Learning from experience in the context of autonomous ships: an opportunity for a step change in generating safety knowledge?

N P Ventikos and K Louzis
Maritime Risk Group, Laboratory for Maritime Transport, School of Naval Architecture and Marine Engineering, National Technical University of Athens (NTUA), 9 Iroon Polytechniou St., Zografou 15773, Greece
E-mail: niven@deslab.ntua.gr, klouzis@mail.ntua.gr

Abstract. The maritime industry has been increasingly trying to incorporate more proactive approaches for safety both in the design and operation phases of the life-cycle of ships. However, learning from experience has remained a mostly reactive exercise in the aftermath of major marine accidents and its effectiveness is questionable considering the recurrence of accidents with common contributing factors. In addition, the development of autonomous ships that will be radically different and more complex systems begs the question whether learning needs to be redefined to ensure an adequate level of safety performance throughout their life-cycle. In this context, this paper presents a novel framework for managing risk knowledge inspired by the way the biological immune system remembers not previously encountered threats to implement a faster immune response when the same or similar threats are faced in the future. In this novel framework learning is described as a distributed life-cycle process with interacting components in the design and operation phases. As this framework is equally applicable to conventional and autonomous ships, the latter are considered an opportunity to change the way the maritime industry thinks about learning from experience.

1. Introduction
Learning from experience in the maritime industry has meant analysing mostly major accidents to understand how they occurred and implementing measures to avoid their recurrence. This reactive type of learning has led to large scale regulatory revisions that contribute to maintaining maritime safety. However, there is evidence that the industry is not effectively incorporating knowledge from experience as there are recurring accidents with common contributing factors. A most illustrative example is provided by Schröder-Hinrichs et al. [1], who have compared the accident of the Titanic in 1912 to that of Costa Concordia in 2012 and concluded that despite the technology being radically different the contributing human and organizational factors have essentially remained the same. The authors attribute this constant to the propensity of the industry to respond to accidents by implementing solutions that only address immediate causes, independently from one another, and are therefore ineffective to address the underlying conditions.

In addition, the complexity and novelty introduced to the maritime domain by the expected deployment of ships that will be operating with some degree of autonomy casts doubts as to
whether mainly depending on reactive learning will be sufficient for maintaining an adequate level of safety. Therefore, there is a need to implement more proactive and forward thinking approaches to learning. These approaches may rely on constant monitoring of the operational state of the system to improve the identification of unsafe states and the application of measures for reverting to a safe state. Subsequently, this information may be turned into knowledge that may provide meaningful feedback into the design process and used to modify operational parameters.

The objective of this paper is to highlight the limitations of the current approach to learning from experience in the maritime industry and propose a novel approach for risk knowledge management. This approach aims to change how we think about learning from experience by adapting the concept of immune memory that biological organisms use to increase the speed of their immune response in the future after having successfully dealt with a specific external threat. This is achieved by generating a memory of good safety solutions for complex marine systems that may provide feedback back to the design phase and increase the effectiveness of dealing with recurring safety threats during operation. This bio-inspired approach may be used for decision support, as well as for automated decision-making at lower and higher levels of autonomy respectively. In this context, we believe that the development of autonomous ship concepts may be an opportunity for a step change in how the maritime industry benefits from operational experience and generates meaningful knowledge to avert recurring maritime disasters.

The rest of this paper is structured as follows. Section 2 provides an overview of what learning from experience means in the maritime industry and how it is currently accomplished. Section 3 highlights the limitations in the learning process by reviewing the relevant literature and attempts to answer the question of how learning may change in the context of autonomous ships. Section 4 outlines the conceptual framework that forms the basis of our novel approach and includes a description of analogies with concepts from the immune system. Section 5 describes the novel framework for risk knowledge management and illustrates how it could work in practice through an example. The paper concludes with the benefits of the proposed change in thinking compared to the traditional approach to learning and some insight into the next steps of our research.

2. Learning from Experience in the Maritime Industry

Ships, like other industrial systems, are designed to operate under specific assumptions and constraints that may not hold during operation. The operational environment includes many factors, such as the weather conditions, the compliance of human operators to prescribed procedures, and pressures from the economic environment. Due to the stochastic nature of operational factors, there is an inherent limitation during design to define measures for controlling risk for every possible combination of conditions and system states. Therefore, the concept of learning in a safety context is an important element for continuous improvement of safety performance that complements the ability to foresee unwanted consequences that may arise during operation. According to Jacobsson et al. [2], learning (from incidents) is defined as the capability to avoid the recurrence of incidents and improve safety by taking measures based on the knowledge extracted from experience. This safety knowledge includes what kind of unwanted consequences may occur, their contributing factors, and how their occurrence and severity may be limited [3].

