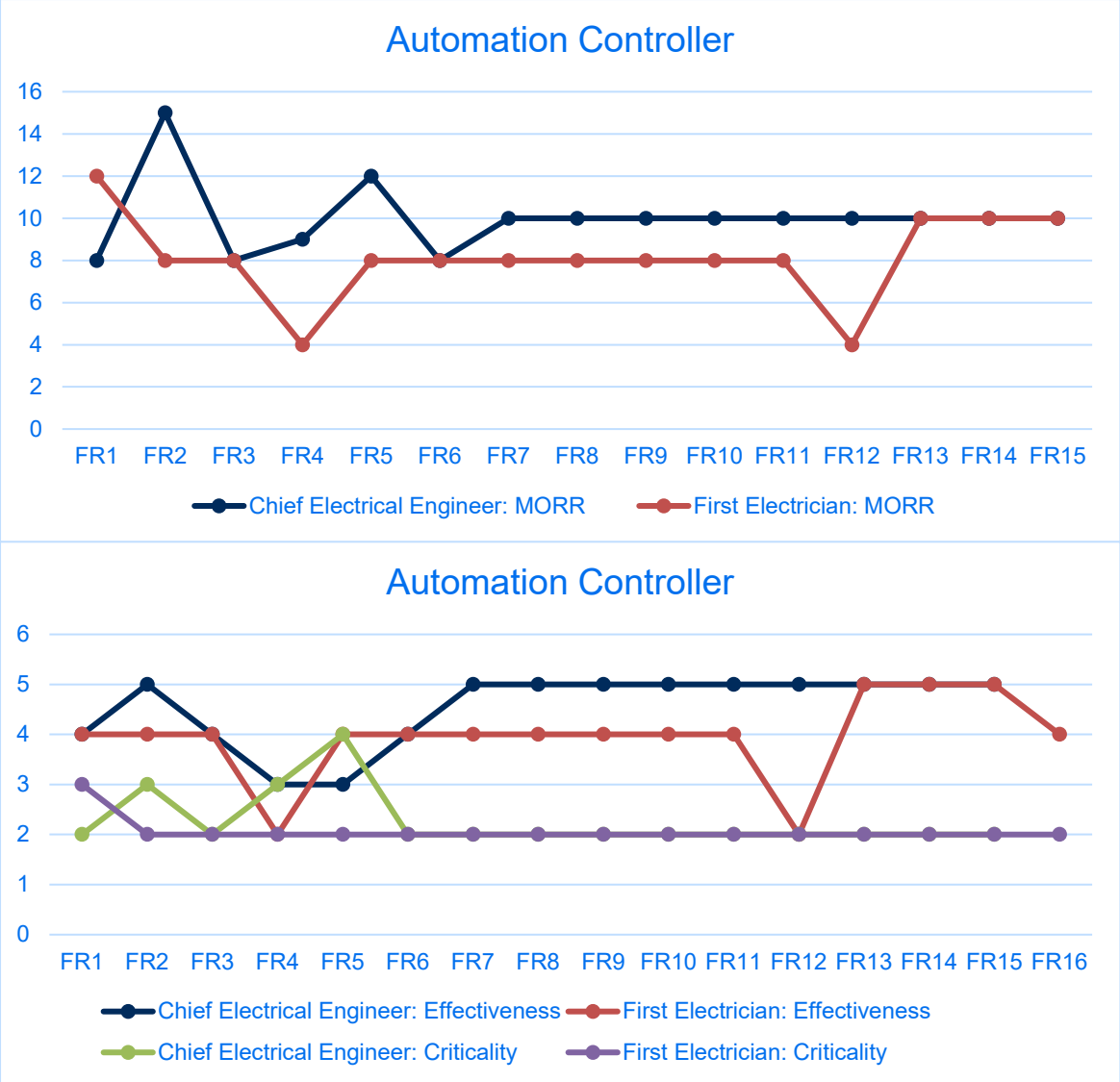


Figure 30: Automation auditees effectiveness and criticality comparison

What we can see from the results is a general tracking of the individuals on board's perception of the magnitude of risk reduction, with a few individual outliers for each controller i.e. FR 7&8 on the ECR controller, and FR2, 4 & 12 of the automation controller.

Regarding both effectiveness and criticality there is a strong correlation between the auditees, however this is unsurprising considering the previously noted trend of MORR.

The auditees show focus towards detection of the hazard itself rather than the precursor i.e. operational status in the STPA referred to whether hydrocarbons are flowing through the pipes while the auditee believe this to mean exposed high temperature surface detection.

Auditees also believed high pressure indication doesn't exist – only low pressure to detect when a leak has occurred (again concentrating on when a leak has occurred rather than detecting the potential cause of the breach – the elevated pressure).

It also appeared that there were a number of contradictions between auditee answers. In one example, an auditee stated only low-pressure alarms are in place, while the other stated that low- and high-pressure alarms are fitted.

Continuing in this vein, one auditee stated there is no way to detect if a critical function is inhibited, while another states there is a system in place to check for such inhibits.

One continuous theme in the audit is that those audited all concur that there is no way to detect exposed surfaces over 220°C despite the SOLAS requirement to shield these and prevent their occurrence. This begs the question therefore, how do we know if we meet the requirement? This would suggest there is a gap between how operators deal with oil mist releases and how high temperature surfaces are detected. While oil mist detectors are being introduced to detect the leak of a flammable oil, the detection of the other primary fire precursor (exposed hot surfaces) in the machinery space appears neglected.

An additional finding of interest during the audit was the statement suggesting that engineers are trained to recognise the symptoms of an imminent failure of an engine, but with the volume of data presented, they would be susceptible to information overload, and could fail to take appropriate action.

The audit highlighted that there is a closer alignment between the STPA and the auditees on factors close to the sharp end i.e. the automation controller, and also that discrepancies between perceived safety barriers on the ship appeared prevalent.

A specific analysis of the gaps highlighted during the audit will now be expanded.

6.4 Audit FR Gap Analysis

In light of the functional requirements which were noted as not being complied with, a gap analysis is carried out to determine if there is a requirement for these to be in place (within SOLAS, the ISM Code or DNVGL Class requirements), and if these could be complied with in

an alternative way/ if a barrier could credibly be implemented to allow these requirements to be complied with. This approach is instigated as a result of the observation that not all the auditees agree on which FRs are complied with. This could indicate some inconsistency on the feedback loops and assumptions made by personnel on the ship, and the subsequent control actions taken. In the potential absence of available barriers which can eliminate the gaps in the non-complied with FRs, potential barriers to improve consistency in the assumptions of personnel should be investigated.

Table 9: Audit non compliances

Controller	Auditee	FR ID	UCA	CF	FR	Auditee stated reason for non-compliance
Automation	Chief Electrical Engineer	1	Ship automation does not provide engineers operational status (H1-3)	Indication is not clearly represented due to poorly illuminated LED/ dirt obscuration	Operational status shall be easily discernible, and indicator shall be clear and visible	No system in place to indicate temperature above 220°C. However, Flame and Smoke detectors are in place and this will activate if the temp increases. If there is a leak, then pressure drop will indicate a leak. There is no specific system to measure temperature increase. Only detectors of flame and smoke will give this indication
		2	Ship automation does not alarm to pressure deviation in the oil systems (H2-3)	No feedback exists on stream pressure because no sensor is in place, resulting in no alarm signal on pressure deviation, resulting in pipework rupture	Stream pressure shall be known to the process controller.	No system to indicate high pressure. However, drop in pressure will result in an alarm
		3	Ship automation does not provide an alarm during an oil leak (H2-3)	Ship automation receives sensor data of reduced pressure as a result of a leak but misinterprets the data as normal operation as the set point is not relevant to the design tolerance, therefore does not send alarm, resulting in continual leak	Set points applied to alarm to system pressure drop in the event of a leak shall be set based on the anticipated pressure which could be presented through a break in containment.	The pressure drop sensors are not fitted from fire safety point of view, but to protect the engine from severe damage.

		4	Ship automation does not shutdown the fuel supply when exposed hot surface exists (H-1).	No automation in place to shutdown fuel supply on reception of exposed hot surface alarm	Equipment posing a threat of H1 shall have means of automated shutdown linked to hot surface detectors.	No such system fitted
	First Electrician	5	Ship automation does not alarm to exposed hot surface (H-1)	No sensor provided to detect presence of an exposed hot surface therefore no alarm can be presented.	Presence of exposed hot surfaces (>250°C) ER shall be known to the process controller.	No temperature sensor fitted to measure temperature of hot surfaces. However, exhaust gas temperature sensors would indicate hot surface on the engine. Also, smoke and flame detectors can indicate same.
		6	Ship automation does not provide ECR operational status (H1-3)	Signal from the sensor has been inhibited during maintenance and not brought back online.	Upon equipment start-up, warnings shall be presented if sensors are inhibited.	No alarm fitted to indicate inhibiters are not removed
		7	Ship automation does not shutdown the fuel supply when exposed hot surface exists (H-1).	No automation in place to shutdown fuel supply on reception of exposed hot surface alarm	Equipment posing a threat of H1 shall have means of automated shutdown linked to hot surface detectors.	The increase in temperature would be detected by smoke or flame alarm but this will not shut down the engine or fuel system automatically.
Engineer	First Engineer	8	Engineer doesn't shutdown or stop the fuel supply when strain on the components exceeds design threshold (H-2, H-3)	Engineers are unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces.	Engineers shall be aware of precursors which can lead to H-2, and when shutdown of the supply should take place.	Engineers are aware of the hazard. There is no visible or audible alarm to indicate this situation. However, parameters can be monitored. But, will they be able to process the amount of information available to them?

				Training inadequate, therefore fuel supply is not shutdown the moments before a hazard is realised.		
		9	Engineer starts repair, but doesn't complete when faulty equipment is present (H-1, H-2, H-3)	Engineer begins maintenance but is called to tend to other issues and does not complete the maintenance/ repair. No log exists to prevent activation of the equipment. Incomplete repair results in flammable material release on start-up	Staffing shall allow for planned maintenance of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.	Additional manpower would further enhance this process.

6.5 Analysis of GAPs/ Non-Compliance

6.5.1 FR ID 1:

The auditee focused on the hazard itself rather than the precursor before the hazard begins to be realised. ‘Operational status’ in the case of the query refers to whether hydrocarbons are flowing through the pipes, and the requirement to detect operation to prevent an operator taking action which would result in the release of flammable material. It is possible the STPA could have been clearer, but the jump of the auditee to consider the detection of H-1 as ‘operational status’ can be taken as an indicator of where personnel on the ship focus.

The second automation auditee noted that this FR was complied with.

DNVGL Class requirement states “The machinery shall be so arranged that inadvertent operation, caused by human error, cannot lead to the reduced safety of the ship and personnel” (197). DNVGL class requirements for piping systems also states that indication shall exist (198) which shows the open or closed position of valves which can indicate the operational status of flow. This is further detailed by DNVGL (199) where indicators for various systems are detailed on the control and monitoring of propulsion engines. This defines that local alarms (i.e. for pressure/ temperature) should be present for systems such as the fuels oil and lubrication oi systems.

6.5.2 FR ID 2 & 3:

The auditee notes that no high-pressure sensors are in place, only low pressure to detect a leak. This again highlights the focus towards detecting when one of the Hazards (H2-3) has already occurred.

The auditee confirms that low pressure sensors are in place, but that these are not used from a fire safety perspective. This shows again that there is a discrepancy between the awareness of fire precursors further left on the bowtie but not to consider these a fire precursor.

The other automation auditee noted that both high- and low-pressure sensors are in place.

SOLAS (194) presents the requirement to detect low pressure gas alarms to highlight the potential loss of containment as discussed by the auditee. SOLAS does also however note

that an alarm system shall be present for all important pressures, temperatures and fluid levels within an automatic alarm and control system.

DNVGL state that lubrication oil pressure for rotation machinery is a function which should be monitored (197) to maintain safe operation (in the context of avoiding equipment damage as noted by the auditee), but does not specify whether this is the monitoring of high or low pressure. High pressure sensors are required for other applications such as oil burners (198) and steam heated steam generators (200).

6.5.3 FR ID 4, 5 & 7:

The auditees state there are no systems in place to detect excessive temperatures above the level of H-1. This is corroborated between all auditees, and each also state that smoke and flame detectors could be used to detect high temperatures. This shows again that there is a discrepancy between fire detection (detection of the loss we are trying to prevent), and detection of the precursors which could lead to the loss.

SOLAS (90) requires hot surfaces over 220°C to be insulated/ shielded. With no sensors in place during operation this presents a risk of unknown SOLAS breaches. The focus of SOLAS is aiming to eliminate hot surfaces through installation and separation from the flammable material, however this is at contrast to how the ship and SOLAS address oil leaks. With oil leaks, the provision of attempting to eliminate the leak, but also detect the presence of oil in the atmosphere in the event of a leak are applied. With hot surfaces, detection in operation is left entirely to manual detection, or waiting until ignition occurs, then detecting the fire.

DNVGL class requires “Surfaces with temperatures above 220°C which may be impinged as a result of a flammable oil system failure shall be properly insulated” (197). A further class requirement states that where “adverse” conditions are experienced, provision for temperature sensors shall be considered in machinery spaces (201).

6.5.4 FR ID 6:

The auditee in this case has indicated there are no available functions which would indicate a critical function is inhibited. This is in direct contradiction to the statement from the other

automation auditee who states the functional requirement is complied with and that “System monitors malfunctions and inhibited functions”.

DNVGL class requirements state, with respect to system operation and maintenance “The system shall not remain in test mode unintentionally, and an active test mode shall be clearly indicated on the operator interface” (201).

6.5.5 FR ID 8:

The auditee indicates that the engineers are aware of the conditions which would result in the release of flammable material, however no clear indication exists anywhere for this. Concern is also raised over the volume of information presented and the engineer capability to address such a large volume of data.

DNVGL provide a wide range of factors which should be monitored for safe operation of machinery (197, 199) including propeller speed, stream pressures, boiler water levels etc. This corroborates what the auditee states regarding a large volume of data, all relevant to a potential break in containment/ failure, but with such a large volume of data appropriate action may not always be reliable. A simplified system of operating and providing information could be of benefit here, but is only highlighted as a concern when viewing the hazards with respect to systemic (in this case the interaction between humans and the machines providing data) causal factors.

6.5.6 FR ID 9:

The auditee indicates they don’t know if this FR is complied with, and that it would appear to be dependent upon manpower availability. As this will likely be influenced by external market factors and controlled by the company, this shows an example precursor which would be highlighted in the STPA sheet for the controllers higher in the corporate or industry hierarchy. The ISM Code (91) discusses clear communication between shipboard staff and senior management as being important to the maintenance of safety. The provision of adequate staff with appropriate training is therefore an important tenet of this code.

6.5.7 Discussion on Non-Compliances

When considering the non-compliances from each auditee, there is no corroborated non-compliance between multiple auditees. This therefore shows two possibilities:

1. There is a non-compliance, but some staff believe there is a barrier in place
2. There is no non-compliance, but some staff do not know about the barrier in place

Neither of these are positive outcomes therefore further review of the non-compliances is required.

It is also worth noting that a functional requirement may not have been implemented in design and therefore if it is a non-compliance, this is not an automatic non-conformity. For example, such a FR may have been discarded on the principle of ALARP. This therefore shows the importance of the audit being directly based from the FRs agreed upon in design, such that audit questions are verifiable against FRs which should be in place, and relevant for the current context.

As discussed by Reiman and Pietikäinen (202) an indicator of safety, or otherwise, is the ‘Understanding of hazards’. Encapsulated within this understanding are a number of measures including ‘the extent to which the personnel understand the hazards that are connected to their work’, and also ‘the extent of personnel’s awareness of the technical/physical condition of systems, structures and components’. The findings from this process, and specifically from the audit, show there are ways of detecting such indicators. To demonstrate this, the research will focus on two specific non compliances shown in Table 10.

Table 10: Non-compliances of interest

Controller	Unsafe Control Action	Causal Factor	Functional Requirement
Automation	Ship automation does not provide an alarm during an oil leak (H2-3)	Ship automation receives sensor data of reduced pressure as a result of a leak but misinterprets the data as normal operation as the set point is not relevant to the design tolerance, therefore does not send alarm, resulting in continual leak	Set points applied to alarm to system pressure drop in the event of a leak shall be set based on the anticipated pressure which could be presented through a break in containment.
	Ship automation does not shutdown the fuel supply when exposed hot surface exists (H-1).	No automation in place to shutdown fuel supply on reception of exposed hot surface alarm	Equipment posing a threat of H1 shall have means of automated shutdown linked to hot surface detectors.

The first non-compliance is of interest as it relates to the detection of leaks and leak precursors which appears to be of interest in general to ship operators, with the increasing advent of oil leak detection systems and the consideration of clean room type engine rooms. This is also interesting specifically in reference to the audit as it appeared to highlight a conflict in the answers between auditees and does not align with the findings on the ship drawings where it appeared that such sensors are in fact in place (noting there is also confusion around their intended application within the equipment documentation) (203). This shows the scope for improvement in how this barrier is applied which is to be further elaborated.

The next non-compliance is of interest specifically to design as it addresses the issue of exposed hot surfaces which are not permissible in SOLAS. This non-conformance would seem to exist across the industry where there appears to be an acceptance that such exposed hot surfaces simply cannot be automatically detected by fixed detection technology but are monitored periodically when the ship is in port. This non-conformance presents a potentially significant area for improvement and possible introduction or strengthening of the barriers in place to prevent/ detect exposed hot surfaces, which has been highlighted in this research as a serious issue in ship machinery spaces.

6.6 Alternative FR Compliance

It was demonstrated that in general the functional requirements had a high degree of compliance. Considering this, it was decided to review potential alternative methods of functional requirement compliance which may in some way benefit the operator. This benefit could present itself as either a cost reduction to maintain the same level of compliance, or through an additional measure applied to strengthen a barrier in place which fulfils a functional requirement.

A selection of functional requirements was extracted from the audit based on the magnitude of risk reduction factor assigned by the auditees. The highest ranking MORR FRs were extracted, which were also corroborated as 'important' in the STPA. Table 11 highlights one such FR.

Table 11: Candidate for FR compliance review

Controller	Unsafe Control Action	Causal Factor	Functional Requirement
ECR	ECR provides status of imminent/ existing leak from oil system too late meaning engineer/ chief engineer does not provide a fix in time (H2-3)	Sensors to detect imminent/ existing oil leak are incorrectly positioned meaning the situation has to escalate to generate an alarm.	Sensors intended to detect imminent/ existing oil leak shall be strategically placed to detect pressure increases/ excessive vibration/ oil mist at the locations these are likely to exist.

When reviewing the FRs with scope for improvement or strengthening, the FR in Table 11 presented itself as both interesting for review while also aligning with a similar requirement stated in Table 10. This FR is therefore selected for further examination. Finding a solution for the FR in Table 11 could automatically also address the FR in Table 10 if adequately addressed in the SMS.

The primary factor for consideration is:

- Implement leak prognostics (monitoring of safety critical segments of piping system)

From a review of the auditee responses and the analysis of drawings/ equipment details/ data analysis, the sensors appear to be present which would show the 'perceived' non-conformance in fact has a barrier in place (203). Confusion may reasonably exist, however, regarding the location of such sensors, the intention behind their application, and whether these sensors would be effective in achieving the functional requirement. There is, however, a discrepancy in engineer answers as to whether they are used and what they are used for as discussed in the previous section. This begs the question of whether they are being used, and if so, are they being used correctly? It is due to this uncertainty that we will aim to strengthen this barrier. This has been identified using the proposed method by addressing the systemic issues surrounding leak prevention systemically. It may be that an 'adequate' system was agreed in design (the sensors which are currently in place), but it has been shown using the methodology applied in this thesis, with a direct link to the audit, that in the current operating context this barrier is ineffective (a clear break in control and feedback in the current context).

When reviewing the criticality of implementing the FR we must look at any previous occurrences of the unsafe control action having resulted in a fire in the past. The FR states *'Sensors intended to detect imminent/ existing oil leak shall be strategically placed to detect pressure increases/ excessive vibration/ oil mist at the locations these are likely to exist'.* When reviewing stated causation of fires in the past, the vast majority are a result of a release of flammable material from wear and tear of the pipework and equipment, often through excessive vibration, increased pressure etc. through the pipework (204) (205). Should the functional requirement of detecting these conditions be implemented we should, in theory, be able to provide engineers the ability on board to prevent the occurrence of the break in containment, and certainly prevent the presence of multiple hazards occurring concurrently to result in fire.

For this particular finding, it is proposed that a move towards improved sensor prognostics which results in simple and easy to understand instructions/ information to engineers will present a suitable way to implement and utilise the sensors which are already applied which would provide a higher degree of certainty around their application and therefore

effectiveness. This approach closely resembles the concept of Observability in Depth (206). This is similar to defence in depth but focuses on monitoring and identifying an emerging hazardous situation and preventing accidents from occurring. Fundamentally it requires barriers to be observable and therefore capable of analysis. As the sharp end, causes of engine room fires appear to be recurring, these emerging hazardous situations should be relatively easy to identify and monitor, and may even be monitored already as the audit would appear to highlight.

There is a big question mark over the cost effectiveness of the current application of sensor technology which is failing as a result of systemic shortcomings. The aim here therefore is to put that money to better use by strengthening the application of these sensors.

The result of this analysis in practice would therefore aim to highlight the critical areas of pipework where the hazard is credible, and determine 1) what needs to be detected (pressure, temperature, flow, vibration etc.), and 2) how is the data aggregated to present a simple and easily understood warning system for engineers on board?

The following figure presents a typical operating range and fictional readings from a basic pressure sensor.

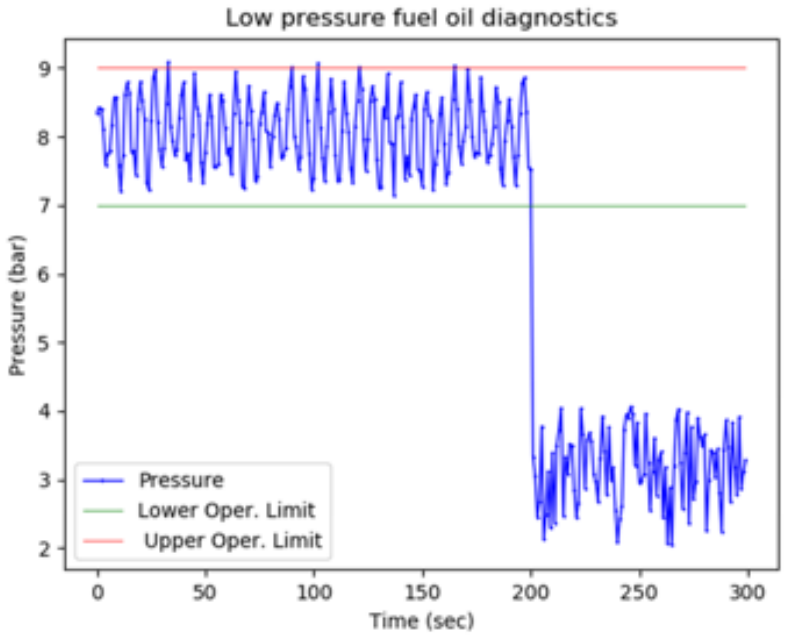


Figure 31: Theoretic conceptualisation of pressure indication (207)

Figure 32 demonstrates the move towards hazard realisation, and three example sensors which can be put in place which currently operate in isolation. The figure demonstrates the potential benefit of combined data analysis to predict a route towards a failure and provide simple alarms and information to engineers such that a potential fire precursor can be dealt with as soon as possible.

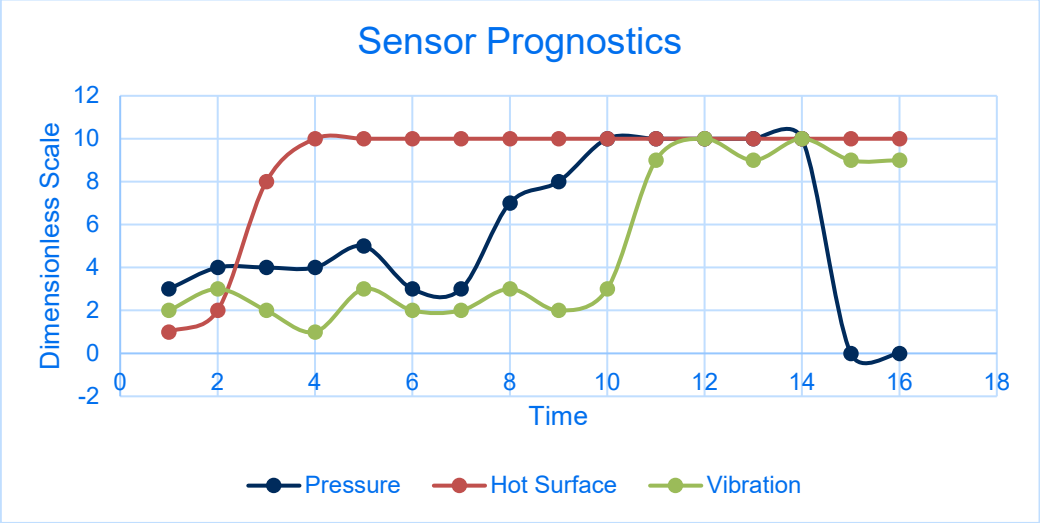


Figure 32: Theoretic conceptualisation of sensor prognostics

At time point 15, the pipe transferring flammable material has ruptured (as a result of a process upset which increased the stream pressure coupled with an elevated vibration resulting in fatigue), and with the presence of a high temperature surface from time point 4, an ignition becomes not possible, but likely. Time point 15 appears to be the earliest point the current sensors would become effective.

The following figure shows points at which the system is healthy, where two levels of pre-alarm could occur in an effective DBM system, and where an alarm should be triggered requiring action as part of a potential 'traffic light' based system. Normal operation can be considered between 1-4 of the dimensionless scale, the safety margin can be considered between 4-8, and anything above 8, or a registered value of 0 (see Figure 34), triggers an alarm state (either pre or major alarm depending on the condition of the linked sensors).

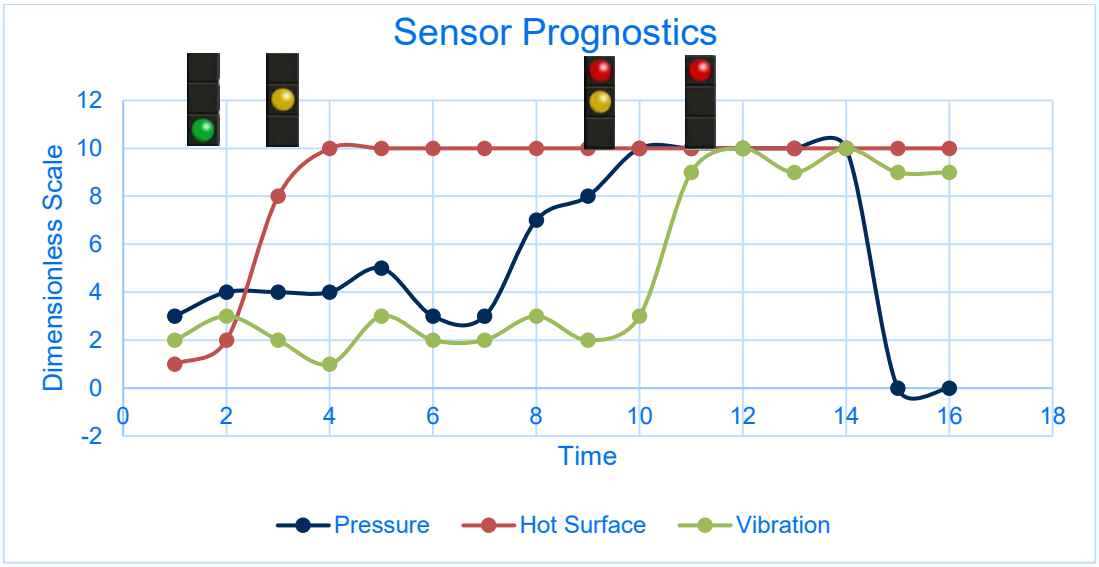


Figure 33: Sensor prognostics with Traffic Light based warning system

While the figures above review events where all sensors are operating as intended, the system can account for sensor failure where the sensor health is measured. This allows the reliability of sensors to be considered. The following figure presents the same system where a sensor failure occurs (zero signal is detected indicating sensor failure). Note this does not automatically result in an alarm, but rather increases the overall risk to the system and does not raise an alarm until there is corroboration that the risk level is increasing.

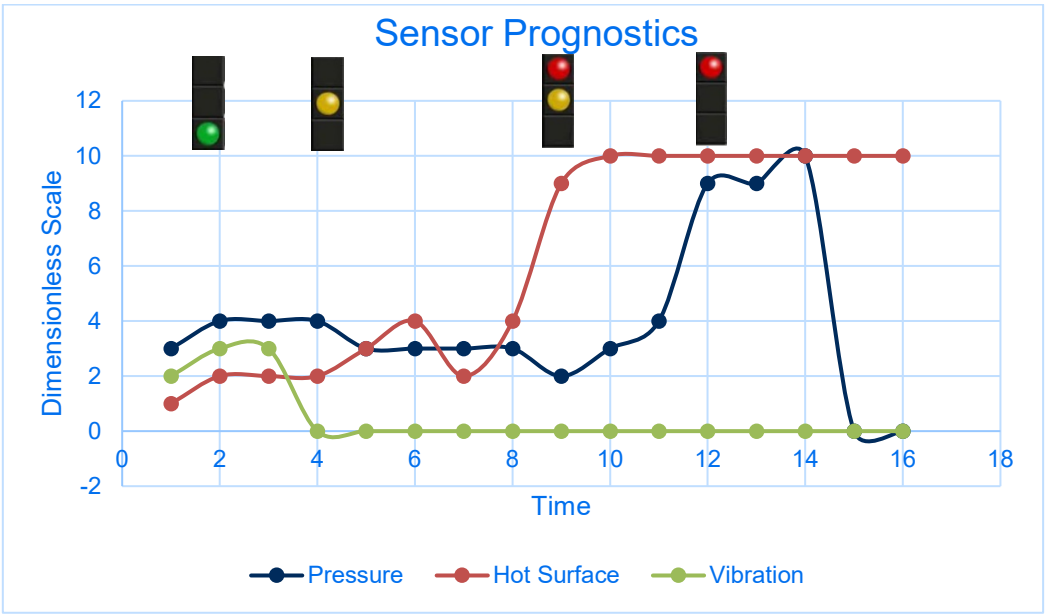


Figure 34: Sensor prognostics with Traffic Light based warning system with sensor failure

In this example the major event occurs at point 15 as before, however the first level of pre alarm occurs upon detection of the vibration sensor failure, then the second level of pre alarm occurs when this failure is combined with an elevated exposed hot surface detected, with the final major alarm when this is also coupled with an elevated pressure reading indicating a leak is credible. When combined with the uncertainty around vibration and knowledge of an exposed hot surface, action must be taken.

Note this does not address the problems previously highlighted with automatically detecting exposed hot surfaces. The method, however, would be credible to allow an exposed hot surface which is manually detected (either when in port or at sea by either ship personnel or a certifying authority), to be placed in to the sensor prognostics system to provide a holistic real time risk update. When the exposed hot surface is remedied, the risk is removed from the system. As technology emerges in the future, the barrier which provides compliance with the functional requirement of detecting hot surfaces can be updated in the SHORE documentation.

With this output providing a critical input to any safety barrier improvement initiative, a need emerges for a simple to follow and easy to use method where the process and methodology can be applied to improve safety of a facility in design and operation.

While the purpose of this thesis is not to develop a specific DBM system, it has resulted in the development of SHORE, a methodology of applying HAZID which will provide the critical input to any such system, with a direct link to the continuous auditing process for integration to the SMS to ensure safe operations in a fluctuating context. Regardless of whether DBM (or any other method of barrier analysis) is applied at the sharp end through use of sensors or across the entire prevention and mitigation phases, this thesis has provided a critical input in applying SOTA fire safety to ensure performance based fire safety is applied and maintained on a facility. The methodology has also been proven useful in highlighting areas for future R&D resource focus. If a FR cannot be met with current technology and would be effective and critical, this would be a useful area of future research to develop a barrier which could comply with the requirement.

The thesis will now show the method and process which has been presented in this thesis and Appendices A-C, represented in a simplified form which takes a user through the SHORE process. SHORE was developed and applied in conducting the analysis discussed in Chapter 5, the validation in Chapter 6, and is refined in light of that validation to its form as presented in Chapter 7. It is proposed that SHORE will provide the critical input to any potential DBM/ ‘traffic light’ system of barrier implementation or improvement system for safety. It can also be the critical input for SMS integration.

7 Systemic HAZID and Operational Risk Evaluation (SHORE)

7.1 What does SHORE Contribute to HAZID?

As discussed in the critical review, it does not matter how robust a protective barrier is if it does not account for the interaction between humans, that technology and the specific environment it is placed within. The approach applied in the method presented in this thesis, defined as the Systemic HAZID and Operational Risk Evaluation (SHORE) methodology, allows new requirements to be highlighted on a functional level which account for the entire socio technical context. It also allows existing barriers in their existing state to be improved and made useful by analysing their potential systemic failures. Strengthening a failing barrier through defence in depth does not equate to safety.

It must be kept in mind, however, when proposing any new barriers (incl. sensors / automated monitoring) as a result of the proposed approach that traditional quantitative/ qualitative methods may be required for cost benefit analysis. This does not negate the application of the approach however as it has been shown to discover previously unaddressed gaps in the HAZID stage.

The hypothesis states: *It is hypothesised these fires continually occur through systemic failures not being addressed in design and operation. This hypothesis portrays systemic uncertainty/ causal factors may not be fully addressed when applying traditional methods of HAZID and operational auditing which has led to fire remaining a prominent risk to maritime operations.*

To test this hypothesis, it was predicted that if a structured fire safety approach is implemented accounting for interaction between humans, technology and the environment across the entire prevention and mitigation spectrum, opportunities for improvement in machinery space fire safety would present themselves. It was stated these improvements could take the form of strengthening existing safety barriers by addressing factors not considered when such barriers

are placed in isolation with no consideration of context, or perhaps new/ alternative barriers will be discovered which will improve fire safety.

Within the application of the design portion of SHORE in Chapter 5, the following are a sample of the findings which show this hypothesis has been proven accurate. The following shows example FRs discovered which are not addressed on board, with no evidence of them having been considered/ documented during the original HAZID:

- Sensors analysing pressure across the oil systems with the intent of detecting abnormal operations outside of safe operating limits (e.g. Ship Automation FR 7.1.1 – 7.4.2; 14.1.1 – 14.2.1). Pressure sensors are used within the ER equipment, so the technology exists, and money has been spent on it, but these were not being used effectively as a fire preventative function but rather as a detector of a leak occurring. They have therefore been applied as a mitigative function as the technology exists, rather than arriving at a reasonable application of the technology further back in the bowtie from a systemic HAZID. It also subsequently emerged these devices are also not particularly effective at the intended function as a result of delayed response times (addressed in Ship Automation FR 15.1.1 – 15.3.1), device positioning (addressed in Ship Automation FR 18.4.1, Ship Control Room FR 9.1.1) etc. using traditional mass/ volume balance Leak Detection System (LDS) approaches (203). This shows that even within the limitations of the technology, there is scope for the effectiveness of such existing sensors to be addressed when applying the approach presented in this thesis.
- Exposed high temperature surface detection occurs in many of the developed FRs (e.g. Engineer FR 5.1.1 – 5.4.2, 15.1.1 – 15.3.1, Ship Automation FR 9.1.1 – 9.4.2, 16.1.1 – 16.3.1). Numerous avoidable causal factors are shown to result in exposed high temperature surfaces with no means of detecting this outside of manual inspection. Exposed high temperature surfaces are often accepted as common place, which was also the case during the SEAMAN project (207). For example, during site

inspection it was assumed exposed hot surfaces would be found on the trip to the engine room and this was the case, with the inspector claiming this is the case on virtually every engine room survey. The very nature of this discounting is, in itself, a finding of systemic risk of exposed high temperature surfaces. While there may not be a simple solution to the problem, the functional requirement still needs to be documented and addressed in some way, otherwise we have continual creep and an expectation that at some point we will have a leak which will inevitably lead to contacting an exposed hot surface.

- Vibration sensors are a clear highlighted barrier to detect creeping fatigue of machinery to detect the movement towards pipework/ equipment operating out with its safe operating limits leading to inevitable failure (e.g. Ship Automation FR 10.1.1 – 10.4.2, 17.1.1 – 17.3.1, 21.1.1 – 28.1.1, Engineer FR 20.2.1, Chief Engineer FR 15.2.1). Technological limitations may impact installation of an adequate system, but for R&D into new methods of preventing fire (i.e. DBM), this process has highlighted a critical input which should be considered in such a system.
- Multiple causal factors were discovered relating to communication failures such as that found in the Le Boreal fire (e.g. Chief Engineer FR 1.1.2, 10.1.1, Ship Automation 1.1.1 – 1.3.1, 2.1.1, 10.1.1, Ship Control Room 4.1.1, 11.1.1). When analysing physical barriers in a traditional approach, the control and feedback loops can easily be overlooked which render the money spent on strengthening physical barriers ineffective. Should a systemic analysis have been carried out it is credible the lack of communication and barrier feedback would have prevented the event from occurring. This is easy to say in hindsight, but within the very nature of the systemic approach, this is the type of failure aimed to be addressed. This is also in addition to the implementation of traditional physical barriers with increased emphasis on them operating effectively in their operational context.

- Ship Control Room FRs 17.1.1 – 17.4.1 highlight the dangers associated with not shutting down the engine when it exceeds the design threshold. Interestingly, during the audit it was suggested that engineers are trained to recognise the symptoms of an imminent failure of an engine, but with the volume of data presented, they would be susceptible to information overload (First Engineer fourth UCA question), and could fail to take appropriate action. Questions were not posed to the ship personnel on presentation of engine operational data during the audit. This was raised un-prompted, showing a systemic risk not addressed on the site, which both site personnel know about and was highlighted during the process described in this thesis. Interestingly this issue is captured in the STPA under FR 11.1.1 of the engineer controller but was not included in the audit due to limiting the number of FRs to be included. The FR discusses issues associated with data overload where the engineer is unable to make appropriate safety decisions.

A hypothesis which emerges from this would be that these findings would only become more prominent the further back we go from the sharp end. This is, however, scope for future research and is not evaluated further.

When we review the traditional approaches to HAZID, the results of safety cases generated in the offshore industry, are often arrived at through event trees and other quantitative risk models which fall under the same shortcomings of those discussed in this thesis. SHORE addresses this during the HAZID stage by focusing entirely on structured systemic risk analysis detailing the control action contexts and credible loss scenarios.

The methodology meets the framework as discussed by Wang (161) in meeting the following 5 criteria to address hazard identification and analysis:

1. Identification of hazards
2. Assessment of risk associated with the hazard
3. Ways of managing the risks identified
4. Cost-benefit assessment of the options

5. Decisions on which options to select

A more recent document governing the management of risk is ISO 31000 (208), in which the SHORE methodology also presents use in assisting operators in meeting their requirements. The following details some of those requirements the approach directly addresses:

- Managing risk considers the external and internal context of the organization, including human behaviour and cultural factors.
- Ensure managing risk is efficient, effective, and consistent.
- The principles within the document are there to assist a company manage uncertainty within the organisation.
- Appropriate and timely involvement of stakeholders enables their knowledge, views, and perceptions to be considered.
- Risks can emerge, change, or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges, and responds to those changes and events in an appropriate and timely manner
- Leadership must ensure that the risk management framework remains appropriate to the context of the organization
- Integrating risk management relies on an understanding of organizational structures and context

SHORE provides a template for systemic risk analysis which automatically moves to an audit template for operational review in the SMS. It provides the HAZID and operational audit function. It is up to operators how they apply their cost benefit analysis to select the specific barriers to be implemented, and operators will have an existing preferred method of doing this. The approach does, however, provide guidance on the magnitude of risk reduction provided by each functional requirement to assist with the decision making, as well as its primary function of measuring perceptions across the organisation. This can be tailored based on the operator's risk philosophy. Once the selected functional requirements highlighted through the

HAZID process are implemented, the audit portion of SHORE then verifies the specific implemented functional requirements remain robust and valid.

The importance of the HAZID function which structurally decomposes the system to address effective fire prevention has been presented. The second part of the process relates to the automatic transfer of the HAZID and analysis to the audit portion of SHORE – a critical and novel function as demonstrated in the validation exercise to provide an impact on moving towards fire free operations.

7.2 What does SHORE Contribute to Auditing?

For continuous operation and incorporation in the SMS, the novel auditing portion of this methodology allows for the performance-based nature of systemic fire prevention applied on a functional rather than physical level. Physical barriers, however, can be used to achieve the functional requirement and are therefore still included. The context and original assumptions will be continually reviewed as part of the audit process presented. Audits are presented as semi structured interviews derived directly from the HAZID portion of the approach, with personnel who fall under the specific controller being audited (i.e. engineer, first engineer etc.). The usability assessment of the early version of this was used favourably on the validation audit of the HAZID approach and audit discussed in Chapter 6.

As audits historically look backwards at what has been done, or what is being done ‘now’, it is important the approach engages those being audited on what is important moving forward, such that further update and innovation to the HAZID, hazard analysis and barrier implementation is implemented as part of the facility lifecycle. This becomes a critical part of the evolution and continual application of SHORE, incorporated in the SMS. This is achieved by presenting the control actions, contexts, causal factors and functional requirements to the auditee such that comment is made on all areas. This will present the most up to date information from the site, This feedback can then be fed back into the HAZID perpetually through the lifecycle.

The tool presented by Mitchell (167) further demonstrates the need for the approach to address HAZID, hazard analysis and benchmarking of an organisation's operations against its own assumptions and safety practices, rather than against other operators in the same field. If those safety barriers determined during design, and subsequently implemented, are safety critical and certification of the ship has occurred as a result of them, operational audits and assessments should be measured against those original assumptions and barriers. This would be beneficial over auditing what is often applied elsewhere which may not have been relevant to that specific facility, operator or context.

When reviewing the importance of innovation in financial auditing, Manita (168) emphasises the importance of critical thinking and evaluation of data in auditing. It would appear therefore beneficial to have a sole representative, group of representatives or organisation to manage the process. With SHORE starting at the beginning with HAZID, and working through to operational audits for continual improvement, the critical thinking and interpretation of the data received will be easily gathered by those responsible for the generation and maintenance of the data and documentation. This is likely to be the operator or class society for example. The emerging application of, and access to, 'big data' and dynamic barrier management, coupled with the novelty in the methodology presented in this thesis, may in the future allow improvements to emerge which previously and currently cannot be seen. This is an area of potential further study.

Overall, there is very little by way of safety audit research literature specifically for fire safety in the marine industry, however several commercially available packages are used in safety auditing as previously discussed. These tools, however, do not derive directly from the design and HAZID processes and do not directly account for the structural decomposition of the socio technical context, showing novelty in the approach discussed herein.

Issues previously discussed include a common lack of application of the systemic nature of risk and consideration of the high consequence, low likelihood incidents. Performance based functional requirement setting is therefore critical in any method used for HAZID and operational auditing. An audit based directly from the HAZID, which generates the

performance and functional requirements directly from the organisation's context, increases the relevance of the audit to verify the initial assumptions. This is one of the primary functions of the SHORE methodology.

The issue of internal audits becoming literal checkbox exercises with independence and impartiality lost is also a concern which SHORE addresses. The methodology will remove such issues where audits continue to be carried out in house. For example, SHORE bases the audit investigations directly from the HAZID, meaning when the functional requirements are selected, they are selected from the requirements which should be in place, and audits their presence and effectiveness. Such an approach will allow management (or potentially a 3rd party) to continue to fulfil their obligations in active monitoring, while also maintaining that independence in audit which is critical to effective auditing.

The difficulty for an auditor to strike the balance between being locked on the rails of an audit and applying so much discretion the audit is not repeatable is also of concern. As a result, the SHORE methodology focuses on the functional level directly from HAZID in design and focuses on the performance-based goals of the barriers. The audit therefore verifies if the barriers placed to achieve that performance-based objective are still in place and still relevant. Ideally the user will also be the user during HAZID and will therefore already be familiar with the notion of the system, controllers, unsafe control actions and all the other critical factors applied in developing those functional requirements from the structured approach to applying systemic risk analysis in fire prevention.

The limitations highlighted on audit effectiveness (174) show the clear importance of audits not simply covering whether a barrier is physically in place, but rather whether the functional requirement of a particular area of safety is effective. This is the primary novel aspect of this research and approach and is the foundation of the methodology presented.

So how does such an approach provide value to an operator in auditing. If a company's resilience is measured by how it can recover or deal with an unexpected event (high consequence/ low likelihood), asking if a barrier is in place does not directly address this as the barrier may be in place and operational, but the event may happen anyway. Conversely,

asking if a functional requirement is fulfilled which is in place to prevent fire, for example, is a more appropriate audit query to measure the resilience at that point in time against a hazard identified during design. This is particularly useful as the earlier HAZID process has also addressed high consequence/ low likelihood systemic failures.

SHORE therefore focuses on the performance based functional level, where such requirements are drawn directly from the systemic hazard analysis used in hazard identification during design.

While this approach does not specifically aim to address a measure of operational resilience, the philosophy behind operational resilience is at the heart of it. SHORE aims to provide a prescriptive method and guide to the implementation of performance-based fire prevention for HAZID and operational auditing.

The methodology developed aims to apply a similar philosophy behind the method presented by Costella et al. (176) as discussed in Chapter 3.9.2. Where SHORE expands on this is to use the approach in HAZID and automatically generate the audit from this HAZID. That way the approach is implemented from conception to operation, ensuring audit relevance, and incorporation of societal and contextual issues in the application of barriers to fulfil the functional requirements. The MAHS method was also found to be very specific to the industry it was developed for, which created confusion when tested elsewhere. This shows the importance of the approach starting generic, allowing application cross industry, then structurally becoming more specific.

Costella's method implemented a scoring system as previously discussed. This presents some flexibility from the auditor in how they have perceived the situation. If a functional requirement, however, was to be directly assessed as a pass/ fail, it can be addressed in binary form. Where evidence of compliance or non-compliance is to be presented, and multiple personnel are audited, this would provide the auditor with a more useful metric of whether safety is being achieved. Further, a more useful 'score' could be applied by the auditee in relation to their perception of effectiveness and criticality of that functional requirement. Where such factors have also been applied during design by the design team during HAZID, this

would present the auditor with an appreciation of the true nature of the operational situation, and also a comparison between the current perception in the field vs the perception at the time of design. This can also present data on whether the original assumptions on the risk/ effectiveness/ criticality of a functional requirement remains valid in the field.

As an audit method, the method presented by Costella is closely related to the method prescribed in this thesis, however Costella focuses on the audit processes and provides a checklist of areas for the auditor to question. The end goal of the method is to provide an overall score for the company performance across the variables of safety. These areas are based on the resilience engineering philosophy, closely related to the philosophy of a structured decomposition of the system used during HAZID to identify causal factors and implement functional requirements to account for systemic failures. The gap exists in pulling the two together into a single process which will allow consistency in its approach and specifically verify if the assumptions made during HAZID remain relevant.

The results of the audit following the MAHS approach presents the scorings against each facet of safety rather than highlighting specific functional requirements which are degraded. This tool therefore applies the philosophy behind this thesis, but in the effort to rate a company's overall health and safety management system. This form of auditing is therefore beneficial in verifying the performance of a specific barrier i.e. the management system. What has been completed in this thesis and presented in SHORE, is an expansion of the approach to cover specific operations and decompose each controller to specifically identify those requirements which are no longer fulfilled, with a view to continued safe operations in the field. Essentially SHORE analyses the health of the overall system, in addition to the individual barriers and requirements within that system.

The MAHS approach may present questions which are similar to those asked using the SHORE methodology, but the set questions within the MAHS approach are focused on the management level of safety. This cannot automatically be moved and tailored to all layers of the control structure. Using SHORE, the questions posed during the audit will be aimed at the responsible controller for the functional requirement, whether a manager at the blunt end or

an engineer at the sharp end. As this is tailored directly from the HAZID process, the questions pulled from the STPA will automatically be relevant to that controller.

The methodology was found to be useful in the case study HAZID and audit, particularly when connecting the two directly, which will now be discussed.

7.3 Pulling Together the HAZID and Audit Process

From the HAZID analysis and the subsequent audit made during the case study in this thesis, the monitoring of signals in place is recommended to allow a more easily understood and effective system of fire prevention to be implemented on board.

It is also recommended that the STPA process, outputs and audit can be implemented in the Safety Management System (SMS). Being able to account for causal factors which would otherwise likely have been overlooked, coupled with the cost benefit argument (in strengthening barriers which are already in place) provides the benefit of providing more holistic and robust safety systems to be implemented and operated. Through integration of the HAZID results into the audit process, this presented a snapshot of the risk profile on board with respect to the operational level barriers, and through application of technology we can obtain a snapshot of risk from the automated barriers. This can also show areas where risk perception and perception of FR compliance may vary between auditees, providing an easy to assess and validated way of deciding which barriers require improvement. This can form a pivotal part of the operational phase of risk assessment and holistic safety.

The following are just some specific examples and evidence that connection of HAZID and audit applying the systemic approach discussed in this thesis provides enhanced fire safety in barrier implementation, management, and operational safety. These assist in proving the hypothesis and demonstrates novelty of the research and findings:

- The FR ‘Stream pressure shall be known to the process controller’ resulted in contradiction in response on board the ship. There was also uncertainty within the STPA working group during the case study as to whether this was implemented.

Regardless of the ultimate finding on whether sensors were in place, if this was intended to be in place during design and a contradiction in response is found during the audit, the barrier implemented is obviously not effective. This is a clear finding which is found directly from applying the approach presented herein. This contradiction is discussed in Chapter 6.

- The FR 'Equipment posing a threat of H1 shall have means of automated shutdown linked to hot surface detectors' is responded that no such system is fitted. It is credible that with limitations in technology this FR was not credible using instrumentation. It is an important FR, however, which has not been addressed during design or operation. Exposed hot surfaces would require to be considered as a SOLAS requirement, but the response of 'no system fitted' (paraphrased), and therefore no compliance is an interesting finding from the audit. This could prompt an investigation into how the FR can be complied with even if there is currently no instrumentation technology to provide it. This can then be input to the HAZID, FR, associated barriers, then put into place. It can then be followed up in a subsequent audit to discover if the site response is different.
- The FR 'Presence of exposed hot surfaces (>250°C) ER shall be known to the process controller' is responded with 'No temperature sensor fitted to measure temperature of hot surfaces… smoke and flame detectors can indicate same'. This would infer that the FR of detecting the fire precursor of an exposed hot surface (to prevent fire) uses fire detection used as a hot surface monitor (for fire mitigation). This would show the FR of prevention is not fully understood on board, showing a failing of the HAZID specified FR.
- The FR 'Engineers shall be aware of precursors which can lead to H-2, and when shutdown of the supply should take place' is responded with 'Engineers are aware of the hazard… there is no visible or audible alarm to indicate this situation... parameters can be monitored… will they be able to process the amount of information available

to them?'. This shows that during HAZID, automation may have been put in place to provide the information, but in practice during operation it is discovered the barrier is not effective with clear feedback significantly lacking.

- With the audits monitoring perception of MORR, this can correspond with the MORR values generated during design. If there is a substantial deviation from the perceived importance of a FR once the facility is in operation this provides scope for investigation as it shows a variation is potential risk. Having this tied directly to the original HAZID assumptions allows for easy update where risk has evolved, or a FR deemed acceptable during design is now no longer effective or required. This could provide cost savings where a FR is no longer required but has an OPEX cost associated with it. This money can therefore be diverted to an area of greater concern. This is representative of the evolution of risk and 'safety' being a fluid principle.

Note there is uncertainty surrounding whether the FRs questioned were ever intended to be applied as there appeared to be no documentation on what was implemented during design, what they intended to achieve and how the health of such barriers is to be monitored. Where deviation therefore exists, it is uncertain if this is a deviation from design, or deviation from good practice which was never implemented (perhaps justifiably so). This shows a critical benefit in documenting HAZID and FR decisions and keeping these live which are then directly audited. Questions during audit are therefore based solely on documented FRs which must be implemented to maintain safety. This removes uncertainty when a FR is not complied with. If it is not complied with, there must be follow up to strengthen the barrier or query if the requirement is still valid.

An additional example of one application which may have benefited from the SHORE methodology is the fire on board Le Boreal. It is cautiously noted that hindsight may allow any methodology to promote its use would have prevented an accident. As the fire on board Le Boreal was specifically a systemic failure, with SHORE specifically addressing such failures, additional weight is added to the argument.

The following brief overview is discussed considering the available technologies which could have been/ were installed on board. This can demonstrate if such an approach as discussed in this thesis could have been implemented to reduce the likelihood of the event from occurring.

- Loss Scenario 1: Release of Flammable Material (H-2)
    - Filter on DG4 needs to be replaced – initial stages of maintenance successful: initial feedback success
    - Filter removed on incorrect DG without knowing it was at pressure: feedback failure
    - This scenario occurs because of inadequate feedback and a subsequent incorrect control action implemented – this is a clear unsafe control action. Failure of SMS
- Loss Scenario 2: Exposed Hot Surfaces (H-1)
    - Hot surface exposed on the exhaust manifold through wear and tear of lagging: poor feedback and control (maintenance/ inspection)
    - No analytics to detect the exposed excessive temperature: lack of feedback
    - Damaged lagging and exposed surface not insulated, leading to exposed hot surface: failure of control

From review of the STPA (Appendix A), we can see that such failures in control and feedback are anticipated in the analysis. As per the 'Engineer' controller, Functional Requirement 10.1.1:

- Control action: Engineer begins repair during operation state (i.e. pressurised) (H-2, H-3)
- Unsafe Control Action: Engineer attends operational equipment to conduct maintenance. No indication exists at the equipment that it is operational. Engineer breaks containment while equipment operational

- Functional Requirement: Design of safety critical equipment shall distinctly indicate (passively and actively) its operational status to prevent H2-3.

The functional requirement above relates to the release of flammable materials, however the following functional requirement, also in the ‘Engineer’ controller, could have prevented the presence of the ignition source (FR 15.2.1 and FR15.2.2), which is also a requirement to achieve the ignition:

- Control action: Engineer doesn't shutdown, stop or remove the engine from service when exposed hot surfaces exist (H-1)
- Unsafe Control Action: Engineers unaware of exposed hot surfaces as there are no sensors to reveal their presence, therefore hot surfaces remain exposed.
- Functional Requirement 1: System shall be able to provide alarms in high risk areas to the presence of H-1.
- Functional Requirement 2: System shall be in place to flag up and record presence of H-1.

It is also important to note this failure of control/ feedback is only in the ER. If we continue further up in the SCD, we will almost certainly find failures in control and feedback loops at higher levels which could also help prevent the hazardous scenario. What is certainly clear is that carrying out a retrospective STPA shows that the ignition was almost inevitable with the lack of controls and feedback present at the sharp end (ER).

It is fair to say that when we move away from the direct contact with the hazardous scenario being controlled (i.e. ship automation) the signals of barrier degradation we look for are heavily reliant on audits. Moving forward this may not be the most effective method of barrier monitoring, as it is not an ideal method of maintaining staff ‘buy in’ with respect to fire safety if they are too common. Audits should therefore be used strategically and only query specific criteria of importance. There is a concerted attempt using SHORE to avoid overuse of the

audit function, but within the STPA it continually appears as the obvious (possibly the only) way to monitor barrier degradation with current technology on those higher controllers.

As the process allows the system to be analysed as a whole, through the calculation of control and feedback loops, there is a direct utility for the approach in the HAZID coupling with auditing. One can isolate a controller during an audit and query the functional requirements which relate to control and feedback from that controller. It provides an easy way to implement a phased audit path (from either internal or 3rd party experts) which can, over a suitable review cycle, cover all controllers in the system, and all implemented FRs throughout the lifecycle of the ship.

While this specific case study audit focused on the sharp end and hardware in place, this can easily be applied further back in the bow tie and further up the hierarchy tree. This would simply involve analysis of the controllers higher in the hierarchy in the audit and verifying if gaps exist with those functional requirements determined. This can be used to generate new barriers or enhance processes already in place to strengthen them. This is where the approach has a direct relationship with the SMS and could be used in SMS development and maintenance.

Traditionally safety is “achieved” (in the eyes of regulators and most operators) by compliance, i.e. you go through a standard check list. This is, however, not good enough, as the standard requirements are generic and incomplete, and do not consider assumptions and their capability to change through the facility lifecycle. Therefore, IMO is moving towards the goal-based, essentially safety case based, approach. The approach requires a systematic and ship specific hazard identification and analysis to identify hazards and provide evidence of their control (i.e. presence of barriers). Even though this is not required now, some operators nevertheless would do it in house for internal audits or other purposes. A representative from the cruise operator RCCL, during the SEAMAN project, stated “compliance is the starting point not the end goal”.

The work completed thus far in the pursuit of improved fire prevention safety barriers is in line with the safety case approach. This serves as the foundation for the development of the

SHORE methodology, addressing hazard identification based on systemic risk analysis with a direct link to operational auditing and risk evaluation.

At present hazard identification fails to structurally address systemic risk and is still based on traditional methods to determine what safety barriers are required. These approaches are useful in analysing cost benefit analysis, however there is a gap in analysing the interactions between events, functions, and controllers within the system, which invariably leads to accidents. The SHORE methodology presented has shown a novel approach to incorporate the systemic risk analysis at the HAZID stage to identify the functional requirements of the system and marry this to systemic operational audits. This allows operators to directly address fire prevention using the performance/ goal-based approach through the entire facility lifecycle.

With respect to auditing, there is currently no direct link to the original assumptions made during design, or a direct appreciation of the barriers implemented in design. SHORE provides a direct link to the HAZID and assumptions made during design allowing for more effective audits and continual improvements in facility operations. This will also directly bring the systemic risk analysis into the audit – something audits currently fail to address.

The limitations highlighted on audit effectiveness (174) show the clear importance of auditing not simply covering whether a barrier is physically in place, but rather whether the functional requirement of a particular area of safety is effective. This is one of the primary novel aspect of the approach discussed in this thesis and is the foundation of the proposed audit function of the approach.

To present a methodology which applies systemic risk analysis to both design and operational audits presents novelty and applies the philosophies behind the current state of the art in academic research to both HAZID and auditing.

The simplified version of SHORE presented in Appendix D formalises the approach allowing users to follow the process and method developed within this thesis and validated on the Allure case study, to arrive at a systemic generation of hazards during design, which directly links to the auditing process. This allows quick and effective investigation of the validity of original

design assumptions/ implemented barriers. At present a gap exists in the state of the art in pulling these two critical factors together.

SHORE is the first structured systemic fire prevention tool which can be applied across the facility lifecycle, which can be made integral to the SMS, fundamentally considering the socio technical context and fire prevention as its primary drivers.

7.4 Notes on the Simplified SHORE 'Tool'

The following is intended to provide a narrative in the application of SHORE, showing the flow of the actions to be implemented, followed by a practical representation of typical inputs which would be input to arrive at a complete analysis.

The following shows the basic steps (as also presented in Appendix D) to be followed in sequence which SHORE structurally processes through:

- Construct the safety control diagram
- State the controller being addressed and provide details
- State the hazards which can lead to fire (or any other loss where specified)
- Specify the controller's Control Actions (CAs)
- Specify contexts in which those actions would become Unsafe Control Actions (UCAs)
- Specify Causal Factors (CFs) which would lead to UCAs being made
- Specify Functional Requirements (FRs) which would prevent those causal factors
- Categorise UCAs and CFs
- Propose potential barriers
- Propose the signals and requirements of such barriers
- State any known historical occurrence of the causal factor resulting in the hazard
- Rank the effectiveness and criticality of the functional requirement and calculate the magnitude of risk reduction (MORR)
- Operations: Conduct the audit:
    - Highlight a sample of FRs

- Query the controller if the functional requirement is addressed, providing evidence and explanation
- Have the auditee rank the effectiveness and criticality of the FR
- If there is uncertainty over whether a FR is complied with and it is ranked as important by either the auditee or designer, address this in the barrier improvement system.
- If there is a significant discrepancy between importance of a functional requirement between the designer and the auditee, investigate this. There may be opportunity for improvement here in training, risk management, procedures etc.
- If there are discrepancies between auditees on whether a FR is complied with or not, investigate this as barrier requires to be strengthened.
- If there are multiple barriers found to be missing or not effective, apply these in a barrier improvement system, potentially applying data aggregation of barrier performance and application into the traffic light system.

- Conduct the audit at a reasonable interval, populating the checklist with different controllers and functional requirements contained in the worksheets. This is the primary input to the SMS continual improvement and safety barrier monitoring process.

The template of the proposed approach is presented in Appendix D. The following presents example inputs and extracts from each page of the simplified tool for reference.

7.4.1 SCD Tab

This introductory tool to the SHORE methodology does not currently provide functionality to create a safety control diagram. Many existing tools exist which are purpose built for this function and a link is provided to such tools in order that the SCD can be created, then pasted in (209, 210).

Note these (and other) tools also provide further functionality towards carrying out an STPA which are fundamentally similar to those found in Appendix D. In order, however, to achieve

and integrate the novel aspects of this research (effectiveness/ criticality metrics, direct link to audit generation), such factors are integrated, tailored, and expanded upon in SHORE.

