2019-06-07

Factors Affecting Cyber Risk in Maritime

Tam, Kimberly

Factors Affecting Cyber Risk in Maritime

Kimberly Tam
kimberly.tam@plymouth.ac.uk
University of Plymouth

Kevin Jones
kevin.jones@plymouth.ac.uk
University of Plymouth

***Abstract*—To ensure the safety of ships and ports, groups and individuals, at all levels of the maritime sector, use analysis to identify potential hazards and their outcomes. One of the most relied upon methods is using a risk assessment tool to define and prioritise threats. A disadvantage of most existing assessment frameworks, however, is their inability to update risks dynamically as factors, such as the environment, change. In the maritime sector, a range of dynamic factors is needed to measure risks, but most conventional frameworks are unable to use them to revise and update their risk profiles. In addition to static and dynamic, maritime operational risks can be affected by elements classified as cyber, cyber-physical, or physical in nature. This demonstrates the relatively equal presence of information and operational technology (i.e. IT/OT) used, however most quantitative risk assessment frameworks are normally limited to one or the other. This article explores the full range of cyber-related risk factor types within maritime in order to evaluate applicable risk frameworks and suggest improvements that could help each of those tools assess maritime-cyber risks specifically.**

***Index Terms*—cyber, dynamic, risk, maritime, cyber-physical**

I. Introduction

Maritime industries are responsible for transporting 90% of the world's goods [1], requiring widespread infrastructure and fleets of specially designed ships. Moreover this sector, worth trillions, has an unmatched reach across international waters and an increasing presence within the cyber domain. This exposes people and goods to a complex, diverse, range of factors that affect their risks; the top 2018 risk considered in maritime and shipping being business interruptions [2]. However, in a new development, cyber incidences (i.e., accidents, intentional attacks) are both a fast-rising and considerable threat to the maritime community, ranking as the 2^{nd} highest risk in 2018 [3]. This is a significant jump from five years ago, when it ranked 15^{th}. Since then, the vulnerabilities of a modern systems-of-systems ship layout and the high demands on international shipping has increased the risk of cyber-related accidents, but also the risk of an intentional exploit or attack. The recent Costco and Maersk incidences have drawn even more attention to the importance of cyber-risk management in the maritime industry, but with little understanding how that should be establish, particularly on ships at sea [4], [5].

In an attempt to prevent untoward situations, other industries have, in the past, adopted methods of risk assessment and prevention. It has been estimated that the maritime sector is roughly twenty years behind these industries [6], partially due to the slow progression of technological advancement. However, as seen with technology today and in the near future (e.g., autonomous, remote control, augmented reality), maritime has quickly reached the point where it needs to, more seriously, consider risk assessment procedures. In general, quantitative risk assessments are popular for evaluating and managing risk [7]–[10] and have been used to analyse specific physical, no cyber considered, ship risks [11]. Some of these assessment tools are also model-based (e.g., Coras [9]). The steps for risk assessment can be generalised in to three key steps, threat identification, assessment or modelling, and risk profile output. However, conventional risk assessments normally do these steps sequentially and in isolation to identify significant risks and maintain safety. This has the disadvantage of being entirely static, as it fails to adapt to changes in the factors and variations of risks as events take place. This has contributed to accidents in the past, such as the BP Texas refinery accident which killed 15 people and injured another 170 [12].

Although existing maritime risk assessment frameworks can evaluate physical risks, this sector needs to develop cyber-related risk management since existing solutions tend to be static and disregards dynamic factors. Therefore, the purpose of this article is to (1) examine how the maritime risk landscape can be modelled in terms of cyber, physical, static, and dynamic factors, (2) determine which are relevant for measuring maritime risk, and (3) determine if they are accounted for in existing frameworks. Specifically we evaluate National Institute of Standards and Technology (NIST [13], [14]), Failure mode and effects analysis (FMEA [15]), and Marine Cyber-Risk Assessment (MaCRA [16]). Section II covers background material for maritime and risk assessment. Section III analyses risk factors ranging through cyber, physical, dynamic, and static. Section IV looks at how current risk assessments cope with these risk factors, backed with survey data acquired for this paper, and concludes with Section V.

II. Background

Modern maritime security, including cyber-security, is a relatively new accepted concept [17]–[19], wrought from evolving Information Technology (IT) and Operational Technology (OT) systems. Shore-side port infrastructure has probably had its largest advancement in IT. At sea and on ships, however, IT and OT have advanced more equally. While individuals in this sector are familiar with physical risk assessment, they are less so with cyber. Hence this section is dedicated to understanding the current state of maritime technology and risk assessment methodology, which will then be broken down in Section III to determine what factors an ideal maritime cyber-related risk assessment method should measure to be fully effective.

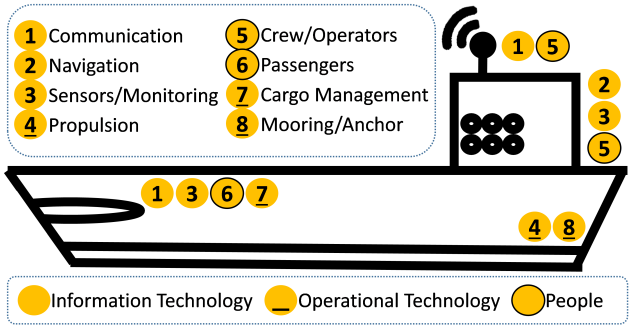

Fig. 1. General IT, OT, and human elements to be found on a generic ship.

