MARITIME CYBERSECURITY RISK MANAGEMENT: A DISCUSSION ON CURRENT AND FUTURE REGULATORY COMPLIANCE APPROACHES

Christos Kontovas[1*], Chia-Hsun Chang[1]

[1]Liverpool John Moores University, Liverpool, L3 3AF, United Kingdom

(*c.kontovas @ ljmu.ac.uk)

Abstract

The evolving landscape of cybersecurity in the maritime industry poses significant challenges due to inadequate security controls for vulnerable onboard systems. Recognising these risks, the International Maritime Organization (IMO) has mandated that cyber risk management be integrated into safety management systems in alignment with the ISM Code. Effective cyber risk management requires a holistic approach, addressing diverse threats and their potential impact on both individual systems and overall ship safety and environmental protection. This paper examines the regulatory framework underpinning maritime cybersecurity and highlights its reliance on methodologies adapted from the Information Technology (IT) industry. This shift marks a departure from traditional safety and environmental risk management practices historically employed by the IMO. This paper explores a novel cyber risk management approach proposed by the International Association of Classification Societies (IACS), and a case study is presented to illustrate its applicability. This framework provides a comprehensive strategy that integrates IT and Operational Technology (OT) systems, addressing the complexities of interconnected onboard and external networks. By presenting this approach, the paper contributes to advancing cybersecurity in the maritime sector, offering a promising solution to current challenges and laying a foundation for future resilience in maritime operations.

Keywords

Maritime Cybersecurity, Risk Assessment, Cyber risk, Cyber security

Please cite as follows:

Kontovas C. and C.H. Chang (2025) "Maritime Cybersecurity Risk Management: A Discussion on Current and Future Regulatory Compliance Approaches", Proceedings of the IAME Conference 2025, 25-27 June, Bergen, Norway.

1 Introduction

The maritime industry is the cornerstone of global economic sustainability. According to UNCTAD (2024), over 80% of international trade by volume is transported by sea, underscoring the industry's critical role in facilitating global commerce. The shipping industry has historically focused on safety considerations, ensuring the safe transport of goods across the world's oceans. In recent decades, the industry has addressed a range of security-related issues, including the prevention of piracy and armed robbery against ships, counter-terrorism measures, and the prevention of drug smuggling and other illicit activities. With the advent of digitalisation, the industry is increasingly integrating advanced software and hardware systems both on vessels and within shore-based infrastructure. The growing reliance on information technology (IT) in international trade has heightened concerns about cybersecurity (Kanwal et al., 2022). These cybersecurity concerns are not limited to the shipping industry but extend to all modes of transport. The increased use of autonomous systems further exacerbates these concerns (Chang et al., 2021).

It can be argued that much of the global maritime safety policy has been developed reactively, in response to serious accidents that have resulted in human casualties and environmental damage, such as oil spills (Kontovas and Psaraftis, 2009). This reactive approach has been questioned by the industry, arguing that the maritime industry should not wait for accidents to occur before modifying existing rules or proposing new ones. Instead, a proactive safety culture that anticipates hazards before they result in accidents has been widely adopted in other industries, such as nuclear and aerospace. The international shipping industry has begun to adopt this proactive approach through the implementation of 'Formal Safety Assessment' (FSA), a risk-based methodology adopted by the International Maritime Organisation (IMO) primarily used for safety-related assessments.

Risk assessment and risk management are generally preferred methods for addressing various risks, including safety, environmental, security, and cybersecurity risks. The shipping industry has a long tradition of employing risk-based and risk-informed approaches. Specifically, the academic literature on cybersecurity risk assessment and management is continually expanding. Bolbot et al. (2022) conducted a literature review and bibliometric analysis of maritime cybersecurity-related literature and highlighted those studies on 'Cyber risk assessment and treatment' constitute the largest category. Numerous methods are reported to be used for cybersecurity risk assessment and treatment in the maritime sector, particularly in academic literature (Bolbot et al. 2020, 2022; Erbas et al., 2024). Current maritime cybersecurity risk assessments are conducted using either qualitative analyses, such as System-Theoretic Process Analysis (STPA), Hazard Identification (HAZID), Failure Mode and

Effects Analysis (FMEA), and Bayesian Networks (Park et al. 2023), or traditional quantitative risk analysis methods, such as Bow-Tie analysis (Progoulakis et al., 2021; Park et al. 2024) and risk matrices (Yoo and Park, 2021).

