Dealing with novel and emerging threats in the maritime industry: The need for an alternative Life – Cycle Risk Management Framework

Nikolaos P. VENTIKOS[a,1] and Konstantinos LOUZIS[a]
[a] *National Technical University of Athens, School of Naval Architecture and Marine Engineering, Laboratory for Maritime Transport, Maritime Risk Group*

Abstract. Developments in the maritime industry, such as the increasing size of container and cruise ships, and the automated/autonomous ship concepts, yield technical and operational challenges throughout the life-cycle of ships. New interactions increase complexity, resulting in unforeseeable system states and risk fluctuations. Despite the development of approaches that address some of the limitations of current risk management, the sub-systems of the ship are mostly treated separately with only partial consideration of interactions between risk factors. The main goal of this paper is to introduce a novel framework for managing life-cycle risk in the maritime domain, where the ship is viewed as an integrated complex system that is subject to change throughout its life-cycle. The focus is on enhancing the adaptive capability of the system to respond to evolving dynamics and deal with unknown and emerging safety threats. In addition, to avoid potential problem shifting between life-cycle stages, interactions between risk factors and risk propagation are considered. In this context, a change in perspective for maritime safety is also proposed, based on the concept of biomimicry, considering that biological systems typically adapt in a dynamic environment to deal with emerging threats.

Keywords. Life-cycle risk management, complex systems, maritime safety, risk analysis, uncertainty, biomimicry

1. Introduction

The maritime industry is currently experiencing fast-paced technological and operational changes, that are driven by market needs, and/or new regulatory requirements. Important developments in the maritime industry include increasing ship size (e.g., there are projections for 50,000 TEU container ships by the year 2050 [1]), remote/automated and autonomous ship concepts, and navigation in harsh environments. These are driven by needs such as greater efficiency and economies of scale, as well as a need to reduce maritime accidents attributed to the human element [2]. With the development of innovative modular ship designs and more efficient ship-building techniques and the emergence of new risks that threaten operation, these

[1] Corresponding author, Nikolaos P. Ventikos, 9 Iroon Polytechniou st., Zografou 15773, Greece; E-mail: niven@deslab.ntua.gr.

transitions have an impact on every stage of the life-cycle of ships. The challenges for maritime safety [3] include both foreseeable risks and unknown hazards. Situations that have not been encountered before, such as the emergence of an operational field where conventional and automated or fully autonomous ships might co-exist and interact [4], will introduce greater uncertainties to risk management. Another source of uncertainty is related to the increasing complexity of marine systems due to rapid technological development and the integration of advanced digital systems. In the continuously evolving maritime landscape, we need to re-examine the capacity of the established risk management practices to deal effectively with future threats to safety.

The goal of this paper is to introduce a novel framework for managing life-cycle risk in the maritime domain. The proposed framework considers the ship as an integrated complex system that is subject to change throughout its life-cycle, as well risk propagation among life-cycle phases. The paper is structured as follows: Section 2 reviews the state-of-the-art in maritime risk management; Section 3 presents the systems approach to safety and risk; Section 4 describes the use of life-cycle thinking for safety; Section 5 outlines our research objectives and presents an initial approach to the proposed Life-Cycle Risk Framework. The paper concludes with a roadmap of future research, as well as some comments on the potential impact of our research.

2. State-of-the-art in maritime risk management

Maritime risk management has relied on reactive policies in the wake of major accidents and catastrophes [5] for addressing system vulnerabilities. The result is a complex international framework of prescriptive regulations that enforces compliance with minimum standards and increases administrative burden for operators and seafarers alike. In a step towards more proactive policies, the International Maritime Organization (IMO) introduced Goal-Based Standards (GBS) and the safety level concept [6], where regulations define an acceptable level of risk and the details are left to the designers. The concept of GBS allows the development of innovative ship designs that might not be approved by the standard prescriptive regulations. In this context, Papanikolaou et al. [7] have outlined a framework for Risk-Based Design (RBD) that uses risk-based approaches for determining the safety level of a design solution. Approaches that specifically focus on the role of the human element in accidents have also been developed. Acknowledging the potentially beneficial role of the human element in normal safe operation Hollnagel et al. [8] have introduced the SAFETY-II concept. The principles of Resilience Engineering are employed to enhance human, or in general system, performance when disruptions in the functionality of the system occur due to unexpected changes in external conditions [9].