A. Maritime Technology

The maritime sector is, and has been, a critical component in global trade and transportation. In its past, physical attacks like piracy were a common threat, and thus assessing those risks are well established. More specifically, risk factors like geographic location, cargo value, and attacker resources helped mariners and shipowners quantify the risks of certain voyages etc. The introduction of electronic systems, the first sonar being used on ships in the early 1900's, was then quickly followed by integration of cyber-systems both off-shore and in a ship's work environment. Each new system was introduced to decrease workloads and improve safety. Unfortunately, this resulted in the relatively quick development of a complex computing environment. Moreover, as they were primarily designed to improve efficiency and safety, these information and operational systems presented many cyber-security vulnerabilities. That said, it is impossible to discount the human element, which can add or mitigate risks [20], [21].

The introduction of larger, more technologically advanced ships, such as the modern oil tanker developed in the 1870's, the introduction of containerisation in the 1970's, and the continual evolution of passenger ships, has drastically changed the maritime risk landscape by introducing cyber and cyber-physical risks. This article defines cyber-physical primarily as attacks with both cyber and physical elements [22]. Much of the these attributes are the result of both information technology (e.g., navigation systems) and operational technology (e.g., propulsion systems). Because of all the physical operations required in shipping, the amount of physical and cyber factors are fairly even, particularly when compared to conventional computing systems. This mirrors other transportation sectors, however the magnitude of cargo volume and distance/time travelled within maritime is significantly more. Lastly, the most recent introduction of internet, complex networking (e.g., the Internet-of-things), and wireless communications has compounded the existing cyber-related risks in maritime. To help demonstrate this, Figure 1 shows the location of several IT, OT, and human elements on a generalised ship. The categories of the IT and OT systems are relatively generic and may encompass several systems (e.g., navigational ECDIS, AIS) but provides background info.

B. Risk Assessment Methodology

Within risk assessment methodology there are two core methods, qualitative and quantitative. While qualitative assessment focuses on prioritising individual risks based on probability of occurrences, the latter focuses on numerically analysing risk by assigning numerical risk values. Today, the majority of maritime physical risk assessments are based on probability statistics. These methods are quite reliable, supported by an extensive amount of historical statistics needed for risk assessment [23]–[25]. As discussed further in Section III, this makes it very difficult to develop a qualitative risk assessment framework for cyber-risks in maritime. Not only is there very little data, because of limit reporting abilities and as it a new, growing risk, but the evolution of maritime-cyber makes the data volatile enough that it is very difficult to develop reliable probabilities. This, in turn, makes it difficult to build a qualitative maritime cyber-risk assessment.

For the rest of this paper, the focus will be on quantitative risk assessments for the reasons above [7]–[9], [11], [16]. The majority of qualitative assessment methods make use of mathematical or computing models, which simplify the problem by only considering the factors that are relevant to the risk. Because of this, the benefits and negatives of this method depend on what elements are being modelled; their relevance, the quantity or set size, and the overall coverage of the set. Benefits of qualitative risk analysis is often more objectivity when derived from solid facts. Negatives of this approach have been experienced in the early days of the financial market, early 2000's, where a poor set range, or diversity, meant the model was unable to consider unusual tail events.

Many quantitative risk analysis models reduce these issues by reducing the problem, choosing a very specific scenario to analyse. This has been seen in [7] and [11], which can limit the problem to a specific target, geographic location, or outcome (e.g., ship collision). A model that encompass more elements can be used to assess more risks, however, the performance overhead from more computations can be hindering. Moreover, when complex models are mostly executed by human experts, there is a likelihood that errors will be introduced. Complex models can be difficult to understand as well, although it has been found that graphically displayed complex risks, as CORAS does, can improve understanding [26], [27].

III. Maritime Risk Factors

This article has briefly discussed IT (e.g., information sharing), OT (e.g., physical operations), and the human element in an maritime environment. These three have been considered the top categories of risk factors, however, each element belonging to these categories can be further categorised into static or dynamic, and physical or cyber factors that should be modelled to assess risk. This is particularly important in the maritime environment today, with the rise of cyber-physical systems [28]. This detail of element categorising is unusual in related works, and will allow this research to assess how effective existing risk assessments can be for maritime.

TABLE I
CATEGORIES OF KEY FACTORS TO CONSIDER WHEN ASSESSING MARITIME CYBER RISK ON SHIPS.

	Risk Factor	Static	Dynamic	Cyber	Physical
H	Crew_L	training, history*	health, resources	ID/password, internet use	location, health, devices (BYOD)
H	Operators_R	training, history*	health, resources	communication	health
H	Passengers_L	history*	health, resources	internet use, communication	location, health, devices (BYOD)
H	$\neg\text{Operators}_R$	history	resources, incentives	internet use, communication	location
IT	Navigation	protocols, hardware	software, use	software, network use	hardware (e.g., ECDIS, AIS, NAVTEX)
IT	Communication	protocols, hardware	software, use	ID, software, access	hardware (e.g., GMDSS, LRIT, SSAS)
IT	Sensors	hardware, network	devices*, use, software	network, access	hardware, locations
IT	Monitoring	hardware, network	software, use	access control, network	hardware, access
OT	Propulsion	hardware, mechanisms	use, environment	terminals, communication	mechanisms (propeller), access
OT	Cargo	contents*, history*	environment (temp)	tags, internal sensors	location, health
OT	Moor/Anchor	mechanisms, crew*	protocols, environment	protocols, communication	mechanisms, location, crew
OT	Engineering	crew*, mechanisms	environment (temp)	terminals, communication	mechanisms (engines), environment, crew

H - Human, IT - information technology, OT - operational technology, * - static if single voyage, dynamic if assessing longer period of time

A. Static Factors

Each of the following subsections for static, dynamic, physical, and cyber factors (i.e. Section III.A-III.D) will discuss how they affect risks within the human (H), IT and OT risk categories established earlier on. For the interested reader, more details on human threats (e.g., criminal, hactivists) can be found in [18], [29]. A mapping of risk factors can also be found in Table I to help demonstrate their connections to risk.