However, the purpose of this paper is not to discuss the academic literature but rather to explore approaches related to regulatory compliance at a global level, specifically the requirements set by the IMO. In 2017, the IMO adopted its first guidelines on 'Maritime Cyber Risk Management'- hereafter referred to as the IMO Cyber Guidelines (see IMO, 2017a). These were essentially based on the industry-led work published by BIMCO (BIMCO, 2016) - hereafter referred to as the BIMCO Guidelines. The IMO also emphasizes integrating cybersecurity into the Safety Management System (SMS), and with IMO Resolution MSC.428(98), it requires Administrations (i.e., Member States) to ensure that cyber risks are appropriately addressed in safety management systems (IMO, 2017b).

The IMO Guidelines highlighted that risk management has traditionally focused on operations in the physical domain to support safe shipping. However, *"greater reliance on digitization, integration, automation, and network-based systems has created an increasing need for cyber risk management in the shipping industry"* (MSC-FAL.1/Circ.3/Rev.2[1]). For guidance on cyber risk management, the IMO Cyber Guidelines refer to standards such as the ISO/IEC 27001 (ISO,2022) standard on Information Technology and the United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST 2.0 Framework) (NIST,2024).

Given that much work on managing cyber risk, particularly for IT systems, has been performed in other non-maritime sectors, there has been an increased use of such tools or their adaptation to the maritime environment. This shift represents a significant change in risk management mentality within the shipping industry, which has traditionally relied on classical frameworks for managing risks, such as the Formal Safety Assessment. A clear example of the introduction of these 'new to the maritime industry approaches' can be seen in the very definition of risk; in a safety context, risk is defined as the combination of probability/frequency and consequences. In IT-related standards such as ISO-IEC 27005:2024, information security risks are associated with the potential for threats to exploit vulnerabilities. Similarly, the BIMCO Guidelines define risk as a combination of impact and likelihood, with the latter being a combination of vulnerability and threat.

[1] In this paper we cite IMO documents using the standard code for MSC (FAL) publications; for example MSC (F) x/y/z, where x is session, y is agenda item, and z is document number of agenda item. IMO documents and Circulars do not appear in the reference list of this paper.

However, recent submissions to the IMO, such as one by the International Association of Classification Societies (IACS) (see IMO doc. MSC 108/INF.11), propose a risk assessment approach to be incorporated into safety management systems that is more aligned with traditional safety-related risk assessment and can offer a holistic approach covering both IT and OT (operational technology) systems.

To this end, this paper will present an overview of the relevant approaches and focus on the latest developments that might bring back a traditional risk management approach to the maritime cybersecurity domain. The rest of the paper is structured as follows: Section 2 explores historical and contemporary approaches to risk management, with a focus on cybersecurity, including case studies demonstrating the application of newer methodologies. Section 3 introduces the innovative maritime cybersecurity risk management framework outlined in IACS Recommendation 171, illustrated with a case study on Electronic Chart Display and Information System (ECDIS). Suggestions for future research are integrated into the discussion of the case study and presented in the Conclusions, Section 4, which also includes a concise comparison with other regulatory compliance strategies.

2 Discussion on Current Risk Management Approaches

2.1 Risk Assessment: Historical Developments at the IMO

2.1.1 Formal Safety Assessment: Risks related to maritime safety and environmental protection

The Formal Safety Assessment (FSA) was probably the first risk assessment technique employed by the IMO. It is described as "*a rational and systematic process for assessing the risk related to maritime safety and the protection of the marine environment and for evaluating the costs and benefits of IMO's options for reducing these risks"* (see FSA Guidelines in MSC Circ. 1023).

FSA originates from the tradition of technical risk assessment, with methods tracing back to the Nuclear Industry in the 1960s. Similar approaches were used in Quantitative Risk Assessment (QRA) and the industrial regime in Norway, as well as the 'Safety Case' regimes in the United Kingdom (UK) offshore industry. The FSA Guidelines have their roots in the 1992 UK House of Lords report on ship safety (the so-called Lord Carver report) and the original proposal of the FSA concept to the IMO by the UK in MSC 62 (1993). This was followed by the FSA Interim Guidelines in 1997 and the 2001 FSA Guidelines adopted in MSC 74. The FSA Guidelines have since been superseded by MSC-MEPC.2/Circ.12/Rev.2 (April 2018), with the latest revision (Rev.3) approved by MEPC in December 2024 and awaiting approval at the next MEPC; see IMO (2018).