Such approaches introduce significant advances to the maritime risk field. However, they do not directly address the increasing complexity and socio-technical nature of marine systems due to the interactions among the different sub-systems. The rationale of controlling risks in reasonably plausible adverse scenarios, based on historical data or expert judgement, is limited when faced with emerging risks [10] from the changing technological and operational landscape. Recent experience from major accidents has shown that there are scenarios that cannot be imagined during design and may potentially result in black swan type situations [11]. In environments with deep uncertainties, Aven [12] has also questioned the validity and reliability of risk assessment results that are based on expected losses without considering the uncertainties that relate to the strength of the background knowledge and the supporting assumptions. Expected losses are the standard metric for risk quantification and are derived from the definition of risk by Lowrance [13]. The main limitation of this metric is that it oversimplifies the maritime risk picture by treating high probability – low consequence risks in a similar manner to low probability – high consequence risks, where uncertainties are more pronounced. Conventional risk quantification also offers a static picture, which does not account for the changing characteristics of marine systems throughout their life-cycle due to factors such as improper maintenance or frequent crew turnover. However, because marine systems are inherently dynamic, interactions among risk factors over the life-cycle may result in risk propagation with an unknown effect on the total safety level.

3. The systems approach to safety and risk

A complex system incorporates several components with non-linear interactions and, as a result, presents emergent behaviours that are dynamic in response to environmental stimuli. Marine systems are becoming increasingly complex, with increasing digitalisation and the emergence of new operational practices, such as remote operations. Maritime operations are conducted by complex systems where tightly coupled intelligent agents cooperate [14]. Complex systems with distributed control and interacting components, such as a maritime supply chain, exhibit features such as self-organization and adaptivity [15]. According to Leveson [16], safety is one of the emergent properties of complex systems and therefore, it does not only depend on the safety of individual components but also on their interactions. Because risk factors in complex systems are neither independent nor mutually exclusive, which is a premise of the reductionist logic, accidents may occur even if all system components work reliably [17].

Grabowski et al. [18] have noted that the management of safety in complex systems is affected by risk migration among different parts of the system, by the fact that risk contributing factors may have long incubation periods, and by problematic identification of human and organisational error. Haimes [19] has attempted to improve the effectiveness of risk management for complex systems by expanding the definition of risk by Kaplan and Garrick. The concept of complex risk is time-dependent and conditioned upon the states of the system, which are a function of its performance, vulnerability, and resilience. In this context, risk is defined as a vector with the same units as the vector of consequences. After critically reviewing this formulation, Aven [20] noted that the concepts of system risk, vulnerability, and resilience explicitly depend on how the system is modelled, and that background knowledge uncertainty is not considered. The need to include uncertainty in the definition of risk is also expressed by Vatn [21] because complexity induces uncertainties in a risk analysis context.

4. Life-Cycle thinking applied to safety

The false assumption that a system is static has been identified by Leveson [22] as one of the main reasons many efforts to improve safety are neither cost-effective nor efficient. In fact, Bahr [23] claims that hazard evaluation in every life-cycle phase is the most cost-effective way for controlling risk. Although life-cycle thinking has been applied to environmental (e.g., Life Cycle Assessment of marine air emissions by Chatzinikolaou and Ventikos [24]) and financial problems, its application to safety problems has been limited. In a survey of the relevant literature we have identified the following approaches: various combinations of LCA and risk analysis, and assessment of total life-cycle risk. Breedveld [25] has noted that Life-Cycle Based Risk Assessment is an emerging term that reflects a new perspective on safety analysis based on life-cycle thinking. In the domain of nanotechnology, Sweet and Strohm [26] have proposed using LCA for focusing a more detailed risk analysis in a specific phase of the product life-cycle. In the context of structural integrity, Decò and Frangopol [27] have applied an interesting approach for optimizing the maintenance of road bridges, considering the total life cycle risk and the dynamic structural characteristics. Liu et al. [28] developed a methodology for analysing risk in every phase of the life-cycle of an offshore platform, considering several different risk factors such as environmental, technical, economic, managerial, and behavioural. Ramadhan et al. [29] measured the total life cycle risk for a palm oil production plant by summing expected losses of life for every life-cycle phase and considered them as an additional criterion for optimization.

The concept of life-cycle safety management has also emerged in the maritime risk field. The Total Risk Management System (TRMS) [30] is based on the development of an Integrated Risk Model that quantifies total risk levels and a Risk Processor that is used for generating both static and dynamic accident scenarios. The Ship Safety Assessment Model (SSAM) [31] follows a systems approach for developing a functional model of the ship that is subsequently used either for RBD or risk monitoring during operation. Vassalos [32] has defined Life Cycle Risk Management (LCRM) as a formal process for addressing the risks during the operation of a ship, by reducing and/or mitigating risk during design and managing the residual risk during normal operation as well as in operational crises. These concepts employ an integrated approach to addressing risks during normal operation and emergencies. Common elements include risk reduction during the design phase, management of residual risk during operation by continuously monitoring safety performance, and a direct feedback loop linking design and operation.

