

Towards an explanation of why onboard fires happen: The Case of an Engine Room Fire on the Cruise Ship “Le Boreal”

Romanas Puisa, Stuart Williams, and Dracos Vassalos

Abstract

As the cruise ship industry enjoys continuous growth and penetration into new markets, good safety records must be maintained to achieve business objectives. Unfortunately, serious incidents and accidents reoccur on modern cruise ships and hence a better understanding of why this continues to happen is needed. This paper contributes towards a better understanding of underlying causal factors behind onboard fires, focusing on consequential engine room fires in particular. By analysing a recent fire incident on an almost new cruise ship built to the latest standards, we reveal potential deficiencies in maritime safety control and suggest how they can be rectified. The incident analysis was guided by systemic method CAST, which enables to explore a complex socio-technical system responsible for safety control. The analysis provides a different, more comprehensive explanation of, and response to, the incident from that in the official accident investigation report. Given the systemic nature of suggested causal scenarios, they are capable to explain and preclude other incidents. From a practical point of view, the findings would allow developing and maintaining robust safety management systems, which are currently required onboard.

Keywords: *Accident analysis; CAST; STAMP; fire; engine room; maritime; cruise*

1 Introduction

1.1 Problem statement

The cruise ship industry is forecast to achieve 5% growth in 2018 and reach 27.2 million passenger worldwide [1]. This will involve the introduction of new ships as well as the continuous expansion into exotic markets such as Arctic and Antarctica. Alongside societal concerns about the impact on environmental [2], safe operation in these hostile areas has always attracted special attention. With the limited number of ships and Search and Rescue (SAR) stations around, timely assistance in case of a fire, or other incident, is unlikely. Evacuation is also highly undesirable and might turn out to be as equally risky as remaining onboard. Particularly consequential have been fires in engine rooms (ERs). An ER fire can disable the entire vessel by causing, for instance, a power loss (blackout), which might lead to inhabitability, collision, grounding, and other dangers. Some of the recent incidents with cruise ships include *Zenith* in 2013, *Carnival Liberty and Triumph*, *Splendour of the Seas*, and *Le Boreal* in 2015. More than a decade ago, a study by Det Norske Veritas (DNV) reported that two thirds of ship fires have started in the engine room, with more than half of them resulting from the contact between combustible oil mist and high temperature surfaces [3]. Little has changed since then, as this very scenario continues to be reported as the immediate fire cause [4]; all the above mentioned incidents. So why has this decades-long problem proved so intractable?

We argue that despite the recommended scope of marine safety investigations, the reconstruction of causal factors is simply incomplete. The International Maritime Organization’s (IMO’s) causality investigation code requires “going far beyond the immediate evidence and looking for underlying conditions, which may be remote from the site of the marine casualty or maritime incident, and which may cause other future marine casualties and marine incidents. Marine safety investigations should, therefore, be seen as a means of identifying not only immediate causal factors but also failures that may be present in the whole chain of responsibility.” [5, p. 15]. Thus, the scope of accident analysis is supposed to explain both *what* happened (e.g., an engineer made maintenance errors that led to the release of flammable material) and *why* this was allowed to happen (e.g., inadequate training). The first question is normally answered by revealing *direct* and *contributing* causal factors such as human errors, inadequate management or poor preventative design, whereas

the second question requires an analysis of *systemic* factors, such as dysfunctional interactions at the system level [6, 7, p. 28].

However, there is a difference between the expected and actual practice of accident analysis. Multiple reviews of accident investigation reports on fires in engine rooms show that the investigations were limited to the context in which proximate events occurred, with a limited focus on wider organisational issues [8-10]. The investigations were specifically biased towards technical failures as preconditions for unsafe acts, and proximate, directly-linkable organisational influences as contributing, latent factors. Some systemic causal factors were also tabulated, however, while such a list may be useful for frequency analysis to identify the 'most frequent cause', it is not particularly suitable for a coherent explanation of flawed interactions. Hence, no determination of "failures that may be present in the whole chain of responsibility." [5, p. 15] is possible. This linear thinking inhibits the accident analysis in going beyond failures at the 'sharp end' [11], failing to sufficiently explain the non-linear interactions within the socio-technical context of systems such as large cruise ships [12]. The bias towards proximate events is also introduced in the final stages of accident investigation, namely during the development of recommendations. Recommendations for remedial actions are often tailored to the existing capacity—of the shipping company—to implement them [13], and the fixes in a chain of proximate events would be seen as the simplest ones to put into practice.

The lack of systems thinking in accident analysis is behind this situation, and makes the accident analysis and responses incomplete. Systemic analysis could provide additional insights, e.g. [14, 15], and inform the explanation of accident causation and the right choice of remedial actions [11]. Systems thinking implies a different explanation of accidents, assuming that accidents happen due to uncontrolled performance variability and coincidence, rather than specific failures, and accidents cannot be explained by simplistic cause-effect relations [16, p. 201]. The pertinent safety strategy would then involve the monitoring of performance variability and the build-up of coincidences. The build-up of coincidences can be characterised by the presence of dysfunctional interactions within the system which can be distant in space and time. The interactions would typically have nonlinear effects and, therefore, their immediate impact on system safety, when coincidences of unfavourable events actually occur, is not conspicuous and hardly predictable. These observations introduce additional requirements for safety management, such as the presence of an effective feedback mechanism on both blunt and sharp ends. For example, an engineer/manager receives a timely, system-wide assessment of his/her actions and is able to revoke them if necessary and control the dysfunctional interactions within the entire system [7, p. 31].

In summary, the systems approach assumes that an incident or accident is a clear indicator that a safety control system as a whole is inadequate, and it may need to be redesigned [17, p. 403]. For instance, a new feedback loop may need to be added or requirements for an existing feedback loop may need to be amended. To determine what changes are required, a good understanding must be established as to how the safety control system in question works and which interactions are problematic.