For the purpose of this paper there are four types of human categories, local on-ship crew ($crew_L$), remote operators ($operators_R$), on-ship passengers ($passengers_L$), and remote non-operator people ($\neg operators_R$). As local crew and passengers, if they exist, are unlikely to leave a ship mid-voyage, their history prior boarding are static factors. For a crewman this includes their training based on set standards. Although training standards change with the times [20], and there are slight variations across different groups, the training for a crew member is static at the point they are on a ship, as they are unlikely to receive extra training during a voyage. On the other hand, while the history of the individual people are static per voyage, it is likely to change as people disembark and embark at ports. These factors are important, as they establish previous criminal records or vulnerabilities (e.g., health, finance). Assessing human risk with both static and dynamic risk factors has been done previously [30], [31], although it has primarily been used on sex offenders, where static factors include history and dynamic factors include substance abuse. A significant shift in maritime that shall occur in the future is remote control and autonomy [16], which may shift crew risk factors towards remote operators.

Much like how the amount and types of people on-board differ between ship types (e.g., cruise, tanker), on-board IT systems also vary. However, because of standards set, and altered, by the IMO International Convention for Safety of Life at Sea [19], ships of similar types are mandated to have standard IT systems. These have been loosely categorised into navigation, communication (e.g., human to human, machine to machine), sensors, and monitoring. The last two were previously combined in Figure 1 as they possessed similar capture and network technology, however, their risk factors diverge more when considered in depth (Table I). Because of existing standards, the static factors of ship IT systems are primarily their hardware, established networks, and protocols to use those networks. Changes to these factors happen much less often than crew change, and even if hardware or physical network nodes are upgraded or otherwise changed, the ship is unlikely to undergo these alterations during normal operations. Instead, retrofitting normally stalls normal operations. Therefore the main risks to consider with these elements, is static vulnerabilities in the supply chain and maintenance. These static factors increase inherent risks. This could be structural issues, where IT system hardware is vulnerable physically, or in a cyber-sense, if a back door was built in for intruder access.

For OT this paper makes a distinction between hardware and mechanisms, although a mechanism could be considered a subset. Here, the term hardware is used in the computing sense while mechanisms, like a propeller or winch, have physical operations. Table I also differentiates propulsion from engineering unlike Figure 1. While the figure considered them nearly identical in terms of function and physical location on-board, risk factors in engineering have a much more diverse outcome and has more crew interaction. This differentiation may be even more pronounced in the future, as ship engineering OT is becoming more sophisticated and interactive with IT [32]. Risks from these static features tend to result in accidents, as the vulnerability is constant, while dynamic factors can be changed to trigger an attack. A flaw in computer hardware or OT mechanisms could lead to a damaging event, while a shortcoming in crew training could result in the mishandling of systems. For example, there was a rise in engineering-related accidents after a global shift to a new type of fuel [2].

B. Dynamic Factors

Being able to measure factors as they change is critical when analysing risk over a significant amount of time, or if elements are likely to change at a quick pace. Both are relevant to shipping, as voyages can take months, the life cycle of ship is an average of 20 years [33] (at least 5 years more than the average aircraft), and the speed at which cyber elements change can be relatively quick. Therefore, to fully analyse relevant shipping risks across a number of ships, environments, and scenarios, dynamic factors must be considered.

When assessing the dynamic risk factors of people, for those involved with shipping operations, remote and local, it is important to consider changes in "health", i.e. mental, physical, and financial. Threats to these could make an individual vulnerable to blackmail or manipulation from a malicious party, or become a malicious entity. Examples of sextortion and blackmail have been seen on ships, as well as disgruntled employees becoming insider threats and passengers accidentally leaking information [18], [29], [34]–[36]. These factors can change at any time, triggered by an event such as a fishing email. This is a common event on-shore (e.g. at a port), but also happens on a ship. Over a 5-day period, GTMaritime mail gateways scan a million messages, 31,836 of which are spam and 2,196 contain actual malware or viruses [37]. Of the last type of human considered, both non-crew and non-passenger, the only people of interest are malicious third parties. In the cyber-realm that means different types of hackers [16], along with physical attackers like criminals, or pirates, and those interested in warfare. Therefore, the only people who can affect maritime risk in the $\neg operators_R$ category are attackers, therefore the dynamic elements worth measuring are their resources and goals, which can easily change.

The primary dynamic factors for risk within maritime IT systems is their software and use. The majority of IT ship systems, particularly on the bridge (e.g., ECDIS, AIS, GMDSS, SSAS), are single purpose. The primary example is ECDIS (Electronic Chart Display and Information System), which has an underlying OS [38]. This OS, normally Windows but occasionally Linux, has the capacity to do many things but is used purely for executing ECDIS to navigate. This limitation on use can reduce the risks. However, there are enough use-cases (e.g., updating charts) and misuse cases that can affect risk dynamically. Unlike navigation, communication and monitoring (e.g., CCTV) systems, ship sensors have a plethora of applications. Moreover, the design of sensor networks and the cost/simplicity of individual sensors today means that sensor networks are versatile, dynamic, and spread widely. This is becoming more relevant with Internet-of-Things (IoT) in maritime, particularity in smart container tags for shipping. How sensor readings are made and stored, and how they affect decisions (i.e., man-made and machine-made), affect the risk of the ship. This includes cargo, which can be temperature sensitive or motion sensitive, people (e.g., carbon-dioxide levels), and the ship's physical and cyber safety.

