Comparison of diesel-electric with hybrid-electric propulsion system safety using System-Theoretic Process Analysis

V Bolbot, G Theotokatos, E Boulougouris, D Vassalos, Maritime Safety Research Centre, The University of Strathclyde, UK

SUMMARY

Cruise ship industry is rapidly developing, with both the vessels size and number constantly growing up, which renders ensuring passengers, crew and ship safety a paramount necessity. Collision, grounding and fire are among the most frequent accidents on cruise ships with high consequences. In this study, a hazard analysis of diesel-electric and hybrid-electric propulsion system is undertaken using System-Theoretic Process Analysis (STPA). The results demonstrate significant increase in potential hazardous scenarios due to failures in automation and control systems, leading to fire and a higher number of scenarios leading to propulsion and power loss in hybrid-electric propulsion systems than on a conventional cruise-ship propulsion system. Results also demonstrate that STPA enhancement is required to compare the risk of two propulsion systems.

1. INTRODUCTION

Developments over the recent past have driven the maritime industry towards reducing exhaust gas emissions and fuel consumption. Specific areas have been designated, the so-called Emission Control Areas (ECAs), where stringent limits for NOx and SOx emissions are applied [1]. At the same time, considerable reduction in the attained Energy Efficiency Design Index (EEDI), which is used to depict the vessel CO_2 emissions, is required by the International Maritime Organisation (IMO) from new built vessels [1]. In addition, the maritime industry is going through periods of high fuel prices, resulting in high operating costs. Furthermore, in 2018, Norway has adopted a resolution to achieve zero-emissions in world heritage fjords the latest by 2026 with application to cruise ships and ferry vessels [2]. The above render attractive the use of alternative fuels and propulsion systems, including Hybrid-Electric Propulsion (HEP) with hybrid power supply, where diesel-generators and batteries are used to ship power needs, and pure electrical propulsion, where batteries are used to store the energy required for ship functions, to meet the regulatory requirements in a cost-effective way.

Hybrid-electric and pure electric propulsion systems have already been applied on a number of existing vessels, while new vessels with HEP are under development. *MV Viking Lady*, an offshore supply vessel equipped with 500 kWh battery system has been in operation since 2013 [3]. *MV Ampere* is the world's first fully electric battery powered ferry vessel with battery capacity of 1,040 kWh deployed on a route in Norway [4]. *MV Hallaig*, *MV Lochinvar* and *MV Catriona* ferries, three sister vessels with 700 kWh battery capacity on each, are currently in operation in Scotland [5]. Two cruise ships with HEP system, allowing ship sailing by using batteries for 30 minutes are expected to be delivered in 2019 [6]. A hybrid-electric icebreaker cruise ship is under development by *PONANT*, *Stirling Design International*, *Aker Arctic* and *VARD* with scheduled ship delivery in 2021 [7]. Considering that battery technology is being constantly developed, with increasing energy density and decreasing procurement cost [8], it can be expected that use of batteries will be extended to larger size cruise ships in the near future.

The HEP achieves energy efficiency improvement by running D/G sets at optimum load by peak load shaving and functioning as spinning reserve [8-10]. Implementation of HEP leads to D/G sets downsizing, which also supports D/G sets operation at their most efficient load ranges [8]. Other advantages include higher redundancy in system and lower emissions due to charging of batteries from local grid in harbour [8, 10]. Disadvantages include relatively high cost of batteries procurement [8, 10], large batteries size and weight [9], limited number of recharging cycles [9] and addition of new hazardous scenarios to the system [8].

On cruise ships though, with passenger number equivalent to a number of inhabitants of a town, ensuring safety of propulsion system is paramount as any malfunctions may lead to propulsion loss and, in turn, to collision, contact or grounding, which may end up in significant human loss [11-13]. In addition, the introduction of batteries can lead to an increased risk of fire, explosion and crew intoxication [8]. A fire on hybrid-electric tugboat occurred due to malfunction of Battery Management System[14], whilst a number of similar events have occurred in other industries. In this respect, it is crucial to ensure that all these scenarios are identified and properly addressed during the system design.