In the maritime industry, learning from experience has traditionally been based on a reactive approach that mainly focuses on investigating singular casualties with major consequences. The international instrument that regulates how marine casualties are reported and investigated is the Casualty Investigation Code [4] of the International Maritime Organization (IMO). According to this Code, a marine safety investigation involves the independent collection and
analysis of evidence, identification of causal factors (mechanical, human and organizational factors), and safety recommendations with the aim to prevent future casualties and incidents through regulatory amendments that may either affect ship design or operation. The Code stipulates that all marine casualties shall be reported but reserves mandatory investigation by the Flag State of the ship for very serious casualties that involves total ship loss or a death or severe damage to the environment. The investigation of casualties other than very serious is optional based on a vague criterion of the potential for preventing future casualties and incidents.

In addition to enabling learning from major accidents, the IMO also places shipping companies responsible for investigating incidents and casualties and using that information to improve their operational within the context of their Safety Management Systems (SMS); mandated by the IMO International Safety Management (ISM) Code [5, 6]. The ISM Code also includes a more proactive type of learning that comes from analysing near-misses, as defined in [7], which is based on the assumption that near-misses share common causes with casualties. A filtering process is recommended for selecting which near-misses will go through in-depth investigation based on, inter alia, the potential for loss and the likelihood of recurrence. The investigation includes the identification of causal factors and recommendations to address causes by revising company policies, practices, and procedures.

The maritime industry therefore places an emphasis on learning from experience to improve safety performance by involving all main actors of the maritime domain throughout the life-cycle of the ship. The IMO considers operational experience from major accidents (through Flag State investigations) to implement regulatory revisions, while shipping companies are obligated to learn from their experience to improve their operating procedures. Therefore, there are two distinct feedback loops for improving safety, one within operation and one from operation to the design phase. This approach is based more on reactive, rather than proactive, learning.

As part of the efforts to implement more forward-looking, proactive risk management approaches, the paradigm of Life-Cycle Risk Management has emerged. This is defined as a continuous, iterative process throughout the lifetime of a system that is combined with managing the knowledge generated in the different life-cycle phases by using information feedback loops [8]. The difference with the established, reactive learning is that this paradigm uses risk-based approaches in every phase of the life-cycle and is therefore anticipative and proactive. In the maritime industry, the most comprehensive descriptions of this concept have been provided by Lee [9] and Vassalos and Papanikolaou [10, 11]. The basic idea is that a risk model is constructed in the design phase and subsequently used in the operation phase for real-time risk monitoring, which in turn provides feedback both within operation and from operation to design. Continuous risk monitoring is the basic mechanism with which proactive learning from operational experience may therefore be implemented. In the same context, Kang et al. [12] have described a ship safety assessment model, which is used in operation as a monitoring and decision-making support tool and for updating a damage effects estimation database based on observations in operation.

3. Challenges in learning
According to a review of the learning from incidents literature from Stemn et al. [13], learning is the result of the interaction among several factors including what goes into the analysis (learning input), how the analysis is conducted (learning process), who conducts the analysis (learning agent), and in what conditions the analysis is conducted (learning context). The authors suggest that the quality of learning strongly depends on the organizational culture that supports the process, the competence of the learning agents, and the willingness of organizations to mainly focus on major accidents under external pressures (e.g., social, regulatory etc.). To better highlight the limitations of the learning input and process in the maritime industry, this paper will use the CHain of Accident Investigation steps (CHAIN) model proposed by Lindberg et
al. [14]. This model breaks the process of learning from accidents into the following steps: 1) Reporting of events that may be subject to investigation, 2) Selection of the candidates with the most promising potential for learning, 3) Investigation that involves the implementation of specific procedures and methodologies for analysing the collected information, 4) Dissemination of the analysis results to interested parties, 5) Prevention that involves making recommendations based on the lessons learned and implementing them for preventing future occurrences, and 6) Evaluation of the experience feedback process itself. To that we may add the process of storing information to a knowledge base for future reference, as described by Dupsteen and Guldenmund [15].

