Systems Approach to Accident Analysis: Engine Room Fire on Cruise Ship "Le Boreal"

Romanas Puisa, *r.puisa@strath.ac.uk*

Stuart Williams, *stuart.williams@strath.ac.uk*

Dracos Vassalos, *d.vassalos@strath.ac.uk*

Maritime Safety Research Centre of University of Strathclyde

ABSTRACT

The current explanation of accidents is derived from an analysis of proximate events and some contributing causal factors, whereas the role of a wider socio-technical context that give rise to systemic causal mechanisms is often left unexplained. The paper describes analysis results of a recent maritime incident with the purpose to illuminate the causal factors, including systemic ones, and offers a different, more comprehensive explanation of the incident causation to that which is given in the accident investigation report. The study seeks to provide valuable input for enhancements in overall maritime safety control and proactive safety management at the ship and shipping company levels. With the gained knowledge, resources committed to risk management can be better allocated, reducing associated costs and improving on business objectives.

Keywords: *accident analysis; CAST; STAMP; fire; engine room;*

1 INTRODUCTION

The sinking of RMS Titanic in 1912 has become symbolic of risk at sea, and has been used as a global metaphor for avoidable catastrophe, overconfidence, complacency and any other folly. It gave a useful lesson, the sobering realisation that safety was lagging behind technological advancements which were available in support of commercial course. And the accident causes were much deeper and wider than was concluded at the time. The investigation was limited to decision errors on the part of the Master: "*Captain Smith had failed to take proper heed of ice warnings. Collision was the direct result of steaming into a dangerous area at too high speed*" (Butler, 1998), and the role of systemic causal factors, which had been present a long time before the ship was even built, was not explained. These were the absence of harmonised safety regulations and safety control (recall the hasty introduction of SOLAS[1] in the aftermath) (Angel, 2012), overconfidence and complacency ("…*I can best describe my experiences in nearly 40 years at sea … [as]… uneventful.*"[2] (Fitzgibbon, 2012), inadequate preparedness reflected in the limited number of lifeboats, etc.), and the commercial pressure on White Star Line company to cross the Atlantic ahead of competitors. The latter contributed to a recently discovered fact about a coal fire in the engine room, burning for days before the tragic voyage and still during it (Taplin, 2017). As a result, the ship was at risk of serious explosions, which contributed to the Captain's decision to speed up. Although the fire had been contained, it had weakened an adjacent watertight bulkhead which buckled under the water pressure, making the collision with the iceberg fatal. As we show in this paper, this story of Titanic is not an anachronism, and it serves as the epitome of complex causation behind maritime accidents. Maritime accident

[1] International Convention for the Safety of Life at Sea (SOLAS) is an international maritime treaty which sets minimum safety standards in the construction, equipment and operation of merchant ships.

[2] Captain Smith in 1907: *'When anyone asks me how I can best describe my experiences in nearly 40 years at sea, I merely say, uneventful. Of course, there have been winter gales, and storms and fog and the like, but in all my experience I have never been in any accident of any sort worth speaking about. I have seen but one vessel in distress in all my years at sea – a brig, the crew of which were taken off in a small boat in charge of my third officer. I never saw a wreck and have never been wrecked, nor was I ever in any predicament that threatened to end in disaster of any sort. You see, I am not very good material for a story.'*

analysis needs to look for the bigger picture, so the safety problem can be reconstructed and understood better, and consequently addressed in a more cost effective way.

Marine accident investigations serve to inform improvements in design and operational practices. This is an evolutionary strategy for risk management, which aims to create safer systems through progressive enhancements in response to lessons from the latest incidents and accidents (Rasmussen, 1997). Accident analysis, therefore, plays a decisive role in safety development. However, this process is only as good as the core understanding derived from accident analysis and the explanation of causes. In the worst case, an inaccurate accident investigation could cause the wrong changes to be implemented in rules and regulations. The current explanation of accidents remains limited to proximate events (e.g., oil leaks, hot surfaces) and contributing causal factors (e.g., poor maintenance, inadequate SMS), whereas the role of a wider socio-technical context that has given rise to systemic causal mechanisms behind major maritime accidents is hardly explained, despite the evidence (recall the case with Titanic and Le Boreal later described in the paper). Consequently, investments in safety programmes can prove futile and problematic in the end.

Following on from the epitomic circumstances around the Titanic disaster, fires in engine rooms (ER) continue to remain one of the safety challenges for the shipping industry. A study by Det Norske Veritas – Germanischer Lloyd (DNV-GL) claims that two thirds of ship fires have started in the ER, with more than half of them resulting from the contact between combustible oils and high temperature surfaces. Recent examples with passenger ships include Zenith in 2013, Carnival Liberty, Splendour of the Seas, and Le Boreal in 2015, to name a few.

In this paper, we use a systemic accident model to capture causal factors behind a recent ER fire onboard of cruise ship Le Boreal. To this end, we adopted systemic accident model Systems-Theoretic Accident Model and Processes (STAMP) and its method for causal analysis called Causal Analysis using System STAMP (CAST) (N. Leveson, 2011). In contrast to conventional sequential and epidemiological models (e.g., Domino theory, Swiss cheese) which have permeated the current approach to accident analysis, the CAST process allows the analysis of the entire socio-technical system, going beyond proximate events and contributing factors. The presented work analyses the causation of the Le Boreal incident in terms of three types of causal factors. These are a chain of proximate events (direct factors), contributing conditions that allowed the proximate events to occur, and systemic factors that pushed the system towards the state of heightened risk (Johnson, 1980; Rasmussen, 1997). The direct and contributing causal factors can be aligned in a chain of concatenated events (typically post hoc) preceding an unwanted event such as the fire outbreak. They are represented as linear links from causes to effects and hence are easy to understand and communicate. In contrast, the systemic, underlying causal factors have nonlinear effect on the unwanted outcome, and they can only be captured and explained by a systemic accident model such as CAST.