The primary reference for designing safe systems is the IMO regulations [15] and classification society rules [16]. However, additional hazard and risk assessment studies may be required to ensure safe design and class approval [15, 16]. The only available and known safety study on HEP system is given in [3], which is a high level study. Other studies have referred to potential safety issues on HEP systems but did not follow a hazard identification method for their analysis [14]. Pertinent literature reveals the research gap, which is a hazard analysis of HEP system

using well-established or novel methods and comparison with the standard diesel-electric propulsion. The research gap leads to the aim of this study, which is to analyse the safety of HEP system using System-Theoretic Process Analysis and to compare it with standard Diesel-Electric Propulsion (DEP) in terms of the developed hazards, number of potential hazardous scenarios and causal factors.

This paper is organised as following. In section two, the selected method and the rationale behind the method are presented. In section three, a short description of the system and system functionalities is provided. In section four, the analysis results and safety recommendations are given. In section five, the main findings of this study are summarised.

2. METHODOLOGY

Hazard identification and analysis is the process of defining all possible scenarios or sequences of events, which can lead to a hazard realisation [17]. A number of traditional methods can be used for analysis of power propulsion systems including Preliminary Hazard Analysis (PHA), HAZard and Operability studies (HAZOP) and Failure Modes and Effects Analysis (FMEA) [17]. However, these methods have been criticised for not addressing properly the automation functions in the system [17-20]. Control and automation though has an important role for power generation on cruise ships using either standard or diesel-electric or hybrid-electric propulsion system [21]. For this reason, the System-Theoretic Process Analysis (STPA) method has been selected for hazard identification. Another advantage of STPA is that it can be implemented on functional level, not requiring the exact details of the system and vessel. In this way the identified hazardous scenarios will have applicability to other ship types and similar propulsion systems. The method steps are presented in Figure 1 and described in more detail in the following.

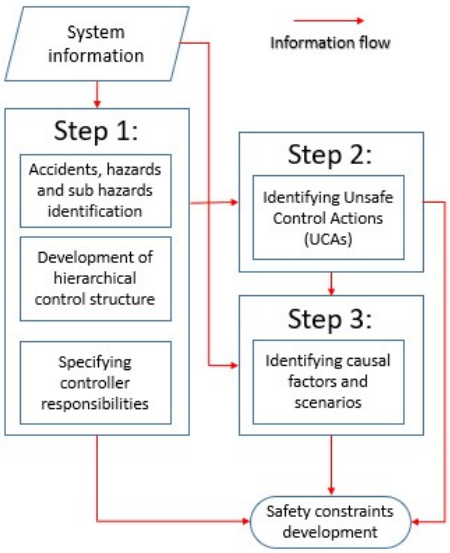

Figure 1 STPA steps.

STPA defines the accident as: "an undesired and unplanned event that results in loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, financial loss, etc." [22]. The hazards in the STPA framework are understood as: "system states or set of conditions that together with a worst-case set of environmental conditions, will lead to an accident" [22]. The hazards in STPA are viewed on a system level, so they go beyond the single failures that may occur in the system and should be referred to a specific state of the system. Sub hazards are considered states in a worst-case scenario leading to hazard realisation. Generic requirements can be specified, based on the hazards and sub hazards.

The development of a functional control structure is one of the differentiating points of the STPA analysis, compared with the other methods [22]. Usually, it starts with a high-level abstraction of the system and proceeds to a more detailed system description. The initial control structure consists of the high-level controller, the human operator and the controlled process with the basic control, feedback and communication links. A more detailed description would incorporate a hierarchy of controllers. Both high-level and detailed control structure can be used for the safety analysis at different system design stages.

After the development of the basic control structure, the next step is its refinement. The required actions include the identification a) of each controller responsibilities; b) of the process model with process variables and potential process variable values; c) of the control actions; d) the behaviour of the actuators; e) the information from the sensors; f) the information from the other controllers.

The actual hazards identification starts by finding the Unsafe Control Actions (UCAs). The possible ways to proceed are either by using the control actions types as initially proposed for the STPA [23] or by using the context tables as proposed in [18]. Herein, the second of the two approaches has been selected. According to both approaches, the possible UCAs can be of the following seven types [22]:

- Not providing the action leads to a hazard.
- Providing of a UCA that leads to a hazard.
- Providing the control action too late.
- Providing the control action too early.
- Providing the control action out of sequence.
- Control action is stopped too soon
- Control action is applied for too long.

According to the STPA, there is also another type of UCA, when the safe control action is provided but is not followed. This type of failure mode is addressed during the identification of causal factors in the second step of the method. Similarly, with the system hazards, safety constraints can be derived for the UCAs, aiding the identification of possible safety barriers.