The dynamic factors of OT are similar to IT in that they are also dependent on how they are used by other systems and people. Unlike IT, however, the amount of OT being operated by humans is much lower, as it is limited to a subset of the local crew. Very few OT systems allow remote control at this point in time, whereas ship IT systems are more connected to the Internet. This may change especially if more ships trend towards autonomy. As OT systems interact with the physical world, dynamic risks also include ship surroundings, such as sand banks and port structures. As the ship moves and environments change, these factors for measuring risks are uniquely dynamic in transportation sectors, such as maritime.

C. Cyber Factors

Measuring cyber risk has been done many times across various sectors and their systems. However, very little has been done in the maritime sector which has been estimated to be 20 years behind cyber-security trends [6] based on cyber-crime law and the rate of technological integration. Moreover the unique systems, protocols, and the movement across physical and cyber spaces mean that traditional methods of risk assessment cannot be easily applied without modification. However, the basic concept of communications human-to-human, machine-to-human, and machine-to-machine still affect risk. For human-cyber interactions, the factors to measure for risk are human identifications and security (e.g., ID cards, passwords), who they communicate with, and how. For remote operators and hackers this is the primary risk element to analyse. This is also a significant factor for local crew and passengers with easier, local, access. This same connection can be used to exploit people and propagate viruses [34], [37].

Within information technology, specialised navigation systems like ECDIS, as mentioned earlier, have a set of protocols for interactions with local networks and the wider Internet. This limits the risks to the use of those protocols, and the security of the network. Specialised communication technology like marine radio also have fixed use protocols, which can limit the possible risks. For more versatile networks, those hosting sensors, cameras and internet-based communications, they must consider user identification and passwords and user permissions. Particularly for CCTV and other sensitive monitors or sensors, access control is an important part of assessing risks. For a ship's cyber security it must also consider the physical patterns of crew and any existing passengers on-board, even more than the change of personnel in all other work environments. Not only is the timing and number of such changes significant, but on international voyages the nationalities and employers of people on-board can vary significantly. This is a fairly unique and potentially significant contributing factor to risk, with a significant dynamic aspect.

Of the three categories, operational technology on ships and at ports are the least Internet connected. However, this does not mean that they don't have some kind of networking technology involved (e.g., SCADA) or that this may not change in the future [32]. To access OT networks on ships it must be done at specific terminals, currently primarily in engineering instead of the bridge, a centre for IT systems. These networks have known vulnerabilities, however, because of the current access requirements, it is really only local crew that can affect these risks. SCADA and similar networks types enable cyber communications, although not with the same bandwidth and reach as the Internet, which can contribute to maritime-cyber risks. This can be seen in similar, yet different, studies of SCADA security in other sectors like water, power, and rail [39]–[42]. Because operational technology have both physical and cyber elements, their presence, scale in size, and uses mean that maritime security is equally, and uniquely, cyber and physically orientated when considering risk.

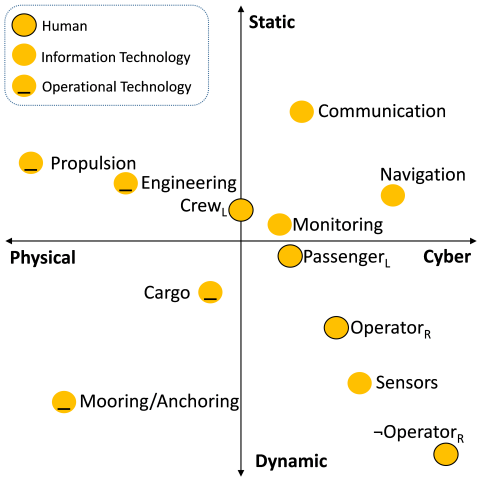

Fig. 2. Risk factor compass to show strongest influenced characteristics.

TABLE II
HIGH OVERVIEW OF RISK OUTCOMES GIVEN A FACTOR.

Risk Factor	Finance Loss	Loss of Life	Env. Damage
Crew$_L$	2 + [1-3]	2 + [1-3]	1 + [1-3]
Operators$_R$	3 + [1-4]	1 + [1-2]	1 + [1-2]
Passengers$_L$	2 + [2-4]	2 + [1-3]	1 + [1-3]
¬Operators$_R$	3 + [2-5]	2 + [1-3]	1 + [1-2]
Navigation	2 + [1-3]	3 + [1-4]	2 + [1-4]
Comms.	2 + [1-2]	2 + [1-3]	1 + [1-2]
Sensors	2 + [1-2]	2 + [1-3]	2 + [1-3]
Monitoring	1 + [1-3]	2 + [1-2]	1 + [1-1]
Propulsion	2 + [1-3]	3 + [1-4]	3 + [1-3]
Cargo	4 + [1-5]	3 + [1-5]	2 + [1-3]
Moor/Anchor	2 + [1-2]	2 + [1-2]	3 + [1-3]
Engineering	2 + [1-3]	2 + [1-3]	2 + [1-2]

$$Risk_{(F,L,E)} = StaticRisk + DynamicRisk[low - high] \quad (1)$$

Risk	1-None	2-Few	3-Some	4-Often	5-Severe
Static	No Risk	Inherent	Inherent	Inherent	pervasive
Dynamic	No Risk	Fluctuates	Fluctuates	Fluctuates	pervasive