The paper focuses on identification of causal factors that led to the fire incident, ignoring the events following the fire outbreak. Hence, the focus is on accident prevention.

The paper is organised as follows. Section 2 provides a summary of the incident. Section 3 explains the methodology used, Section 4 performs the actual incident analysis, Section 5 summarises the analysis results and recommendations, and Section 6 concludes the paper.

2 INCIDENT SUMMARY

Cruise ship *Le Boreal (*IMO no. 9502506*)* was built by Fincantieri in 2010 to be operated by Compagnie du Ponant, a cruise ship operator, under French flag. The ship is 10,944 GT, 142.1 m in length, 18 m in beam and 4.8 m in draught, and carries 264 passengers and 136 crew. The vessel is powered by 2 x 2300 kW electric motors; four 1600 kW diesel-generators (Wärtsilä 8L20) and one Caterpillar emergency generator rated at of 800 kW.

On 18 November 2015, the vessel suffered a major engine room fire, which caused the loss of all power and left her drifting. The fire broke out at the diesel generator (DG) No. 3 turbo-blower and rapidly spread via the bunched electric cables, to the upper decks of the engine compartment. The captain ordered the ship, with 347 passengers and crew, to be abandoned early in the morning. A distress call was issued just after 2 a.m. while it was near Cape Dolphin, the northerly point of East Falkland, Falkland Islands. As the vessel was drifting towards the coast, the master made the decision to drop anchor and to evacuate the passengers and almost all the crewmembers, with the support of the Royal Navy and of the L'AUSTRAL, her sister-ship owned

by the same company. There were no injuries to the passengers or crew.

The incident was subsequently investigated by French marine casualty investigation board, Bureau d'Enquêtes sur les Événements de Mer (BEAmer), which issued its findings in a report in July 2016. The report was developed in compliance with the "Code for the Investigation of Marine Casualties and Accidents" as per IMO Resolution MSC 255(84) and the EU regulation N°1286/2011 on a common methodology for investigating marine casualties and incidents. The report is accessible online (BEAmer, 2016).

Table 1: Timeline before the fire (17-18 Nov 2015)

11:20	Hotel Officer (HO) begins a patrol
11:30	HO notices that a duplex filter is clogged on DG4 and switches to the reserve filter, he detects an odour of exhaust gases.
11:35	HO ends the patrol and logs parameters in the logbook in the Engine Control Room (ECR)
00:00	Engineering Officer (EO) starts his shift, HO reports about the filter and exhaust smell. EO stays in ECR
00:10	HO attempts to replace the clogged filter on DG3, which was running. Unscrews the cover. Pressurised oil leaks. HO observes a fireball next to turbo-blower exhaust elbow of DG3
00:16	File alarm sounds

The investigation found the following contributing conditions that led to the incident occurring:

- The HO had concerns about the quality of the Heavy Fuel Oil (HFO) being used, which contributed to the decision to replace the reserve filter without waiting for a mechanic rating to arrive in the morning.
- The established practice was to replace the filter cartridges very frequently (2 to 3 times a day, versus the manufacturer's recommendation of every 1,000 hours). This was understood to be due to switching from HFO to Marine Diesel Oil (MDO), which quickly clogged filters.
- There was no coding system, no interlock mechanism to preclude the filter replacement when under pressure existed.
- The HO was alone, therefore there was no benefit of a cross check. The understaffing was identified during the investigation: a rating had been needed to assist in ER.
- During the patrol (shortly before the incident), the HO did not notice any problem with the lagging cover of the turbo-blower exhaust elbow of DG3, which was likely dysfunctional already. No action was taken to rectify the hazard, as a result.

The investigation concluded that "the engineer officer who carried out the replacement of a clogged fuel filter element had been presumably misled by a faulty visual memory and undertook the disassembly of an element under pressure" (BEAmer, 2016). That is, the investigators alluded to the human error. BEAmer recommended that the company consider the addition of a mechanic rating during the night watches and reengineer the fuel system to segregate MDO and HFO, which shared the same fuel feeding line (the filter clogged rapidly when shifting to MDO). The company made changes by forbidding solitary maintenance of the fuel feeding lines, migrating to a new generation of filters with a fuel pressure warning device and a purge valve, and installing a protection screen to prevent the contact between oil sprays and unprotected high temperature surfaces.

3 METHODOLOGY

The adopted methodology rests on CAST that allows examining the entire socio-technical system, taking into account both separate variables and systemic causal factors (N. Leveson, 2011; N. G. Leveson, Daouk, Dulac, & Marais, 2003). CAST has been applied to analyse individual railway, aviation and maritime accidents (Kim, Nazir, & Øvergård, 2016; Song, Zhong, & Zhong, 2012; Wong, 2004); comparisons also exist with other accident analysis methods (Salmon, Cornelissen, & Trotter, 2012; Underwood & Waterson, 2014).

As STAMP is based on systems and control theories, it treats safety as a dynamic control problem where the role of feedback loops is essential for control. The objective of CAST is essentially to identify scenarios that show where and why safety constraints were inadequately enforced by the safety control structure. CAST uses a generic taxonomy to classify control flows that constitute hazards, which then may lead to accidents (Figure 1). We use the definition of a safety hazard as "a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss" (N. Leveson, 2011).