1.2 Contribution

This paper applies a systems approach to a recent fire incident in the engine room (ER) to unravel dysfunctional interactions within the entire system that was responsible for safety control. We specifically reconstruct a serious ER fire on the cruise ship *Le Boreal*, which was en route to Antarctica in 2015. By applying the systems approach, we illuminate dysfunctional interactions that gave rise to direct, contributing and, in particular, systemic causal factors behind the incident. Given that the fleet-side safety control system is sufficiently generic and it is analogous to other control systems in the industry, the revealed flaws are of global reach. To the best of our knowledge, the systems approach has not been applied to this notorious fire scenario where leaked oil mist (or spray) comes into contact with an unprotected high temperature surface (typically above 220°C). Hence, this paper fills this void. The added value of the analysis is comparable to other applications of the systems approach to accident analysis [18-21].

From the methodological point of view, we exemplify another application of the accident analysis method CAST, which is based on the systemic accident model STAMP (Systems-Theoretic Accident Model and Processes) [7, 22]. As the method is relatively new, there is a general interest—especially in the maritime domain—in applications of CAST to various incidents and accidents. This method was selected based on the

fact that CAST would often lead to a deeper and different explanation, typically involving new causal factors to those concluded in investigations [22]. Therefore, we also recorded the degree of dissimilarity, in essence the inquiry gap, between the findings.

1.3 Outline

The remainder of the paper is organised as follows. Section 2 provides a summary of the incident. Section 3 explains the analysis methodology adopted. Section 4 outlines the results. Section 5 provides a general discussion of results along with recommendations. Section 6 outlines limitations of the study, whereas Section 7 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 800 kW. At the time of the incident, all four diesel generators (referred to as DG1, DG2, DG3, and DG4) were online and fed with heavy fuel oil (HFO 380).

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 the French marine casualty investigation board, Bureau d'Enquêtes sur les Événements de Mer (BEAmer), which published its findings 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 [23]¹.

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

11:20pm	- Hotel Officer (HO) begins a patrol in the engine room.
11:30pm	- HO notices that an inlet fuel filter (Bollfilter duplex filter) to DG4 is clogged (indicator is red). - HO senses an odour of exhaust gases. - HO switches the DG4 duplex filter to its clean reserve cartridge, isolating the clogged filter cartridge which is now offline and can be safely replaced. -
11:35pm	- HO ends the patrol and logs findings in the logbook in the Engine Control Room (ECR);
Midnight	- Engineering Officer (EO) starts his shift, HO reports about the intention to replace the clogged filter cartridge and the presence of exhaust gas smell. - EO checks the operation of engine room ventilation. - Both offices suspect exhaust gas leaks from the funnels.
00:10am	- HO goes to the fuel treatment room and enters the DG compartment to replace the clogged filter cartridge.

¹ The accident investigation report can be downloaded from http://www.bea-mer.developpement-durable.gouv.fr/IMG/pdf/BEAMER-FR_LE_BOREAL_2015.pdf

	<ul style="list-style-type: none"> - But instead of approaching the DG4 filter, whose clogged cartridge was previously isolated and is now offline, HO unscrews the cover of the DG3 filter, which is not clogged and online (pressurised). Fuel duplex filters to DG3 and DG4 are only one meter apart (see Figure 1). - This leads to a spray of pressurised fuel towards DG3 turbo-blower and HO. HO steps back and observes a fireball next to DG3 turbo-blower exhaust elbow. - Without retightening the filter cover, HO rushes to ERC and requests an office of the watch (OOW) to stop DG3 and DG4. OOW also stops the two other generators, due to overload. - The vessel experiences a blackout until a backup DG starts.
00:16am	<ul style="list-style-type: none"> - Fire alarm sounds, BRAVO code is triggered. - HI-FOG system triggered automatically over all four generators and in the fuel treatment room. - Watertight and fireproof doors are shutdown from the bridge.

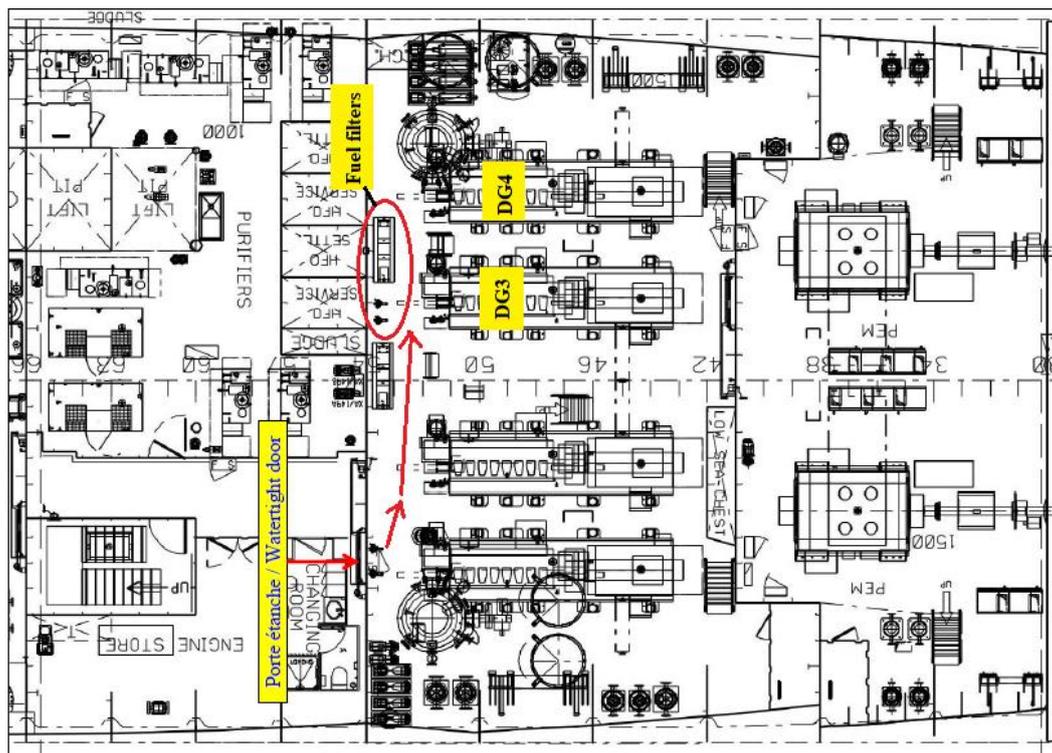


Figure 1: Location of the diesel generators DG3 and DG4, and fuel filters. The arrow indicate the path taken by the hotel office to replace the clogged filter cartage (adopted from [231])