D. Physical Factors

The last category of factors that affect maritime risk, as discussed here, is physical. For people, risk for operators, local and remote, and passengers is measured by their physical health and the devices they bring on board. This is becoming more important today with bring your own devices (BYOD) and the increase use of smart phones and USB enabled devices (e.g., e-cigarettes, cameras) that can spread malware. For physical outcomes, other risks can be tied to lithium batteries and other device components that can cause a physical hazard. For all human risk elements, location is another risk factor. For some this is static, as most cyber-attackers and remote operators do not change their physical location. However for people on a ship, their location is dynamic which may alter the risks involved. For example, close proximity to fishing, terrorist, or high-traffic hot spots affect different risks. Lastly, the human element affects IT/OT physical security as local crew, and sometimes passengers, can touch those systems.

For both IT and OT, there are physical components that can both affect risk and be affected by risks. The computational hardware of the systems need physical access security as well as cyber-access security. In addition, those that may be exposed to harsh environmental factors, like sensors, have different risks. This can include sensing equipment inside the ship, monitoring volatile cargo or the inner workings of the engines, or externally measuring the wind, water, etc. Outcomes of these vulnerabilities and risks will be discussed further in the next subsection. The main difference between IT and OT when considering physical risks is that, again, OT relies less on computing hardware and includes mechanisms like motors, robotic arms, and winches to perform tasks like propulsion and cargo handling. Furthermore, there is currently less automation with OT devices, requiring more physical interactions and command sequences from crew. Because OT interacts heavily with the environment (e.g., mooring to a pier, unloading cargo to a truck), physical elements that affect risk must be considered in order to fully assess maritime risks.

E. Risk Outcomes

The compass in Figure 2 demonstrates how factors of risk range across the physical, cyber, static, dynamic spectrum. Moreover, each category of human, IT, and OT are biased to certain quadrants of the compass due to their inherent natures. For example OT trends toward more physical, and remote humans tend to affect dynamic cyber risks more than local crew or passengers. This demonstrates how the unique blend of these factors create a distinct maritime risk landscape. However, before continuing to current risk assessment frameworks for maritime, and whether they aptly cover the range of factors for measuring risk, this section discusses the potential outcomes of these risks. Part of determining which risks require solutions is understanding the types of outcomes and their potential severity. The types of risk outcomes considered in this paper, which can be applied to human, IT, and OT entities, are denial-of-service (DoS), misdirect, damage, theft, and obfuscate. Ultimately, these risks can result in outcomes such as loss of finance, loss of life, and environmental damage.

Table II breaks down the potential severity of risk outcomes when considering the human, IT, and OT factors within maritime. Outcomes are shown ultimately as loss of life, finance, and damage to the surrounding environment. Each of these can be achieved with the types of attacks mentioned earlier (e.g., DoS). However, for now, only the ultimate outcome is considered. To estimate the severity of risk in each of these categories, when considering a certain factor, the level of risk is calculated from adding the static risk with the dynamic risk, see eq (1), both of which consider physical and cyber.

As previously mentioned, static risks are inherent in the design of a system or person (e.g., past behaviours) and they are unchanging. Therefore the risk associated is either non existent, or a constant risk. In Table II, this is shown with values 1 to 5, with the most severe level saying this risk can be found readily and with severe outcomes. Because dynamic risks can be a range of values depending on context, the dynamic risk value is shown as a range of potential values.

IV. Maritime Risk Assessment

Knowing how maritime factors affect risk, it is now possible to evaluate how well risk assessment tools can be applied to the unique maritime sector. The first requirement of a useful assessment framework is the ability to account for all factors of risk, which, as discussed in Section III, includes cyber, physical, static and dynamic. Secondly, the frameworks will be assessed on their prioritisation abilities, to determine the top risks and concerns so they can be dealt with immediately. Lastly, the risk assessment frameworks will be evaluated on their user-friendly aspect, namely if they are helpful in human-based decision making. Understanding how current risk frameworks achieve these three assessment goals will determine how they will need to change to adapt to maritime. In detail, we will gain an understanding of how these will need to change for future applications in ships and ports that are autonomous, remote-control, or use augmented reality.

A. Risk Framework Comparison

The risk frameworks that will be evaluated and compared are NIST, FMEA, and MaCRA (introduced in Section I). There are many NIST frameworks for assessing various risks, however, this article will focus on the management of IT systems [13] and Industrial Control Systems security (ICS) [14]. The latter is very similar to what is considered OT systems, however this is very specialised to manufacturing and distributions around the site, not national or international transportation. The NIST IT risk framework assumes that the physical and network security, once established, is set or static, but that would not be true if the systems were on-board moving ships. Another concern is that the two NIST frameworks are dissimilar and would need to be combined somehow to cover both physical and cyber risks. Moreover, the ICS risk framework is not versatile enough to assess maritime risks, while the IT framework is more applicable for just IT.

The most concerning limitation to NIST frameworks, however, is the lack dynamic risk measurements. This has been a factor in OT incidences, or more specifically ICS, and has previously resulted in loss of life [12]. Similarly, FMEA does not consider dynamic features, however, this is more clearly by design, as its purpose is to identify all possible failures in a design, process, product, or service in its early stages of design or re-design [15]. This makes FMEA a useful assessment tool for inherent flaws, or what this paper has labelled as static risk. This makes FMEA and NIST useful in static risk assessment, physical or cyber, but less so with dynamic risks. However, both these frameworks use gradients of risk in order to rank the risks they do analyse and prioritise risk management strategies. While highly effective in most environments, because of the wide range of risks in maritime cyber (see Figure2), they are likely to be less effective. With ranked risks one can prioritise fixing major flaws. If done thoroughly, FMEA could mitigate the dynamic risks once a ship is released, however, mitigate every risk no matter how minor is not cost effective, and during the lifetime of a ship (average 20 years) significant unseen risks can arise as global circumstances change.