The second step in the hazard identification of the STPA has the purpose of determining all the scenarios and causal factors leading to the UCAs. This is done by examining the hazardous scenarios including software and physical failures as well as design errors. There are several ways to organize the results of the hazardous scenarios by using tables or lists. In this work, the process was augmented by a checklist, developed on the basis of previous studies [24, 25]. The main categories of causal factors are:

- Inappropriate control input
- Hardware failure
- Software faulty implementation
- Software faulty design
- Erroneous or missing input
- Inadequate control command transmission
- Flawed execution due to faults in actuator or physical process
- Conflicting control actions

3. SYSTEMS DESCRIPTION

The conventional diesel-electric and hybrid-electric propulsion system single line diagram is presented in Figure 3 whilst functional control structure for both systems is given in Figure 2. Two switchboards and engine rooms are available to comply with Safe Return to Port rules requirements [26]. The power network is of the Alternate Current type. It has been also assumed that DEP plant operates with the bus-tie circuit breaker connected. Power Management System (PMS) starts/stops the engines based on ship consumers electric load demand. Switchover between the plant Diesel Generators (D/G) is implemented based on the D/G sets running hours. The PMS can implement a fast-electrical load reduction for the propulsion motors and bow thrusters as well as preferential tripping functions (fast load reduction) by tripping Heat Ventilation Air Conditioning (HVAC) units.

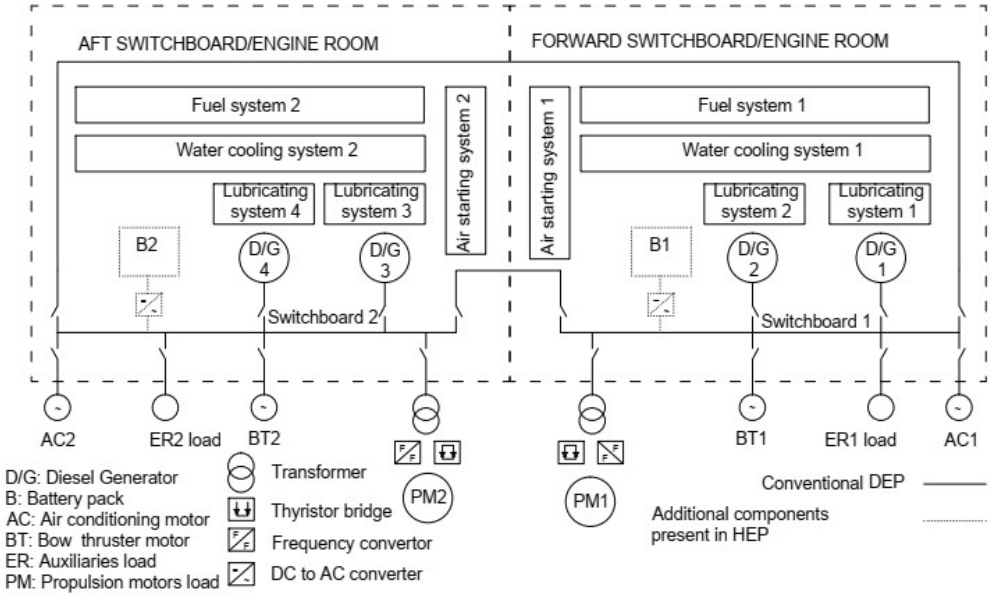

Figure 3 Single line diagram of conventional and hybrid power network.