5. Research objectives and initial approach to the proposed framework

Our main research objective is to structure risk-averting strategies for safety assurance throughout the life-cycle of complex marine systems in an uncertain and evolving environment with emerging risks. More specific objectives of our research include the following: a) analyze and evaluate total safety level for marine systems as a function of time, b) determine risk propagation among different life-cycle phases to avoid problem shifting, and c) determine the uncertainties related to risk quantification. To achieve these objectives, we aim to develop a novel conceptual and methodological risk management framework that will provide a structured approach to managing through-life safety. This framework will incorporate elements from the fields of complex system safety, life-cycle thinking for safety management, and ideas based on the functionality of the Biological Immune System (BIS) for safety modelling.

There is an interesting analogy for complex marine systems if we consider external and internal safety threats as antigens and risk control options as antibodies that are employed in organizing effective risk control strategies/responses. The BIS is a strongly adaptive system that defends an organism against external threats (antigens) and from parts of itself that are dysfunctional. The BIS responds to future threats based on its previous encounters with antigens [33] and continuously evolves its definition of the normal state of the organism by interacting with the environment [34]. Artificial Immune Systems (AIS) are a conceptual framework that uses theoretical immunology concepts (e.g., negative selection and danger theory) to construct computational systems for practical problem-solving [33]. According to Negoita [35], the AIS framework alters the perception of how system faults are managed and allows the development of adaptive complex system models that are open to the environment. AIS applications include pattern recognition, robotics, maintenance systems [36], and computer security, for learning, anomaly detection, and optimization [37]. Indicatively, Perhinschi et al. [38] have employed various methodologies, such as genetic algorithms, artificial neural networks, and fuzzy logic, in the AIS framework for evaluating the magnitude of a failure in an aircraft and identifying which sub-systems have been affected.

The proposed Life-Cycle Risk Framework may be used for managing system health throughout the entire life-cycle, which consists of the following high-level phases: Design, Learning, Operation, and Adaptation (Figure 1). In this context, the system is viewed as an adaptive and evolving entity that must maintain its safety performance within acceptable levels determined as a function of the ability of the system to fulfil its mission. The continuous monitoring and evaluation of safety performance will result in effective risk-control strategies and feedback among the different phases of the life-cycle. Therefore, this framework aims at proactively detecting and evaluating dangerous situations and at providing early warning for the deterioration of system safety.

Figure 1 shows how the Life-Cycle Risk Framework may be utilized for managing through-life system health by continuously monitoring risk levels as a function of system states and time. System health management will be based on a functional safety model of the system, which may be part of a digital twin of the vessel [39], and a supporting AIS model. These models may be used for measuring system safety performance throughout the life-cycle, either via simulation during design or as real-time risk monitoring during the learning, operation, and adaptation phases. The AIS model will detect deviations from the boundaries of acceptably safe operation and migrations towards unsafe system states. This model may be trained from generic historical casualty data and data generated during the growth period of the system to generate an initial immune response from previously encountered threats. A more refined immune response may be generated by the interaction between the threats to system safety (antigens) with the antibodies of the AIS model during the operation and adaptation periods of the system for dealing with emerging threats that have not been encountered before. The output of the Life-Cycle Risk Framework process will be strategies for controlling risk levels throughout the life-cycle. Indicative applications for conventional vessels would be either as a design tool for assessing the effectiveness of specific risk control strategies, or as a real-time operational tool for proactively avoiding the migration of the system towards unsafe states. For autonomous vessels, an example application would be an Artificial Intelligence unit that uses concepts from the framework for autonomous, risk-based decision making throughout their life-cycle.

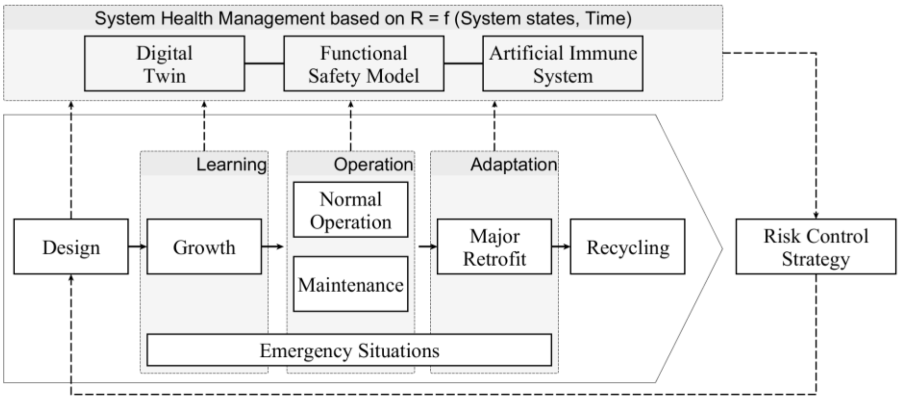

Figure 1. High-level approach to managing system health with the Life-Cycle Risk Framework concept.