Even though casualty and incident reporting is mandatory in the maritime industry, it is considered that significant under-reporting exists. This means that a large number of incidents is never reported. In their study of maritime under-reporting, Psarros et al. [16] and Hassel et al. [17] have estimated that about 50% of the actual incidents may go unreported. It is obvious that this situation severely limits the opportunities for learning from experience. A similar problem has been observed for near-miss reporting, where near-misses are either not reported or do not provide useful information. This issue has been acknowledged by the IMO as being driven by factors such as, the fear of liability and complacency about known deficiencies [18]. Another issue that limits the learning potential is the publicly available accident reports mostly concern major accidents, while the data from shipping companies and P&I Clubs are confidential and are shared with the rest of the industry on a clearly voluntary basis [19].

Regarding selection of cases for in-depth analysis, Flag States mostly investigate accidents with major consequences and shipping companies are left to decide on their own which events to analyse based on consequence severity and likelihood of re-occurrence. Classification societies provide methodological guidance to companies for selecting which casualties and incidents to analyse. For example, DNVGL’s risk-based approach is implemented with risk matrices to prioritize events based on the frequency of occurrence and the severity of the consequences, while ABS evaluates learning potential mainly based on frequency and the presence of actual losses. In either case and even though the investigation of near-misses is encouraged, the focus remains on high-consequence and low-frequency events that excludes a large number of other types of incidents that may provide useful lessons from experience [13].

A significant limitation regarding the analysis of selected events relates to the assumptions, theories, and corresponding methods on which the investigation is based, either implicitly or explicitly. Hollnagel [20] has noted that, for example, root cause analysis implies the existence of a single or multiple sequence of events that led to the accident and therefore the investigation will try to detect such a sequence even if there is none to be found, adhering to the "What-You-Look-For-Is-What-You-Find" principle. In addition, even though the guidance from both the IMO and Classification Societies emphasize the need to uncover deeper organizational causes, and apply a systemic perspective, the sequential rationale remains the same. However, to maximise learning from experience requires shifting the focus of investigation from single point failures (either at the sharp or at the blunt end) to understanding how the interaction of factors led to the development of hazardous conditions and how the system as a whole may be improved.

Regarding the recommendations to prevent future occurrences, Pomeroy and Sherwood Jones [21] note that marine incident investigations are often too narrowly focused on single occurrences as the recommendations are restricted to addressing immediate causes that have been identified. Therefore, the recommendations do not have wider applicability to similar situations. In addition, since recommendations target identified causes, as though they were independent from each other, they are often ineffective towards improving work-as-done. For example, trying to ensure compliance to actually ineffective procedures rather sustains the delusion that work-as-imagined can be accomplished.

Adding to the limitations of the established reactive approach to learning, it is noted that
although the Life-Cycle Risk Management approaches (referred to in the previous section) conceptually include proactive learning through information feedback loops, they are still at an early stage of development [11]. Therefore, they do not provide any concrete methodological details as to how this could be implemented in practice. Even though the approach from Kang et al. [12] attempts to shed light on this issue by including the damage effects estimation database, the details of its structure and how it may be updated from real-time data have not been described in detail. Furthermore, it is understood that only consequences of adverse events are updated and not their probability, which provides a single-sided view of the overall risk picture.

Considering learning from experience and its limitations in the context of the future operation of autonomous ships begs the question whether the learning process will be required to change. Autonomous ships will likely represent a decidedly different and more complex system compared to conventional ships as they will include many innovative technologies and advanced software that have not been thoroughly tested in operation and for which past experience is simply nonexistent. For such systems, total reliance on the analysis of past experience for safety learning will probably prove ineffective, requiring more reliance on proactive risk analysis [22]. According to Pomeroy and Earthy [19], mostly relying on reactive learning in increasingly complex and digitalized ship systems will not be sufficient because complexity on one hand conceals the root causes and on the other hand gives rise to new types of incidents that have never been experienced before. For example, incidents that arise from the inability of the ship operators to understand how the system works, which is likely to result in poor diagnosis of symptoms and an inability to recognise a developing unsafe state.

We believe that the development of autonomous ships are an opportunity to change our thinking on how the industry learns from experience from a mainly reactive mode to a more proactive approach that would extract safety knowledge before an accident actually happens. This means that the main learning input would not be accident information but data that reflect the operation of the system and increase our understanding of its behaviour. According to Ale [23], the availability of big data that may be used to model and evaluate the behaviour of the system as a whole removes the necessity to pre-define what is considered a failure and therefore increases the effectiveness of proactive risk analysis by reducing the uncertainties of trying to imagine what can go wrong.