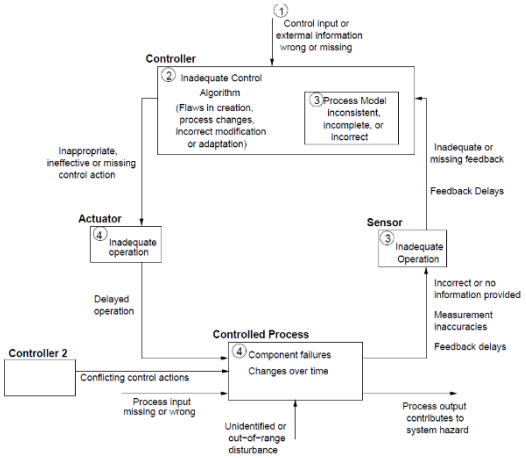

Figure 1: Generic classification of control flaws that lead to hazards (N. Leveson, 2011)

Then, given a particular accident description, the CAST process is as follows:

1. Identify the system(s) and hazard(s) involved in the loss.
2. Identify the system safety constraints and system requirements associated with that hazard.
3. Document a safety control structure in place to control the hazard and enforce the safety constraints.
4. Determine the proximate events leading to the loss.
5. Analyse the loss at the physical system level. Identify the contribution of hazard control flows to the loss.
6. Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level.
7. Examine overall coordination and communication contributors to the loss.
8. Determine the dynamics and changes in the system and the system control structure relating to the loss and any weakening of the safety control over time.
9. Generate recommendations.

The first two steps serve the understanding of physical hazards (controlled hazardous processes) and safety constraints (engineering and/or management) put in place to control them. A hierarchical safety control structure is then built upon this, so these constraints can be effectively enforced. The safety control structure (step 3) also outlines the system under consideration. It defines the system boundaries that enclose the system elements considered for analysis. The purpose of a safety control structure is to control hazards by enforcing safety constraints. This structure includes the roles and responsibilities of each component (subsystem) in the structure as well as the controls provided or created to execute their responsibilities and the relevant feedback provided to them to help them do this (N. Leveson, 2011). The role of each component in the safety control structure is described as follows:

- Safety requirements and constraints to be controlled/enforced
- Means of controls/enforcement
- Context
  - Roles and responsibilities
  - Environmental and behaviour-shaping factors
- Dysfunctional interactions, failures, and flawed decisions leading to erroneous control actions
- Reasons for the flawed control actions and dysfunctional interactions (as shown in Figure 1).

4 ANALYSIS

4.1 System involved in the incident

The purpose of a ship is to transport goods and people in the most cost efficient way, subject to schedule, safety, environmental and other requirements. A general safety requirement implies that risk to health and safety of people has to be maintained below some intolerable level and has to be further reduced as low as practicable. To this end, a safety control system has been established to control a number of safety hazards (risks), with a fire being one of them. In the Le Boreal incident, the high-level safety control system comprised the ship itself (Le Boreal), shipping company (Compagnie du Ponant), shipyard (Fincantieri), maritime administration (Registre International Français - RIF, Centres de Sécurité des Navires - CSN), class society (Bureau Veritas - BV), and International Maritime Organisation (IMO), as shown in Figure 2.

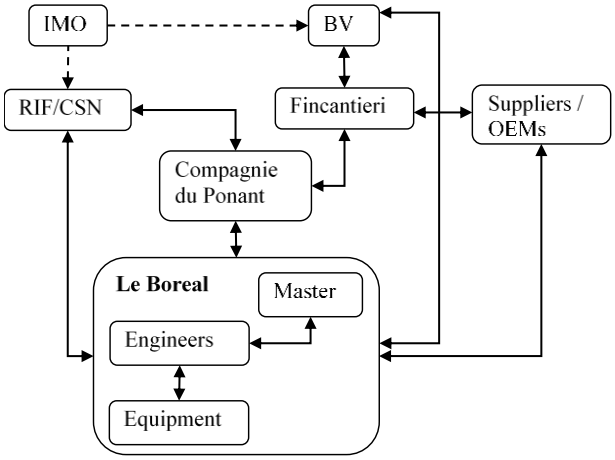

Figure 2: Parties involved in safety control (high-level representation)

Each component in the system has its specific function (responsibilities) in safety control (Kristiansen, 2005). Thus, IMO issues safety standards for construction, equipment and operation of ships, receives feedback from member states, inter-governmental organisations, and non-governmental organisations. The IMO has no power to enforce international safety regulations (hence the dashed lines in Figure 2), as this task is passed to flag states. The class society controls technical standards on behalf of the flag state and insurers during design, construction and operation. It also carries out regular surveys and inspections to ensure continuing compliance with the standards. Acting on behalf of the state, a maritime administration enforces international safety regulations by issuing safety certificates (STCW, ISM Code, MLC etc.)[3], carrying out flag state inspection of operational vessels etc. This includes, inter alia, the control of minimal safe manning, qualification of seafarers, hours of work, medical certificates etc. The shipyard builds, integrates, tests and repairs the vessel and equipment to the owner's specification and safety rules and regulations, and develops operational and maintenance requirements with respect to safety. The corresponding input from original equipment manufacturers (OEMs) and suppliers with whom the shipyard closely cooperates (e.g., Wärtsilä supplies diesel generators), is essential here. This information becomes an integral part of onboard operational manuals and the safety management system. The equipment have to be type approved by classification societies and to comply with safety regulations such as Machinery Directive (2006/42/EC), SOLAS, and others. The shipping company is responsible for crewing, operation and maintenance of the vessel on behalf of the ship owner. It develops and maintains a safety management system (SMS) according to the ISM Code, which specifies responsibility, authority and interrelation of key personnel. The company is responsible to ensure adequate resources, including their training and selection, and shore-based support. The ship is under command of the master who has superior responsibility for safe ship operation and implementation of the SMS onboard. Engineers are responsible for safe operation and maintenance of equipment.

As Figure 2 indicates, there are two-way interactions in safety control, involving control actions and feedback. As explained in Section 3 and to be discussed below, dysfunctions in these interactions (e.g., wrong control actions, untimely feedback) constituted the causal factors of the Le Boreal incident.