7.4.2 UCAs Tab

Fill in the spaces in the B column next to each header (controller, input, output etc.) for a single controller. There should be a separate sheet for each controller shown in the SCD to allow simplification and clarity in what is being analysed.

Controller	
Objective/ responsibility	
Input	
Output	
Constraints	

Define the hazards. The designer can include as many hazards as they wish. Two are included in the template, but this can be increased by inserting rows.

Hazard ID	**Hazard Description**
H1	
H2	
...	

Do not insert rows between 2-7 as cells E2-E7 are used as specific reference fields.

Example information for an engineer is shown below:

Controller	Engineer
Objective/ responsibility	Maintain equipment within the ER, ensuring hot surfaces and breaks in containment do not occur.
Input	Instruction from Chief Engineer/ ECR. Initiative while in the ER. Sensor readings.
Output	Repair of equipment. Maintenance of equipment. Reports to Chief Engineer/ Company. Feedback to ECR. Manual process control when required.
Constraints	Resources, Time, Instructions, Training, Autonomy
Hazard ID	**Hazard Description**
H1	Release of flammable oil
H2	Exposed hot surface

Manually input every control action for the controller which is related to the control of the stated hazards, including the specific context which would make the action unsafe. Assign a unique ID i.e. CA1, CA2 etc. This will also allow the auto fill option in excel to be used to auto populate the field when all control actions are input.

Control Action ID	Control Action	Unsafe Context	Unsafe Control Action
CA1	Break containment on equipment		
CA2	switch off equipment		
	Report on equipment integrity		

Note: do not insert rows to add control actions between other control actions as this will impact the auto populate in later sections. This is an area for future improvement should this template be put in place for commercial application. This specific template serves as a basic tool for application of the SHORE methodology, or a technical specification for a future commercial product.

Select the unsafe context (from the drop-down box) in which the control action would potentially result in the hazard being analysed.

Control Action ID	Control Action	Unsafe Context	Unsafe Control Action
CA1	Break containment on equipment	Providing	
CA2	switch off equipment	Not Providing	
CA3	Report on equipment integrity	Not Providing	

Not Providing
Providing
Too early
Too late
Stopped to soon/ duration applied = too short
Stopped too late/ duration applied = too long

Manual enter the unsafe control action stating the controller, the control action, the unsafe context, and the result, with a link back to the specific hazard ID which is realised.

Control Action ID	Control Action	Unsafe Context	Unsafe Control Action
CA1	Break containment on equipment	Providing	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)
CA2	switch off equipment	Not Providing	Engineer does not switch off equipment when the equipment operating outside of the safe operating limits (H-2, H-3)
CA3	Report on equipment integrity	Not Providing	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)

Note there may be multiple unsafe contexts and unsafe control actions associated with a single control action so ensure these are all listed before proceeding.

7.4.3 CFs Tab

From the UCAs tab, the initial fields will be pre-populated as below:

Control Action ID	Unsafe control action	Causal Factor Category	Causal Factor	Casual Factor ID
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)			
CA2	Engineer does not switch off equipment when the equipment operating outside of the safe operating limits (H-2, H-3)			
CA3	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)			

Do not insert columns between F-N as cells F1-N1 are used as specific reference fields.

The user must now define the causal factors which can result in the unsafe control action. Select the causal factor category from the drop-down box:

Control Action ID	Unsafe control action	Causal Factor Category	Causal Factor	Casual Factor ID
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)			
CA2	Engineer does not switch off equipment when the equipment operating outside of the safe operating limits (H-2, H-3)			
CA3	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)			

Inadequate input from other controllers/ environment
Inadequate control algorithm/ inadequate responsibilities, knov
Inconsistent process/ mental model
Incomplete process/ mental model
Inadequate feedback
Inadequate control action
Unruly controlled process
Other

Then manually enter the specific causal factor and enter a unique identifier i.e. CF1, CF2 which can also utilise the auto fill function.

Control Action ID	Unsafe control action	Causal Factor Category	Causal Factor	Casual Factor ID
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	Inadequate input from other controllers/ environment	No direct communication to the control room to advise if the equipment is operational or otherwise	CF1
CA2	Engineer does not switch off equipment when the equipment operating outside of the safe operating limits (H-2, H-3)	Inadequate feedback	No sensors in place to monitor and present safe operating limits to the engineer	CF2
CA3	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)	Inadequate control algorithm/ inadequate responsibilities, knowledge or skills	Engineer is not aware there is a requirement to report on loss of integrity	CF3

It is likely that there will be multiple causal factors in various causal factor categories for a single unsafe control action as auto populated form the UCA form. The user must therefore insert new rows and copy the relevant fields to add these multiple causal factors. Care must be taken that when the relevant row is copied, that the correct control action ID and unsafe control action reference values are implemented with reference to the UCA tab.

When changes are made retrospectively to either remove irrelevant rows or add new causal factors later in the process, care should be taken to verify the impact on other tabs and ensure IDs are revalidated and consistent through the worksheet.

An example of a retrospectively added causal factor to CA1, with updated Causal Factor ID list is shown below:

Control Action ID	Unsafe control action	Causal Factor Category	Causal Factor	Casual Factor ID
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	Inadequate input from other controllers/ environment	No direct communication to the control room to advise if the equipment is operational or otherwise	CF1
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	Inconsistent process/ mental model	Indication in the control room shows the equipment is isolated, but indication at the equipment shows it is operational. Conflicting information so the engineer selects the information allowing the work to be completed.	CF2
CA2	Engineer does not switch off equipment when the equipment operating outside of the safe operating limits (H-2, H-3)	Inadequate feedback	No sensors in place to monitor and present safe operating limits to the engineer	CF3
CA3	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)	Inadequate control algorithm/ inadequate responsibilities, knowledge or skills	Engineer is not aware there is a requirement to report on loss of integrity	CF4

Care must be taken to update the FRs tab when changes are made to the CFs tab.

7.4.4 FRs Tab

From the CFs tab, the initial fields will be pre-populated as below:

ID-UCA	UCA	CF ID	Causal factor	ID-FR	Functional requirements
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	CF1	No direct communication to the control room to advise if the equipment is operational or otherwise		
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	CF2	Indication in the control room shows the equipment is isolated, but indication at the equipment shows it is operational. Conflicting information so the engineer selects the information allowing the work to be completed.		
CA2	Engineer does not switch off equipment when the equipment operating outside of the safe operating	CF3	No sensors in place to monitor and present safe operating limits to the engineer		
CA3	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair	CF4	Engineer is not aware there is a requirement to report on loss of integrity		

The user will then manually input the performance based functional requirement which if successfully implemented will result in the elimination of the causal factor. Each FR can then be assigned a unique identifier as with the CFIDs.

ID-UCA	UCA	CF ID	Causal factor	ID-FR	Functional requirements
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	CF1	No direct communication to the control room to advise if the equipment is operational or otherwise	FR1	Engineers in the machinery space who will be interefering with equipement shall have a direct line of communication to the ECR.
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	CF2	Indication in the control room shows the equipment is isolated, but indication at the equipment shows it is operational. Conflicting information so the engineer selects the information allowing the work to be completed.	FR2	Breaking containment shall only ocurr when there is no contradictory information regarding operational state.
CA2	Engineer does not switch off equipment when the equipment operating outside of the safe operating	CF3	No sensors in place to monitor and present safe operating limits to the engineer		Safety critical operational data (i.e. pressure) shall be monitored and presented to ship personnel.
CA3	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-	CF4	Engineer is not aware there is a requirement to report on loss of integrity		Roles and responsibilities shall be clearly documented and known by staff.

The designer then enters the UCA and CF category. Once a category has been entered, this will appear as a drop-down option for future FRs. This will allow the categories to be easily searchable and consistent when the analysis is complete.

Causal factor	ID-FR	Functional requirements	UCA Category	CF Category
No direct communication to the control room to advise if the equipment is operational or otherwise	FR1	Engineers in the machinery space who will be interefering with equipement shall have a direct line of communication to the ECR.	Maintenance	Inadequate communication
Indication in the control room shows the equipment is isolated, but indication at the equipment shows it is operational. Conflicting information so the engineer selects the information allowing the work to be completed.	FR2	Breaking containment shall only ocurr when there is no contradictory information regarding operational state.	Inadequate maintenance/ repair	Inadequate feedback of equipment status/ health
No sensors in place to monitor and present safe operating limits to the engineer	FR3	Safety critical operational data (i.e. pressure) shall be monitored and presented to ship personnel.	Incident response	Inadequate feedback of hazard in the ER to the ECR
Engineer is not aware there is a requirement to report on loss of integrity	FR4	Roles and responsibilities shall be clearly documented and known by staff.	Reporting	Training
0			Maintenance Inadequate maint Incident response Reporting	
0				
0				
0				
0				
0				

The relevant signals and barriers can then be manually populated, and the hazard selected from the drop-down list (linked to the hazards stated in the UCA sheet).

Any previously known occurrences of the specific causal factor can then be listed which will assist with the criticality analysis.

Note: The incident may have occurred elsewhere than the specific application being analysed in the STPA, but if it is credible the same issue could be applied to the hazards being analysed, it should be included if relevant.

Barrier effectiveness and criticality can then be selected from the drop-down lists (effectiveness as previously defined in Table 2) and summarised below.

Effectiveness = the chance of achieving the desired effect/outcome:

Eliminate hazard = 6

Prevent systemic factors of incident = 5

Prevent contributing factors of incident = 4

Prevent direct factors of incident = 3

Control incident (stopping from propagating to accident/loss) = 2

Reduce damage (loss) = 1

Criticality = how safety critical it is to implement this requirement

Step One:

Low Priority: The causal factor is not currently known to have led to previous incidents. Go to Step 2.

High Priority (4): The causal factor led to previous incidents and is dealt with by existing barriers

Very High Priority (5): The causal factor led to previous incidents and is not dealt with by existing barriers.

Step Two (for low priority):

Scenario is improbable (i.e. effective barriers are in place) - Very Low Priority (1)

No record of incident in the past but is covered by existing barriers - Low Priority (2)

It is probable but not addressed/overlooked - Medium Priority (3)

This will then automatically populate a Magnitude of Risk Reduction (MORR) value and colour it as per the risk matrix.

Functional requirements	UCA Category	CF Category	Relevant barriers	Signals and their requirements	Hazard	Previous occurrence in Incident/ Accident (Y/N) + incident ref	Barrier Effectiveness	Criticality	Magnitude of risk reduction
Engineers in the machinery space who will be interefering with equipement shall have a direct line of communication to the ECR.	Maintenance	Inadequate communication	Permit to work procedure	Communication channel between control room and engineer must exist, with engineers empowered to stop the job. Audit of embracing of maintenance management system.		Le Boreal	4	4	16
Breaking containment shall only ocurr when there is no contradictory information regarding operational state.	Inadequate maintenance/ repair	Inadequate feedback of equipment status/ health	Visual indicator (e.g. engine operational)	Indicator reading in real time.		Le Boreal	3	4	12
Safety critical operational data (i.e. pressure) shall be monitored and presented to ship personnel.	Incident response	Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Pressure sensors with diagnostics showing sensor health status.		Splendour of the Seas, Carnival Triumph	3	5	15
Roles and responsibilities shall be clearly documented and known by staff.	Reporting	Training	Training/ Competence Management System	Audit of Competence and job knowledge.		N/A	4	3	12

7.4.5 Audit Tab

From the FRs tab, the initial fields will be pre-populated as below:

Controller	Unsafe Control Action	Causal Factor	Functional Requirement
Engineer	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	No direct communication to the control room to advise if the equipment is operational or otherwise	Engineers in the machinery space who will be interefering with equipement shall have a direct line of communication to the ECR.
Engineer	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	Indication in the control room shows the equipment is isolated, but indication at the equipment shows it is operational. Conflicting information so the engineer selects the information allowing the work to be completed.	Breaking containment shall only ocurr when there is no contradictory information regarding operational state.
Engineer	Engineer does not switch off equipment when the equipment operating outside of the safe operating limits (H-2, H-3)	No sensors in place to monitor and present safe operating limits to the engineer	Safety critical operational data (i.e. pressure) shall be monitored and presented to ship personnel.
Engineer	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-	Engineer is not aware there is a requirement to report on loss of integrity	Roles and responsibilities shall be clearly documented and known by staff.

Before carrying out the audit, the auditor will select a number of functional requirements of their choosing and present these during the audit. As part of a continual audit process, the FRs can be rotated such that all implemented FRs are audited over the course of the facility lifecycle.

During the audit, the auditor asks if the FR is complied with (providing evidence and explanation if required) and the auditee is asked to rank the effectiveness and criticality using the drop-down menus.

Functional Requirement	Is the functional requirement addressed?	Evidence (if required)	Explaination (if require)	How do you rank the effectiveness of the functional requirement = 1-6	How do you rank the criticality of the functional requirement = 1-5
Engineers in the machinery space who will be interefering with equipement shall have a direct line of communication to the ECR.	Yes	Radio required under permit to work		4	2

The completed audit sheet then presents the FRs which are complied with along with evidence, and the comparison between the design based STPA MORR, and the auditee ranked MORR. The auditor can then take the data and interpret accordingly.

Is the functional requirement addressed?	Evidence (if required)	Explaination (if require)	How do you rank the effectiveness of the functional requirement = 1-6	How do you rank the criticality of the functional requirement = 1-5	Evidence/ Explaination Notes	Additional Notes	STPA MORR	Auditee MORR
Yes	Radio required under permit to work		4	2			16	8

8 Conclusions and Future Work

The problem which initiated the research described in this thesis was that maritime machinery spaces regularly have fires from, seemingly, the same causal factors. This research initially aimed to determine why this is the case, and if there is an opportunity for strengthening fire safety through alternative methods, or through modification of the existing means of applying fire safety in these spaces.

The current approach to fires in machinery spaces was postulated to be reactive in nature, primarily focusing on detection of already materialised hazards, ignition, or explosion itself. It was also postulated there is primary focus on dealing with individual safety barriers in isolation at the sharp end with little consideration to the overall system of safety control including the interactions between humans, technology, and the environment.

It was hypothesised these fires continually occur through systemic failures not being addressed in design and operation. To test the hypothesis, a structured systemic fire safety approach was implemented to investigate if opportunities for improvement in machinery space fire safety would present themselves.

The critical review established that the focus of the current approach to fire safety in machinery spaces focuses predominantly on direct causal factors and mitigation measures. The current approach also does not effectively consider the impact of systemic failures. When fire occurs, there has been a control failure in the system. If the control is adequate, the fire will not occur. The fire does, however, occur because the sharp end focus is too little too late.

Taking a closer look at incident prevention, the bias towards direct causal factors is likely to be attributed to the widespread application of linear, event-based models to accident analysis. This linear thinking focuses on incident events and their patterns, which are the visible tip of the iceberg, but systematically fail to explain the underlying structure and process/ mental models that give rise to those events. Therefore, the modern paradigm of systems thinking

had to be addressed. The approach of applying systems thinking was therefore selected to address the hypothesis that a more structured approach to fire safety, accounting for the whole system and encompassing more of the left on the bowtie, will present improvements.

Combining a structured approach with an appreciation of the system of safety control was investigated to present some improvements in safety barrier application and management. Safety auditing was also shown to have scope for improvement in addressing the systemic nature of risk. Current auditing relies heavily on checkboxes and can be either too stringent on the auditor to keep the questioning on rails or can have the opposite effect of being too open ended that repeatability becomes a challenge. As the marine industry applies performance-based design, it was proposed that audits should follow suit and be based upon such a goal-based design.

Applying this systemic approach is one in which the groundwork already exists, with SOLAS allowing for alternative design arrangements with respect to fire safety. With the ability to address alternative design arrangements and treat barrier application and monitoring based on their functional requirement, we move towards a goal-based approach allowing designers the freedom to meet those requirements in a manner appropriate to the facility. Should auditing follow suit this presents performance-based fire safety throughout the entire facility lifecycle.

A case study/ experiment was then conducted to confirm the hypothesis: If a structured fire safety approach is implemented which accounts for interaction between humans, technology and the environment across the entire prevention and mitigation spectrum, opportunities for improvement in machinery space fire safety will present themselves.

The analysis in this thesis tested if a systemic HAZID provided additional benefit in presenting functional requirements which could influence new safety barriers or help strengthen existing barriers, which otherwise would have been overlooked. The research also investigated if there is benefit in carrying out an operational audit directly from such a HAZID process.

To test whether the approach would result in new systems of detection/ hazard monitoring, the thesis applied STPA to specific hazards in an engine room of an operational cruise ship in the form of a case study. The aim was to determine causal factors, rank these causal factors with respect to criticality and effectiveness, and determine if the functional requirements were in place, or if new technologies or strategies could be applied to address these causal factors and improve holistic fire safety on board passenger ships.

The findings were then validated within a group of experts from within the marine industry within the case study. The case study was carried out by analysing the controllers of fire safety in a machinery space within the confines of an organisation. Functional requirements were defined for the system based on the control actions implemented by each controller. To verify the presence of the functional requirements an audit was carried out to verify the HAZID and investigate the benefit of applying an audit directly from the HAZID.

An interesting route for further study emerged in relation to accident investigation being linked with barrier criticality as defined in this thesis. The criticality metric appears to be currently skewed by accident investigations failing to identify systemic causes further left on the bowtie, or higher up in the control hierarchy. As we therefore proposed functional requirements further left on the bowtie, the criticality based on historical occurrence decreases. It is believed this is not reflective of those systemic failures never having occurred, but rather that they were not documented. It is proposed that accident investigations consider a more widespread application of the systemic approach to allow more accurate criticality assignment when considering the magnitude of risk reduction criteria in the HAZID stage.

The research demonstrated that the SOTA systems-based approach allows greater effectiveness of the preventative barriers as it fundamentally deals with breakdown in control leading to an incident i.e. prevention. Application of the developed structured systemic HAZID discovered causal factors and functional requirements which would not have been discovered applying traditional approaches, neglecting the system and its interactions. This was clear when discussing the findings during the case study where no systemic considerations were

documented for future verification during design. Also discovered was the presence of varying perceptions of whether certain functional requirements were in place or not, with no documented decision-making process to refer to. With this HAZID process providing a critical input to any safety barrier improvement initiative, the requirement became clear for a simple to follow method where the process and methodology can be applied to improve safety of a facility in design and operation.

During the HAZID validation and site audit, it became clear that by applying the audit directly from the systemic HAZID, audits become more effective at discovering gaps which otherwise would have been overlooked. The audit demonstrated benefit in coupling the HAZID documentation with the audit questions. Highlighting gaps in control and feedback throughout the system components, which are assumed during HAZID, flags clear routes to failure and allows the company to take pre-emptive action to avert the realisation of these unsafe control actions. Basing safety barriers and audits from these functional requirements has been demonstrated to presents a higher degree of resilience against such events.

The research subsequently introduces SHORE, a method and process of applying HAZID, which will provide the critical input to DBM, with a direct link to the continuous auditing process for integration to the SMS to ensure safe operations in a fluctuating context. It has also demonstrated the importance of SOTA in fire safety applying such an approach. It has been demonstrated that if we treat the problem of fire prevention as a control issue, and we can maintain control, fires in machinery spaces will become a confine of history.

The novelty applied in this thesis is simply applying the systemic approach structurally in both HAZID and Audit to create fire safety as an emerging principle.

In addition to the novelty of applying a structured systemic HAZID to fire safety in the maritime industry, there is also novelty in the particular type of structural approach being used - the use of a systemic accident model for hazard identification and analysis as a direct input to barrier selection and/or performance improvement, which is also directly integrated into the audit

process. This thesis presents the first example of how this can be used to comply with the performance-based method of fire safety design within SOLAS, and directly integrate into the SMS for application within the facility lifecycle.

With respect to the immediate impact of the research, the SHORE method has been applied as part of a global research project with a world leader in operating cruises and an industry leading class society. The method and audit during the case study resulted in critical inputs in improving fire safety in machinery spaces which is now being driven forward within the operator, with consideration being made at the time of writing of integrating the approach into the operator SMS process.

Connected with this impact is the development of the simplified SHORE tool which has scope for commercialisation and application into the wider safety community. This allows the application of the SHORE method higher in the safety control hierarchy which opens up an interesting area of further study, to investigate the findings when the approach extends to the upper echelons of control in the maritime, or any other, industry. Also of interest for future research is the integration of the SHORE methodology into traditional QRA abd the challenges associated with this. These opportunities for further research are discussed in Chapter 10.

Also interesting with respect to future study is the continual expansion of DBM, with the presented method at the heart of barrier selection based on functional requirements. The emerging application of, and access to, ‘big data’ and DBM, coupled with the SHORE approach, may in the future allow improvements to emerge which previously and currently cannot be seen, the possibility of which becomes the elimination of fire as a credible threat.

Connected to the future study in DBM is the issue of response time of the system, and how this differs depending on where you are in the control structure. The response time of alarm to failing barriers at the sharp end must be rapid i.e. the detection of an oil mist which could contact an exposed hot surface at any point. When barriers at the organisational end of the spectrum begin to fail, however, such a rapid response may not be required or even desirable.

This variation in response time and how to address it across the system is an interesting area for future research into DBM.

9 Wider Academic Application

One finding within the case study discovered hardware which appears to have been installed with the intention of detecting leaks is not adequately managed as shown during the audit. It was also shown that it was credible the barrier may not even be known ship personnel. This research would encourage the application of the approach to identify similar situations in any other industry, reviewing not only fire as the potential accident to be prevented. The wider application allows designers and auditors to identify those barriers in place which are not well monitored/ understood/ applied, and apply meaningful metrics of safety review i.e. from a technical perspective using sensor prognostics to existing hardware to provide a cost effective solution to barrier strengthening. The cost-effective argument to this enlightening of the current situation is elementary as the hardware is already in place, we simply investigate whether it is effective. This can be applied with structured consideration of what the performance based functional requirement is for each causal factor's elimination to prevent fire. This is opposed to a mindset of 'the technology is available so we should install it and we will therefore gain 'x' amount of risk reduction as calculated', but with little or no assessment to the functional requirements behind its application and subsequent socio technical failure modes.

This argument is also applicable when reviewing softer barriers, despite the case study specific findings relating primarily to technological shortcomings and the human interactions and perceptions around them. From a societal level, the control and feedback loops are equally as important in achieving whatever 'safety' is in those occasions.

What is equally applicable from an academic perspective is the finding that if you consider physical measures only, then you focus on addition of sensors, for example pressure/ vibration sensors. Sensors may already exist, the capabilities of which are not widely known (as previously discussed). The fact is leaks continue to occur therefore control is ineffective. It would appear the failure is in the original assumptions in design. Is it adequate, and does it provide safety, by adding more sensors but without reviewing the original design assumptions? Addition of sensors for the sake of adding sensors will compound the issue of

data overload with no consideration of the sensor capability, perceived capability, and relevance on what the ‘normal’ operational status looks like. The consideration therefore in decision making to achieve a functional requirement to meet a performance objective, by applying a structured systemic HAZID with associated audit, can be applied to prevent any safety related event, in any field (including but by no means limited to aviation, finance, medicine, business etc.). The only requirement is that the HAZID is conducted by those who are aware of the players or controllers in the system. A background in safety is not an absolute requirement, only that one understands the method and the field/ system being reviewed. The method can be used from an operational perspective to ensure safe operations with the barriers available, or as a research and development or product/ procedure development method. In analysing the system, we can deliberate gaps in available technology or approaches which can provide the focus for relevant and specific innovation.

To highlight the variety of applications and benefit the SHORE approach can provide with respect to academic contribution and impact, I will briefly consider the control and feedback loops surrounding knife crime prevention and mitigation. This problem is somewhat removed from the problem of fire safety in a marine machinery space, but the measures show a potential benefit. If measures are put in place from a governmental level, there will be control and feedback loops which govern such actions. Analysing the controllers in the system along with their control, feedback loops, and contexts in which the decisions are made could reveal a greater understanding of what actions are effective, which actions are ineffective, and what potential causal factors are overlooked.

This example also provides weight to the arguments around prevention vs mitigation effectiveness. An understanding of the controllers and the effectiveness of their actions allows the more accurate identification of the causal factors of the problem and therefore a performance-based solution to prevent such activities.

An increased focus on preventative measures in tackling the systemic causes of knife crime has resulted in a decrease in associated crime, specifically within Scotland since 2005 (211). The approach to knife crime of treating the issue as a public health issue collaborating with

the NHS, education and social work, rather than solely treating it as a policing issue, in an attempt to focus on preventative measures has shown benefit in reducing such crime. While these measures did not specifically apply the approach as determined in this thesis, the idea of, for example, moving away from unnecessary jail terms which would become a subsequent barrier to employment and societal integration (212) would be classed as an 'unsafe control action' of the police (the controller) which could ultimately lead to more violent crime.

Contrast prevention with mitigation-based approaches such as stop and search applied in London, for example. With the increase in knife crime, this may highlight the importance of identifying systemic causal factors and preventing them, rather than mitigating at the unfortunately termed 'sharp' end. It is noteworthy however, that evidence suggests mitigation such as stop and search is ineffective as a 'deterrent', but may be effective as an investigatory power (213). This shows the importance of reviewing the full system and that one must understand the nature of control and feedback loops through the controllers to implement an effective system of control to both prevent and mitigate, while also implementing effective control and feedback loops.

Everyday life in the 21st century involves the interactions between humans, machines and the environment, and this trend is only increasing. Against all odds, if society can do the unthinkable by eliminating fires in engine rooms by analysis of the system, accounting for such human/ machine/ environmental interactions, while structurally removing the potential systemic routes to failure, there is no limit to previously perceived unavoidable hazards being removed from society in our everyday lives/ business ventures. Where we continually live with 'acceptable risk', this can in the future become 'unacceptable'.

10 Limitations

Omitted from the critical review is an examination of the current ‘best practices’ which may be applied by individual companies which are used in conjunction with the rules applied from regulatory or governing bodies. As it was not credible to analyse a suitable range of these internal practices, the review focused only on governing and public rules and standards.

When reviewing FSA, six out of seven data sources for cost effectiveness review were at least ten years old. However, given the fundamental challenges associated with QRA and its application, it is likely that more recent studies would have resulted in similar outcomes. The data sources were selected primarily because of their relevance to the subject matter in hand which was deemed more important than selecting more recent studies on adjacent subjects.

Also excluded from the analysis are underlying factors which fall under the responsibility of controllers above the company in the control structure. These controllers will have an impact on fire safety, for example the effect of political pressures, societal expectations on safety, global economy, any assumptions behind FSA implementation or results etc. During the STPA, however, it was deemed that looking only from the company down would be sufficient to prove the hypothesis proposed. This limitation impacts the results of this thesis as these external controllers will almost certainly impact the controllers in this thesis and affect the controls and feedback loops of the system. It is also likely these omitted controllers will have gaps in control and feedback which are causal factors towards the realisation of the hazards analysed. This is therefore a limitation, but also an interesting area of future study.

During the audit stage of the case study, functional requirements were presented which were assumed to be implemented in some way. This was discussed within the group comprising of class society, system integrator and ship operator personnel. As there was no documented HAZID to reference from which the ship was built, the original design assumptions could not be verified.

Equally, within the audit, it was not possible to verify all 600+ functional requirements across the system so a limited representative sample was selected. This means only a limited sample of functional requirements were audited and therefore the scope of compliance across the entire STPA could not be verified. This would be proposed to be implemented as part of a SMS across a facility lifecycle.

The accident investigation review was also limited to existing research literature on the topic and a small limited sample of fires I provide an overview of. This was deemed sufficient to provide a suitable snapshot of the current focus of accident investigations.

It is important to note at this stage the importance of historical accident or near miss data in the criticality review stage. Should certain causal factors at the organisational level, for example, be omitted from the accident investigation, this could potentially result in an artificially low criticality metric for that causal factor. Consideration should be given to this in the analysis of the findings and future research into this field and that of accident investigation.

The final limitation in the thesis and methodology is an issue which is widely associated with the systemic method. This is the integration into traditional Quantitative Risk Assessment (QRA). At this point the role of the SHORE methodology is to present accurate and additional causal factors which could be directly input to a traditional QRA. The problem is presented in the volume of causal factors which are presented using the SHORE methodology. Applying all of these factors into a traditional QRA and maintain this in operation may not be optimal, or even possible. This therefore continues the discussion around relevance and usefulness of QRA as we move to a systemic basis of risk analysis and barrier implementation. The systems-based approach presents systemic causal factors which can lead to a high consequence, low likelihood event which may traditionally be discounted. This causal factor, however, may be negligeable in cost to protect against and therefore would be logical to implement a preventative functional requirement. To address all of these issues within a QRA would be laborious and challenging, while still inclusive of the limitations of traditional QRA.

Further work should take place to investigate how, as systems evolve and SOTA changes with respect to the most appropriate accident models, we can address risk assessment more appropriately and move past traditional QRA and its associated limitations.

References

1. MIRG BS. Baltic Sea Maritime incident response group project 2014-2016. Finnish Border Guard; 2016.
2. Roueche L, Worldwide Ferry Safety Association, editor Ferry Safety in the Developing World, Challenges
and Opportunities. Passenger Ship Safety Conference.
3. Benito L, editor Taken from Big Data Technology for Maritime Safety. IMO International Conference; 2017; Busan, South Korea.
4. RCL RCCL. http://www.rclcorporate.com/rcl-innovators-are-big-names-at-new-research-center/ 2017 [
5. EMSA, Sweden STRIo, Veritas B, AB SR. Study investigating cost effective measures for reducing the risk from fires on ro-ro passenger ships (FIRESAFE), Appendix: Sensitivity and Uncertainty Analysis. 2016.
6. Papanikolaou A, Nikolaos P. Eliopoulou, Eleftheria. Statistical Analysis of ship accidents that occurred in the period 1990-2012 and assessment of safety level of ship types. Maritime Technology and Engineering; Lisbon2015.
7. Engine Room Fires Can Be Avoided [press release]. Der Norske Veritas2000.
8. Baalisampang T, Abbassi R, Garaniya V, Khan F, Dadashzadeh M. Review and analysis of fire and explosion accidents in maritime transportation. Ocean Engineering. 2018;158:350-66.
9. Protiviti. The road to resiliency: Building a robust audit plan for operational resilience. 2019.
10. Holmberg JE. Defense ‐ in ‐ Depth. Handbook of Safety Principles. 2017:42-62.
11. IMO. MSC-MEPC.2/Circ.12/ Rev.1 Revised Guidelines for formal safety assessment (FSA) for use in the IMO rule making process. International Maritime Organisation; 2015.
12. Perrow C. Normal accidents: Living with high risk technologies-Updated edition: Princeton university press; 2011.
13. Kääriäinen JS, editor High Pressure Water Mist Fire Protection Systems. ASME Turbo Expo 2007: Power for Land, Sea, and Air; 2007: American Society of Mechanical Engineers.
14. Liu Z, Kim AK. A review of water mist fire suppression systems—fundamental studies. Journal of fire protection engineering. 1999;10(3):32-50.
15. Arvidson M. Large-scale water spray and water mist fire suppression system tests for the protection of Ro–Ro cargo decks on ships. Fire technology. 2014;50(3):589-610.
16. Bistrović, Kezić, Komorčec. Historical Development of Fire Detection System Technology on Ships. https://hrcak.srce.hr/1126212013.
17. Vassalos D. Damage stability and survivability–‘nailing’passenger ship safety problems. Ships and Offshore Structures. 2014;9(3):237-56.
18. Cichowicz J, Olufsen O, GL D, Vassalos D, editors. Ro-Ro passenger ships–from Stockholm Agreement to SOLAS2020. Proceedings of the 17 th International Ship Stability Workshop; 2019. Helsinki, Finland: Aalto University.
19. Vanem E, Skjong R. Designing for safety in passenger ships utilizing advanced evacuation analyses—A risk based approach. Safety Science. 2006;44(2):111-35.
20. Ha S, Ku N-K, Roh M-I, Lee K-Y. Cell-based evacuation simulation considering human behavior in a passenger ship. Ocean engineering. 2012;53:138-52.
21. Möller N, Hansson SO. Principles of engineering safety: Risk and uncertainty reduction. Reliability Engineering & System Safety. 2008;93(6):798-805.
22. Bahr NJ. System safety engineering and risk assessment: a practical approach: CRC Press; 2014 2014.
23. Hollnagel E. Barriers and accident prevention: Routledge; 2016.
24. Lees F, Mannan S. Lees' Loss Prevention in the Process Industries, Hazard Identification, Assessment and Control. Fourth Edition ed: Butterworth-Heinemann; 2012.
25. Wróbel K, Montewka J, Kujala P. System-theoretic approach to safety of remotely-controlled merchant vessel. Ocean Engineering. 2018;152:334-45.
26. Leveson. Engineering a Safer World: Systems Thinking Applied to Safety: The MIT Press; 2012.
27. EMSA. Published maritime casualty investigation reports 2018 [Available from: https://emcipportal.jrc.ec.europa.eu/index.php?id=44.
28. DNVGL. Recommended practice: Engine room fire prevention. 2018 January Report No.: DNVGL-RP-0279.

29. IMO. History of SOLAS fire protection requirements London: International Maritime Organisation, http://www.imo.org/en/OurWork/Safety/FireProtection/Pages/History-of-fire-protection-requirements.aspx; [Available from: http://www.imo.org/en/OurWork/Safety/FireProtection/Pages/History-of-fire-protection-requirements.aspx.
30. McNay J, Puisa R, Vassalos D. Analysis of effectiveness of fire safety in machinery spaces. Fire Safety Journal. 2019;108.
31. Lundberg J, Rollenhagen C, Hollnagel E. What-You-Look-For-Is-What-You-Find – The consequences of underlying accident models in eight accident investigation manuals. Safety Science. 2009;47(10):1297-311.
32. Kristiansen S. Maritime transportation: safety management and risk analysis. 2005.
33. Turner BA. Disasters, Man-Made. London: Wykeham Publications; 1978.
34. Dekker S, Pruchnicki S. Drifting into failure: theorising the dynamics of disaster incubation. Theoretical Issues in Ergonomics Science. 2014;15(6):534-44.
35. Rasmussen J. Risk management in a dynamic society: a modelling problem. Safety science. 1997;27(2):183-213.
36. J. R. Risk management, adaptation, and design for safety. Springer; 1994.
37. Leveson NG. Applying systems thinking to analyze and learn from events. Safety science. 2011;49(1):55-64.
38. Read G, Salmon P, Lenné M. Sounding the warning bells: The need for a systems approach to understanding behaviour at rail level crossings. Applied Ergonomics 44: Elsevier; 2013.
39. Besnard D, Hollnagel E. I want to believe: some myths about the management of industrial safety Cogn Tech Work (2014) 16: 13. : Springer; 2014.
40. Hollnagel E. Safety-I and safety-II: the past and future of safety management: CRC Press; 2018.
41. Meadows DH. Thinking in systems: A primer: chelsea green publishing; 2008.
42. Leveson, Dulac. Incorporating safety in early system architecture trade studies. Journal of Spacecraft and Rockets. 2009;46(2):430-7.
43. Qureshi ZH. A review of accident modelling approaches for complex socio-technical systems. Proceedings of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems - Volume 86; Adelaide, Australia. 1387046: Australian Computer Society, Inc.; 2007. p. 47-59.
44. Dekker S. Drift into failure : from hunting broken components to understanding complex systems. Farnham, Surrey, England ;: Ashgate; 2011.
45. Rokseth B, Utne IB, Vinnem JE. A systems approach to risk analysis of maritime operations. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability. 2017;231(1):53-68.
46. Wang YF, Xie M, Ng KM, Habibullah MS. Probability analysis of offshore fire by incorporating human and organizational factor. Ocean Engineering. 2011;38(17):2042-55.
47. Wang YF, Qin T, Li B, Sun XF, Li YL. Fire probability prediction of offshore platform based on Dynamic Bayesian Network. Ocean Engineering. 2017;145:112-23.
48. Su S, Wang L. Three dimensional reconstruction of the fire in a ship engine room with multilayer structures. Ocean Engineering. 2013;70:201-7.
49. Jin Y, Jang B-S. Probabilistic fire risk analysis and structural safety assessment of FPSO topside module. Ocean Engineering. 2015;104:725-37.
50. Salem AM. Use of Monte Carlo Simulation to assess uncertainties in fire consequence calculation. Ocean Engineering. 2016;117:411-30.
51. Jin Y, Jang B-S, Kim J. Fire risk analysis procedure based on temperature approximation for determination of failed area of offshore structure: Living quarters on semi-drilling rig. Ocean Engineering. 2016;126:29-46.
52. Kim SJ, Lee DH, Hong HM, Ahn SH, Park JB, Seo JK, et al. Methods for determining the optimal arrangement of water deluge systems on offshore installations. Ocean Engineering. 2016;114:236-49.
53. Kang HJ, Choi J, Lee D, Park BJ. A framework for using computational fire simulations in the early phases of ship design. Ocean Engineering. 2017;129:335-42.
54. Lee DH, Paik JK, Seo JK. Efficient water deluge nozzles arrangement on offshore installations for the suppression of pool fires. Ocean Engineering. 2018;167:293-309.
55. Wang J, Jiao Y, Shi L, Xie Q, Li G, Liu J, et al. An experimental and non-dimensional study on the vertical temperature distribution of a sealed ship engine room fire. Ocean Engineering. 2018;165:22-33.

56. Wang J, Li G, Shi L, Xie Q, Zhang S. A mathematical model for heat detector activation time under ship fire in a long-narrow space. Ocean Engineering. 2018;159:305-14.
57. Yang R, Khan F, Yang M, Kong D, Xu C. A numerical fire simulation approach for effectiveness analysis of fire safety measures in floating liquefied natural gas facilities. Ocean Engineering. 2018;157:219-33.
58. Kim BJ, Kwan Seo J, Hyo Park J, Sung Jeong J, Keun Oh B, Hoon Kim S, et al. Load characteristics of steel and concrete tubular members under jet fire: An experimental and numerical study. Ocean Engineering. 2010;37(13):1159-68.
59. Kim JH, Kim DC, Kim CK, Islam MS, Park SI, Paik JK. A study on methods for fire load application with passive fire protection effects. Ocean Engineering. 2013;70:177-87.
60. Kim SJ, Lee J, Kim SH, Seo JK, Kim BJ, Ha YC, et al. Nonlinear structural response in jet fire in association with the interaction between fire loads and time-variant geometry and material properties. Ocean Engineering. 2017;144:118-34.
61. Wu B, Zong L, Yip TL, Wang Y. A probabilistic model for fatality estimation of ship fire accidents. Ocean Engineering. 2018;170:266-75.
62. IMO. MSC.1/Circ.1321, 2009 Guidelines for Measures to Prevent Fires in Engine Rooms and Cargo Pump Rooms. International Maritime Organisation; 2009.
63. INNOVA E. Insights on innovation management in Europe: Tangible Results from IMP3rove. 2008.
64. Strategyzer. The Value Proposition Canvas 2020 [Available from: https://www.strategyzer.com/canvas/value-proposition-canvas.
65. Hollnagel E. Barriers and accident prevention: or how to improve safety by understanding the nature of accidents rather than finding their causes. Hampshire: Ashgate. 2016.
66. Johnson WG. MORT safety assurance systems: Marcel Dekker Inc; 1980.
67. Hollnagel. Risk+barriers=safety? Safety Science. 2008;46(2):221-9.
68. Delvosalle C, Fiévez C, Pipart A, Fabrega JC, Planas E, Christou M, et al. Identification of reference accident scenarios in SEVESO establishments. Reliability Engineering & System Safety. 2005;90(2-3):238-46.
69. Greenfield S. Dynammic barrier management. ESREL2016; 28/09/16; Glasgow2016.
70. Saleh JH, Marais KB, Bakolas E, Cowlagi RV. Highlights from the literature on accident causation and system safety: Review of major ideas, recent contributions, and challenges. Reliability Engineering & System Safety. 2010;95(11):1105-16.
71. Heinrich H, Peterson D, Roos N. Industrial Accident Prevention. 5th Edition ed: McGraw Hill, New York; 1980.
72. Reason J. Human Error: Cambridge University Press; 1990.
73. EMSA EMSA. Safety Analysis of Data Reported in EMCIP, Analysis on Marine Casualties and Incidents Involving Fishing Vessels. April, 2018.
74. Everett C, Hall T, Insley S. NASA Accident Precursor Analysis Handbook, National Aeronautics and Space Administration Office of Safety and Mission Assurance2011.
75. Leveson N. An STPA Primer. 2013.
76. Pomeroy R, Earthy J. Merchant shipping's reliance on learning from incidents - A habit that needs to change for a challenging future. Safety Science Journal. Jan 2017;99:45-57.
77. Goerlandt F, Montewka J. Maritime transportation risk analysis: Review and analysis in light of some foundational issues. Reliability Engineering & System Safety. 2015;138:115-34.
78. Carroll J. Organizational Learning Activities in High-Hazard Industries: The Logics Underlying Self-Analysis1998. 699-717 p.
79. Leveson N. A new accident model for engineering safer systems. Safety Science. 2004;42(4):237-70.
80. Schröder-Hinrichs JU, Baldauf M, Ghirxi KT. Accident investigation reporting deficiencies related to organizational factors in machinery space fires and explosions. Accident Analysis & Prevention. 2011;43(3):1187-96.
81. Rollenhagen C, Westerlund J, Lundberg J, Hollnagel E. The context and habits of accident investigation practices: A study of 108 Swedish investigators. Safety Science. 2010;48(7):859-67.
82. Hollnagel E. Cognitive reliability and error analysis method (CREAM): Elsevier; 1998.
83. Cardis PA. CASMET. Casualty Analysis Methodology for Maritime Operations. Athens: National Technical University of Athens; 1999. Contract No.: C01.FR.003.
84. Hollnagel E. CREAM - Cognitive Reliability and Error Analysis Method Personal website2012 [Available from: http://erikhollnagel.com/ideas/cream.html.
85. EMSA EMSA. Annual Overview of Marine Casualties and Incidents. 2017.

86. IMO. MSC 87/26 Report of the maritime safety committee on its eighty seventh session. 2010.
87. IMO. MSC/Circ.1002 Guidelines on Alternative Design and Arrangements for Fire Safety. International Maritime Organisation; 2001.
88. IMO. MSC.Circ.1212 Guidelines on Alternative Design and Arrangements for SOLAS Chapters II-I and III. International Maritime Organisation; 2006.
89. SFPE, NFPA. The SFPE Engineering Guide to Performance-Based Fire Protection Analysis and Design of Buildings. 2nd Edition ed: Society of Fire Protection Engineers and National Fire Protection Association; 2005.
90. International Convention for Safety of Life at Sea, SOLAS, Consolidated Edition. Sect. Chapter II, Regulation Four (2014).
91. IMO. ISM code : International safety management code and guidelines for its implementation. 4th edition, 2014 edition. ed2014.
92. ISO. FSS Code International Code for Fire Safety Systems. International Maritime Organisation; 2015.
93. ISO. ISO 14520:2015 Gaseous fire-extinguishing systems -- Physical properties and system design. 3rd Edition ed2015.
94. IEC IEC. IEC 61511 Functional safety - Safety instrumented systems for the process industry sector. IEC, Geneva, Switzerland: IEC; 2017.
95. IMO. MSC.1/Circ.1533 Revised Guidelines on Evacuation Analysis for New and Existing Passenger Ships. International Maritime Organisation; 2016.
96. Lloyd's. Top 10 classification societies: Lloyd's List Maritime Intelligence; 2017 [Available from: https://lloydslist.maritimeintelligence.informa.com/LL1120174/Top-10-classification-societies-2017.
97. ClassNK. 18-490 Rules for Integrated Fire Control Systems. 2018.
98. ClassNK. 18-460 Rules and Guidance for the Survey and Construction of Steel Ships, Part R Fire Protection, Detection and Extinction. 2018.
99. ABS. Guidance Notes on Fire-Fighting Systems. American Bureau of Shipping; 2015.
100. Lloyd's. Lloyd's Register Guidance Notes for Risk Based Analysis: Fire Loads and Protection. Lloyd's Register Group; 2014.
101. DNVGL. Rules for Classification of Ships, Part 4 Systems and Components, Chapter 11, Fire Safety. DNVGL Høvik2015.
102. DNV-GL. Rules for Classification: Ships DNVGL-RU-SHIP Pt.6 Ch.5. Edition July 2018, amended February 2019. 2019.
103. ISO. BS EN ISO 12100:2010 Safety of machinery – General Principles for design – Risk assessment and risk reduction. BSI; 2010.
104. EU. Directive 2006/42/EC of the European Parliament
and of the Council of 17 May 2006 on Machinery, and Amending Directive 95/16/EC
(recast). 2006.
105. IMO. MSC 83/INF.2 Formal Safety Assessment Consolidated text of MSC/Circ.1023-MEPC/Circ.392. International Maritime Organisation; 2007.
106. Breinholt C, Ehrke K-C, Papanikolaou A, Sames PC, Skjong R, Strang T, et al. SAFEDOR–The Implementation of Risk-based Ship Design and Approval. Procedia - Social and Behavioral Sciences. 2012;48:753-64.
107. IMO. MSC 85/17/1 FSA - Cruise Ships, Formal Safety Assessment, Submitted by Denmark. International Maritime Organisation; 2008.
108. IMO. MSC 85/INF.2 FSA - Cruise Ships, Details of Formal Safety Assessment, Submitted by Denmark. International Maritime Organisation; 2008.
109. Wikman J, Evegren F, Rahm M, Leroux J, Breuillard A, Kjellberg M, et al. Study investigating cost effective measures for reducing the risk from fires on ro-ro passenger ships (FIRESAFE). European Maritime Safety Agency; 2017.
110. EMSA, Sweden STRIo, Offshore BVM, Rederi S. Second study investigating cost-efficient measures for reducing the risk from fires on ro-ro passenger ships (FIRESAFE II). 2018.
111. Skjong R, Eknes M, editors. Economic activity and societal risk acceptance. Proc ESREL; 2001.
112. Skjong R, Eknes ML. Societal risk and societal benefits. Risk, Decision and Policy. 2002;7(1):57-67.
113. Yang Z, Wang J, Li K. Maritime safety analysis in retrospect. Maritime Policy & Management. 2013;40(3):261-77.
114. Kontovas CA, Psaraftis HN. Formal safety assessment: a critical review. Marine technology. 2009;46(1):45-59.
115. Psaraftis HN. Formal safety assessment: an updated review. Journal of Marine Science and Technology. 2012;17(3):390-402.

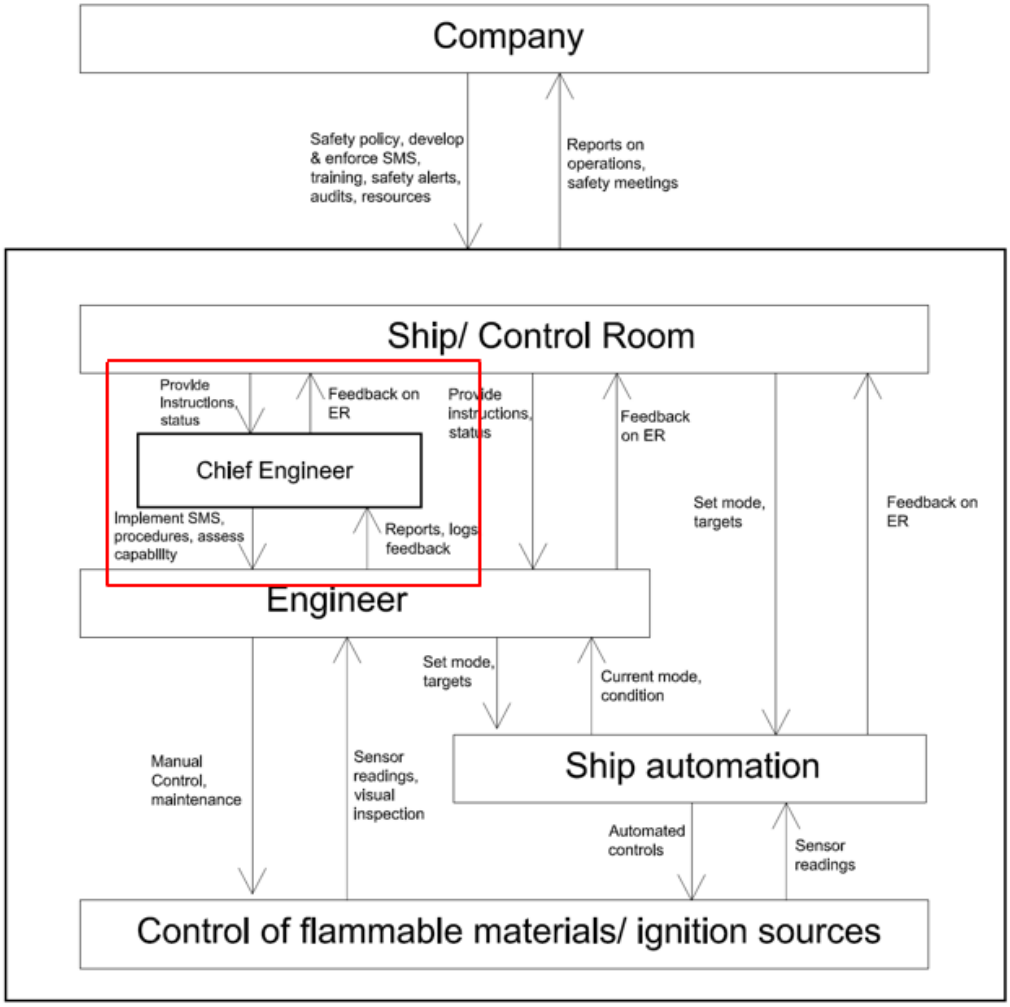
116. Skjong R, Wentworth BH, editors. Expert judgment and risk perception. The Eleventh International Offshore and Polar Engineering Conference; 2001: International Society of Offshore and Polar Engineers.
117. Puisa R, Lin L, Bolbot V, Vassalos D. Unravelling causal factors of maritime incidents and accidents. Safety Science. 2018;110:124-41.
118. Puisa R, Williams S, Vassalos D. Towards an explanation of why onboard fires happen: The case of an engine room fire on the cruise ship “Le Boreal”. Applied Ocean Research. 2019;88:223-32.
119. Rae A, McDermid J, Alexander R. The science and superstition of quantitative risk assessment. Journal of Systems Safety. 2012;48(4):28.
120. Beer J. The true significance of common cause failures in accidents. University of York, York. 2011.
121. Machol R. Principles of Operations Research—10. The Titanic Coincidence. Interfaces. 1975;5(3):53-4.
122. Dekker S. The criminalization of human error in aviation and healthcare: A review. Safety science. 2011;49(2):121-7.
123. Woods DD, Johannesen LJ, Cook RI, Sarter NB. Behind human error: Cognitive systems, computers and hindsight. Dayton Univ Research Inst (Urdi) OH; 1994.
124. Dekker S. The field guide to understanding'human error': Ashgate Publishing, Ltd.; 2014.
125. Leveson NG. Safeware. System Safety and Computers Addison Wesley. 1995.
126. Sarter NB, Woods DD, Billings CE. Automation surprises. Handbook of human factors and ergonomics. 1997;2:1926-43.
127. Sormunen O-VE, Goerlandt F, Häkkinen J, Posti A, Hänninen M, Montewka J, et al. Uncertainty in maritime risk analysis: Extended case study on chemical tanker collisions. Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment. 2015;229(3):303-20.
128. Wikman J, Evegren F, Rahm M, Leroux J, Breuillard A, Kjellberg M, et al. Study investigating cost effective measures for reducing the risk from fires on ro-ro passenger ships (FIRESAFE). Appendix: Sensitivity and Uncertainty Analyses. EMSA; 2016. Contract No.: EMSA/OP/01/2016.
129. Akyildiz H, Mentes A, Helvacioglu IH, editors. Formal Safety Assessment of Cargo Ships at Coasts and Open Seas of Turkey. ASME 2012 31st International Conference on Ocean, Offshore and Arctic Engineering; 2012: American Society of Mechanical Engineers Digital Collection.
130. Akyildiz H. Formal Safety Assessment of a Fishing Vessel. Gidb Magazinr. 2015;1:31-46.
131. Lois P, Wang J, Wall A, Ruxton T. Formal safety assessment of cruise ships. Tourism management. 2004;25(1):93-109.
132. Guarin L, Konovessis D, Vassalos D. Safety level of damaged RoPax ships: risk modelling and cost-effectiveness analysis. Ocean Engineering. 2009;36(12-13):941-51.
133. Goerlandt F, Hänninen M, Ståhlberg K, Montewka J, Kujala P. 25. Simplified Risk Analysis of Tanker Collisions in the Gulf of Finland. Miscellaneous Problems in Maritime Navigation, Transport and Shipping: Marine Navigation and Safety of Sea Transportation. 2011:181.
134. Wu B, Yan X, Wang Y, Soares CG. Selection of maritime safety control options for NUC ships using a hybrid group decision-making approach. Safety science. 2016;88:108-22.
135. Correia P. European Marine Casualty Information Platform a common EU taxonomy. 5th International Conference on Collision and Grounding of Ships (ICCGS); Espoo, Finland2010.
136. Beamer. Marine Safety Investigation Report, Fire in the engine compartment on board the Expedition-Cruiser Liner Le Boreal on 18th November 2015. 2016.
137. MSIU TM. Safety Investigation Report: MV Zenith, Fire in the Engine Room, 2013 Marine Safety Investigation Unit; 2014.
138. MAIB. Sea Gale Fire on 20 May 2014, Marine Accident Report. Danish Maritime Accident Investigation Board; 2015.
139. Lundberg J, Rollenhagen C, Hollnagel E. What you find is not always what you fix—How other aspects than causes of accidents decide recommendations for remedial actions. Accident Analysis & Prevention. 2010;42(6):2132-9.
140. Carroll J. Incident reviews in high-hazard industries: sensemaking and learning under ambiguity and accountability. Industrial and Environmental Crisis Quarterly. 1995:175-97.
141. Photonic ASA, editor Fiber Optic Linear Heat Monitoring. Passenger Ship Safety; 2017; Southampton.
142. APM M. Oil Mist Detector Air Particle Monitor, Reference Manual, FGD-MAN-0077, Rev 7. 2017.
143. Tyco. IR6003/7 IR Oil Mist/ Smoke Detector, Technical Product Sales Data Sheet, Oil and Gas. 2015.

144. DASPOS, editor Oil Mist and Gas Leakage Detection – Early Warning System. Passenger Ship Safety; 2017.
145. IMO. MSC/Circ.1086 Code of Practice for Atmospheric Oil Mist Detectors. International Maritime Organisation; 2003.
146. Photonics R. https://rebellionphotonics.com/products.html [
147. FLIR. http://www.flir.com/security/display/?id=83533 [
148. Kim DH. Introduction to systems thinking: Pegasus Communications Waltham, MA; 1999.
149. DNVGL. Incident Investigation: Expert analysis is the key to preventing recurrences [Available from: www.dnvgl.com/services/incident-investigation-1095.
150. Sklet S. Methods for accident investigation. Norwegian University of Science and Technology; 2002.
151. Lundberg J, Rollenhagen C, Hollnagel E, Rankin A. Strategies for dealing with resistance to recommendations from accident investigations. Accident Analysis & Prevention. 2012;45:455-67.
152. Rothblum AM. Human Error and Marine Safety. National Safety Council Congress and Expo, Orlando, FL.2000.
153. Norman DA. Categorization of action slips. Psychological review. 1981;88(1):1.
154. Norman DA. The 'problem'with automation: inappropriate feedback and interaction, not 'over-automation'. Phil Trans R Soc Lond B. 1990;327(1241):585-93.
155. Puisa R, Williams S, Vassalos D. Systems Approach to Accident Analysis: Engine Room Fire on Cruise Ship "Le Boreal". International Maritime Conference on Design for Safety; 16-21 September Kobe, Japan2018.
156. Rasmussen J. Information Processing and Human–Machine Interaction: An Approach to Cognitive Engineering, North-Holland Series in System Science and Engineering, 12: North-Holland New York; 1986.
157. Fleming KN, Silady FA. A risk informed defense-in-depth framework for existing and advanced reactors. Reliability Engineering & System Safety. 2002;78(3):205-25.
158. Duijm NJ. Safety-barrier diagrams as a safety management tool. Reliability Engineering & System Safety. 2009;94(2):332-41.
159. Hollnagel E. The ETTO principle: efficiency-thoroughness trade-off: why things that go right sometimes go wrong: CRC Press; 2017.
160. Puisa R. Dynamic barrier management - methodology. University of Strathclyde Maritime Safety Research Centre; 2020. Contract No.: D1-UoS.
161. Wang J. The current status and future aspects in formal ship safety assessment. Safety Science. 2001;38(1):19-30.
162. Wang J. Maritime Risk Assessment and its Current Status. Quality and Reliability Engineering International. 2006;22:3-19.
163. Wang J. Offshore safety case approach and formal safety assessment of ships. Journal of Safety Research. 2002;33(1):81-115.
164. DNVGL. Group Technology and Research Position paper, Maintaining Confidence: Dynamic risk management for enhancing safety. 2017.
165. Geddes A, Laverick S, McBride A, McIntyre GT. Severity and Outcome Assessment score: a useful tool for auditing orthognathic surgery. British Journal of Oral and Maxillofacial Surgery. 2019;57(3):246-50.
166. Aude V, Yolande L, Pierre S. Feasibility and impact of national peer reviewed clinical audits in radiotherapy departments. Radiotherapy and Oncology. 2020;144:218-23.
167. Mitchell R, Friswell R, Mooren L. Initial development of a practical safety audit tool to assess fleet safety management practices. Accident Analysis & Prevention. 2012;47:102-18.
168. Manita R, Elommal N, Baudier P, Hikkerova L. The digital transformation of external audit and its impact on corporate governance. Technological Forecasting and Social Change. 2020;150:119751.
169. Asante-Appiah B. Does the severity of a client's negative environmental, social and governance reputation affect audit effort and audit quality? Journal of Accounting and Public Policy. 2020:106713.
170. Stolker R, Karydas D, Rouvroye J. A comprehensive approach to assess operational resilience. Eindhoven University of Technology.
171. McDonald N. *Organizational Resilience and Industrial Risk*. In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds). *Resilience Engineering, concepts and precepts*: Ashgate Publishing Limited; 2006. p. pp 155-80.
172. Allford L. The auditing of process safety. Journal of Loss Prevention in the Process Industries. 2016;43:747-52.
173. Wilkinson P. The Role of "active Monitoring" in Preventing Major Accidents. 2014.
174. HSE. Buncefield: Why Did it Happen? : Health and Safety Executive; 2011.

175. Blewett V, O'Keeffe V. Weighing the pig never made it heavier: Auditing OHS, social auditing as verification of process in Australia. Safety Science. 2011;49(7):1014-21.
176. Costella MF, Saurin TA, de Macedo Guimarães LB. A method for assessing health and safety management systems from the resilience engineering perspective. Safety Science. 2009;47(8):1056-67.
177. Saurin TA, Carim Júnior GC. Evaluation and improvement of a method for assessing HSMS from the resilience engineering perspective: A case study of an electricity distributor. Safety Science. 2011;49(2):355-68.
178. Culture S. iAuditor Checklists by Safety Culture 2020 [Available from: https://safetyculture.com/checklists/.
179. ROSPA. Audit Selection Tool 2019 [Available from: https://www.rospa.com/Safety-Consultants/Work/Safety-Audits/Audit-Selection-Tool.
180. Media S. Safety Media Access Health and Safety Software [Available from: https://safetymedia.co.uk/?gclid=EAIaIQobChMI9LeZ6YTC6QIViKztCh3ehgG_EAAYAiAAEgJOkvD_BwE.
181. IAEA. Comprehensive Audits of Radiotherapy Practices: A Tool for Quality Improvement. Quality Assurance Team for Radiation Oncology (QUATRO)2007.
182. Hollnagel E, Woods D. Epilogue: Resilience Engineering Precepts. https://www.researchgate.net/profile/David_Woods11/publication/265074845_Epilogue_Resilience_Engineering_Precepts/links/546b62c70cf2397f7831bdfc/Epilogue-Resilience-Engineering-Precepts.pdf2006.
183. Andrews G. Was it foreseeable? Lecture to UKELG University of Leeds2016.
184. Dekker S. Past the edge of chaos. Lund University School of Aviation; 2006.
185. Woods DD. Escaping failures of foresight. Safety Science. 2009;47(4):498-501.
186. Buzancic, Primorac B, Parunov J. Review of Statistical Data on Ship Accidents. Maritime Technology and Engineering. 2016:809-14.
187. Eliopoulou E, Papanikolaou A, Voulgarellis M. Statistical analysis of ship accidents and review of safety level. Safety Science. 2016;85:282-92.
188. Konovessis D, Vassalos D. Risk evaluation for RoPax vessels. Institution of Mechanical Engineers Part M Journal of Engineering for the Maritime Environment. 2008.
189. Ikeagwuani UM, John GA. Safety in maritime oil sector: Content analysis of machinery space fire hazards. Safety Science. 2013;51(1):347-53.
190. Foundation LR. Insight report on safety in the passenger ferry industry: A global safety challenge. Lloyd's Register Foundation; 2018.
191. Underwood P, Waterson P, Braithwaite G. 'Accident investigation in the wild' – A small-scale, field-based evaluation of the STAMP method for accident analysis. Safety Science. 2016;82:129-43.
192. Underwood P, Waterson P. Systems thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models. Accident Analysis & Prevention. 2014;68:75-94.
193. de Ruijter A, Guldenmund F. The bowtie method: A review. Safety Science. 2016;88:211-8.
194. International Convention for Safety of Life at Sea, SOLAS,
Consolidated Edition. Sect. Chapter II Part E: Operational Requirements (2014).
195. DNVGL, RCCL, Strathclyde Uo. SEAMAN Project Workshop, Miami, 24-26 February. https://meet.dnvgl.com/sites/SEAMAN/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/SEAMAN/OneNote/SEAMAN&action=default2019.
196. Puisa R, Bolbot V, Ihle I. Development of functional safety requirements for DP-driven servicing of wind turbines. 7th European STAMP Workshop & Conference; Helsinki: Aalto University; 2019.
197. DNVGL. Rules for Classification, Ships, Part 4 Systems and components, Chapter 1 Machinery systems, general. 2018.
198. DNVGL. Rules for classification, Ships, Part 4 Systems and components, Chapter 6 Piping systems. 2019.
199. DNVGL. Rules and classification, Ships, Part 6 Additional class notations, Chapter 2 Propulsion, power generation and auxiliary systems. 2019.
200. DNVGL. Rules for classification, Ships, Part 4, Systems and components, Chapter 7 Pressure equipment. 2019.
201. DNVGL. Rules for classification, Ships, Par 4 Systems and components, Chapter 9 Control and monitoring systems. 2019.
202. Reiman T, Pietikäinen E. Leading indicators of system safety – Monitoring and driving the organizational safety potential. Safety Science Journal. 2012;50:1993-2000.