The following sections describe such an approach that takes cues from the biological domain and specifically the functionality of the immune system, which we consider as being a beneficial source of inspiration as it implements a learn-as-you-go approach to dealing with threats that the organism has never encountered before.

4. A conceptual bio-inspired framework
The immune system is a distributed and complex system of cells and molecules on which biological organisms depend for defence against foreign pathogens. The functionality of the immune system mainly depends on the mechanisms of detection and immune response [24]. The detection process involves distinguishing between the self, which includes own parts of the organism, and the nonself, which includes pathogens with the capacity to cause harm. The elimination process involves choosing the right effectors for a specific pathogen, while minimizing the damage caused to the organism. The immune system employs a multi-layered strategy to defend against pathogens that includes the innate and adaptive immune systems. The innate immune system provides a first level of defence with a pre-programmed (inherited) generic ability to detect and respond to certain types of pathogens, while the adaptive immune system identifies and responds to pathogens not previously encountered by the organism against which innate immunity is not sufficient by itself [24]. However, it is noted that the two systems are not independent because they interact to implement a combined immune response. The adaptive
immune system depends on a mechanism for learning, which is conducted during the primary immune response, and on a mechanism for retaining and re-using information (memory), which is conducted during the secondary immune response when the organism faces the same or a similar pathogen in the future. The benefit of this strategy is that the secondary immune response is a much faster process compared to the primary response and therefore the exponential replication of pathogens may be more effectively controlled to minimize the damage to the organism. The immune system uses a multitude of different components that interact in complex ways and therefore immune memory may be understood as a high-level behaviour or property of the system that emerges from the distributed functioning of multiple components. In addition, immune memory is associative as it is effective even for similar antigens to ones previously encountered, and robust as its functionality is not stopped even if some "memory cells" are lost [25].

Although immune memory is well understood as a high-level behaviour, how information are stored exactly has only been theorised so far. According to [26], the prevailing theories are clonal selection and immune network theory. The main difference between these theories is on how the information is retained by the immune system in the long run; either through "memory cells" or through a network structure that constantly mimics the presence of the pathogen [25]. In this paper we consider the immune system mechanisms of learning and memory as a way to bias the immune repertoire (antibodies) from a random structure to one that is more specific to the threats the organism has encountered in its environment [27]. The result is an effective improvement of the capability to detect threats by implementing a faster immune response and significantly reducing the probability of widespread damage.

In our previous work [28, 29] we have introduced a novel Life-Cycle Risk Framework, which describes a process for managing risk throughout the life-cycle inspired by the mechanisms of the biological immune system for dealing with threats throughout the lifetime of organisms. This is accomplished by a multi-layered risk management strategy that is distributed across the life-cycle phases and includes: 1) the Risk Control Options (RCOs) that are determined in the design phase and target known risks (analogous to innate immunity), 2) an Adaptive Risk Control functionality that targets unknown risks encountered during operation (analogous to adaptive immunity), and 3) a Risk Knowledge Management process that feeds information to both the operation and design phases (analogous to immune memory). This paper elaborates on the risk knowledge management process of our Life-Cycle Risk Framework and attempts to show the potential improvements in the traditional process for learning from operational experience by adapting ideas from the functionality of the biological immune system. The conceptual basis of our Life-Cycle Risk Framework includes the basic definitions shown in Table 1, which provide an analogy with the concepts of the immune system. It should be noted that a system state may be described as a set of safety indicators with values in defined ranges that remain constant or
Table 1. Definitions for the basic concepts of the Life-Cycle Risk Framework and analogies to concepts of the immune system.

| Immune system | System Description | Description |
|---------------|-------------------|-------------|
| Self          | Safe system state | Specific combination of conditions, external and internal, for which the system operates safely (i.e., with acceptable risk) |
| Nonself       | Unsafe system state | Specific combination of conditions, external and internal, for which the system operates with an increased likelihood of adverse consequences (e.g., increased probability of accident, unacceptable risk) |
| Antibody      | Detector of hazardous state | Classifier that distinguishes between safe/unsafe (self/nonself) |
| Immune response | Risk Control Options (RCOs) | Strategies to eliminate safety threats and revert the system to the safe state |