6. Conclusions

Transitions in the maritime industry such as increasing ship size, navigation in harsh environments, and the development of automated and autonomous ship concepts present challenges to maritime safety. Marine systems become more complex with more digital components and, as a result, new risks are emerging from situations that have never been encountered before. The current approach to maritime risk management does not address complexity or the dynamic nature of risk and therefore has limitations in dealing with emerging threats throughout the life-cycle.

The main objective of our research is to analyse and evaluate the level of safety throughout the life-cycle of marine systems in an uncertain environment with emerging risks. We propose the development of a novel Life-Cycle Risk Framework for complex dynamic marine systems that will be based on a systems approach to safety and risk, will consider risk propagation throughout the life-cycle, and will employ the AIS framework as a basis for safety modelling. The immune system has several interesting properties and behaviours that provide a useful paradigm for solving a diverse set of computational problems. In the next steps of our research we intend to further refine and elaborate upon the high-level approach to this framework.

The Life-Cycle Risk Framework aims to shift the focus of maritime safety research from trying to foresee every possible adverse scenario and its potential consequences, to enhancing the capability of a complex system to adapt to variable external conditions and to respond to any safety threat. The proposed framework aims to incorporate an alternative way of thinking about the safety problem that may strengthen the ability of marine systems to deal with novel and emerging threats effectively throughout their life-cycle.

7. Acknowledgements

The work of Mr. Konstantinos Louzis is partially supported by a PhD Research Fellowship from the Special Account for Research Grants of the National Technical University of Athens (NTUA).

References

[1] S. Saxon, and M. Stone, Container shipping: The next 50 years, 2017.

[2] Ø.J. Rødseth, and H.C. Burmeister, Developments toward the unmanned ship, 2012.

[3] Z.L. Yang, J. Wang, and K.X. Li, Maritime safety analysis in retrospect, *Marit. Policy Manag.* **40** (2013) 261–277.

[4] K. Wróbel, J. Montewka, and P. Kujala, Towards the assessment of potential impact of unmanned vessels on maritime transportation safety, *Reliab. Eng. Syst. Saf.* **165** (2017) 155–169.

[5] E. Hollnagel, A tale of two safeties, *Nucl. Saf. Simul.* **4** (2013) 1–9.

[6] IMO, MSC 81/6/2, Goal-based New Ship Construction Standards, Safety Level Approach, Submitted by Denmark, Germany, Norway and Sweden, 2006.

[7] C.D. Soares, A. Jasionowski, J. Jensen, D. McGeorge, A. Papanikolaou, E. Poylio, P.C. Sames, R. Skjong, J.S. Juhl, and D. Vassalos, Risk-Based Ship Design: Methods, Tools And Applications, Springer-Verlag, Berlin Heidelberg, 2009.

[8] E. Hollnagel, R.L. Wears, and J. Braithwaite, From Safety-I to Safety-II: A White Paper, *Resilient Heal. Care Net Publ. Simultaneously by Univ. South. Denmark, Univ. Florida, USA, Macquarie Univ. Aust.* (2015).

[9] E. Hollnagel, D.D. Woods, and N. Leveson, Resilience Engineering: Concepts and Precepts, Ashgate Publishing Company, Burlington, USA, 2006.

[10] R. Flage, and T. Aven, Emerging risk - Conceptual definition and a relation to black swan type of events, *Reliab. Eng. Syst. Saf.* **144** (2015) 61–67.

[11] T. Aven, Implications of black swans to the foundations and practice of risk assessment and management, *Reliab. Eng. Syst. Saf.* **134** (2015) 83–91.

[12] T. Aven, On how to define, understand and describe risk, *Reliab. Eng. Syst. Saf.* **95** (2010) 623–631.

[13] W.W. Lowrance, Of Acceptable Risk: Science and the Determination of Safety, *J. Electrochem. Soc.* **123** (1976) 373C.

[14] R. Patriarca, and J. Bergström, Modelling complexity in everyday operations: functional resonance in maritime mooring at quay, *Cogn. Technol. Work*. (2017) 1–19.

[15] S. Caschili, and F.R. Medda, A review of the maritime container shipping industry as a complex adaptive system, *Interdiscip. Descr. Complex Syst.* **10** (2012) 1–15.