As the paper is focusing on prevention, Table 1 only describes the timeline of events and direct causes before the fire incident is registered. The investigation report also lists the following contributing factors:

- 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.
- 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 the 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 or adjust maintenance actions, 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" [23]. That is, the investigators alluded to the human error. BEAmer recommended that the company considers 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

To achieve the objective of the paper, we use the systemic accident model STAMP [7, 22]. In contrast to other systemic models, STAMP better embodies systems thinking [24] and it is the most frequently cited [25]. The STAMP-based accident analysis follows a series of steps, referred to as Causal Analysis based on STAMP (CAST). CAST allows examining the entire socio-technical system, taking into account both separate causes and systemic causal factors (interactions). CAST has been applied to individual railway, aviation and maritime accidents [26-28]. Comparisons also exist with other accident analysis methods [24, 29]. The key element of CAST is a hierarchical control structure (HCS), which represents a functional model of the safety control system. The HCS developed is explained in Section 3.1, with Section 3.2 addressing the use of it while analysing the accident investigation report.

3.1 Hierarchical safety control structure

The HCS is a functional system model that is composed of feedback control loops. By system we are referring to the complete maritime safety control system, which includes international and state regulators, manufacturers, ship management companies, ships and their crew and equipment, and others. In the Le Boreal incident, the high-level safety control system comprised the ship itself (Le Boreal), shipping company (Compagnie du Ponant), shipyard (Fincantieri), suppliers (e.g., Wärtsilä supplying diesel generators), the maritime administration (Registre International Français (RIF), Centres de Sécurité des Navires (CSN)), class society (Bureau Veritas (BV)), and the International Maritime Organisation (IMO), as shown in Figure 2. An effective HCS will adequately enforce safety constraints on the behaviour of individual system elements (subsystems) and interactions between them, so that the hazards at the sharp-end are controlled. An accident occurs when such safety constraints are enforced inadequately.

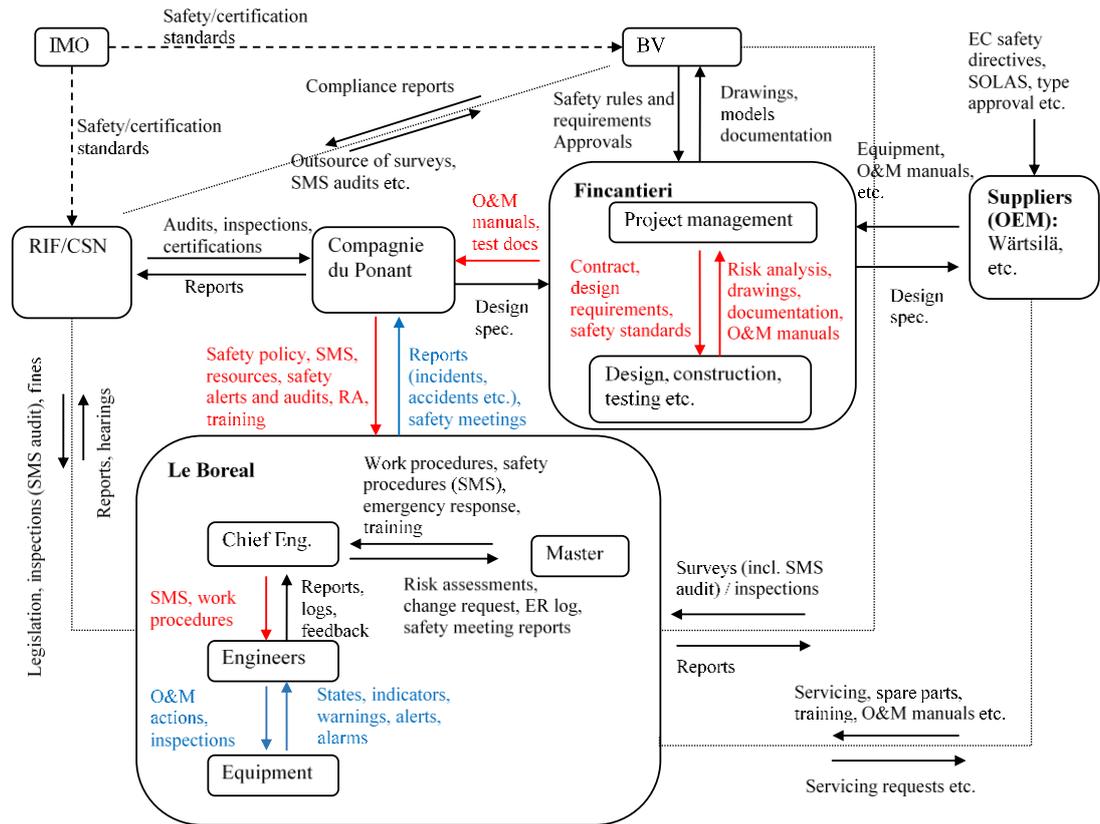


Figure 2: Safety control structure (coloured arrows and text are explained in Section 4)

Each component (subsystem) in the system has its specific functional responsibility in safety control, and this function is implemented through control actions and feedback information on the success of control actions. 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.)², carrying out flag state inspection of operational vessels etc. This includes 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 supplied diesel generators), is essential here. This information becomes an integral part of onboard operational manuals and the safety management system. The equipment has 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 human 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. The Chief Engineer (CE) is responsible for all operations and maintenance of machinery equipment, as well as for safety of subordinate

² The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), International Safety Management Code (ISM Code), Maritime Labour Convention (MLC).

engineers. He specifically ensures compliance with the rules and regulations and the internal SMS, carries out frequent inspections of equipment, and issues standing orders for each crew member under his command in accordance with the routine maintenance schedule as prescribed by equipment manufactures. 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 corresponding feedback. As explained in Section 3 and to be discussed below, dysfunctions in these interactions (e.g., wrong control actions or untimely feedback) constitute the causal factors of the Le Boreal incident.