4.2 Hazards and system safety requirements and constraints

One of the high-level hazards that was not properly controlled in the incident could be described as: *Routine maintenance actions (or the lack thereof) led (immediately or later) to uncontrolled release of hazardous energy (e.g., high temperature surfaces above >220℃, combustible oil mist in the atmosphere).*

The corresponding generic safety requirements (SR) would be necessary to prevent such a situation and effectively mitigate its consequences, should it nevertheless occur (as per six functions of defences by (Reason, 1993)):

- Protection (SR1): Barriers shall be provided between the hazards and the potential victims under normal operating conditions.
- Detection (SR2): The occurrence of an off-normal condition, an unsafe act or the presence of hazardous substances shall be timely detected.
- Warning (SR3): The presence of and the nature of the hazard shall be signalled to those likely to be exposed to its dangers.
- Recovery (SR4): The system shall be restored to a safe state as quickly as possible.
- Containment (SR5): The spread of the hazard in the event of a failure in any or all of the prior to defensive function shall be restricted.

[3] The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), International Safety Management Code (ISM Code), Maritime Labour Convention (MCL).

- Escape (SR6): The safe evacuation of all potential victims after an accident shall be ensured.

With respect to prevention in particular, additional safety requirements can be added as follows (as per three types of barriers by (N. G. Leveson, 1995)):

- Lockout (SR7): A dangerous event shall be prevented from occurring, or something or someone shall be prevented from entering a dangerous area or state.
- Lockin (SR8): A safe system state or condition shall be maintained or preserved.
- Interlock (SR9): A correct sequencing of actions/events shall be enforced or events (of which simultaneous occurrence is hazardous) shall be isolated in time or by physical barriers.

In the Le Boreal incident, some of these safety requirements were violated:

- SR1: The hotel officer (HO) was not protected from the explosion in his vicinity (the result of the contact between the oil spray and unprotected high temperature surface).
- SR7, SR2, SR3: The HO was not prevented from undertaking the replacement of the fuel filter which was in use and hence under pressure. The hazardous action by the HO was not detected and there was no warning about the imminent danger.
- SR8: A safe operating condition of the DG was not preserved.
- SR9: The hotel officer was not instructed/reminded to follow a safe sequence of maintenance actions (e.g., by an assistant engineer) and/or there was no automatic interlock mechanism that would shut down the DG or fuel supply.
- SR2, SR3: The inadequate thermal insulation of the turbo-blower exhaust elbow had not been timely detected and consequently no warning about the unprotected heat source was given.

An accident cause is the presence of dysfunctional interactions in the safety control of the system, the interactions that led to the violation of the safety constraints (N. Leveson, 2011). Hence, the answers as to why the above safety requirements were not enforced or adequately controlled lie in the safety control system that appeared to be dysfunctional. The entire safety control structure has to be analysed, looking for dysfunctional interactions between its components (subsystems), along with an explanation

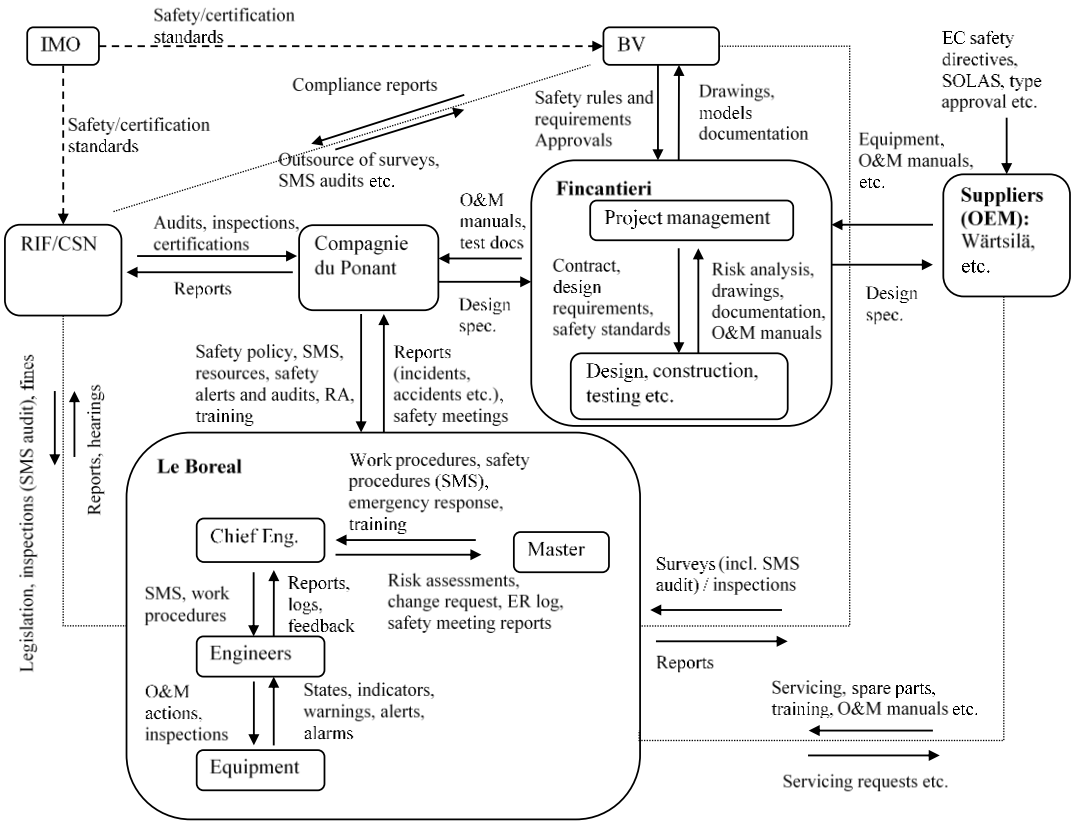

Figure 3: Safety control structure (shown information flows are not exhaustive)

as to how they could give rise to direct and contributing events that preceded the incident.