203. **Alexandros K**. Dynamic barrier management - Barrier performance diagnostics and prognostics. University of Strathclyde Maritime Safety Research Centre; 2020. Contract No.: D3B-UoS.
204. Authority BM. Carnival Triumph joint report of the investigation into an engine room fire on February 10th, 2013. 2014.
205. Authority BM. Report of the investigation into the forward engine room fire which occurred on the 22nd October 2015. 2017.
206. Saleh JH, Marais KB, Favaro FM. System safety principles: A multidisciplinary engineering perspective. Journal of loss prevention in the process industries2014. p. 283-94.
207. McNay J. SEAMAN - Engine room fire risk model. University of Strathclyde Maritime Safety Research Centre; 2020. Contract No.: D3A-UoS.
208. BSI. ISO 31000: 2018 Risk Management - Guidelines. 2018.
209. Safety AS. STAMP/STPA and SCDL Diagrams 2020 [Available from: https://astah.net/products/system-safety-diagrams/.
210. Stuttgart SergotUo. XSTAMPP (eXtensible STAMP Platform) 2019 [Available from: https://github.com/SE-Stuttgart/XSTAMPP.
211. BBC. How Scotland stemmed the tide of knife crime 2019 [Available from: https://www.bbc.co.uk/news/uk-scotland-45572691.
212. NewScientist. What London's police can learn from Glasgow's approach to knife crime 2019 [Available from: https://www.newscientist.com/article/2195953-what-londons-police-can-learn-from-glasgows-approach-to-knife-crime/.
213. FullFact. The UK's independent fact checking charity: Does Stop and Search Work? [Available from: https://fullfact.org/crime/does-stop-search-work/.

Appendix A: STPA Application on a Cruise Ship Machinery Space


Company
Safety policy, develop & enforce SMS, training, safety alerts, audits, resources
Reports on operations, safety meetings
Ship/ Control Room
Provide Instructions, status
Feedback on ER
Chief Engineer
Implement SMS, procedures, assess capability
Reports, logs feedback
Provide instructions, status
Feedback on ER
Set mode, targets
Feedback on ER
Engineer
Set mode, targets
Current mode, condition
Manual Control, maintenance
Sensor readings, visual inspection
Ship automation
Automated controls
Sensor readings
Control of flammable materials/ ignition sources

Chief Engineer

Objective/ responsibility	Set procedures, ensuring hot surfaces and breaks in containment do not occur. Provide instruction to ensure fire does not occur.
Input	Instruction from ECR. Maintenance reports. Initiative in providing direct instruction. Sensor readings.
Output	Instruction to engineers. Maintenance procedures. Reports to Company. Feedback to ECR.
Constraints	Resources, Time, Training, Company Pressures

Hazards

H1	Hot surfaces (>220degC) in ER
H2	Leak from pressurised oil systems
H3	Failure to contain oil leak

Actions	Control Action	Not providing	Providing	Too early	Too late	Stopped to soon (applied too short)	Applied too long
A1	Inspect equipment	Chief engineer does not detect loss of integrity during inspection (H1-3) Chief engineer does not detect incorrect implementation of equipment as per manufacturer guidelines during inspection (H2-3)	Chief engineer interferes with equipment and doesn't return to its original condition during inspection (H1-3)		Chief engineer inspects equipment too late to find damaged/ degraded equipment (H1-3)	Chief engineer does not complete inspection when hot surfaces or damaged/ degraded equipment present (H1-3)	
A2	Report on integrity	Chief engineer does not report on loss of integrity to ECR/ engineers to instruct the repair to be completed (H1-3)	Chief engineer report on integrity is too vague when a specific repair is required (H1-3)		Chief engineer reports on integrity too late when damaged/ degraded equipment remains in place (H1-3)		
A3	Repair equipment	Chief engineer doesn't repair equipment when faulty equipment present (H1-3)	Chief engineer begins repair during operational state (i.e. pressurised) (H2-3) Chief engineer repairs equipment but does not complete/ implement the repair correctly (H1-3)	Chief engineer starts repairing equipment before making necessary preparations (H1-3)	Chief engineer repairs equipment too late when damaged/ faulty equipment exists (H1-3)	Chief engineer starts repair, but doesn't complete when faulty equipment is present (H1-3)	
A4	Shutdown engine	Chief engineer doesn't shutdown the engine when exposed hot surfaces exist (H1-3) Chief engineer doesn't shutdown the engine when strain on the engine components exceed design threshold (H2-3)	Chief engineer shuts down the engine and does not immediately reduce load on other engines which become temporarily overloaded (H-1, H-2)		Chief engineer shuts down the engine too late when a fuel/ lube oil release exists (H2-3) Chief engineer doesn't shutdown the engine fast enough when exposed hot surfaces exist (H1-3)		
A5	Shutdown fuel supply	Chief engineer doesn't shutdown the fuel supply when strain on the components exceed design threshold (H2-3)			Chief engineer shuts down the fuel supply too late when a fuel/ lube oil release exists (H2-3)		
A6	Release water mist	Chief engineer doesn't release the water mist when exposed hot surfaces exist and oil mist in the atmosphere is detected/suspected (H-1)			Chief Engineer releases the water mist too late when leak exists (H-1). Chief Engineer releases the water mist too late when exposed hot surface exists (H-1)	Chief engineer stops the water mist too soon when exposed hot surfaces have existed and oil mist in the atmosphere is detected/suspected (H-1)	
A7	Write maintenance procedure	Chief engineer not writing a maintenance procedure results in no/ inconsistent maintenance leading to H1-3. Chief engineer not writing a maintenance procedure results in engineers carrying out repair/ inspection without formal procedure resulting in H1-3.	Chief engineer provides a maintenance procedure which is not adequate to ensure prevention of H1-3.				
A8	Read maintenance report	Chief engineer does not read maintenance report therefore does not know about required repairs (H1-3)	Chief engineer reads the report but doesn't understand the results (H1-3)		Chief engineer reads the report too late meaning by the time the repair is placed in the work order a failure has already occurred (H1-3)		
A9	Authorise engineer competence	Chief engineer does not authorise engineer competence resulting in engineers conducting work above their competence level (H1-3)	Chief engineer authorises competence of an engineer who does not have competence for specific procedures relating to H1-3.				

ID	Unsafe control action	Inadequate input (missing, wrong, too late/early etc.) / out-of-range disturbances	Inadequate control algorithm (fault, data handling etc.) /Inadequate responsibilities, knowledge or skills	Inconsistent process (mental) model	Design of incomplete process (mental) model	Inadequate feedback (incomplete, too late, missing, etc.)	Inadequate control path (too late, etc.)	Unruly controlled process
		Engineer asks for second opinion on damaged/ fatigued equipment but advises the chief engineer to check the wrong equipment.	Chief engineer is not aware of what to look for/ what the signs are of loss of integrity of the hotbox due to lack of skills/ knowledge.					
1	**Chief engineer does not detect loss of integrity during inspection (H1-3)**							
		ECR advises on damaged/ fatigued equipment but advises the chief engineer to check the wrong equipment.	Chief engineer does not believe it is his/ her responsibility to look for loss of integrity.					
2	**Chief engineer does not detect incorrect implementation of equipment as per manufacturer guidelines during inspection (H2-3)**	Manufacturer specific guidelines are not provided to verify equipment against.		Chief engineer has worked with similar equipment and believes the set up should be the same, but in fact the manufacturer recommends some differences.		The tools available to the Chief engineer are insufficient to detect integrity loss of the fuel supply pipework i.e. no torque wrench to verify torque level of the bolts.		
3	**Chief engineer interferes with equipment and doesn't return to its original condition during inspection (H1-3)**		Chief engineer does not have the training/ skillset to adequately understand the impact of interfering with equipment to get a closer inspection, resulting in continued hot surface exposure, or damaged/ fatigued equipment.					
4	**Chief engineer inspects equipment too late to find damaged/ degraded equipment (H1-3)**			Engineer reports damaged equipment which could result in H1-3 but the chief engineer deems it unimportant and dismisses the information.			Engineers report damaged equipment which could result in H1-3 to chief engineer but the chief engineer is too busy to address the concern.	
5	**Chief engineer does not complete inspection when hot surfaces or damaged/ degraded equipment present (H1-3)**		Chief engineer does not have training on how to complete a check and therefore does not complete it.	Chief engineer believes the inspection is complete but is unaware of additional checks which are required.				
6	**Chief engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H1-3)**		Chief engineer is not trained in report writing and fail to communicate the loss of integrity to the hierarchy meaning management are unaware of fatigue to the hot box, fatigue of the fuel supply system, or hot surfaces.	Chief engineer inspects the equipment, registers the loss of integrity of the hot box but is not aware that this presents the risk of H-3, therefore does not take or recommend action to fix.				
			Chief engineer is instructed of a required upgrade. The work is carried out in an uncontrolled/ undocumented way. Company is unaware of what equipment is upgraded/ what is outstanding.	Chief engineer inspects the equipment, registers the loss of integrity of the fuel supply pipework but is not aware that this presents the risk of H-2, therefore does not take or recommend action to fix.				
7	**Chief engineer report on integrity is too vague when a specific repair is required (H1-3)**		Chief engineer is not trained in report writing and fails to communicate the specific equipment requiring repair, leading to confusion when the repair is then to be completed. Inadequate repair completed due to vague report, resulting in remaining fatigue of the hot box, fatigue of the fuel supply system, or hot surfaces.					
8	**Chief engineer reports on integrity too late when damaged/ degraded equipment remains in place (H1-3)**						Chief engineer workload too busy that no time is dedicated to writing the report and the loss of integrity is reported too late.	
9	**Chief engineer doesn't repair equipment when faulty equipment present (H1-3)**		Company is made aware of a vulnerability associated with a piece of process equipment (i.e. fuel supply connection vulnerability to leak). Instruction is provided down the chain of command to the chief engineer to implement the solution but this is not implemented due to a perceived low priority status.				Faulty condition (i.e. seal gaps in the hot box) becomes normalised. No repair/ replacement carried out.	
10	**Chief engineer begins repair during operational state (i.e. pressurised) (H2-3)**	No indication exists at the equipment that it is operational. Chief engineer breaks containment while equipment operational	Chief engineer decides to implement a fix while conducting an impromptu ER inspection. It is perceived as a quick fix so normal protocols are not followed.	Control room advise equipment is offline. Chief engineer breaks containment while equipment operational		Incorrect indication exists at the equipment that it is not operational due to faulty sensor. Chief engineer breaks containment while equipment operational		
			Chief engineer is not trained on the equipment they begin to repair. Repair is not adequately completed resulting in break in containment/ excessive operating temperatures	The chief engineer has worked				

11	**Chief engineer repairs equipment but does not complete/ implement the repair correctly (H1-3)**	Chief engineer is not informed of the specific requirements of the manufacturer due to information overload of manuals/ data on the machine.	Chief engineer takes a reading of a hot surface incorrectly and insulates/ places lagging in the wrong location. Hot surface remains exposed Chief engineer unaware of how to apply the manufacturer guidelines when checking equipment (i.e. bolts on the fuel supply pipework) due to a lack of qualification/ competence.	on similar engines before and believe he/she knows the manufacturer requirements. In fact the requirements are different/ have been updated, resulting in a misinterpretation of the requirements.		
12	**Chief engineer starts repairing equipment before making necessary preparations (H1-3)**		Arrival of other required personnel taking too long so chief engineer decides to begin the repair due to a lack of knowledge of the risks.		Chief engineer does not check if the equipment is isolated/ shutdown and begins the repair due to excessive work pressures.	Chief engineer believes equipment is isolated/ shutdown and due to work pressures, begins the repair.
13	**Chief engineer starts repair, but doesn't complete when faulty equipment is present (H1-3)**	Chief engineer does not have the correct tools or replacement parts to complete the job, therefore the repair is stopped before the fault is rectified.	Chief engineer begins the repair but comes up against a repair process he/ she is unfamiliar with and stops mid way through.			An emergency elsewhere takes the chief engineer away from the repair which has been started, meaning the fault is not rectified.
14	**Chief engineer doesn't shutdown the engine when exposed hot surfaces exist (H1-3)**		Chief engineer is aware of exposed hot surfaces (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. unacceptable pressure in fuel supply pipework, excessive vibration which could cause an imminent rupture), meaning no shutdown action is taken.		Chief engineer unaware of exposed hot surfaces as there are no sensors to reveal their presence therefore hot surfaces remain exposed.	Chief engineer is aware of exposed hot surfaces but this is taken as normal, therefore engines remain operational and exposed hot surfaces remain in place.
15	**Chief engineer doesn't shutdown the engine when strain on the engine components exceed design threshold (H2-3)**		Chief engineer is unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces. Training inadequate, therefore engine is not shutdown the moments before a hazard is realised.		No sensors are in place to provide the chief engineer information on the system operating condition (i.e. excessive fuel supply pressure, vibration etc.) in which a decision can be made to shutdown the engine to prevent the hazards H-1 to H-3.	
16	**Chief engineer shuts down the engine and does not immediately reduce load on other engines which become temporarily overloaded (H-1, H-2)**		Chief engineer is unaware of the design loads which could be generated elsewhere by shutting down the engine. Training inadequate, therefore engine is shutdown causing a hazard to be realised elsewhere.		No warnings are in place to advise on the impact of the decision to shutdown the engine on the remainder of the system, therefore action is taken with no knowledge of the effect.	
17	**Chief engineer shuts down the engine too late when a fuel/ lube oil release exists (H2-3)**				Response time of sensors showing excessive conditions are not designed to provide a fast response alarm. No sensors in place to advise chief engineer of leak of oil, therefore shutdown relies on CCTV footage check or word from the ER.	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability. Engine shutdown buttons are not easily accessible, delaying the time taken to shutdown the engine.
18	**Chief engineer doesn't shutdown the engine fast enough when exposed hot surfaces exist (H1-3)**				Response time of sensors showing exposed hot surfaces are not designed to provide a fast response alarm.	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability. Engine shutdown buttons are not easily accessible, delaying the time taken to shutdown the engine.
19	**Chief engineer doesn't shutdown the fuel supply when strain on the components exceed design threshold (H2-3)**		Chief engineer is unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces. Training inadequate, therefore fuel supply is not shutdown the moments before a hazard is realised.	Chief engineer has seen the threshold be exceeded before without rupture. Complacency dictates decision making rather than value of threshold exceedance.	No sensors are in place to provide the engineer information on the system operating condition (i.e. excessive fuel supply pressure, vibration etc.) in which a decision can be made to shutdown the engine to prevent the hazards H-1 to H-3.	Manual valve seized shut due to lack of use.
20	**Chief engineer shuts down the fuel supply too late when a fuel/ lube oil release exists (H2-3)**		Engine shutdown does not automatically stop supply of fuel to that engine. Chief engineer unaware of fuel continually being sent to the engine which has been shutdown due to a leak.	Chief engineer incorrectly assumes an engineer will tend to the problem.	No sensors are in place to provide the chief engineer information on the system operating condition (i.e. low fuel supply pressure indicating a leak), therefore the leak continues until CCTV/ inspection reveals failure	

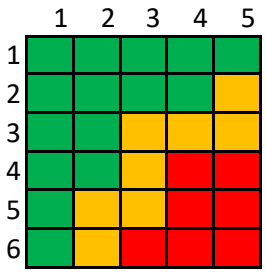
21	**Chief engineer doesn't release the water mist when exposed hot surfaces exist and oil mist in the atmosphere is detected/suspected (H-1)**		Chief engineer unaware that release of the deluge could potentially prevent an ignition. The assumption is prevalent that it should not be used until a fire breaks out.		Chief engineer is unaware that the combination of exposed hot surfaces and oil leak presents a high threat of fire.	Chief engineer is unaware of exposed hot surfaces as no sensors are in place to detect them.	Fire in the room damages equipment resulting in incomplete control action, therefore hot surfaces remain in place elsewhere which could cause further escalation.
					Chief engineer is unaware that the combination of exposed hot surfaces and imminent oil leak presents a high threat of fire.	Chief engineer is unaware of an imminent oil leak. Chief engineer is unaware of oil leak in the room.	Valve seized shut due to lack of use.
22	**Chief engineer releases the water mist too late when leak exists (H-1).**	Chief engineer prevents the release of the water mist system as they believe the alarms indicating oil leak are false alarms. Water mist only released when further alarms are received.					Water mist release mechanism has been inhibited during maintenance and not brought back online.
23	**Chief engineer releases the water mist too late when exposed hot surface exists (H-1)**	Chief engineer prevents the release of the water mist system as they believe the alarms indicating exposed hot surfaces are false alarms. Water mist only released when further alarms are received.					Water mist release mechanism has been inhibited during maintenance and not brought back online.
24	**Chief engineer stops the water mist too soon when exposed hot surfaces have existed and oil mist in the atmosphere is detected/suspected (H-1)**			Chief engineer believes the deluge will have completed it's job and switches it off, despite the hot surface remaining in place.			
25	**Chief engineer not writing a maintenance procedure results in no/ inconsistent maintenance leading to H1-3.**	Chief engineer has no documentation on what equipment is on the ship therefore cant write a maintenance procedure. Company has no requirement for equipment posing a risk of H1-3 to have a procedure for maintenance.	Chief engineer does not realise it is his/ her responsibility to write and implement the maintenance procedure.	Chief engineer incorrectly assumes a maintenance procedure is already in place.		Engineers are in the habit of maintaining equipment without a procedure therefore do not request a procedure from the chief engineer.	
26	**Chief engineer not writing a maintenance procedure results in engineers carrying out repair/ inspection without formal procedure resulting in H2-3.**			Chief engineer incorrectly assumes engineers will know how to carry out a repair.			
27	**Chief engineer provides a maintenance procedure which is not adequate to ensure prevention of H1-3.**	Chief engineer has no documentation on what equipment is on the ship therefore writes up an inaccurate maintenance procedure.	Chief engineer makes incorrect assumptions on what equipment is present and writes up the procedure based on this.	Chief engineer believes the maintenance procedure is complete and covers all necessary steps to prevent H1-3.		Engineers are aware of shortcomings in the procedure but find workarounds rather than report the required change to the chief engineer.	
28	**Chief engineer does not read maintenance report therefore does not know about required repairs (H1-3)**	Chief engineer does not know the maintenance report is available for review.	Chief engineer does not place importance on reading the repair/ maintenance reports.				Chief engineer does not have available time to read the maintenance reports due to excessive workload.
29	**Chief engineer reads the report but doesn't understand the results (H1-3)**	The content of the report is not clear and concise.	The chief engineer does not have the training on the specifics the maintenance report details.				
30	**Chief engineer reads the report too late meaning by the time the repair is placed in the work order a failure has already occurred (H1-3)**	Urgent action is required from the maintenance report but this is not communicated to the chief engineer.					Chief engineer does not have available time to read the maintenance reports due to excessive workload.
31	**Chief engineer does not authorise engineer competence resulting in engineers conducting work above their competence level (H1-3)**	Company has no requirement to measure competence of engineering staff.		No record of competence is maintained meaning the chief engineer makes assumptions of individual competence.			Lack of staffing/ time pressures/ urgent repair means an engineer has to conduct maintenance/ repair beyond their authorised competence.
32	**Chief engineer authorises competence of an engineer who does not have competence for specific procedures relating to H1-3.**	Chief engineer does not have a requirements specification for competence to measure against.		Chief engineer assumes due to competence in other areas, the engineer will be competent in adjacent areas of engineering.			Time pressures/ staff shortages force an authorisation of competence above the reality.

ID-UCA	UCA	ID-CF	Causal factors	ID-FR	Functional requirements	UCA Category	CF Category	Relevant barriers	Signals and their requirements	Hazard (Oil Leak[OL]/ Hot Surface [HS])	Previous occurrence in Incident/ Accident (Y/N) + incident ref	Barrier Effectiveness	Criticality	Magnitude of risk reduction
1	Chief engineer does not detect loss of integrity during inspection (H1-3)	1.1	Engineer asks for second opinion on damaged/ fatigued equipment but advises the chief engineer to check the wrong equipment.	1.1.1	Equipment in the ER which poses a risk of H1-3 shall be clearly and easily identifiable.	Detection/inspection including reporting	Maintenance and operation procedures	Hot box/ fuel supply pipework inspection/ maintenance procedure. Hot surface inspection procedure.	ER audit/ inspection of equipment tagging/ identification.	OL + HS		4	3	12
				1.1.2	Equipment under investigation/ where repair is required shall be clearly tagged.				Audit of engineer awareness of tagging/ marking for specific tasks and how to use them. Audit of on board availability of tags. Audit of embracing of maintenance management system.	OL + HS	(Y) - Le Boreal	4	4	16
		1.2	ECR advises on damaged/ fatigued equipment but advises the chief engineer to check the wrong equipment.	1.2.1	Equipment in the ER which poses a risk of H1-3 shall be clearly and easily identifiable.				ER audit/ inspection of equipment tagging/ identification.	OL + HS		4	3	12
				1.2.2	Equipment under investigation/ where repair is required shall be clearly tagged.				Audit of engineer awareness of tagging/ marking for specific tasks and how to use them. Audit of on board availability of tags. Audit of embracing of maintenance management system.	OL + HS	(Y) - Le Boreal	4	4	16
		1.3	Chief engineer is not aware of what to look for/ what the signs are of loss of integrity due to lack of skills/ knowledge.	1.3.1	Chief engineers shall be able to recognise hot box and fuel supply pipework/ engine loss of integrity which can lead to H2-3.		Knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence.	OL + HS		4	2	8
		1.4	Chief engineer does not believe it is his/ her responsibility to look for loss of integrity.	1.4.1	Chief engineer shall be aware fire prevention is everyone's responsibility regardless of seniority when there is a risk of H2-3.		Knowledge (training/ competence)	Enforcement of responsibilty	Audit of process including actions in hypothetical situations.	OL + HS	(Y) - MV Zenith	5	4	20
		2.1	Manufacturer specific guidelines are not provided to verify equipment against.	2.1.1	Manufacturer guidelines shall be available to all engineering staff.		Maintenance and operation procedures	Hot box/ fuel supply pipework inspection/ maintenance procedure.	Audit of chief engineer awareness of manufacturer guidelines. Audit of on board availability of manufacturer guidelines. Audit of embracing of maintenance management system.	OL		4	2	8
2	Chief engineer does not detect incorrect implementation of equipment as per manufacturer guidelines during inspection (H2-3)	2.2	Chief engineer has worked with similar equipment and believes the set up should be the same, but in fact the manufacturer recommends some differences.	2.2.1	Staff shall follow the requirements of the equipment manufacturer regardless of familiarity with similar equipment.	Detection/inspection including reporting	Maintenance and operation procedures	Hot box/ fuel supply pipework inspection/ maintenance procedure.	Audit of chief engineer awareness of manufacturer guidelines. Audit of on board availability of manufacturer guidelines. Audit of embracing of maintenance management system.	OL		4	2	8
		2.3	The tools available to the chief engineer are insufficient to detect integrity loss of the fuel supply pipework i.e. no torque wrench to verify torque level of the bolts.	2.3.1	Specific tools shall be available where manufacturer specifications require such tools to prevent H2-3.		Maintenance and operation procedures	Tooling and spares procedure	Audit of engineer awareness of tools for specific tasks and how to use them. Audit of on board availability of tools. Audit of embracing of maintenance management system.	OL	(Y) - Splendour of the Seas, Accident Event 190434	3	4	12
3	Chief engineer interferers with equipment and doesn't return to its original condition during inspection (H1-3)	3.1	Chief engineer does not have the training/ skillset to adequately understand the impact of interfering with equipment to get a closer inspection, resulting in continued hot surface exposure, or damaged/ fatigued equipment.	3.1.1	Chief engineer shall be capable of returning equipment back into service in a safe state to prevent H1-3.	Maintenance / repair	Knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS	(Y) - Splendour of the Seas, Accident Event 207584	4	5	20
4	Chief engineer inspects equipment too late to find damaged/ degraded equipment (H1-3)	4.1	Engineer reports damaged equipment which could result in H1-3 but the chief engineer deems it unimportant and dismisses the information.	4.1.1	Chief engineer should be aware of the threat posed by H1-3 to provide priority to such information.	Detection/inspection including reporting	Knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS		4	2	8
		4.2	Engineers report damaged equipment which could result in H1-3 to chief engineer but the chief engineer is too busy to address the concern.	4.2.1	Staffing and priorities shall allow for inspection to take place when this relates to H1-3.		Resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
5	Chief engineer does not complete inspection when hot surfaces or damaged/ degraded equipment present (H1-3)	5.1	Chief engineer does not have training on how to complete a check and therefore does not complete it.	5.1.1	Chief engineer shall be aware of what an unsafe condition of equipment is which can lead to H1-3 and how to recognise this	Detection/inspection including reporting	Knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence.	OL + HS		4	3	12
		5.2	Chief engineer believes the inspection is complete but is unaware of additional checks which are required.	5.2.1	Instructions relating to inspection of equipment posing a risk of H1-3 shall be specific and complete.		Knowledge (training/ competence)	Hot box/ fuel supply pipework inspection/ maintenance procedure. Hot surface inspection procedure.	Audit of contents of maintenance routines. Audit of chief engineer compliance with the routines. Audit of embracing of maintenance management system.	OL + HS		3	3	9
6	Chief engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H1-3)	6.1	Chief engineer is not trained in report writing and fails to communicate the loss of integrity to the hierarchy meaning management are unaware of fatigue to the hot box, fatigue of the fuel supply system, or hot surfaces.	6.1.1	Chief engineer shall be aware of how to present clear and concise reports relating to work or equipment posing a risk of H1-3.	Detection/inspection including reporting	Knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS		4	3	12
				6.1.2	Chief engineer shall be aware of what is a safety critical maintenance requirement in preventing H1-3.			Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS		4	3	12
		6.2	Chief engineer is instructed of a required upgrade. The work is carried out in an uncontrolled/ undocumented way. Company is unaware of what equipment is upgraded/ what is outstanding.	6.2.1	Repair/ upgrade work which breaks containment or replaces a part where this creates a risk of H1-3 shall have the change logged.		Maintenance and operation procedures	Change management system	Audit of report writing compliance. Audit of embracing of maintenance management system.	OL + HS		3	3	9
				6.2.2	Staffing and priorities shall allow for report writing to take place when this relates to potential precursors to hazards leading to H1-3.			Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
		6.3	Chief engineer inspects the equipment, registers the loss of integrity of the hot box but is not aware that this presents the risk of H-3, therefore does not take or recommend action to fix.	6.3.1	Chief engineer shall be familiar with what can lead to a hazard with respect to the hot box, leading to H-3.		Knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence.	OL	(Y) - MV Zenith, Splendour of the Seas	4	5	20
		6.4	Chief engineer inspects the equipment, registers the loss of integrity of the fuel supply pipework but is not aware that this presents the risk of H-2, therefore does not take or recommend action to fix.	6.4.1	Chief engineer shall be familiar with what can lead to a hazard with respect to the fuel supply pipework, leading to H-2.		Knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence.	OL	(Y) - MV Zenith	4	5	20
7	Chief engineer report on integrity is too vague when a specific repair is required (H1-3)	7.1	Chief engineer is not trained in report writing and fails to communicate the specific equipment requiring repair, leading to confusion when the repair is then to be completed. Inadequate repair completed due to vague report, resulting in remaining fatigue of the hot box, fatigue of the fuel supply system, or hot surfaces.	7.1.1	Chief engineer shall be aware of how to provide clear and concise reports relating to work or equipment posing a risk of H1-3.	Detection/inspection including reporting	Knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS		4	3	12
8	Chief engineer reports on integrity too late when damaged/ degraded equipment remains in place (H1-3)	8.1	Chief engineer workload too busy that no time is dedicated to writing the report and the loss of integrity is reported too late.	8.1.1	Staffing and priorities shall allow for report writing to take place when this relates to H1-3.	Detection/inspection including reporting	Resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
9	Chief engineer doesn't repair equipment when faulty equipment present (H1-3)	9.1	Company is made aware of a vulnerability associated with a piece of process equipment (i.e. fuel supply connection vulnerability to leak). Instruction is provided down the chain of command to the chief engineer to implement the solution but this is not implemented due to a perceived low priority status.	9.1.1	When equipment vulnerability can lead to H1-3 and a known mitigating factor is provided, this shall be implemented.	Maintenance / repair	Maintenance and operation procedures	Equipment Maintenance/ Manufacturer Compliance Procedure	Audit of procedures and review of maintenance logs can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS		4	2	8
		9.2	Faulty condition (i.e. seal gaps in the hot box) becomes normalised. No repair/ replacement carried out.	9.2.1	Chief engineer shall be aware of what an unsafe condition of equipment is which can lead to H1-3.		Normalisation of risk	Training/ Competence Management System	Audit of Competence.	OL + HS		4	5	20
				9.2.2	Chief engineer shall be free to question company about suitability of situations which may lead to H1-3, even if it has 'always been this way'.			Open forum of communication	Audit of process including actions in hypothetical situations.	OL + HS	(Y) - MV Zenith, Sea Gale, Splendour of the Seas	5	4	20
10	Chief engineer begins repair during operation state (i.e. pressurised) (H2-3)	10.1	No indication exists at the equipment that it is operational. Chief engineer breaks containment while equipment operational	10.1.1	Design of safety critical equipment shall distinctly indicate (passively and actively) its operational status to prevent H2-3.	Maintenance / repair	Knowledge (inadequate feedback)	Visual indicator (e.g. engine operational)	Indicator reading in real time.	OL	(Y) - Le Boreal	3	5	15
		10.2	Chief engineer decides to implement a fix while conducting an impromptu ER inspection. It is perceived as a quick fix so normal protocols are not followed.	10.2.1	All work which involves breaking containment shall follow on board rules and procedures to avoid H2-3.		Knowledge (inadequate feedback)	Permit to work procedure	Audit of procedural compliance. Alarm required if audit shows poor practice against permit to work instructions.	OL		4	3	12
		10.3	Control room advise equipment is offline. Chief engineer breaks containment while equipment operational	10.3.1	Sensors indicating operational status shall have a reliability up time of 99%-99.9% (SIL2) to prevent H2-3.		Knowledge (inadequate feedback)	Safety critical equipment operational procedure	IEC61508/ proven in use audits can be used to signal performance. Audit of embracing of maintenance management system.	OL		4	3	12
				10.3.2	Where conflict between feedback exists, work shall stop pending further investigation to prevent H2-3.			Permit to work procedure	Communication channel between control room and engineer must exist, with engineers empowered to stop the job. Audit of embracing of maintenance management system.	OL		4	3	12
		10.4	Incorrect indication exists at the equipment that it is not operational due to faulty sensor. Chief engineer breaks containment while equipment operational	10.4.1	Sensors indicating operational status shall have a reliability up time of 99%-99.9% (SIL2) to prevent H2-3.		Knowledge (inadequate feedback)	Safety critical equipment operational procedure	IEC61508/ proven in use audits can be used to signal performance. Audit of embracing of maintenance management system.	OL		4	2	8
		11.1	Chief engineer is not informed of the specific requirements of the manufacturer due to information overload of manuals/ data on the machine.	11.1.1	Instructions on hazard prevention of H1-3 shall be specific and clear.		Maintenance and operation procedures	Generation of task specific, clear instruction.	Audit of capability and task instruction.	OL + HS	(Y) - Carnival Triumph	4	5	20
		11.2	Chief engineer is not trained on the equipment they begin to repair. Repair is not adequately completed resulting in break in containment/ excessive operating temperatures	11.2.1	Ship chief engineer shall be familiar with equipment which poses a risk of H1-3.		Knowledge (training/ competence)	Training/ Competence Management System	Audits should be used to monitor engineers have the necessary training.	OL + HS	(Y) - Le Boreal	4	5	20
11	Chief engineer repairs equipment but does not complete/ implement the repair correctly (H1-3)	11.3	Chief engineer takes a reading of a hot surface incorrectly and insulates/ places lagging in the wrong location. Hot surface remains exposed	11.3.1	During inspection relating to the prevention of H-1, chief engineer shall be able to verify the exact location of the hot surface.	Maintenance / repair	Knowledge (training/ competence)	Hot surface inspection procedure	Audit of performance can be the signal of compliance.	HS		4	3	12
				11.3.2	Chief engineer shall be able to use the equipment appropriately in carrying out this inspection H-1.			Training/ Competence Management System	Audits should be used to monitor engineers have the necessary training.	HS		4	3	12
		11.4	Chief engineer unaware of how to apply the manufacturer guidelines when checking equipment (i.e. bolts on the fuel supply pipework) due to a lack of qualification/ competence.	11.4.1	Chief engineer shall be familiar with equipment on board where a risk of H1-3 exists and trained on all potential actions required to be made on that equipment.		Knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence. Alarm when equipment on board which an engineer is unable to address.	OL + HS		4	2	8
		11.5	The chief engineer has worked on similar engines before and believe he/she knows the manufacturer requirements. In fact the requirements are different/ have been updated, resulting in a misinterpretation of the requirements.	11.4.2	Actions shall always be based on the manufacturer guidance, regardless of experience level and experience on other equipment where a risk of H1-3 exists.		Knowledge (training/ competence)	Maintenance procedure being based on manufacturer guidance	Audit of procedural compliance. Alarm required if audit shows poor practice against what is specified by manufacturer.	OL + HS	(Y) - Carnival Triumph, Accident Event 275191	4	5	20
12	Chief engineer starts repairing equipment before making necessary preparations (H1-3)	12.1	Arrival of other required personnel taking too long so chief engineer decides to begin the repair due to a lack of knowledge of the risks.	12.1.1	Work shall not begin until all required personnel are present to avoid H-2.	Maintenance / repair	Knowledge (training/ competence)	Permit to work procedure	Audit of procedures can be the signal of performance.	OL	(Y) - Le Boreal, Freedom of the Seas, Audit Safety Event 188275, 191114, Accident Event 268034, 218465	4	4	16
				12.1.2	Chief engineer shall be aware of what can lead to an unsafe condition of equipment leading to H1-3 during repair and the reasons for the requirements within the permit to work.			Training/ Competence Management System	Audit of Competence.	OL + HS		4	5	20
		12.3	Chief engineer does not check if the equipment is isolated/ shutdown and begins the repair due to excessive work pressures.	12.3.1	Staffing shall allow for repairs of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.		Knowledge (training/ competence)	Adequate staffing and task allocation	Audit of performance can be the signal of compliance.	OL + HS		4	3	12
		12.4	Chief engineer believes equipment is isolated/ shutdown and due to work pressures, begins the repair.	12.4.1	Staffing shall allow for repairs of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.		Knowledge (training/ competence)	Adequate staffing and task allocation	Audit of performance can be the signal of compliance.	OL + HS		4	3	12
13	Chief engineer starts repair, but doesn't complete when faulty equipment is present (H1-3)	13.1	Chief engineer does not have the correct tools or replacement parts to complete the job, therefore the repair is stopped before the fault is rectified.	13.1.1	Inventories shall be kept stocked with spares holding to allow for unforeseen circumstances and repair work required while at sea to equipment posing a risk of H1-3 (o-rings, bolts, fittings, lagging).	Maintenance / repair	Maintenance and operation procedures	Tooling and spares procedure	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS	(Y) - Carnival Triumph, Audit Safety Event 273012, Accident Event 190434	4	4	16
		13.2	Chief engineer begins the repair but comes up against a repair process he/ she is unfamiliar with and stops mid way through.	13.2.1	Repair shall only be started when Chief engineer has availability to complete it, with fire prevention tasks preventing H1-3 taking priority, unless otherwise instructed ECR.			Adequate staffing and task allocation	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS		4	2	8
				13.2.2	Chief engineer shall be familiar with equipment on board which poses a risk of H1-3 and trained on all potential actions required to be made on that equipment.		Knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence. Alarm when equipment on board which an engineer is unable to address.	OL + HS		4	3	12
				13.2.3	If a job remains unfinished, equipment shall be made safe and records shall be maintained to show the job is unfinished. Unfinished repair shall be marked accordingly (e.g. lockout-tagout / LOTO)			Permit to work procedure	Audit of procedures can be the signal of performance.	OL + HS		4	2	8
		13.3	An emergency elsewhere takes the chief engineer away from the repair which has been started, meaning the fault is not rectified.	13.3.1	Equipment shall not be reintroduced until fault which can lead to H1-3 is rectified.		Maintenance and operation procedures	Hazardous equipment operation procedure	Audit of procedures can be the signal of performance. Indicator showing fault which requires acknowledgement	OL + HS		4	3	12
				13.3.2	Staffing shall allow for planned maintenance of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.			Adequate staffing and task allocation	Audit of performance can be the signal of compliance.	OL + HS		4	2	8
14	Chief engineer doesn't shutdown, stop or remove the engine from service when exposed hot surfaces exist (H1-3)	14.1	Chief engineer is aware of exposed hot surfaces (which are taken as normal), but is unaware of other risk factors which would require an engine shutdown (i.e. unacceptable pressure in fuel supply pipework, excessive vibration which could cause an imminent rupture), meaning no shutdown action is taken.	14.1.1	System shall be able to detect and alarm to pressure in excess of the manufacturer specification in the fuel supply system, and vibration in excess of the manufacturer specification which could indicate the presence of or potential for H2-3.	Manual action / automation / fire prevention	Knowledge (inadequate feedback)	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - MV Zenith, Splendour of the Seas, Accident Event 207960, 231717, 224659, Incident Event 202364	3	5	15
				14.1.2	System to detect oil leaks in the hot box and the engine room shall be provided (H2-3).			Safety Instrumented System	Diagnostics showing sensor health status.	OL		3	5	15
				14.1.3	Chief engineer shall be aware of precursors which can lead to H2-3 and when shutdown of the engine should take place when coupled with H-1.			Engine operation procedure	Audits should be used to monitor engineers have the necessary training.	OL + HS		4	5	20
		14.2	Chief engineer unaware of exposed hot surfaces as there are no sensors to reveal their presence therefore hot surfaces remain exposed.	14.2.1	System shall be able to provide alarms in high risk areas to the presence of H-1.		Knowledge (inadequate feedback)	Safety Instrumented System	Thermal sensors with diagnostics showing sensor health status.	HS	(Y) - Le Boreal, MV Zenith, Splendour of the Seas, Carnival Triumph. Accident Event 269956	3	5	15
				14.2.2	System shall be in place to flag up and record presence of H-1.			Hot surface inspection procedure	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	HS		4	5	20

		14.3	Chief engineer is aware of exposed hot surfaces but this is taken as normal, therefore engines remain operational and exposed hot surfaces remain in place.	14.3.1	Chief engineer shall be aware of the requirements of SOLAS regarding the presence of H-1.		Knowledge (training/ competence)	SOLAS/ safety training	Audit of attitude and compliance.	HS	Incident Event 202364	5	5	25
15	Chief engineer doesn't shutdown or stop the engine when strain on the engine components exceed design threshold (H2-3)	15.1	Chief engineer is unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces. Training inadequate, therefore engine is not shutdown the moments before a hazard is realised.	15.1.1	Chief engineer shall be aware of precursors to engine failure which can lead to H1-3 and when shutdown of the engine should take place.	Manual action / automation / fire prevention	Knowledge (training/ competence)	Training/ Competence Management System.	Audits should be used to monitor engineers have the necessary training.	OL	(Y) - Sea Gale, Accident Event 210991, 222338	4	5	20
		15.2	No sensors are in place to provide the chief engineer information on the system operating condition (i.e. excessive fuel supply pressure, vibration etc.) in which a decision can be made to shutdown the engine to prevent the hazards H-1 to H-3.	15.2.1	System shall be capable of detecting a potentially unsafe operating condition for fuel/ oil pressure, temperature, flow rate, vibration and engine power output/ load which can lead to H2-3.		Knowledge (inadequate feedback)	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Splendour of the Seas, Carnival Triumph, Accident Event 198060, 210991, 222338, 192706	3	5	15
16	Chief engineer shuts down the engine and does not immediately reduce load on other engines which become temporarily overloaded (H-1, H-2)	16.1	Chief engineer is are unaware of the design loads which could be generated elsewhere by shutting down the engine. Training inadequate, therefore engine is shutdown causing a hazard to be realised elsewhere.	16.1.1	Chief engineer shall be aware of the impact of shutting down an engine on other systems where this could lead to increased risk of H2-3 elsewhere.		Knowledge (training/ competence)	Training/ Competence Management System.	Audits should be used to monitor engineers have the necessary training.	OL		4	3	12
		16.2	No warnings are in place to advise on the impact of the decision to shutdown the engine on the remainder of the system, therefore action is taken with no knowledge of the effect.	16.2.1	Where an engine is to be shutdown remotely, system should be in place to monitor and advise of the impact of shutdown (H2-3). Engine shutdown directly in the ER shall remain unaffected and is to be used in an emergency.	Manual action / automation / fire prevention	Knowledge (inadequate feedback)	Safety Instrumented System	Diagnostics showing sensor health status. Sensors produce an overall risk level which updates based on projections should a DG be shutdown. Health shall be monitored against manufacturer provided tolerances (i.e. pressure in the fuel supply system shall not exceed xbar/psi)	OL	(Y) - Accident Event 210991, 222338	3	5	15
17	Chief engineer shuts down the engine too late when a fuel/ lube oil release exists (H2-3)	17.1	Response time of sensors showing excessive conditions are not designed to provide a fast response alarm.	17.1.1	Any sensors which are in place to detect anomalies in engine conditions which could lead to a H-2 (fuel/ oil pressure, temperature, flow) shall be fast response and shall present the alarm and reading to engineers in real time.		Knowledge (inadequate feedback)	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Accident Event 192706	3	5	15
		17.2	No sensors in place to advise chief engineer of leak of oil, therefore shutdown relies on CCTV footage check or word from the ER.	17.2.1	System to detect oil leaks in the hot box and the engine room shall be provided (H2-3).	Manual action / automation / fire prevention	Knowledge (inadequate feedback)	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Le Boreal, MV Zenith, Splendour of the Seas, Accident Event 207960, 231717, 224659, Incident Event 202364	3	5	15
		17.3	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.	17.3.1	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.		Inadequate hardware design	Emergency shutdown Procedure	Function testing of the shutdown valves at regular intervals. Function testing of fuel pump shutdown. Results of this testing can provide a reliability value which can be taken into account on the overall risk ranking.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph	2	5	10
		17.4	Engine shutdown buttons are not easily accessible, delaying the time taken to shutdown the engine.	17.4.1	Access to the emergency push buttons for both engine shutdown and fuel supply shutdown shall be accessible from multiple locations/ directions from the engine to prevent or mitigate H2-3.		Inadequate hardware design	Emergency shutdown Procedure	Design review of the locations. Maintenance of the pushbuttons to ensure safe operation.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph, Audit Safety Event 191114	2	4	8
18	Chief engineer doesn't shutdown the engine fast enough when exposed hot surfaces exist (H1-3)	18.1	Response time of sensors showing exposed hot surfaces are not designed to provide a fast response alarm.	18.1.1	Any sensors which are in place to detect H-1 shall be fast response and shall present the alarm to engineers in real time.		Knowledge (inadequate feedback)	Safety Instrumented System	Diagnostics showing sensor health status.	HS		3	3	9
		18.2	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.	18.2.1	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.	Manual action / automation / fire prevention	Inadequate hardware design	Emergency shutdown Procedure	Function testing of the shutdown valves at regular intervals. Function testing of fuel pump shutdown. Results of this testing can provide a reliability value which can be taken into account on the overall risk ranking.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph	2	5	10
		18.3	Engine shutdown buttons are not easily accessible, delaying the time taken to shutdown the engine.	18.3.1	Access to the emergency push buttons for both engine shutdown and fuel supply shutdown shall be accessible from multiple locations/ directions from the engine to prevent or mitigate H2-3.		Inadequate hardware design	Emergency shutdown Procedure	Design review of the locations. Maintenance of the pushbuttons to ensure safe operation.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph, Audit Safety Event 191114	2	4	8
		19.1	Chief engineer is unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces. Training inadequate, therefore fuel supply is not shutdown the moments before a hazard is realised.	19.1.1	Chief engineer shall be aware of precursors which can lead to H-2, and when shutdown of the supply should take place.		Knowledge (training/ competence)	Training procedure	Audits should be used to monitor chief engineers have the necessary training.	OL	(Y) - Splendour of the Seas, Accident Event 210991, 222338	4	5	20
19	Chief engineer doesn't shutdown or stop the fuel supply when strain on the components exceed design threshold (H2-3)	19.2	Chief engineer has seen the threshold be exceeded before without rupture. Complacency dictates decision making rather than value of threshold exceedance.	19.2.1	Chief engineer shall take action when an unsafe conditions are presented, regardless of historical experiences/ near misses.	Manual action / automation / fire prevention	Knowledge (training/ competence)	Training procedure	Audits should be used to monitor chief engineers reliance on past experiences vs operator manuals/ guidance.	OL		4	3	12
		19.3	No sensors are in place to provide the chief engineer information on the system operating condition (i.e. excessive fuel supply pressure, vibration etc.) in which a decision can be made to shutdown the engine to prevent the hazards H-1 to H-3.	19.3.1	System shall be able to detect and alarm at the point a manufacturer stated operating condition is breached for fuel/ oil pressure, temperature, flow rate, vibration and engine power output/ load to prevent H-2.		Knowledge (inadequate feedback)	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Splendour of the Seas, Carnival Triumph, Accident Event 198060, 210991, 222338, 192706	3	5	15
		19.4	Manual valve seized shut due to lack of use.	19.4.1	Shut off valves used to prevent or mitigate H2-3 shall be subject to operation and inspection during maintenance as per manufacturer recommendation.		Maintenance and operation procedures	Physical barrier function test procedure	Audit of procedures and review of maintenance logs can be the signal of performance. Audit of embracing of maintenance management system.	OL	(Y) - Splendour of the Seas, Carnival Triumph, Accident Event 207612	4	5	20
		20.1	Engine shutdown does not automatically stop supply of fuel to that engine. Chief engineer unaware of fuel continually being sent to the engine which has been shutdown due to a leak.	20.1.1	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.		Knowledge (inadequate feedback)	Emergency shutdown procedure	Function testing of the shutdown valves at regular intervals. Function testing of fuel pump shutdown. Results of this testing can provide a reliability value which can be taken into account on the overall risk ranking.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph, Accident Event 224659	2	5	10
20	Chief engineer shuts down the fuel supply too late when a fuel/ lube oil release exists (H2-3)	20.2	Chief engineer incorrectly assumes an engineer will tend to the problem.	20.2.1	Where a risk of H2-3 exists, action shall immediately be taken to avoid the hazard. If action is delegated to another party, verification of status and completion shall be provided.	Manual action / automation / fire prevention	Maintenance and operation procedures	Emergency shutdown procedure	Audit of shutdown procedure & team communication	OL		4	3	12
		20.3	No sensors are in place to provide the chief engineer information on the system operating condition (i.e. low fuel supply pressure indicating a leak), therefore the leak continues until CCTV/ inspection reveals failure	20.3.1	System shall be capable of detecting pressure outwith manufacturer specification indicative of increased risk of H2-3 in the fuel supply pipework, and oil leaks shall be detectable in the hot box and in the ER (H2-3).		Knowledge (inadequate feedback)	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Splendour of the Seas, Accident Event 231717, 224659, Incident Event 202364	3	5	15
		21.1	Chief engineer unaware that release of the deluge could potentially prevent an ignition. The assumption is prevalent that it should not be used until a fire breaks out.	21.1.1	Chief engineer shall be aware of how to use the water mist system, and where it can assist in the elimination of H-1 when a leak or break in containment is likely/ has occurred.		Knowledge (training/ competence)	Training procedure/ Emergency procedure	Diagnostics showing sensor health status which can flag a potentially imminent break in containment/ or presence of fuel/ oil mist. Audit of engineer training and knowledge of water mist release.	HS	(Y) - Accident Event 224659, Incident Event 202364, Carnival Triumph, Splendour of the Seas [specifically referenced in the incident report that water mist release could have prevented the fire in the first place]	4	5	20
		21.2	Chief engineer is unaware that the combination of exposed hot surfaces and oil leak presents a high threat of fire.	21.2.1	Chief engineer shall be able to recognise the dangers associated with exposed hot surfaces (H-1) and presence of an oil leak (H2-3).		Knowledge (training/ competence)	Training/ Competence Management System. Alarm management procedure.	Audit of Competence. Diagnostics showing sensor health status which can flag a potentially imminent break in containment/ or presence of fuel/ oil mist. Audit of engineer training and knowledge of water mist release.	HS		4	3	12
		21.3	Chief engineer is unaware that the combination of exposed hot surfaces and imminent oil leak presents a high threat of fire.	21.3.1	Engineers shall be able to recognise the dangers associated with exposed hot surfaces (H-1) and the likelihood of imminent presence of an oil leak (H2-3).		Knowledge (training/ competence)	Training/ Competence Management System. Alarm management procedure.	Audit of Competence. Diagnostics showing sensor health status which can flag a potentially imminent break in containment/ or presence of fuel/ oil mist. Audit of engineer training and knowledge of water mist release.	HS		4	3	12
21	Chief engineer doesn't release the water mist when exposed hot surfaces exist and oil mist in the atmosphere is detected/suspected (H-1)	21.4	Chief engineer is unaware of exposed hot surfaces as no sensors are in place to detect them.	21.4.1	System shall be able to provide alarms in high risk areas of the presence of H-1.	Manual action / automation / fire prevention	Knowledge (inadequate feedback)	Safety Instrumented System	Diagnostics showing sensor health status.	HS	(Y) - Splendour of the Seas, Accident Event 269956	3	5	15
				21.4.2	Inspection shall be conducted to flag up and record any risk of H-1.			Hot surface inspection procedure	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	HS		4	5	20
		21.5	Chief engineer is unaware of an imminent oil leak.	21.5.1	System shall be in place to alarm to an imminent break in containment (H2-3) to remove the risk of H-1.		Knowledge (inadequate feedback)	Emergency procedure	Diagnostics showing sensor health status which can flag a potentially imminent break in containment/ or presence of fuel/ oil mist. Audit of engineer training and knowledge of water mist release.	HS	(Y) - MV Zenith, Splendour of the Seas, Accident Event 207960, 231717, 224659, Incident Event 202364	4	5	20
		21.6	Chief engineer is unaware of oil leak in the room.	21.6.1	System shall be in place to alarm to an imminent break in containment (H2-3) to remove the risk of H-1.		Knowledge (inadequate feedback)	Safety Instrumented System	Diagnostics showing sensor health status.	HS	(Y) - MV Zenith, Splendour of the Seas, Accident Event 207960, 231717, 224659, Incident Event 202364	3	5	15
		21.7	Fire in the room damages equipment resulting in incomplete control action, therefore hot surfaces remain in place elsewhere which could cause further escalation.	21.7.1	Water mist system shall be able to continue operation in the event of a fire (H-1).		Knowledge (inadequate feedback)	Emergency shutdown Procedure	Audit of design.	HS	(Y) - Splendour of the Seas	2	4	8
				21.7.2	Chief engineer shall be aware of the requirement and how to release water mist system in the event of a fire if it is not already active.			Training procedure/ Emergency procedure	Audit of procedures can be the signal of performance.	HS		4	4	16
		21.8	Valve seized shut due to lack of use.	21.8.1	Water mist release valves used to prevent or mitigate H-1 shall be subject to operation and inspection during maintenance as per manufacturer recommendation.		Maintenance and operation procedures	Physical barrier function test procedure	Audit of procedures and review of maintenance logs can be the signal of performance. Audit of embracing of maintenance management system.	HS	(Y) - Accident Event 274465	4	5	20
22	Chief engineer releases the water mist too late when leak exists (H-1).	22.1	Chief engineer prevents the release of the water mist system as they believe the alarms indicating oil leak are false alarms. Water mist only released when further alarms are received.	22.1.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.	Alarm management, maintenance	Alarm management	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		2	2	4
		22.2	Water mist release mechanism has been inhibited during maintenance and not brought back online.	22.2.1	Upon completion of maintenance, all inhibits shall be removed.		Maintenance procedure	Audit of maintenance procedure	Audit of maintenance process	HS		2	2	4
23	Chief engineer releases the water mist too late when exposed hot surface exists (H-1)	23.1	Chief engineer prevents the release of the water mist system as they believe the alarms indicating oil leak are false alarms. Water mist only released when further alarms are received.	23.1.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.	Alarm management, maintenance	Alarm management	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		2	2	4
		23.2	Water mist release mechanism has been inhibited during maintenance and not brought back online.	23.2.1	Upon completion of maintenance, all inhibits shall be removed.		Maintenance procedure	Audit of maintenance procedure	Audit of maintenance process	HS		2	2	4
24	Chief engineer shuts down the water mist too soon when exposed hot surfaces have existed and oil mist in the atmosphere is detected/suspected (H-1)	24.1	Chief engineer believes the water mist will have completed it's job and switches it off, despite the hot surface remaining in place.	24.1.1	Chief engineer shall be aware of emergency response and on the factors to review in assuming a situation no longer poses a risk of H-1.	Manual action / automation / fire prevention	Knowledge (training/ competence)	Training procedure/ Emergency procedure	Audit of procedures can be the signal of performance.	HS	(Y) - Splendour of the Seas	4	5	20
25	Chief engineer not writing up a maintenance procedure results in no/ inconsistent maintenance leading to H1-3.	25.1	Chief engineer has no documentation on what equipment is on the ship therefore can't write a maintenance procedure.	25.1.1	Original manufacturer documentation pertaining to equipment on board shall be available at all times.	Maintenance / repair	Maintenance and operation procedures	Document control procedure	Audit of document control availability.	OL + HS		4	1	4
		25.2	Company has no requirement for equipment posing a risk of H1-3 to have a procedure for maintenance.	25.2.1	Where equipment poses a risk of H1-3, a planned maintenance procedure shall be implemented.		Maintenance and operation procedures	Maintenance process	Audit of procedures can be the signal of performance.	OL + HS		4	2	8
		25.3	Chief engineer does not realise it is his/ her responsibility to write and implement the maintenance procedure.	25.3.1	Roles and responsibilities shall be clearly documented and communicated.		Task allocation, communication	Specific and clear job roles and responsibilities	Audit of knowledge of job function	OL + HS		4	1	4
		25.4	Chief engineer incorrectly assumes a maintenance procedure is already in place.	25.4.1	Maintenance reports shall include reference to the procedure in which the task was completed against.		Maintenance and operation procedures	Maintenance process	Audit of procedures can be the signal of performance.	OL + HS		4	2	8
		25.5	Engineers are in the habit of maintaining equipment without a procedure therefore do not request a procedure from the chief engineer.	25.5.1	Where a process creates the risk of H1-3, a procedure shall be in place to safely complete the operation.		Maintenance and operation procedures	Maintenance process	Audit of procedures can be the signal of performance.	OL + HS		4	2	8
26	Chief engineer not writing up a maintenance procedure results in engineers carrying out repair/ inspection without formal procedure resulting in H1-3.	26.1	Chief engineer incorrectly assumes engineers will know how to carry out a repair.	26.1.1	Maintenance reports shall include reference to the procedure in which the task was completed against.	Maintenance / repair	Maintenance and operation procedures	Maintenance process	Audit of procedures can be the signal of performance.	OL + HS		4	2	8
		27.1	Chief engineer has no documentation on what equipment is on the ship therefore can't write a maintenance procedure.	27.1.1	Original manufacturer documentation pertaining to equipment on board shall be available at all times.		Maintenance and operation procedures	Document control procedure	Audit of document control availability.	OL + HS		4	1	4
		27.2		27.2.1	Maintenance procedures shall be based on the specific equipment on board, unique to the ship.		Maintenance and operation procedures	Maintenance process	Audit of maintenance procedures.	OL + HS		4	2	8
27	Chief engineer provides a maintenance procedure which is not adequate to ensure prevention of H1-3.	27.3	Chief engineer makes incorrect assumptions on what equipment is present and writes up the procedure based on this.	27.2.2	Any changes to equipment on board posing a risk of H1-3 shall be immediately reflected in the maintenance procedure.	Maintenance / repair	Maintenance and operation procedures	Maintenance process	Audit of maintenance procedures and change management.	OL + HS		4	2	8
		27.4	Chief engineer believes the maintenance procedure is complete and covers all necessary steps to prevent H1-3.	27.4.1	Maintenance procedures on equipment posing a risk of H1-3 shall also include all requirements of the manufacturer.		Maintenance and operation procedures	Hot box/ fuel supply pipework inspection/ maintenance procedure.	Audit of chief engineer awareness of manufacturer guidelines. Audit of on board availability of manufacturer guidelines. Audit of maintenance procedures.	OL + HS		4	1	4
		27.5	Engineers are aware of shortcomings in the procedure but find workarounds rather than report the required change to the chief engineer.	27.5.1	Deviations from the maintenance procedure shall be authorised by the chief engineer.		Maintenance and operation procedures	Hot box/ fuel supply pipework inspection/ maintenance procedure.	Audit of chief engineer awareness of manufacturer guidelines. Audit of application of maintenance procedures.	OL + HS		4	1	4
		28.1	Chief engineer does not know the maintenance report is available for review.	28.1.1	Chief engineer shall receive notification when maintenance reports are available for review.		Maintenance and operation procedures	Document control procedure	Audit of document control transparency/ communication.	OL + HS		4	1	4
28	Chief engineer does not read maintenance report therefore does not know about required repairs (H1-3)	28.2	Chief engineer does not place importance on reading the repair/ maintenance reports.	28.2.1	Chief engineer shall review and acknowledge maintenance reports when they are available.	Maintenance / repair	Maintenance and operation procedures	Document control procedure	Audit of document control transparency/ communication.	OL + HS		4	1	4
		28.3	Chief engineer does not have available time to read the maintenance reports due to excessive workload.	28.3.1	Staffing and priorities shall allow for maintenance report review to take place when this relates to H1-3.		Resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	2	8
29	Chief engineer reads the report but doesn't understand the results (H1-	29.1	The content of the report is not clear and concise.	29.1.1	Engineers shall be aware of how to present clear and concise reports relating to work or equipment posing a risk of H1-3.	Maintenance /	Training/ Competence Management System	Knowledge (training/ competence)	Audit of Competence and job knowledge.	OL + HS		4	3	12

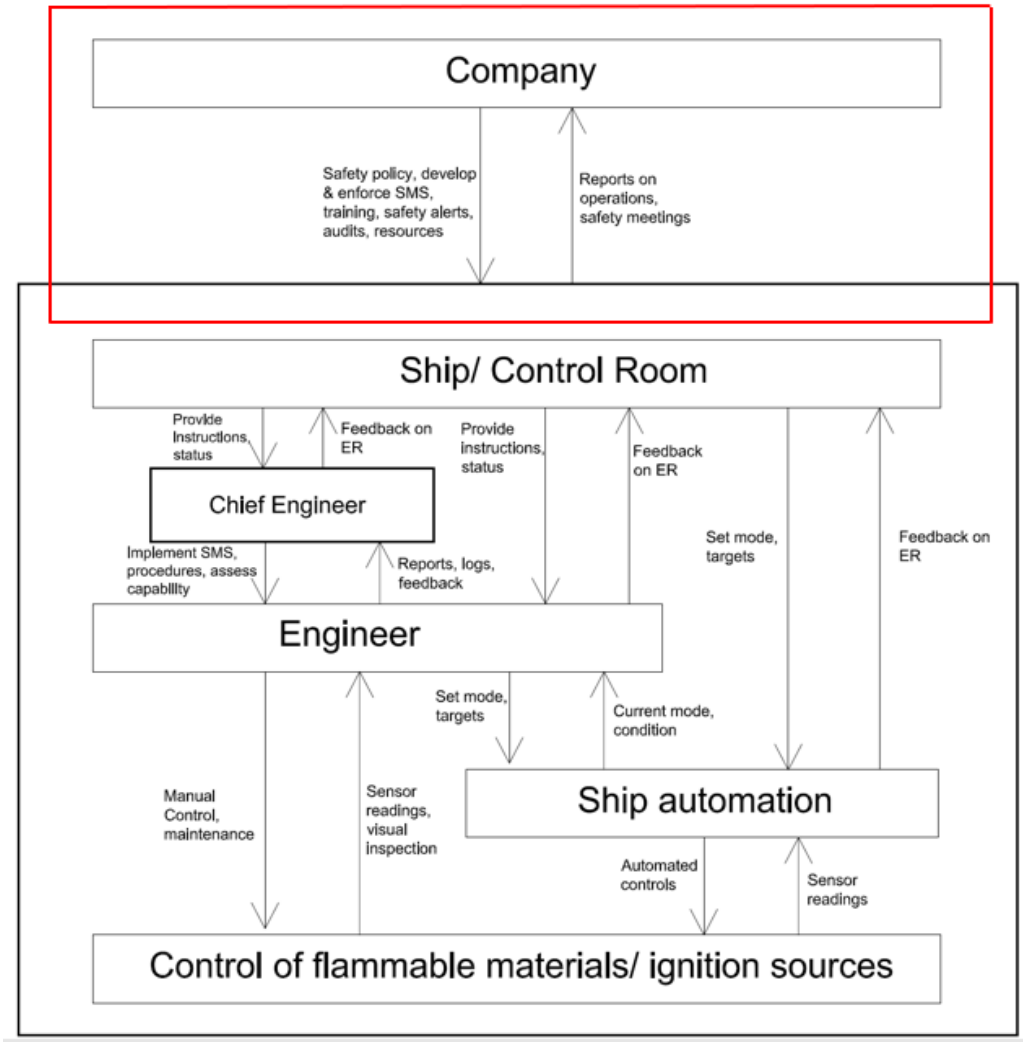
	3)	29.2	The chief engineer does not have the training on the specifics the maintenance report details.	29.2.1	Chief engineer shall be aware of maintenance and inspection requirements where equipment poses a risk of H1-3.	repair	Training/ Competence Management	Knowledge (training/ competence)	Audit of Competence and job knowledge.	OL + HS	4	3	12
30	Chief engineer reads the report too late meaning by the time the repair is placed in the work order a failure has already occurred (H1-3)	30.1	Urgent action is required from the maintenance report but this is not communicated to the chief engineer.	30.1.1	Chief engineer shall receive notification when maintenance reports are available for review.	Maintenance / repair	Maintenance and operation procedures	Document control procedure	Audit of document control transparency/ communication.	OL + HS	4	1	4
				30.1.2	Chief engineer shall review and acknowledge maintenance reports when they are available.			Document control procedure	Audit of document control transparency/ communication.	OL + HS	4	1	4
		30.2	Chief engineer does not have available time to read the maintenance reports due to excessive workload.	30.2.1	Staffing and priorities shall allow for maintenance report review to take place when this relates to H1-3.		Resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS	4	2	8
31	Chief engineer does not authorise engineer competence resulting in engineers conducting work above their competence level (H1-3)	31.1	Company has no requirement to measure competence of engineering staff.	31.1.1	Competence of personnel required to maintain/ repair equipment posing a risk of H1-3 shall be demonstrated.	Maintenance / repair	Training/ Competence Management System	Knowledge (training/ competence)	Audit of Competence and job knowledge.	OL + HS	4	3	12
		31.2	No record of competence is maintained meaning the chief engineer makes assumptions of individual competence.	31.2.1	Competence of personnel required to maintain/ repair equipment posing a risk of H1-3 shall be documented.		Training/ Competence Management System	Knowledge (training/ competence)	Audit of Competence requirements log.	OL + HS	4	3	12
		31.3	Lack of staffing/ time pressures/ urgent repair means an engineer has to conduct maintenance/ repair beyond their authorised competence.	31.3.1	Staffing and priorities shall allow for competence review and assigning of only competent engineers to take place when this relates to H1-3.		Resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS	4	2	8
32	Chief engineer authorises competence of an engineer who does not have competence for specific procedures relating to H1-3.	32.1	Chief engineer does not have a requirements specification for competence to measure against.	32.1.1	Minimum competence requirements for all maintenance/ repair tasks posing a risk of H1-3 shall be specified based on manufacturer guidelines as a minimum.	Maintenance / repair	Maintenance and operation procedures	Knowledge (training/ competence)	Audit of Competence and job knowledge.	OL + HS	4	3	12
		32.2	Chief engineer assumes due to competence in other areas, the engineer will be competent in adjacent areas of engineering.	32.2.1	Competence of personnel specifically relating to the task in hand in maintaining/ repairing equipment posing a risk of H1-3 shall be documented and required for task posing a risk of H1-3.		Training/ Competence Management System	Knowledge (training/ competence)	Audit of Competence and job knowledge.	OL + HS	4	3	12
		32.3	Time pressures/ staff shortages force an authorisation of competence above the reality.	32.3.1	Staffing and priorities shall allow for adequate competence review to take place when this relates to H1-3.		Resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Audit of competence.	OL + HS	4	2	8

Barrier Criticality



Barrier Effectiveness

Scale of Colours
Green = 1-8
Amber = 9-15
Red = 16-30


Company
Safety policy, develop & enforce SMS, training, safety alerts, audits, resources
Reports on operations, safety meetings
Ship/ Control Room
Provide Instructions, status
Feedback on ER
Chief Engineer
Implement SMS, procedures, assess capability
Reports, logs, feedback
Provide instructions, status
Feedback on ER
Set mode, targets
Feedback on ER
Engineer
Set mode, targets
Current mode, condition
Manual Control, maintenance
Sensor readings, visual inspection
Ship automation
Automated controls
Sensor readings
Control of flammable materials/ ignition sources

Company

Objective/ responsibility	Operate safe/ fire free operations on board the ships. Ensure ships are protecting personnel, facilities and the environments from fire.
Input	Reports on operations, safety meetings, feedback from ship, (External factors to be considered in the future: feedback from other companies, feedback from safety authorities, feedback from accidents)
Output	Safety policy, development and enforcement of the SMS, training, safety alerts, audits, supply of resources
Constraints	Financially competitive market, competitive timetable, cistomer expectation

Hazards

H1	Hot surfaces (>220degC) in ER
H2	Leak from pressurised oil systems
H3	Failure to contain oil leak

Actions	**Control Action**	**Not providing**	**Providing**	**Too early**	**Too late**	**Stopped to soon (applied too short)**	**Applied too long**
A1	Provide resources to ship	Company does not provide resources to ship when resources are required to conduct maintenance to equipment posing a risk of H1-3. Company does not provide resources to ship when staffing is required to ensure SMS is followed to avoid H1-3. Company does not provide resources when specific equipment is required/ needs upgraded, to avoid H1-3.	Company provides resources when difference resources are required to maintain the system in preventing H1-3.		Company provides resources to ship too late when resources are required to conduct maintenance to equipment posing a risk of H1-3. Company provides resources to ship too late when staffing is required to ensure SMS is followed to avoid H1-3. Company provides resources to ship too late when specific equipment is required/ needs upgraded, to avoid H1-3.	Company stops providing resources to the ship too soon when an equipment upgrade is not completed, leading to H1-3. Company stops providing resources too soon when continual maintenance of the system is required, leading to H1-3.	
A2	Inspect fire safety	Company does not inspect fire safety on board its fleet when fire safety measures are not adequate, posing a risk of H1-3 Company does not inspect fire safety measures when staff on board do not believe fire safety is a priority.	Company inspects fire safety when the ship has been prepared for inspection, hiding signs of risk of H1-3.	Company inspects fire safety too early when hazards posing a risk of H1-3 are not yet introduced on the ship.	Company inspects fire safety on board its fleet too late when fire safety measures are not adequate, posing a risk of H1-3	Company stops inspecting fire safety too soon, before fully investigating the hazards poising a risk of H1-3.	
A3	Publish SMS	Company does not publish the SMS when the ship requires guidance on safety on board related to H1-3	Company publishes SMS when there is no way of getting this information to the ship, leading to H1-3				
A4	Enforce SMS	Company does not enforce the SMS when the ship is unaware of how to deal with fire safety, leading to H1-3 Company does not enforce the SMS when the ship has no priority on fire safety, leading to H1-3			Company enforces the SMS too late, when the standrad of fire safety has already dropped (H1-3)		
A5	Train ship personnel	Company does not train ship personnel when competence is required to maintain fire free operations (H1-3)					
A6	Warn ship of fire safety threat	Company does not provide a fire safety warning to the fleet of ships when information is received that a known flaw exists on board, increasing the risk of H1-3			Company provides a fire safety warning to the fleet of ships too late when information is received that a known flaw exists on board, increasing the risk of H1-3		
A7	Investigate/ implement safety improvements	Company does not investigate or implement innovation/ improvement in safety meaning operations and facilities remain outdated and begin ageing, leading to H1-3	Company investigates safety improvements and implements them blindly without consideration of whether they improve or reduce holistic fire safety, leading to H1-3		Company investigates safety improvements too late, meaning the safety improvements are applied after the risk of H1-3 already exists	Company stops investigating safety improvements too soon, before a potential solution to prevent H1-3 specific to their fleet is discovered.	