3.2 Analysis process

The objective is to identify scenarios that show where and why safety constraints were inadequately enforced within the safety control structure. Given a particular accident description, the CAST process follows the steps in Table 2.

Table 2: Generic CAST steps

CAST step	Comments
Identify the system(s) and hazard(s) involved in the loss	Taken from the report.
Identify the system safety constraints and system requirements associated with that hazard.	Defined in Table 3.
Determine the proximate events leading to the loss.	Taken from the report.
Analyse the loss at the physical system level. Identify the contribution of hazard control flows to the loss.	Taken from the report.
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.	Analysing the HCS with the guidance of the STAMP accident model.
Examine overall coordination and communication contribution to the loss.	
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.	
Generate recommendations.	

As Table 2 indicates, the accident investigation report already contained the basic information necessary for the analysis. Further information was inferred while exploring the HCS. Thus, the analysis starts by extracting information from the accident reports about what has happened and what unsafe control actions were issued, and by whom. This information is directly found in a description of proximate events leading to the loss (Table 1). The next steps are focusing on why these unsafe control actions were issued, or why it made sense to issue them in the given context. As the system elements in the HCS are connected through functional causal links of control, feedback and communication channels, one can navigate vertically and horizontally through the control structure, analysing individual elements of the control system. There are two basic causal scenarios behind unsafe control actions:

1. An adequate control action was issued, but it was not correctly executed or executed at all.
2. An inadequate control action was issued or no action was issued when required.

The first scenario requires a look into the control path and the controlled process itself. For instance, it could be that a control action (e.g., inspection) did not reach the controlled process (e.g., fuel lines) because of faults in actuation mechanisms (e.g., inspections are delayed or temporally waived). Equally, the control process could have been made dysfunctional by the influence of out-of-range disturbances (e.g., excessive overload or vibrations). There could have been conflict with other controllers also responsible for the same control process. The second scenario is more complicated, and it requires an examination of the controller itself, which could be a human, organisation, or an automated controller. The adequacy of its process model, or a mental model for humans, the influence of external inputs from supra-controllers or the environment, and the adequacy of feedback about the control process and success of control actions must be determined.

When the control is carried out by people, one of the guiding principles behind the analysis is the assumption that people and organisations act according to their best knowledge and ability, with the tools and information available at the time. That is, as long as the information about controlled processes is accurate, training is right, and tools are appropriate, no unsafe action can be expected [30]. The objective is to understand *why* people did what they did and *why* they could not act differently [31]. The same principle applies to machine controllers, but the questions are *why* designers, and regulators made, or accepted, specific design assumptions which turned out to be wrong in a given situation.

Figure 3 demonstrates how the CAST analysis starts at the level of the physical process and moves up by formulating the questions to be answered at higher levels of the HCS. The process is recursive, producing an analogous diagram for each element of the HCS. Thus, at the physical level, the dysfunctional interaction between the engineer and the equipment (diesel generators, fuel filters, exhaust piping) was the direct cause of the incident. In particular, the control action taken operating hazardous equipment was unsafe. The reason why the engineer made this decision, as concluded in the investigation, was due to the fact that there were no adequate feedback and prevention mechanisms in place to control the right sequence of actions. The absence of timely and accurate feedback led to an inconsistent mental model, i.e. the wrong understanding about the system state. *Hence, the first question is why the feedback and prevention mechanisms were not in place?* This points to designers and equipment manufacturers. The investigation report indicates that the engineer carried out the maintenance without waiting for a mechanic rating coming in the morning. It would be reasonable to assume—and there is no contradiction in the report—that the engineer followed the established practice by taking this initiative. *Hence, the question is why the SMS or management (Chief Engineer) allowed this risky practice?*

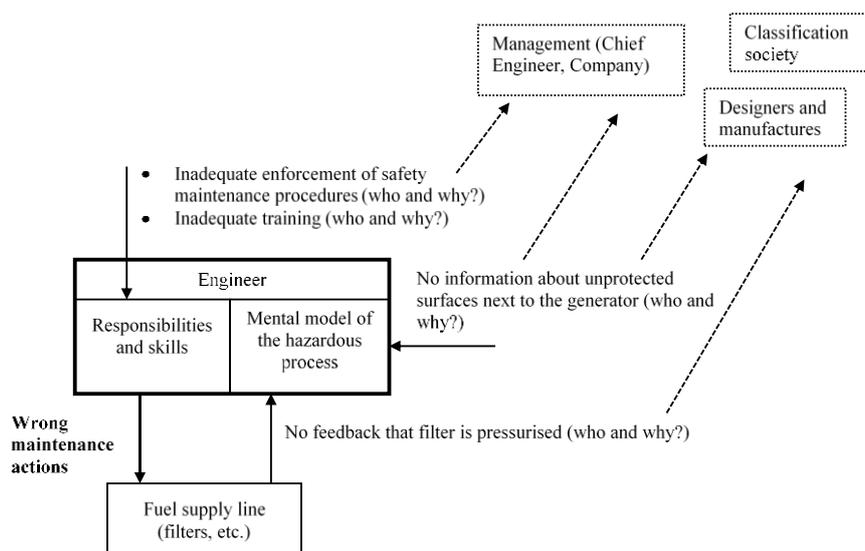


Figure 3: The starting point for the analysis

Alternatively, the engineer may not have understood the safe maintenance procedures or his responsibilities. Hence, the question is why the engineer might not be familiar with the safe maintenance procedures or his responsibilities, 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 question is why the heat source was not timely detected and warned about, i.e. why the feedback about the hazard was missing? Were there objective or/and subjective factors that made the detection difficult? Did the engineers receive necessary training to detect such hazards in given circumstances?