5. A bio-inspired approach to Risk Knowledge Management

In our bio-inspired framework, learning is based on gathering Risk Knowledge that is used to improve the capabilities to: a) recognise unsafe states (i.e., reduce false classification), and b) respond effectively to a given unsafe state and revert to a safe state. The continual improvement of the recognition and response capabilities enable the system to address the same or similar safety threats faster in the future and therefore reduce the risk of unwanted consequences. Improving the recognition capability is based on a dynamic redefinition of what is considered an unsafe state and is implemented by updating the designed detector set. Improving the response capability is based on recording successful risk control strategies for reverting to the safe state and correlating them to the specific unsafe state (effectively recording a state transition).

The gathered Risk Knowledge is part of two informational feedback loops, one within the operation phase of the life-cycle and one from operation to the design phase. The first feedback loop is used to improve the operation of ships or fleets of ships by updating the available detector repertoire and the corresponding RCOs. The second feedback loop is used to improve the design at a wider scale (e.g., by ship type) by reducing the uncertainty of the potential consequences (i.e., risk) from updated sets of unsafe states and redefining the corresponding RCOs. In addition, our framework considers how the system changes in the operation phase as it progresses from the growth and maturity towards the adaptation and aging sub-phase. This transition is accompanied by a potential increase in false classifications as a previously safe state could turn into an unsafe state considering the changes in the system parameters (e.g., reduced structural strength due to inadequate steel renewal - maintenance). To maintain an adequate level of safety performance, this situation would also require updating the available Risk Knowledge by updating the detector - RCO sets.

Figure 2 shows the bio-inspired framework for managing risk knowledge throughout the life-cycle, which includes distributed processes that form a closed loop between the design and operational phases. It is noted that the operational phase is further divided into sub-phases that reflect the potential changes in safety performance as the system develops throughout its...
Figure 2. Framework for Risk Knowledge Management throughout the life-cycle.

Life-cycle. Operation and maintenance is the sub-phase where the system grows and matures by steadily improving its safety performance through encounters with different known and unknown safety threats. Life extension is the sub-phase where the system may be adapted (e.g., through retrofitting), which changes the parameters defined during the design phase, and where the system ages, which signals a potential decline in safety performance. Emergency is the sub-phase where the system enters in case operational risk control fails to prevent an incident and consequence mitigation is required.

The Risk Knowledge Management framework involves an interaction between a risk knowledge base in the design phase that captures information on known risks and corresponding RCOs and an operational memory that captures information on newly encountered unsafe states and corresponding RCOs determined during operation. In the design phase, the risk knowledge base provides the definition of known unsafe states of the system that essentially reflect the known risks during operation as the uncertainty of being in such a state and of the potential consequences given a certain level of knowledge (see Equation 1). This conceptualization of risk is adapted from the $(A, C, U | K)$ risk perspective formulated by Aven [31].

$$\text{Unsafe states} \Rightarrow R = (ST, C, U | K)$$  \hspace{1cm} (1)

where, ST are the unsafe states, C are the potential consequences, U is the related uncertainty, and K is the level of knowledge. The definition of unsafe states provide the basis for determining detectors that distinguish between safe and unsafe states. The antibodies in the immune system have a y-shaped structure, where the arms are (randomly) variable and bind with specific pathogens and the tail is constant with a few variations and binds with different effector cells (e.g., macrophages, natural killer cells etc.) that determine the specific immune response [24]. Following this paradigm, the structure of the detectors is as shown in Equation 2 where they also correspond to specific RCOs that may be used to revert back to the safe state.

$$\text{Detector} = \left\{ \begin{array}{l}
\text{State} \\
\text{Safety Index given Risk} \\
\text{RCOs}
\end{array} \right\}$$  \hspace{1cm} (2)

where Unsafe state = \{Safety indicators with specific values\}, Safety Index = \{Safe, Unsafe\}, Risk = \{Acceptable, Not Acceptable\}, and RCOs = \{Measures specific to the unsafe state\}. 

[Table and Diagram]
Detector sets are initially defined in the design phase by training on specific data sets that include a description of system states with safety indicators and a known evaluation of the safety index (i.e., safe or unsafe). The training data sets should reflect the known risks that are recorded in the risk knowledge base. The designed detector sets form the detector repertoire that is the basis for monitoring risk during operation. In the design phase the safe/unsafe state (self/nonself) cannot be completely captured because the training data sets are necessarily limited and therefore there must exist some unknown combinations of safety indicators that correspond to an actually unsafe state that may be falsely classified as safe during operation. This situation is a "new" hazardous state that cannot be correctly identified given our designed recognition capability, i.e. the designed set of detectors.