4.3 Safety control structure

A high-level safety control structure (SCS) was earlier shown in Figure 2, but more detailed one is necessary for the incident analysis in the following sections (Figure 3). The safety responsibilities of the actors involved in safety control are explained in Section 4.1, with the exception of the Chief Engineer (CE) who is included in the more detailed version in Figure 3. The CE is responsible, inter alia, for all operations and maintenance of machinery equipment, as well as for safety of subordinate engineers. He specifically ensures compliance with the rules and regulations and internal safety management system (SMS), carries out frequent inspections of equipment, issues standing orders for each crew member under his command, in accordance with the routine maintenance schedule as prescribed by equipment manufactures.

4.4 Chain of proximate events

The chain of proximate events is described in Table 1.

4.5 Analysis of the physical process

On the level of the physical processes, the dysfunctional interaction between the engineers (the hotel officer / HO and engineering officer / EO) and the equipment (diesel generators, fuel filters, exhaust piping) was the direct cause of the incident. In particular, the control actions of the hazardous equipment (i.e., the maintenance of the duplex fuel filter) was inadequate. The reason why the HO made this decision was related to the fact that there were no adequate feedback and prevention mechanisms in place to inform the right decision (see the violation of safety constraints SR7, SR2, SR3, and SR9 in Section 4.2). The absence of timely and accurate feedback led to an inconsistent mental (process) model, i.e. the wrong understanding about the system state (Figure 1). Hence, the first question is why the feedback and prevention mechanisms were not in place? Such mechanisms could be engineering (e.g., a coding system preventing access to the nuts of the cover of the filter in operation, an interlock, visual/audio warning) or organisational (e.g., an assistant engineer). The investigation report indicates that the HO carried out the maintenance without waiting for a mechanic rating coming in the morning. It would be reasonable to assume—and there is contradiction in the report—that the HO followed the safety maintenance procedures by taking this initiative.

Another reason for the wrong control actions could be related to the flaws in the control algorithm (Figure 1), i.e. the understanding of safe maintenance procedures or responsibilities. Hence, the second question is why the engineer might not be as familiar with the safe maintenance procedures or his responsibilities as he should be? Did he receive adequate training?

The explosion would not have happened had the surface of the turbo-blower exhaust elbow been properly thermo-insulated. The third question is why the heat source was not timely detected and warned about? That is, why the feedback about the hazard was missing? Alternatively, why the adequate detection (visual or automatic), assessment and action mechanism was not in place? Did automatic detection fail? Where there objective or/and subjective factors that made the detection difficult (impossible)? Did the engineers receive necessary training to detect such hazards in given circumstances?

Although other safety constraints were also violated (see Section 4.2), we will address them indirectly through our analysis of the above questions only. Note, our adopted line of thought assumes the engineer acted according the best of his knowledge, training and information available at the time. As long as the information about the controlled process state is accurate and training is right, no unsafe action can be expected (N. Leveson, 2011). This contrasts with the conventional approach where his actions would typically be considered as erroneous, with the identified human error being attributed as the key cause and, often would result in the end of the accident analysis. In the modern thinking the human error is not the end or outcome, but is the start of accident analysis (Dekker, 2014). Human errors are not causes but symptoms of deeper issues in the system. Hence, the analysis has to involve the higher levels of safety control to understand the factors that gave rise to unsafe decisions by the engineers working in the immediate contact with the hazardous processes (at the sharp end) they control.

4.6 Analysis of higher levels of safety control

Moving up the levels of the safety control structure, we further determine how and why each successive higher level allowed or contributed to the inadequate control at the physical process level. We use the earlier formulated questions to guide the analysis.

The Chief Engineer (CE) was responsible for controlling safe work procedures in the engine room. That did not happen due to one or several reasons (Figure 1 and Figure 3): inadequate feedback, inconsistent process (mental) model of the controlled system, inadequate skills (unclear responsibilities, incompetence, lack of training), inappropriate control/management actions, or wrong/missing control/input from the top.

Inadequate feedback. The investigation underlined the staffing problem, which had led to the HO working alone, without the benefit of a crosscheck. The report gives no evidence about the awareness of the CE about it, was he aware? If not why? There is also no evidence about the CE awareness about established practice of frequently replacing fuel filters. Was he aware or why not? What was done about it, e.g. were risks assessed?

Inconsistent process (mental) model. The CE's understanding about the O&M practices remains unclear, unless the above questions are answered.

Inadequate skills. The investigation report provides no direct evidence of the CE inadequately exercising his responsibilities, nor is there evidence of any factors that would undermine his actions. However, the presence of unprotected high temperature surfaces points to an inadequate enforcement of the SMS, i.e. insufficient control of safe work practices. Given the unsafe actions by the engineer, it remains unclear whether the HO was completely familiar with the safe maintenance procedures and had received adequate training. Did the CE take actions to make sure it was the case? Or, if the CE felt the training was inadequate, did he promulgate the training issue to the Captain and the Company? Did a tracking system to monitor training exist? However, there is no basis to assume that had the CE been aware of the maintenance risks, the problem would be communicated up the management system. Was it communicated but not addressed yet? There is no evidence about this in the report. Was the CE unaware of the maintenance risks? If so, that could be related to the lack of skills in risk assessment or deficiencies in the methods used and practiced, leading to complacency as a result. So, did the SMS provide an adequate means of assessing risks? Were adequate resources available for this purpose? Who was responsible to provide such resources?

Flawed supra-control/input. The CE reports to the Master. There is no evidence in the report whether the staffing problem reached the top of the Company and was not timely addressed because of other priorities, or complacency. However, a question could be asked if that had been the case? If it had, this would point out to flaws in safety control on the part of Master/Company. The fact that the risky maintenance was carried out, indicates flaws in the SMS and insufficient training of CE and engineers on safe work procedures, SMS, and risk assessment. That is, the safety control on the part of Company could be deficient. However, whether the Company was receiving adequate and timely feedback about risks onboard, i.e. feedback on the SMS, resources etc. remains unknown from the investigation report. The understanding of this would shed light on how and why the safety control by the Master/Company was deficient. In order to move lessons up and down though the control structure a safety information system must be part of the SMS.