The analysis outcome comprises a set of dysfunctional interactions showing inadequate control, or feedback, or both, between the system elements. The relevancy of explored interactions to the incident, whether these interactions were dysfunctional or not, was determined based on the system-level hazards and corresponding safety requirements and constraints (Table 3). These requirements are explicit and implicit in the international safety management code [32], Machinery Directive, and others. We used the definition of a safety hazards as “a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss” [7]. The safety constraints were decomposed, through system engineering decomposition, into safety constraints on subsystems and individual components. These hazards

Table 3: System-level hazards and constraints

Hazards	Safety requirements and constraints and their decomposition at lower levels (subsystems)
H1. Design process overlooks hazardous scenarios that can materialise during operation and/or maintenance	C1. Safety assessment in design shall be adequate <ul style="list-style-type: none"> • Design rules and standards shall be up to date • Pertinent design rules and standards shall be used and applied correctly • Hazard analysis methods shall be adequate to identify all plausible safety hazards
H2. Manufacturing deviates from the design assumptions	C2. Safety assessment during manufacturing shall be adequate <ul style="list-style-type: none"> • Design assumptions shall be well documented and communicated to manufactures • Communication between designers and manufacturers shall be adequate • Design must be reviewed and validated/tested (e.g., sea trials)
H3. Onboard safety management system overlooks safety hazards or does not address them adequately	C3. Design assumptions and the actual operation shall match (work as imagined vs. work as done) <ul style="list-style-type: none"> • Design assumptions shall be well documented and communicated to the shipping company • SMS shall reflect all design assumptions, including design limitations • The impact of changes shall be reflected in updates to operational procedures C4. SMS shall be verified, validated and constantly updated <ul style="list-style-type: none"> • SMS shall be approved by relevant authorities • Design modifications and operational changes shall be well documented and reflected in SMS • Hazard control measures (engineering and management) shall be kept adequate • New hazards shall be identified and control measures timely implemented • Crew shall be familiar with the ship and its safety procedures at all times • Continuous communication/information exchange between the company and the ship shall be ensured

3.3 Classification of causal factors

The identified dysfunctional interactions show what actually happened immediately and long before the incident. They would act as direct (proximate), contributing, or systemic factors in the accident causation [6]. This classification broadly reflects the intended scope of marine safety investigation [5, p. 15], and it was used to classify dysfunctional interactions according to the categories in Table 4. The table also explains how the classification of causal factors corresponds to the elements of a control loop analysed by CAST; this is also illustrated in Figure 4.

Table 4: Classification of accident causes in three causal categories

Causal factor	Determination	Examples
<p>Direct (D)</p> <p>Subsystem level. Proximate events to the incident within the same subsystem. Corresponds to inadequacies in direct control and controlled processes.</p>	<p>Found in accident analysis</p>	<p>Failures in passive and active safety systems (thermal insulation, leak prevention, condition monitoring, etc.), and in their inspection and maintenance actions.</p>
<p>Contributing / underlying (C)</p> <p>Inter-subsystem level. Within the same subsystem or contiguous subsystems. Corresponds to inadequacies in feedback, controller or/and input to the controller.</p>		<p>Dysfunctional safety management system, unclear communication and responsibilities and roles, poor crew training and supervision, inadequate manning, irregular fire drills, neglect of good practices.</p>
<p>Systemic (S)</p> <p>System level. Between subsystems. Have a nonlinear effect on contributing and proximate events. Corresponds to flaws in control or/and feedback within the wider system.</p>	<p>Inferred during accident analysis</p>	<p>Weak safety culture, ineffective inter-organisational links, deficient safety assessment, flawed standards, practices and regulatory oversight.</p>

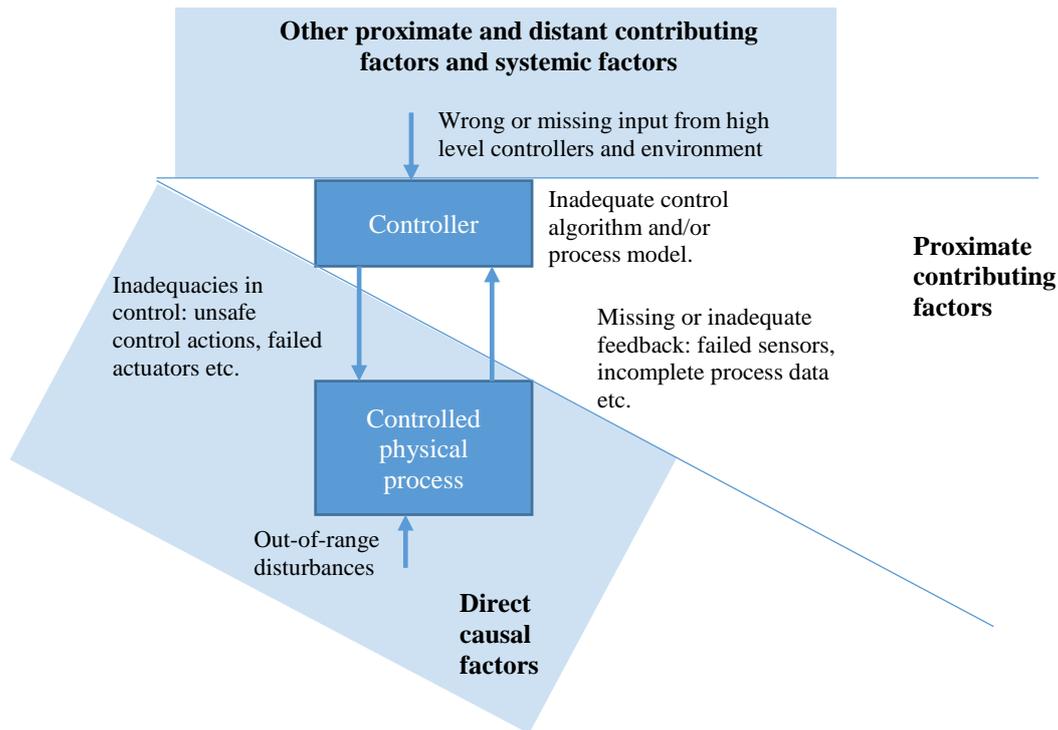


Figure 4: Linkage between the reported causal factors (or simply causes) in accident investigation and control loop elements