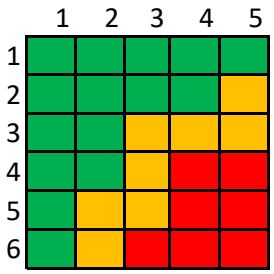
ID	Unsafe control action	Inadequate input (missing, wrong, too late/early etc.) / out-of-range disturbances	Inadequate control algorithm (fault, data handling etc.) /Inadequate responsibilities, knowledge or skills	Inconsistent process (mental) model	Design of incomplete process (mental) model	Inadequate feedback (incomplete, too late, missing, etc.)	Inadequate control path (too late, etc.)	Unrully controlled process
1	**Company does not provide resources to ship when resources are required to conduct maintenance to equipment posing a risk of H1-3.**		Company does not assign maintenance based resource decisions to personnel with experience/ knowledge of fire risk on board. Costs are cut in maintenance resource allocation in order for the company to remain competitive in the marketplace	Company do not believe the request from ship for resource to maintain the system is required.		Company is not informed of resource requirement as the ship personnel believe they can maintain equipment with the resources they have.		
2	**Company does not provide resources to ship when staffing is required to ensure SMS is followed to avoid H1-3.**		Costs are cut in staffing levels in order for the company to remain competitive in the marketplace Company does not have the staff in house who can audit and enfores the SMS on board the ship	Company believe the SMS will be followed on the ship and does not provide resource to enforce it		Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship		
3	**Company does not provide resources when specific equipment is required/ needs upgraded, to avoid H1-3.**		Company does not assign equipment upgrade decisions to personnel with experience/ knowledge of fire risk on board. Upgrade projects are cut in order for the company to remain competitive in the marketplace	Company does not believe the request from ship for equipment upgrade is required.		Company is not aware of a required equipment upgrade to prevent fire		
4	**Company provides resources when difference resources are required to maintain the system in preventing H1-3.**		Company does not assign maintenance based resource decisions to personnel with experience/ knowledge of equipment on board.	Company provides resource for maintenance but the resources are not sufficient to adequately maintain the systems to prevent H1-3.		Company is informed of the incorrect resource which is really required to maintain the equipment		
5	**Company provides resources to ship too late when resources are required to conduct maintenance to equipment posing a risk of H1-3.**		Company does not assign maintenance based resource decisions to personnel with experience/ knowledge of fire risk on board. Company does not appreciate the time sensitive nature of the resource request in order to prevent fire on the ship			Company is not informed of resource requirement as the ship personnel believe there is no priority on maintaining the system.	Company has the resource required to maintain the ship systems posing a threat of H1-3, but it takes too long to get this resouce to the ship requiring the resource.	
6	**Company provides resources to ship too late when staffing is required to ensure SMS is followed to avoid H1-3.**		Company does not have the staff in house who can audit and enfores the SMS on board the ship therefore inspection/ enforcement is delayed			Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship, and inspection is delayed		
7	**Company provides resources to ship too late when specific equipment is required/ needs upgraded, to avoid H1-3.**		Company does not assign upgrade based resource decisions to personnel with experience/ knowledge of fire risk on board. Company does not appreciate the time sensitive nature of the resource request in order to prevent fire on the ship			Company is not informed of resource requirement as the ship personnel believe there is no priority on upgrading the system.	Company has the resource required to upgrade the equipment posing a threat of H1-3, but it takes too long to get this resouce to the ship requiring the resource.	
8	**Company stops providing resources to the ship too soon when an equipment upgrade is not completed, leading to H1-3.**		Company are under financial pressures and the upgrade is beginning to cost more than anticipated therefore the upgrade is halted before the risk of H1-3 is removed.			Company believes the upgrade is complete and pulls the resources required to complete the project.		
9	**Company stops providing resources too soon when continual maintenance of the system is required, leading to H1-3.**	Company is not aware of the maufacturer requirement of the equipment with respect to continual maintenance.	Company are under financial pressures and the maintenance budget is more than acceptable therefore the maintenance is relaxed.					
10	**Company does not inspect fire safety on board its fleet when fire safety measures are not adequate, posing a risk of H1-3**	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship	Company does not have available resource to conduct a fire safety inspection	Company assumes fire safety measures on board the ship must be adequate as an SMS is in place.		Company are not made aware of fire safety issues/ near misses which have ocurred on the ship. Company enforces zero tolerance to fire and has a punitive culture therefore the ship does not pass on near miss data to company.		
11	**Company does not inspect fire safety measures when staff on board do not believe fire safety is a priority.**		Company are informed by the staff on the ship that fire safety is adequate, and therefore do not conduct an inspection.			Company are unaware of fire safety issues on board the ship as the ship staff do not percieve precursors of H1-3 as a priority and do not log or report them.		
12	**Company inspects fire safety when the ship has been prepared for inspection, hiding signs of risk of H1-3.**	Company promotes a punitive approach to fire safety issues, meaning in preparation for inspection the ship ensures the fire risk areas are patched up, misleading the company to the state of fire safety during normal operations.				Company provides fair warning of inspection of the ship, meaning personnel on the ship mend any issues which have been tolerated in order to 'pass' the inspection.		
13	**Company inspects fire safety too early when hazards posing a risk of H1-3 are not yet introduced on the ship.**		Company inspect the engine room before a voyage, before the engines are operations, therefore missing signs of risk of H1-3	Company inspects equipment immediately post commissioning and believes this is suitable for the life of the equipment. Further follow up inspections do not take place as wear and tear impact fire safety				
14	**Company inspects fire safety on board its fleet too late when fire safety measures are not adequate, posing a risk of H1-3**	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship	Company does not have available resource to conduct a fire safety inspection				Company are made aware of a potential breach to fire safety level but this is not treated with urgency resulting in a delay to remedial action.	
15	**Company stops inspecting fire safety too soon, before fully investigating the hazards poising a risk of H1-3.**		Company representative is not fully familiar with the equipment which poses a risk of H1-3 and believe all hazardous components have been inspected.					
16	**Company does not publish the SMS when the ship requires guidance on safety on board related to H1-3**	No communication path exists where the ship can request guidance on safety or the generation of a SMS	Company personnel do not know who owns responsibilty for publishing the SMS Company are not aware they have to publish a SMS for safe operations on board.	Company assumes an SMS is in place but this is not verified as being published and available				

17	**Company publishes SMS when there is no way of getting this information to the ship, leading to H1-3**	Ship and company do not have regular contact or communication so the company does not realise the ship is unaware of the SMS			No communication path exists where the company can advise the ship of guidance on safety or the generation of a SMS
18	**Company does not enforce the SMS when the ship is unaware of how to deal with fire safety, leading to H1-3**	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship	Company does not have available resource to enforce the SMS	Company assumes fire safety measures on board the ship must be adequate as an SMS is in place.	
19	**Company does not enforce the SMS when the ship has no priority on fire safety, leading to H1-3**	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship	Company does not have available resource to enforce the SMS	Company assumes fire safety measures on board the ship must be adequate as an SMS is in place.	
20	**Company enforces the SMS too late, when the standrad of fire safety has already dropped (H1-3)**	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship	Company does not have available resource to enforce the SMS	Company assumes fire safety measures on board the ship must be adequate as an SMS is in place.	No communication path exists where the ship can advise on real time safety concerns
21	**Company does not train ship personnel when competence is required to maintain fire free operations (H1-3)**	Ship does not have the authority to advise the company on the training requirements specific to the ship and fire safety	Company does not have available resource to provide training for staff Trainer provided by the company is not competent in training specifically for fire safety on board the ship in question	Company does not provide relevant training to the risks curenlty on board the ship as the company does not understand those risks No avenue for feedback exists from ship personnel to the company that the training is adequate, therefore company continues to incorrectly assume the training is suitable.	
22	**Company does not provide a fire safety warning to the fleet of ships when information is received that a known flaw exists on board, increasing the risk of H1-3**	The responsible person within the company is not informed of the safety warning.	Company is under financial pressure and implementing the fix to the known problem would be too expensive, therefore warning is not issued	Company does not appreciate the serious safety implication of the warning with respect to the equipment on their fleet	
23	**Company provides a fire safety warning to the fleet of ships too late when information is received that a known flaw exists on board, increasing the risk of H1-3**	The responsible person within the company is notavailable in order to pass on the warning as soon as possible.			Company does not appreciate the time sensitive nature of the warning with respect to the equipment on their fleet
24	**Company does not implement innovation/ improvements in safety meaning operations and facilities remain outdated and begin ageing, leading to H1-3**		Financial constraints prevent the company from innovating in fire safety, or conducting research into fire safety improvements	Company believes procurement of adequate equipment is sufficient to maintain fire free operations and does not focus on innovation or improvement of existing systems	
25	**Company investigates safety improvements and implements them blindly without consideration of whether they improve or reduce holistic fire safety, leading to H1-3**		Company personnel are not adequately trained to impement a safety requirement or policy from management	Company believes any proposed improvement on fire safety should be implimented, regardless of how it intagrates on to the ship.	
26	**Company investigates safety improvements too late, meaning the safety improvements are applied after the risk of H1-3 already exists**		Company does not have available resources to investigate fire safety regularly therefore is not aware of the requiremet for improvement so investigation into improvement is carried out too late		Company does not begin to investigate safety improvements until there have been numerous near misses
27	**Company stops investigating safety improvements too soon, before a potential solution to prevent H1-3 specific to their fleet is discovered.**		Financial constraints prevent the company from concluding fire safety research into fire safety improvements	Company believe they have developed a suitable improvement to fire safety when in fact further work is required to complete the innovation.	

ID-UCA	UCA	ID-CF	Causal factors	ID-FR	Functional requirements	UCA Category	CF Category	Relevant barriers	Signals and their requirements	Hazard (Oil Leak[OL]/ Hot Surface [HS])	Previous occurrence in Incident/ Accident (Y/N) + incident ref	Barrier Effectiveness	Criticality	Magnitude of risk reduction
1	Company does not provide resources to ship when resources are required to conduct maintenance to equipment posing a risk of H1-3.	1.1	Company does not assign maintenance based resource decisions to personnel with experience/ knowledge of fire risk on board.	1.1.1	Personnel shall only be selected to conduct fire safety related maintenance when competency in that field is recorded.	Resource provision	Competency	Resource selection procedure	Records of competency/ audit of competency and procedure adherence.	OL + HS		5	3	15
		1.2	Costs are cut in maintenance resource allocation in order for the company to remain competitive in the marketplace	1.2.1	Fire safety shall always be demonstrated to maintain safe operations regardless of external influences. If costs are reduced, fire safety shall be addressed in a more cost effective way, without reducing safety.		Cost	Resource selection procedure	Analysis of trends of increased safety related incidents, increased non-compliance of procedures/ policies	OL + HS		5	3	15
		1.3	Company do not believe the request from ship for resource to maintain the system is required.	1.3.1	Rejection of a safety specific request from the ship shall require a meeting with senior ship personnel to justify/ discuss the request rejection.		Inadequate communication between ship and management	Resource selection procedure	Records of discussions regarding safety upgrade requests, audit of procedures	OL + HS		5	2	10
		1.4	Company is not informed of resource requirement as the ship personnel believe they can maintain equipment with the resources they have.	1.4.1	Ship/ company responsible and qualified person shall specify the minimum resource requirement to maintain equipment on board the ship.		Task/ resource Assignment	Resource selection procedure	Audit of resource specification, maintenance activities	OL + HS		5	3	15
2	Company does not provide resources to ship when staffing is required to ensure SMS is followed to avoid H1-3.	2.1	Costs are cut in staffing levels in order for the company to remain competitive in the marketplace	2.1.1	Fire safety shall always be demonstrated to maintain safe operations regardless of external influences. If costs are reduced, fire safety shall be addressed in a more cost effective way, without reducing safety.		Cost	Resource selection procedure	Analysis of trends of increased safety related incidents, increased non-compliance of procedures/ policies	OL + HS		5	3	15
		2.2	Company does not have the staff in house who can audit and enforce the SMS on board the ship	2.2.1	When company does not have staff in house to audit and enforce the SMS, staff shall be recruited or this shall be outsourced.		Cost/ competency	Internal staff, 3rd party experts	Documentation of SMS enforcement, competency audit, use of expert 3rd parties	OL + HS		5	3	15
		2.3	Company believe the SMS will be followed on the ship and does not provide resource to enforce it	2.3.1	Upon implementation of the SMS, enforcement of the SMS shall be determined. Assuming the SMS will be enforced shall no be allowed.		Inadequate communication between ship and management	Audit of SMS and enforcement measures	Documentation of SMS enforcement	OL + HS		5	1	5
		2.4	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship	2.4.1	Provision shall exist allowing near miss reporting to the company in the event of any fire safety related near misses.		Inadequate communication between ship and management	Audit of safety procedures	Trends regarding safety related incidents offshore.	OL + HS		5	1	5
3	Company does not provide resources when specific equipment is required/ needs upgraded, to avoid H1-3.	3.1	Company does not assign equipment upgrade decisions to personnel with experience/ knowledge of fire risk on board.	3.1.1	Personnel shall only be selected to make fire safety related decisions when competency in that field is recorded.	Resource provision	Task Assignment	Resource selection procedure	Records of competency/ audit of competency and procedure adherence.	OL + HS		5	3	15
		3.2	Upgrade projects are cut in order for the company to remain competitive in the marketplace	3.2.1	Fire safety shall always be demonstrated to maintain safe operations regardless of external influences. If costs are reduced, fire safety shall be addressed in a more cost effective way, without reducing safety.		Cost	Resource selection procedure	Analysis of trends of increased safety related incidents, increased non-compliance of procedures/ policies	OL + HS		5	3	15
		3.3	Company does not believe the request from ship for equipment upgrade is required.	3.3.1	Rejection of a safety specific request from the ship shall require a meeting with senior ship personnel to justify/ discuss the request rejection.		Inadequate communication between ship and management	Resource selection procedure	Records of discussions regarding safety upgrade requests, audit of procedures	OL + HS		5	2	10
		3.4	Company is not aware of a required equipment upgrade to prevent fire	3.4.1	Provision shall exist allowing ship personnel to request equipment upgrades related to safety		Inadequate communication between ship and management	Audit of safety procedures	Safety related requests and acknowledgments	OL + HS		5	1	5
4	Company provides resources when different resources are required to maintain the system in preventing H1-3.	4.1	Company does not assign maintenance based resource decisions to personnel with experience/ knowledge of equipment on board.	4.1.1	Personnel shall only be selected to make fire safety related decisions when competency in that field is recorded.	Resource provision	Task Assignment	Resource selection procedure	Records of competency/ audit of competency and procedure adherence.	OL + HS		5	3	15
				4.1.2	Personnel shall only be selected to make equipment upgrade decisions when competency on the specific ship equipment is recorded.			Resource selection procedure	Records of competency/ audit of competency and procedure adherence.	OL + HS		5	3	15
		4.2	Company provides resource for maintenance but the resources are not sufficient to adequately maintain the systems to prevent H1-3.	4.2.1	Ship/ company responsible and qualified person shall specify the minimum resource requirement to maintain equipment on board the ship.		Task/ resource Assignment	Resource selection procedure	Audit of resource specification, maintenance activities	OL + HS		5	3	15
		4.3	Company is informed of the incorrect resource which is really required to maintain the equipment	4.3.1	Equipment manufacturer/ competent internal resource/ external 3rd party shall verify the resource specification for maintenance of equipment posing a fire risk.		Task/ resource Assignment	Resource selection procedure	Audit of resource specification, maintenance activities	OL + HS		5	3	15
5	Company provides resources to ship too late when resources are required to conduct maintenance to equipment posing a risk of H1-3.	5.1	Company does not assign maintenance based resource decisions to personnel with experience/ knowledge of fire risk on board.	5.1.1	Personnel shall only be selected to make fire safety related decisions when competency in that field is recorded.		Task Assignment	Resource selection procedure	Records of competency/ audit of competency and procedure adherence.	OL + HS		5	3	15
		5.2	Company does not appreciate the time sensitive nature of the resource request in order to prevent fire on the ship	5.2.1	Resource requests shall indicate the urgency of the request and whether the request inhibits maintenance from being conducted immediately.		Resource Assignment	Resource provision procedure	Analysis of time taken to supply resource when the request is urgent.	OL + HS		5	1	5
		5.3	Company is not informed of resource requirement as the ship personnel believe there is no priority on maintaining the system.	5.3.1	Ship personnel shall inform the company of resource requirements in order to conduct adequate maintenance.	Resource provision	Task Assignment	Maintenance procedure	Analysis of maintenance logs, audit of full maintenance being carried out	OL + HS		5	3	15
		5.4	Company has the resource required to maintain the ship systems posing a threat of H1-3, but it takes too long to get this resource to the ship requiring the resource.	5.4.1	Resources required to conduct maintenance shall be supplied before stocks become depleted, eliminating down time where no resource required for maintenance is on board.		Resource Assignment	Resource provision procedure	Analysis of resource supply when the request is generated.	OL + HS		5	3	15
6	Company provides resources to ship too late when staffing is required to ensure SMS is followed to avoid H1-3.	6.1	Company does not have the staff in house who can audit and enforce the SMS on board the ship therefore inspection/ enforcement is delayed	6.1.1	When company does not have staff in house to audit and enforce the SMS, staff shall be recruited or this shall be outsourced.		Cost/ competency	Internal staff, 3rd party experts	Documentation of SMS enforcement, competency audit, use of expert 3rd parties	OL + HS		5	3	15
		6.2	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship, and inspection is delayed	6.2.1	Provision shall exist allowing near miss reporting to the company in the event of any fire safety related near misses.		Inadequate communication between ship and management	Audit of safety procedures	Trends regarding safety related incidents offshore/ inspection record.	OL + HS		5	1	5
				6.2.2	Inspection shall not be delayed on the basis of assumed safety adequacy.			Audit of inspection history	Inspection regularity becoming relaxed/ skipped inspections becoming the norm	OL + HS		5	3	15
7	Company provides resources to ship too late when specific equipment is required/ needs upgraded, to avoid H1-3.	7.1	Company does not assign upgrade based resource decisions to personnel with experience/ knowledge of fire risk on board.	7.1.1	Personnel shall only be selected to make fire safety related decisions when competency in that field is recorded.		Task Assignment	Resource selection procedure	Records of competency/ audit of competency and procedure adherence.	OL + HS		5	3	15
		7.2	Company does not appreciate the time sensitive nature of the resource request in order to prevent fire on the ship	7.2.1	Resource requests shall indicate the urgency of the request and whether the request inhibits maintenance from being conducted immediately.		Resource Assignment	Resource provision procedure	Analysis of time taken to supply resource when the request is urgent.	OL + HS		5	1	5
		7.3	Company is not informed of resource requirement as the ship personnel believe there is no priority on upgrading the system.	7.3.1	Ship personnel shall inform the company of resource requirements in order to conduct equipment upgrade.	Resource provision	Task Assignment	Management of change procedure	Analysis of upgrade logs, audit of upgrades being carried out	OL + HS		5	3	15
		7.4	Company has the resource required to upgrade the equipment posing a threat of H1-3, but it takes too long to get this resource to the ship requiring the resource.	7.4.1	Resources required to complete an equipment upgrade shall be supplied before stocks become depleted, eliminating down time where no resource required for upgrade is on board.		Resource Assignment	Resource provision procedure	Analysis of resource supply when the request is generated.	OL + HS		5	3	15
8	Company stops providing resources to the ship too soon when an equipment upgrade is not completed, leading to H1-3.	8.1	Company are under financial pressures and the upgrade is beginning to cost more than anticipated therefore the upgrade is halted before the risk of H1-3 is removed.	8.1.1	Where an upgrade is proposed, work shall not begin until it is certain that resources are available to fully complete the upgrade.		Cost	Upgrade planning procedure	Audit of upgrade project plan vs. completion	OL + HS		5	1	5
				8.1.2	When an upgrade is started, it shall be completed to an equivalent level of fire safety from the moment before upgrade occurred.			Upgrade planning procedure	Audit of upgrade project plan vs. completion	OL + HS		5	1	5
		8.2	Company believes the upgrade is complete and pulls the resources required to complete the project.	8.2.1	Resource provision will only be removed when the ship personnel/ expert 3rd party have authorised that the upgrade is complete.		Task Assignment	Management of change procedure	Analysis of upgrade logs, audit of upgrades being carried out	OL + HS		5	3	15
9	Company stops providing resources too soon when continual maintenance of the system is required, leading to H1-3.	9.1	Company is not aware of the manufacturer requirement of the equipment with respect to continual maintenance.	9.1.1	Maintenance routines shall be based upon manufacturer recommendations and any applicable 3rd party advice on maintenance requirements.	Resource provision	Maintenance procedure	Audit of maintenance procedures	Inspection of maintenance requirements against manufacturer requirements	OL + HS		5	3	15
		9.2	Company are under financial pressures and the maintenance budget is more than acceptable therefore the maintenance is relaxed.	9.2.1	Authorisation shall be granted from the manufacturer before deviating from the requirements which could lead to increased risk of H1-3		Maintenance procedure	Audit of maintenance procedures	Inspection of maintenance requirements against manufacturer requirements	OL + HS		5	3	15
10	Company does not inspect fire safety on board its fleet when fire safety measures are not adequate, posing a risk of H1-3	10.1	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship	10.1.1	Provision shall exist allowing near miss reporting to the company in the event of any fire safety related near misses.		Inadequate communication between ship and management	Audit of safety procedures	Trends regarding safety related incidents offshore.	OL + HS		5	1	5
		10.2	Company does not have available resource to conduct a fire safety inspection	10.2.1	When company does not have staff in house to inspect fires safety, staff shall be recruited or this shall be outsourced.		Cost/ competency	Internal staff, 3rd party experts	Competency audit, use of expert 3rd parties	OL + HS		5	3	15
		10.3	Company assumes fire safety measures on board the ship must be adequate as an SMS is in place.	10.3.1	Company shall implement enforcement of the SMS or instruct an expert 3rd part to enforce it on their behalf.		Inadequate communication between ship and management	Audit of SMS enforcement	Audit of SMS enforcement	OL + HS		5	1	5
		10.4	Company are not made aware of fire safety issues/ near misses which have occurred on the ship.	10.4.1	Provision shall exist allowing near miss reporting to the company in the event of any fire safety related near misses.		Inadequate communication between ship and management	Audit of safety procedures	Trends regarding safety related incidents offshore.	OL + HS		5	1	5
		10.5	Company enforces zero tolerance to fire and has a punitive culture therefore the ship does not pass on near miss data to company.	10.5.1	Ship shall be encouraged to be honest and proactive regarding fire safety incidents.		Inadequate communication between ship and management	Audit of near miss documentation/ staff attitudes to safety reporting	Trends regarding safety related incidents offshore.	OL + HS		5	1	5
11	Company does not inspect fire safety measures when staff on board do not believe fire safety is a priority.	11.1	Company are informed by the staff on the ship that fire safety is adequate, and therefore do not conduct an inspection.	11.1.1	Inspection shall not be cancelled on the basis of assumed safety adequacy.		Misleading communication between ship and management	Audit of inspection history	Inspection regularity becoming relaxed/ skipped inspections becoming the norm	OL + HS		5	3	15
		11.2	Company are unaware of fire safety issues on board the ship as the ship staff do not perceive precursors of H1-3 as a priority and do not log or report them.	11.2.1	Staff on board the ship hall be aware of the criticality associated with fire safety on board, assuring near misses and safety concerns are communicated to the company.	Resource provision	Inadequate communication between ship and management	Audit of fire safety perception on board the ship/ record of near misses.	Trends regarding safety attitudes n the ship/ safety related incidents offshore.	OL + HS		5	1	5
				11.2.2	Provision shall exist allowing near miss reporting to the company in the event of any fire safety related near misses.			Audit of safety procedures	Trends regarding safety related incidents offshore.	OL + HS		5	1	5
12	Company inspects fire safety when the ship has been prepared for inspection, hiding signs of risk of H1-3.	12.1	Company promotes a punitive approach to fire safety issues, meaning in preparation for inspection the ship ensures the fire risk areas are patched up, misleading the company to the state of fire safety during normal operations.	12.1.1	Company shall promote an honest and open policy with respect to near miss reporting and inspections/ concerns such that the company have an accurate impression of fire safety status on board		Inadequate communication between ship and management	Audit of staff attitudes to safety	Staff judgement of company attitude to safety, near miss/ accident reporting history	OL + HS		5	1	5
		12.2	Company provides fair warning of inspection of the ship, meaning personnel on the ship mend any issues which have been tolerated in order to 'pass' the inspection.	12.2.1	Inspections of safety on board shall range from planned in advance to short notice fire safety inspections by either component company personnel or expert 3rd party.		Inspection Procedure	Audit of safety inspection schedule	Analysis of safety findings between short term and long term planned inspections	OL + HS		5	3	15
13	Company inspects fire safety too early when hazards posing a risk of H1-3 are not yet introduced on the ship.	13.1	Company inspect the engine room before a voyage, before the engines are operations, therefore missing signs of risk of H1-3	13.1.1	Inspections shall be conducted both when the engine room is in full operation and when in port to gain a full understanding of fire safety.		Inspection Procedure	Audit of safety inspection schedule	Analysis of safety findings between ship in port and ship at sea inspections	OL + HS		5	3	15
		13.2	Company inspects equipment immediately post commissioning and believes this is suitable for the life of the equipment. Further follow up inspections do not take place as wear and tear impact fire safety	13.2.1	Inspections shall be conducted both after inspection and routinely through the life of the ship to gain a full understanding of fire safety.	Resource provision	Inspection Procedure	Audit of safety inspection schedule	Analysis of safety findings throughout the life of the ship	OL + HS		5	3	15
14	Company inspects fire safety on board its fleet too late when fire safety measures are not adequate, posing a risk of H1-3	14.1	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship	14.1.1	Provision shall exist allowing near miss reporting to the company in the event of any fire safety related near misses.		Inadequate communication between ship and management	Audit of safety procedures	Trends regarding safety related incidents offshore.	OL + HS		5	1	5
				14.1.2	Inspection shall not be delayed on the basis of assumed safety adequacy.			Audit of inspection history	Inspection regularity becoming relaxed/ skipped inspections becoming the norm	OL + HS		5	3	15
		14.2	Company does not have available resource to conduct a fire safety inspection	14.2.1	When company does not have staff in house to inspect fires safety, staff shall be recruited or this shall be outsourced.		Cost/ competency	Internal staff, 3rd party experts	Competency audit, use of expert 3rd parties	OL + HS		5	3	15
		14.3	Company are made aware of a potential breach to fire safety level but this is not treated with urgency resulting in a delay to remedial action.	14.3.1	When company are made aware of a possible safety breach, a responsible and competent person (internal or external) shall review the requirements		Competency	Internal staff, 3rd party experts	Documentation of SMS enforcement, competency audit, use of expert 3rd parties	OL + HS		5	3	15
15	Company stops inspecting fire safety too soon, before fully investigating the hazards poising a risk of H1-3.	15.1	Company representative is not fully familiar with the equipment which poses a risk of H1-3 and believe all hazardous components have been inspected.	15.1.1	Company safety representative shall be competent in the field of fire safety for their responsible assets.	Resource provision	Competency	Internal staff, 3rd party experts	Audit of minimum competency	OL + HS		5	3	15
16	Company does not publish the SMS when the ship requires guidance on safety on board related to H1-3	16.1	No communication path exists where the ship can request guidance on safety or the generation of a SMS	16.1.1	Ship personnel shall have direct contact with a responsible company representative for SMS guidance		Inadequate communication between ship and management	Audit of SMS enforcement	Audit of SMS enforcement	OL + HS		5	1	5
		16.2	Company personnel do not know who owns responsibility for publishing the SMS	16.2.1	Responsibilities regarding the SMS shall be clearly documented and informed	SMS	Task allocation	Staffing procedure	Audit of roles and responsibilities	OL + HS		5	1	5
		16.3	Company are not aware they have to publish a SMS for safe operations on board.	16.3.1	Company shall maintain fire safety competency in house, or rely on expert 3rd parties for advice on safety requirements.		Competence	Competency procedure	Documentation of competency audit, use of expert 3rd parties	OL + HS		5	3	15
		16.4	Company assumes an SMS is in place but this is not verified as being published and available	16.4.1	Company shall maintain fire safety competency in house to enforce the SMS, staff shall be recruited or this shall be outsourced.		Task allocation	Internal staff, 3rd party experts	Documentation/ verification of SMS, competency audit, use of expert 3rd parties	OL + HS		5	3	15
17	Company publishes SMS when there is no way of getting this information to the ship, leading to H1-3	17.1	Ship and company do not have regular contact or communication so the company does not realise the ship is unaware of the SMS	17.1.1	Ship and company shall maintain regular contact to discuss safety concerns and the SMS on the ship		Communication	Audit of SMS awareness	Audit of SMS enforcement	OL + HS		5	1	5
		17.2	No communication path exists where the company can advise the ship of guidance on safety or the generation of a SMS	17.2.1	Company personnel shall have direct contact with the ship representatives for SMS guidance		Inadequate communication between ship and management	Audit of SMS enforcement	Audit of SMS enforcement	OL + HS		5	1	5
18	Company does not enforce the SMS when the ship is unaware of how to deal with fire safety, leading to H1-3	18.1	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship	18.1.1	Provision shall exist allowing near miss reporting to the company in the event of any fire safety related near misses.		Inadequate communication between ship and management	Audit of safety procedures	Trends regarding safety related incidents offshore.	OL + HS		5	1	5
		18.2	Company does not have available resource to enforce the SMS	18.2.1	When company does not have staff in house to enforce the SMS, staff shall be recruited or this shall be outsourced.		Cost/ competency	Internal staff, 3rd party experts	Documentation of SMS enforcement, competency audit, use of expert 3rd parties	OL + HS		5	3	15
		18.3	Company assumes fire safety measures on board the ship must be adequate as an SMS is in place.	18.3.1	Company shall implement enforcement of the SMS or instruct an expert 3rd part to enforce it on their behalf.		Inadequate communication between ship and management	Audit of SMS enforcement	audit of SMS enforcement	OL + HS		5	1	5
		19.1	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship	19.1.1	Provision shall exist allowing near miss reporting to the company in the event of any fire safety related near misses.		Inadequate communication between ship and management	Audit of safety procedures	Trends regarding safety related incidents offshore.	OL + HS		5	1	5

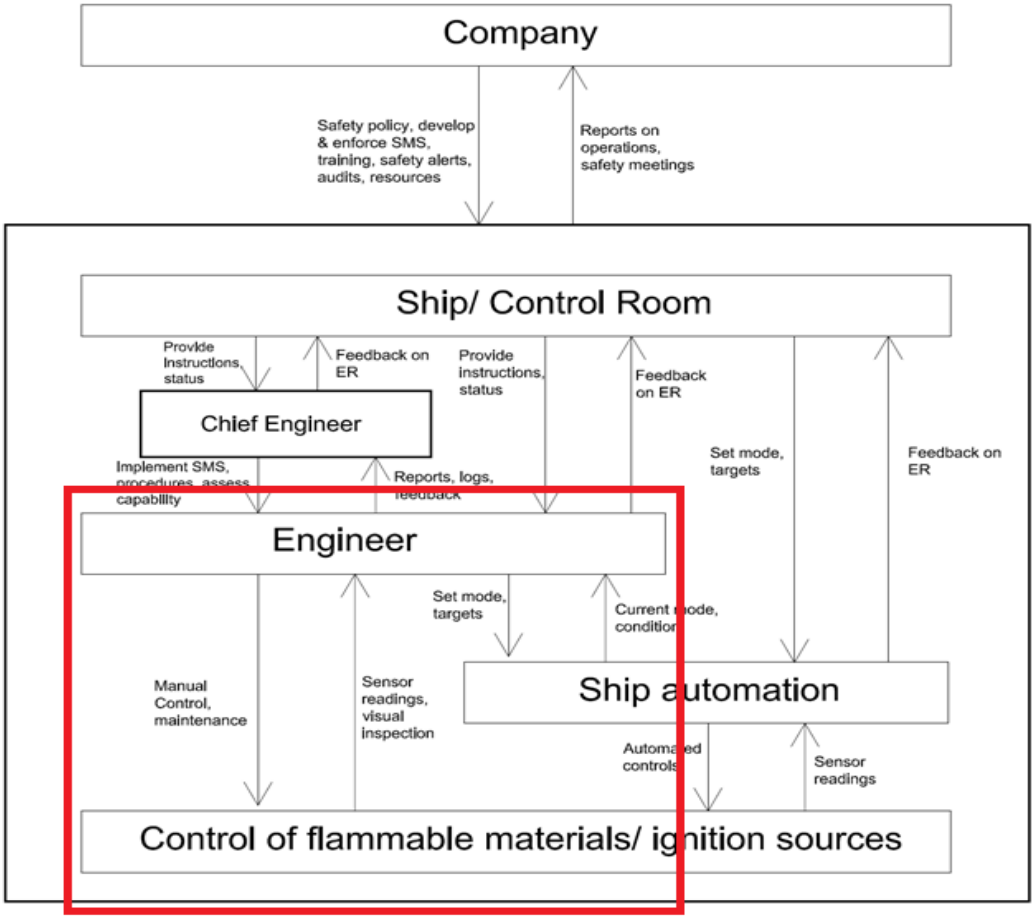
19	Company does not enforce the SMS when the ship has no priority on fire safety, leading to H1-3	19.2	Company does not have available resource to enforce the SMS	19.2.1	When company does not have staff in house to enforce the SMS, staff shall be recruited or this shall be outsourced.	Resource provision	Cost/ competency	Internal staff, 3rd party experts	Documentation of SMS enforcement, competency audit, use of expert 3rd parties	OL + HS	5	3	15
		19.3	Company assumes fire safety measures on board the ship must be adequate as an SMS is in place.	19.3.1	Company shall implement enforcement of the SMS or instruct an expert 3rd part to enforce it on their behalf.		Inadequate communication between ship and management	Audit of SMS enforcement	audit of SMS enforcement	OL + HS	5	1	5
		20.1	Company does not receive feedback of any safety issues therefore believes safety must be very good on the ship	20.1.1	Provision shall exist allowing near miss reporting to the company in the event of any fire safety related near misses.		Inadequate communication between ship and management	Audit of safety procedures	Trends regarding safety related incidents offshore.	OL + HS	5	1	5
				20.1.2	Inspection shall not be delayed on the basis of assumed safety adequacy.			Audit of inspection history	Inspection regularity becoming relaxed/ skipped inspections becoming the norm	OL + HS	5	3	15
20	Company enforces the SMS too late, when the standard of fire safety has already dropped (H1-3)	20.2	Company does not have available resource to enforce the SMS	20.2.1	When company does not have staff in house to enforce the SMS, staff shall be recruited or this shall be outsourced.	Resource provision	Cost/ competency	Internal staff, 3rd party experts	Documentation of SMS enforcement, competency audit, use of expert 3rd parties	OL + HS	5	3	15
		20.3	Company assumes fire safety measures on board the ship must be adequate as an SMS is in place.	20.3.1	Company shall implement enforcement of the SMS or instruct an expert 3rd part to enforce it on their behalf.		Inadequate communication between ship and management	Audit of SMS enforcement	Audit of SMS enforcement	OL + HS	5	1	5
		20.4	No communication path exists where the ship can advise on real time safety concerns	20.4.1	Ship personnel shall have direct contact with a responsible company representative for SMS enforcement		Inadequate communication between ship and management	Audit of SMS enforcement	Audit of SMS enforcement	OL + HS	5	1	5
21	Company does not train ship personnel when competence is required to maintain fire free operations (H1-3)	21.1	Ship does not have the authority to advise the company on the training requirements specific to the ship and fire safety	21.1.1	The ship shall have the ability and opportunity to specify the specific training requirements of the specific ship with company.	Competence	Inadequate autonomy on fire safety	Training specification	Training provision audit	OL + HS	5	1	5
		21.2	Company does not have available resource to provide training for staff	21.2.1	When company does not have training staff resource in house, staff shall be recruited or this shall be outsourced.		Cost/ competency	Internal staff, 3rd party experts	Documentation of competency audit, use of expert 3rd parties	OL + HS	5	3	15
		21.3	Trainer provided by the company is not competent in training specifically for fire safety on board the ship in question	21.3.1	Any person/ company involved in safety related training shall be competent in the field of training provided.		Training provision	Training specification	Audit of minimum competency	OL + HS	5	1	5
		21.4	Company does not provide relevant training to the risks currently on board the ship as the company does not understand those risks	21.4.1	The ship shall have the ability and opportunity to specify the specific training requirements of the specific ship with company.		Competency	Training specification	Training provision audit	OL + HS	5	1	5
		21.5	No avenue for feedback exists from ship personnel to the company that the training is adequate, therefore company continues to incorrectly assume the training is suitable.	21.5.1	Safety related training shall provide a feedback function for participants to rate relevancy and provide comment back to company.		Training provision	Training feedback	Audit of training feedback/ training relevance	OL + HS	5	1	5
22	Company does not provide a fire safety warning to the fleet of ships when information is received that a known flaw exists on board, increasing the risk of H1-3	22.1	The responsible person within the company is not informed of the safety warning.	22.1.1	Responsible safety representative within the company shall be known throughout the company and also publicly available for external suppliers to contact		Inadequate communication within the company	Specified and public roles and responsibilities	Audit of contact detail availability	OL + HS	5	1	5
		22.2	Company is under financial pressure and implementing the fix to the known problem would be too expensive, therefore warning is not issued	22.2.1	When a safety warning is received, the equipment issue shall be mitigated to an equivalent level of fire safety intended from historical operations.	Communication	Cost	Upgrade planning procedure	Audit of continual improvement indicators/ initiative upgrade projects	OL + HS	5	1	5
				22.2.2	Warnings shall be passed to the ship when received and authorisation shall be granted from the manufacturer before deviating from the specified requirements			Audit of maintenance procedures	Inspection of maintenance requirements against manufacturer requirements	OL + HS	5	3	15
		22.3	Company does not appreciate the serious safety implication of the warning with respect to the equipment on their fleet	22.3.1	Company shall maintain fire safety competency in house, or rely on exert 3rd party for advice on safety related warnings.		Competence	Competency procedure	Documentation of competency audit, use of expert 3rd parties	OL + HS	5	3	15
23	Company provides a fire safety warning to the fleet of ships too late when information is received that a known flaw exists on board, increasing the risk of H1-3	23.1	The responsible person within the company is not available in order to pass on the warning as soon as possible.	23.1.1	Responsible fire safety representative shall be available at all times	Communication	Task allocation	Staffing procedure	Audit of deputisation	OL + HS	5	1	5
		23.2	Company does not appreciate the time sensitive nature of the warning with respect to the equipment on their fleet	23.2.1	Fire safety warnings shall indicate the urgency of the warning and whether the request inhibits safe operation immediately.		Competency	Resource provision procedure	Audit of safety procedure	OL + HS	5	3	15
24	Company does not implement innovation/ improvements in safety meaning operations and facilities remain outdated and begin ageing, leading to H1-3	24.1	Financial constraints prevent the company from innovating in fire safety, or conducting research into fire safety improvements	24.1.1	Company shall stay abreast of the latest in safety innovation in the industry through either participation in the innovation itself, or maintaining awareness of the activities of others through industry shared knowledge	Innovation	Cost	Safety representatives, knowledge sharing	Audit of participation in safety events/ research projects/ safety product and system development	OL + HS	5	1	5
		24.2	Company believes procurement of adequate equipment is sufficient to maintain fire free operations and does not focus on innovation or improvement of existing systems	24.2.1	Company shall not rely solely on safety equipment in isolation and will maintain knowledge of the latest in safety innovation in the industry		Competence	Safety representatives, knowledge sharing	Audit of attitude to safety regarding equipment procurement; participation in safety events/ research projects/ safety product and system development	OL + HS	5	3	15
25	Company investigates safety improvements and implements them blindly without consideration of whether they improve or reduce holistic fire safety, leading to H1-3	25.1	Company personnel are not adequately trained to implement a safety requirement or policy from management	25.1.1	When company does not have trained staff resource in house, staff shall be recruited or this shall be outsourced.	Innovation	Cost/ competency	Internal staff, 3rd party experts	Documentation of competency audit, use of expert 3rd parties	OL + HS	5	3	15
		25.2	Company believes any proposed improvement on fire safety should be implemented, regardless of how it integrates on to the ship.	25.2.1	Company shall not rely solely on safety equipment in isolation and will ensure holistic safety is addressed in all decisions		Competence	Safety representatives, knowledge sharing	Audit of attitude to safety regarding equipment procurement; Audit of competence	OL + HS	5	3	15
26	Company investigates safety improvements too late, meaning the safety improvements are applied after the risk of H1-3 already exists	26.1	Company does not have available resources to investigate fire safety regularly therefore is not aware of the requirement for improvement so investigation into improvement is carried out too late	26.1.1	Company shall stay abreast of the latest in safety innovation in the industry through either participation in the innovation itself, or maintaining awareness of the activities of others through industry shared knowledge	Innovation	Competence	Safety representatives, knowledge sharing	Audit of participation in safety events/ research projects/ safety product and system development	OL + HS	5	1	5
		26.2	Company does not begin to investigate safety improvements until there have been numerous near misses	26.2.1	Company shall be proactive in investigation of safety improvements, ensuring safety standards do not drop below those acceptable at commissioning.		Cost/ competency	Safety representatives, knowledge sharing	Audit of continuous improvement policies, participation in safety events/ research projects/ safety product and system development	OL + HS	5	1	5
27	Company stops investigating safety improvements too soon, before a potential solution to prevent H1-3 specific to their fleet is discovered.	27.1	Financial constraints prevent the company from concluding fire safety research into fire safety improvements	27.1.1	Fire safety shall always be demonstrated to maintain safe operations regardless of external influences. If costs are reduced, fire safety shall be addressed in a more cost effective way, without reducing safety.	Innovation	Cost	Resource selection procedure	Analysis of trends of increased safety related incidents, increased non-compliance of procedures/ policies	OL + HS	5	3	15
		27.2	Company believe they have developed a suitable improvement to fire safety when in fact further work is required to complete the innovation.	27.2.1	Company shall be proactive in investigation of safety improvements, ensuring safety standards do not drop below those acceptable at commissioning.		Cost/ competency	Safety representatives, knowledge sharing	Audit of continuous improvement policies, participation in safety events/ research projects/ safety product and system development	OL + HS	5	1	5
				27.2.2	Company shall not rely on a singular project improvement and shall ensure holistic safety is addressed in all decisions			Safety representatives, knowledge sharing	Audit of attitude to safety regarding equipment procurement; Audit of competence	OL + HS	5	3	15

Barrier Criticality



Barrier Effectiveness

Scale of Colours
Green = 1-8
Amber = 9-15
Red = 16-30


Company
Safety policy, develop & enforce SMS, training, safety alerts, audits, resources
Reports on operations, safety meetings
Ship/ Control Room
Provide Instructions, status
Feedback on ER
Chief Engineer
Implement SMS, procedures, assess capability
Reports, logs, feedback
Provide instructions, status
Feedback on ER
Set mode, targets
Feedback on ER
Engineer
Set mode, targets
Current mode, condition
Manual Control, maintenance
Sensor readings, visual inspection
Ship automation
Automated controls
Sensor readings
Control of flammable materials/ ignition sources

Engineer

Objective/ responsibility	Maintain equipment within the ER, ensuring hot surfaces and breaks in containment do not occur.
Input	Instruction from Chief Engineer/ ECR. Initiative while in the ER. Sensor readings.
Output	Repair of equipment. Maintenance of equipment. Reports to Chief Engineer/ Company. Feedback to ECR. Manual process control when required.
Constraints	Resources, Time, Instructions, Training, Autonomy

Hazards

H1	Hot surfaces (>220degC) in ER
H2	Leak from pressurised oil systems
H3	Failure to contain oil leak

Actions	Control Action	Not providing	Providing	Too early	Too late	Stopped to soon (applied too short)	Applied too long
A1	Inspect Equipment	Engineer does not detect loss of integrity during inspection (H-2, H-3) Engineer does not detect incorrect implementation of equipment as per manufacturer guidelines during inspection (H-2, H-3)	Engineer interferers with equipment and doesn't return to its original condition during inspection (H-1, H-2, H-3)		Engineer inspects equipment too late to find damaged/ degraded equipment (H-1, H-2, H-3)	Engineer does not complete inspection when hot surfaces or damaged/ degraded equipment present (H-1, H-2, H-3)	
A2	Report on integrity	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)	Engineer report on integrity is too vague when a specific repair is required (H-1, H-2, H-3)		Engineer reports on integrity too late when damaged/ degraded equipment remains in place (H-1, H-2, H-3)		
A3	Repair equipment	Engineer doesn’t repair equipment when faulty equipment present (H-1, H-2, H-3)	Engineer begins repair during operation state (i.e. pressurised) (H-2, H-3) Engineer repairs equipment but does not complete/ implement the repair correctly (H-1, H-2, H-3)	Engineer starts repairing equipment before making necessary preparations (H-1, H-2, H-3)	Engineer repairs equipment too late when damaged/ faulty equipment exists (H-1, H-2, H-3)	Engineer starts repair, but doesn't complete when faulty equipment is present (H-1, H-2, H-3)	
A4	Shutdown Engine	Engineer doesn't shutdown the engine when exposed hot surfaces exist (H-1) Engineer doesn't shutdown the engine when strain on the engine components exceeds design threshold (H-2, H-3)	Engineer shuts down the engine and does not immediately reduce load on other engines which become temporarily overloaded (H-1, H-2)		Engineer shuts down the engine too late when a fuel/ lube oil release exists (H-2, H-3) Engineer doesn't shutdown the engine fast enough when exposed hot surfaces exist (H-1)		
A5	Shutdown Fuel Supply	Engineer doesn't shutdown the fuel supply when strain on the components exceeds design threshold (H-2, H-3)			Engineer shuts down the fuel supply too late when a fuel/ lube oil release exists (H-2, H-3)		
A6	Release Water Mist	Engineer doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)			Engineer releases the water mist too late when leak exists (H-1). Engineer releases the water mist too late when exposed hot surface exists (H-1)	Engineer stops the water mist too soon when hot exposed surfaces have existed and oil mist in atmosphere is detected/suspected (H-1)	

ID	Unsafe control action	Inadequate input (missing, wrong, too late/early etc.) / out-of-range disturbances	Inadequate control algorithm (fault, data handling etc.) /Inadequate responsibilities, knowledge or skills	Inconsistent process (mental) model	Design of incomplete process (mental) model	Inadequate feedback (incomplete, too late, missing, etc.)	Inadequate control path (too late, etc.)	Unruly controlled process
1	**Engineer does not detect loss of integrity during inspection (H-2, H-3)**		Engineer is not aware of what to look for/ what the signs are of loss of integrity of the hotbox due to lack of skills/ knowledge. Engineer does not believe it is his/ her responsibility to look for loss of integrity.			Time constraints on the engineer mean the inspection is only partially completed therefore loss of integrity of the hot box is not found.	The interval between inspections of the hot box and fuel supply pipework is too lengthy resulting in severe degradation between inspections not being detected. Planned maintenance routine instructs engineer to carry out inspection but this is not completed as the engineer has too many other tasks assigned and the requirement for inspection slips off the radar and is not followed up.	
2	**Engineer does not detect incorrect implementation of equipment as per manufacturer guidelines during inspection (H-2, H-3)**	Planned maintenance routine does not provide instruction of inspection intervals meaning the engineer does not get tasked with inspecting the equipment.				The tools available to the engineer are insufficient to detect integrity loss of the fuel supply pipework i.e. no torque wrench to verify torque level of the bolts.		
3	**Engineer interferers with equipment and doesn't return to its original condition during inspection (H-1, H-2, H-3)**		Engineer does not have the training/ skillset to adequately understand the impact of interfering with equipment to get a closer inspection, resulting in continued hot surface exposure, or damaged/ fatigued equipment.					
4	**Engineer inspects equipment too late to find damaged/ degraded equipment (H-1, H-2, H-3)**	Planned maintenance routine does not provide instruction of inspection intervals meaning the engineer does not get tasked with inspecting the equipment on time to detect dangerous fatigue.					Engineer workload too full resulting in critical inspection being delayed resulting in damaged equipment remaining in place.	
5	**Engineer does not complete inspection when hot surfaces or damaged/ degraded equipment present (H-1, H-2, H-3)**	Planned maintenance routine instruction did not specifically call out the requirement to check for damaged fuel supply pipework or exposed hot surfaces.	Engineer does not have training on how to complete a check and therefore does not complete it.	Engineer believes the inspection is complete but is unaware of additional checks which are required.			Engineer is called to complete another task, meaning the inspection is not completed.	
6	**Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)**		Engineers are not trained in report writing and fail to communicate the loss of integrity to the hierarchy meaning management are unaware of fatigue to the hot box, fatigue of the fuel supply system, or hot surfaces. Engineers are instructed of a required upgrade. The work is carried out in an uncontrolled/ undocumented way. Company are unaware of what equipment is upgraded/ what is outstanding.	Engineer inspects the equipment, registers the loss of integrity of the hot box but is not aware that this presents the risk of H-3, therefore does not take or recommend action to fix. Engineer inspects the equipment, registers the loss of integrity of the fuel supply pipework but is not aware that this presents the risk of H-2, therefore does not take or recommend action to fix.			Engineer workload too busy that no time is dedicated to writing the report and the loss of integrity is not reported. Engineer workload too busy that no time is dedicated to writing the report therefore hierarchy are unaware of project completion status. Decisions are therefore made based on the assumption that equipment is repaired/ in full working order.	
7	**Engineer report on integrity is too vague when a specific repair is required (H-1, H-2, H-3)**		Engineers are not trained in report writing and fail to communicate the specific equipment requiring repair, leading to confusion when the repair is then to be completed. Inadequate repair completed due to vague report, resulting in remaining fatigue of the hot box, fatigue of the fuel supply system, or hot surfaces.				Engineer workload too busy that not enough time is dedicated to writing the report therefore it is left vague resulting in inadequate repair of hot box/ fuel supply/ exposed hot surfaces	
8	**Engineer reports on integrity too late when damaged/ degraded equipment remains in place (H-1, H-2, H-3)**						Engineer workload too busy that no time is dedicated to writing the report and the loss of integrity is reported too late.	
9	**Engineer doesn't repair equipment when faulty equipment present (H-1, H-2, H-3)**		Engineer receives feedback that equipment is faulty but does not attend to the failure due to the faulty equipment alarm slipping his/ her mind. Equipment continues to be faulty and over time containment is broken/ excessive hot surfaces continue Company are made aware of a vulnerability associated with a piece of process equipment (i.e. fuel supply connection vulnerability to leak). Instruction is provided down the chain of command to the engineer to implement the solution but this is not implemented due to a perceived low priority status.	No sensor is applied to check for failures of equipment therefore the Engineer is not informed of a faulty/ damaged piece of equipment. No remedial action is therefore taken resulting in a break in containment from weakened equipment/ exposed hot surface due to faulty equipment operation		Feedback shows equipment is faulty. Engineer attends to conduct maintenance but maintains the wrong piece of equipment. Work completed but originally faulty piece of equipment remains. Subsequent feedback suggesting fault remains and is assumed to be a false alarm as the repair has taken place, leading to a break in containment/ hot surface	Faulty condition (i.e. seal gaps in the hot box) becomes normalised. No repair/ replacement carried out.	