To achieve its objectives, the IMO's guidelines on the application of FSA recommend a five-step approach: hazard identification, risk assessment, risk control options, cost-benefit assessment, and recommendations for decision-making. FSA is a traditional risk assessment approach focused on justifying IMO's rules and regulations. Step 4 of the process examines the economics of proposed measures to address risks and whether their costs outweigh societal benefits. Initially, FSA primarily addressed human safety but was later updated to include 'Environmental risk evaluation criteria on prevention of oil spill from ships', thus encompassing risks related to oil spill protection. Some academic papers have explored incorporating other aspects into FSA, such as security (Yang, 2016), air pollution, CO2 emissions (Kontovas and Psaraftis, 2010), and the impact of collisions with whales (Sèbe et al, 2019). Currently, FSA addresses events involving fatalities, injuries, ship loss or damage, other property loss or damage, or environmental damage. While it could be extended to cover all the aforementioned domains, including cybersecurity, it has primarily been used for safety and oil pollution. It is worth noting that FSA follows the essential steps of a risk assessment methodology in line with ISO 31000:2009, which provides principles and generic guidelines on risk management as codified by the International Organization for Standardization (ISO).

2.1.2 Maritime Security – The ISPS Code

The International Ship and Port Facility Security Code (ISPS Code) is a comprehensive set of measures designed to enhance the security of ships and port facilities. It was developed in response to perceived threats to ships and port facilities following the 9/11 attacks in the United States. The Code aims to provide a standardised, consistent framework for evaluating risk, enabling Member States to offset changes in threat with changes in vulnerability for ships and port facilities by determining appropriate security levels and corresponding security measures.

Security assessments under the ISPS Code focus on identifying and evaluating risks to ensure that appropriate security measures are in place to mitigate these risks. This includes assessing the security of ships and port facilities, identifying potential threats, and implementing measures to reduce the likelihood and impact of security incidents. The definition of risk in the relevant guide for maritime security and the ISPS Code (IMO, 2021) encompasses three key components: threat, vulnerability, and impact. In the security context, the IMO approach thus deviates from the classical risk concept of probability and consequence, introducing vulnerability (i.e., weaknesses or gaps in security that could be exploited by a threat) and defining impact as the potential consequences or severity of damage if the threat were to exploit the vulnerability.

2.2 Maritime Cybersecurity Management

Maritime cybersecurity has been on the IMO agenda for over a decade. Canada submitted a document entitled ‘Measures toward enhancing maritime cybersecurity’ (see IMO doc. FAL 39/7) to the 39th meeting of the IMO's Facilitation Committee (FAL), proposing *"the development of Guidelines on maritime cybersecurity in light of the dramatic increases in the use of cyber systems across the maritime sector and related risks".* A follow-up submission by Canada and the United States (MSC 94/4/1) to the 94th MSC meeting (September 2014) highlighted the need for cybersecurity guidelines specifically developed for the maritime sector to *"help protect ports, terminals, vessels, and other stakeholders, as well as help mitigate the effects of successful attacks and intrusions and prevent disruptions to international trade, by providing guidance on areas of cybersecurity".*

With cooperation between the two committees (MSC and FAL), the first attempt to address the issue was MSC.1/Circular.1526 – Interim Guidelines on Maritime Cyber Risk Management – (June 2016). These guidelines were short-lived and were replaced by a circular issued by both committees as MSC-FAL.1/Circ.3, ‘Guidelines on Maritime Cyber Risk Management ‘(July 2017). By resolution MSC.428(98) ‘Maritime Cyber Risk Management in Safety Management Systems’, the Guidelines linked cyber threats with the ISM Code, which had been in place since the mid-1990s. Various guidelines and guides for maritime cybersecurity were developed, such as the BIMCO Guidelines mentioned in the introduction and those published by major Classification Societies such as Lloyd's Register, the American Bureau of Shipping, and DNV (Det Norske Veritas).

Fast-forward to 2024, the initial BIMCO Guidelines have been revised multiple times, with the latest (fourth) version made available in December 2020. An updated version of the IMO circular MSC-FAL.1/Circ.3/Rev.3, ‘Revised Guidelines on Maritime Cyber Risk Management’ was approved by the IMO’s Maritime Safety Committee meeting (MSC 108) in May 2024. The IMO Cyber Guidelines present a high-level approach to cyber risk management and urge users to refer to Administration requirements, as well as relevant international and industry standards and best practices. The mentioned standards include the ISO/IEC 27001 standard on Information Technology and the International Association of Classification Societies (IACS) Unified Requirements (UR) E26 ('Cyber resilience of ships') and E27 (‘Cyber resilience of onboard systems and equipment’). The Guidelines and industry documents referenced are the BIMCO Guidelines, the Consolidated IACS Recommendation on cyber resilience (Rec 166), the United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST 2.0 Framework), and the IAPH Cybersecurity Guidelines for Ports and Port Facilities.