3.4 Criteria for gap analysis

Gap analysis involved the identification of the gap between the incident causes reported in the investigation and revealed during the CAST analysis. Specifically, we aimed to establish whether an observed or inferred dysfunctional interaction was also captured in the official accident investigation. Sometimes, the same flawed interaction would be mentioned in investigation conclusions and recommendations and we would hence classify it as *included (Y)*. If, however, the report contained an explicit narrative of some causal factors, but not reflect them in conclusions and recommendations, we would classify such a causal effect as *partly included (P)*. The rest of identified dysfunctional interactions were classified as *not included (N)*.

4 Results

4.1 Summary

Table 5 lists dysfunctional interactions identified across the entire HCS, while searching for the answers as to who was responsible for ensuring the enforcement of the safety constraints (Table 3) and why they were not adequately enforced.

Table 5: Summary of dysfunctional interactions in safety control of the Le Boreal incident (symbols and abbreviations are explained in Table 4 and Section 3.4)

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

4.2 Gap analysis

The shaded rows in 4 correspond to the interactions that were overlooked in the accident investigation report (explained in Section 4.3). There are three contributing factors and three systemic factors. One of the contributing factors was only partly addressed in the investigation. The systemic causal factors, which violated system safety constraints C1 and C3 (Table 3), were inferred by exploring the functional links to the designers / manufacturers. The graphical representation of the dysfunctional interactions is shown in Figure 2. The blue lines indicate the interactions identified in the investigation report, whereas the red ones denote the additional dysfunctional interactions identified through the CAST analysis. The following section provides the rationale of why these extra interactions were added.

4.3 Unanswered questions

Figure 2 highlights the interactions (in red) that were discounted during the accident investigation. The discussion below provides the rationale as to why these interactions were considered dysfunctional during the CAST analysis.

Chief Engineer (CE) was responsible for controlling safe work procedures in the engine room. That did not happen for several reasons: 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 led to the Hotel Officer (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's awareness about established practice of frequently replacing fuel filters. Was he aware or why not? What was done about it, e.g. were hazards 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 HO, it remains unclear whether he was completely familiar with the safe maintenance procedures and had received adequate training. Did the CE take actions to make sure that was the case? Or, if the CE felt the training was inadequate, did he raise 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 hazards, the problem would not 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 hazards? If so, that could be related to the lack of skills in hazard assessment or deficiencies in the methods used and practiced, leading to complacency as a result. Did the SMS provide an adequate means of assessing hazards? Were adequate resources available for this purpose? Who was responsible to provide such resources?
- *Flawed 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 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 hazard assessment. It appears that 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.

Further to the investigation conclusions, the Company potentially provided 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. Firstly, the Company was aware about the staffing and other problems, but had not addressed them in time. Secondly, the Company was unaware about the problems, because the ship management had not identified them as hazards. 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 hazards remains unclear, unless the above questions are answered. However, it appears there was limited awareness about design related hazards, design limitations or safety barriers (defences). The engine room was missing a number of barriers 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 an 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 hazards 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 the 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, such as scenarios of when heat sources are undetected or remain present for a period of time and when maintenance of pressurised fuel lines are carried out, by a thorough safety assessment and modifying the SMS accordingly. So, was a safety assessment carried out? What methods and 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 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. 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. 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 [33], which contains essential health and safety requirements for machinery. The directive requires that the manufacturer (or his representative) carry out a 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 where the role of the human element was more visible. This design limitation may not been assessed due to one of the following:

- Safety standards/requirements were not obeyed.
- Risk assessment overlooked the hazard.
- Risk assessment ruled out the hazard scenario from considerations because either its probability or consequence was assumed to be negligible, or both.

- There was no risk assessment requirement at all for the shipyard, neither from the ship owner nor from the class society, or it was assumed that the designers would deal with the situation anyway.

The shipyard and OEM receive feedback from the class society in terms of approvals and certifications, and potentially from the Company on the Operation and Maintenance (O&M) aspects. Was the feedback adequate? As discussed earlier, there were several design related hazards which were either inadequately communicated to the Company or the risk assessment conducted, as required by Machinery Directive, did not adequately consider human factor aspects and omitted the maintenance hazard, as pointed out before. Nevertheless, the ship design, equipment and O&M manuals were approved, complying with design rules and other requirements. This raises the question 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.

Another design decision was to have all the diesel generators side by side, without any longitudinal, fire resistant bulkhead separating them. The collocation of diesel generators and their associated cabling meant that all power, except for the emergency diesel generator, was lost. The fire burned along the cable runs which had limited separation. The decision appears to be wrong in hindsight, but it was sensible at the time, given the safety requirements when designed. Only later a new requirement, known as “Safe Return to Port” MSC.216 (82), came into force. The regulation enforces redundancy for safety critical systems, such as propulsion and others, to improve ship’s survivability from fires and other damages. It is, however, surprising that safer alternative engine room arrangements were not considered during design safety assessment, bearing in mind the mission of the ship was to travel to very remote, high latitude locations. Or, perhaps, the fire scenario was considered to be too unlikely for the safety measures to be cost effective.

5 Discussion

The initial explanation of the incident stood on three pillars (see Section 2):

- Human error when replacing the fuel filter and inspecting thermal insulation;
- Management error in providing inadequate manning in engine room on the night shift;
- Design flaw in the fuel system segregation of heavy (HFO) and light fuels (MDO).