TABLE III
Risk assessment framework comparison for maritime.

	NIST	FMEA	MACRA
Cyber Risks	✓✓	✓	✓✓✓
Physical Risks	✓✓	✓✓✓	✓✓
Static Risks	✓✓✓	✓✓✓	✓
Dynamic Risks	✓		✓✓✓
Well established	✓✓✓	✓✓✓	✓
Appropriate audience	✓	✓	✓✓✓

✓= some, ✓✓= yes, ✓✓✓= yes and integrated into framework

Unfortunately, the human element plays a minor roll in the NIST and FMEA frameworks discussed so far. Again, NIST has a separate framework for this (i.e., SP 800-53 Personnel Security) and it is not clear whether, if combined, they could cover the range of risks discussed for maritime. FMEA has branched into human error (e.g., health-care [43]), but it is also considered a separate use and not integrated with IT/OT assessments. While future ships may shrink crew sizes, it is highly unlikely that crew will be completely removed from the sector. It has been estimated that autonomous ships, with all life support systems removed, can reduce operational costs significantly [44], however, if a passenger ship already requires human safe conditions it is not worth the considerable risk of running those ships without a crew. Frameworks like NIST also suggest using a significant number of accessible specialists to combat such risks. The problem with this is, as seen in Figure 2, the scope of possible risk even on-board can be daunting. It would be unreasonable to expect sufficient levels of expertise on-board or remotely available, which is another issue to consider for maritime risk. Lastly, the targeted audience in the NIST documents are predominately high-level management and security experts, which is less relevant to the range of audience types actively interested in maritime security (see survey results in Section IV.B) and FMEA results can vary hugely depending on the investigation team.

The last framework evaluated is MaCRA [29], which is less tested but more maritime orientated (see Table III). This framework is relatively new and not well established, however it was destined specifically for maritime. Moreover, much focus has been placed on measuring dynamic risks as technology evolve, i.e. reactive, as seen in this assessment of autonomous ships [16]. Another drawback of this framework's early stages of development is the lack of widespread data required to calculate the risks. While an effort has been made to assess features in the maritime context, MaCRA does not assess static risks as thoroughly as dynamic, as those are established outside of shipping operations. However, a simple solution would be to feed FMEA data on static risks to MaCRA. As FMEA would not be applied to maritime context, but instead be used to assess the manufacturing plants and processes, it would not need to be heavily altered to successfully enhance MaCRA maritime risk assessments. This seems may be a more viable solution than merging parts of several NIST frameworks, create a new one for the missing dynamic aspect, and then ensure that they are applicable to marine.

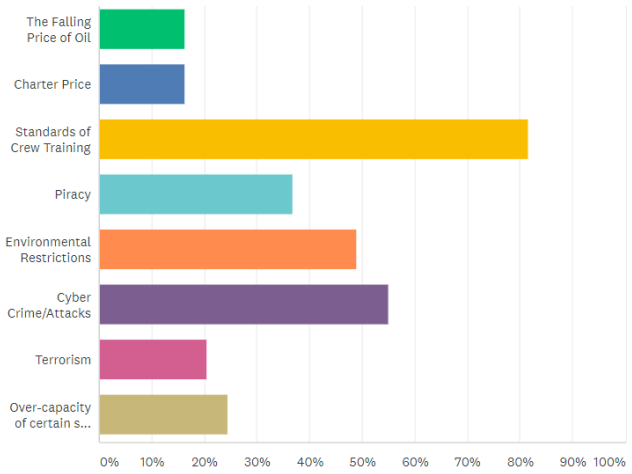

Fig. 3. Significant concerns facing the maritime industry.

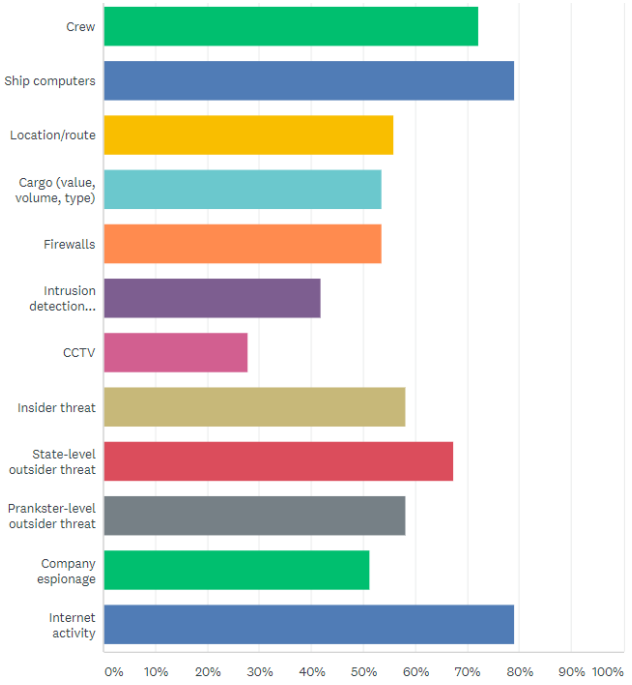

Fig. 4. Factors that have an effect on maritime cyber risks.