10	**Engineer begins repair during operation state (i.e. pressurised) (H-2, H-3)**	Engineer attends operational equipment to conduct maintenance. No indication exists at the equipment that it is operational. Engineer breaks containment while equipment operational		Engineer attends operational equipment to conduct maintenance. Indication exists at the equipment that it is operational. Control room advise equipment is offline. Engineer breaks containment while equipment operational	Engineer attends operational equipment to conduct maintenance. Incorrect indication exists at the equipment that it is not operational due to faulty sensor. Engineer breaks containment while equipment operational	
11	**Engineer repairs equipment but does not complete/ implement the repair correctly (H-1, H-2, H-3)**	Engineer is not informed of the specific requirements of the manufacturer due to information overload of manuals/ data on the machine. Planned maintenance routine does not provide engineer with the instructions of what the manufacturer requires, but rather instruction based on past experience and practice.	Engineer is not trained on the equipment they are instructed to repair. Repair is not adequately completed resulting in break in containment/ excessive operating temperatures Engineer takes a reading of a hot surface incorrectly and insults/ places lagging in the wrong location. Hot surface remains exposed Engineer unaware of how to apply the manufacturer guidelines when checking equipment (i.e. bolts on the fuel supply pipework) due to a lack of qualification/ competence.	The engineer has worked on similar engines before and believe he/she knows the manufacturer requirements. In fact the requirements are different/ have been updated, resulting in a misinterpretation of the requirements.		Engineer begins maintenance but is called to tend to other issues and does not complete the maintenance/ repair. No log exists to prevent activation of the equipment. Incomplete repair results in flammable material release on start-up
12	**Engineer starts repairing equipment before making necessary preparations (H-1, H-2, H-3)**	Approval for the work order takes too long so engineer decides to continue with the repair without approval.	Arrival of other required personnel taking too long so engineer decides to begin the repair due to a lack of knowledge of the risks.		Engineer does not check if the equipment is isolated/ shutdown and begins the repair due to excessive work pressures.	Engineer believes equipment is isolated/ shutdown and due to work pressures, begins the repair.
13	**Engineer repairs equipment too late when damaged/ faulty equipment exists (H-1, H-2, H-3)**		Engineer receives feedback that equipment is faulty but does not attend to the failure due to work approval order. The equipment is brought back online before the engineer can tend to the faulty equipment resulting in a break in containment/ hot surface.			Engineer receives feedback that equipment is faulty but does not attend to the failure due to an extensive workload. The equipment is brought back online before the engineer can tend to the faulty equipment resulting in a break in containment/ hot surface
14	**Engineer starts repair, but doesn't complete when faulty equipment is present (H-1, H-2, H-3)**	Engineer does not have the correct tools or replacement parts to complete the job, therefore the repair is stopped before the fault is rectified.	Engineer begins the repair but comes up against a repair process he/ she is unfamiliar with and stops mid way through.			An emergency elsewhere takes the engineer away from the repair which has been started, meaning the fault is not rectified. Engineer begins maintenance but is called to tend to other issues and does not complete the maintenance/ repair. No log exists to prevent activation of the equipment. Incomplete repair results in flammable material release on start-up
15	**Engineer doesn't shutdown the engine when exposed hot surfaces exist (H-1)**		Engineers are aware of exposed hot surfaces (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. unacceptable pressure in fuel supply pipework, excessive vibration which could cause an imminent rupture), meaning no shutdown action is taken.		Engineers unaware of exposed hot surfaces as there are no sensors to reveal their presence therefore hot surfaces remain exposed.	Engineers are aware of exposed hot surfaces but this is taken as normal, therefore engines remain operational and exposed hot surfaces remain in place.
16	**Engineer doesn't shutdown the engine when strain on the engine components exceeds design threshold (H-2, H-3)**		Engineers are unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces. Training inadequate, therefore engine is not shutdown the moments before a hazard is realised.		No sensors are in place to provide the engineer information on the system operating condition (i.e. excessive fuel supply pressure, vibration etc.) in which a decision can be made to shutdown the engine to prevent the hazards H-1 to H-3.	
17	**Engineer shuts down the engine and does not immediately reduce load on other engines which become temporarily overloaded (H-1, H-2)**		Engineers are unaware of the design loads which could be generated elsewhere by shutting down the engine. Training inadequate, therefore engine is shutdown causing a hazard to be realised elsewhere.		No warnings are in place to advise on the impact of the decision to shutdown the engine on the remainder of the system, therefore action is taken with no knowledge of the effect.	
18	**Engineer shuts down the engine too late when a fuel/ lube oil release exists (H-2, H-3)**				Response time of sensors showing excessive conditions are not designed to provide a fast response alarm. No sensors in place to advise engineer of leak of oil, therefore shutdown relies on CCTV footage check or word from the ER.	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability. Engine shutdown buttons are not easily accessible, delaying the time taken to shutdown the engine.

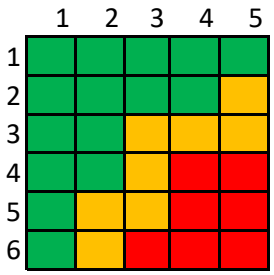
19	**Engineer doesn't release the deluge when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)**			Response time of sensors showing exposed hot surfaces are not designed to provide a fast response alarm.	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.	
					Engine shutdown buttons are not easily accessible, delaying the time taken to shutdown the engine.	
20	**Engineer doesn't shutdown the fuel supply when strain on the components exceeds design threshold (H-2, H-3)**		Engineers are unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces. Training inadequate, therefore fuel supply is not shutdown the moments before a hazard is realised.	No sensors are in place to provide the engineer information on the system operating condition (i.e. excessive fuel supply pressure, vibration etc.) in which a decision can be made to shutdown the engine to prevent the hazards H-1 to H-3.	Manual valve seized shut due to lack of use.	
21	**Engineer shuts down the fuel supply too late when a fuel/ lube oil release exists (H-2, H-3)**		Engine shutdown does not automatically stop supply of fuel to that engine. Engineers unaware of fuel continually being sent to the engine which has been shutdown due to a leak.	No sensors are in place to provide the engineer information on the system operating condition (i.e. low fuel supply pressure indicating a leak), therefore the leak continues until CCTV/ inspection reveals failure		
22	**Engineer doesn't release the deluge when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)**		Engineers unaware that release of the deluge could potentially prevent an ignition. The assumption is prevalent that it should not be used until a fire breaks out.	Engineer is unaware that the combination of exposed hot surfaces and oil leak presents a high threat of fire.	Engineer is unaware of exposed hot surfaces as no sensors are in place to detect them.	Fire in the room damages equipment resulting in incomplete control action, therefore hot surfaces remain in place elsewhere which could cause further escalation.
				Engineer is unaware that the combination of exposed hot surfaces and imminent oil leak presents a high threat of fire.	Engineer is unaware of an imminent oil leak. Engineer is unaware of oil leak in the room.	Valve seized shut due to lack of use.
	Engineer releases the water mist too late when leak exists (H-1).	Engineer prevents the release of the water mist system as they believe the alarms indicating oil leak are false alarms. Water mist only released when further alarms are received.				Water mist release mechanism has been inhibited during maintenance and not brought back online.
	Engineer releases the water mist too late when exposed hot surface exists (H-1)	Engineer prevents the release of the water mist system as they believe the alarms indicating exposed hot surfaces are false alarms. Water mist only released when further alarms are received.				Water mist release mechanism has been inhibited during maintenance and not brought back online.
23	**Engineer stops the deluge too soon when hot exposed surfaces have existed and oil mist in atmosphere is detected/suspected (H-1)**		Engineer believes the deluge will have completed it's job and switches it off, despite the hot surface remaining in place.			

ID-UCA	UCA	ID-CF	Causal factors	ID-FR	Functional requirements	UCA Category	CF Category	Relevant barriers	Signals and their requirements	Hazard (Oil Leak[OL]/ Hot Surface [HS])	Previous occurrence in Incident/ Accident (Y/N) + incident ref	Barrier Effectiveness	Criticality	Magnitude of risk reduction
1	Engineer does not detect loss of integrity during inspection (H-2, H-3)	1.1	Engineer is not aware of what to look for/ what the signs are of loss of integrity due to lack of skills/ knowledge.	1.1.1	Engineers shall be aware of onboard procedures related to equipment integrity, specifically where this can lead to H2-3.	Inadequate detection/ inspection	Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audit of procedural knowledge and compliance.	OL	(Y) - MV Zenith, Sea Gale, Splendour of the Seas, Accident Event 272486, 209564, 189577, 231717, 217752, 269956, 232700, Incident Event 202364, 207329	4	5	20
				1.1.2	Engineers shall be able to recognise hot box and fuel supply pipework/ engine loss of integrity which can lead to H2-3.			Training/ Competence Management System	Audit of Competence.	OL		4	5	20
		1.2	Engineer does not believe it is his/ her responsibility to look for loss of integrity.	1.2.1	Engineers shall be empowered to discuss potential fire hazards and be aware fire prevention is everyone's responsibility when there is a risk of H2-3.		Inadequate knowledge (training/ competence)	Enforcement of responsibility	Audit of process including actions in hypothetical situations.	OL	(Y) - MV Zenith	5	4	20
		1.3	Time constraints on the engineer mean the inspection is only partially completed therefore loss of integrity of the hot box is not found.	1.3.1	Staffing and priorities shall allow for manufacturer/ ship specific inspection to take place when this relates to potential precursors to hazards leading to H-3.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL	(Y) - Carnival Triumph, Accident Event 217752	4	4	16
		1.4	The interval between inspections of the hot box and fuel supply pipework is too lengthy resulting in severe degradation between inspections not being detected.	1.4.1	Manufacturer requirements to prevent H2-3 shall be met.		Inadequate maintenance/ inspection	Work plan/ monitoring system	Log of completed maintenance - verification of compliance with manufacturer requirements. Alarm when manufacturer maintenance intervals are exceeded.	OL	(Y) - Carnival Triumph, Accident Event 275191	4	5	20
				1.4.2	Staffing and priorities shall allow for manufacturer/ ship specific inspection to take place when this relates to potential precursors to hazards leading to H2-3.			Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL		4	5	20
		1.5	Planned maintenance routine requires engineer to carry out inspection but this is not completed as the engineer has too many other tasks assigned and the requirement for inspection slips off the radar and is not followed up.	1.5.1	Staffing shall allow for manufacturer/ ship specific inspection to take place when this relates to potential precursors to hazards leading to H2-3.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL	(Y) - MV Zenith, Sea Gale, Carnival Triumph, Accident Event 275191, 217752	4	5	20
2	Engineer does not detect incorrect implementation of equipment as per manufacturer guidelines during inspection (H-2, H-3)	2.1	Planned maintenance routine does not provide instruction of inspection intervals meaning the engineer does not get tasked with inspecting the equipment.	2.1.1	Task lists for maintenance of the hot box and fuel supply pipework shall account for manufacturer guidelines to prevent H2-3.	Inadequate detection/ inspection	Inadequate maintenance/ inspection	Hot box/ fuel supply pipework inspection/ maintenance procedure	Finalisation of design should include inspection of the maintenance routine and verification of compliance against manufacturer requirement. Audit should ensure maintenance routine is continually applied at required period. Audit of embracing of maintenance management system. Audit of embracing of maintenance management system.	OL	(Y) - Le Boreal, Splendour of the Seas, Carnival Triumph, Accident Event 275191	3	5	15
				2.1.2	Maintenance task list shall be clear and easily followed to prevent H2-3.			Hot box/ fuel supply pipework inspection/ maintenance procedure	Audit of engineer knowledge of maintenance routines and where these come from. Audit of knowledge of where to retrieve the routines. Audit of embracing of maintenance management system.	OL		3	5	15
		2.2	The tools available to the engineer are insufficient to detect integrity loss of the fuel supply pipework i.e. no torque wrench to verify torque level of the bolts.	2.2.1	Specific tools shall be available where manufacturer specifications require such tools to prevent H2-3.		Inadequate resources	Tooling and spares procedure	Audit of engineer awareness of tools for specific tasks and how to use them. Audit of on board availability of tools. Audit of embracing of maintenance management system.	OL	(Y) - Splendour of the Seas, Accident Event 190434	3	4	12
3	Engineer interferers with equipment and doesn't return to its original condition during inspection (H-1, H-2, H-3)	3.1	Engineer does not have the training/ skillset to adequately understand the impact of interfering with equipment to get a closer inspection, resulting in continued hot surface exposure, or damaged/ fatigued equipment.	3.1.1	Engineers shall be capable of returning equipment back into service in a safe state to prevent H1-3.	Inadequate maintenance / repair	Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS	(Y) - Splendour of the Seas, Accident Event 207584	4	5	20
4	Engineer inspects equipment too late to find damaged/ degraded equipment (H-1, H-2, H-3)	4.1	Planned maintenance routine does not provide instruction of inspection intervals meaning the engineer does not get tasked with inspecting the equipment on time to detect dangerous fatigue.	4.1.1	Task lists for maintenance of the hot box and fuel supply pipework shall be based directly from manufacturer guidelines to prevent H2-3.	Inadequate detection/ inspection	Inadequate maintenance and operations	Hot box/ fuel supply pipework inspection/ maintenance procedure	Finalisation of design should include inspection of the maintenance routine and verification of compliance against manufacturer requirement. Audit should ensure maintenance routine is continually applied at required period. Audit of embracing of maintenance management system.	OL	(Y) - Le Boreal, MV Zenith, Sea Gale, Splendour of the Seas, Carnival Triumph, Accident Event 275191	3	5	15
				4.1.2	Maintenance tasks there to prevent H1-3 shall be clearly instructed to engineers.			Hot box/ fuel supply pipework inspection/ maintenance procedure	Audit of engineer knowledge of maintenance routines and where these come from. Audit of knowledge of where to retrieve the routines. Audit of embracing of maintenance management system.	OL + HS		3	5	15
		4.2	Engineer workload too full resulting in critical inspection being delayed resulting in damaged equipment remaining in place.	4.2.1	Staffing and priorities shall allow for manufacturer/ ship specific inspection to take place when this relates to potential precursors to hazards leading to H1-3.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS	(Y) - MV Zenith, Sea Gale, Carnival Triumph, Accident Event 217752	4	4	16
5	Engineer does not complete inspection when hot surfaces or damaged/ degraded equipment present (H-1, H-2, H-3)	5.1	Planned maintenance routine/ work instruction did not specifically call out the requirement to check for damaged fuel supply pipework or exposed hot surfaces.	5.1.1	Instructions relating to inspection of equipment posing a risk of H1-3 shall specifically address H1-3.	Inadequate detection/ inspection	Inadequate maintenance and operations	Hot box/ fuel supply pipework inspection/ maintenance procedure. Hot surface inspection procedure.	Audit of contends of maintenance routines. Audit of engineer compliance with the routines. Audit of embracing of maintenance management system.	OL + HS	(Y) - MV Zenith, Splendour of the Seas, Carnival Triumph, Accident Event 217752	3	5	15
		5.2	Engineer does not have training on how to complete a check and therefore does not complete it.	5.2.1	Engineers shall be aware of what an unsafe condition of equipment is which can lead to H1-3 and how to recognise this		Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence.	OL + HS	(Y) - MV Zenith, Accident Event 269956, Incident Event 202364	4	5	20
		5.3	Engineer believes the inspection is complete but is unaware of additional checks which are required.	5.3.1	Instructions relating to inspection of equipment posing a risk of H1-3 shall be specific and complete.		Inadequate knowledge (training/ competence)	Hot box/ fuel supply pipework inspection/ maintenance procedure. Hot surface inspection procedure.	Audit of contends of maintenance routines. Audit of engineer compliance with the routines. Audit of embracing of maintenance management system.	OL + HS	(Y) - Le Boreal	3	5	15
		5.4	Engineer is called to complete another task, meaning the inspection is not completed.	5.4.1	Staffing and priorities shall allow for inspection to take place when this relates to H1-3.		Inadequate operational contextual awareness	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS	(Y) - MV Zenith, Sea Gale, Accident Event 217752	4	4	16
				5.4.2	Equipment, posing a risk of H1-3, where inspection has not been completed shall remain an active task until complete.			Permit to work procedure	Audit of procedures can be the signal of performance. Indicator showing fault which requires acknowledgement	OL + HS		4	4	16
6	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)	6.1	Engineers are not trained in report writing and fail to communicate the loss of integrity to the hierarchy meaning management are unaware of fatigue to the hot box, fatigue of the fuel supply system, or hot surfaces.	6.1.1	Engineers shall be aware of how to present clear and concise reports relating to work or equipment posing a risk of H1-3.	Inadequate reporting to management	Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS		4	3	12
				6.1.2	Engineers shall be aware of what is a safety critical maintenance requirement in preventing H1-3.			Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS		4	3	12
		6.2	Engineers are instructed of a required upgrade. The work is carried out in an uncontrolled/ undocumented way. Company are unaware of what equipment is upgraded/ what is outstanding.	6.2.1	Repair/ upgrade work which breaks containment or replaces a part where this creates a risk of H1-3 shall have the change logged.		Inadequate maintenance and operations	Change management system	Audit of report writing compliance. Audit of embracing of maintenance management system.	OL + HS		3	3	9
				6.2.2	Staffing and priorities shall allow for report writing to take place when this relates to potential precursors to hazards leading to H1-3.			Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
		6.3	Engineer inspects the equipment, registers the loss of integrity of the hot box but is not aware that this presents the risk of H-3, therefore does not take or recommend action to fix.	6.3.1	Engineers shall be familiar with what can lead to a hazard with respect to the hot box, leading to H-3.		Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence.	OL	(Y) - MV Zenith, Splendour of the Seas	4	5	20
		6.4	Engineer inspects the equipment, registers the loss of integrity of the fuel supply pipework but is not aware that this presents the risk of H-2, therefore does not take or recommend action to fix.	6.4.1	Engineers shall be familiar with what can lead to a hazard with respect to the fuel supply pipework, leading to H-2.			Training/ Competence Management System	Audit of Competence.	OL	(Y) - MV Zenith	4	5	20
		6.5	Engineer workload too busy that no time is dedicated to writing the report and the loss of integrity is not reported.	6.5.1	Staffing and priorities shall allow for report writing to take place when this relates to H1-3.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
		6.6	Engineer workload too busy that no time is dedicated to writing the report therefore hierarchy are unaware of project completion status. Decisions are therefore made based on the assumption that equipment is repaired/ in full working order.	6.6.1	Staffing and priorities shall allow for report writing to take place when this relates to H1-3.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
7	Engineer report on integrity is too vague when a specific repair is required (H-1, H-2, H-3)	7.1	Engineers are not trained in report writing and fail to communicate the specific equipment requiring repair, leading to confusion when the repair is then to be completed. Inadequate repair completed due to vague report, resulting in remaining fatigue of the hot box, fatigue of the fuel supply system, or hot surfaces.	7.1.1	Engineers shall be aware of how to provide clear and concise reports relating to work or equipment posing a risk of H1-3.	Inadequate reporting to management	Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS		4	3	12
		7.2	Engineer workload too busy that not enough time is dedicated to writing the report therefore it is left vague resulting in inadequate repair of hot box/ fuel supply/ exposed hot surfaces	7.2.1	Staffing and priorities shall allow for report writing to take place when this relates to H1-3.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
8	Engineer reports on integrity too late when damaged/ degraded equipment remains in place (H-1, H-2, H-3)	8.1	Engineer workload too busy that no time is dedicated to writing the report and the loss of integrity is reported too late.	8.1.1	Staffing and priorities shall allow for report writing to take place when this relates to H1-3.	Inadequate reporting to management	Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
9	Engineer doesn't repair equipment when faulty equipment present (H-1, H-2, H-3)	9.1	Engineer receives feedback that equipment is faulty but does not attend to the failure due to the faulty equipment alarm slipping his/ her mind. Equipment continues to be faulty and over time containment is broken/ excessive hot surfaces continue	9.1.1	Feedback from equipment indicating a fault which could lead to H1-3 shall not be ignored with no action.	Inadequate detection/ inspection	Inadequate task management	Visual indicator (e.g. lagging worn exposing hot surface); Safety procedure	Indicator showing fault. Requires action to silence. Can only be inhibited 'x' number of times.	OL + HS		3	2	6
				9.1.2	When a fault is identified which can lead to H1-3, inspection shall be completed within a time period related to the criticality/ risk posed from the equipment.			Maintenance/ inspection procedure	Audit of procedures and review of maintenance logs can be the signal of performance.	OL + HS		4	2	8
		9.2	Company are made aware of a vulnerability associated with a piece of process equipment (i.e. fuel supply connection vulnerability to leak). Instruction is provided down the chain of command to the engineer to implement the solution but this is not implemented due to a perceived low priority status.	9.2.1	When equipment vulnerability can lead to H1-3 and a known mitigating factor is provided, this shall be implemented.		Inadeqtate corporate risk perception	Equipment Maintenance/ Manufacturer Compliance Procedure	Audit of procedures and review of maintenance logs can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS		4	2	8
		9.3	No sensor is applied to check for failures of equipment therefore the Engineer is not informed of a faulty/ damaged piece of equipment. No remedial action is therefore taken resulting in a break in containment from weakened equipment/ exposed hot surface due to faulty equipment operation	9.3.1	System shall be able to monitor real time health status of engine and fuel supply system, providing alarms when faults which can lead to H1-3 occur.	Inadequate maintenance/ repair	Inadequate feedback of equipment status/ health	Sensors monitoring health of a system; visual indicators (e.g. fuel filters are clogged)	Indication of health status (including pressure, temperature, load) at x frequency; alert/ alarm when a fault condition is presented.	OL + HS	MV Zenith, Audit Safety Event 273004, Accident Event 198060, 205791, 192706	3	5	15
				9.3.2	Inspection of equipment posing a risk of H1-3 shall be inspected at a frequency stated in the maintenance routine, based on the risk posed from equipment.			Equipment Inspection/ Manufacturer Compliance Procedure	Audit of procedures and review of maintenance logs can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS		3	5	15
		9.4	Feedback shows equipment is faulty. Engineer attends to conduct maintenance but maintains the wrong piece of equipment. Work completed but originally faulty piece of equipment remains. Subsequent feedback suggesting fault remains and is assumed to be a false alarm as the repair has taken place, leading to a break in containment/ hot surface	9.4.1	Design of safety critical equipment shall distinctly indicate (passively and actively) its health status to prevent H2-3.		Inadequate knowledge (training/ competence)	Visual indicator (e.g. fuel filters have a clogging indicator),	Indicator reading at x frequency. Where the indicator relates to a direct fire precursor, this should be presented accordingly.	OL		3	5	15
				9.4.2	When a fault is identified which can lead to H1-3, that equipment shall be easily identifiable for repair.			Equipment tagging procedure	Audit of procedures can be the signal of performance.	OL + HS		4	4	16
				9.4.3	When a fault is identified which can lead to H1-3, engineers shall only maintain equipment that is faulty.			Permit to work procedure	Results of assessment of engineers on their knowledge of safety procedures can be recorded as the barrier signal. Assessment is done every x weeks	OL + HS	Audit Safety Event 273004	4	4	16
				9.4.4	Fault detection of safety critical equipment which can lead to H1-3 shall maintain frequency of false alarms that does not degrade confidence in the system from engineers.			Safety critical equipment reliability	IEC61508/ proven in use audits can be used to signal performance.	OL + HS		3	5	15

		9.5	Faulty condition (i.e. seal gaps in the hot box) becomes normalised. No repair/ replacement carried out.	9.5.1	Engineers shall be aware of what an unsafe condition of equipment is which can lead to H1-3.		Inadequate appreciation/ comprehension of risk	Training/ Competence Management System	Audit of Competence.	OL + HS	(Y) - MV Zenith, Sea Gale, Splendour of the Seas	4	5	20
				9.5.2	Engineers shall be free to question suitability of situations which may lead to H1-3, even if it has 'always been this way'.			Forum for open comminucation	Audit of process including actions in hypothetical situations.	OL + HS		5	4	20
		10.1	Engineer attends operational equipment to conduct maintenance. No indication exists at the equipment that it is operational. Engineer breaks containment while equipment operational	10.1.1	Design of safety critical equipment shall distinctly indicate (passively and actively) its operational status to prevent H2-3.		Inadequate feedback of equipment status/ health	Visual indicator (e.g. engine operational)	Indicator reading in real time.	OL	(Y) - Le Boreal	3	5	15
10	Engineer begins repair during operation state (i.e. pressurised) (H-2, H-3)	10.2	Engineer attends operational equipment to conduct maintenance. Indication exists at the equipment that it is operational. Control room advise equipment is offline. Engineer breaks containment while equipment operational	10.2.1	Sensors indicating operational status shall have a reliability up time of 99%-99.9% (SIL2) to prevent H2-3.	Inadequate maintenance/ repair	Inadequate feedback between equipment, personnel in the ER and the ECR	Safety critical equipment operational procedure	IEC61508/ proven in use audits can be used to signal performance. Audit of embracing of maintenance management system.	OL		4	3	12
				10.2.2	Where conflict between feedback exists, work shall stop pending further investigation to prevent H2-3.			Permit to work procedure	Communication channel between control room and engineer must exist, with engineers empowered to stop the job. Audit of embracing of maintenance management system.	OL		4	3	12
		10.3	Engineer attends operational equipment to conduct maintenance. Incorrect indication exists at the equipment that it is not operational due to faulty sensor. Engineer breaks containment while equipment operational	10.3.1	Sensors indicating operational status shall have a reliability up time of 99%-99.9% (SIL2) to prevent H2-3.		Inadequate feedback of equipment status/ health	Safety critical equipment operational procedure	IEC61508/ proven in use audits can be used to signal performance. Audit of embracing of maintenance management system.	OL		4	2	8
		11.1	Engineer is not informed of the specific requirements of the manufacturer due to information overload of manuals/ data on the machine.	11.1.1	Instructions on hazard prevention of H1-3 shall be specific and clear.		Inadequate maintenance procedures	Generation of task specific, clear instruction.	Audit of capability and task instruction.	OL + HS	(Y) - Carnival Triumph	4	5	20
		11.2	Planned maintenance procedure does not provide engineer with the instructions of what the manufacturer requires, but rather instruction based on past experience and practice.	11.2.1	Instruction shall be based on the manufacturer guidance in preventing H1-3.		Inadequate maintenance and operations	Maintenance procedure being based on manufacturer guidance	Audit of procedural compliance. Alarm required if audit shows poor practice against what is specified by manufacturer.	OL + HS	(Y) - Carnival Triumph, Accident Event 275191	4	5	20
		11.3	Engineer is not trained on the equipment they are instructed to repair. Repair is not adequately completed resulting in break in containment/ excessive operating temperatures	11.3.1	Ship engineers shall be familiar with equipment which poses a risk of H1-3.		Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audits should be used to monitor engineers have the necessary training.	OL + HS	(Y) - Le Boreal	4	5	20
				11.3.2	Tasks posing a risk of H1-3 shall only be assigned which are within the capability of engineers assigned the task.			Training/ Competence Management System	Training records must be updated with competence gained. Task assigners must have knowledge of the core competence before assigning tasks. Audits can monitor signal performance.	OL + HS		4	5	20
		11.4	Engineer takes a reading of a hot surface incorrectly and insulates/ places lagging in the wrong location. Hot surface remains exposed	11.4.1	During inspection relating to the prevention of H-1, engineer shall be able to verify the exact location of the hot surface.		Inadequate knowledge (training/ competence)	Hot surface inspection procedure	Audit of performance can be the signal of compliance.	HS		4	3	12
				11.4.2	Engineer shall be able to use the equipment appropriately in carrying out this inspection H-1.			Training/ Competence Management System	Audits should be used to monitor engineers have the necessary training.	HS		4	3	12
11	Engineer repairs equipment but does not complete/ implement the repair correctly (H-1, H-2, H-3)	11.5	Engineer unaware of how to apply the manufacturer guidelines when checking equipment (i.e. bolts on the fuel supply pipework) due to a lack of qualification/ competence.	11.5.1	Engineers shall be familiar with equipment on board where a risk of H1-3 exists and trained on all potential actions required to be made on that equipment.	Inadequate maintenance/ repair	Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence. Alarm when equipment on board which an engineer is unable to address.	OL + HS		4	2	8
		11.6	The engineer has worked on similar engines before and believe he/she knows the manufacturer requirements. In fact the requirements are different/ have been updated, resulting in a misinterpretation of the requirements.	11.6.1	Actions/ maintenance shall always be based on the manufacturer guidance, regardless of experience level and experience on other equipment where a risk of H1-3 exists.		Inadequate knowledge (training/ competence)	Maintenance procedure being based on manufacturer guidance	Audit of procedural compliance. Alarm required if audit shows poor practice against what is specified by manufacturer.	OL + HS	(Y) - Carnival Triumph, Accident Event 275191	4	5	20
		11.7	Engineer begins maintenance but is called to tend to other issues and does not complete the maintenance/ repair. No log exists to prevent activation of the equipment. Incomplete repair results in flammable material release on start-up	11.7.1	Tasks which increase the risk of H1-3 shall only be assigned when the engineer has availability to complete them.		Inadequate operational contextual awareness	Adequate staffing and task allocation	Audit of procedures can be the signal of performance.	OL + HS		4	4	16
				11.7.2	Engineers shall not leave the job site until the job is complete where this could result in H1-3, unless in the case of an emergency.			Permit to work procedure	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS		4	4	16
				11.7.3	If a job remains unfinished, equipment shall be made safe and records shall be maintained to show the job is unfinished. Unfinished repair shall be marked accordingly (e.g. lockout-tagout / LOTO)			Permit to work procedure	Audit of procedures can be the signal of performance.	OL + HS	(Y) - Accident Event 217752	4	4	16
				11.7.4	Staffing shall allow for planned maintenance of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.			Adequate staffing and task allocation	Audit of performance can be the signal of compliance.	OL + HS		4	4	16
		12.1	Approval for the work order takes too long so engineer decides to continue with the repair without approval.	12.1.1	No work which will result in an increase of risk of H1-3 shall take place prior to work order approval.		Inadequate appreciation/ comprehension of risk	Permit to work procedure	Audit of procedures can be the signal of performance.	OL + HS		4	2	8
		12.2	Arrival of other required personnel taking too long so engineer decides to begin the repair due to a lack of knowledge of the risks.	12.2.1	Work shall not begin until all required personnel are present to avoid H-2.		Inadequate knowledge (training/ competence)	Permit to work procedure	Audit of procedures can be the signal of performance.	OL	(Y) - Le Boreal, Freedom of the Seas, Audit Safety Event 188275, 191114, Accident Event 268034, 218465	4	4	16
12	Engineer starts repairing equipment before making necessary preparations (H-1, H-2, H-3)			12.2.2	Engineers shall be aware of what can lead to an unsafe condition of equipment leading to H1-3 during repair and the reasons for the requirements within the permit to work.	Inadequate maintenance/ repair		Training/ Competence Management System	Audit of Competence.	OL + HS		4	5	20
		12.3	Engineer does not check if the equipment is isolated/ shutdown and begins the repair due to excessive work processes.	12.3.1	Staffing shall allow for repairs of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.		Inadequate appreciation/ comprehension of risk	Adequate staffing and task allocation	Audit of performance can be the signal of compliance.	OL + HS		4	3	12
		12.4	Engineer believes equipment is isolated/ shutdown and due to work pressures, begins the repair.	12.4.1	Staffing shall allow for repairs of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.		Inadeqtate resource provision	Adequate staffing and task allocation	Audit of performance can be the signal of compliance.	OL + HS		4	3	12
		13.1	Engineer receives feedback that equipment is faulty but does not attend to the failure due to work approval order. The equipment is brought back online before the engineer can tend to the faulty equipment resulting in a break in containment/ hot surface.	13.1.1	Approval of safety critical work related to a risk of H1-3 shall be prioritised to ensure swift repair is carried out.		Inadequate lockout/ inhibit of faulty equipment	Maintenance prioritisation procedure	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS		4	3	12
				13.1.2	When a fault is identified which can lead to H1-3, equipment shall be taken out of service. Equipment shall not be capable of reintroduction until fault is acknowledged/ rectified.			Hazardous equipment operation procedure	Audit of procedures can be the signal of performance. Indicator showing fault which requires acknowledgement	OL + HS		4	3	12
13	Engineer repairs equipment too late when damaged/ faulty equipment exists (H-1, H-2, H-3)			13.2.1	Tasks which increase the risk of H1-3 shall only be assigned when the engineer has availability to complete them.	Inadequate maintenance/ repair		Adequate staffing and task allocation	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS		4	2	8
		13.2	Engineer receives feedback that equipment is faulty but does not attend to the failure due to an extensive workload. The equipment is brought back online before the engineer can tend to the faulty equipment resulting in a break in containment/ hot surface	13.2.2	Staffing shall allow for planned maintenance of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.		Inadequate lockout/ inhibit of faulty equipment	Adequate staffing and task allocation	Audit of performance can be the signal of compliance.	OL + HS		4	2	8
				13.2.3	Equipment shall not be capable of reintroduction of equipment which poses a risk of H1-3 until fault is acknowledged/ rectified.			Hazardous equipment operation procedure	Audit of procedures can be the signal of performance. Indicator showing fault which requires acknowledgement	OL + HS		4	2	8
				13.2.4	Sign-off of work which if not completed could result in H1-3 shall be signed off as a priority.			Adequate staffing and task allocation	Audit of procedures and KPIs can be the signal of performance.	OL + HS		4	2	8
		14.1	Engineer does not have the correct tools or replacement parts to complete the job, therefore the repair is stopped before the fault is rectified.	14.1.1	Inventories shall be kept stocked with spares holding to allow for unforeseen circumstances and repair work required while at sea to equipment posing a risk of H1-3 (o-rings, bolts, fittings, lagging).		Inadeqtate resource provision	Tooling and spares procedure	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS	(Y) - Carnival Triumph, Audit Safety Event 273012, Accident Event 190434	4	4	16
				14.2.1	Tasks shall only be assigned when the engineer has availability to complete them with fire prevention tasks preventing H1-3 taking priority, unless otherwise instructed by chief engineer.			Adequate staffing and task allocation	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS		4	2	8
		14.2	Engineer begins the repair but comes up against a repair process he/ she is unfamiliar with and stops mid way through.	14.2.2	Engineers shall be familiar with equipment on board which poses a risk of H1-3 and trained on all potential actions required to be made on that equipment.		Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence. Alarm when equipment on board which an engineer is unable to address.	OL + HS		4	3	12
				14.2.3	If a job remains unfinished, equipment shall be made safe and records shall be maintained to show the job is unfinished. Unfinished repair shall be marked accordingly (e.g. lockout-tagout / LOTO)			Permit to work procedure	Audit of procedures can be the signal of performance.	OL + HS		4	2	8
				14.3.1	Equipment shall not be reintroduced until fault which can lead to H1-3 is rectified.		Inadequate operational contextual awareness	Hazardous equipment operation procedure	Audit of procedures can be the signal of performance. Indicator showing fault which requires acknowledgement	OL + HS		4	3	12
14	Engineer starts repair, but doesn't complete when faulty equipment is present (H-1, H-2, H-3)	14.3	An emergency elsewhere takes the engineer away from the repair which has been started, meaning the fault is not rectified.	14.3.2	Staffing shall allow for planned maintenance of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.	Inadequate maintenance/ repair		Adequate staffing and task allocation	Audit of performance can be the signal of compliance.	OL + HS		4	2	8
				14.4.1	Tasks related to equipment posing a risk of H1-3 shall only be assigned when the engineer has availability to complete them.			Adequate staffing and task allocation	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS		4	2	8
		14.4	Engineer begins maintenance but is called to tend to other issues and does not complete the maintenance/ repair. No log exists to prevent activation of the equipment. Incomplete repair results in flammable material release on start-up	14.4.2	Engineers shall not leave the job site until the job is complete where the equipment being worked on poses a risk of H1-3 unless in the case of an emergency or planned work interruption (i.e. end of shift, permit to work pause).		Inadequate operational contextual awareness	Permit to work procedure	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	OL + HS		4	2	8
				14.4.3	If a job remains unfinished, equipment shall be made safe and records shall be maintained to show the job is unfinished. Unfinished repair shall be marked accordingly (e.g. lockout-tagout / LOTO)			Permit to work procedure	Audit of procedures can be the signal of performance.	OL + HS		4	2	8
				14.4.4	Staffing shall allow for planned maintenance of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.			Adequate staffing and task allocation	Audit of performance can be the signal of compliance.	OL + HS		4	2	8
		15.1	Engineers are aware of exposed hot surfaces (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. oil leak, unacceptable pressure in fuel supply pipework, excessive vibration which could cause an imminent rupture), meaning no shutdown action is taken.	15.1.1	System shall be able to detect and alarm to pressure in excess of the manufacturer specification in the fuel supply system, and vibration in excess of the manufacturer specification which could indicate the presence of or potential for H2-3.		Inadequate knowledge (training/ competence)	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - MV Zenith, Splendour of the Seas, Accident Event 207960, 231717, 224659, Incident Event 202364	3	5	15
				15.1.2	System to detect oil leaks in the hot box and the engine room shall be provided (H2-3).			Safety Instrumented System	Diagnostics showing sensor health status.	OL		3	5	15
15	Engineer doesn't shutdown, stop or remove the engine from service when exposed hot surfaces exist (H-1)			15.1.3	Engineers shall be aware of precursors which can lead to H2-3 and when shutdown of the engine should take place when coupled with H-1.	Inadequate incident response		Engine operation procedure	Audits should be used to monitor engineers have the necessary training.	OL + HS		4	5	20
		15.2	Engineers unaware of exposed hot surfaces as there are no sensors to reveal their presence therefore hot surfaces remain exposed.	15.2.1	System shall be able to provide alarms in high risk areas to the presence of H-1.		Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Thermal sensors with diagnostics showing sensor health status.	HS	(Y) - Le Boreal, MV Zenith, Splendour of the Seas, Carnival Triumph. Accident Event 269956	3	5	15
				15.2.2	System shall be in place to flag up and record presence of H-1.			Hot surface inspection procedure	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	HS		4	5	20
		15.3	Engineers are aware of exposed hot surfaces but this is taken as normal, therefore engines remain operational and exposed hot surfaces remain in place.	15.3.1	Engineers shall be aware of the requirements of SOLAS regarding the presence of H-1.		Inadequate appreciation/ comprehension of risk	SOLAS/ safety training	Audit of attitude and compliance.	HS	Incident Event 202364	5	5	25

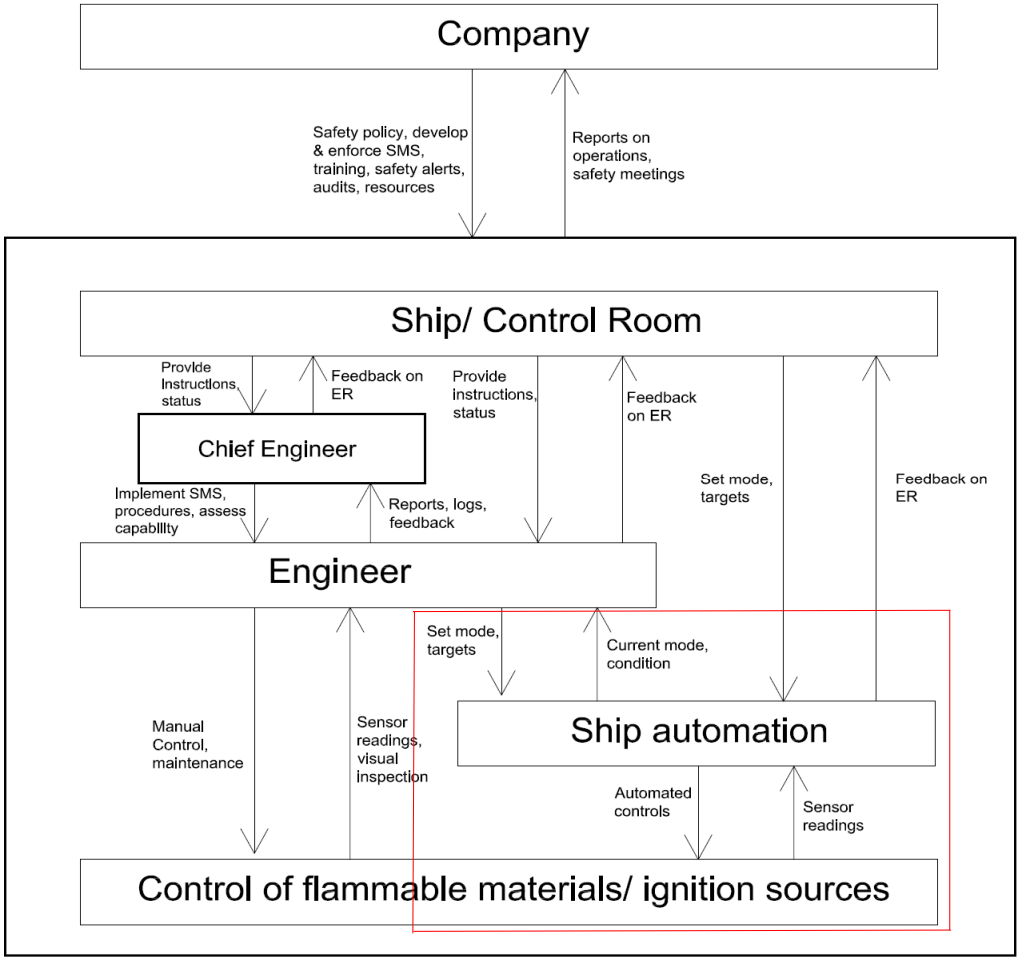
16	Engineer doesn't shutdown or stop the engine when strain on the engine components exceeds design threshold (H-2, H-3)	16.1	Engineers are unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces. Training inadequate, therefore engine is not shutdown the moments before a hazard is realised.	16.1.1	Engineers shall be aware of precursors to engine failure which can lead to H1-3 and when shutdown of the engine should take place.	Inadequate incident response	Inadequate knowledge (training/ competence)	Training/ Competence Management System.	Audits should be used to monitor engineers have the necessary training.	OL	(Y) - Sea Gale, Accident Event 210991, 222338	4	5	20
		16.2	No sensors are in place to provide the engineer information on the system operating condition (i.e. excessive fuel supply pressure, vibration etc.) in which a decision can be made to shutdown the engine to prevent the hazards H-1 to H-3.	16.2.1	System shall be capable of detecting a potentially unsafe operating condition for fuel/ oil pressure, temperature, flow rate, vibration and engine power output/ load which can lead to H2-3.		Inadequate feedback of equipment status/ health	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Splendour of the Seas, Carnival Triumph, Accident Event 198060, 210991, 222338, 192706	3	5	15
17	Engineer shuts down the engine and does not immediately reduce load on other engines which become temporarily overloaded (H-1, H-2)	17.1	Engineers are unaware of the design loads which could be generated elsewhere by shutting down the engine. Training inadequate, therefore engine is shutdown causing a hazard to be realised elsewhere.	17.1.1	Engineers shall be aware of the impact of shutting down an engine on other systems where this could lead to increased risk of H2-3 elsewhere.	Inadequate incident response	Inadequate knowledge (training/ competence)	Training/ Competence Management System.	Audits should be used to monitor engineers have the necessary training.	OL		4	3	12
		17.2	No warnings are in place to advise on the impact of the decision to shutdown the engine on the remainder of the system, therefore action is taken with no knowledge of the effect.	17.2.1	Where an engine is to be shutdown remotely, system should be in place to monitor and advise of the impact of shutdown (H2-3). Engine shutdown directly in the ER shall remain unaffected and is to be used in an emergency.		Inadequate feedback of equipment status/ health	Safety Instrumented System	Diagnostics showing sensor health status. Sensors produce an overall risk level which updates based on projections should a DG be shutdown. Health shall be monitored against manufacturer provided tolerances (i.e. pressure in the fuel supply system shall not exceed xbar/psi)	OL	(Y) - Accident Event 210991, 222338	3	5	15
18	Engineer shuts down the engine too late when a fuel/ lube oil release exists (H-2, H-3)	18.1	Response time of sensors showing excessive conditions are not designed to provide a fast response alarm.	18.1.1	Any sensors which are in place to detect anomalies in engine conditions which could lead to a H-2 (fuel/ oil pressure, temperature, flow) shall be fast response and shall present the alarm and reading to engineers in real time.	Inadequate incident response	Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Accident Event 192706	3	5	15
		18.2	No sensors in place to advise engineer of leak of oil, therefore shutdown relies on CCTV footage check or word from the ER.	18.2.1	System to detect oil leaks in the hot box and the engine room shall be provided (H2-3).		Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Le Boreal, MV Zenith, Splendour of the Seas, Accident Event 207960, 231717, 224659, Incident Event 202364	3	5	15
		18.3	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.	18.3.1	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.		Inadequate safety system design	Emergency shutdown Procedure	Function testing of the shutdown valves at regular intervals. Function testing of fuel pump shutdown. Results of this testing can provide a reliability value which can be taken into account on the overall risk ranking.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph	2	5	10
		18.4	Engine shutdown buttons are not easily accessible, delaying the time taken to shutdown the engine.	18.4.1	Access to the emergency push buttons for both engine shutdown and fuel supply shutdown shall be accessible from multiple locations/ directions from the engine to prevent or mitigate H2-3.		Inadequate safety system design	Emergency shutdown Procedure	Design review of the locations. Maintenance of the pushbuttons to ensure safe operation.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph, Audit Safety Event 191114	2	4	8
19	Engineer doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	19.1	Response time of sensors showing exposed hot surfaces are not designed to provide a fast response alarm.	19.1.1	Any sensors which are in place to detect H-1 shall be fast response and shall present the alarm to engineers in real time.		Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Diagnostics showing sensor health status.	HS		3	3	9
		19.2	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.	19.2.1	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.	Inadequate incident response	Inadequate safety system design	Emergency shutdown Procedure	Function testing of the shutdown valves at regular intervals. Function testing of fuel pump shutdown. Results of this testing can provide a reliability value which can be taken into account on the overall risk ranking.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph	2	5	10
		19.3	Engine shutdown buttons are not easily accessible, delaying the time taken to shutdown the engine.	19.3.1	Access to the emergency push buttons for both engine shutdown and fuel supply shutdown shall be accessible from multiple locations/ directions from the engine to prevent or mitigate H2-3.		Inadequate safety system design	Emergency shutdown Procedure	Design review of the locations. Maintenance of the pushbuttons to ensure safe operation.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph, Audit Safety Event 191114	2	4	8
20	Engineer doesn't shutdown or stop the fuel supply when strain on the components exceeds design threshold (H-2, H-3)	20.1	Engineers are unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces. Training inadequate, therefore fuel supply is not shutdown the moments before a hazard is realised.	20.1.1	Engineers shall be aware of precursors which can lead to H-2, and when shutdown of the supply should take place.		Inadequate knowledge (training/ competence)	Training procedure	Audits should be used to monitor engineers have the necessary training.	OL	(Y) - Splendour of the Seas, Accident Event 210991, 222338	4	5	20
		20.2	No sensors are in place to provide the engineer information on the system operating condition (i.e. excessive fuel supply pressure, vibration etc.) in which a decision can be made to shutdown the engine to prevent the hazards H-1 to H-3.	20.2.1	System shall be able to detect and alarm at the point a manufacturer stated operating condition is breached for fuel/ oil pressure, temperature, flow rate, vibration and engine power output/ load to prevent H-2.	Inadequate incident response	Inadequate feedback of equipment status/ health	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Splendour of the Seas, Carnival Triumph, Accident Event 198060, 210991, 222338, 192706	3	5	15
		20.3	Manual valve seized shut due to lack of use.	20.3.1	Shut off valves used to prevent or mitigate H2-3 shall be subject to operation and inspection during maintenance as per manufacturer recommendation.		Inadequate maintenance and operations	Physical barrier function test procedure	Audit of procedures and review of maintenance logs can be the signal of performance. Audit of embracing of maintenance management system.	OL	(Y) - Splendour of the Seas, Carnival Triumph, Accident Event 207612	4	5	20
21	Engineer shuts down the fuel supply too late when a fuel/ lube oil release exists (H-2, H-3)	21.1	Engine shutdown does not automatically shutdown supply of fuel to that engine. Engineers unaware of fuel continually being sent to the engine which has been shutdown due to a leak.	21.1.1	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.	Inadequate incident response	Inadequate safety system design	Emergency shutdown procedure	Function testing of the shutdown valves at regular intervals. Function testing of fuel pump shutdown. Results of this testing can provide a reliability value which can be taken into account on the overall risk ranking.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph, Accident Event 224659	2	5	10
		21.2	No sensors are in place to provide the engineer information on the system operating condition (i.e. low fuel supply pressure indicating a leak), therefore the leak continues until CCTV/ inspection reveals failure	21.2.1	System shall be capable of detecting pressure outwith manufacturer specification indicative of increased risk of H2-3 in the fuel supply pipework, and oil leaks shall be detectable in the hot box and in the ER (H2-3).		Inadequate feedback of equipment status/ health	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Splendour of the Seas, Accident Event 231717, 224659, Incident Event 202364	3	5	15
22	Engineer doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	22.1	Engineers unaware that release of the water mist could potentially prevent an ignition. The assumption is prevalent that it should not be used until a fire breaks out.	22.1.1	Engineers shall be aware of how to use the water mist system, and where it can assist in the elimination of H-1 when a leak or break in containment is likely/ has occurred.		Inadequate knowledge (training/ competence)	Training procedure/ Emergency procedure	Diagnostics showing sensor health status which can flag a potentially imminent break in containment/ or presence of fuel/ oil mist. Audit of engineer training and knowledge of water mist release.	HS	(Y) - Accident Event 224659, Incident Event 202364, Carnival Triumph, Splendour of the Seas [specifically referenced in the incident report that water mist release could have prevented the fire in the first place]	4	5	20
		22.2	Engineer is unaware that the combination of exposed hot surfaces and oil leak presents a high threat of fire.	22.2.1	Engineers shall be able to recognise the dangers associated with exposed hot surfaces (H-1) and presence of an oil leak (H2-3).		Inadequate knowledge (training/ competence)	Training/ Competence Management System. Alarm management procedure.	Audit of Competence. Diagnostics showing sensor health status which can flag a potentially imminent break in containment/ or presence of fuel/ oil mist. Audit of engineer training and knowledge of water mist release.	OL		4	3	12
		22.3	Engineer is unaware that the combination of exposed hot surfaces and imminent oil leak presents a high threat of fire.	22.3.1	Engineers shall be able to recognise the dangers associated with exposed hot surfaces (H-1) and the likelihood of imminent presence of an oil leak (H2-3).		Inadequate knowledge (training/ competence)	Training/ Competence Management System. Alarm management procedure.	Audit of Competence. Diagnostics showing sensor health status which can flag a potentially imminent break in containment/ or presence of fuel/ oil mist. Audit of engineer training and knowledge of water mist release.	OL		4	3	12
		22.4	Engineer is unaware of exposed hot surfaces as no sensors are in place to detect them.	22.4,1	System shall be able to provide alarms in high risk areas of the presence of H-1.	Inadequate incident response	Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Diagnostics showing sensor health status.	HS	(Y) - Splendour of the Seas, Accident Event 269956	3	5	15
				22.4.2	Inspection shall be conducted to flag up and record any risk of H-1.			Hot surface inspection procedure	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	HS		4	5	20
		22.5	Engineer is unaware of an imminent oil leak.	22.5.1	System shall be in place to alarm to an imminent break in containment (H2-3).		Inadequate feedback of hazard in the ER to the ECR	Emergency procedure	Diagnostics showing sensor health status which can flag a potentially imminent break in containment/ or presence of fuel/ oil mist. Audit of engineer training and knowledge of water mist release.	OL	(Y) - MV Zenith, Splendour of the Seas, Accident Event 207960, 231717, 224659, Incident Event 202364	4	5	20
		22.6	Engineer is unaware of oil leak in the room.	22.6.1	System shall be in place to allow for an oil leak to generate an alarm (H2-3).		Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - MV Zenith, Splendour of the Seas, Accident Event 207960, 231717, 224659, Incident Event 202364	3	5	15
		22.7	Fire in the room damages equipment resulting in incomplete control action, therefore hot surfaces remain in place elsewhere which could cause further escalation.	22.7.1	water mist system shall be able to continue operation in the event of a fire (H-1).		Inadequate safety system design	Emergency shutdown Procedure	Audit of design.	HS	(Y) - Splendour of the Seas	2	4	8
				22.7.2	Engineers shall be aware of the requirement and how to release water mist system in the event of a fire if it is not already active.			Training procedure/ Emergency procedure	Audit of procedures can be the signal of performance.	HS		4	4	16
		22.8	Valve seized shut due to lack of use.	22.8.1	water mist release valves used to prevent or mitigate H-1 shall be subject to operation and inspection during maintenance as per manufacturer recommendation.		Inadequate maintenance and operations	Physical barrier function test procedure	Audit of procedures and review of maintenance logs can be the signal of performance. Audit of embracing of maintenance management system.	OL	(Y) - Accident Event 274465	4	5	20
23	Engineer releases the water mist too late when leak exists (H-1).	23.1	Engineer prevents the release of the water mist system as they believe the alarms indicating oil leak are false alarms. Water mist only released when further alarms are received.	23.1.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.	Inadequate incident response	Inadequate emergency response	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		2	2	4
		23.2	Water mist release mechanism has been inhibited during maintenance and not brought back online.	23.2.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance and operations	Audit of maintenance procedure	Audit of maintenance process	HS		2	2	4
24	Engineer releases the water mist too late when exposed hot surface exists (H-1)	24.1	Engineer prevents the release of the water mist system as they believe the alarms indicating hot surface are false alarms. Water mist only	24.1.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.	Inadequate incident response	Inadequate emergency response	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		2	2	4
		24.2	Water mist release mechanism has been inhibited during maintenance and not brought back online.	24.2.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance and operations	Audit of maintenance procedure	Audit of maintenance process	HS		2	2	4
25	Engineer shuts down the water mist too soon when hot exposed surfaces have existed and oil mist in atmosphere is detected/suspected (H-1)	25.1	Engineer believes the water mist will have completed it's job and switches it off, despite the hot surface remaining in place.	25.1.1	Engineer shall be aware of emergency response and on the factors to review in assuming a situation no longer poses a risk of H-1.	Inadequate incident response	Inadequate knowledge (training/ competence)	Training procedure/ Emergency procedure	Audit of procedures can be the signal of performance.	HS	(Y) - Splendour of the Seas	4	5	20

Barrier Criticality



Barrier Effectiveness

Scale of Colours
Green = 1-8
Amber = 9-15
Red = 16-30


Company
Safety policy, develop & enforce SMS, training, safety alerts, audits, resources
Reports on operations, safety meetings
Ship/ Control Room
Provide Instructions, status
Feedback on ER
Chief Engineer
Implement SMS, procedures, assess capability
Reports, logs, feedback
Provide instructions, status
Feedback on ER
Set mode, targets
Feedback on ER
Engineer
Set mode, targets
Current mode, condition
Manual Control, maintenance
Sensor readings, visual inspection
Ship automation
Automated controls
Sensor readings
Control of flammable materials/ ignition sources

Ship Automation

Objective/ responsibility	Direct, sharp end control of the hazardous process through automation, maintaining the safe operating limits of the process.
Input	Safe operating limit settings, sensor readings
Output	Sensor readings, automated controls, current mode
Constraints	Instrumentation functionality, set points, maintenance, design.