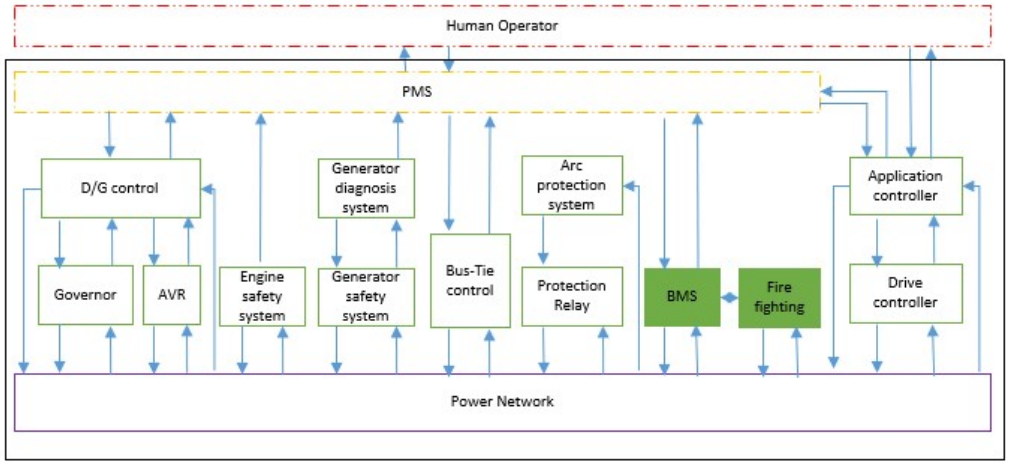

Figure 2 Functional control structure.

The D/G sets operate in the droop mode and their power output is regulated by speed governor and Automatic Voltage Regulator (AVR). Several safety systems are used to trip D/G sets and propulsion motors if a fault had been observed. The DEP control network is also considered to be isolated from other networks, so no hazardous scenarios are developed in the system because of cyber-attacks. It is also considered that the human operator neither reduces nor introduces new hazards.

In the investigated HEP system, in addition to the components present in conventional DEP, one battery pack per switchboard with current converter is considered. The battery output and condition are controlled by a dedicated Battery Management System (BMS) which monitors the actual battery health state and the battery and cell capacity and controls the battery cells charge status, the discharging/charging rate, the converters power output and the battery auxiliary systems. The BMS communicates with PMS to determine the actual power status and power demand implementing in this way the Energy Management System functions. The BMS also communicates with fire-fighting systems to determine the battery operating status. Battery capacity is considered adequate to cover the whole ship power demand for a limited period. The battery has been considered of Li-Ion type.

4. RESULTS AND DISCUSSION

Based on previous Formal Safety Assessment studies, the following causality scenarios can be considered as accidents [27]:

- Collision [A-1]
- Contact [A-2]
- Grounding [A-3]
- Fire [A-4]
- Explosion [A-5]
- Machinery damage [A-6]
- Foundering [A-7]
- Operating personnel injury or death [A-8]

These accidents are not fully disjoint, as a fire can lead to collision and vice versa [28]. In addition, numerous hazards can be connected to the accidents on a cruise ship and there can be interactions between different hazards. Herein, the most important and those related to the system under analysis are referred to [11, 27]:

- Propulsion loss [H-1] leading to collision, contact and grounding accidents. The propulsion loss can be further developed into the following sub hazards:
    - D/G sets overload [H-1-1].
    - Transients [H-1-2].
    - Imbalanced power generation [H-1-3]
    - D/G sets unavailability [H-1-4]
    - Batteries unavailability [H-1-5]
    - Propulsion motors unavailability [H-1-6]
- Flammable liquid on hot surfaces in the engine room and other conditions leading to [H-2] fire in engine room.
- Uncontrolled electrical faults in equipment leading to [H-3] fire and explosions in system components or blackout (propulsion loss).
- Toxic/flammable atmosphere in battery room leading to crew intoxication or fire [H-4].
- Anomalous conditions in batteries leading to fire and thermal runaway [H-5].
- Arson – deliberate act resulting in fire [H-6].
- Human erroneous operation [H-7]
- Cyber-attack leading to any of previous hazards [H-8].
- Water ingress [H-9]

Although, it is acknowledged that there is contribution from hazards [H-6]-[H-9] to the overall system risk, these hazards can be considered as external to the system presented in Figure 3 and Figure 2 and thus their analysis has been omitted.

The developed control structure has been already provided in Figure 2. The difference between the two propulsion systems can be found in the presence of Battery Management System and additional interactions between the fire-fighting system and the propulsion system. The description of responsibilities of each controller and their control actions, although necessary for the analysis have been omitted for brevity purposes.

In total, 160 and 228 potential UCAs have been identified in DEP and HEP system, respectively. The increase in UCAs number can be attributed to the increase in the number of control actions implemented by BMS. However, as it can be viewed, it leads to a significant increase in the number of potential UCAs (more than 40%). The distribution of UCAs per hazards is given in Figure 5. As it can be seen from this figure, the number of hazardous scenarios other than propulsion loss, leading to fire or crew intoxication is significantly higher in the investigated HEP system in comparison with the DEP system. The number of scenarios leading to propulsion loss is also significantly higher. These results do not necessary imply that the risk level is higher in the investigated hybrid-electric system than the risk in conventional DEP system, rather that there are much more paths to the accident in hybrid-electric systems than in DEP, which must be carefully controlled. This also indicates that a successful cyber-attack on a hybrid-electric vessel will lead to more hazardous scenarios than in conventional cruise ship vessels.