However, the question is how we may be aware of a false classification in light of our belief that the system state is in a safe state. An indication could be provided by analysing the risk given the specific state, which would imply trying to predict how the system may respond to the specific conditions and what would be the likelihood of the potential consequences. It should be noted that such risk analysis must be forward-looking and depend on a holistic understanding of the operation of the system and not on identifying hazards that may or may not have occurred in the past. If there is a mismatch between the result of the detection process (e.g., Safety index = Safe) and the calculated level of risk (e.g., Risk = High) then a false classification would be assumed and the given state would be evaluated as unsafe. This information would subsequently be used to update the detector repertoire, which would make the detection of the same or similar state in the future faster because the detectors would classify it correctly and the risk analysis step would be avoided. However, real-time risk analysis is a resource intensive process and therefore it should be conducted for only a subset of "safe" classifications that are suspected to be false. For example, for situations that cannot be clearly classified as safe or unsafe, perhaps at the boundary between self/nonself.

A consequence of not being able to correctly identify a given state as unsafe is that RCOs would not be activated and therefore the situation has a high likelihood to result in unwanted consequences. If the misclassification is recognized then an Adaptive Risk Control process would take place to evaluate different combinations of available RCOs and choose the best one for minimizing the level of risk given the specific state. The result of this optimization process would be fed into the detector repertoire, which would make the response to the same or similar state in the future faster because the optimization step would be avoided. In case the Adaptive Risk Control process fails to revert the system to a safe state and an incident takes place, then the focus is shifted towards determining the best option for mitigating the potential consequences. The resulting RCOs would again be fed into the Risk Knowledge element for faster future reference. The Risk Knowledge element of this framework would therefore contain sets of "new" hazardous states that correspond to specific detectors and RCOs, as shown in Equation 3.

\[
\text{Risk Knowledge} = \left\{ \begin{array}{c} \text{States'} \\ \text{Detectors'} \\ \text{RCOs'} \end{array} \right\} \quad (3)
\]

The Risk Knowledge element subsequently provides feedback into the Risk Knowledge Base in the design phase, which will in turn provide input for redefining the unsafe states and for regenerating sets of detectors and RCOs. The updated information on the unsafe states provides a better understanding of the corresponding risk by increasing the knowledge on which risk is assessed and reducing the related uncertainties. Therefore, our risk understanding is updated as shown in Equation 4.

\[
R' = (ST', C', U' < U | K' > K)
\]

9
To better illustrate how this framework might work in practice, let us consider a hypothetical example of a conventional ship in a dangerous situation where the recognition of an unsafe state fails. The following is a brief description of the scenario under consideration. A ship is sailing at maximum service speed through an area where there is low visibility due to dense fog and dense marine traffic. In addition, the bridge team mainly depend on the on-board navigational equipment for verifying their position and the position of other vessels without maintaining a proper lookout for optical verification of obstacles. In this case, the state of the system may be described as shown in Equation 5.

\[
\text{State} = \begin{cases} \\
\text{Visibility} = \text{Low}, \text{Traffic} = \text{Dense}, \text{Speed} = \text{High}, \text{Situation awareness} = \text{Low} \\
\end{cases}
\]

Although this situation is not uncommon in ship navigation, it is the first time the particular crew on the particular ship had been in a similar situation. As a result, the state is falsely classified as safe and no RCOs are considered necessary. The corresponding detector is shown in Equation 6.

\[
\text{Detector} = \{\text{State}, \text{Safety Index} = \text{Safe}\mid \text{Risk Level} = \text{Acceptable}, \text{RCOs} = \emptyset\}
\]

However, a risk analysis of this state would reveal that there is an unacceptably high likelihood of a collision as a result of the high uncertainties relating to situation awareness due to the adverse weather conditions and that low visibility reduces the range of optical obstacle recognition. An additional risk factor would be the high speed of the vessel that reduces the ability to effectively take evasive action once an obstacle has been detected. Therefore, RCOs such as speed reduction would be warranted and the new detector would take the form shown in Equation 7.

\[
\text{Detector}' = \{\text{State}, \text{Safety Index} = \text{Unsafe}\mid \text{Risk} = \text{Unaccept.}, \text{RCOs} = \text{Speed reduction}\}
\]