Hazards

H1	Hot surfaces (>220degC) in ER
H2	Leak from pressurised oil systems
H3	Failure to contain oil leak

Actions	Control Action	Not providing	Providing	Too early	Too late	Stopped to soon (applied too short)	Applied too long
A1	Provide status	Ship automation does not provide engineers operational status (H1-3)	Ship Automation provides incorrect status to engineers (H1-3)		Ship automation provides operational status to engineers too late (H1-3)		
		Ship automation does not provide ECR operational status (H1-3)	Ship Automation provides incorrect status to ECR (H1-3)		Ship automation provides operational status to ECR too late (H1-3)		
A2	Alarm/ alert	Ship automation does not alarm to pressure deviation in the oil systems (H2-3)	Ship automation provides an alarm when pressure in the oil systems is normal (H2-3)		Ship automation alarms too late to pressure deviation in the oil systems (H2-3)		
		Ship automation does not provide an alarm during an oil leak (H2-3)			Ship automation provides an alarm too late during an oil leak (H2-3)		
		Ship automation does not alarm to exposed hot surface (H-1)	Ship automation provides an alarm when there is no exposed hot surface (H2-3)		Ship automation alarms too late to exposed hot surface (H-1)		
		Ship automation does not alarm to excessive vibration (H2-3)	Ship automation provides an alarm when vibration levels are normal (H2-3)		Ship automation alarms too late to excessive vibration (H2-3)		
A3	Shutdown engine	Ship automation does not shutdown the engine when there is a pressure deviation in the oil systems (H2-3)	Ship automation shuts down the engine when pressure in the oil systems is normal (H2-3)		Ship automation shuts down the engine too late when there is a pressure deviation in the oil systems (H2-3)		
		Ship automation does not shutdown the engine during an oil leak (H2-3)			Ship automation shuts down the engine too late during an oil leak (H2-3)		
		Ship automation does not shutdown the engine when exposed hot surface exists (H-1).	Ship automation shuts down the engine when there is no exposed hot surface (H2-3)		Ship automation shuts down the engine too late when exposed hot surface exists (H-1).		
		Ship automation does not shutdown the engine when excessive vibration exists (H2-3)	Ship automation shuts down the engine when vibration levels are normal (H2-3)		Ship automation shuts down the engine too late when excessive vibration exists (H2-3)		
A4	Shutdown fuel supply	Ship automation does not shutdown the fuel supply when there is a pressure deviation in the oil systems (H2-3)	Ship automation shuts down the fuel supply when pressure in the oil systems is normal (H2-3)		Ship automation shuts down the fuel supply too late when there is a pressure deviation in the oil systems (H2-3)		
		Ship automation does not shutdown the fuel supply during an oil leak (H2-3)			Ship automation shuts down the fuel supply too late during an oil leak (H2-3)		
		Ship automation does not shutdown the fuel supply when exposed hot surface exists (H-1).	Ship automation shuts down the fuel supply when there is no exposed hot surface (H2-3)		Ship automation shuts down the fuel supply too late when exposed hot surface exists (H-1).		
		Ship automation does not shutdown the fuel supply when excessive vibration exists (H2-3)	Ship automation shuts down the fuel supply when vibration levels are normal (H2-3)		Ship automation shuts down the fuel supply too late when excessive vibration exists (H2-3)		
A5	Start-up engine/ fuel supply	Engine/ fuel supply not started when an adjacent engine is over its design load (H1-3)	Engine/ fuel supply started when low pressure exists due to an existing leak (H2-3)		Engine/ fuel supply started too late when an adjacent engine is over its design load (H1-3)		
			Engine/ fuel supply started when equipment is intended to be out of service (H2-3)				
A6	Release water mist	Ship automation doesn't release the water mist when leak exists (H-1).			Ship automation releases the water mist too late when leak exists (H-1).	Ship automation stops the water mist release too soon when oil leak is still present (H-1)	
		Ship automation doesn't release the water mist when exposed hot surface exists (H-1)			Ship automation releases the water mist too late when exposed hot surface exists (H-1)	Ship automation stops the water mist release too soon when exposed hot surface still exists (H-1)	

ID	Unsafe control action	Inadequate input (missing, wrong, too late/early etc.) / out-of-range disturbances	Inadequate control algorithm (fault, data handling etc.) /Inadequate responsibilities, knowledge or skills	Inconsistent process (mental) model	Design of incomplete process (mental) model	Inadequate feedback (incomplete, too late, missing, etc.)	Inadequate control path (too late, etc.)	Unruly controlled process
	Ship automation does not provide engineers operational status (H1-3)	Indication is not clearly represented due to poorly illuminated LED/ dirt obscuration.				No sensor is provided for ship automation that the fuel oil system/ engine is operational as there is no sensor in place. The engineer then proceeds to conduct maintenance on the system and breaks containment.	Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status. Signal from the sensor has been inhibited during maintenance and not brought back online.	
	Ship automation does not provide ECR operational status (H1-3)	Indication is not clearly represented due to poorly illuminated LED/ dirt obscuration.				No sensor is provided for ship automation that the fuel oil system/ engine is operational as there is no sensor in place. The ECR then instructs engineer to conduct maintenance on the system and breaks containment.	Signal from the sensor has been inhibited during maintenance and not brought back online.	
	Ship Automation provides incorrect status to engineers (H1-3)					Faulty sensor does not detect operational status, therefore misleading the engineer that the equipment is not operational. Sensor is not located in the correct position to detect operational indicators, meaning the signal provides misleading information.		
	Ship Automation provides incorrect status to ECR (H1-3)					Faulty sensor does not detect operational status, therefore misleading the ECR that the equipment is not operational. Sensor is not located in the correct position to detect operational indicators, meaning the signal provides misleading information.		
	Ship automation provides operational status to engineers too late (H1-3)			A excessive time delay has been implemented in the control system to avoid spurious signals based on standard system fluctuations, meaning the true operational status is presented too late.			Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status.	
	Ship automation provides operational status to ECR too late (H1-3)			A excessive time delay has been implemented in the control system to avoid spurious signals based on standard system fluctuations, meaning the true operational status is presented too late.			Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status.	
	Ship automation does not alarm to pressure deviation in the oil systems (H2-3)	Ship automation receives sensor data of pressure deviation but misinterprets the data as normal operation as the set point is not relevant to the design tolerance, therefore does not send alarm, resulting in pipework rupture.	Ship automation receives sensor data of pressure deviation, sends the alarm signal but the alarm is not clearly presented in the control room as the pressure indicator is not designed as an alarm worthy of noting in the control room, and is not designed to be treated as a fire precursor			No feedback exists on stream pressure because no sensor is in place, resulting in no alarm signal on pressure deviation, resulting in pipework rupture	Signal from the sensor has been inhibited during maintenance and not brought back online.	
	Ship automation does not provide an alarm during an oil leak (H2-3)	Airflow through the ER/ leak conditions transfer the oil mist/ spray away from the oil mist detectors resulting in no detection and continual leak. Ship automation receives sensor data of reduced pressure as a result of a leak but misinterprets the data as normal operation as the set point is not relevant to the design tolerance, therefore does not send alarm, resulting in continual leak	Ship automation receives sensor data of oil mist/ leak, sends the alarm signal but the alarm is not clearly presented in the control room as a flammable atmosphere is not designed as an alarm worthy of noting in the control room and is not designed to be treated as a fire precursor			No sensor provided to detect presence of an oil leak/ mist therefore no alarm can be presented.	Signal from the oil mist sensor has been inhibited during maintenance and not brought back online.	
	Ship automation does not alarm to exposed hot surface (H-1)	Ship automation receives sensor data that exposed hot surfaces are present but misinterprets the data as normal conditions, as the set point is not relevant to what constitutes a 'hot surface' resulting in an exposed ignition source	Ship automation receives sensor data of exposed hot surface, sends the alarm signal but the alarm is not clearly presented in the control room as a flammable atmosphere is not designed as an alarm worthy of noting in the control room and is not designed to be treated as a fire precursor			No sensor provided to detect presence of an exposed hot surface therefore no alarm can be presented.	Signal from the thermal sensor has been inhibited during maintenance and not brought back online.	
	Ship automation does not alarm to excessive vibration (H2-3)	Ship automation receives sensor data that excessive vibration is present but misinterprets the data as normal conditions, as the set point is not relevant to what constitutes a risk to pipework rupture.	Ship automation receives sensor data of excessive vibration, sends the alarm signal but the alarm is not clearly presented in the control room as excessive vibration is not designed as an alarm worthy of noting in the control room and is not designed to be treated as a fire precursor			No sensor provided to detect presence of excessive vibration therefore no alarm can be presented.	Signal from the vibration sensor has been inhibited during maintenance and not brought back online.	
	Ship automation provides an alarm when pressure in the oil systems is normal (H2-3)	Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm, sending an alarm. This results in incorrect actions being taken by engineers by shutting down a process which causes excessive load on another part of the system, rupturing the pipework Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm sending an alarm. This results in incorrect actions being taken by engineers by inspecting equipment.						
	Ship automation provides an alarm when there is no exposed hot surface (H2-3)	Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm, sending an alarm. This results in incorrect actions being taken by engineers by shutting down a process which causes excessive load on another part of the system, rupturing the pipework Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm sending an alarm. This results in incorrect actions being taken by engineers by inspecting equipment by removing a protective lagging, revealing an exposed hot surface						
	Ship automation provides an alarm when vibration levels are normal (H1-3)	Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm, sending an alarm. This results in incorrect actions being taken by engineers by shutting down a process which causes excessive load on another part of the system, rupturing the pipework Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm sending an alarm. This results in incorrect actions being taken by engineers by inspecting equipment by removing a protective lagging, revealing an exposed hot surface.						
	Ship automation alarms too late to pressure deviation in the oil systems (H2-3)	Feedback on oil system pressure provided to ship automation too late due to an excessively high set point for alarm, allowing an unsafe pressure to have occurred before alarm is sent resulting in no alarm signal on increased pressure, resulting in pipework rupture					Signal from the sensor has been inhibited by a time delay implemented during maintenance as a result of regular false alarms.	
	Ship automation provides an alarm too late during an oil leak (H2-3)	Feedback on oil mist/ spray provided to ship automation too late to alert ship automation of an oil leak because the sensor does not have a clear line of sight to the release point, leading to continued oil leak. Feedback on oil system pressure provided to ship automation too late due to an excessively low set point for alarm, allowing an unsafe pressure to have occurred before alarm is sent resulting in no alarm signal on reduced pressure as a result of pipework rupture, resulting in continual leak					Signal from the sensor has been inhibited by a time delay implemented during maintenance as a result of regular false alarms.	
	Ship automation alarms too late to	Feedback on hot surfaces provided to ship automation too late to alert ship automation of an exposed hot surface because the sensor does not have a clear line of sight to the hot surface when it is initially exposed, which leads to an ignition source					Signal from the sensor has been inhibited by a time delay	

exposed hot surface (H-1)				implemented during maintenance as a result of regular false alarms.
	Feedback on hot surfaces provided to ship automation too late to alert ship automation of an exposed hot surface because the set point is higher than the auto ignition temperature for the atomised fuel.			
	Feedback on vibration provided to ship automation too late to alert ship automation of excessive vibration because the sensor does not have direct contact with the equipment at risk of fatigue through vibration.			
Ship automation alarms too late to excessive vibration (H2-3)	Feedback on vibration provided to ship automation too late to alert ship automation of excessive vibration because the set point is higher than the point at which break in containment can occur (either through a 'Time Weighted Average [TWA]' of long term exposure, or a 'Short Term Exposure Limit [STEL]' through a short duration intense vibration).			Signal from the sensor has been inhibited by a time delay implemented during maintenance as a result of regular false alarms.
				Lack of maintenance has resulted in the shutdown action being faulty and not operating.
Ship automation does not shutdown the engine when there is a pressure deviation in the oil systems (H2-3)	Ship automation receives sensor data of increased pressure but misinterprets the data as normal operation due to incorrect set point settings therefore does not send shutdown signal, resulting in break in containment	No automation in place to shutdown engine on reception of pressure deviation alarm	Shutdown action is on different engine from where the pressure deviation is present through incorrectly programmed control system	Sensors indicate unsafe pressure in pipework and issues command to shutdown the engine. No shutdown measures exist in the engine. Control action not completed
	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating pressure deviation are false alarms			Automated shutdown action has been inhibited during maintenance and not brought back online.
	Ship automation receives sensor data that an oil leak is present but misinterprets the data as normal conditions due to excessively high set points for automated action, resulting in continued engine operation which could be leaking flammable materials			Lack of maintenance has resulted in the shutdown action being faulty and not operating.
Ship automation does not shutdown the engine during an oil leak (H2-3)	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating oil leak are false alarms	No automation in place to shutdown engine on reception of oil leak alarm		Sensors indicate oil leak and issues command to shutdown the engine. No shutdown measures exist in the engine. Control action not completed
	Ship automation receives sensor data of reduced pressure as a result of a leak but misinterprets the data as normal operation due to incorrect set point settings therefore does not send shutdown action, resulting in continued engine operation and leak			Automated shutdown action has been inhibited during maintenance and not brought back online.
	Ship automation receives sensor data that an exposed hot surface is present but misinterprets the data as normal conditions due to inaccuracy in measurements and set points for automated action, resulting in continued engine operation and exposed hot surface	No automation in place to shutdown engine on reception of exposed hot surface alarm		Lack of maintenance has resulted in the shutdown action being faulty and not operating.
Ship automation does not shutdown the engine when exposed hot surface exists (H-1).	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating exposed hot surface are false alarms	Ship automation receives sensor data that exposed hot surfaces are present but misinterprets the data as normal conditions as the process model is not programmed to recognise exposed hot surfaces as a fire precursor, which leads to no engine shutdown and continued exposure of an ignition source		Sensors indicate exposed hot surface and issues command to shutdown the engine. No shutdown measures exist in the engine. Control action not completed
	No feedback exists to alert ship automation of exposed hot surfaces as sensors have no direct field of view directly to the hot surface which leads to no engine shutdown and continued exposure of an ignition source			Automated shutdown action has been inhibited during maintenance and not brought back online.
	Ship automation receives sensor data that excessive vibration is present but misinterprets the data as normal conditions due to inaccuracy in measurements and set points for automated action, resulting in continued engine operation and increasing fatigue	No automation in place to shutdown engine on reception of excessive vibration		Lack of maintenance has resulted in the shutdown action being faulty and not operating.
Ship automation does not shutdown the engine when excessive vibration exists (H2-3)	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating excessive vibration are false alarms	Ship automation receives sensor data that excessive vibration is present but misinterprets the data as normal conditions as the process model is not programmed to recognise this as a fire precursor, which leads to no engine shutdown		Sensors indicate excessive vibration and issues command to shutdown the engine. No shutdown measures exist in the engine. Control action not completed
	No feedback exists to alert ship automation of excessive vibration as sensors have no direct contact with equipment subject to vibration fatigue which leads to no engine shutdown			Automated shutdown action has been inhibited during maintenance and not brought back online.
Ship automation shuts down the engine when pressure in the oil systems is normal (H2-3)	Ship automation misinterprets the signals received from the engine and assumes a system deviation has taken place due to inappropriate set point selection and sends a shutdown signal. This results in increased load elsewhere on the system, breaking containment		Shutdown action is intended for a different engine from where the pressure deviation is present through incorrectly programmed control system, increasing demand on the already fault engine	
Ship automation shuts down the engine when there is no exposed hot surface (H2-3)	Ship automation misinterprets the signals received from the engine and assumes a system deviation has taken place due to inappropriate set point selection and sends a shutdown signal. This results in increased load elsewhere on the system, breaking containment		Shutdown action is intended for a different engine from where the exposed hot surface is present through incorrectly programmed control system	
Ship automation shuts down the engine when vibration levels are normal (H2-3)	Feedback on excessive stream pressure provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on increased pressure, resulting in engine break in containment			Feedback on excessive stream pressure provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on increased pressure, resulting in engine break in containment
Ship automation shuts down the engine too late when there is a pressure deviation in the oil systems (H2-3)		No automation in place to shutdown engine therefore manual detection relied upon which has a delayed response.		Automated shutdown action has been inhibited during maintenance and not brought back online.
	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating pressure deviation are false alarms. Shutdown only activated when further alarms are received.			Feedback on excessive stream pressure provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on increased pressure, resulting in engine break in containment
	Feedback on oil leak provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on oil leak			Feedback on oil leak provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on oil leak
Ship automation shuts down the engine too late during an oil leak (H2-3)		No automation in place to shutdown engine therefore manual detection relied upon which has a delayed response.		Automated shutdown action has been inhibited during maintenance and not brought back online.
	ECR/ engineer prevents the automated shutdown as they			

	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating oil leak are false alarms. Shutdown only activated when further alarms are received.			Feedback on oil leak provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on oil leak
	Feedback on exposed hot surface provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on engine			Feedback on exposed hot surface provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on engine
Ship automation shuts down the engine too late when exposed hot surface exists (H-1).		No automation in place to shutdown engine therefore manual detection relied upon which has a delayed response.		Automated shutdown action has been inhibited during maintenance and not brought back online.
	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating exposed hot surface are false alarms. Shutdown only activated when further alarms are received.			Feedback on exposed hot surface provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on engine
	Feedback on excessive vibration provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on engine			Feedback on excessive vibration provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on engine
Ship automation shuts down the engine too late when excessive vibration exists (H2-3)		No automation in place to shutdown engine therefore manual detection relied upon which has a delayed response.		Automated shutdown action has been inhibited during maintenance and not brought back online.
	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating excessive vibration are false alarms. Shutdown only activated when further alarms are received.			Feedback on excessive vibration provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on engine
	Ship automation receives sensor data of increased pressure but misinterprets the data as normal operation due to incorrect set point settings therefore does not send shutdown signal, resulting in break in containment			Lack of maintenance has resulted in the shutdown action being faulty and not operating.
Ship automation does not shutdown the fuel supply when there is a pressure deviation in the oil systems (H2-3)		No automation in place to shutdown fuel supply on reception of pressure deviation alarm	Shutdown action is on different fuel supply from where the pressure deviation is present through incorrectly programmed control system	Sensors indicate unsafe pressure in pipework and issues command to shutdown the fuel supply. No shutdown measures exist in the fuel supply. Control action not completed
	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating pressure deviation are false alarms			Automated shutdown action has been inhibited during maintenance and not brought back online.
	Ship automation receives sensor data that an oil leak is present but misinterprets the data as normal conditions due to excessively high set points for automated action, resulting in continued fuel supply which could be leaking flammable materials			Lack of maintenance has resulted in the shutdown action being faulty and not operating.
Ship automation does not shutdown the fuel supply during an oil leak (H2-3)	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating oil leak are false alarms	No automation in place to shutdown fuel supply on reception of oil leak alarm		Sensors indicate oil leak and issues command to shutdown the fuel supply. No shutdown measures exist in the fuel supply. Control action not completed
	Ship automation receives sensor data of reduced pressure as a result of a leak but misinterprets the data as normal operation due to incorrect set point settings therefore does not send shutdown action, resulting in continued fuel supply			Automated shutdown action has been inhibited during maintenance and not brought back online.
	Ship automation receives sensor data that an exposed hot surface is present but misinterprets the data as normal conditions due to inaccuracy in measurements and set points for automated action, resulting in continued fuel supply, which could rupture and meet the hot surface	No automation in place to shutdown fuel supply on reception of exposed hot surface alarm		Lack of maintenance has resulted in the shutdown action being faulty and not operating.
Ship automation does not shutdown the fuel supply when exposed hot surface exists (H-1).	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating exposed hot surface are false alarms	Ship automation receives sensor data that exposed hot surfaces are present but misinterprets the data as normal conditions as the process model is not programmed to recognise exposed hot surfaces as a fire precursor, which leads to no fuel supply shutdown and continued exposure of an ignition source in an area processing flammable materials		Sensors indicate exposed hot surface and issues command to shutdown the fuel supply. No shutdown measures exist in the fuel system. Control action not completed
	No feedback exists to alert ship automation of exposed hot surfaces as sensors have no direct field of view directly to the hot surface which leads to no engine fuel supply shutdown and continued exposure of an ignition source in an area processing flammable materials			Automated shutdown action has been inhibited during maintenance and not brought back online.
	Ship automation receives sensor data that excessive vibration is present but misinterprets the data as normal conditions due to inaccuracy in measurements and set points for automated action, resulting in continued fuel supply operation and increasing fatigue	No automation in place to shutdown fuel supply on reception of excessive vibration		Lack of maintenance has resulted in the shutdown action being faulty and not operating.
Ship automation does not shutdown the fuel supply when excessive vibration exists (H2-3)	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating excessive vibration are false alarms	Ship automation receives sensor data that excessive vibration is present but misinterprets the data as normal conditions as the process model is not programmed to recognise this as a fire precursor, which leads to no fuel supply shutdown		Sensors indicate excessive vibration and issues command to shutdown the engine. No shutdown measures exist in the fuel supply. Control action not completed
	No feedback exists to alert ship automation of excessive vibration as sensors have no direct contact with equipment subject to vibration fatigue which leads to no fuel supply shutdown			Automated shutdown action has been inhibited during maintenance and not brought back online.
Ship automation shuts down the fuel supply when pressure in the oil systems is normal (H2-3)	Ship automation misinterprets the signals received from the fuel supply system and assumes a system deviation has taken place due to inappropriate set point selection and sends a shutdown signal. This results in increased load elsewhere on the system, breaking containment		Shutdown action is intended for a different fuel supply from where the pressure deviation is present through incorrectly programmed control system, increasing demand on the already fault engine	
Ship automation shuts down the fuel supply when there is no exposed hot surface (H2-3)	Ship automation misinterprets the signals received from the engine and assumes a system deviation has taken place due to inappropriate set point selection and sends a shutdown signal. This results in increased load elsewhere on the system, breaking containment		Shutdown action is intended for a different fuel supply from where the exposed hot surface is present through incorrectly programmed control system	
Ship automation shuts down the fuel supply when vibration levels are normal (H2-3)	Ship automation misinterprets the signals received from the fuel supply and assumes a system deviation has taken place due to inappropriate set point selection and sends a shutdown signal. This results in increased load elsewhere on the system, breaking containment		Shutdown action is intended for a different fuel supply from where the exposed hot surface is present through incorrectly programmed control system	

	Feedback on excessive stream pressure provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on increased pressure, resulting in fuel supply break in containment				Feedback on excessive stream pressure provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on increased pressure, resulting in engine break in containment
Ship automation shuts down the fuel supply too late when there is a pressure deviation in the oil systems (H2-3)		No automation in place to shutdown fuel supply therefore manual detection relied upon which has a delayed response.			Automated shutdown action has been inhibited during maintenance and not brought back online.
	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating pressure deviation are false alarms. Shutdown only activated when further alarms are received.				Feedback on excessive stream pressure provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on increased pressure, resulting in engine break in containment
	Feedback on oil leak provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on oil leak				Feedback on oil leak provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on oil leak
Ship automation shuts down the fuel supply too late during an oil leak (H2-3)		No automation in place to shutdown fuel supply therefore manual detection relied upon which has a delayed response.			Automated shutdown action has been inhibited during maintenance and not brought back online.
	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating oil leak are false alarms. Shutdown only activated when further alarms are received.				Feedback on oil leak provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on oil leak
	Feedback on exposed hot surface provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on fuel supply				Feedback on exposed hot surface provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on fuel supply
Ship automation shuts down the fuel supply too late when exposed hot surface exists (H-1).		No automation in place to shutdown fuel supply therefore manual detection relied upon which has a delayed response.			Automated shutdown action has been inhibited during maintenance and not brought back online.
	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating exposed hot surface are false alarms. Shutdown only activated when further alarms are received.				Feedback on exposed hot surface provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on fuel supply
	Feedback on excessive vibration provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on fuel supply				Feedback on excessive vibration provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on fuel supply
Ship automation shuts down the fuel supply too late when excessive vibration exists (H2-3)		No automation in place to shutdown fuel supply therefore manual detection relied upon which has a delayed response.			Automated shutdown action has been inhibited during maintenance and not brought back online.
	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating excessive vibration are false alarms. Shutdown only activated when further alarms are received.				Feedback on excessive vibration provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on fuel supply
Engine/ fuel supply not started when an adjacent engine is over its design load (H1-3)	Set points not accurate to start-up adjacent engines before design deviation thresholds are exceeded.	No logic present to automate the control of multiple engines to ensure a steady load application.		Faulty sensors cannot detect adjacent engine in excess of design load and automate start-up of adjacent engines through lack of maintenance.	Engine which would have been started up due to automated start-up is out of service for maintenance
Engine/ fuel supply started when low pressure exists due to an existing leak (H2-3)	Engine shows low efficiency, therefore automation increases/ start-up the fuel supply, sending flammable materials to the source of the leak.				
Engine/ fuel supply started when equipment is intended to be out of service (H2-3)					Engine which is started up to assist other engines, is out of service for maintenance, but starts up anyway.
Engine/ fuel supply started too late when an adjacent engine is over its design load (H1-3)	Set points not accurate to start-up adjacent engines before design deviation thresholds are exceeded.	No logic present to automate the control of multiple engines to ensure a steady load application. Engine/ fuel supply not started until manual intervention occurs.		Faulty sensors cannot detect and automate start-up of adjacent engines through lack of maintenance. Manual start-up required which is delayed.	
Ship automation doesn't release the water mist when leak exists (H-1).	ECR/ engineer prevents the release of the water mist system as they believe the alarms indicating oil leak are false alarms	No automation in place to automatically release deluge on reception of sufficient alarm alarms indicating oil leak	Water mist released in the wrong location from where the leak is present as the leak detectors are incorrectly programmed to the automated release		
Ship automation doesn't release the water mist when exposed hot surface exists (H-1)	ECR/ engineer prevents the release of the water mist system as they believe the alarms indicating exposed hot surfaces are false alarms	No automation in place to automatically release deluge on reception of sufficient alarm alarms indicating exposed hot surface	Water mist released in the wrong location from where the exposed hot surface is present as the leak detectors are incorrectly programmed to the automated release		Automated water mist release has been inhibited during maintenance and not brought back online. Lack of maintenance has resulted in the water mist valves seizing shut, meaning water mist cannot be released.
Ship automation releases the water mist too late when leak exists (H-1).	ECR/ engineer prevents the release of the water mist system as they believe the alarms indicating oil leak are false alarms. Water mist only released when further alarms are received.	No automation in place to automatically release deluge on reception of sufficient alarm alarms indicating oil leak. Release only occurs on manual detection of a leak.		Sensors which detect the presence of oil leak are not a fast enough response to provide fast response water mist release.	Automated water mist release has been inhibited during maintenance and not brought back online.

Ship automation releases the water mist too late when exposed hot surface exists (H-1)	ECR/ engineer prevents the release of the water mist system as they believe the alarms indicating exposed hot surfaces are false alarms. Water mist only released when further alarms are received.	No automation in place to automatically release deluge on reception of sufficient alarm alarms indicating exposed hot surface. Release only occurs on manual detection of a hot surface.	Sensors which detect the presence of exposed hot surface are not a fast enough response to provide fast response water mist release.	Automated water mist release has been inhibited during maintenance and not brought back online.
Ship automation stops the water mist release too soon when oil leak is still present (H-1)	ECR/ engineer prevents the release of the water mist system as they believe the leak no longer presents a risk.		Sensors show the oil leak has been removed therefore deluge is stopped. The oil leak continues without water mist presence.	Fire erupts, causing short on power supply, stopping the deluge. Water mist release water capacity is depleted and actions to stop the leak have not yet been completed.
Ship automation stops the water mist release too soon when exposed hot surface still exists (H-1)	ECR/ engineer prevents the release of the water mist system as they believe the exposed hit surface no longer presents a risk.		Sensors show the exposed hot surface has been removed therefore deluge is stopped. The exposed hot surface re-emerges without water mist presence.	Fire erupts, causing short on power supply, stopping the deluge. Water mist release water capacity is depleted and actions to remove the exposed hot surface have not yet been completed.

ID-UCA	UCA	ID-CF	Causal factors	ID-FR	Functional requirements	UCA Category	CF Category	Relevant barriers	Signals and their requirements	Hazard (Oil Leak[OL]/ Hot Surface [HS])	Previous occurrence in Incident/ Accident (Y/N) + incident ref	Barrier Effectiveness	Criticality	Magnitude of risk reduction
1	Ship automation does not provide engineers operational status (H1-3)	1.1	Indication is not clearly represented due to poorly illuminated LED/ dirt obscuration.	1.1.1	Operational status shall be easily discernible and indicator shall be clear and visible.	Inadequate operational feedback	Inadequate operational feedback	Indication design. Maintenance of alarms and indicators.	Audit of indicator management. Audit of maintenance.	OL + HS	Le Boreal	4	4	16
		1.2	No sensor is provided for ship automation that the fuel oil system/ engine is operational as there is no sensor in place. The engineer then proceeds to conduct maintenance on the system and breaks containment.	1.2.1	Operational status shall be shown at the machine.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design.	OL + HS	Le Boreal	4	4	16
		1.3	Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status.	1.3.1	Operational status indicators shall operate in real time, providing an indication of status with 1 second of accuracy.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design. Function testing.	OL + HS	Le Boreal	4	4	16
		1.4	Signal from the sensor has been inhibited during maintenance and not brought back online.	1.4.1	All inhibiting measures implemented during maintenance shall be reinstated upon task completion. Upon equipment start-up, warnings shall be presented if sensors are inhibited.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL + HS		4	3	12
				1.4.2				Function testing	Audit of design and sensor performance.					0
2	Ship automation does not provide ECR operational status (H1-3)	2.1	Indication is not clearly represented due to poorly illuminated LED/ dirt obscuration.	2.1.1	Operational status shall be easily discernible and indicator shall be clear and visible.	Inadequate operational feedback	Inadequate operational feedback	Indication design. Maintenance of alarms and	Audit of indicator management. Audit of maintenance.	OL + HS	Le Boreal	4	4	16
		2.2	No sensor is provided for ship automation that the fuel oil system/ engine is operational as there is no sensor in place. The ECR then instructs engineer to conduct maintenance on the system and breaks containment.	2.2.1	Operational status shall be known to the process controller.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design.	OL + HS	Le Boreal	4	4	16
		2.3	Signal from the sensor has been inhibited during maintenance and not brought back online.	2.3.1	All inhibiting measures implemented during maintenance shall be reinstated upon task completion. Upon equipment start-up, warnings shall be presented if sensors are inhibited.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL+HS		4	3	12
				2.3.2				Function testing	Audit of design and sensor performance.					12
3	Ship Automation provides incorrect status to engineers (H1-3)	3.1	Faulty sensor does not detect operational status, therefore misleading the engineer that the equipment is not operational.	3.1.1	Sensors used to show operational status shall be reliable on demand	Inadequate operational feedback	Inadequate hardware design/ maintenance	Function testing	Availability/ reliability study/ statistics	OL + HS		4	3	12
				3.1.2	Sensors shall be maintained in line with manufacturer recommendations.			Audit of maintenance	Audit of maintenance process					0
		3.2	Sensor is not located in the correct position to detect operational indicators, meaning the signal provides misleading information.	3.2.1	Sensors used to show operational status shall be placed in direct contact with the process which it is measuring		Inadequate safety system design	Sensor design, Signalling	Verification of design.	OL + HS		4	3	12
4	Ship Automation provides incorrect status to ECR (H1-3)	4.1	Faulty sensor does not detect operational status, therefore misleading the ECR that the equipment is not operational.	4.1.1	Sensors used to show operational status shall be reliable on demand	Inadequate operational feedback	Inadequate hardware design/ maintenance	Function testing	Availability/ reliability study/ statistics	OL + HS		4	3	12
				4.1.2	Sensors shall be maintained in line with manufacturer recommendations.			Audit of maintenance procedure	Audit of maintenance process	OL + HS		4	3	0
		4.2	Sensor is not located in the correct position to detect operational indicators, meaning the signal provides misleading information.	4.2.1	Sensors used to show operational status shall be placed in direct contact with the process which it is measuring		Inadequate safety system design	Sensor design, Signalling	Verification of design.	OL + HS		4	3	12
5	Ship automation provides operational status to engineers too late (H1-3)	5.1	An excessive time delay has been implemented in the control system to avoid spurious signals based on standard system fluctuations, meaning the true operational status is presented too late.	5.1.1	Time delays shall not be beyond the point at which the operational status needs to be know. i.e. time delay of no greater than 10 seconds.	Inadequate operational feedback	Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design.	OL + HS		4	2	8
		5.2	Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status.	5.2.1	Operational status indicators shall operate in real time, providing an indication of status with 1 second of accuracy.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design. Function testing.	OL + HS		4	3	12
6	Ship automation provides operational status to ECR too late (H1-3)	6.1	An excessive time delay has been implemented in the control system to avoid spurious signals based on standard system fluctuations, meaning the true operational status is presented too late.	6.1.1	Time delays shall not be beyond the point at which the operational status needs to be know. i.e. time delay of no greater than 10 seconds.	Inadequate operational feedback	Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design.	OL + HS		4	2	8
		6.2	Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status.	6.2.1	Operational status indicators shall operate in real time, providing an indication of status with 1 second of accuracy.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design. Function testing.	OL + HS		4	3	12
7	Ship automation does not alarm to pressure deviation in the oil systems (H2-3)	7.1	Ship automation receives sensor data of pressure deviation but misinterprets the data as normal operation as the set point is not relevant to the design tolerance, therefore does not send alarm, resulting in pipework rupture.	7.1.1	Set points applied to alarm to system pressure deviation from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety)	Inadequate feedback of the hazard	Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		7.2	Ship automation receives sensor data of pressure deviation, sends the alarm signal but the alarm is not clearly presented in the control room as the pressure indicator is not designed as an alarm worthy of noting in the control room, and is not designed to be treated as a fire precursor	7.2.1	Pressure deviation alarms shall be easily discernible and alarm shall be clear and visible.		Inadequate feedback of the hazard	Indication design. Maintenance of alarms and indicators.	Audit of indicator management. Audit of maintenance.	OL		3	2	6
		7.3	No feedback exists on stream pressure because no sensor is in place, resulting in no alarm signal on pressure deviation, resulting in pipework rupture	7.2.2	Training shall ensure engineers are aware of pressure deviation and the risk this poses to H2-3.			Training Procedure	Audit of engineer awareness					0
				7.3.1	Stream pressure shall be known to the process controller.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design.	OL		3	2	6
		7.4	Signal from the sensor has been inhibited during maintenance and not brought back online.	7.4.1	All inhibiting measures implemented during maintenance shall be reinstated upon task completion.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	3	9
				7.4.2	Upon equipment start-up, warnings shall be presented if sensors are inhibited.			Function testing	Audit of design and sensor performance.					0
8	Ship automation does not provide an alarm during an oil leak (H2-3)	8.1	Airflow through the ER/ leak conditions transfer the oil mist/ spray away from the oil mist detectors resulting in no detection and continual leak.	8.1.1	Room conditions accounting for extremes of high air movement and no air flow shall be taken into consideration in the design of oil mist detection systems.	Inadequate feedback of the hazard	Inadequate safety system design	Sensor design	Verification of design. Function testing.	OL		3	2	6
		8.2	Ship automation receives sensor data of reduced pressure as a result of a leak but misinterprets the data as normal operation as the set point is not relevant to the design tolerance, therefore does not send alarm, resulting in continual leak	8.2.1	Set points applied to alarm to system pressure drop in the event of a leak shall be set based on the anticipated pressure which could be presented through a break in containment.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		8.3	Ship automation receives sensor data of oil mist/ leak, sends the alarm signal but the alarm is not clearly presented in the control room as a flammable atmosphere is not designed as an alarm worthy of noting in the control room and is not designed to be treated as a fire precursor	8.3.1	Oil mist/ leak alarms shall be easily discernible and indicator shall be clear and visible. Oil mist releases shall be treated with the same urgency as a fire.	Inadequate feedback of the hazard	Inadequate feedback of the hazard	Indication design. Audit of actions on alarms.	Audit of indicator management. Audit of emergency response.	OL		3	3	9
		8.4	No sensor provided to detect presence of an oil leak/ mist therefore no alarm can be presented.	8.4.1	Presence of oil mist both within the hot box and the ER shall be known to the process controller.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design.	OL	(Y) Splendour of the Seas, Carnival Triumph	3	5	15
		8.5	Signal from the oil mist sensor has been inhibited during maintenance and not brought back online.	8.5.1	All inhibiting measures implemented during maintenance shall be reinstated upon task completion.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	3	9
				8.5.2	Upon equipment start-up, warnings shall be presented if sensors are inhibited.			Function testing	Audit of design and sensor performance.					0
9	Ship automation does not alarm to exposed hot surface (H-1)	9.1	Ship automation receives sensor data that exposed hot surfaces are present but misinterprets the data as normal conditions, as the set point is not relevant to what constitutes a 'hot surface' resulting in an exposed ignition source	9.1.1	Set points applied to alarm to exposed hot surfaces shall be set based on detecting surfaces of over 220 deg C. A suitable factor of safety shall be implemented, and design shall allow for full coverage of all credible areas where they can occur.	Inadequate feedback of the hazard	Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	HS		3	2	6
		9.2	Ship automation receives sensor data of exposed hot surface, sends the alarm signal but the alarm is not clearly presented in the control room as a flammable atmosphere is not designed as an alarm worthy of noting in the control room and is not designed to be treated as a fire precursor	9.2.1	Exposed hot surface alarms shall be easily discernible and indicator shall be clear and visible. Exposed hot surfaces shall be treated with the urgency required of a significant fire precursor.		Inadequate feedback of the hazard	Indication design. Audit of actions on alarms.	Audit of indicator management. Audit of emergency response.	HS		3	3	9
		9.3	No sensor provided to detect presence of an exposed hot surface therefore no alarm can be presented.	9.3.1	Presence of exposed hot surfaces (>250 deg C) ER shall be known to the process controller.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design.	HS	Most ER fires, Splendour, Carnival Triumph etc.	3	5	15
		9.4	Signal from the thermal sensor has been inhibited during maintenance and not brought back online.	9.4.1	All inhibiting measures implemented during maintenance shall be reinstated upon task completion. Upon equipment start-up, warnings shall be presented if sensors are inhibited.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	HS		3	3	9
				9.4.2				Function testing	Audit of design and sensor performance.					0
10	Ship automation does not alarm to excessive vibration (H1-3)	10.1	Ship automation receives sensor data that excessive vibration is present but misinterprets the data as normal conditions, as the set point is not relevant to what constitutes a risk to pipework rupture.	10.1.1	Set points applied to alarm to excessive vibration from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety)	Inadequate feedback of the hazard	Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL + HS		3	2	6
		10.2	Ship automation receives sensor data of excessive vibration, sends the alarm signal but the alarm is not clearly presented in the control room as excessive vibration is not designed as an alarm worthy of noting in the control room and is not designed to be treated as a fire precursor	10.2.1	Excessive vibration alarms shall be easily discernible and indicator shall be clear and visible. Excessive vibration shall be treated with the urgency required of a fire precursor.		Inadequate feedback of the hazard	Indication design. Audit of actions on alarms.	Audit of indicator management. Audit of emergency response.	OL + HS		3	3	9
		10.3	No sensor provided to detect presence of excessive vibration therefore no alarm can be presented.	10.3.1	Presence of excessive vibration shall be known to the process controller.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design.	OL + HS		3	5	15
		10.4	Signal from the vibration sensor has been inhibited during maintenance and not brought back online.	10.4.1	All inhibiting measures implemented during maintenance shall be reinstated upon task completion. Upon equipment start-up, warnings shall be presented if sensors are inhibited.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL + HS		3	3	9
				10.4.2				Function testing	Audit of design and sensor performance.					0
11	Ship automation provides an alarm when pressure in the oil systems is normal (H2-3)	11.1	Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm, sending an alarm. This results in incorrect actions being taken by engineers by shutting down a process which causes excessive load on another part of the system, rupturing the pipework	11.1.1	Set points applied to alarm to system pressure deviation from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety), but not within the safe operating limit.	Inadequate feedback of the hazard	Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		11.2	Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm sending an alarm. This results in incorrect actions being taken by engineers by inspecting equipment by breaking containment.	11.2.1			Inadequate process model							0
12	Ship automation provides an alarm when there is no exposed hot surface (H2-3)	12.1	Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm, sending an alarm. This results in incorrect actions being taken by engineers by shutting down a process which causes excessive load on another part of the system, rupturing the pipework	12.1.1	Set points applied to alarm to exposed hot surfaces shall be set based on detecting surfaces of over 220 deg C. A suitable factor of safety shall be implemented, and design shall allow for full coverage of all credible areas where they can occur.	Inadequate feedback of the hazard	Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		12.2	Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm sending an alarm. This results in incorrect actions being taken by engineers by inspecting equipment by removing a protective lagging, revealing an exposed hot surface	12.2.1			Inadequate process model							0
13	Ship automation provides an alarm when vibration levels are normal (H1-3)	13.1	Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm, sending an alarm. This results in incorrect actions being taken by engineers by shutting down a process which causes excessive load on another part of the system, rupturing the pipework	13.1.1	Set points applied to alarm to excessive vibration from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety), but not within the standard safe operating limit.	Inadequate feedback of the hazard	Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		13.2	Ship automation misinterprets the signals received from the ER as the set point is not relevant to what constitutes a design deviation causing false alarm sending an alarm. This results in incorrect actions being taken by engineers by inspecting equipment by removing a protective lagging, revealing an exposed hot surface.	13.2.1	Set points applied to alarm to excessive vibration from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety), but not within the standard safe operating limit.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	HS		3	2	6
14	Ship automation alarms too late to pressure deviation in the oil systems (H2-3)	14.1	Feedback on oil system pressure provided to ship automation too late due to an excessively high set point for alarm, allowing an unsafe pressure to have occurred before alarm is sent resulting in no alarm signal on increased pressure, resulting in pipework rupture	14.1.1	Set points applied to alarm to system pressure deviation from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety)	Inadequate feedback of the hazard	Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		14.2	Signal from the sensor has been inhibited by a time delay implemented during maintenance as a result of regular false alarms.	14.2.1	Time delays shall not be beyond the point at which the operational status needs to be know. i.e. time delay of no greater than 10 seconds.		Inadequate maintenance	Sensor design, Signalling	Verification of design.	OL		3	2	6
15	Ship automation provides an alarm too late during an oil leak (H2-3)	15.1	Feedback on oil mist/ spray provided to ship automation too late to alert ship automation of an oil leak because the sensor does not have a clear line of sight to the release point, leading to continued oil leak.	15.1.1	Sensors used to detect oil leak shall be placed in direct contact with the equipment at risk oil leak, accounting for extremes of air movements.		Inadequate safety system design	Sensor design, Signalling	Verification of design.	OL		3	3	9
		15.2	Feedback on oil system pressure provided to ship automation too late due to an excessively low set point for alarm, allowing an unsafe pressure to have occurred before alarm is sent resulting in no alarm signal on reduced pressure as a result of pipework rupture, resulting in continual leak	15.2.1	Set points applied to alarm to system pressure drop in the event of a leak shall be set based on the anticipated pressure which could be presented through a break in containment.	Inadequate feedback of the hazard	Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		15.3	Signal from the sensor has been inhibited by a time delay implemented during maintenance as a result of regular false alarms.	15.3.1	Time delays shall not be beyond the point at which the operational status needs to be know. i.e. time delay of no greater than 10 seconds.		Inadequate maintenance	Sensor design, Signalling	Verification of design.	OL		3	2	6
16	Ship automation alarms too late to exposed hot surface (H-1)	16.1	Feedback on hot surfaces provided to ship automation too late to alert ship automation of an exposed hot surface because the sensor does not have a clear line of sight to the hot surface when it is initially exposed, which leads to an ignition source	16.1.1	Sensors used to show exposed hot surfaces shall be placed in direct contact with the equipment at risk of exposed hot surface.		Inadequate safety system design	Sensor design, Signalling	Verification of design.	HS		3	3	9
		16.2	Feedback on hot surfaces provided to ship automation too late to alert ship automation of an exposed hot surface because the set point is higher than the auto ignition temperature for the atomised fuel.	16.2.1	Set points applied to alarm to exposed hot surfaces shall be set based on detecting surfaces of over 220 deg C. A suitable factor of safety shall be implemented, and design shall allow for full coverage of all credible areas where they can occur.	Inadequate feedback of the hazard	Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	HS		3	2	6

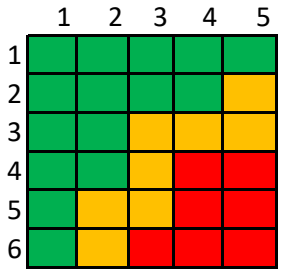
		16.3	Signal from the sensor has been inhibited by a time delay implemented during maintenance as a result of regular false alarms.	16.3.1	Time delays shall not be beyond the point at which the operational status needs to be know. i.e. time delay of no greater than 10 seconds.		Inadequate maintenance	Sensor design, Signalling	Verification of design.	HS		3	2	6
		17.1	Feedback on vibration provided to ship automation too late to alert ship automation of excessive vibration because the sensor does not have direct contact with the equipment at risk of fatigue through vibration.	17.1.1	Sensors used to show excessive vibration status shall be placed in direct contact with the equipment at risk of fatigue failure.		Inadequate safety system design	Sensor design, Signalling	Verification of design.	OL + HS		3	3	9
17	**Ship automation alarms too late to excessive vibration (H1-3)**	17.2	Feedback on vibration provided to ship automation too late to alert ship automation of excessive vibration because the set point is higher than the point at which break in containment can occur (either through a 'Time Weighted Average [TWA]' of long term exposure, or a 'Short Term	17.2.1	Set points applied to alarm to excessive vibration from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety), but not within the standard safe	Inadequate feedback of the hazard	Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL + HS		3	2	6
		17.3	Signal from the sensor has been inhibited by a time delay implemented during maintenance as a result of regular false alarms.	17.3.1	Time delays shall not be beyond the point at which the operational status needs to be know. i.e. time delay of no greater than 10 seconds.		Inadequate maintenance	Sensor design, Signalling	Verification of design.	OL + HS		3	2	6
		18.1	Ship automation receives sensor data of increased pressure but misinterprets the data as normal operation due to incorrect set point settings therefore does not send shutdown signal, resulting in break in containment	18.1.1	Set points applied to alarm to system pressure deviation from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety)		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		18.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating pressure deviation are false alarms	18.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		18.3	No automation in place to shutdown engine on reception of pressure deviation alarm	18.3.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to pressure sensors.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL	(Y) Piet Engine Fire Leak Data Event ID 90244	3	4	12
18	**Ship automation does not shutdown the engine when there is a pressure deviation in the oil systems (H2-3)**	18.4	Shutdown action is on different engine from where the pressure deviation is present through incorrectly programmed control system	18.4.1	Automated shutdown shall be based directly from the sensors installed on that machine.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
		18.5	Lack of maintenance has resulted in the shutdown action being faulty and not operating.	18.5.1	Maintenance shall be in accordance with the manufacturer guidelines. Equipment shall also achieve an availability/ reliability of 99% for safety related sensors.		Inadequate maintenance	Sensor design, Signalling	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		18.6	Sensors indicate unsafe pressure in pipework and issues command to shutdown the engine. No shutdown measures exist in the engine. Control action not completed	18.6.1	Equipment posing a risk of H1-3 shall be capable of remote, automated shutdown.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	2	6
		18.7	Automated shutdown action has been inhibited during maintenance and not brought back online.	18.7.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		19.1	Ship automation receives sensor data that an oil leak is present but misinterprets the data as normal conditions due to excessively high set points for automated action, resulting in continued engine operation which could be leaking flammable materials	19.1.1	Set points applied to alarm to system pressure drop in the event of a leak shall be set based on the anticipated pressure which could be presented through a break in containment.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		19.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating oil leak are false alarms	19.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		19.3	Ship automation receives sensor data of reduced pressure as a result of a leak but misinterprets the data as normal operation due to incorrect set point settings therefore does not send shutdown action, resulting in continued engine operation and leak	19.3.1	Set points applied to alarm to system pressure drop in the event of a leak shall be set based on the anticipated pressure which could be presented through a break in containment.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL	(Y) Piet Engine Fire Leak Data Event ID 90244	3	4	12
19	**Ship automation does not shutdown the engine during an oil leak (H2-3)**	19.4	No automation in place to shutdown engine on reception of oil leak alarm	19.4.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to oil leak detectors.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL	(Y) Splendour of the Seas, Carnival Triumph	3	5	15
		19.5	Lack of maintenance has resulted in the shutdown action being faulty and not operating.	19.5.1	Maintenance shall be in accordance with the manufacturer guidelines. Equipment shutdown measures shall achieve an availability/ reliability of 99%.		Inadequate maintenance	Sensor design, Signalling	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		19.6	Sensors indicate oil leak and issues command to shutdown the engine. No shutdown measures exist in the engine. Control action not completed	19.6.1	Equipment posing a risk of H2-3 shall be capable of remote, automated shutdown.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	2	6
		19.7	Automated shutdown action has been inhibited during maintenance and not brought back online.	19.7.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		20.1	Ship automation receives sensor data that an exposed hot surface is present but misinterprets the data as normal conditions due to inaccuracy in measurements and set points for automated action, resulting in continued engine operation and exposed hot surface	20.1.1	Set points applied to alarm to exposed hot surfaces shall be set based on detecting surfaces of over 220 deg C. A suitable factor of safety shall be implemented, and design shall allow for full coverage of all credible areas where they can occur.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	HS		3	2	6
		20.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating exposed hot surface are false alarms	20.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		3	2	6
		20.3	No feedback exists to alert ship automation of exposed hot surfaces as sensors have no direct field of view directly to the hot surface which leads to no engine shutdown and continued exposure of an ignition source	20.3.1	Sensors used to detect exposed hot surfaces shall be placed with clear contact/ field of view with the equipment at risk.		Inadequate safety system design	Sensor design	Verification of design.	HS		3	3	9
20	**Ship automation does not shutdown the engine when exposed hot surface exists (H-1).**	20.4	No automation in place to shutdown engine on reception of exposed hot surface alarm	20.4.1	Equipment posing a threat of H1 shall have means of automated shutdown linked to exposed hot surface sensors.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS	(Y) Splendour of the Seas, Carnival Triumph	3	5	15
		20.5	Ship automation receives sensor data that exposed hot surfaces are present but misinterprets the data as normal conditions as the process model is not programmed to recognise exposed hot surfaces as a fire precursor, which leads to no engine shutdown and continued exposure of an ignition source	20.5.1	Exposed hot surface (>220 deg C) alarms shall be treated as a significant fire precursor with respect to automated shutdown/ cooling. Maintenance shall be in accordance with the manufacturer guidelines.		Inadequate process model	Audit of actions on alarms.	Audit of emergency response.	HS		3	3	9
		20.6	Lack of maintenance has resulted in the shutdown action being faulty and not operating.	20.6.1	Equipment shutdown measures shall achieve an availability/ reliability of 99%.		Inadequate maintenance	Sensor design, Signalling	Audit of alarm management. Availability/ reliability of sensors.	HS		3	2	6
		20.7	Sensors indicate exposed hot surface and issues command to shutdown the engine. No shutdown measures exist in the engine. Control action not completed	20.7.1	Equipment posing a risk of H-1 shall be capable of remote, automated shutdown.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS		3	2	6
		20.8	Automated shutdown action has been inhibited during maintenance and not brought back online.	20.8.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	HS		3	2	6
		21.1	Ship automation receives sensor data that excessive vibration is present but misinterprets the data as normal conditions due to inaccuracy in measurements and set points for automated action, resulting in continued engine operation and increasing fatigue	21.1.1	Set points applied to alarm to excessive vibration from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety), but not within the standard safe operating limit.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		21.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating excessive vibration are false alarms	21.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		21.3	No feedback exists to alert ship automation of excessive vibration as sensors have no direct contact with equipment subject to vibration fatigue which leads to no engine shutdown	21.3.1	Sensors used to show excessive vibration status shall be placed in direct contact with the equipment at risk of fatigue failure.		Inadequate safety system design	Sensor design, Signalling	Verification of design.	OL		3	3	9
21	**Ship automation does not shutdown the engine when excessive vibration exists (H2-3)**	21.4	No automation in place to shutdown engine on reception of excessive vibration	21.4.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to vibration sensors.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
		21.5	Ship automation receives sensor data that excessive vibration is present but misinterprets the data as normal conditions as the process model is not programmed to recognise this as a fire precursor, which leads to no engine shutdown	21.5.1	Excessive vibration alarms shall be treated as a significant fire precursor with respect to automated shutdown. Maintenance shall be in accordance with the manufacturer guidelines.		Inadequate process model	Audit of actions on alarms.	Audit of emergency response.	OL		3	3	9
		21.6	Lack of maintenance has resulted in the shutdown action being faulty and not operating.	21.6.1	Equipment shutdown measures shall achieve an availability/ reliability of 99%.		Inadequate maintenance	Sensor design, Signalling	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		21.7	Sensors indicate excessive vibration and issues command to shutdown the engine. No shutdown measures exist in the engine. Control action not completed	21.7.1	Equipment posing a risk of H2-3 shall be capable of remote, automated shutdown.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	2	6
		21.8	Automated shutdown action has been inhibited during maintenance and not brought back online.	21.8.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		22.1	Ship automation misinterprets the signals received from the engine and assumes a system deviation has taken place due to inappropriate set point selection and sends a shutdown signal. This results in increased load elsewhere on the system, breaking containment	22.1.1	Set points applied to alarm to system pressure deviation from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety), but not within the safe operating limits.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
22	**Ship automation shuts down the engine when pressure in the oil systems is normal (H2-3)**	22.2	Shutdown action is intended for a different engine from where the pressure deviation is present through incorrectly programmed control system, increasing demand on the already faulty engine	22.2.1	Automated shutdown shall be based directly from the sensors installed on that machine.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
		23.1	Ship automation misinterprets the signals received from the engine and assumes a system deviation has taken place due to inappropriate set point selection and sends a shutdown signal. This results in increased load elsewhere on the system, breaking containment	23.1.1	Set points applied to alarm to exposed hot surfaces shall be set based on detecting surfaces of over 220 deg C. A suitable factor of safety shall be implemented, and design shall allow for full coverage of all credible areas where they can occur.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
23	**Ship automation shuts down the engine when there is no exposed hot surface (H2-3)**	23.2	Shutdown action is intended for a different engine from where the exposed hot surface is present through incorrectly programmed control system	23.2.1	Automated shutdown shall be based directly from the sensors installed on that machine.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
		24.1	Ship automation misinterprets the signals received from the engine and assumes a system deviation has taken place due to inappropriate set point selection and sends a shutdown signal. This results in increased load elsewhere on the system, breaking containment	24.1.1	Set points applied to alarm to excessive vibration from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety), but not within the standard safe		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
24	**Ship automation shuts down the engine when vibration levels are normal (H2-3)**	24.2	Shutdown action is intended for a different engine from where the exposed hot surface is present through incorrectly programmed control system	24.2.1	Automated shutdown shall be based directly from the sensors installed on that machine.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
		25.1	Feedback on excessive stream pressure provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on increased pressure, resulting in engine break in containment	25.1.1	Oil system pressure sensors shall operate in real time, providing an indication of status with 1 second of accuracy.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design. Function testing.	OL		3	3	9
		25.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating pressure deviation are false alarms. Shutdown only activated when further alarms are received.	25.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		25.3	No automation in place to shutdown engine therefore manual detection relied upon which has a delayed response.	25.3.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to pressure sensors.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL	(Y) Piet Engine Fire Leak Data Event ID 90244	3	4	12
25	**Ship automation shuts down the engine too late when there is a pressure deviation in the oil systems (H2-3)**	25.4	Feedback on excessive stream pressure provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on increased pressure, resulting in engine break in containment	25.4.1	Shutdown measures shall be maintained in line with manufacturer recommendations.	Inadequate emergency reponse	Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	3	9
		25.5	Automated shutdown action has been inhibited during maintenance and not brought back online.	25.5.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		25.6	Feedback on excessive stream pressure provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on increased pressure, resulting in engine break in containment	25.6.1	Emergency shutdown measures shall operate at a sufficiently fast response to reduce oil flow pressure where this has exceeded safe levels.		Inadequate safety system design	Emergency shutdown design	Verification of design. Function testing.	OL		3	3	9
		26.1	Feedback on oil leak provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on oil leak	26.1.1	Oil leak detectors shall operate in real time, providing an indication of status with 1 second of accuracy.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design. Function testing.	OL		3	3	9
		26.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating oil leak are false alarms. Shutdown only activated when further alarms are received.	26.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	OL	(Y) Carnival Triumph	3	4	12
		26.3	No automation in place to shutdown engine therefore manual detection relied upon which has a delayed response.	26.3.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to oil mist detectors.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
26	**Ship automation shuts down the engine too late during an oil leak (H2-3)**	26.4	Feedback on oil leak provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on oil leak	26.4.1	Shutdown measures shall be maintained in line with manufacturer recommendations.	Inadequate emergency reponse	Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	3	9
		26.5	Automated shutdown action has been inhibited during maintenance and not brought back online.	26.5.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		26.6	Feedback on oil leak provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on oil leak	26.6.1	Emergency shutdown measures shall operate at a sufficiently fast response to isolate flammable materials before they reach an ignition source.		Inadequate safety system design	Emergency shutdown design	Verification of design. Function testing.	OL		3	3	9
		27.1	Feedback on exposed hot surface provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on engine	27.1.1	Exposed hot surface detectors shall operate in real time, providing an indication of status with 1 second of accuracy.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design. Function testing.	HS		3	3	9
		27.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating exposed hot surface are false alarms. Shutdown only activated when further alarms are received.	27.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		3	2	6
		27.3	No automation in place to shutdown engine therefore manual detection relied upon which has a delayed response.	27.3.1	Equipment posing a threat of H1 shall have means of automated shutdown linked to hot surface detectors.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS		3	1	3
27	**Ship automation shuts down the engine too late when exposed hot surface exists (H-1).**	27.4	Feedback on exposed hot surface provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on engine	27.4.1	Shutdown measures shall be maintained in line with manufacturer recommendations.	Inadequate emergency reponse	Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	HS		3	3	9
		27.5	Automated shutdown action has been inhibited during maintenance and not brought back online.	27.5.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	HS		3	2	6
		27.6	Feedback on exposed hot surface provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on engine	27.6.1	Emergency shutdown measures shall operate at a sufficiently fast response to remove continued operation which would sustain or increase the exposed hot surface.		Inadequate safety system design	Emergency shutdown design	Verification of design. Function testing.	HS		3	3	9
		28.1	Feedback on excessive vibration provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on engine	28.1.1	Vibration sensors shall operate in real time, providing an indication of status with 1 second of accuracy.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design. Function testing.	OL		3	3	9
		28.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating excessive vibration are false alarms. Shutdown only activated when further alarms are received.	28.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
28	**Ship automation shuts down the engine too late when excessive**	28.3	No automation in place to shutdown engine therefore manual detection relied upon which has a delayed response.	28.3.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to vibration sensors.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3

	vibration exists (H2-3)														
		28.4	Feedback on excessive vibration provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on engine	28.4.1	Shutdown measures shall be maintained in line with manufacturer recommendations.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	3	9
		28.5	Automated shutdown action has been inhibited during maintenance and not brought back online.	28.5.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		28.6	Feedback on excessive vibration provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on engine	28.6.1	Emergency shutdown measures shall operate at a sufficiently fast response to eliminate excessive vibration on a potentially fatigued piece of equipment.		Inadequate safety system design	Emergency shutdown design	Verification of design. Function testing.	OL		3	3	9
		29.1	Ship automation receives sensor data of increased pressure but misinterprets the data as normal operation due to incorrect set point settings therefore does not send shutdown signal, resulting in break in containment	29.1.1	Set points applied to alarm to system pressure deviation from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety)		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		29.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating pressure deviation are false alarms	29.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		29.3	No automation in place to shutdown fuel supply on reception of pressure deviation alarm	29.3.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to pressure sensors.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL	(Y) Piet Engine Fire Leak Data Event ID 90244	3	4	12
29	**Ship automation does not shutdown the fuel supply when there is a pressure deviation in the oil systems (H2-3)**	29.4	Shutdown action is on different fuel supply from where the pressure deviation is present through incorrectly programmed control system	29.4.1	Automated shutdown shall be based directly from the sensors installed on that machine.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
		29.5	Lack of maintenance has resulted in the shutdown action being faulty and not operating.	29.5.1	Maintenance shall be in accordance with the manufacturer guidelines. Equipment shutdown measures shall achieve an availability/ reliability of 99%.		Inadequate maintenance	Sensor design, Signalling	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		29.6	Sensors indicate unsafe pressure in pipework and issues command to shutdown the fuel supply. No shutdown measures exist in the fuel supply. Control action not completed	29.6.1	Equipment posing a risk of H2-3 shall be capable of remote, automated shutdown.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	2	6
		29.7	Automated shutdown action has been inhibited during maintenance and not brought back online.	29.7.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		30.1	Ship automation receives sensor data that an oil leak is present but misinterprets the data as normal conditions due to excessively high set points for automated action, resulting in continued fuel supply which could be leaking flammable materials	30.1.1	Set points applied to alarm to system pressure drop in the event of a leak shall be set based on the anticipated pressure which could be presented through a break in containment.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		30.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating oil leak are false alarms	30.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		30.3	Ship automation receives sensor data of reduced pressure as a result of a leak but misinterprets the data as normal operation due to incorrect set point settings therefore does not send shutdown action, resulting in continued fuel supply	30.3.1	Set points applied to alarm to system pressure drop in the event of a leak shall be set based on the anticipated pressure which could be presented through a break in containment.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL	(Y) Piet Engine Fire Leak Data Event ID 90244	3	4	12
30	**Ship automation does not shutdown the fuel supply during an oil leak (H2-3)**	30.4	No automation in place to shutdown fuel supply on reception of oil leak alarm	30.4.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to oil leak detectors. Maintenance shall be in accordance with the manufacturer guidelines.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL	(Y) Splendour of the Seas, Carnival Triumph	3	4	12
		30.5	Lack of maintenance has resulted in the shutdown action being faulty and not operating.	30.5.1	Equipment shutdown measures shall achieve an availability/ reliability of 99%.		Inadequate maintenance	Sensor design, Signalling	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		30.6	Sensors indicate oil leak and issues command to shutdown the fuel supply. No shutdown measures exist in the fuel supply. Control action not completed	30.6.1	Equipment posing a risk of H2-3 shall be capable of remote, automated shutdown.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	2	6
		30.7	Automated shutdown action has been inhibited during maintenance and not brought back online.	30.7.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		31.1	Ship automation receives sensor data that an exposed hot surface is present but misinterprets the data as normal conditions due to inaccuracy in measurements and set points for automated action, resulting in continued fuel supply, which could rupture and meet the hot surface	31.1.1	Set points applied to alarm to exposed hot surfaces shall be set based on detecting surfaces of over 220 deg C. A suitable factor of safety shall be implemented, and design shall allow for full coverage of all credible areas where they can occur.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	HS		3	2	6
		31.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating exposed hot surface are false alarms	31.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		3	2	6
		31.3	No feedback exists to alert ship automation of exposed hot surfaces as sensors have no direct field of view directly to the hot surface which leads to no engine fuel supply shutdown and continued exposure of an ignition source in an area processing flammable materials	31.3.1	Sensors used to detect exposed hot surfaces shall be placed with clear contact/ field of view with the equipment at risk.		Inadequate safety system design	Sensor design	Verification of design.	HS		3	3	9
31	**Ship automation does not shutdown the fuel supply when exposed hot surface exists (H-1).**	31.4	No automation in place to shutdown fuel supply on reception of exposed hot surface alarm	31.4.1	Equipment posing a threat of H1 shall have means of automated shutdown linked to hot surface detectors.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS	(Y) Splendour of the Seas, Carnival Triumph	3	5	15
		31.5	Ship automation receives sensor data that exposed hot surfaces are present but misinterprets the data as normal conditions as the process model is not programmed to recognise exposed hot surfaces as a fire precursor, which leads to no fuel supply shutdown and continued exposure of an ignition source in an area processing flammable materials	31.5.1	Exposed hot surface (>220 deg C) alarms shall be treated as a significant fire precursor with respect to automated shutdown/ cooling. Maintenance shall be in accordance with the manufacturer guidelines.		Inadequate process model	Audit of actions on alarms.	Audit of emergency response.	HS		3	3	9
		31.6	Lack of maintenance has resulted in the shutdown action being faulty and not operating.	31.6.1	Equipment shutdown measures shall achieve an availability/ reliability of 99%.		Inadequate maintenance	Sensor design, Signalling	Audit of alarm management. Availability/ reliability of sensors.	HS		3	2	6
		31.7	Sensors indicate exposed hot surface and issues command to shutdown the fuel supply. No shutdown measures exist in the fuel system. Control action not completed	31.7.1	Equipment posing a risk of H-1 shall be capable of remote, automated shutdown.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS		3	2	6
		31.8	Automated shutdown action has been inhibited during maintenance and not brought back online.	31.8.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	HS		3	2	6
		32.1	Ship automation receives sensor data that excessive vibration is present but misinterprets the data as normal conditions due to inaccuracy in measurements and set points for automated action, resulting in continued fuel supply operation and increasing fatigue	32.1.1	Set points applied to alarm to excessive vibration from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety), but not within the standard safe operating limit.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
		32.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating excessive vibration are false alarms	32.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		32.3	No feedback exists to alert ship automation of excessive vibration as sensors have no direct contact with equipment subject to vibration fatigue which leads to no fuel supply shutdown	32.3.1	Sensors used to show excessive vibration status shall be placed in direct contact with the equipment at risk of fatigue failure.		Inadequate safety system design	Sensor design, Signalling	Verification of design.	OL		3	3	9
32	**Ship automation does not shutdown the fuel supply when excessive vibration exists (H2-3)**	32.4	No automation in place to shutdown fuel supply on reception of excessive vibration	32.4.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to vibration sensors.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
		32.5	Ship automation receives sensor data that excessive vibration is present but misinterprets the data as normal conditions as the process model is not programmed to recognise this as a fire precursor, which leads to no fuel supply shutdown	32.5.1	Excessive vibration alarms shall be treated as a significant fire precursor with respect to automated shutdown. Maintenance shall be in accordance with the manufacturer guidelines.		Inadequate process model	Audit of actions on alarms.	Audit of emergency response.	OL		3	3	9
		32.6	Lack of maintenance has resulted in the shutdown action being faulty and not operating.	32.6.1	Equipment shutdown measures shall achieve an availability/ reliability of 99%.		Inadequate maintenance	Sensor design, Signalling	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		32.7	Sensors indicate excessive vibration and issues command to shutdown the engine. No shutdown measures exist in the fuel supply. Control action not completed	32.7.1	Equipment posing a risk of H2-3 shall be capable of remote, automated shutdown.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	2	6
		32.8	Automated shutdown action has been inhibited during maintenance and not brought back online.	32.8.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		33.1	Ship automation misinterprets the signals received from the fuel supply system and assumes a system deviation has taken place due to inappropriate set point selection and sends a shutdown signal. This results in increased load elsewhere on the system, breaking containment	33.1.1	Set points applied to alarm to system pressure deviation from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety) but not within the safe operating limit.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
33	**Ship automation shuts down the fuel supply when pressure in the oil systems is normal (H2-3)**	33.2	Shutdown action is intended for a different fuel supply from where the pressure deviation is present through incorrectly programmed control system, increasing demand on the already faulty engine	33.2.1	Automated shutdown shall be based directly from the sensors installed on that machine.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
		34.1	Ship automation misinterprets the signals received from the engine and assumes a system deviation has taken place due to inappropriate set point selection and sends a shutdown signal. This results in increased load elsewhere on the system, breaking containment	34.1.1	Set points applied to alarm to exposed hot surfaces shall be able to detect surfaces >220 deg C but not within the standard safe operating limit of machinery.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
34	**Ship automation shuts down the fuel supply when there is no exposed hot surface (H2-3)**	34.2	Shutdown action is intended for a different fuel supply from where the exposed hot surface is present through incorrectly programmed control system	34.2.1	Automated shutdown shall be based directly from the sensors installed on that machine.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
		35.1	Ship automation misinterprets the signals received from the fuel supply and assumes a system deviation has taken place due to inappropriate set point selection and sends a shutdown signal. This results in increased load elsewhere on the system, breaking containment	35.1.1	Set points applied to alarm to excessive vibration from safe levels shall be less than those specified by the manufacturer as being within the design tolerance (including a factor of safety), but not within the standard safe operating limit.		Inadequate process model	Sensor design, Signalling	Verification of design. Function testing.	OL		3	2	6
35	**Ship automation shuts down the fuel supply when vibration levels are normal (H2-3)**	35.2	Shutdown action is intended for a different fuel supply from where the exposed hot surface is present through incorrectly programmed control system	35.2.1	Automated shutdown shall be based directly from the sensors installed on that machine.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
		36.1	Feedback on excessive stream pressure provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on increased pressure, resulting in fuel supply break in containment	36.1.1	Oil system pressure sensors shall operate in real time, providing an indication of status with 1 second of accuracy.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design. Function testing.	OL		3	3	9
		36.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating pressure deviation are false alarms. Shutdown only activated when further alarms are received.	36.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
		36.3	No automation in place to shutdown fuel supply therefore manual detection relied upon which has a delayed response.	36.3.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to pressure sensors.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL	(Y) Piet Engine Fire Leak Data Event ID 90244	3	4	12
36	**Ship automation shuts down the fuel supply too late when there is a pressure deviation in the oil systems (H2-3)**	36.4	Feedback on excessive stream pressure provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on increased pressure, resulting in engine break in containment	36.4.1	Shutdown measures shall be maintained in line with manufacturer recommendations.	Inadequate emergency reponse	Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	3	9
		36.5	Automated shutdown action has been inhibited during maintenance and not brought back online.	36.5.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		36.6	Feedback on excessive stream pressure provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on increased pressure, resulting in engine break in containment	36.6.1	Emergency shutdown measures shall operate at a sufficiently fast response to reduce oil flow pressure where this has exceeded safe levels.		Inadequate safety system design	Emergency shutdown design	Verification of design. Function testing.	OL		3	3	9
		37.1	Feedback on oil leak provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on oil leak	37.1.1	Oil leak detectors shall operate in real time, providing an indication of status with 1 second of accuracy.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design. Function testing.	OL		3	3	9
		37.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating oil leak are false alarms. Shutdown only activated when further alarms are received.	37.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	OL	(Y) Carnival Triumph	3	4	12
37	**Ship automation shuts down the fuel supply too late during an oil leak (H2-3)**	37.3	No automation in place to shutdown fuel supply therefore manual detection relied upon which has a delayed response.	37.3.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to oil leak detectors.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3
		37.4	Feedback on oil leak provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on oil leak	37.4.1	Shutdown measures shall be maintained in line with manufacturer recommendations.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	3	9
		37.5	Automated shutdown action has been inhibited during maintenance and not brought back online.	37.5.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		37.6	Feedback on oil leak provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on oil leak	37.6.1	Emergency shutdown measures shall operate at a sufficiently fast response to isolate flammable materials before they reach an ignition source.		Inadequate safety system design	Emergency shutdown design	Verification of design. Function testing.	OL		3	3	9
		38.1	Feedback on exposed hot surface provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on fuel supply	38.1.1	Exposed hot surface detectors shall operate in real time, providing an indication of status with 1 second of accuracy.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design. Function testing.	HS		3	3	9
		38.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating exposed hot surface are false alarms. Shutdown only activated when further alarms are received.	38.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		3	2	6
		38.3	No automation in place to shutdown fuel supply therefore manual detection relied upon which has a delayed response.	38.3.1	Equipment posing a threat of H1 shall have means of automated shutdown linked to hot surface detectors.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS		3	1	3
38	**Ship automation shuts down the fuel supply too late when exposed hot surface exists (H-1).**	38.4	Feedback on exposed hot surface provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on fuel supply	38.4.1	Shutdown measures shall be maintained in line with manufacturer recommendations.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	HS		3	3	9
		38.5	Automated shutdown action has been inhibited during maintenance and not brought back online.	38.5.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	HS		3	2	6
		38.6	Feedback on exposed hot surface provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on fuel supply	38.6.1	Emergency shutdown measures shall operate at a sufficiently fast response to remove continued operation which would sustain or increase the exposed hot surface.		Inadequate safety system design	Emergency shutdown design	Verification of design. Function testing.	HS		3	3	9
		39.1	Feedback on excessive vibration provided too late due to delays in sensor readings due to technology selection resulting in delayed shutdown action on fuel supply	39.1.1	Vibration sensors shall operate in real time, providing an indication of status with 1 second of accuracy.		Inadequate feedback of the hazard	Sensor design, Signalling	Verification of design. Function testing.	OL		3	3	9
		39.2	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating excessive vibration are false alarms. Shutdown only activated when further alarms are received.	39.2.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	OL		3	2	6
39	**Ship automation shuts down the fuel supply too late when excessive**	39.3	No automation in place to shutdown fuel supply therefore manual detection relied upon which has a delayed response.	39.3.1	Equipment posing a threat of H2-3 shall have means of automated shutdown linked to vibration sensors.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	OL		3	1	3