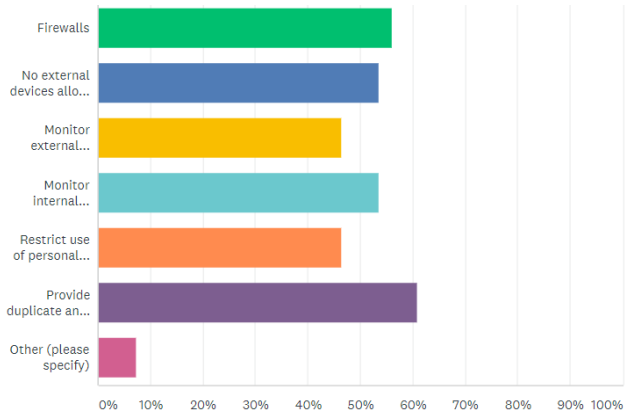

Fig. 5. Actions to reduce cyber risks in maritime.

B. Survey Results

To further assess the usability of certain frameworks, concerning maritime security, we conducted a survey for this paper. This survey consisted of 22 questions regarding maritime security factors, training, and use. Of the 55 participants, 45.5% of them were mariners and port officers, roughly 19% were trainers/trainees, 10% was higher management, and 6% were high ranking security specialists (e.g., chief information officer, information system security officer). The remaining participants included maritime services, equipment providers, regulators, insurers, IT system owners or support, and academics. It is important to note that only roughly 15% of these participants identified themselves as being a part of the targeted audience of the NIST frameworks examined [13], [14]. Moreover, FMEA primarily targets manufactures only, meaning it is applicable to roughly 5% of those who were interested enough in maritime cyber-security to take this survey. While 41% of participants were not familiar with risk assessment in general, however, 22% knew of NIST.

Of these participants, over 80% ranked crew training standards as the top problem, with cyber crime and attacks ranking at second with 56% (see Figure 3). Moreover, 57% of participants said that they have not received any training in cyber-security, and 80% of participants believe that specific maritime cyber training would be more useful to their daily tasks than generic cyber-security training. With regards to cyber incidences, participants thought IT was the most vulnerable technology at 51%, however 38% believed IT and OT were equally, and significantly, at risk. This demonstrates how both IT and OT need to be considered when assessing risk, which are more easily assessed with the existing FMEA and MaCRA frameworks. As described previously, NIST assesses IT very well, but is less capable of assessing IT/OT and humans blended together and, therefore, less applicable to maritime.

According to participants, their top three cyber crime concerns are malware (26%), phishing scams (16%) and web-based attacks (16%). Other surveys have had similar results with this query [45], [46]. However, these surveys rarely ask about what factors play into these risks. Even though these concerns seem primarily IT-based, and therefore can be solved with IT cyber-security solutions, in the maritime sector a wide range of physical, dynamic factors must be considered as seen in Figure 4. While ship computers and internet activity are ranked as critical cyber-factors by 79% of participants, over 50% of participants also identified ship location, route, cargo, crew, and insider threats as factors in risk. As shown in Sector III, these elements represent both dynamic and static factors.

This survey supports the idea that maritime cyber security is a mix of cyber, physical, static and dynamic elements. Moreover, participants confirmed that this range of elements should be considered while assessing the security of ships and ports. To better assess these assets in the future, it is therefore important to modify existing frameworks to work in the maritime ethos or to continue develop maritime-specific framework until they are equally well known and usable.

V. Conclusions

The maritime sector is not only a significant aspect of modern life and supports a multi-billion industry, nations depend on its services. Although relatively behind in terms of technology, it is becoming more imperative to consider maritime cyber-security to ensure safe and reliable operations. However, maritime is not new to risks, as physical risks are well understood. Moving forward, it is important to combine current physical risk assessment with cyber-knowledge, as well as consider static and dynamic risks. This paper demonstrated the importance of this by highlighting the types of factors (i.e., human, information technology, operational technology) that affect maritime risk and evaluating existing frameworks. It further evaluated these frameworks and examined maritime risks using results of a survey conducted for this article and from a wide range of participants. This helped us further conclude that there is no well-established risk assessment framework adequately suited for maritime, and suggest combinations or enhancements to current frameworks (i.e., NIST, FMEA, MaCRA) in order to improve maritime safety.

References

[1] International Chamber of Shipping, "Shipping and world trade," http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade, 2018.

[2] Allianz Global Corporate and Specialty SE, "Safety and shipping review," 2018.

[3] ——, "Allianz risk barometer," 2018.

[4] V. Rajamanickam, "COSCO's cyber attack and the importance of maritime cybersecurity," *FreightWaves*, July 2018. [Online]. Available: https://www.freightwaves.com/news/technology/coscos-cyber-attack-and-the-importance-of-maritime-cybersecurity

[5] Maersk, "A. P. Moller Maersk improves underlying profit and grows revenue in first half of the year," 2017. [Online]. Available: https://edit.maersk.com/en/the-maersk-group/press-room/press-release-archive/2017/8/a-p-moller-maersk-interim-report-q2-2017

[6] K. Belmont, "Maritime cybersecurity: Cyber cases in the maritime enviroment," American association of Port authorities, 2016.

[7] F. Flammini, A. Gaglione, N. Mazzocca, and P. C, "Quantitative security risk assessment and management for railway transportation infrastructures," International Conference on Critical Information Infrastructure Security, 2008.

[8] NIST, "Guide for conducting risk assessments - information security," NIST Special publication 800-30, 2012.

[9] M. S. Lund, B. Solhaug, and K. Stlen, *Model-Driven Risk Analysis: The CORAS Approach*. Springer Publishing Company, Incorporated, 2010.