While these causal factors definitely explained what happened, and the recommended remedial actions were aimed to fix them, there are other scenarios which were not addressed but could be caused by the same underlying conditions. For instance, the presence of inadequate management on the part of Chief Engineer, due to insufficient feedback about the maintenance practices, a deficient SMS which s/he had to enforce, or simply inadequate training (see Section 4.3), resulted in unprotected hot surfaces which could serve as heat sources for oil mist released in a myriad of other different ways. The suggested inadequate communication between the shipyard and the shipping company resulted in the deficient SMS, i.e. the hazardous design limitation that led to the human error was not reflected in maintenance procedures and training.

There was also a clear drift from the manufacturer requirements (i.e., design assumptions) with respect to replacement of fuel filters. The accident report highlights that when the switch between HFO and MDO occurred, the duplex filters had to be replaced every few hours, instead of the manufacturer’s recommendation of every 1,000 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 risk assessment carried out so the maintenance practice could be justified? 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 cleaner burning light oil or alternative fuels? The deviation from design assumptions, given they are correct, is a well-known causal factor behind many accidents [17].

The question is how many other design limitations and hazards did not become part of the SMS, creating a situation where dormant hazards remained unknown with another incidents waiting to happen. The only way

to remove this uncertainty is to perform a thorough hazard analysis, looking for deficiencies in the SMS and any need for upgrades. This is reflected in safety requirement C4 (Table 3) aimed at safety assurance and change management which are key elements of any safety management system. Clearly, it was inadequately enforced.

We also highlighted that there could have been deficiencies in hazard analysis, or safety assessment in general, during design. The engine manufacturer was supposed to comply with the Machinery Directive which addresses the human-machine interface through a systematic process of safety assessment. Nevertheless, the direct cause behind the incident was not designed out or effectively alleviated, considering a worst-case scenario when the SMS or its enforcement would simply overlook such a human error, or it could be triggered by other unanticipated factors. The fact that conventional approach to safety assessment such as probabilistic safety assessment (PSA) is generally limited to rather simple technical systems and is often inadequate when analysing a socio-technical systems is well researched [7, p. 33]. The PSA is commonly used, although not explicitly required, in development of safety rules in the maritime domain, e.g. [34], and it is also a preferred methodology when assessing safety and effectiveness of safety barriers [35]. Therefore, it may not come as a surprise that this scenario was overlooked or discarded as unlikely.

It is important to point out that the investigation identified individual failures, deviation and errors at different levels of safety control, but disregarded the flawed interactions (e.g., between the management and the engineer, shipyard and company etc.). As described in the introduction, finding and fixing failures or errors is too simplistic, for systems can be completely reliable (no failures or errors), but unsafe [7, p. 3]. In the absence of failures, the presence of dysfunctional interactions and build-up of coincidences can create an unexpected incident scenario, which is impossible to predict just by looking at what can fail. Equally, there are systems that are safe but unreliable, the resilient systems that constantly have incidents but manage to recover quickly [36]. The reason for maintaining the focus on failures and deviations (unsafe acts) is reflective of the current understand of how accidents happen. Accidents are investigated, analysed, and responded to according to the principles of “What You Look For Is What You Find” and “What You Find Is What You Learn/Fix” [37]. So, given an accident model assumed, in this case it should have been the Swiss cheese interpretation [38], the accident will be analysed by looking for failures and deviations [16, p. 201]. The more one finds, the better, although in practice the analysis often stops prematurely. This is the present practice in accident investigation [7, p. 349], and this does not exclude the maritime domain [8]. To remedy this situation, systemic accident models should be adopted, enabling systems thinking during analysis and more cost effective recommendations [11].

So where does it take us, practically? It takes us towards a more robust process of safety management, the process of development and upkeep of an adequate SMS. The company responsible for this shall, therefore, take into account the following three aspects:

1. Communication with manufacturers. Two scenarios possible. First, it could be that communication of design assumptions and limitations is really good, but manufactures have weak safety assessment practices and, hence, the provided documentation does not contain critical hazards. Second, the manufactures may use a comprehensive safety assessment and able to identify many nontrivial hazards, but the communication of them is poor. The second scenario may be easier to eliminate by requesting to, for instance, improve the O&M documentation. But because of the first scenario in particular, the company should consider a hazard analysis of O&M practices on a new ship.
2. Accident investigations. If investigations duly follow the investigation code that requires to look for a bigger picture, they can indeed reveal systemic causes as well (such as the one above). This can help strengthen the SMS in, likely, a more cost effective way.
3. Change management. As O&M practices might drift—some for good, others for bad reasons—from manufacturer guidelines, such deviations from design assumptions should be timely detected and assessed. This accentuate the need to have a good communication with manufacturers, for some critical design assumptions may not be part of O&M documentation at all.

6 Limitations

The analysis results 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. Their safety surveys and audits, for instance, were supposed to recognise solitary maintenance as hazardous, but they did not. However, we felt it would be too speculative to include this causal link.

It should also be noted that CAST is a worst-case analysis method, i.e. not a best-case or most-likely-case method. Being a worst-case, qualitative method, CAST considers causal scenarios exhaustively, although, in the best-case, some of them might have not happened at all. However, having an exhaustive list of causal scenarios is obviously beneficial.

7 Conclusions

This paper contributes towards a better understanding of underlying causes behind engine room fires on modern ships. The used case of cruise ship Le Boreal has essentially demonstrated how an concealed gap between ‘work as imagined’ and ‘work as done’ can lead to accidents [39]. However, to come to this observation, a systemic approach to accident analysis had to be used. The unravelled causal factors help better explain *why* the incident happened and how the entire system of safety control can be improved. We have suggested three actions that would improve safety management systems, which are mandatory on ships as per the ISM Code [32]. The suggestions would not be limited to just eliminating similar incidents, but would more broadly affect overall maritime safety control and proactive safety management at the ship and shipping company levels.