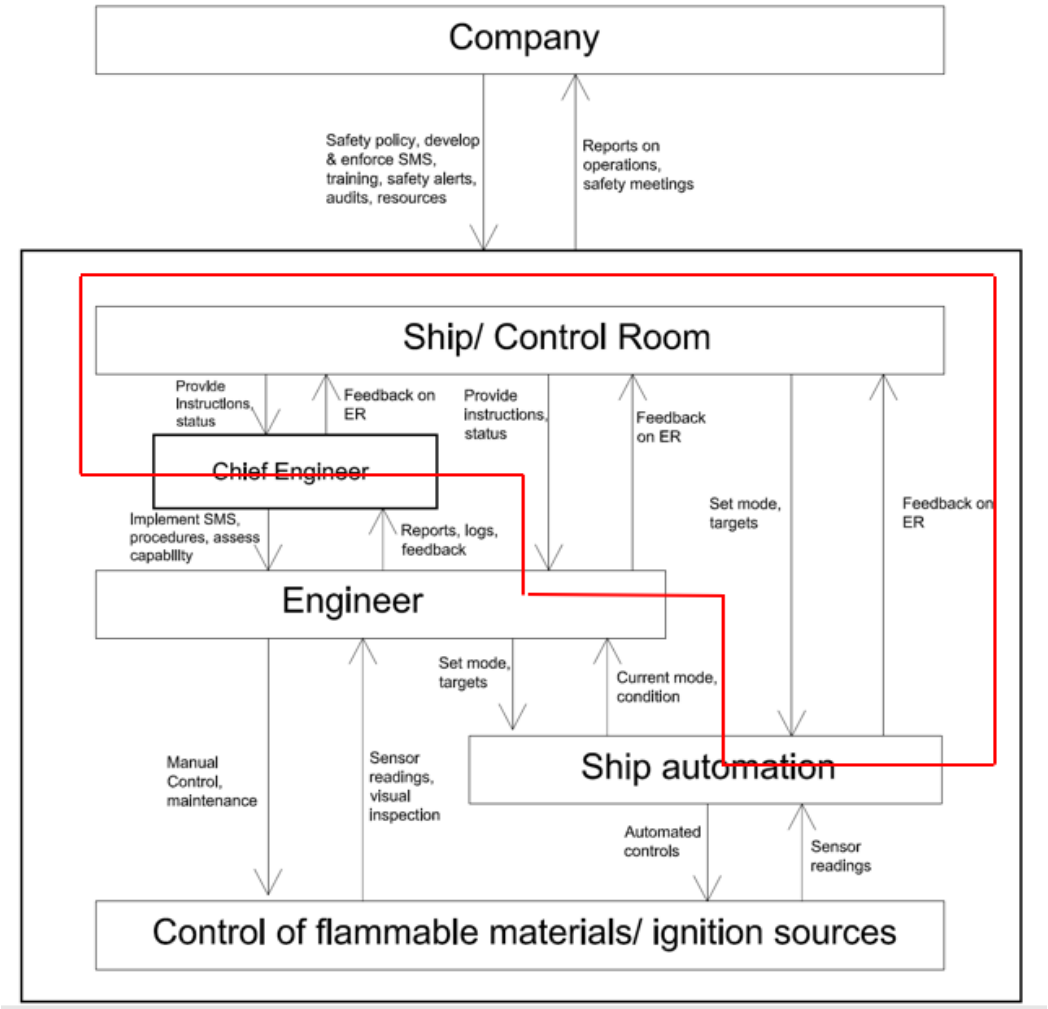
	vibration exists (H2-3)	39.4	Feedback on excessive vibration provided, shutdown command sent but mechanical shutdown is delayed due to wear and tear of equipment and inadequate maintenance resulting in delayed shutdown action on fuel supply	39.4.1	Shutdown measures shall be maintained in line with manufacturer recommendations.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	3	9
		39.5	Automated shutdown action has been inhibited during maintenance and not brought back online.	39.5.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	OL		3	2	6
		39.6	Feedback on excessive vibration provided, shutdown command sent but mechanical shutdown is delayed due to equipment spec not being of a sufficiently fast response resulting in delayed shutdown action on fuel supply	39.6.1	Emergency shutdown measures shall operate at a sufficiently fast response to eliminate excessive vibration on a potentially fatigued piece of equipment.		Inadequate safety system design	Emergency shutdown design	Verification of design. Function testing.	OL		3	3	9
		40.1	Set points not accurate to start-up adjacent engines before design deviation thresholds are exceeded.	40.1.1	Set points at which adjacent engines are started up shall ensure that operating engines to not exceed the safe operating thresholds with respect to load.		Inadequate process model	Function testing	Verification of design. Function testing.	OL + HS		3	3	9
		40.2	No logic present to automate the control of multiple engines to ensure a steady load application.	40.2.1	Automation shall ensure adjacent engines can be utilised to reduce excessive loads on operational engines.		Inadequate safety system design	Function testing	Verification of design. Function testing.	OL + HS	(Y) Splendour of the Seas	3	4	12
40	**Engine/ fuel supply not started when an adjacent engine is over its design load (H1-3)**	40.3	Faulty sensors cannot detect adjacent engine in excess of design load and automate start-up of adjacent engines through lack of maintenance.	40.3.1	Sensors used to show operational status shall be reliable on demand	Inadequate emergency reponse	Inadequate maintenance	Function testing	Availability/ reliability study/ statistics	OL + HS		3	3	9
				40.3.2	Sensors shall be maintained in line with manufacturer recommendations.			Audit of maintenance procedure	Audit of maintenance process			3	0	0
		40.4	Engine which would have been started up due to automated start-up is out of service for maintenance	40.4.1	Where no engine is available to alleviate the excessive load suitable warnings shall be provided to the ECR and engineers of the increased risk of fire.		Inadequate redundancy measures	Alarm management procedure	Audit of alarm management	OL + HS		3	2	6
				40.4.2	Maintenance teams shall ensure engines which are out of service are reintroduced as soon as possible.			Audit of maintenance procedure	Audit of maintenance process			3	3	9
41	**Engine/ fuel supply started when low pressure exists due to an existing leak (H2-3)**	41.1	Engine shows low efficiency, therefore automation increases/ starts up the fuel supply, sending flammable materials to the source of the leak.	41.1.1	Upon increase/ start-up of the fuel, if an increase in pressure is not detected at the engine within 5 seconds, fuel supply shall be stopped.	Inadequate emergency reponse	Inadequate process model	Audit of actions on alarms.	Audit of emergency response. Function testing.	OL	(Y) Splendour of the Seas	3	5	15
42	**Engine/ fuel supply started when equipment is intended to be out of service (H2-3)**	42.1	Engine which is started up to assist other engines, is out of service for maintenance, but starts up anyway.	42.1.1	Engines which are out of service shall not be capable of start-up.	Inadequate emergency reponse	Inadequate maintenance	Lock outs of equipment, inhibits	Verification of design. Function testing.	OL		3	3	9
		43.1	Set points not accurate to start-up adjacent engines before design deviation thresholds are exceeded.	43.1.1	Set points at which adjacent engines are started up shall ensure that operating engines to not exceed the safe operating thresholds with respect to load.		Inadequate process model	Function testing	Verification of design. Function testing.	OL + HS		3	3	9
43	**Engine/ fuel supply started too late when an adjacent engine is over its design load (H1-3)**	43.2	No logic present to automate the control of multiple engines to ensure a steady load application. Engine/ fuel supply not started until manual intervention occurs.	43.2.1	Automation shall ensure adjacent engines can be utilised to reduce excessive loads on operational engines.	Inadequate emergency reponse	Inadequate safety system design	Function testing	Verification of design. Function testing.	OL + HS	(Y) Splendour of the Seas	3	4	12
		43.3	Faulty sensors cannot detect and automate start-up of adjacent engines through lack of maintenance. Manual start-up required which is delayed.	43.3.1	Sensors used to show operational status shall be reliable on demand		Inadequate maintenance	Function testing	Availability/ reliability study/ statistics	OL + HS		3	1	3
				43.3.2	Sensors shall be maintained in line with manufacturer recommendations.			Audit of maintenance procedure	Audit of maintenance process			3	0	0
		44.1	ECR/ engineer prevents the release of the water mist system as they believe the alarms indicating oil leak are false alarms	44.1.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		2	2	4
		44.2	No automation in place to automatically release deluge on reception of sufficient alarm alarms indicating oil leak	44.2.1	Equipment posing a threat of H1 shall have means of automated water mist release linked to oil leak detectors.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS		2	2	4
44	**Ship automation doesn't release the water mist when leak exists (H-1).**	44.3	Water mist released in the wrong location from where the leak is present as the leak detectors are incorrectly programmed to the automated release	44.3.1	Water mist release shall be based directly from the sensors installed on that machine.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS		2	1	2
		44.4	Automated water mist release has been inhibited during maintenance and not brought back online.	44.4.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	HS		2	2	4
		44.5	Lack of maintenance has resulted in the water mist valves seizing shut, meaning water mist cannot be released.	44.5.1	Maintenance shall be in accordance with the manufacturer guidelines. Water mist release measures shall achieve an availability/ reliability of 99%.		Inadequate maintenance	Audit of maintenance procedure, Function testing	Audit of maintenance. Availability/ reliability of water mist system.	HS		2	2	4
		45.1	ECR/ engineer prevents the release of the water mist system as they believe the alarms indicating exposed hot surfaces are false alarms	45.1.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		2	2	4
		45.2	No automation in place to automatically release deluge on reception of sufficient alarm alarms indicating exposed hot surface	45.2.1	Equipment posing a threat of H1 shall have means of automated water mist release linked to oil leak detectors.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS	(Y) Splendour of the seas, Carnival Triumph	2	4	8
45	**Ship automation doesn't release the water mist when exposed hot surface exists (H-1)**	45.3	Water mist released in the wrong location from where the exposed hot surface is present as the leak detectors are incorrectly programmed to the automated release	45.3.1	Water mist release shall be based directly from the sensors installed on that machine.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS		2	1	2
		45.4	Automated water mist release has been inhibited during maintenance and not brought back online.	45.4.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	HS		2	2	4
		45.5	Lack of maintenance has resulted in the water mist valves seizing shut, meaning water mist cannot be released.	45.5.1	Maintenance shall be in accordance with the manufacturer guidelines. Water mist release measures shall achieve an availability/ reliability of 99%.		Inadequate maintenance	Audit of maintenance procedure, Function testing	Audit of maintenance. Availability/ reliability of water mist system.	HS		2	2	4
		46.1	ECR/ engineer prevents the release of the water mist system as they believe the alarms indicating oil leak are false alarms. Water mist only released when further alarms are received.	46.1.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		2	2	4
		46.2	No automation in place to automatically release deluge on reception of sufficient alarm alarms indicating oil leak. Release only occurs on manual detection of a leak.	46.2.1	Equipment posing a threat of H1 shall have means of automated water mist release linked to oil leak detectors.		Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS		2	2	4
46	**Ship automation releases the water mist too late when leak exists (H-1).**	46.3	Sensors which detect the presence of oil leak are not a fast enough response to provide fast response water mist release.	46.3.1	Oil mist detectors shall operate at a sufficiently fast response to immediately mitigate any ignition sources within the vicinity of the leak.	Inadequate emergency reponse	Inadequate safety system design	Sensor design, Signalling	Verification of design. Function testing.	HS		2	3	6
		46.4	Automated water mist release has been inhibited during maintenance and not brought back online.	46.4.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	HS		2	2	4
		47.1	ECR/ engineer prevents the release of the water mist system as they believe the alarms indicating exposed hot surfaces are false alarms. Water mist only released when further alarms are received.	47.1.1	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.		Inadequate mental model	Alarm management procedure. Fault rectification.	Audit of alarm management. Availability/ reliability of sensors.	HS		2	2	4
47	**Ship automation releases the water mist too late when exposed hot surface exists (H-1)**	47.2	No automation in place to automatically release deluge on reception of sufficient alarm alarms indicating exposed hot surface. Release only occurs on manual detection of a hot surface.	47.2.1	Equipment posing a threat of H1 shall have means of automated water mist release.	Inadequate emergency reponse	Inadequate safety system design	Equipment design	Verification of design. Function testing.	HS	(Y) Splendour of the seas, Carnival Triumph	2	4	8
		47.3	Sensors which detect the presence of exposed hot surface are not a fast enough response to provide fast response water mist release.	47.3.1	Exposed hot surface detectors shall operate at a sufficiently fast response to immediately mitigate any ignition sources within the vicinity.		Inadequate safety system design	Sensor design, Signalling	Verification of design. Function testing.	HS		2	3	6
		47.4	Automated water mist release has been inhibited during maintenance and not brought back online.	47.4.1	Upon completion of maintenance, all inhibits shall be removed.		Inadequate maintenance	Audit of maintenance procedure	Audit of maintenance process	HS		2	2	4
		48.1	ECR/ engineer prevents the release of the water mist system as they believe the leak no longer presents a risk.	48.1.1	Engineer shall be aware of emergency response and on the factors to review in assuming a situation no longer poses a risk of H-1.		Inadequate mental model	Training procedure/ Emergency procedure	Audit of procedures can be the signal of performance.	HS	(Y) - Splendour of the Seas	2	5	10
48	**Ship automation stops the water mist release too soon when oil leak is still present (H-1)**	48.2	Sensors show the oil leak has been removed therefore deluge is stopped. The oil leak continues without water mist presence.	48.2.1	Engineers shall be made aware of an automated stop to the water mist release to verify if the leak remains in the ER.	Inadequate emergency reponse	Inadequate emergency response	Audit of actions on alarms.	Audit of indicator management. Audit of emergency response.	HS		2	3	6
		48.3	Fire erupts, causing short on power supply, stopping the deluge.	48.3.1	Fire safety system supply cabling shall be fire resistant.		Inadequate safety system design	Audit of design	Verification of design	HS		2	3	6
		48.4	Water mist release water capacity is depleted and actions to stop the leak have not yet been completed.	48.4.1	Water mist systems shall be capable of continuing water deluge on hazardous equipment through back up supplies i.e. seawater		Inadequate safety system design	Audit of design	Verification of design	HS		2	3	6
		49.1	ECR/ engineer prevents the release of the water mist system as they believe the exposed hot surface no longer presents a risk.	49.1.1	Engineer shall be aware of emergency response and on the factors to review in assuming a situation no longer poses a risk of H-1.		Inadequate mental model	Training procedure/ Emergency procedure	Audit of procedures can be the signal of performance.	HS	(Y) - Splendour of the Seas	2	5	10
49	**Ship automation stops the water mist release too soon when exposed hot surface still exists (H-1)**	49.2	Sensors show the exposed hot surface has been removed therefore deluge is stopped. The exposed hot surface re-emerges without water mist presence.	49.2.1	Engineers shall be made aware of an automated stop to the water mist release to verify if the hot surface remains in the ER.	Inadequate emergency reponse	Inadequate emergency response	Audit of actions on alarms.	Audit of indicator management. Audit of emergency response.	HS		2	3	6
		49.3	Fire erupts, causing short on power supply, stopping the deluge.	49.3.1	Fire safety system supply cabling shall be fire resistant.		Inadequate safety system design	Audit of design	Verification of design	HS		2	3	6
		49.4	Water mist release water capacity is depleted and actions to remove the exposed hot surface have not yet been completed.	49.4.1	Water mist systems shall be capable of continuing water deluge on hazardous equipment through back up supplies i.e. seawater		Inadequate safety system design	Audit of design	Verification of design	HS		2	3	6

Barrier Criticality

Barrier Effectiveness



Scale of Colours
Green = 1-8
Amber = 9-15
Red = 16-30


Company
Safety policy, develop & enforce SMS, training, safety alerts, audits, resources
Reports on operations, safety meetings
Ship/ Control Room
Provide Instructions, status
Feedback on ER
Provide instructions, status
Feedback on ER
Chief Engineer
Set mode, targets
Feedback on ER
Implement SMS, procedures, assess capability
Reports, logs, feedback
Engineer
Set mode, targets
Current mode, condition
Manual Control, maintenance
Sensor readings, visual inspection
Ship automation
Automated controls
Sensor readings
Control of flammable materials/ ignition sources

Engine Control Room (ECR)

Objective/ responsibility	Oversee actions of the chief engineer, engineer and automation controllers. Provide instruction or actions to prevent exposed hot surfaces or the release of flammable materials. Reporting back to the company on operations and safety.
Input	Feedback from Chief Engineer/ engineers and automation sensors. Instructions, policies and resources from the company.
Output	Instructions to chief engineer/ engineer, setting the automation requirements. Reports back to the company.
Constraints	Resources, Time, Instructions, Training, Autonomy

Hazards

H1	Hot surfaces (>220degC) in ER
H2	Leak from pressurised oil systems
H3	Failure to contain oil leak

	Actions	**Not providing**	**Providing**	**Too early**	**Too late**	**Stopped to soon (applied too short)**	**Applied too long**
A1	Report on operations and safety	ECR does not report on loss of integrity to company who would approve a review of safety (H-1, H-2, H-3)	ECR report on integrity to company is too vague when a specific alteration/ upgrade is required (H-1, H-2, H-3) ECR report on integrity is inaccurate concealing safety issues on board.		ECR reports on inegrity too late when equipment requiring replacement/ upgrade remains in place (H-1, H-2, H-3)		
A2	Provide Status to Chief Engineer/ Engineer	ECR does not provide operational status meaning engineer/ chief engineer breaks containment (H2-3) ECR does not provide status of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1) ECR does not provide status of imminent/ existing leak from oil system meaning engineer/ chief engineer does not provide a fix (H2-3)	ECR provides incorrect operational status meaning engineer/ chief engineer breaks containment (H2-3)		ECR provides status too late of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1) ECR provides status of imminent/ existing leak from oil system too late meaning engineer/ chief engineer does not provide a fix (H2-3)		
A3	Provide Instruction to Chief Engineer/ Engineer	ECR does not provide instruction to chief engineer/ engineer when exposed hot surfaces or potential/ existing oil leak is present (H1-3)	ECR provides instruction to break containment when equipment is operational (H2-3) ECR provides instruction to ignore the exposed hot surfaces (H-1)		ECR provide instruction to chief engineer/ engineer too late therefore measures to remedy exposed hot surfaces or potential/ existing oil leak are not implemented (H1-3)		
A4	Set operating mode of automation	ECR does not set operating mode of automation when automation is required to detect/ prevent exposed hot surfaces or an oil leak (H1-3)	ECR sets an inapproriate operating mode of automation when automation is required to detect/ prevent exposed hot surfaces or an oil leak (H1-3)				
A5	Shutdown Engine	ECR doesn't shutdown the engine when exposed hot surfaces exist (H-1) ECR doesn't shutdown the engine when strain on the engine components exceeeds design threshold (H-2, H-3)	ECR shuts down the engine and does not immediately reduce load on other engines which become temporarely overloaded (H-1, H-2)		ECR shuts down the engine too late when a fuel/ lube oil release exists (H-2, H-3) ECR doesn't shutdown the engine fast enough when exposed hot surfaces exist (H-1)		
A6	Shutdown Fuel Supply	ECR doesn't shutdown the fuel supply when strain on the components exceeeds design threshold (H-2, H-3)			ECR shuts down the fuel suply too late when a fuel/ lube oil release exists (H-2, H-3)		
A7	Release Water Mist	ECR doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)			ECR releases the water mist too late when leak exists (H-1). ECR releases the water mist too late when exposed hot surface exists (H-1)	ECR stops the water mist too soon when hot exposed surfaces have existed and and oil mist in atmosphere is detected/suspected (H-1)	

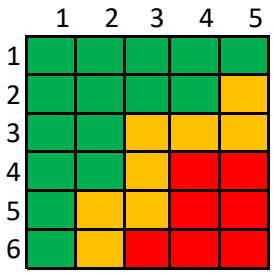
ID	Unsafe control action	Inadequate input (missing, wrong, too late/early etc.) / out-of-range disturbances	Inadequate control algorithm (fault, data handling etc.) /Inadequate responsibilities, knowledge or skills	Inconsistent process (mental) model	Design of incomplete process (mental) model	Inadequate feedback (incomplete, too late, missing, etc.)	Inadequate control path (too late, etc.)	Unrully controlled process
	ECR does not report on loss of integrity to company who would approve a review of safety (H-1, H-2, H-3)		Company liaison on the ship is not trained in report writing and fails to communicate the loss of integrity to the hierarchy meaning management are unaware of the ocurrence of fatigue to the hot box, fatigue of the fuel supply system, or exposed hot surfaces. ECR instructs engineers to implement a required upgrade. The work is carried out in an uncontrolled/ undocumented way. Company are unaware of what equipment is upgraded/ what is outstanding.	ECR is made aware of exposed hot surfaces/ the potential for oil system rupture but these signals have become normalised over time.			Workload of staff on the ship too extensive that no time is dedicated to writing the report and the loss of integrity is not reported to the company. Ship believe any issues associated with exposed hot surfaces or leak potential are in hand, therefore do not pass on the information to the company. The ship fails to notice a trend towards failure.	
	ECR report on integrity to company is too vague when a specific alteration/ upgrade is required (H-1, H-2, H-3)	Input from engineers/ sensors does not provide specific enough information to pinpoint the exact nature of the risk.	Company liaison on the ship is not trained in report writing and fails to communicate the loss of integrity to the hierarchy meaning management are unaware of the ocurrence of fatigue to the hot box, fatigue of the fuel supply system, or exposed hot surfaces.				Workload of staff on the ship too extensive that not enough time is dedicated to writing the report therefore it is left vague resulting in inadequate repair of hot box/ fuel suply/ exposed hot surfaces	
	ECR reports on inegrity too late when equipment requiring replacement/ upgrade remains in place (H-1, H-2, H-3)		Company liaison on the ship completes the report but this is not submitted immediately to company as it is viewed as a low priority task.				Workload of staff on the ship too extensive that no time is dedicated to writing the report and the loss of integrity is not reported to the company quickly enough.	
	ECR does not provide operational status meaning engineer/ chief engineer breaks containment (H2-3)	There are no sensors available in the ER which provide a real time feed to the ECR regarding equipment operational status.					Personnel in the ECR are overrun with data and work and do not have time to respond to the operational status request from engineers.	
	ECR does not provide status of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1)		Personnel in the ECR do not recognise the dangers associated with exposed hot surfaces.	ECR is made aware of exposed hot surfaces but these signals have become normalised over time.			Personnel in the ECR are overrun with data and work and do not have time to respond to the presence of exposed hot surfaces.	
	ECR does not provide status of imminent/ existing leak from oil system meaning engineer/ chief engineer does not provide a fix (H2-3)			ECR is made aware of the potential for oil system rupture but these signals have become normalised over time.			Personnel in the ECR are overrun with data and work and do not have time to respond to the imminent/ existing oil leak alarm.	
	ECR provides incorrect operational status meaning engineer/ chief engineer breaks containment (H2-3)	Incorrect readings sent from a faulty sensor means the ECR does not provide accurate information to the engineers.		Engineers in the ECR misinterpret the data sent from sensors and issues incorrect information on operational status.			Personnel in the ECR are overrun with data and work and quickly provide a reading of operational status which is incorrect due to confusion due to work overload.	
	ECR provides status too late of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1)			ECR is made aware of exposed hot surfaces/ the potential for oil system rupture but these signals have become normalised over time.		Sensors to detect exposed hot surfaces are incorrectly positioned meaning the hot surfaces has to expand to generate an alarm.	Personnel in the ECR are overrun with data and work and do not notice the alert of hot surfaces.	
	ECR provides status of imminent/ existing leak from oil system too late meaning engineer/ chief engineer does not provide a fix (H2-3)					Sensors to detect imminent/ existing oil leak are incorrectly positioned meaning the situation has to escalate to generate an alarm.	Personnel in the ECR are overrun with data and work and do not notice the alert of imminenet/ existing oil leak.	
	ECR does not provide instruction to chief engineer/ engineer therefore measures to remedy exposed hot surfaces or potential/ existing oil leak are not implemented (H1-3)			No direct communication exists between ECR and engineers in the ER.			Personnel in the ECR are overrun with data and work and do not issue instruction to deal with exposed hot surface or imminent/ existing oil leak.	
	ECR provides instruction to break containment when equipment is operational (H2-3)		ECR personnel do not understand that the breaking of containment on the equipment will release oil, being operational. ECR personnel do not check if the equipment is operational and issue the instruction.				Personnel in the ECR are overrun with data and the work must be completed quickly. Time pressures result in oversight in instructing to break containment when the equipment is operational.	
	ECR provides instruction to ignore the exposed hot surfaces (H-1)		ECR personnel treat exposed hot surfaces (which breach SOLAS rules) as normal and do not treat this as a hazard.				Personnel in the ECR are overrun with data and the work must be completed quickly. Time pressures result in the instruction to ignore the exposed hot surface.	
	ECR provide instruction to chief engineer/ engineer too late therefore measures to remedy exposed hot surfaces or potential/ existing oil leak are not implemented (H1-3)						Personnel in the ECR are overrun with data and work and do not notice the alert of hot surfaces or imminent/ existing oil leak.	
	ECR does not set operating mode of automation when automation is required to detect/ prevent exposed hot surfaces or an oil leak (H1-3)		ECR personnel are not familiar with the sensors and actions associated with them to set the operating mode.	No specific responsibility is placed on the ECR to ensure the automation is programmed correctly.			Personnel in the ECR have too great a workload to program the automation system correctly.	
	ECR sets an inapproriate operating mode of automation when automation is required to detect/ prevent exposed hot surfaces or an oil leak (H1-3)						ECR personnel are not familiar with manufacturer recommended settings. ECR personnel alter the settings as a result of false alarms.	

ECR doesn't shutdown the engine when exposed hot surfaces exist (H-1)	No function exists in the ECR to allow the detection of an exposed hot surface to annunciate in the ECR.	ECR is aware of exposed hot surfaces (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. unacceptable pressure in fuel supply pipework, excessive vibration which could cause an imminent rutpture), meaning no shutdown action is taken.		ECR unaware of exposed hot surfaces as there are no sensors to reveal their presence therefore hot surfaces remain exposed. ECR unaware of exposed hot surfaces as there is no communication with the engineers in the ER who have found the hot surface.	ECR is aware of exposed hot surfaces but this is taken as normal, therefore engines remain operational and exposed hot surfaces remain in place.
ECR doesn't shutdown the engine when strain on the engine components exceeeds design threshold (H-2, H-3)	No function exists in the ECR to allow the detection of design threshold being breached to annunciate in the ECR.	ECR is aware of exceeding the design threshold (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. exposed hot surfaces), meaning no shutdown action is taken.		ECR unaware of engine load as there are no sensors to reveal design load being exceeded.	ECR is aware of engine load but this is taken as normal, therefore engines remain operational.
ECR shuts down the engine and does not immediately reduce load on other engines which become temporarely overloaded (H-1, H-2)		ECR is unaware of the design loads which could be generated elsewhere by shuting down the engine.		No warnings are in place to advise on the impact of the decision to shutdown the engine on the remainder of the system, therefore action is taken with no knowledge of the effect.	
ECR shuts down the engine too late when a fuel/ lube oil release exists (H-2, H-3)				Response time of sensors showing excessive conditions are not designed to provide a fast response alarm. No sensors in place to advise engineer of leak of oil, therefore shutdown relies on CCTV footage check or word from the ER.	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.
ECR doesn't shutdown the engine fast enough when exposed hot surfaces exist (H-1)	No function exists in the ECR to allow the detection of an exposed hot surface to annunciate in the ECR.	ECR is aware of exceeding the design threshold (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. exposed hot surfaces), meaning quick shutdown action is not taken.		Response time of sensors showing exposed hot surfaces are not designed to provide a fast response alarm.	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability. ECR is aware of exposed hot surfaces but this is taken as normal, therefore engines remain operational.
ECR doesn't shutdown the fuel supply when strain on the components exceeeds design threshold (H-2, H-3)	No function exists in the ECR to allow the detection of design threshold being breached to annunciate in the ECR.	ECR personnel are unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces. ECR is aware of exceeding the design threshold (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. exposed hot surfaces), meaning no shutdown action is taken.		ECR unaware of engine load as there are no sensors to reveal design load being exceeded.	Manual valve siezed shut due to lack of use. ECR is aware of engine load but this is taken as normal, therefore engines remain operational.
ECR shuts down the fuel suply too late when a fuel/ lube oil release exists (H-2, H-3)		Engine shutdown does not automatically stop supply of fuel to that engine. ECR unaware of fuel continally being sent to the engine which has been shutdown due to a leak.		No sensors are in place to provide the ECR information on the system operating condition (i.e. low fuel supply pressure indicating a leak), therefore the leak continues until CCTV/ inspection reveals failure	
ECR doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	No function exists in the ECR to allow the detection of an exposed hot surface/ oil leak to annunciate in the ECR.	ECR unaware that release of the deluge could potentially prevent an ignition. The assumption is prevalent that it should not be used until a fire breaks out.	ECR unaware that the combination of exposed hot surfaces and oil leak presents a high threat of fire.	No direct communication between engineers in the ER and the ECR to advise that water mist should be activated.	Fire in the room damages equipment resulting in incomplete control action, therefore hot surfaces remain in place elsewhere which could cause further escalation. Valve siezed shut due to lack of use.
ECR releases the water mist too late when leak exists (H-2, H-3).	No function exists in the ECR to allow the detection of an oil leak to annunciate in the ECR.			No direct communication between engineers in the ER and the ECR to advise that water mist should be activated.	
ECR releases the water mist too late when exposed hot surface exists (H-1)	No function exists in the ECR to allow the detection of an exposed hot surface to annunciate in the ECR.			No direct communication between engineers in the ER and the ECR to advise that water mist should be activated.	
ECR stops the water mist too soon when hot exposed surfaces have existed and and oil mist in atmosphere is detected/suspected (H-1)			ECR believes the deluge will have completed it's job and switches it off, despite the hot surface remaining in place.		

ID-UCA	UCA	ID-CF	Causal factors	ID-FR	Functional requirements	UCA Category	CF Category	Relevant barriers	Signals and their requirements	Hazard (Oil Leak[OL]/ Hot Surface [HS])	Previous ocurrence in Incident/ Accident (Y/N) + incident ref	Barrier Effectiveness	Criticality	Magnitude of risk reduction
1	ECR does not report on loss of integrity to company who would approve a review of safety (H-1, H-2, H-3)	1.1	Company liaison on the ship is not trained in report writing and fails to communicate the loss of integrity to the hierarchy meaning management are unaware of the ocurrence of fatigue to the hot box, fatigue of the fuel supply system, or exposed hot surfaces.	1.1.1	Engineers shall be aware of how to present clear and concise reports relating to work or equipment posing a risk of H1-3.	Inadequate reporting to management	Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS		4	3	12
		1.2	ECR instructs engineers to implement a required upgrade. The work is carried out in an uncontrolled/ undocumented way. Company are unaware of what equipment is upgraded/ what is outstanding.	1.2.1	Repair/ upgrade work which breaks containment or replaces a part where this creates a risk of H1-3 shall have the change logged.		Inadequate maintenance/ inspection	Change management system	Audit of report writing compliance. Audit of embracing of maintenance management system.	OL + HS		3	3	9
				1.2.2	Staffing and priorities shall allow for report writing to take place when this relates to potential precursors to hazards leading to H1-3.			Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
		1.3	ECR is made aware of exposed hot surfaces/ the potential for oil system rupture but these signals have become normalised over time.	1.3.1	Exposed hot surfaces beyond that allowable by SOLAS, and warnings of imminent oil leak shall be addressed immediately.		Inadequate appreciation/ comprehension of risk	Maintenance and operational procedures.	Audit of procedural complaince, record of exposed hot surfaces/ breaches in safe operation of oil systems (i.e. pressure increases above acceptable threshold).	OL + HS		3	3	9
		1.4	Workload of staff on the ship too extensive that no time is dedicated to writing the report and the loss of integrity is not reported to the company.	1.4.1	Staffing and priorities shall allow for report writing to take place when this relates to H1-3.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
		1.5	Ship believe any issues associated with exposed hot surfaces or leak potential are in hand, therefore do not pass on the information to the company. The ship fails to notice a trend towards failure.	1.5.1	Staffing and priorities shall allow for report writing directly to the company when this relates to H1-3 to allow the company to have access to data which suggests trends.		Inadequate feedback from ship to company management	Adequate staffing, task allocation an maintence procedure	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
2	ECR report on integrity to company is too vague when a specific alteration/ upgrade is required (H-1, H-2, H-3)	2.1	Input from engineers/ sensors does not provide specific enough information to pinpoint the exact nature of the risk.	2.1.1	Engineers shall be aware of how to provide clear and concise reports relating to work or equipment posing a risk of H1-3.	Inadequate reporting to management	Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS		4	3	12
		2.2	Company liaison on the ship is not trained in report writing and fails to communicate the loss of integrity to the hierarchy meaning management are unaware of the ocurrence of fatigue to the hot box, fatigue of the fuel supply system, or exposed hot surfaces.	2.2.1	Engineers shall be aware of how to present clear and concise reports relating to work or equipment posing a risk of H1-3.		Inadequate knowledge (training/ competence)	Training/ Competence Management System	Audit of Competence and job knowledge.	OL + HS		4	3	12
		2.3	Workload of staff on the ship too extensive that not enough time is dedicated to writing the report therefore it is left vague resulting in inadequate repair of hot box/ fuel suply/ exposed hot surfaces	2.3.1	Staffing and priorities shall allow for report writing to take place when this relates to H1-3.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
3	ECR reports on inegrity too late when equipment requiring replacement/ upgrade remains in place (H-1, H-2, H-3)	3.1	Company liaison on the ship completes the report but this is not submitted immediately to company as it is viewed as a low priority task.	3.1.1	Staffing and priorities shall allow for report writing to take place when this relates to H1-3.	Inadequate reporting to management	Inadequate feedback from ship to company management	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
		3.2	Workload of staff on the ship too extensive that no time is dedicated to writing the report and the loss of integrity is not reported to the company quickly enough.	3.2.1	Staffing and priorities shall allow for report writing to take place when this relates to H1-3.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
4	ECR does not provide operational status meaning engineer/ chief engineer breaks containment (H2-3)	4.1	There are no sensors available in the ER which provide a real time feed to the ECR regarding equipment operational status.	4.1.1	Operational status of equipment posing a risk of H2-3 shall be presented in real time in the ECR.	Inadequate maintenance/ repair	Inadequate feedback of operational status in the ER to the ECR	Design requirements, verification of design	Audit of design, function testing of operational status readings	OL	Le Boreal	4	4	16
		4.2	Personnel in the ECR are overrun with data and work and do not have time to respond to the operational status request from engineers.	4.2.1	Staffing and priorities shall allow for operational status requests from the ER to be addressed immediately.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL		4	3	12
5	ECR does not provide status of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1)	5.1	Personnel in the ECR do not recognise the dangers associated with exposed hot surfaces.	5.1.1	Requirements of SOLAS regarding the presence of H-1 shall be known by engineers.		Inadequate knowledge (training/ competence)	SOLAS/ safety training	Audit of attitude and compliance.	HS	Incident Event 202364	5	5	25
		5.2	ECR is made aware of exposed hot surfaces but these signals have become normalised over time.	5.2.1	Exposed hot surfaces beyond that allowable by SOLAS shall be addressed immediately.	Inadequate detection/ inspection	Inadequate appreciation/ comprehension of risk	Maintenance and operational procedures.	Audit of procedural complaince, record of exposed hot surfaces.	OL + HS		3	3	9
		5.3	Personnel in the ECR are overrun with data and work and do not have time to respond to the presence of exposed hot surfaces.	5.3.1	Staffing and priorities shall allow for exposed hot surface alarms in the ER to be addressed immediately.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	HS		3	3	9
6	ECR does not provide status of imminent/ existing leak from oil system meaning engineer/ chief engineer does not provide a fix (H2-3)	6.1	ECR is made aware of the potential for oil system rupture but these signals have become normalised over time.	6.1.1	Warnings of imminent oil leak shall be addressed immediately.		Inadequate appreciation/ comprehension of risk	Maintenance and operational procedures.	Audit of procedural complaince, record of breaches in safe operation of oil systems (i.e. pressure increases above acceptable threshold).	OL + HS		3	3	9
		6.2	Personnel in the ECR are overrun with data and work and do not have time to respond to the imminent/ existing oil leak alarm.	6.2.1	Staffing and priorities shall allow for imminent oil leak alarms in the ER to be addressed immediately.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL		4	3	12
7	ECR provides incorrect operational status meaning engineer/ chief engineer breaks containment (H2-3)	7.1	Incorrect readings sent from a faulty sensor means the ECR does not provide accurate information to the engineers.	7.1.1	Sensors indicating operational status shall have a reliability up time of 99%-99.9% (SIL2) to prevent H2-3.		Inadequate feedback of hazard in the ER to the ECR	Safety critical equipment reliability	IEC61508/ proven in use audits can be used to signal performance. Audit of embracing of maintenance management system.	OL		4	2	8
		7.2	Engineers in the ECR misinterpret the data sent from sensors and issues incorrect information on operational status.	7.2.1	Operational status shall be displayed clearly in a simple manner in the control room.	Inadequate maintenance/ repair	Inadequate operational contextual awareness	Dsign requirements	Audit of design requirements, audit of operational adequacy.	OL		4	3	12
				7.2.2	Training procedure shall include running through verification of operational status.			Training procedure	Audits should be used to monitor personnel have the necessary training.	OL		4	3	12
		7.3	Personnel in the ECR are overrun with data and work and quickly provide a reading of operational status which is incorrect due to confusion due to work overload.	7.3.1	Staffing and priorities shall allow for operational status to be provided accurately.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL		4	3	12
				7.3.2	Operational status shall be clearly presented and identifiable in the control room.			Dsign requirements	Audit of design requirements, audit of operational adequacy.	OL		4	3	12
8	ECR provides status too late of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1)	8.1	ECR is made aware of exposed hot surfaces/ the potential for oil system rupture but these signals have become normalised over time.	8.1.1	Exposed hot surfaces beyond that allowable by SOLAS, and warnings of imminent oil leak shall be addressed immediately.		Inadequate appreciation/ comprehension of risk	Maintenance and operational procedures.	Audit of procedural complaince, record of exposed hot surfaces/ breaches in safe operation of oil systems (i.e. pressure increases above acceptable threshold).	OL + HS		3	3	9
		8.2	Sensors to detect exposed hot surfaces are incorrectly positioned meaning the hot surfaces has to expand to generate an alarm.	8.2.1	Sensors intended to detect exposed hot surfaces shall be strategically placed to detect exposed hot surfaces at the locations these are likely to exist.	Inadequate detection/ inspection	Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Audit of design, function testing	HS	Most ER fires	3	5	15
		8.3	Personnel in the ECR are overrun with data and work and do not notice the alert of hot surfaces.	8.3.1	Alarms presenting the presence of hot surfaces shall be clear in audibility and visual signalling.		Inadequate resources / time	Design requirements	Audit of design requirements, audit of operational adequacy.	HS		3	3	9
9	ECR provides status of imminent/ existing leak from oil system too late meaning engineer/ chief engineer does not provide a fix (H2-3)	9.1	Sensors to detect imminent/ existing oil leak are incorrectly positioned meaning the situation has to escalate to generate an alarm.	9.1.1	Sensors intended to detect imminent/ existing oil leak shall be strategically placed to detect pressure increases/ excessive vibration/ oil mist at the locations these are likely to exist.	Inadequate detection/ inspection	Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Audit of design, function testing	OL	Most ER fires	3	5	15
		9.2	Personnel in the ECR are overrun with data and work and do not notice the alert of imminenet/ existing oil leak.	9.2.1	Alarms presenting the presence of imminenet/ existing oil leak shall be clear in audibility and visual signalling.		Inadequate resources / time	Design requirements	Audit of design requirements, audit of operational adequacy.	OL		3	3	9
10	ECR does not provide instruction to chief engineer/ engineer therefore measures to remedy exposed hot surfaces or potential/ existing oil leak are not implemented (H1-3)	10.1	No direct communication exists between ECR and engineers in the ER.	10.1.1	Engineers in the ER shall have a direct line of real time communication to the ECR.	Inadequate maintenance/ repair	Inadequate feedback between equipment, personnel in the ER and the ECR	Maintenance/ inspection procedure	Audit of procedure and maintenance activity.	HS		3	1	3
		10.2	Personnel in the ECR are overrun with data and work and do not issue instruction to deal with exposed hot surface or imminent/ existing oil leak.	10.2.1	Staffing and priorities shall allow for exposed hot surfaces/ imminent oil leak alarms in the ER to be addressed immediately.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		3	3	9
11	ECR provides instruction to break containment when equipment is operational (H2-3)	11.1	ECR personnel do not understand that the breaking of containment on the equipment will release oil, being operational. ECR personnel do not check if the equipment is operational and issue the instruction.	11.1.1	Maintenance procedure for breaking containment shall require operational verification to be carried out and verified before breaking in containment ocurrs.	Inadequate maintenance/ repair	Inadequate maintenance/ inspection	Maintenance/ inspection procedure	Audit of procedure and maintenance activity.	OL	Le Boreal	4	4	16
		11.2	Personnel in the ECR are overrun with data and the work must be completed quickly. Time pressures result in oversight in instructing to break containment when the equipment is operational.	11.2.1	Staffing and priorities shall allow for the process of operational status verification to take place adequately.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL		4	3	12
12	ECR provides instruction to ignore the exposed hot surfaces (H-1)	12.1	ECR personnel treat exposed hot surfaces (which breach SOLAS rules) as normal and do not treat this as a hazard.	12.1.1	Requirements of SOLAS shall be maintained.	Inadequate maintenance/ repair	Inadequate knowledge (training/ competence)	SOLAS/ safety training	Audit of attitude and compliance.	HS	Incident Event 202364	5	5	25
		12.2	Personnel in the ECR are overrun with data and the work must be completed quickly. Time pressures result in the instruction to ignore the exposed hot surface.	12.2.1	Staffing and priorities shall allow for exposed hot surfaces in the ER to be addressed immediately.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	HS		3	3	9
13	ECR provide instruction to chief engineer/ engineer too late therefore measures to remedy exposed hot surfaces or potential/ existing oil leak are not implemented (H1-3)	13.1	Personnel in the ECR are overrun with data and work and do not notice the alert of hot surfaces or imminent/ existing oil leak.	13.1.1	Alarms presenting the presence of imminent/ existing oil leak or exposed hot surface shall be clear in audibility and visual signalling.	Inadequate incident/ emergency reponse	Inadequate resources / time	Design requirements	Audit of design requirements, audit of operational adequacy.	OL + HS		3	3	9
14	ECR does not set operating mode of automation when automation is required to detect/ prevent exposed hot surfaces or an oil leak (H1-3)	14.1	ECR personnel are not familiar with the sensors and actions associated with them to set the operating mode.	14.1.1	Where personnel do not have experience with hardware, manufacturer or class recommendations shall be followed with respect to operating mode.	Inadequate detection/ inspection	Inadequate knowledge (training/ competence)	Design requirements	Audit of design requirements, audit of operational adequacy.	OL + HS		4	3	12
		14.2	No specific responsibility is placed on the ECR to ensure the automation is programmed correctly.	14.2.1	Responsibilities shall be clearly documented and advised to personnel such that operating mode is always programmed.		Inadequate task allocation	Design requirements, roles and responsibilities clearly distributed	Audit of procedure and system design.	OL + HS		4	3	12
		14.3	Personnel in the ECR have too great a workload to program the automation system correctly.	14.3.1	Staffing and priorities shall allow for correct autmation programming to take place when this relates to H1-3.		Inadequate resources / time	Adequate staffing and task allocation	Audit of staffing levels and procedure compliance. Alert when staffing levels reduce, but workload remains constant. Signals of task completion - are tasks being completed within anticipated timeframes.	OL + HS		4	3	12
15	ECR sets an inapproriate operating mode of automation when automation is required to detect/ prevent exposed hot surfaces or an oil leak (H1-3)	15.1	ECR personnel are not familiar with manufacturer recommended settings.	15.1.1	Where personnel do not have experience with hardware, manufacturer or class recommendations shall be sought and followed with respect to operating mode.	Inadequate detection/ inspection	Inadequate knowledge (training/ competence)	Design requirements	Audit of design requirements, audit of operational adequacy.	OL + HS		4	3	12
		15.2	ECR personnel alter the settings as a result of false alarms.	15.2.1	Where false alarms are a regular ocurrence, manufacturer or class recommendations shall be sought and followed with respect to operating mode.		Inadequate maintenance/ inspection	Design requirements	Audit of design requirements, audit of operational adequacy.	OL + HS		4	3	12
		16.1	No function exists in the ECR to allow the detection of an exposed hot surface to annunciate in the ECR.	16.1.1	Personnel in the ECR shall be alerted to the detection of exposed hot surfaces in the ER.		Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Audit of design, function testing	HS		3	1	3
			ECR is aware of exposed hot surfaces (which are taken as normal), but are unaware of other risk factors which would	16.2.1	System shall be able to detect and alarm to pressure in excess of the maufacturer specification in the fuel supply system, and vibration in excess of the maufacturer specification which could indicate the presence of or potential for H2-3.		Inadequate	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - MV Zenith, Spleandour of the	3	5	15

		16.2	require an engine shutdown (i.e. existing oil leak, unacceptable pressure in fuel supply pipework, excessive vibration which could cause an imminent rutpture), meaning no shutdown action is taken.	16.2.2	System to detect oil leaks in the hot box and the engine room shall be provided (H2-3).		appreciation/ comprehension of risk	Safety Instrumented System	Diagnostics showing sensor health status.	OL	Seas, Accident Event 207960, 231717, 224659, Incident Event 202364	3	5	15
16	ECR doesn't shutdown the engine when exposed hot surfaces exist (H-1)			16.2.3	Engineers shall be aware of precursors which can lead to H2-3 and when shutdown of the engine should take place when coupled with H-1.	Inadequate incident/ emergency reponse		Engine operation procedure	Audits should be used to monitor engineers have the necessary training.	OL + HS		4	5	20
		16.3	ECR unaware of exposed hot surfaces as there are no sensors to reveal their presence therefore hot surfaces remain exposed.	16.3.1	System shall be able to provide alarms in high risk areas to the presence of H-1.		Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Thermal sensors with diagnostics showing sensor health status.	HS	(Y) - Le Boreal, MV Zenith, Splendour of the Seas, Carnival Triumph. Accident Event 269956	3	5	15
				16.3.2	System shall be in place to flag up and record presence of H-1.			Hot surface inspection procedure	Audit of procedures can be the signal of performance. Audit of embracing of maintenance management system.	HS		4	5	20
		16.4	ECR unaware of exposed hot surfaces as there is no communication with the engineers in the ER who have found the hot surface.	16.4.1	Engineers in the ER shall have a direct line of real time communication to the ECR.		Inadequate feedback of hazard in the ER to the ECR	Maintenance/ inspection procedure	Audit of procedure and maintenance activity.	HS		3	1	3
		16.5	ECR is aware of exposed hot surfaces but this is taken as normal, therefore engines remain operational and exposed hot surfaces remain in place.	16.5.1	Requirements of SOLAS shall be maintained.		Inadequate appreciation/ comprehension of risk	SOLAS/ safety training	Audit of attitude and compliance.	HS	Incident Event 202364	5	5	25
		17.1	No function exists in the ECR to allow the detection of design threshold being breached to annunciate in the ECR.	17.1.1	Design threshold detectors (i.e. oil system pressure) in the ER shall have an alarm function within the ECR which will alert ECR personnel to the presence of potential breaks in containment.		Inadequate feedback of operational status in the ER to the ECR	Safety Instrumented System	Audit of design, function testing	OL		4	1	4
		17.2	ECR is aware of exceeding the design threshold (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. exposed hot surfaces), meaning no shutdown action is taken.	17.2.1	ECR personnel shall be aware of precursors which can lead to H-2, and when shutdown should take place.		Inadequate knowledge (training/ competence)	Training procedure	Audits should be used to monitor personnel have the necessary training.	OL	(Y) - Splendour of the Seas, Accident Event 210991, 222338	4	5	20
17	ECR doesn't shutdown the engine when strain on the engine components exceeds design threshold (H-2, H-3)	17.3	ECR unaware of engine load as there are no sensors to reveal design load being exceeded.	17.3.1	System shalll be capable of detecting a potentially unsafe operating condition for fuel/ oil pressure, temperature, flow rate, vibration and engine power output/ load which can lead to H2-3.	Inadequate incident/ emergency reponse	Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Splendour of the Seas, Carnival Triumph, Accident Event 198060, 210991, 222338, 192706	3	5	15
		17.4	ECR is aware of engine load but this is taken as normal, therefore engines remain operational.	17.4.1	ECR shall shutdown engines when the safe operating threshold is exceeded.		Inadequate knowledge (training/ competence)	Fire prvention safety training	Audit of attitude and compliance.	OL		4	3	12
		18.1	ECR is unaware of the design loads which could be generated elsewhere by shutting down the engine.	18.1.1	Engineers shall be aware of the impact of shutting down an engine on other systems where this could lead to increased risk of H2-3 elsewhere.		Inadequate knowledge (training/ competence)	Training/ Competence Management System.	Audits should be used to monitor engineers have the necessary training.	OL		4	3	12
18	ECR shuts down the engine and does not immediately reduce load on other engines which become temporarely overloaded (H-1, H-2)	18.2	No warnings are in place to advise on the impact of the decision to shutdown the engine on the remainder of the system, therefore action is taken with no knowledge of the effect.	18.2.1	Where an engine is to be shutdown remotely, system should be in place to monitor and advise of the impact of shutdown (H2-3).	Inadequate incident/ emergency reponse	Inadequate operational contextual awareness	Safety Instrumented System	Diagnostics showing sensor health status. Sensors produce an overall risk level which updates based on projections should a DG be shutdown. Health shall be monitored against manufacturer provided tolerances (i.e. pressure in the fuel supply system shall not exceed xbar/psi)	OL	(Y) - Accident Event 210991, 222338	3	5	15
		19.1	Response time of sensors showing excessive conditions are not designed to provide a fast response alarm.	19.1.1	Any sensors which are in place to detect anomolies in engine conditions which could lead to a H-2 (fuel/ oil pressure, temperature, flow) shall be fast response and shall present the alarm and reading to the ECR in real time.		Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Accident Event 192706	3	5	15
19	ECR shuts down the engine too late when a fuel/ lube oil release exists (H-2, H-3)	19.2	No sensors in place to advise engineer of leak of oil, therefore shutdown relies on CCTV footage check or word from the ER.	19.2.1	System to detect oil leaks in the hot box and the engine room shall be provided (H2-3).	Inadequate incident/ emergency reponse	Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Le Boreal, MV Zenith, Splendour of the Seas, Accident Event 207960, 231717, 224659, Incident Event 202364	3	5	15
		19.3	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.	19.3.1	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.		Inadeqaute safety system design	Emergency shutdown Procedure	Function testing of the shutdown valves at regular intervals. Function testing of fuel pump shutdown. Results of this testing can provide a reliability value which can be taken into account on the overall risk ranking.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph	2	5	10
		20.1	No function exists in the ECR to allow the detection of an exposed hot surface to annunciate in the ECR.	20.1.1	Personnel in the ECR shall be alerted to the detection of exposed hot surfaces in the ER.		Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Audit of design, function testing	HS		3	1	3
		20.2	ECR is aware of exceeding the design threshold (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. exposed hot surfaces), meaning quick shutdown action is not taken.	20.2.1	ECR personnel shall be aware of precursors which can lead to H-1, and when shutdown should take place.		Inadequate knowledge (training/ competence)	Training procedure	Audits should be used to monitor personnel have the necessary training.	OL	(Y) - Splendour of the Seas, Accident Event 210991, 222338	4	5	20
20	ECR doesn't shutdown the engine fast enough when exposed hot surfaces exist (H-1)	20.3	Response time of sensors showing exposed hot surfaces are not designed to provide a fast response alarm.	20.3.1	Any sensors which are in place to detect H-1 shall be fast response and shall present the alarm to the ECR in real time.	Inadequate incident/ emergency reponse	Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Diagnostics showing sensor health status.	HS		3	3	9
		20.4	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.	20.4v	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.		Inadeqaute safety system design	Emergency shutdown Procedure	Function testing of the shutdown valves at regular intervals. Function testing of fuel pump shutdown. Results of this testing can provide a reliability value which can be taken into account on the overall risk ranking.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph	2	5	10
		20.5	ECR is aware of exposed hot surfaces but this is taken as normal, therefore engines remain operational.	20.5.1	Requirements of SOLAS shall be maintained.		Inadequate appreciation/ comprehension of risk	SOLAS/ safety training	Audit of attitude and compliance.	HS	Incident Event 202364	5	5	25
		21.1	No function exists in the ECR to allow the detection of design threshold being breached to annunciate in the ECR.	21.1.1	Design threshold detectors (i.e. oil system pressure) in the ER shall have an alarm function within the ECR which will alert ECR personnel to the presence of potential breaks in containment.		Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Audit of design, function testing	OL		4	1	4
		21.2	ECR personnel are unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces.	21.2.1	ECR personnel shall be aware of precursors which can lead to H-2, and when shutdown of the supply should take place.		Inadequate knowledge (training/ competence)	Training procedure	Audits should be used to monitor personnel have the necessary training.	OL	(Y) - Splendour of the Seas, Accident Event 210991, 222338	4	5	20
21	ECR doesn't shutdown the fuel supply when strain on the components exceeds design threshold (H-2, H-3)	21.3	ECR is aware of exceeding the design threshold (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. exposed hot surfaces), meaning no shutdown action is taken.	21.3.1	ECR personnel shall be aware of precursors which can lead to H-2, and when shutdown of the supply should take place.	Inadequate incident/ emergency reponse	Inadequate knowledge (training/ competence)	Training procedure	Audits should be used to monitor personnel have the necessary training.	OL	(Y) - Splendour of the Seas, Accident Event 210991, 222338	4	5	20
		21.4	ECR unaware of engine load as there are no sensors to reveal design load being exceeded.	21.4.1	System shall be able to detect and alarm at the point a manufacturer stated operating condition is breached for fuel/ oil pressure, temperature, flow rate, vibration and engine power output/ load to prevent H-2.		Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Splendour of the Seas, Carnival Triumph, Accident Event 198060, 210991, 222338, 192706	3	5	15
		21.5	Manual valve siezed shut due to lack of use.	21.5.1	Shut off valves used to prevent or mitigate H2-3 shall be subect to operation and inspection during maintenance as per manufacturer recommendation.		Inadequate maintenance/ inspection	Physical barrier function test procedure	Audit of procedures and review of maintenance logs can be the signal of performance. Audit of embracing of maintenance management system.	OL	(Y) - Splendour of the Seas, Carnival Triumph, Accident Event 207612	4	5	20
		21.6	ECR is aware of engine load but this is taken as normal, therefore engines remain operational.	21.6.1	ECR shall shutdown engines when the safe operating threshold is exceeded.		Inadequate knowledge (training/ competence)	Fire prvention safety training	Audit of attitude and compliance.	OL		4	3	12
		22.1	Engine shutdown does not automatically stop supply of fuel to that engine. ECR unaware of fuel continally being sent to the engine which has been shutdown due to a leak.	22.1.1	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.		Inadequate feedback of hazard in the ER to the ECR	Emergency shutdown procedure	Function testing of the shutdown valves at regular intervals. Function testing of fuel pump shutdown. Results of this testing can provide a reliability value which can be taken into account on the overall risk ranking.	OL	(Y) - Sea Gale, Splendour of the Seas, Carnival Triumph, Accident Event 224659	2	5	10
22	ECR shuts down the fuel suply too late when a fuel/ lube oil release exists (H-2, H-3)	22.2	No sensors are in place to provide the ECR information on the system operating condition (i.e. low fuel supply pressure indicating a leak), therefore the leak continues until CCTV/ inspection reveals failure	22.2.1	System shall be capable of detecting pressure outwith manufacturer specification indicative of increased risk of H2-3 in the fuel supply pipework, and oil leaks shall be detectalbe in the hot box and in the ER (H2-3).	Inadequate incident/ emergency reponse	Inadequate feedback of operating status in the ER to the ECR	Safety Instrumented System	Diagnostics showing sensor health status.	OL	(Y) - Splendour of the Seas, Accient Event 231717, 224659, Incident Event 202364	3	5	15
		23.1	No function exists in the ECR to allow the detection of an exposed hot surface/ oil leak to annunciate in the ECR.	23.1.1	Hot surface detectors in the ER shall have an alarm function within the ECR which will alert ECR personnel to the presence of H-1.		Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Audit of design, function testing	HS + OL		3	1	3
		23.2	ECR unaware that release of the deluge could potentially prevent an ignition. The assumption is prevalent that it should not be used until a fire breaks out.	23.2.1	ECR personnel shall be aware of how to use the water mist system, and where it can assist in the elimination of H-1 when a leak or break in containment is likely/ has ocurred.		Inadequate knowledge (training/ competence)	Training procedure/ Emergency procedure	Diagnostics showing sensor health status which can flag a potentially imminent break in containment/ or presence of fuel/ oil mist. Audit of engineer trainikng and knowedge of water mist release.	HS	(Y) - Accident Event 224659, Incident Event 202364, Carnival Triumph, Splendour of the Seas [specifically referenced in the incident report that water mist release could have prevented the fire in the first place]	4	5	20
23	ECR doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	23.3	ECR unaware that the combination of exposed hot surfaces and oil leak presents a high threat of fire.	23.3.1	ECR personnel shall be able to recognise the dangers associated with exposed hot surfaces (H-1) and presence of an oil leak (H2-3).	Inadequate incident/ emergency reponse	Inadequate knowledge (training/ competence)	Training/ Competence Management System. Alarm management procedure.	Audit of Competence. Diagnostics showing sensor health status which can flag a potentially imminent break in containment/ or presence of fuel/ oil mist. Audit of engineer trainikng and knowedge of water mist release.	OL		4	3	12
		23.4	No direct communication between engineers in the ER and the ECR to advise that water mist should be activated.	23.4.1	Engineers in the ER shall have a direct line of real time communication to the ECR.		Inadequate feedback between equipment, personnel in the ER and the ECR	Maintenance/ inspection procedure	Audit of procedure and maintenance activity.	HS		3	1	3
		23.5	Fire in the room damages equipment resulting in incomplete control action, therefore hot surfaces remain in place elsewhere which could cause further escalation.	23.5.1	Water mist system shall be able to continue operation in the event of a fire (H-1).		Inadeqaute safety system design	Emergency shutdown Procedure	Audit of design.	HS	(Y) - Splendour of the Seas	2	4	8
				23.5.2	ECR personnel shall be aware of the requirement and how to release water mist system in the event of a fire if it is not already active.			Training procedure/ Emergency procedure	Audit of procedures can be the signal of performance.	HS		4	4	16
		23.6	Valve siezed shut due to lack of use.	23.6.1	Water mist release valves used to prevent or mitigate H-1 shall be subect to operation and inspection during maintenance as per manufacturer recommendation.		Inadequate maintenance/ inspection	Physical barrier function test procedure	Audit of procedures and review of maintenance logs can be the signal of performance. Audit of embracing of maintenance management system.	OL	(Y) - Accient Event 274465	4	5	20
24	ECR releases the water mist too late when leak exists (H-2, H-3).	24.1	No function exists in the ECR to allow the detection of an oil leak to annunciate in the ECR.	24.1.1	Oil leak detectors in the ER shall have an alarm function within the ECR which will alert ECR personnel to the presence of oil leaks.	Inadequate incident/ emergency reponse	Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Audit of design, function testing	OL		3	1	3
		24.2	No direct communication between engineers in the ER and the ECR to advise that water mist should be activated.	24.2.1	Engineers in the ER shall have a direct line of real time communication to the ECR.		Inadequate feedback between equipment, personnel in the ER and the ECR	Maintenance/ inspection procedure	Audit of procedure and maintenance activity.	HS		3	1	3
25	ECR releases the water mist too late when exposed hot surface exists (H-1)	25.1	No function exists in the ECR to allow the detection of an exposed hot surface to annunciate in the ECR.	25.1.1	Personnel in the ECR shall be alerted to the detection of exposed hot surfaces in the ER.	Inadequate incident/ emergency reponse	Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Audit of design, function testing	HS		3	1	3
		25.2	No direct communication between engineers in the ER and the ECR to advise that water mist should be activated.	25.2.1	Engineers in the ER shall have a direct line of real time communication to the ECR.		Inadequate feedback between equipment, personnel in the ER and the ECR	Maintenance/ inspection procedure	Audit of procedure and maintenance activity.	HS		3	1	3
26	ECR stops the water mist too soon when hot exposed surfaces have existed and and oil mist in atmosphere is detected/suspected (H-1)	26.1	ECR believes the deluge will have completed it's job and switches it off, despite the hot surface remaining in place.	26.1.1	Deluge shall not be stopped until both hot surfaces have been removed, and oil leak has been contained/ depressurised.	Inadequate incident/ emergency reponse	Inadequate feedback of hazard in the ER to the ECR	Emergency shutdown Procedure	Function testing of the oil leak and hot surface sensors. Audit of procedures.	HS		2	3	6