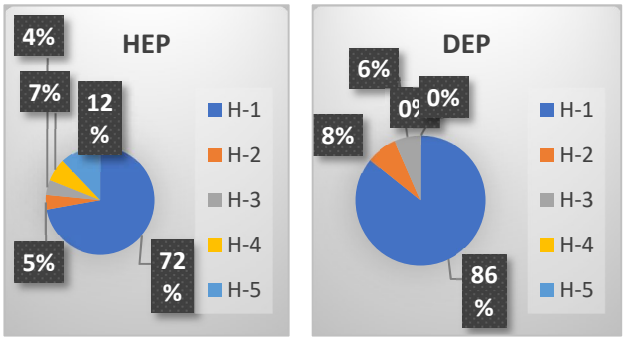

Figure 5 UCAs distribution per hazards.

The distribution of UCAs failure modes for the investigated HEP system is given in Figure 6. The results for the DEP are similar to HEP system. As it can be observed from Figure 6, the primary failure modes are related either to failure to implement the intended control action or to implement the intended action in time or commission errors. These types of control actions as well as actions applied in wrong order are related to the designed safety functions or automated control actions in the investigated system. Stopped too late, stopped too soon and applied too early were related mostly to control actions implemented by the investigated system PID controllers.

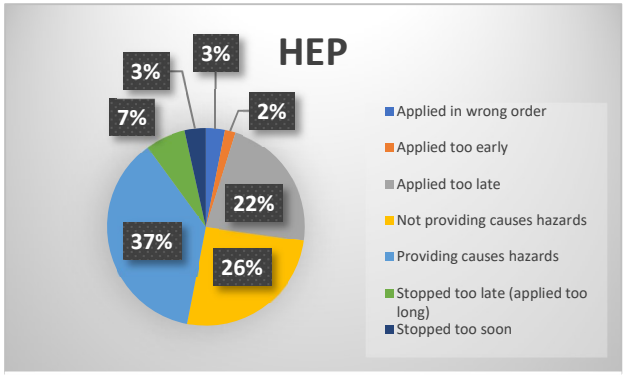

Figure 6 Failure modes distribution.

In total, 2,225 and 1,523 causal factors have been identified for the hybrid-electric and the conventional diesel-electric propulsion systems. The causal factors distribution for the HEP system is given in Figure 4. The results for the conventional DEP are similar. As it can be observed, most scenarios are dependent on installed control software errors, either controller design or implementation errors. Errors in sensors have also been identified as potential causal factors.

Based on the conducted analysis and the derived results comparison, the following safety recommendations can be made:

- In HEP systems, adequate means must be provided to prevent and mitigate scenarios leading to fire to ensure that the hazardous scenarios leading to fire do not lead to higher risk

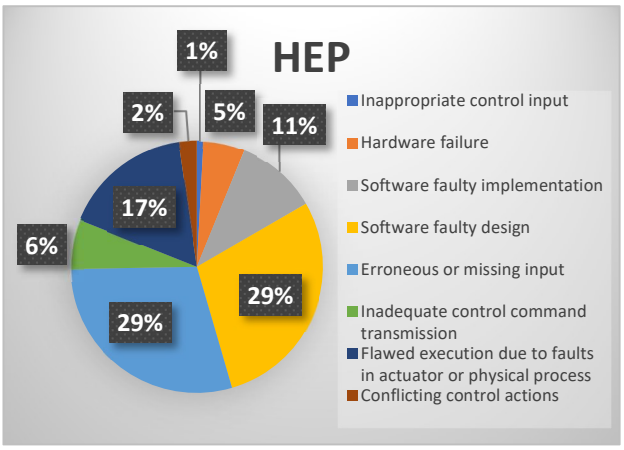

Figure 4 Distribution of causal factors.

in hybrid-electric system than in the conventional system. This includes systems responsible for batteries temperature management and fire-fighting and proper selection of location for batteries.