Methodologically, we have applied the systems approach, the method CAST, to analyse the incident. We believe it was a well justified choice, given the complexity and systemic nature of the causal picture behind a rather typical incident. Although some of the illuminated causal factors were also identified in the accident investigation, we have provided a somewhat different, and more useful, interpretation of them. It is important to point out that the Le Boreal incident did not have a ‘root cause’, nor was it merely caused by unsafe actions of the engineers or even the management. The event was much more complex than that, and its coherent explanation required the analysis of the wider socio-technical context involved in safety control. Many questions, which we raised during the analysis, were potentially not asked during the investigation, for the methodology of accident analysis used by the official accident investigation did not seem to prompt the investigators to assess wider causal factors, i.e. “going far beyond the immediate evidence and looking for underlying conditions, which may be remote from the site of the marine casualty or maritime incident, and which may cause other future marine casualties and marine incidents.” [5, p. 15].

The paper has also shown that the compliance with Machinery Directive (2006/42/EC) may be insufficient for safety. This opens up a new direction for further research in systemic causal factors behind similar incidents.

8 References

- [1] Jordan AE. Cruise Industry Poised for Growth. *The Maritime Executive*; 2018.
- [2] Moor R. Will giant cruise ships destroy the wonders their passengers claim to love? : *The Guardian*; 2018.
- [3] DNV. Engine room fires can be avoided. 2000.
- [4] DNVGL. Recommended practice: Engine room fire prevention. 2018.
- [5] IMO. Causality Investigation Code. Code of the international standards and recommended practices for a safety investigation into a marine casualty or marine incident London: International Maritime Organisation; 2008.
- [6] Johnson WG. MORT safety assurance systems: Marcel Dekker Inc; 1980.
- [7] Leveson N. Engineering a safer world: Systems thinking applied to safety: MIT press; 2011.
- [8] 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;43:1187-96.

- [9] Soner O, Asan U, Celik M. Use of HFACS–FCM in fire prevention modelling on board ships. *Safety Science*. 2015;77:25-41.
- [10] 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.
- [11] Underwood P, Waterson P. Systemic accident analysis: Examining the gap between research and practice. *Accident Analysis & Prevention*. 2013;55:154-64.
- [12] Lindberg A-K, Hansson SO, Rollenhagen C. Learning from accidents—what more do we need to know? *Safety Science*. 2010;48:714-21.
- [13] 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.
- [14] Jenkins DP, Salmon PM, Stanton NA, Walker GH. A systemic approach to accident analysis: a case study of the Stockwell shooting. *Ergonomics*. 2010;53:1-17.
- [15] Johnson CW, de Almeida IM. An investigation into the loss of the Brazilian space programme's launch vehicle VLS-1 V03. *Safety Science*. 2008;46:38-53.
- [16] Hollnagel E. *Barriers and accident prevention*: Routledge; 2016.
- [17] Leveson N. A systems approach to risk management through leading safety indicators. *Reliability Engineering & System Safety*. 2015;136:17-34.
- [18] Santos-Reyes J, Beard AN. A systemic analysis of the Edge Hill railway accident. *Accident Analysis & Prevention*. 2009;41:1133-44.
- [19] Kim H, Haugen S, Utne IB. Assessment of accident theories for major accidents focusing on the MV SEWOL disaster: Similarities, differences, and discussion for a combined approach. *Safety Science*. 2016;82:410-20.
- [20] Kim T-e, Nazir S, Øvergård KI. A STAMP-based causal analysis of the Korean Sewol ferry accident. *Safety science*. 2016;83:93-101.
- [21] Lee S, Moh YB, Tabibzadeh M, Meshkati N. Applying the AcciMap methodology to investigate the tragic Sewol Ferry accident in South Korea. *Applied Ergonomics*. 2017;59:517-25.
- [22] Leveson NG, Daouk M, Dulac N, Marais K. *Applying STAMP in accident analysis*. 2003.
- [23] BEAmer. Marine safety investigation report. Fire in the engine compartment on board the expedition-cruiser liner Le Boreal on 18 November 2015, off Falkland Islands. Bureau d'enquêtes sur les événements de mer (BEAmer); 2016.
- [24] 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.
- [25] Underwood P, Waterson P. A critical review of the STAMP, FRAM and Accimap systemic accident analysis models. *Advances in Human Aspects of Road and Rail Transportation* CRC Press, Boca Raton. 2012:385-94.
- [26] Song T, Zhong D, Zhong H. A STAMP analysis on the China-Yongwen railway accident. *Computer safety, reliability, and security*. 2012:376-87.
- [27] Wong B. A STAMP model of the Überlingen aircraft collision accident: Massachusetts Institute of Technology; 2004.
- [28] Kim T-e, Nazir S, Øvergård KI. A STAMP-based causal analysis of the Korean Sewol ferry accident. *Safety Science*. 2016;83:93-101.
- [29] Salmon PM, Cornelissen M, Trotter MJ. Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Safety Science*. 2012;50:1158-70.
- [30] Dekker S. *The field guide to understanding 'human error'*: Ashgate Publishing, Ltd.; 2014.
- [31] Dekker S. *Just culture: Balancing safety and accountability*: CRC Press; 2016.
- [32] ISM Code. International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code). IMO Document Res. A.741(18). London: IMO; 1993.
- [33] Directive M. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006. *Official Journal of the European Union—0906*. 2006:L157.
- [34] Lois P, Wang J, Wall A, Ruxton T. Formal safety assessment of cruise ships. *Tourism management*. 2004;25:93-109.
- [35] Kaneko F. Methods for probabilistic safety assessments of ships. *Journal of marine science and technology*. 2002;7:1-16.

- [36] Woods DD. Essential characteristics of resilience. *Resilience engineering*: CRC Press; 2017. p. 33-46.
- [37] Hollnagel E. Investigation as an impediment to learning. *Remaining sensitive to the possibility of failure*. 2008.
- [38] Reason J. *Managing the risks of organizational accidents*. 1997.
- [39] Hollnagel E. Why is work-as-imagined different from work-as-done? *Resilient Health Care, Volume 2*: CRC Press; 2017. p. 279-94.