Barrier Criticality



Barrier Effectiveness

Scale of Colours
Green = 1-8
Amber = 9-15
Red = 16-30

Appendix B: STPA Audit Checklist & Guide on a Cruise Ship Machinery Space

Controller	Unsafe Control Action	Causal Factor	Functional Requirement	Is the functional requirement addressed?	Is Evidence Required?	Explaination Required?	How do you rank the effectiveness of the functional requirement = 1-6	How do you rank the criticality of the functional requirement = 1-5	Evidence/ Explaination Notes	Additional Notes
ECR Controller	ECR does not provide status of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1)	Personnel in the ECR do not recognise the dangers associated with exposed hot surfaces.	Requirements of SOLAS regarding the presence of H-1 shall be known by engineers.							
	ECR provides instruction to ignore the exposed hot surfaces (H-1)	ECR personnel treat exposed hot surfaces (which breach SOLAS rules) as normal and do not treat this as a hazard.	Requirements of SOLAS shall be maintained.							
	ECR doesn't shutdown the engine when exposed hot surfaces exist (H-1)	ECR is aware of exposed hot surfaces but this is taken as normal, therefore engines remain operational and exposed hot surfaces remain in place.	Requirements of SOLAS shall be maintained.							
	ECR doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	Valve siezed shut due to lack of use.	Water mist release valves used to prevent or mitigate H-1 shall be subect to operation and inspection during maintenance as per manufacturer recommendation.							
	ECR does not provide instruction to chief engineer/ engineer therefore measures to remedy exposed hot surfaces or potential/ existing oil leak are not implemented (H1-3)	No direct communication exists between ECR and engineers in the ER.	Engineers in the ER shall have a direct line of real time communication to the ECR.							
	ECR doesn't shutdown the engine when exposed hot surfaces exist (H-1)	No function exists in the ECR to allow the detection of an exposed hot surface to annunciate in the ECR.	Personnel in the ECR shall be alerted to the detection of exposed hot surfaces in the ER.							
	ECR doesn't shutdown the fuel supply when strain on the components exceeds design threshold (H-2, H-3)	No function exists in the ECR to allow the detection of design threshold being breached to annunciate in the ECR.	Design threshold detectors (i.e. oil system pressure) in the ER shall have an alarm function within the ECR which will alert ECR personnel to the presence of potential breaks in containment.							
	ECR doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	No function exists in the ECR to allow the detection of an exposed hot surface/ oil leak to annunciate in the ECR.	Hot surface detectors in the ER shall have an alarm function within the ECR which will alert ECR personnel to the presence of H-1.							
	ECR releases the water mist too late when leak exists (H-2, H-3).	No function exists in the ECR to allow the detection of an oil leak to annunciate in the ECR.	Oil leak detectors in the ER shall have an alarm function withiin the ECR which will alert ECR personnel to the presence of oil leaks.							
	ECR does not report on loss of integrity to company who would approve a review of safety (H-1, H-2, H-3)	Company liaison on the ship is not trained in report writing and fails to communicate the loss of integrity to the hierarchy, meaning management are unaware of the ocurrence of fatigue to the hot box, fatigue of the fuel supply system, or exposed hot surfaces.	Engineers shall be aware of how to present clear and concise reports relating to work or equipment posing a risk of H1-3.							
	ECR does not provide operational status meaning engineer/ chief engineer breaks containment (H2-3)	Personnel in the ECR are overrun with data and work and do not have time to respond to the operational status request from engineers.	Staffing and priorities shall allow for operational status requests from the ER to be addressed immediately.							
	ECR shuts down the engine and does not immediately reduce load on other engines which become temporarely overloaded (H-1, H-2)	ECR is unaware of the design loads which could be generated elsewhere by shutting down the engine.	Engineers shall be aware of the impact of shuting down an engine on other systems where this could lead to increased risk of H2-3 elsewhere.							
	ECR shuts down the engine too late when a fuel/ lube oil release exists (H-2, H-3)	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.							
	ECR shuts down the engine and does not immediately reduce load on other engines which become temporarely overloaded (H-1, H-2)	No warnings are in place to advise on the impact of the decision to shutdown the engine on the remainder of the system, therefore action is taken with no knowledge of the effect.	Where an engine is to be shutdown remotely, system should be in place to monitor and advise of the impact of shutdown (H2-3).							
	ECR provides status of imminent/ existing leak from oil system too late meaning engineer/ chief engineer does not provide a fix (H2-3)	Sensors to detect imminent/ existing oil leak are incorrectly positioned meaning the situation has to escalate to generate an alarm.	Sensors intended to detect imminent/ existing oil leak shall be strategically placed to detect pressure increases/ excessive vibration/ oil mist at the locations these are likely to exist.							
	ECR provides status too late of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1)	Sensors to detect exposed hot surfaces are incorrectly positioned meaning the hot surfaces has to expand to generate an alarm.	Sensors intended to detect exposed hot surfaces shall be strategically placed to detect exposed hot surfaces at the locations these are likely to exist.							
Engineer	Engineer does not detect loss of integrity during inspection (H-2, H-3)	Engineer is not aware of what to look for/ what the signs are of loss of integrity due to lack of skills/ knowledge.	Engineers shall be able to recognise hot box and fuel supply pipework/ engine loss of integrity which can lead to H2-3.							
	Engineer does not detect loss of integrity during inspection (H-2, H-3)	The interval between inspections of the hot box and fuel supply pipework is too lengthy resulting in severe degradation between inspections not being detected.	Manufacturer requirements to prevent H2-3 shall be met.							
	Engineer interferers with equipment and doesn't return to its original condition during inspection (H-1, H-2, H-3)	Engineer does not have the training/ skillset to adequately understand the impact of interfering with equipment to get a closer inspection, resulting in continued hot surface exposure, or damaged/ fatigued equipment.	Engineers shall be capable of returning equipment back into service in a safe state to prevent H1-3.							
	Engineer doesn't shutdown or stop the fuel supply when strain on the components exceeds design threshold (H-2, H-3)	Engineers are unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces. Training inadequate, therefore fuel supply is not shutdown the moments before a hazard is realised.	Engineers shall be aware of precursors which can lead to H-2, and when shutdown of the supply should take place.							
	Engineer shuts down the fuel supply too late when a fuel/ lube oil release exists (H-2, H-3)	Engine shutdown does not automatically shutdown supply of fuel to that engine. Engineers unaware of fuel continually being sent to the engine which has been shutdown due to a leak.	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.							
	Engineer doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	Engine shutdown buttons are not easily accessible, delaying the time taken to shutdown the engine.	Access to the emergency push buttons for both engine shutdown and fuel supply shutdown shall be accessible from multiple locations/ directions from the engine to prevent or mitigate H2-3.							
	Engineer releases the water mist too late when exposed hot surface exists (H-1)	Water mist release mechanism has been inhibited during maintenance and not brought back online.	Upon completion of maintenance, all inhibits shall be removed.							
	Engineer starts repair, but doesn't complete when faulty equipment is present (H-1, H-2, H-3)	Engineer begins maintenance but is called to tend to other issues and does not complete the maintenance/ repair. No log exists to prevent activation of the equipment. Incomplete repair results in flammable material release on start-up	Staffing shall allow for planned maintenance of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.							
	Engineer repairs equipment but does not complete/ implement the repair correctly (H-1, H-2, H-3)	Engineer unaware of how to apply the manufacturer guidelines when checking equipment (i.e. bolts on the fuel supply pipework) due to a lack of qualification/ competence.	Engineers shall be familiar with equipment on board where a risk of H1-3 exists and trained on all potential actions required to be made on that equipment.							
	Engineer starts repair, but doesn't complete when faulty equipment is present (H-1, H-2, H-3)	Engineer begins the repair but comes up against a repair process he/ she is unfamiliar with and stops mid way through.	If a job remains unfinished, equipment shall be made safe and records shall be maintained to show the job is unfinished. Unfinished repair shall be marked accordingly (e.g. lockout-tagout / LOTO)							
	Engineer repairs equipment too late when damaged/ faulty equipment exists (H-1, H-2, H-3)	Engineer receives feedback that equipment is faulty but does not attend to the failure due to an extensive workload. The equipment is brought back online before the engineer can tend to the faulty equipment resulting in a break in containment/ hot surface	Tasks which increase the risk of H1-3 shall only be assigned when the engineer has availability to complete them.							
	Engineer repairs equipment but does not complete/ implement the repair correctly (H-1, H-2, H-3)	Engineer unaware of how to apply the manufacturer guidelines when checking equipment (i.e. bolts on the fuel supply pipework) due to a lack of qualification/ competence.	Engineers shall be familiar with equipment on board where a risk of H1-3 exists and trained on all potential actions required to be made on that equipment.							
	Engineer does not detect incorrect implementation of equipment as per manufacturer guidelines during inspection (H-2, H-3)	Planned maintenance routine does not provide instruction of inspection intervals meaning the engineer does not get tasked with inspecting the equipment.	Maintenance task list shall be clear and easily followed to prevent H2-3.							
	Engineer doesn't repair equipment when faulty equipment present (H-1, H-2, H-3)	No sensor is applied to check for failures of equipment therefore the Engineer is not informed of a faulty/ damaged piece of equipment. No remedial action is therefore taken resulting in a break in containment from weakened equipment/ exposed hot surface due to faulty equipment operation	System shall be able to monitor real time health status of engine and fuel supply system, providing alarms when faults which can lead to H1-3 occur.							
	Engineer doesn't shutdown, stop or remove the engine from service when exposed hot surfaces exist (H-1)	Engineers are aware of exposed hot surfaces (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. oil leak, unacceptable pressure in fuel supply pipework, excessive vibration which could cause an imminent rupture), meaning no shutdown action is taken.	System to detect oil leaks in the hot box and the engine room shall be provided (H2-3).							
	Engineer shuts down the engine too late when a fuel/ lube oil release exists (H-2, H-3)	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.							
	Ship automation does not provide engineers operational status (H1-3)	Indication is not clearly represented due to poorly illuminated LED/ dirt obscuration.	Operational status shall be easily discernible and indicator shall be clear and visible.							
	Ship automation does not provide ECR operational status (H1-3)	No sensor is provided for ship automation that the fuel oil system/ engine is operational as there is no sensor in place. The ECR then instructs engineer to conduct maintenance on the system and breaks containment.	Operational status shall be known to the process controller.							
	Ship automation does not provide an alarm during an oil leak (H2-3)	No sensor provided to detect presence of an oil leak/ mist therefore no alarm can be presented.	Presence of oil mist both within the hot box and the ER shall be known to the process controller.							
	Ship automation does not alarm to exposed hot surface (H-1)	No sensor provided to detect presence of an exposed hot surface therefore no alarm can be presented.	Presence of exposed hot surfaces (>250 deg C) ER shall be known to the process controller.							
	Ship automation does not alarm to pressure deviation in the oil systems (H2-3)	No feedback exists on stream pressure because no sensor is in place, resulting in no alarm signal on pressure deviation, resulting in pipework rupture	Stream pressure shall be known to the process controller.							
	Ship automation does not provide an alarm during an oil leak (H2-3)	Ship automation receives sensor data of reduced pressure as a result of a leak but misinterprets the data as normal operation as the set point is not relevant to the design tolerance, therefore does not send alarm, resulting in continual leak	Set points applied to alarm to system pressure drop in the event of a leak shall be set based on the anticipated pressure which could be presented through a break in containment.							
	Ship automation shuts down the engine when pressure in the oil systems is normal (H2-3)	Shutdown action is intended for a different engine from where the pressure deviation is present through incorrectly programmed control system, increasing demand on the already faulty engine	Automated shutdown shall be based directly from the sensors installed on that machine.							
	Ship automation shuts down the engine too late during an oil leak (H2-3)	Automated shutdown action has been inhibited during maintenance and not brought back online.	Upon completion of maintenance, all inhibits shall be removed.							
Automation	Ship automation provides operational status to engineers too late (H1-3)	An excessive time delay has been implemented in the control system to avoid spurious signals based on standard system fluctuations, meaning the true operational status is presented too late.	Time delays shall not be beyond the point at which the operational status needs to be know. I.e. time delay of no greater than 10 seconds.							
	Ship automation provides operational status to engineers too late (H1-3)	Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status.	Operational status indicators shall operate in real time, providing an indication of status with 1 second of accuracy.							
	Ship automation provides operational status to ECR too late (H1-3)	Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status.	Operational status indicators shall operate in real time, providing an indication of status with 1 second of accuracy.							
	Ship automation does not provide ECR operational status (H1-3)	Signal from the sensor has been inhibited during maintenance and not brought back online.	Upon equipment start-up, warnings shall be presented if sensors are inhibited.							
	Ship automation stops the water mist release too soon when oil leak is still present (H-1)	ECR/ engineer prevents the release of the water mist system as they believe the leak no longer presents a risk.	Engineer shall be aware of emergency response and on the factors to review in assuming a situation no longer poses a risk of H-1.							
	Ship automation releases the water mist too late when exposed hot surface exists (H-1)	No automation in place to automatically release deluge on reception of sufficient alarm alarms indicating exposed hot surface. Release only occurs on manual detection of a hot surface.	Equipment posing a threat of H1 shall have means of automated water mist release.							
	Ship automation shuts down the fuel supply too late during an oil leak (H2-3)	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating oil leak are false alarms. Shutdown only activated when further alarms are received.	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.							
	Ship automation does not shutdown the fuel supply when exposed hot surface exists (H-1).	No automation in place to shutdown fuel supply on reception of exposed hot surface alarm	Equipment posing a threat of H1 shall have means of automated shutdown linked to hot surface detectors.							

DEPARTMENT OF NAVAL ARCHITECTURE, OCEAN & MARINE ENGINEERING

UNIVERSITY of STRATHCLYDE MARITIME SAFETY RESEARCH CENTRE

University of Strathclyde Engineering

SEAMAN Fire Hazard Analysis – Allure Audit Four Step Guide

James McNay

MSRC, Department of Naval Architecture, Ocean and Marine Engineering,
University of Strathclyde, Glasgow, UK

Steps of Audit

UNIVERSITY of STRATHCLYDE
MARITIME SAFETY
RESEARCH CENTRE

Step One:

- Introduce the auditee to the spreadsheet which will be completed by you both
- Talk through each column – without yet completing the blank columns

Step Two:

- Explain the 3 hazards of concern
- Explain what an Unsafe Control Action is
- Explain what a Causal Factor is
- Explain what a Functional Requirement is

Note: all explanations on slide 3

Step Three:

- Explain the scale of effectiveness
- Explain the scale of criticality

Note: all explanations on slide 4

Step Four:

- Populate Columns F (drop down box), I, J and K (Columns G and H auto populate based on the answer in Column F)
- Column K will consist of the answer given by the auditee, along with their explained evidence or justification
- Column L is for any additional notes you may have as the auditor

Definitions (Hazards, UCA, CF and FR)

UNIVERSITY of STRATHCLYDE
MARITIME SAFETY
RESEARCH CENTRE

Hazards:

H-1: Exposed Hot surfaces (>220degC) in ER
H-2: Leak from pressurised oil systems
H-3: Failure to contain oil leak

Unsafe Control Actions (UCAs):

Based on the above hazards, the **actions** carried out by the **engineer, automation or control room** are analysed in light of when their **actions could result** in any of those **hazards**.
The UCAs include the **context** in which the action would be unsafe.

Causal Factors (CFs):

Foreseeable causal factors have been generated which could lead to those unsafe control actions.

Functional Requirement (FRs):

Performance/ goal based functional requirements of the system have been presented which would prevent the occurrence of the causal factor.

UNIVERSITY of STRATHCLYDE
MARITIME SAFETY
RESEARCH CENTRE

Definitions (Effectiveness and Criticality)

Effectiveness = the chance of achieving the desired effect/outcome

- Eliminate hazard = 6
- Prevent systemic factors of incident = 5
- Prevent contributing factors of incident = 4
- Prevent direct factors of incident = 3
- Control incident (stopping from propagating to accident/loss) = 2
- Reduce damage (loss) = 1

Criticality = how safety critical is it to implement this requirement

- Scenario is improbable (i.e. effective barriers are in place) = 1
- No record of incident in the past but is covered by existing barriers = 2
- It is probable but not addressed/overlooked - Medium Priority = 3
- The causal factor led to previous incidents and is dealt with by existing barriers = 4
- The causal factor led to previous incidents and is not dealt with by existing barriers = 5

University of
Strathclyde
Glasgow

Appendix C: STPA Audit Results on a Cruise Ship Machinery Space

Controller	Unsafe Control Action	Causal Factor	Functional Requirement	Is the functional requirement addressed?	Is Evidence Required?	Explaination Required?	How do you rank the effectiveness of the functional requirement = 1-6	How do you rank the criticality of the functional requirement = 1-5	Evidence/ Explaination Notes	Additional Notes	FR Spread	STPA Barrier Effectiveness	STPA Criticality	STPA Magnitude of risk reduction
Automation	Ship automation does not provide engineers operational status (H1-3)	Indication is not clearly represented due to poorly illuminated LED/ dirt obscuration.	Operational status shall be easily discernible and indicator shall be clear and visible.	No		State Why in Column J		4	2 No system in place to indicate Temp above 220 Deg C. However, Flame and Smoke detectors are in place and this will activate if the temp increases. If there is a leak, then pressure drop will indicate a leak.	There is no specific system to measure temperature increase. Only detectors of flame and smoke will give this indication.		4	4	16
	Ship automation does not provide ECR operational status (H1-3)	No sensor is provided for ship automation that the fuel oil system/ engine is operational as there is no sensor in place. The ECR then instructs engineer to conduct maintenance on the system and breaks containment.	Operational status shall be known to the process controller.	Yes	Provide Evidence in Column J			5	3 Sensors indicate failure of engine or fuel system.	It is addressed but not overlooked	High Magnitude of Risk Reduction	4	4	16
	Ship automation does not provide an alarm during an oil leak (H2-3)	No sensor provided to detect presence of an oil leak/ mist therefore no alarm can be presented.	Presence of oil mist both within the hot box and the ER shall be known to the process controller.	Yes	Provide Evidence in Column J			4	2 Dirty and clean leak detector alarms are in place. Oil mist detectors are in place			3	5	15
	Ship automation does not alarm to exposed hot surface (H-1)	No sensor provided to detect presence of an exposed hot surface therefore no alarm can be presented.	Presence of exposed hot surfaces (>250 deg C) ER shall be known to the process controller.	Yes	Provide Evidence in Column J			3	3 No system to detect surface temp above 250 Deg C			3	5	15
	Ship automation does not alarm to pressure deviation in the oil systems (H2-3)	No feedback exists on stream pressure because no sensor is in place, resulting in no alarm signal on pressure deviation, resulting in pipework rupture	Stream pressure shall be known to the process controller.	No		State Why in Column J		3	4 No system to indicate high pressure. However, drop in pressure will result in an alarm			3	2	6
	Ship automation does not provide an alarm during an oil leak (H2-3)	Ship automation receives sensor data of reduced pressure as a result of a leak but misinterprets the data as normal operation as the set point is not relevant to the design tolerance, therefore does not send alarm, resulting in continual leak	Set points applied to alarm to system pressure drop in the event of a leak shall be set based on the anticipated pressure which could be presented through a break in containment.	No		State Why in Column J		4	2 The pressure drop sensors are not fitted from fire safety point of view, but to protect the engine from severe damage.		Low Magnitude of Risk Reduction	3	2	6
	Ship automation shuts down the engine when pressure in the oil systems is normal (H2-3)	Shutdown action is intended for a different engine from where the pressure deviation is present through incorrectly programmed control system, increasing demand on the already faulty engine	Automated shutdown shall be based directly from the sensors installed on that machine.	Yes	Provide Evidence in Column J			5	2 Automation system will shut down the engine when oil pressure drops. This is to prevent damage to the engine and not related to fire safety.			3	1	3
	Ship automation shuts down the engine too late during an oil leak (H2-3)	Automated shutdown action has been inhibited during maintenance and not brought back online.	Upon completion of maintenance, all inhibits shall be removed.	Yes	Provide Evidence in Column J			5	2 Lockout Tagout system is implemented with two person check			3	2	6
	Ship automation provides operational status to engineers too late (H1-3)	An excessive time delay has been implemented in the control system to avoid spurious signals based on standard system fluctuations, meaning the true operational status is presented too late.	Time delays shall not be beyond the point at which the operational status needs to be know. i.e. time delay of no greater than 10 seconds.	Yes	Provide Evidence in Column J			5	2 To access controls to change the delay timer parameter is controlled by passwords. Chief Engineer is the only authorized person, who can make changes to this system.			4	2	8
	Ship automation provides operational status to engineers too late (H1-3)	Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status.	Operational status indicators shall operate in real time, providing an indication of status with 1 second of accuracy.	Yes	Provide Evidence in Column J			5	2 System is as designed. No changes have been made to these controls		High effectiveness, low criticality	4	3	12
	Ship automation provides operational status to ECR too late (H1-3)	Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status.	Operational status indicators shall operate in real time, providing an indication of status with 1 second of accuracy.	Yes	Provide Evidence			5	2 System is as designed. No changes have been made to these controls			4	3	12
	Ship automation does not provide ECR operational status (H1-3)	Signal from the sensor has been inhibited during maintenance and not brought back online.	Upon equipment start-up, warnings shall be presented if sensors are inhibited.	Yes	Provide Evidence			5	2 System monitors malfunctions and inhibited functions			4	3	12
	Ship automation stops the water mist release too soon when oil leak is still present (H-1)	ECR/ engineer prevents the release of the water mist system as they believe the leak no longer presents a risk.	Engineer shall be aware of emergency response and on the factors to review in assuming a situation no longer poses a risk of H-1.	Yes				5	2 Engineers are well trained in this aspect			2	5	10
	Ship automation releases the water mist too late when exposed hot surface exists (H-1)	No automation in place to automatically release deluge on reception of sufficient alarm alarms indicating exposed hot surface. Release only occurs on manual detection of a hot surface.	Equipment posing a threat of H1 shall have means of automated water mist release.	Yes				5	2 Manual release can be done from the ECR as well as locally. Automatic release will happen if two sensors are activated at the same time.		Low effectiveness, high criticality	2	4	8
	Ship automation shuts down the fuel supply too late during an oil leak (H2-3)	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating oil leak are false alarms. Shutdown only activated when further alarms are received.	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.	Yes				5	2 The false alarms are tracked on a continuous basis and addressed.			3	4	12
	Ship automation does not shutdown the fuel supply when exposed hot surface exists (H-1).	No automation in place to shutdown fuel supply on reception of exposed hot surface alarm	Equipment posing a threat of H1 shall have means of automated shutdown linked to hot surface detectors.	No					No such system fitted			3	5	15

Controller	Unsafe Control Action	Causal Factor	Functional Requirement	Is the functional requirement addressed?	Is Evidence Required?	Explanation Required?	How do you rank the effectiveness of the functional requirement = 1-6	How do you rank the criticality of the functional requirement = 1-5	Evidence/ Explanation Notes	Additional Notes	FR Spread	STPA Barrier Effectiveness	STPA Criticality	STPA Magnitude of risk reduction
ECR Controller	ECR does not provide status of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1)	Personnel in the ECR do not recognise the dangers associated with exposed hot surfaces.	Requirements of SOLAS regarding the presence of H-1 shall be known by engineers.	Yes	Provide Evidence in Column K			4	2 From experience in previous company as well as discussions on board this ship.			5	5	25
	ECR provides instruction to ignore the exposed hot surfaces (H-1)	ECR personnel treat exposed hot surfaces (which breach SOLAS rules) as normal and do not treat this as a hazard.	Requirements of SOLAS shall be maintained.	Yes	Provide Evidence in Column J				By taking immediate action to treat exposed hot surface		High Magnitude of Risk Reduction	5	5	25
	ECR doesn't shutdown the engine when exposed hot surfaces exist (H-1)	ECR is aware of exposed hot surfaces but this is taken as normal, therefore engines remain operational and exposed hot surfaces remain in place.	Requirements of SOLAS shall be maintained.	Yes	Provide Evidence in Column J				Depending on the situation, an additional engine will be started and the one with hot spot to be shut down. If shutting down the engine can result in a Navigational Incident, then delay the shutting down.			5	5	25
	ECR doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	Valve siezed shut due to lack of use.	Water mist release valves used to prevent or mitigate H-1 shall be subect to operation and inspection during maintenance as per manufacturer recommendation.	Yes				4	2 Shipboard Planned Maintenance System (PMS) covers maintenance and testing routines for these items.	In case of failure of the item, unplanned maintenance is carried out. All maintenance records are maintained in AMOS		4	5	20
	ECR does not provide instruction to chief engineer/ engineer therefore measures to remedy exposed hot surfaces or potential/ existing oil leak are not implemented (H1-3)	No direct communication exists between ECR and engineers in the ER.	Engineers in the ER shall have a direct line of real time communication to the ECR.	Yes	Provide Evidence in Column J				Handover checklist / notes are used during change of watch. Closed loop communication by Duty Engineer with 3rd Engineer, Motorman and Oiler who are in the engine room on duty, by means of VHF and fixed and mobile phones.			3	1	3
	ECR doesn't shutdown the engine when exposed hot surfaces exist (H-1)	No function exists in the ECR to allow the detection of an exposed hot surface to annunciate in the ECR.	Personnel in the ECR shall be alerted to the detection of exposed hot surfaces in the ER.	Yes				4	Alarm system (Autronica) in ECR will be activated by detection of Flame (including high 4 temperature) and smoke sensors.		Low Magnitude of Risk Reduction	3	1	3
	ECR doesn't shutdown the fuel supply when strain on the components exceeds design threshold (H-2, H-3)	No function exists in the ECR to allow the detection of design threshold being breached to annunciate in the ECR.	Design threshold detectors (i.e. oil system pressure) in the ER shall have an alarm function within the ECR which will alert ECR personnel to the presence of potential breaks in containment.	Yes				4	2 Low pressure detection sensors, oil mist detector and dirty leak alarm will alert to the situation.			4	1	4
	ECR doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	No function exists in the ECR to allow the detection of an exposed hot surface/ oil leak to annunciate in the ECR.	Hot surface detectors in the ER shall have an alarm function within the ECR which will alert ECR personnel to the presence of H-1.	Yes	Provide Evidence in Column J			3	Alarm system (Autronica) in ECR will be activated by detection of Flame (including high 2 temperature) and smoke sensors.			3	1	3
	ECR releases the water mist too late when leak exists (H-2, H-3).	No function exists in the ECR to allow the detection of an oil leak to annunciate in the ECR.	Oil leak detectors in the ER shall have an alarm function withiin the ECR which will alert ECR personnel to the presence of oil leaks.	Yes				5	2 Low pressure in Common Rails system will shut down the engine			3	1	3
	ECR does not report on loss of integrity to company who would approve a review of safety (H-1, H-2, H-3)	Company liaison on the ship is not trained in report writing and fails to communicate the loss of integrity to the hierarchy, meaning management are unaware of the ocurrence of fatigue to the hot box, fatigue of the fuel supply system, or exposed hot surfaces.	Engineers shall be aware of how to present clear and concise reports relating to work or equipment posing a risk of H1-3.	Yes	Provide Evidence in Column J			5	Accidents & Incidents Reporting System (AIRTS) is used for reporting. These reports are done by 2 the senior engineers and not the Duty Engineer. But input is taken from the D/E.		High effectiveness, low criticality	4	3	12
	ECR does not provide operational status meaning engineer/ chief engineer breaks containment (H2-3)	Personnel in the ECR are overrun with data and work and do not have time to respond to the operational status request from engineers.	Staffing and priorities shall allow for operational status requests from the ER to be addressed immediately.	Yes	Provide Evidence in Column J			5	Vessel has enough persons on board as required by the Company's PAR level and this is more 2 than the Flag requirement stated in the Minimum Safe Manning Document.			4	3	12
	ECR shuts down the engine and does not immediately reduce load on other engines which become temporarely overloaded (H-1, H-2)	ECR is unaware of the design loads which could be generated elsewhere by shutting down the engine.	Engineers shall be aware of the impact of shuting down an engine on other systems where this could lead to increased risk of H2-3 elsewhere.	Yes	Provide Evidence in Column J			5	C/Es Standing Orders cover similar situations and instructions are provided. Also discussed during 2 various meetings on board.			4	3	12
	ECR shuts down the engine too late when a fuel/ lube oil release exists (H-2, H-3)	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.	Yes	Provide Evidence in Column J			5	2 Engineer was aware that the fuel valves need to be shut down immediately			2	5	10
	ECR shuts down the engine and does not immediately reduce load on other engines which become temporarely overloaded (H-1, H-2)	No warnings are in place to advise on the impact of the decision to shutdown the engine on the remainder of the system, therefore action is taken with no knowledge of the effect.	Where an engine is to be shutdown remotely, system should be in place to monitor and advise of the impact of shutdown (H2-3).	Yes	Provide Evidence in Column J			5	This is done based on experience in previous company and discussions in various meetings 2 onboard. No specific procedure in Safety Management System (SQM)		Low effectiveness, high criticality	3	5	15
	ECR provides status of imminent/ existing leak from oil system too late meaning engineer/ chief engineer does not provide a fix (H2-3)	Sensors to detect imminent/ existing oil leak are incorrectly positioned meaning the situation has to escalate to generate an alarm.	Sensors intended to detect imminent/ existing oil leak shall be strategically placed to detect pressure increases/ excessive vibration/ oil mist at the locations these are likely to exist.	Yes	Provide Evidence in Column J			5	2 Sensors are located at strategical locations			3	5	15
	ECR provides status too late of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1)	Sensors to detect exposed hot surfaces are incorrectly positioned meaning the hot surfaces has to expand to generate an alarm.	Sensors intended to detect exposed hot surfaces shall be strategically placed to detect exposed hot surfaces at the locations these are likely to exist.	Yes	Provide Evidence in Column J			5	2 It is the same sensors as above.			3	5	15

Controller	Unsafe Control Action	Causal Factor	Functional Requirement	Is the functional requirement addressed?	Is Evidence Required?	Explaination Required?	How do you rank the effectiveness of the functional requirement = 1-6	How do you rank the criticality of the functional requirement = 1-5	Evidence/ Explaination Notes	Additional Notes	FR Spread	STPA Barrier Effectiveness	STPA Criticality	STPA Magnitude of risk reduction
ECR Controller	ECR does not provide status of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1)	Personnel in the ECR do not recognise the dangers associated with exposed hot surfaces.	Requirements of SOLAS regarding the presence of H-1 shall be known by engineers.	Yes	Provide Evidence in Column K		5	5	Know from best practice and various courses prior to Certificate of Competency exams.			5	5	25
	ECR provides instruction to ignore the exposed hot surfaces (H-1)	ECR personnel treat exposed hot surfaces (which breach SOLAS rules) as normal and do not treat this as a hazard.	Requirements of SOLAS shall be maintained.	Yes	Provide Evidence in Column J		5	5	Shore technician checks engines for hot spots using thermographic camera regularly and spot checks are done by First Engineer by using the Ship's thermographic camera. Various trainings are also provided.		High Magnitude of Risk Reduction	5	5	25
	ECR doesn't shutdown the engine when exposed hot surfaces exist (H-1)	ECR is aware of exposed hot surfaces but this is taken as normal, therefore engines remain operational and exposed hot surfaces remain in place.	Requirements of SOLAS shall be maintained.	Yes	Provide Evidence in Column J		5	5	The effected engine will be shut down immediately and First Engineer will be contacted to deal with the hot surface.			5	5	25
	ECR doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	Valve siezed shut due to lack of use.	Water mist release valves used to prevent or mitigate H-1 shall be subect to operation and inspection during maintenance as per manufacturer recommendation.	Yes			5	4	This is part of the Ship's approved Planned Maintenance System (PMS)			4	5	20
	ECR does not provide instruction to chief engineer/ engineer therefore measures to remedy exposed hot surfaces or potential/ existing oil leak are not implemented (H1-3)	No direct communication exists between ECR and engineers in the ER.	Engineers in the ER shall have a direct line of real time communication to the ECR.	Yes	Provide Evidence in Column J		4	2	VHF, Mobile and fixed phone systems are used to communicate between ECR and Engine Room personal.			3	1	3
	ECR doesn't shutdown the engine when exposed hot surfaces exist (H-1)	No function exists in the ECR to allow the detection of an exposed hot surface to annunciate in the ECR.	Personnel in the ECR shall be alerted to the detection of exposed hot surfaces in the ER.	Yes			5	4	The ER duty team (3rd Engineer, Motorman & oiler) are trained and will report any damage to shielding / insulation of hot surface and attempt to correct same. If deemed necessary, the engine will be shut down.		Low Magnitude of Risk Reduction	3	1	3
	ECR doesn't shutdown the fuel supply when strain on the components exceeds design threshold (H-2, H-3)	No function exists in the ECR to allow the detection of design threshold being breached to annunciate in the ECR.	Design threshold detectors (i.e. oil system pressure) in the ER shall have an alarm function within the ECR which will alert ECR personnel to the presence of potential breaks in containment.	Yes			4	4	Pressure switches in the system will activate an alarm. Dirty leak alarm will also activate if there is a leak. Fuel supply will be shut of immediately. Quick closing valves will also be activated, if required.			4	1	4
	ECR doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	No function exists in the ECR to allow the detection of an exposed hot surface/ oil leak to annunciate in the ECR.	Hot surface detectors in the ER shall have an alarm function within the ECR which will alert ECR personnel to the presence of H-1.	Yes	Provide Evidence in Column J		4	4	Flame and smoke detectors are in place above each engine			3	1	3
	ECR releases the water mist too late when leak exists (H-2, H-3).	No function exists in the ECR to allow the detection of an oil leak to annunciate in the ECR.	Oil leak detectors in the ER shall have an alarm function withiin the ECR which will alert ECR personnel to the presence of oil leaks.	Yes			4	4	Pressure switches in the system will activate an alarm. Dirty leak alarm will also activate if there is a leak. Fuel supply will be shut of immediately. Quick closing valves will also be activated, if required.			3	1	3
	ECR does not report on loss of integrity to company who would approve a review of safety (H-1, H-2, H-3)	Company liaison on the ship is not trained in report writing and fails to communicate the loss of integrity to the hierarchy, meaning management are unaware of the ocurrence of fatigue to the hot box, fatigue of the fuel supply system, or exposed hot surfaces.	Engineers shall be aware of how to present clear and concise reports relating to work or equipment posing a risk of H1-3.	Yes	Provide Evidence in Column J		3	4	Any malfunction in the engine room, related to the engines, will be reported immediately to Staff Chief to First Engineer.	Verified entries in Mechanical & Electrical malfunction log as well as Leaks Log.	High effectiveness, low criticality	4	3	12
	ECR does not provide operational status meaning engineer/ chief engineer breaks containment (H2-3)	Personnel in the ECR are overrun with data and work and do not have time to respond to the operational status request from engineers.	Staffing and priorities shall allow for operational status requests from the ER to be addressed immediately.	Yes	Provide Evidence in Column J		3	4	Adequate staff is always available in the engine room			4	3	12
	ECR shuts down the engine and does not immediately reduce load on other engines which become temporarily overloaded (H-1, H-2)	ECR is unaware of the design loads which could be generated elsewhere by shutting down the engine.	Engineers shall be aware of the impact of shutting down an engine on other systems where this could lead to increased risk of H2-3 elsewhere.	Yes	Provide Evidence in Column J		2	4	Power Management System will initiate preferential trips of non-critical equipment. Standby engine will start automatically. Then normalcy will be restored after addressing issues.			4	3	12
	ECR shuts down the engine too late when a fuel/ lube oil release exists (H-2, H-3)	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdow capability.	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.	Yes	Provide Evidence in Column J		2	5	While using emergency shutdown, this would automatically shut off the fuel valves. Pre-Lube pump will be shut of manually.	Engineer was aware of additional actions to be taken, depending on the seriousness of the emergency.		2	5	10
	ECR shuts down the engine and does not immediately reduce load on other engines which become temporarily overloaded (H-1, H-2)	No warnings are in place to advise on the impact of the decision to shutdown the engine on the remainder of the system, therefore action is taken with no knowledge of the effect.	Where an engine is to be shutdown remotely, system should be in place to monitor and advise of the impact of shutdown (H2-3).	Yes	Provide Evidence in Column J		2	4	Bridge will be contacted immediately about any consequence in reducing the speed of the vessel. When the engine is remotely shut off, preferential trip will be automatically activated. Then the standby engine will be started automatically. The system display will indicate the impact of the shut down and the preferential trip has to be reset.		Low effectiveness, high criticality	3	5	15
	ECR provides status of imminent/ existing leak from oil system too late meaning engineer/ chief engineer does not provide a fix (H2-3)	Sensors to detect imminent/ existing oil leak are incorrectly positioned meaning the situation has to escalate to generate an alarm.	Sensors intended to detect imminent/ existing oil leak shall be strategically placed to detect pressure increases/ excessive vibration/ oil mist at the locations these are likely to exist.	Yes	Provide Evidence in Column J		3	4	Oil mist detector, T/C vibration monitor, pressure sensors, leak sensors are fitted on strategic locations.			3	5	15
	ECR provides status too late of exposed hot surface meaning engineer/ chief engineer does not provide a fix (H-1)	Sensors to detect exposed hot surfaces are incorrectly positioned meaning the hot surfaces has to expand to generate an alarm.	Sensors intended to detect exposed hot surfaces shall be strategically placed to detect exposed hot surfaces at the locations these are likely to exist.	Yes	Provide Evidence in Column J		4	2	Flame and smoke detectors are placed in strategic locations			3	5	15

Controller	Unsafe Control Action	Causal Factor	Functional Requirement	Is the functional requirement addressed?	Is Evidence Required?	Explaination Required?	How do you rank the effectiveness of the functional requirement = 1-6	How do you rank the criticality of the functional requirement = 1-5	Evidence/ Explaination Notes	Additional Notes	FR Spread	STPA Barrier Effectiveness	STPA Criticality	STPA Magnitude of risk reduction
Automation	Ship automation does not provide engineers operational status (H1-3)	Indication is not clearly represented due to poorly illuminated LED/ dirt obscuration.	Operational status shall be easily discernible and indicator shall be clear and visible.	Yes	Provide Evidence in Column J		4	4	3 Alarm system is easily visible to the ECR			4	4	16
	Ship automation does not provide ECR operational status (H1-3)	No sensor is provided for ship automation that the fuel oil system/ engine is operational as there is no sensor in place. The ECR then instructs engineer to conduct maintenance on the system and breaks containment.	Operational status shall be known to the process controller.	Yes	Provide Evidence in Column J		4	4	2 Sensors are fitted to indicate fuel system and engine is operational.		High Magnitude of Risk Reduction	4	4	16
	Ship automation does not provide an alarm during an oil leak (H2-3)	No sensor provided to detect presence of an oil leak/ mist therefore no alarm can be presented.	Presence of oil mist both within the hot box and the ER shall be known to the process controller.	Yes	Provide Evidence in Column J		4	4	2 Oil mist sensors are fitted			3	5	15
	Ship automation does not alarm to exposed hot surface (H-1)	No sensor provided to detect presence of an exposed hot surface therefore no alarm can be presented.	Presence of exposed hot surfaces (>250 deg C) ER shall be known to the process controller.	No	State Why in Column J		2	4	2 No temperature sensor fitted to measure temperature of hot surfaces. However, exhaust gas temperature sensors would indicate hot surface on the engine. Also, smoke and flame detectors can indicate same.			3	5	15
	Ship automation does not alarm to pressure deviation in the oil systems (H2-3)	No feedback exists on stream pressure because no sensor is in place, resulting in no alarm signal on pressure deviation, resulting in pipework rupture	Stream pressure shall be known to the process controller.	Yes	Provide Evidence in Column J		4	4	2 Pressure sensors are fitted to detect high or low pressure	??		3	2	6
	Ship automation does not provide an alarm during an oil leak (H2-3)	Ship automation receives sensor data of reduced pressure as a result of a leak but misinterprets the data as normal operation as the set point is not relevant to the design tolerance, therefore does not send alarm, resulting in continual leak	Set points applied to alarm to system pressure drop in the event of a leak shall be set based on the anticipated pressure which could be presented through a break in containment.	Yes	Provide Evidence in Column J		4	4	2 Design set pressure has not been altered. However, there is provision to change these settings. Access is strictly restricted to do this.		Low Magnitude of Risk Reduction	3	2	6
	Ship automation shuts down the engine when pressure in the oil systems is normal (H2-3)	Shutdown action is intended for a different engine from where the pressure deviation is present through incorrectly programmed control system, increasing demand on the already faulty engine	Automated shutdown shall be based directly from the sensors installed on that machine.	Yes	Provide Evidence in Column J		4	4	2 Regular tests are conducted on board to ensure that the alarm and shut down systems are functional.			3	1	3
	Ship automation shuts down the engine too late during an oil leak (H2-3)	Automated shutdown action has been inhibited during maintenance and not brought back online.	Upon completion of maintenance, all inhibits shall be removed.	Yes	Provide Evidence in Column J		4	4	2 Permit to work systems are followed. Two person check is also in place			3	2	6
	Ship automation provides operational status to engineers too late (H1-3)	An excessive time delay has been implemented in the control system to avoid spurious signals based on standard system fluctuations, meaning the true operational status is presented too late.	Time delays shall not be beyond the point at which the operational status needs to be know. i.e. time delay of no greater than 10 seconds.	Yes	Provide Evidence in Column J		4	4	2 Design set points has not been altered. However, there is provision to change these settings. Access is strictly restricted to do this.			4	2	8
	Ship automation provides operational status to engineers too late (H1-3)	Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status.	Operational status indicators shall operate in real time, providing an indication of status with 1 second of accuracy.	Yes			4	4	2 Readings are checked on a regular basis.		High effectiveness, low criticality	4	3	12
	Ship automation provides operational status to ECR too late (H1-3)	Sensor in place is not of a sufficiently fast response to provide a 'real time' operational status.	Operational status indicators shall operate in real time, providing an indication of status with 1 second of accuracy.	Yes	Provide Evidence		4	4	2 Readings are checked on a regular basis.			4	3	12
	Ship automation does not provide ECR operational status (H1-3)	Signal from the sensor has been inhibited during maintenance and not brought back online.	Upon equipment start-up, warnings shall be presented if sensors are inhibited.	No			2	4	2 No alarm fitted to indicate inhibiters are not removed			4	3	12
	Ship automation stops the water mist release too soon when oil leak is still present (H-1)	ECR/ engineer prevents the release of the water mist system as they believe the leak no longer presents a risk.	Engineer shall be aware of emergency response and on the factors to review in assuming a situation no longer poses a risk of H-1.	Yes			5	4	2 They are trained			2	5	10
	Ship automation releases the water mist too late when exposed hot surface exists (H-1)	No automation in place to automatically release deluge on reception of sufficient alarm alarms indicating exposed hot surface. Release only occurs on manual detection of a hot surface.	Equipment posing a threat of H1 shall have means of automated water mist release.	Yes			5	4	2 Flame and smoke detectors are fitted and when two sensors are activated, the system will be activated automatically		Low effectiveness, high criticality	2	4	8
	Ship automation shuts down the fuel supply too late during an oil leak (H2-3)	ECR/ engineer prevents the automated shutdown as they believe the alarms indicating oil leak are false alarms. Shutdown only activated when further alarms are received.	The cause of regular false alarms shall be determined and rectified and shall not be accepted as normal. Alarms shall be treated as real events.	Yes			5	4	2 All alarms will be investigated			3	4	12
	Ship automation does not shutdown the fuel supply when exposed hot surface exists (H-1).	No automation in place to shutdown fuel supply on reception of exposed hot surface alarm	Equipment posing a threat of H1 shall have means of automated shutdown linked to hot surface detectors.	No			4	4	2 The increase in temperature would be decked by smoke or flame alarm but this will not shut down the engine or fuel system automatically.			3	5	15

Controller	Unsafe Control Action	Causal Factor	Functional Requirement	Is the functional requirement addressed?	Is Evidence Required?	Explaination Required?	How do you rank the effectiveness of the functional requirement = 1-6	How do you rank the criticality of the functional requirement = 1-5	Evidence/ Explaination Notes	Additional Notes	FR Spread	STPA Barrier Effectiveness	STPA Criticality	STPA Magnitude of risk reduction
	Engineer does not detect loss of integrity during inspection (H-2, H-3)	Engineer is not aware of what to look for/ what the signs are of loss of integrity due to lack of skills/ knowledge.	Engineers shall be able to recognise hot box and fuel supply pipework/ engine loss of integrity which can lead to H2-3.	Yes	Provide Evidence in Column J		4	2	Watchkeeping team in ER (3rd Engineer, Motorman & Oiler) are trained to detect oil leaks from the engine. How to inspect hot boxes. They are constantly monitoring same. ECR will receive alarms (Clean or dirty oil leaks)	Leaks have happened in the past but not due to casual factor.		4	5	20
	Engineer does not detect loss of integrity during inspection (H-2, H-3)	The interval between inspections of the hot box and fuel supply pipework is too lengthy resulting in severe degradation between inspections not being detected.	Manufacturer requirements to prevent H2-3 shall be met.	Yes	Provide Evidence in Column J		4	2	The vessels approved Planned Manteca System (PMS) is based on manufacturers instructions. The work orders from the PMS is carried out in a timely manner.	Sometimes maintenance is delayed due to lack spare parts. Leaks have happened in the past but not due to casual factor.		4	5	20
	Engineer interferers with equipment and doesn't return to its original condition during inspection (H-1, H-2, H-3)	Engineer does not have the training/ skillset to adequately understand the impact of interfering with equipment to get a closer inspection, resulting in continued hot surface exposure, or damaged/ fatigued equipment.	Engineers shall be capable of returning equipment back into service in a safe state to prevent H1-3.	Yes	Provide Evidence in Column J		3	2	Engineers are trained to carry out proper maintenance according to maintenance manual.	Leaks have happened in the past but not due to casual factor.	High Magnitude of Risk Reduction	4	5	20
	Engineer doesn't shutdown or stop the fuel supply when strain on the components exceeds design threshold (H-2, H-3)	Engineers are unaware of the design loads which should not be exceeded due to their potential to break containment/ cause exposed hot surfaces. Training inadequate, therefore fuel supply is not shutdown the moments before a hazard is realised.	Engineers shall be aware of precursors which can lead to H-2, and when shutdown of the supply should take place.	No		State Why in Column J		2	Engineers are aware of the hazard. There is no visible or audible alarm to indicate this situation. However, parameters can be monitored. But, will they be able to process the amount of information available to them?			4	5	20
	Engineer shuts down the fuel supply too late when a fuel/ lube oil release exists (H-2, H-3)	Engine shutdown does not automatically shutdown supply of fuel to that engine. Engineers unaware of fuel continually being sent to the engine which has been shutdown due to a leak.	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.	Yes	Provide Evidence in Column J		2	2	ECR engineers are trained to use emergency shut down as this would automatically shut off fuel supply.	Leaks have happened in the past but not due to casual factor.		2	5	10
	Engineer doesn't release the water mist when exposed hot surfaces exist and oil mist in atmosphere is detected/suspected (H-1)	Engine shutdown buttons are not easily accessible, delaying the time taken to shutdown the engine.	Access to the emergency push buttons for both engine shutdown and fuel supply shutdown shall be accessible from multiple locations/ directions from the engine to prevent or mitigate H2-3.	Yes	Provide Evidence in Column J		2	3	Panel is easily accessible. This panel has controls for Hi-Fog, Emergency stop of the engine and quick closing valves.	The criticality is probably and addressed and not overlooked.	Low Magnitude of Risk Reduction	2	4	8
	Engineer releases the water mist too late when exposed hot surface exists (H-1)	Water mist release mechanism has been inhibited during maintenance and not brought back online.	Upon completion of maintenance, all inhibits shall be removed.	Yes	Provide Evidence in Column J		4	3	Lockout and tagout system, from SQM, is used to ensure are removed.			2	2	4
	Engineer starts repair, but doesn't complete when faulty equipment is present (H-1, H-2, H-3)	Engineer begins maintenance but is called to tend to other issues and does not complete the maintenance/ repair. No log exists to prevent activation of the equipment. Incomplete repair results in flammable material release on start-up	Staffing shall allow for planned maintenance of equipment posing a risk of H1-3, as well as capacity to deal with unplanned activities which increase the risk of H1-3.	Don't Know		State Why in Column J	4	2	Additional manpower would further enhance this process.			4	2	8
Engineer	Engineer repairs equipment but does not complete/ implement the repair correctly (H-1, H-2, H-3)	Engineer unaware of how to apply the manufacturer guidelines when checking equipment (i.e. bolts on the fuel supply pipework) due to a lack of qualification/ competence.	Engineers shall be familiar with equipment on board where a risk of H1-3 exists and trained on all potential actions required to be made on that equipment.	Yes	Provide Evidence in Column J		4	3	Company provides training to all 2nd Engineers and above. This training is conducted by the manufacturer.	The criticality is probably and addressed and not overlooked.		4	2	8
	Engineer starts repair, but doesn't complete when faulty equipment is present (H-1, H-2, H-3)	Engineer begins the repair but comes up against a repair process he/ she is unfamiliar with and stops mid way through.	If a job remains unfinished, equipment shall be made safe and records shall be maintained to show the job is unfinished. Unfinished repair shall be marked accordingly (e.g. lockout-tagout / LOTO)	Yes	Provide Evidence in Column J		4	2	Lockout tagout system is part of the company's SQM and implemented on board.			4	2	8
	Engineer repairs equipment too late when damaged/ faulty equipment exists (H-1, H-2, H-3)	Engineer receives feedback that equipment is faulty but does not attend to the failure due to an extensive workload. The equipment is brought back online before the engineer can tend to the faulty equipment resulting in a break in containment/ hot surface	Tasks which increase the risk of H1-3 shall only be assigned when the engineer has availability to complete them.	Yes	Provide Evidence in Column J		4	2	sufficient redundancy exists on board. The vessel ahs six engines and all are not required at the same time.		High effectiveness, low criticality	4	2	8
	Engineer repairs equipment but does not complete/ implement the repair correctly (H-1, H-2, H-3)	Engineer unaware of how to apply the manufacturer guidelines when checking equipment (i.e. bolts on the fuel supply pipework) due to a lack of qualification/ competence.	Engineers shall be familiar with equipment on board where a risk of H1-3 exists and trained on all potential actions required to be made on that equipment.	Yes	Provide Evidence in Column J		4	2	Company provides training to all 2nd Engineers and above. This training is conducted by the manufacturer.			4	2	8
	Engineer does not detect incorrect implementation of equipment as per manufacturer guidelines during inspection (H-2, H-3)	Planned maintenance routine does not provide instruction of inspection intervals meaning the engineer does not get tasked with inspecting the equipment.	Maintenance task list shall be clear and easily followed to prevent H2-3.	Yes	Provide Evidence in Column J		4	3	PMS job descriptions are detailed and the Engineers have ready access to engine manuals	The criticality is probably and addressed and maybe overlooked.		3	5	15
	Engineer doesn't repair equipment when faulty equipment present (H-1, H-2, H-3)	No sensor is applied to check for failures of equipment therefore the Engineer is not informed of a faulty/ damaged piece of equipment. No remedial action is therefore taken resulting in a break in containment from weakened equipment/ exposed hot surface due to faulty equipment operation	System shall be able to monitor real time health status of engine and fuel supply system, providing alarms when faults which can lead to H1-3 occur.	Yes	Provide Evidence in Column J		4	2	Condition Based Maintenance System is in "pilot" mode on this vessel. The manufacturers of the engines are monitoring the all parameters of all engines when they are running. Any discrepancy is immediately reported to the vessel for corrective actions from the vessel.		Low effectiveness, high criticality	3	5	15
	Engineer doesn't shutdown, stop or remove the engine from service when exposed hot surfaces exist (H-1)	Engineers are aware of exposed hot surfaces (which are taken as normal), but are unaware of other risk factors which would require an engine shutdown (i.e. oil leak, unacceptable pressure in fuel supply pipework, excessive vibration which could cause an imminent rupture), meaning no shutdown action is taken.	System to detect oil leaks in the hot box and the engine room shall be provided (H2-3).	Yes	Provide Evidence in Column J		4	2	Leak detection alarm systems are fitted and functional.			3	5	15
	Engineer shuts down the engine too late when a fuel/ lube oil release exists (H-2, H-3)	Time taken between pushing the engine shutdown button and loads being reduced takes too long due to limitations on the engine shutdown capability.	When an engine is shutdown, fuel supply to that engine shall be shutdown instantly with fast response valve closure and pump shutdown to prevent or mitigate H2-3.	Yes	Provide Evidence in Column J		2	2	ECR engineers are trained to use emergency shut down as this would automatically shut off fuel supply.			2	5	10

Appendix D: Systemic HAZID and Operational Risk Evaluation (SHORE) Simplified Tool

Diagram of Safety Control

*Import diagram of safety control and highlight the controller this STPA sheet relates to.
Tools are available below which can be used to generate the SCD:
https://github.com/SE-Stuttgart/XSTAMPP
https://astah.net/products/system-safety-diagrams/

Controller	Engineer	**Unsafe Contexts:**
Objective/ responsibility	Maintain equipment within the ER, ensuring hot surfaces and breaks in containment do not occur.	Not Providing
Input	Instruction from Chief Engineer/ ECR. Initiative while in the ER. Sensor readings.	Providing
Output	Repair of equipment. Maintenance of equipment. Reports to Chief Engineer/ Company. Feedback to ECR. Manual process control when required.	Too early Too late
Constraints	Resources, Time, Instructions, Training, Autonomy	Stopped to soon/ duration applied = too short Stopped too late/ duration applied = too long

Hazard ID	**Hazard Description**
H1	Release of flammable oil
H2	Exposed hot surface
H1&H2	Release of flammable oil & exposed hot surface

Control Action ID	**Control Action**	**Unsafe Context**	**Unsafe Control Action**
CA1	Break containment on equipment	Providing	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)
CA2	Switch off equipment	Not Providing	Engineer does not switch off equipment when the equipment operating outside of the safe operating limits (H-2, H-3)
CA3	Report on equipment integrity	Not Providing	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)

Control Action ID	Unsafe control action	Causal Factor Category	Causal Factor	Casual Factor ID
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	Inadequate input from other controllers/ environment	No direct communication to the control room to advise if the equipment is operational or otherwise	CF1
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	Inconsistent process/ mental model	Indication in the control room shows the equipment is isolated, but indication at the equipment shows it is operational. Conflicting information so the engineer selects the information allowing the work to be completed.	CF2
CA2	Engineer does not switch off equipment when the equipment operating outside of the safe operating limits (H-2, H-3)	Inadequate feedback	No sensors in place to monitor and present safe operating limits to the engineer	CF3
CA3	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)	Inadequate control algorithm/ inadequate responsibilities, knowledge or skills	Engineer is not aware there is a requirement to report on loss of integrity	CF4

ID-UCA	UCA	CF ID	Causal factor	ID-FR	Functional requirements	UCA Category	CF Category	Relevant barriers	Signals and their requirements	Hazard	Previous occurrence in Incident/ Accident (Y/N) + incident ref	Barrier Effectiveness	Criticality	Magnitude of risk reduction
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	CF1	No direct communication to the control room to advise if the equipment is operational or otherwise	FR1	Engineers in the machinery space who will be interefering with equipement shall have a direct line of communication to the ECR.	Maintenance	Inadequate communication	Permit to work procedure	Communication channel between control room and engineer must exist, with engineers empowered to stop the job. Audit of embracing of maintenance management system.	H1	Le Boreal	4	4	16
CA1	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	CF2	Indication in the control room shows the equipment is isolated, but indication at the equipment shows it is operational. Conflicting information so the engineer selects the information allowing the work to be completed.	FR2	Breaking containment shall only ocurr when there is no contradictory information regarding operational state.	Inadequate maintenance/ repair	Inadequate feedback of equipment status/ health	Visual indicator (e.g. engine operational)	Indicator reading in real time.	H1	Le Boreal	3	4	12
CA2	Engineer does not switch off equipment when the equipment operating outside of the safe operating limits (H-2, H-3)	CF3	No sensors in place to monitor and present safe operating limits to the engineer	FR3	Safety critical operational data (i.e. pressure) shall be monitored and presented to ship personnel.	Incident response	Inadequate feedback of hazard in the ER to the ECR	Safety Instrumented System	Pressure sensors with diagnostics showing sensor health status.	H1	Splendour of the Seas, Carnival Triumph	3	5	15
CA3	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)	CF4	Engineer is not aware there is a requirement to report on loss of integrity	FR4	Roles and responsibilities shall be clearly documented and known by staff.	Reporting	Training	Training/ Competence Management System	Audit of Competence and job knowledge.	H1&H2	N/A	4	3	12

Controller	Unsafe Control Action	Causal Factor	Functional Requirement	Is the functional requirement addressed?	Evidence (if required)	Explaination (if require)	How do you rank the effectiveness of the functional requirement = 1-6	How do you rank the criticality of the functional requirement = 1-5	Evidence/ Explaination Notes	Additional Notes	STPA MORR	Auditee MORR
Engineer	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	No direct communication to the control room to advise if the equipment is operational or otherwise	Engineers in the machinery space who will be interefering with equipement shall have a direct line of communication to the ECR.	Yes	Radio required under permit to work		4	2			16	8
Engineer	Engineer breaks containment on equipment when the equipment is operational (H-2, H-3)	Indication in the control room shows the equipment is isolated, but indication at the equipment shows it is operational. Conflicting information so the engineer selects the information allowing the work to be completed.	Breaking containment shall only ocurr when there is no contradictory information regarding operational state.								12	0
Engineer	Engineer does not switch off equipment when the equipment operating outside of the safe operating limits (H-2, H-3)	No sensors in place to monitor and present safe operating limits to the engineer	Safety critical operational data (i.e. pressure) shall be monitored and presented to ship personnel.								15	0
Engineer	Engineer does not report on loss of integrity to hierarchy who would approve/ instruct the repair to be completed (H-1, H-2, H-3)	Engineer is not aware there is a requirement to report on loss of integrity	Roles and responsibilities shall be clearly documented and known by staff.								12	0