- System operational conditions must be thoroughly understood and addressed in system design. This includes the batteries and actuators degradation mechanisms, potential modifications in the systems and software updates during operation and maintenance.
- Rigorous testing of the system control actions must be implemented for ensuring their functionality during the design, development and trial phase according to hazardous identification process in both diesel-electric and hybrid-electric system. The development and test cost in hybrid-electric system will be higher since the number of scenarios to be addressed is also higher.

From the STPA application to the conventional diesel-electric and HEP system an extensive list of safety requirements for the employed control systems has been derived. However, some of the STPA restrictions have been revealed during the analysis. Potentially, more scenarios could be identified if more refined system representation was used. In addition, STPA is applied for scenarios development, but did not allow risk estimation and scenarios ranking, so the only discussion about potential safety implications can be in terms of hazardous scenarios.

5. CONCLUSIONS

In this study, the STPA has been applied for hazard identification and analysis of a diesel-electric and hybrid-electric propulsion systems. Through its application, hazardous scenarios in automation and control system have been identified and compared.

The main findings can be summarised as follows:

- Hazardous scenarios leading to fire accidents are significantly more in HEP systems, thus they must be carefully controlled.
- Scenarios number leading to propulsion loss and potential collision, contact, grounding is also higher in HEP systems than in conventional DEP systems.
- Failure modes and potential causal factors distributions are similar in hybrid-electric and diesel-electric propulsion systems.
- Special attention must be paid to software design, software testing, sensors redundancy and batteries location in hybrid propulsion system.
- An improvement in STPA method must be considered to allow ranking of different scenarios and estimating risk.

In summary, the results indicate the high importance of proper operation of control and automation systems for diesel-electric and hybrid-electric systems safety. A potential future work could investigate the risk level in more detail by improving the STPA method.

6. ACKNOWLEDGMENTS

The work presented in this paper was partially supported by the "NEXUS – Towards Game-changer Service Operation Vessels for Offshore Windfarms" project that was funded from the European Union's Horizon 2020 research and innovation action under grant agreement N° 774519. The authors are grateful to Dr Romanas Puisa from Maritime Safety Research Centre to Dr George Psarros, Dr Ole Christian Astrup, Dr Rainer Hamann, Dr Pierre C Sames from DNV GL AS and Kevin Douglas from Royal Caribbean for their valuable comments and support. The opinions expressed herein are those of the authors and should not be construed to reflect the views of European Commission or the acknowledged individuals and their associated organisations.

7. REFERENCES

1. International Maritime Organization. Regulations for the prevention of air pollution from ships and NOx technical code 2008. Organization IM, editor. United Kingdom, London: IMO publishing; 2009.
2. GREENPORT. Norway adopts zero-emissions regulations in world heritgate fjords 2018 [Available from: https://www.greenport.com/news101/Regulation-and-Policy/norway-adopts-zero-emissions-regulations-in-world-heritage-fjords.
3. Jeong B, Oguz E, Wang H, Zhou P. Multi-criteria decision-making for marine propulsion: Hybrid, diesel electric and diesel mechanical systems from cost-environment-risk perspectives. Applied Energy. 2018;230:1065-81.
4. Corvus-Energy. World's first all-electric car ferry 2016 [Available from: https://corvusenergy.com/marine-project/mf-ampere-ferry/.
5. Ltd CMA. History of our hybrid ferries 2013 [Available from: http://www.cmassets.co.uk/project/hybrid-ferries-project/.
6. Hurtigruten. Hurtigruten names hybrid explorer ships 2018 [Available from: https://www.hurtigruten.co.uk/about-us/news/new-hybrid-explorer-ships/.
7. Dhanvijay N. Vard to build hybrid LNG cruise vessel for Ponant: Electrans; 2017 [Available from: https://www.electrans.co.uk/vard-to-build-hybrid-lng-cruise-vessel-for-ponant/.
8. Brandsaeter A, Valoen LO, Mollestad E, Haugom GP. In focus – the future is hybrid. DNV GL. 2015.
9. Räsänen J-E. Current and future scale limitation for alternative marine power and propulsion solutions. Power & Propulsion Alternatives for Ships; Rotterdam, Netherlands: The Royal Institution of Naval Architects; 2017.
10. Geertsma RD, Negenborn RR, Visser K, Hopman JJ. Design and control of hybrid power and propulsion systems for smart ships: A review of developments. Applied Energy. 2017;194:30-54.
11. Bolbot V, Theotokatos G, Vassalos D. Using system-theoretic process analysis and event tree analysis for creation of a fault tree of blackout in the Diesel-Electric Propulsion system of a cruise ship. Marine Design XIII, Volume 2: CRC Press; 2018. p. 691-9.
12. Nilsen OV. FSA for Cruise Ships - Task 4.1.1 - Hazid identification. 2005.
13. MAIB. Report on the investigation of the catastrophic failure of a capacitor in the aft harmonic filter room on board RMS Queen Mary 2 while approaching Barcelona 23 September 2010. United Kingdom, Southampton; 2011.
14. Hill DM, Agarwal A, Gully B. A review of engineering and safety considerations for hybrid power (Lithium-Ion) systems in offshore applications. Oil and Gas facilities. 2015;June 2015:68-77.
15. International Maritime Organization. SOLAS: consolidated text of the International Convention of Safety of Life at Sea, 1974, as amended. 6th consolidated edition ed: International Maritime Organization; 2014. 420 p.
16. DNV GL. Additional class notations: Battery power-Part 6 Chapter 2 Section 1 2018.
17. Bolbot V, Theotokatos G, Bujorianu LM, Boulougouris E, Vassalos D. Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review. Reliability Engineering & System Safety. 2019;182:179-93.