The new detector would subsequently be used to update the detector repertoire in the operation phase with the result of faster implementation of the specific RCO the next time the same or a similar unsafe state is encountered because the risk analysis step would be avoided. In addition, the new detector would enrich the Risk Knowledge Base in the design phase of the life-cycle resulting in optimized RCOs to deal with similar situations. It is noted that our framework is equally applicable to conventional and autonomous ships but in the latter case the risk analysis step would need to consider additional factors, such as the difficulty of generating an adequate situation awareness from a remote control centre. The framework’s applicability to conventional ships may be translated into a system that provides decision support to the on-board crew, while for autonomous ships it may be easily automated, because it is a structured and systematic approach, and translated into a system that may be capable of making decisions to maintain an adequate level of safety performance.

6. Conclusions
This paper has attempted to highlight the importance of combining effective learning from experience with proactive approaches to safety, especially considering the possibility for autonomous ship operation. Traditional learning is the process of understanding how accidents occur and implementing measures to prevent them in the future. This process provides limited feedback to the design phase as the investigations focus too much on singular unwanted events and therefore cannot be easily generalized. Autonomous ships will be radically different and
more complex compared to conventional ships and therefore ensuring safe operation will require shifting how we think about learning from a pure reaction to accidents to learning pro-actively (i.e., before an accident occurs) during operation.

This paper has provided a high level description of a framework to manage risk knowledge inspired by the memory property of the immune system, which is part of a broader framework for managing risk throughout the life-cycle of marine systems that we are currently developing. Learning in our framework is described as a distributed life-cycle process that involves a risk knowledge base in the design phase, risk knowledge generation during operation, and two feedback loops - one within operation and one from operation to design. In addition, the process of learning is perceived as the ability to recognise unsafe states of the system and the ability to respond effectively and revert to a safe state. These capabilities are continuously improved during operation by adopting a structured learn-as-you-go rationale that efficiently exploits lessons from experience as the system faces new threats.

Our approach is a systematic way of exploiting safety knowledge from experience and reusing it to avoid unwanted consequences. This will be implemented by developing efficient bio-inspired algorithms that mimic mechanisms of the immune system, such as self/nonself discrimination and negative selection. Compared to the established, reactive approach, it shifts the focus from detecting root causes to detecting a hazardous system state that may signal the occurrence of unwanted consequences. In addition, experience from encounters with specific safety threats during operation is used to look for "similar" risks that may arise in different conditions. Therefore, the learning product is more easily generalizable and risk control becomes more robust by not being limited to taking measures that specifically fit a singular condition. Compared to the proactive, risk-based approaches in the context of Life-Cycle Risk Management, our approach describes an embedded risk knowledge management mechanism that updates the whole risk picture, including how threats are detected given unsafe states and what measures may be taken to counteract them. In addition, our approach employs a systems based rationale, compared to the classical risk modelling used in the existing approaches. This rationale supports learning by continuously and dynamically redefining how unsafe system states are described (i.e., what is considered dangerous in an operational context) given specific risk knowledge. Through this mechanism, the learning product may be more readily integrated in the operational risk knowledge and the risk knowledge base in the design phase. However, it should be noted that, given the early stages of development of these proactive learning approaches, a comprehensive comparison with our approach is currently not possible.

The proposed approach may be equally applicable to conventional ships implemented in the form of decision-support to the crew and to autonomous ships as an automated process. In light of this, we see the development of autonomous ship operation as an opportunity for a step change in how the maritime industry defines learning to benefit from operational experience and generates meaningful knowledge to avert recurring maritime disasters.

In the next steps of our research we will describe in more detail the processes involved in the risk knowledge management framework. Indicatively, our future research will include how risk knowledge gathered in the operation phase may be generalized for inclusion in the risk knowledge base in the design phase, how real-time risk analysis may be conducted during operation, how detectors may be updated through experience, and how RCOs may be generated and optimized during operation.