Moving up the levels, the next safety controller is the Ship/Master and Company. Further to the investigation conclusions and the above discussion in this section, the Company did potentially provide inadequate safety control due to one or several causes discussed as follows.

Inadequate feedback. As indicated above, there is no clear evidence in the report about the adequacy of feedback from the ship management (CE and Master) to the Company. Either scenario is possible. First, the Company was aware about the staffing and other problems, but had not addressed them in time, or second, the Company was unaware about the problems, because the ship management had not identified them as risks. The former case points to the potential conflict between safety and other objectives (e.g., commercial) at the Company, whereas the latter points to the insufficient risk assessment skills of onboard personnel or deficiencies in the SMS.

Inconsistent process (mental) model. The Company's understanding about the organisational risks remains unclear, unless the above questions are answered. However, it is pretty certain there was limited awareness about design related hazards, design limitations or safety barriers (defences). The engine room was missing a number of them such as a coding system preventing access to the nuts of the cover of the filter in operation, an interlock to automatically shut down the DG or fuel line, a visual/audio warning about the pressurised fuel filter, and automatic detection of heat sources and alarms. It is reasonable to assume that the Company would have captured these design limitations in the SMS, had it known about the risks associated. So why did the Company not know about these design

limitations? A possible answer is that they were not adequately communicated by the shipyard or design agent (discussed later).

Inadequate skills/expertise shortage. As highlighted so far, Le Boreal likely operated a SMS with a number of dormant hazards (violated safety requirements). Some of them were design related, while others were operational. Nevertheless, the Company could potentially identify the hazards (e.g., scenarios of when heat sources are undetected/remain present for a period of time, maintenance of pressurised fuel lines are carried out, etc.) by a thorough risk assessment and modifying the SMS accordingly. So, was the assessment carried out? What methods/resources were used? Were those scenarios identified? Why were they not acted upon? Were they assumed to be improbable? These questions are critical to assess the robustness of the safety management systems in the Company fleet. With this in mind, it can be said that this incident was waiting to happen. It would not be surprising to learn that similar unsafe maintenance actions had happened before on this or a sister ship, leading perhaps to unreported near misses. Was this considered during the investigation?

Flawed supra-control/input. The Ship and the Company were controlled by the marine administration and the class society through inspections, surveys, audits and other measures. There is no direct evidence in the report of any flaws in this safety control. However, had the adequacy of manning levels in the engine room ever been questioned by the administration or class? If it had not, then it may have been a potential oversight. If it had been, then why had the Company not been required to act to resolve the issue? These and other questions need to be answered to understand the role of the regulators.

The shipyard and OEMs represent the next subsystems that played a key role in this incident. We represent the shipyard subsystem in terms of three interacting components: project management, design, and construction (Figure 3). The project management (PM) is generally responsible for delivery of a ship design, which is developed by design, testing and other departments. The PM controls design requirements, safety standards and expectations (ship owner's) through specific control and feedback mechanisms shown in Figure 3. The shipyard also acts as an integrator of specialised equipment such as diesel generators and their systems, which are delivered by their manufacturers. The OEM of diesel generators was supposed to comply, inter alia, with Machinery Directive (2006/42/EC), which contains essential health and safety requirements for machinery. The directive requires from the manufacturer (or his representative) to carry out risk assessment on the machinery to check if safety requirements are met. Limits and hazards of the machinery must be determined, including during its intended use and any reasonably foreseeable misuse thereof. It seems the required risk assessment overlooked the Le Boreal scenario and was not identified during the subsequent integration by the shipyard.

Inadequate feedback. The shipyard receives feedback from the class society in terms of approvals and certifications, and potentially from the Company on the O&M aspects. As discussed earlier, there were several design related hazards which were either inadequately communicated to the Company (discussed later) or the risk assessment conducted did not adequately consider human factor aspects, i.e. leaving hazards that could be released during maintenance. Nevertheless, the ship design and O&M manuals were approved, complying with design rules and other requirements. This raises the issue of why the design was approved with these safety hazards? Were these hazards identified during the approval process? Did the class society assume they would be dealt with in the SMS? Did the class communicate this information to the Company? These questions should have been raised during the investigation.

One design decision should be investigated related to having the MDO and HFO share the same fuel treatment systems. The accident report highlights that when the switch between HFO and MDO occurs ,the duplex filters had to be replaced every few hours, instead of the manufacturer's recommendation of every 1000 hours. The need to frequently change filters appears to be related to the shared fuel oil processing system (purifiers, duplex filters and settling tanks). Did anyone question the high usage of fuel filters? Was a design with HFO and MDO segregated considered during the development of the ship design? Since the ship operates in sensitive environments (Arctic and Antarctic) has the Company considered only running on clearer burning light oil or alternative fuels?

Another design decision relates to having all the diesel generators side by side, without any longitudinal bulkhead separating them. The collocation of diesel generators and their associated cabling meant in this case that all power, except for the emergency diesel generator, was lost. The fire burned along the cable runs which had limited

separation. This raises the question of whether alternative engine room arrangements were considered during design, especially considering the mission of the ship was to travel to very remote, high latitude locations? If partial propulsion power had been maintained then the risky total evacuation of the crew and passengers in a high sea state could have potentially been avoided. An alternative could have been to locate a propulsion "emergency"

generator high in the ship powered by a gas turbine.

Inconsistent process (mental) model. The PM may have not known about the hazards due to the absence of feedback from the class society and inputs from design, testing and other departments. The report contains no evidence that was addressed during the investigation.