[16] N. Leveson, A new accident model for engineering safer systems, *Saf. Sci.* **42** (2004) 237–270.

[17] S. Dekker, P. Cilliers, and J.H. Hofmeyr, The complexity of failure: Implications of complexity theory for safety investigations, *Saf. Sci.* **49** (2011) 939–945.

[18] M. Grabowski, J.R.W. Merrick, J.R. Harrald, T.A. Mazzuchi, and J.R. van Dorp, Risk Modeling in Distributed, Large-Scale Systems, in: IEEE Trans. Syst. Man, Cybern. A Syst. Humans, 2000: pp. 651–660.

[19] Y.Y. Haimes, On the complex definition of risk: A systems-based approach, *Risk Anal.* **29** (2009) 1647–1654.

[20] T. Aven, On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience, *Risk Anal.* **31** (2011) 515–522.

[21] J. Vatn, Can we understand complex systems in terms of risk analysis?, *Proc.*

Inst. Mech. Eng. Part O J. Risk Reliab. **226** (2012) 346–358.
[22] N.G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, The MIT Press, Cambridge, Massachusetts, 2011.
[23] N.J. Bahr, System Safety Engineering and Risk Assessment: A Practical Approach, Second Edi, Taylor & Francis, Boca Raton, FL, 2015.
[24] S.D. Chatzinikolaou, and N.P. Ventikos, Critical Analysis of Air Emissions from Ships: Lifecycle Thinking and Results, in: Green Transp. Logist. Quest Win-Win Solut., 2016: pp. 387–412.
[25] L. Breedveld, Combining LCA and RA for the integrated risk management of emerging technologies, *J. Risk Res.* **16** (2013) 459–468.
[26] L. Sweet, and B. Strohm, Nanotechnology—Life-Cycle Risk Management, *Hum. Ecol. Risk Assess. An Int. J.* **12** (2006) 528–551.
[27] A. Decò, and D.M. Frangopol, Life-cycle risk assessment of spatially distributed aging bridges under seismic and traffic hazards, *Earthq. Spectra*. **29** (2013) 127–153.
[28] Z. Liu, Z. Ji, and Y. Lin, Life-Cycle Risk Evaluation for Offshore Platform Based-on Uncertain Grey-AHP Method, in: Proc. ASME 28th Int. Conf. Ocean. Offshore Arct. Eng. OMAE2009, ASME, Honolulu, Hawai, 2009.
[29] N.J. Ramadhan, Y.K. Wan, R.T.L. Ng, D.K.S. Ng, M.H. Hassim, K.B. Aviso, and R.R. Tan, Life cycle optimisation (LCO) of product systems with consideration of occupational fatalities, *Process Saf. Environ. Prot.* **92** (2014) 390–405.
[30] J.K. Lee, Integrated Risk Model for the Management of Ship Safety, in: First Work. Risk-Based Approaches Marit. Ind., 2007.
[31] H.J. Kang, Y.S. Yang, J. Choi, J.K. Lee, and D. Lee, Time basis ship safety assessment model for a novel ship design, *Ocean Eng.* **59** (2013) 179–189.
[32] D. Vassalos, Design for safety, risk-based design, life-cycle risk management, in: RINA Annu. Gen. Meet., 2014.
[33] J. Timmis, T. Knight, L.N. De Castro, E. Hart, L.N. de Castro, and E. Hart, An Overview of Artificial Immune Systems, in: Comput. Cells Tissues, Springer, Berlin, Heidelberg, 2004: pp. 51–91.
[34] Y. Ishida, Immunity-Based Systems: A Design Perspective, Springer-Verlag, Berlin Heidelberg, 2004.
[35] M. Negoita, Artificial Immune Systems — An Emergent Technology for Autonomous Intelligent Systems and Data Mining, in: AIS-ADM 2005, 2005: pp. 19–36.
[36] N. Bayar, S. Darmoul, S. Hajri-Gabouj, and H. Pierreval, Fault detection, diagnosis and recovery using Artificial Immune Systems: A review, *Eng. Appl. Artif. Intell.* **46** (2015) 43–57.
[37] E. Hart, and J. Timmis, Application areas of AIS: The past, the present and the future, *Appl. Soft Comput. J.* **8** (2008) 191–201.
[38] M.G. Perhinschi, H. Moncayo, and J. Davis, Integrated framework for aircraft sub-system failure detection, identification, and evaluation based on the artificial immune system paradigm, *AIAA Guid. Navig. Control Conf. Exhib.* (2009) 1–17.
[39] K.B. Ludvigsen, Digital Twins for Blue Denmark, 2018.