Acknowledgments
The work presented in this paper is part of an on-going PhD by Mr. Konstantinos Louzis and 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] Schröder-Hinrichs J U, Hollnagel E and Baldauf M 2012 WMU Journal of Maritime Affairs 11 151–167 ISSN 16541642
[2] Jacobsson A, Ek Å and Akselsson R 2011 Journal of Loss Prevention in the Process Industries 24 333–343 ISSN 09504230
[3] ESReDA 2015 Barriers to learning from incidents and accidents Tech. rep. European Safety, Reliability & Data Association
[4] IMO 2008 Resolution MSC.255(84), CASUALTY-RELATED MATTERS, Code of the International Standards and Recommended Practices for a Safety Investigation into a Marine Casualty or Marine Incident Tech. rep.
[5] IMO 1993 Resolution A.741(18)-International Management Code (ISM Code) for the safe operation of ships and for pollution prevention Tech. rep.
[6] IMO 2008 MSC.273(85) - Adoption of amendments to the International Safety Management (ISM) Code Tech. rep.
[7] IMO 2008 MSC-MEPC.7/Circ.7, Guidance on near-miss reporting Tech. rep.
[8] De Lemos T and Almeida L D 2001 Assessment and Management of Environmental Risks (Springer) pp 401–407
[9] Lee J K 2007 First Workshop on Risk-Based Approaches in the Maritime Industry
[10] Vassalos D 2014 RINA Annual General Meeting
[11] Vassalos D and Papanikolaou A 2015 12th International Marine Design Conference (Tokyo, Japan)
[12] Kang H J, Yang Y S, Choi J, Lee J K and Lee D 2013 Ocean Engineering 59 179–189 ISSN 00298018
[13] Stemm E, Bofinger C, Cliff D and Hassall M E 2018 Safety Science 101 313–325 ISSN 18791042
[14] Lindberg A K, Hansson S O and Rollenhagen C 2010 Safety Science 48 714–721 ISSN 0925-7535
[15] Drupsteen L and Guldenmund F W 2014 Journal of Contingencies and Crisis Management 22 81–96 ISSN 1468-5973
[16] Psarros G, Skjong R and Eide M S 2010 Accident Analysis and Prevention 42 619–625 ISSN 00014575
[17] Hassel M, Asbjørnslett B E and Hole L P 2011 Accident Analysis and Prevention 43 2053–2063 ISSN 00014575
[18] Storgård J, Erdogan I, Lappalainen J and Tapaninen U 2012 Procedia - Social and Behavioral Sciences 48 1010–1021 ISSN 18770428
[19] Pomeroy R V and Earthy J V 2016 Safety Science 1–13 ISSN 18791042
[20] Hollnagel E 2008 Remaining Sensitive to the Possibility of Failure (Resilience Engineering Perspectives, Ashgate Studies in Resilience Engineering vol 1) ed Hollnagel E, Nemeth C P and Dekker S (CRC Press, Taylor & Francis Group) pp 259–268 ISBN 978-0-7546-4641-9
[21] Pomeroy V and Sherwood Jones B 2006 Learning from Marine Incidents III
[22] Leveson N G 2011 Safety Science 49 55–64 ISSN 09257753
[23] Ale B 2016 Safety and Reliability 36 153–165 ISSN 0961-7353
[24] Holmeyr S A 2001 Design Principles for the Immune System and Other Distributed Autonomous Systems (Santa Fe Institute Studies in the Sciences of Complexity vol 3) ed Segel L A and Cohen I R (New York, USA: Oxford University Press) pp 28–36
[25] Smith D J 1999 Artificial Immune Systems and Their Applications ed Dasgupta D (Berlin, Heidelberg: Springer Berlin Heidelberg) pp 105–114 ISBN 978-3-642-59901-9
[26] Timmis J, Knight T, de Castro L N and Hart E 2004 Computation in Cells and Tissues (Berlin, Heidelberg: Springer) pp 51–91
[27] Perelson A S and Weisbuch G 1997 Reviews of Modern Physics 69 1219–1268
[28] Ventikos N P and Louzis K 2018 Technology and Science for the Ships of the Future (Trieste, Italy: IOS Press) pp 1042–1049
[29] Ventikos N and Louzis K 2019 (In Press) 18th International Congress of the International Maritime Association of the Mediterranean (IMAM 2019) (Varna, Bulgaria)
[30] INCOSE 2015 Systems Engineering Handbook. A Guide for System Life Cycle Processes and Activities 4th ed (Hoboken, NJ, USA: John Wiley & Sons, Inc.) ISBN INCOSE-TP-2003-002-03.2.2 publication Title: INCOSE-TP-2003-002-04
[31] Aven T 2010 Reliability Engineering and System Safety 95 623–631 ISSN 09518320