Inadequate skills/expertise shortage. The design limitations could have not been assessed due to one or several reasons:

- Safety standards/requirements were not obeyed.
- Risk assessment overlooked the hazards.
- Risk assessment ruled out the hazard scenarios from considerations because either their probabilities or consequences were assumed to be negligible, or both.
- There was no risk assessment requirement at all, neither from the ship owner nor from the class society, or it was potentially assumed that the designers would deal with the situation.

Again, there is no information in the report as to whether these or similar questions were addressed.

4.7 Coordination and communication

The analysis in the preceding section shows that a possible reason for the SMS to overlook the design related hazards was the inadequate communication between the shipyard and the Company.

4.8 Dynamics and changes in the system

There was no direct evidence in the report of the organisational drift towards the safety boundaries due to financial difficulties in the company or in the industry in general (Rasmussen, 1997), i.e. changes to operation that could undermine safety. For instance, was the staffing problem in the ER always the case from the beginning? Why the ship was operated on two fuels (HFO / MDO), given that the fuel filters would get clogged with the frequency being significantly higher to the one assumed by the designers? Was the risk of these deviations (changes) from the design intent (if it was so) properly assessed?

5 RESULTS

Table 2 lists the identified dysfunctional interactions after exploring the entire hierarchical safety control (HSC) structure, searching for the answers as to who was responsible for ensuring that the interactions are adequate and why they not happen.

The shaded rows in Table 2 correspond to the interactions that were overlooked in the accident investigation report (discussed in Section 2). In particular, these are three contributing factors and one systemic factor. The CAST analysis pointed to these contributing factors, which involved the Chief Engineer, by taking into account his responsibilities and the functional relationships in the HCS.

The graphical representation of the dysfunctional interactions is shown in Figure 4. The blue lines indicate the interactions identified in the investigation report, whereas the red ones denote the dysfunctional interaction identified through the CAST analysis. It should be noted the performed analysis of the Le Boreal incident could, in principle, have included other elements of the hierarchical control structure, such as the maritime administration and classification society. For instance, why surveys and audits did not recognise the solitary maintenance as hazardous? However, we felt the evidence of the wide causal picture was very weak in this particular case. This cautious approach was applied in in the complete analysis as well. Hence, the CAST analysis was somewhat conservative.

Table 2: Summary of dysfunctional interactions in safety control of the Le Boreal incident

Controller	Controlled	Description	Included?
Engineers	Equipment.	Engineer attempted to switch filters on the wrong generator	Y
Engineers	Equipment	Engineer was not prevented from undertaking unsafe filter change (absence of warning or a coding system on the filter cover)	Y
Engineers	Equipment	Engineer was not informed about poor holding of lagging cover (turbo-blower exhaust elbow) which created exposure to high temperature surface.	Y
Chief Engineer	Engineers	Chief Engineer did not made sure the thermal insulation of turbo-blower exhaust elbow was properly maintained. Did not follow SMS.	N
Chief Engineer	Engineers	Chief Engineer did not made sure that the maintenance manual of fuel filters was strictly followed.	N
Ship management company	Ship	Not robust and vague safety procedures with respect to routine maintenance. Deficient SMS.	P
Ship management company	Ship	Risk due to solitary undertaking of maintenance at night was not assessed and addressed in SMS.	Y
Ship management company	Ship	Master did not well communicate the understaffing (a rating was needed during night watches in fuel treatment compartment)	Y
Project management (ship builder / supplier)	Design, construction, testing	Coding system, interlock, or warning mechanism was not provided on the fuel filter covers to prevent maintenance errors.	Y
Project management (ship builder / supplier)	Design, construction, testing	Safety requirements, analysis methods were inadequate, overlooking the materialised maintenance hazard.	N
Ship builder / supplier	Ship management company	No communication of design limitation / unprotected hazard with respect to maintenance of diesel generators. This was therefore not addressed in the SMS.	N

When it comes to recommendations with respect to these systemic causal factors, safety improvements should target the communication interfaces on the system level, i.e. between the actors involved in safety control. As demonstrated in (Rasmussen, 1997), the absence of global, system level coordination and communication, even though locally the performance of each actor is optimal, has been the underlying causal factor behind maritime and other accidents. The understanding of how the improvements can be achieved on the system level requires further research and hence is beyond this paper. However, the following initiatives on the organisational and company level can contribute to the global change:

- Compliance processes towards Machinery Directive (2006/42/EC) and other regulations should be probed. More research is necessary to better understand the problem.
- The Company makes sure that all design assumptions and limitations (as potential hazards), as well as any deviations during manufacturing, are well documented and communicated to the upper management level of the Company. This should be achievable for newbuilding projects and for some ships in the fleet.