18. Thomas J. Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis: Massachusetts Institute of Technology; 2013.
19. Rokseth B, Utne IB, Vinnem JE. A systems approach to risk analysis of maritime operations. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability. 2017;231(1):53-68.
20. Sulaman SM, Beer A, Felderer M, Höst M. Comparison of the FMEA and STPA safety analysis methods–a case study. Software Quality Journal. 2017:1-39.
21. UK P&I CLUB. Risk Focus: Loss of power. 2015.
22. Leveson N, Thomas J. An STPA Primer. 2015.
23. Leveson N. Engineering a safer world: Systems thinking applied to safety: MIT press; 2011.
24. Blandine A. System theoretic hazard analysis applied to the risk review of complex systems: an example from the medical device industry. Cambridge, MA, USA Massachusetts Institute of Technology; 2013.
25. Becker C, Van Eikema Hommes Q. Transportation systems safety hazard analysis tool (SafetyHAT) user guide (version 1.0). John A. Volpe National Transportation Systems Center; 2014.
26. DNVGL. Guidance for safe return to port projects. DNVGL-CG-00042016.
27. IMO. Formal Safety Assessment - Cruise ships. 2008.
28. Hamann R, Papanikolaou A, Eliopoulou E, Golyshev P. Assessment of safety performance of container ships. Proceedings of the IDFS. 2013:18-26.

8. AUTHORS BIOGRAPHY

Victor Bolbot is a third year PhD student at Naval Architecture, Ocean and Marine Engineering Department of University of Strathclyde, Glasgow. As a PhD student he is conducting research on the safety of complex and Cyber-Physical Systems with focus on power generation systems. His recent research output include publications on safety assessment of power systems on cruise ships, dual-fuel engines and safety assurance methods in Cyber-Physical Systems.

Gerasimos Theotokatos is DNV GL Reader of Safety of Marine Systems at the University of Strathclyde, Department of Naval Architecture Ocean and Marine Engineering. His research focuses on the modelling methods, optimisation and experimental analysis of marine systems and ship energy systems pursuing life-cycle efficiency improvement, their environmental footprint reduction and their safety enhancement.

Evangelos Boulougouris is RCCL Reader of Safety of Marine Operations at the University of Strathclyde, Department of Naval Architecture Ocean and Marine Engineering and Director of the Maritime Safety Research Centre. His main research interests are focused on ships safety and marine design optimisation. He has produced more than 70 publications in journals and international peer-reviewed conferences and 2 chapters in books.

Dracos Vassalos is a Professor of Maritime Safety in the Department of Naval Architecture, Ocean and Marine Engineering at the University of Strathclyde in Glasgow, UK. Professor Vassalos pursued over a 40-year career in industry and academia, promoting the use of scientific approaches in maritime safety and risk, including environmental risk. Professor Vassalos received a Life Achievement Award from the Royal Academy of Engineering in 2011, the Froude Medal from RINA in 2012, the David Taylor Medal from SNAME and a DSC from Strathclyde in 2016 for his life-long contribution to maritime safety.