[10] T. Sommestad, M. Ekstedt, and H. Holm, "The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures," *IEEE Systems Journal*, 2013.

[11] T. Chai, J. Weng, and X. De-qi, "Development of a quantitative risk assessment model for ship collisions in fairways," *Safety Science*, 2017.

[12] BP, "Fatal accident investigation report," Isomerization Unit Explosion Interim Report, 2005.

[13] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," NIST 800-30, 2002.

[14] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to industrial control systems (ics) security," NIST 800-82r2, 2015.

[15] H.-C. Liu, L. Liu, and N. Liu, "Risk evaluation approaches in failure mode and effects analysis: A literature review," *Expert Systems with Applications*, 2013.

[16] K. Tam and K. Jones, "Cyber-risk assessment for autonomous ships," IEEE TCS Cyber Security, 2018.

[17] NATO, "Alliance maritime strategy," 2018. [Online]. Available: http://www.nato.int/cps/en/natohq/official_texts_75615.htm

[18] BIMCO, CLIA, ICS, Intercargo, Intertanko, OCIMF and IUMI, "Guidelines on cyber security onboard ships," BIMCO 2.0 ed. Bagsvaerd, 2017.

[19] International Maritime Organization, "International convention for the safety of life at sea," IMO, 1974.

[20] M. Wingrove, "Lack of training causes ship accidents and detentions," Marine Electronics & Communications, 2016.

[21] A. Rothblum, "Human error and marine safety," International Workshop on Human Factors in Offshore Operations (HFW2002), 2000.

[22] K. Tam and K. D. Jones, "Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping," *Journal of Cyber Policy*, 2018.

[23] J. Montewka, S. Ehlers, F. Goerlandt, T. Hinz, K. Tabri, and P. Kujala, "A framework for risk assessment for maritime transportation systemsa case study for open sea collisions involving ropax vessels," *Reliability Engineering & System Safety*, 2014.

[24] J. Nordstrm, F. Goerlandt, J. Sarsama, P. Leppnen, M. Nissil, P. Ruponen, T. Lbcke, and S. Sonninen, "Vessel triage: A method for assessing and communicating the safety status of vessels in maritime distress situations," *Safety Science*, 2016.

[25] F. Goerlandt and J. Montewka, "Maritime transportation risk analysis: Review and analysis in light of some foundational issues," *Reliability Engineering & System Safety*, 2015.

[26] K. Labunets, F. Paci, F. Massacci, and R. Ruprai, "An experiment on comparing textual vs. visual industrial methods for security risk assessment," in *2014 IEEE 4th International Workshop on Empirical Requirements Engineering (EmpiRE)*, 2014.

[27] T. Stålhane and G. Sindre, "An experimental comparison of system diagrams and textual use cases for the identification of safety hazards," *Int. J. Inf. Syst. Model. Des.*, 2014.

[28] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Design Automation Conference*, 2010.

[29] K. Tam and K. Jones, "MaCRA: A model-based framework for maritime cyber-risk assessment," *WMU Journal of Maritime Affairs*, 2019.

[30] J. Bonta, "Approaches to offender risk assessment: static vs dynamic," Research summary Vol. 4 No. 2, 1999.

[31] A. Beech, C. Friendship, M. Erikson, and R. K. Hanson, "The relationship between static and dynamic risk factors and reconviction in a sample of u.k. child abusers," *Sexual Abuse: A Journal of Research and Treatment*, 2002.

[32] Y. Man, M. Lundh, and S. N. MacKinnon, "Managing unruly technologies in the engine control room: from problem patching to an architectural thinking and standardization," *WMU Journal of Maritime Affairs*, 2018.

[33] International Chamber of Shipping, "Review of maritime transport," *United Nations Conference on Trade and Development (UNCTAD)*, 2018.

[34] U.S. Army Criminal Investigation Command, "Cyber sextortion," CPF 0002-17-CID361-9H, 2017.

[35] CyberKeel, "Maritime cyber-risks," NCC Group Publication, 2014.

[36] ESC Global Security, "Maritime cyber security white paper: Safeguarding data through increased awareness," ESCGS Cyber Security White Papers, 2015.

[37] GTMaritime, "Cyber security in the maritime industry," 2017. [Online]. Available: https://www.gtmaritime.com/cyber-security-maritime-industry/

[38] CyberKeel, "Security risks and weaknesses in ecdis systems," NCC Group Publication, 2014.

[39] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers & Security*, 2016.

[40] J. Leyden, "Water treatment plant hacked, chemical mix changed for tap supplies," The Register, 2016.

[41] H. H. Safa, D. M. Souran, M. Ghasempour, and A. Khazaee, "Cyber security of smart grid and scada systems, threats and risks," in *CIRED Workshop 2016*, 2016.

[42] R. Collins, "The state of cybersecurity in the rail industry," White paper, 2017.

[43] B. Streimelweger, K. Wac, and W. Seiringer, "Improving patient safety through human-factor-based risk management," *Procedia Computer Science*, 2015.

[44] D. MORRIS, "Worlds first autonomous ship to launch in 2018," http://fortune.com/2017/07/22/first-autonomous-ship-yara-birkeland/, 2017.

[45] W. Daszuta and S. Ghosh, "Seafarers' perceptions of competency in risk assessment and management: an empirical study," *WMU Journal of Maritime Affairs*, 2018.

[46] BIMCO, Fairplay, and ABS, "Maritime cyber survey 2018 - the results," IHS Markit, 2018.