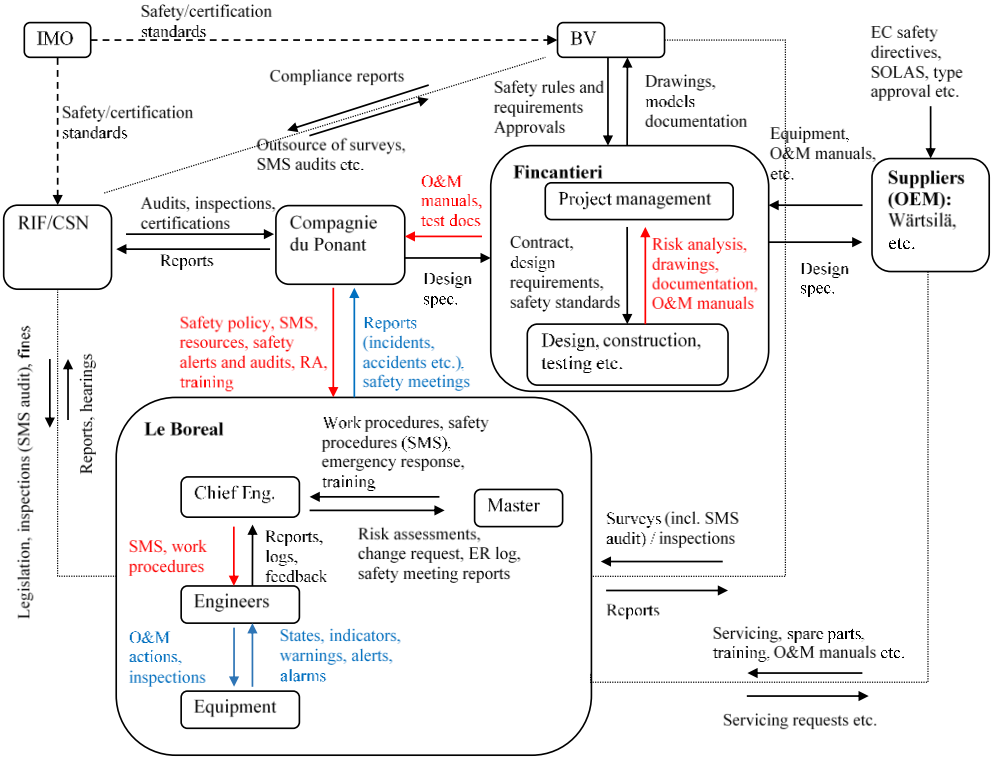

Figure 4: Highlighted dysfunctional interactions that led to Le Boreal incident

- The development of the SMS considers realistic circumstances such as the natural gradient towards least effort by crew, the ubiquitous push for cost effectiveness, and natural work variability (Hollnagel, 2016; Rasmussen, 1997).
- Clear tracking of safety training, safety meetings and the use of active risk management at the user (ship) level that is summarised and reported periodically to the shore management team.
- New hazard analysis methods should be considered in ship design and subsequent development of the SMS. For instance, Systems Theoretic Process Analysis (STPA) is based on STAMP (N. Leveson, 2011) and shows very promising results for identifying hazards in modern designs operated in complex socio-technical systems.
- It is incumbent on the Flag State, regulatory bodies and the IMO to ensure a comprehensive assessment of the accident is completed. This is especially critical since the accident analysis process serves as the engine to drive changes to design, regulations and operational standards. If the accident assessment is flawed or incomplete, then the positive changes needed will not be recognized and created.

6 CONSLUSIONS

The paper has applied the systems approach to analyse the fire incident in the engine room of the cruise ship Le Boreal in 2015. The applied CAST process systemically guided the analysis throughout the entire socio-technical system involved in safety control, analysing individual interactions and their role in the incident. This allowed the process to go beyond the findings of the accident investigation, revealing systemic causal factors, as well as potentially additional direct and contributing factors. The analysis results yielded a wide array of options for remedial actions, which should address: (1) the potentially inadequate communication between the Company and the shipyard and OEMs, (2) inadequate hazard analysis (risk assessment) methods and processes used by the Company, when developing the SMS, the shipyard, and OEMs when assessing design assumptions and limitations. Additionally, the causal role of the regulators could also be significant to the incident. We have discussed how these systemic factors could insidiously give rise to the deficient SMS with the incident waiting to happen.

As the identified causal factors and remedial actions are systemic, they are not limited to the

analysed incident only. These are underlying causes or conditions in overall safety control and could (can) undermine safety of many ships. We believe that the results of our study provide a valuable input to proactive safety management for the ship, company, regulators and governmental organisations. With the knowledge gained, resources committed to risk management can be better allocated, reducing associated costs and improving on business objectives.

7 REFERENCES

Angel, S. (2012). *The Titanic. 'Everything was against us'*.

BEAmer. (2016). Marine safety investigation report. Fire in the engine compartment on board the expedition-cruiser liner Le Boreal on 18 November 2015, off Falkland Islands. In: Bureau d'enquêtes sur les événements de mer (BEAmer).

Butler, D.A. (1998). Unsinkable: Story of RMS Titanic. Mechanicsburg. In: PA: Stackpole Books.

Dekker, S. (2014). *The field guide to understanding'human error'*: Ashgate Publishing, Ltd.

Fitzgibbon, S. (2012). *Titanic: History in an Hour*: HarperPress

Hollnagel, E. (2016). *Barriers and accident prevention*: Routledge.

Johnson, W.G. (1980). *MORT safety assurance systems* (Vol. 4): Marcel Dekker Inc.

Kim, T.-e., Nazir, S., & Øvergård, K.I. (2016). A STAMP-based causal analysis of the Korean Sewol ferry accident. *Safety Science*, *83*(Supplement C), 93-101.

Kristiansen, S. (2005). Maritime transportation: safety management and risk analysis.

Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*: MIT press.

Leveson, N.G. (1995). Safeware. *System Safety and Computers. Addison Wesley*.

Leveson, N.G., Daouk, M., Dulac, N., & Marais, K. (2003). Applying STAMP in accident analysis.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*, *27*(2), 183-213.

Reason, J. (1993). The identification of latent organizational failures in complex systems. In *Verification and validation of complex systems: Human factors issues* (pp. 223-237): Springer.

Salmon, P.M., Cornelissen, M., & Trotter, M.J. (2012). Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Safety Science*, *50*(4), 1158-1170.

Song, T., Zhong, D., & Zhong, H. (2012). A STAMP analysis on the China-Yongwen railway accident. *Computer safety, reliability, and security*, 376-387.

Taplin, S. (2017). Titanic: The New Evidence. In. Channel 4 Viewing Portal.

Underwood, P., & Waterson, P. (2014). 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*, *68*, 75-94.

Wong, B. (2004). *A STAMP model of the Überlingen aircraft collision accident.* Massachusetts Institute of Technology.