2.3 The distinction between Information Technology (IT), Operational Technology (OT) and Computer-based Systems (CBS)

Before getting into the core approach of this paper, it is essential to clarify the distinction between IT and OT systems. Notably, these are not defined in the ISO/IEC 27000 family standards or the US NIST 2.0 Framework. In September 2023, NIST published NIST SP 800-82 Rev. 3 ('Guide to Operational Technology Security') as a separate document, providing guidance on securing OT. OT is defined as encompassing *"a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment)"* (NIST,2024). To the best of our knowledge, this definition and the related approach have not been specifically applied in a maritime context.

According to the IMO Guidelines (MSC-FAL.1/Circ.3/Rev.2), IT systems focus on "*the use of data as information,"* while OT systems focus on *"the use of data to control or monitor physical processes".* The BIMCO Guidelines further elaborate that IT "*covers the spectrum of technologies for data storing and processing, including software, hardware, and communication technologies"*, whereas OT *"includes hardware and software that directly monitor/control physical devices and processes, typically on board"* (IMO,2022).

The IACS UR E26 defines IT as "*devices, software, and associated networking focusing on the use of data as information"*, contrasting with OT, which is defined as *"devices, sensors, software, and associated networking that monitor and control onboard systems"*. OT systems are thus focused on using data to control or monitor physical processes (IACS, 2023a).

Interestingly, IACS UR E26 also provides a definition of a 'Computer Based System' (CBS) as *"a programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBSs onboard include IT and OT systems. A CBS may be a combination of subsystems connected via network. Onboard CBSs may be connected directly or via public means of communications (e.g., Internet) to ashore CBSs, other vessels' CBSs, and/or other facilities"* (IACS, 2023a).

An updated version of the IMO circular MSC-FAL.1/Circ.3/Rev.3, 'Revised Guidelines on Maritime Cyber Risk Management', was approved by MSC 108 in May 2024. These latest guidelines signal a significant shift from using the terms IT and OT to incorporating the IACS UR E26 CBS concept. The abbreviation CBS is now used throughout the Guidelines as an overarching term,

emphasising that *"when looking at CBSs, the distinction between information technology (IT) and operational technology (OT) systems should be considered,"* highlighting the differences between these systems. According to the revised Guidelines, IT refers to CBSs focused on "*the use of data as information, including software, hardware, and communication technologies (e.g., commercial information, or data about the crew, such as salaries, certificates, etc.)",* while OT refers to CBSs focused on *"the use of data to control or monitor physical processes (e.g., the main engine's oil temperature levels, which are forwarded to the control room)"* (IMO, 2022).

2.4 Current IT-inspired cyber risk management approaches and the way forward

As we have seen earlier, the maritime industry has traditionally approached risk management through frameworks designed to address physical and environmental safety. Tools such as the FSA have been central to identifying and mitigating risks related to human safety and environmental protection. These classical methods rely on a well-established definition of risk as a combination of probability or frequency and potential consequences. However, the advent of cyber threats has challenged this traditional paradigm, necessitating a broader, more dynamic approach to risk management that can address the complexities of IT systems.

In addressing cyber risks, the maritime industry has turned to frameworks and tools developed in the IT sector. Frameworks like ISO/IEC 27001 for information security management and NIST 2.0 provide structured approaches to managing and mitigating cyber risks. These IT-inspired frameworks are actually at the core of the BIMCO Guidelines.

However, as highlighted in a recent submission to the IMO by IACS (see IMO doc. MSC 108/6/1) for certain scenarios, IT standards may not be appropriate for OT environments due to different performance and availability requirements. Moreover, cyberattacks on IT systems primarily have economic consequences, while cyberattacks on OT systems can severely impact the safety of the ship, personnel, and the environment.

To tackle the challenges associated with integrated IT and OT systems, the IACS proposed the adoption of its 'Recommendation on Incorporating Cyber Risk Management into Safety Management Systems' (IACS Recommendation 171) in March 2024, as outlined in IMO document MSC 108/INF.11. This recommendation addresses the complexities of onboard systems and their interconnections, both within the ship and with external networks. As such, it presents a promising solution to these challenges and a potential blueprint for the future of maritime cybersecurity.

3 Back to the Future: Maritime Cyber Risk Management based on IACS Rec. 171

In this section we briefly describe how Rec. 171 can be used to manage cyber threats; the interested reader is referred to the actual text for more.

3.1 Introduction to IACS Rec. 171

The IACS Recommendation 171 (Rec.171) represents a significant step forward in the maritime industry's efforts to address cybersecurity risks, particularly in light of the growing integration of IT and OT systems onboard vessels (IACS, 2022). With the IMO requiring that cybersecurity risks be managed within the framework of the International Safety Management (ISM) Code, Rec.171 offers a practical methodology to guide shipowners and operators in incorporating these considerations into their Safety Management Systems (SMS).

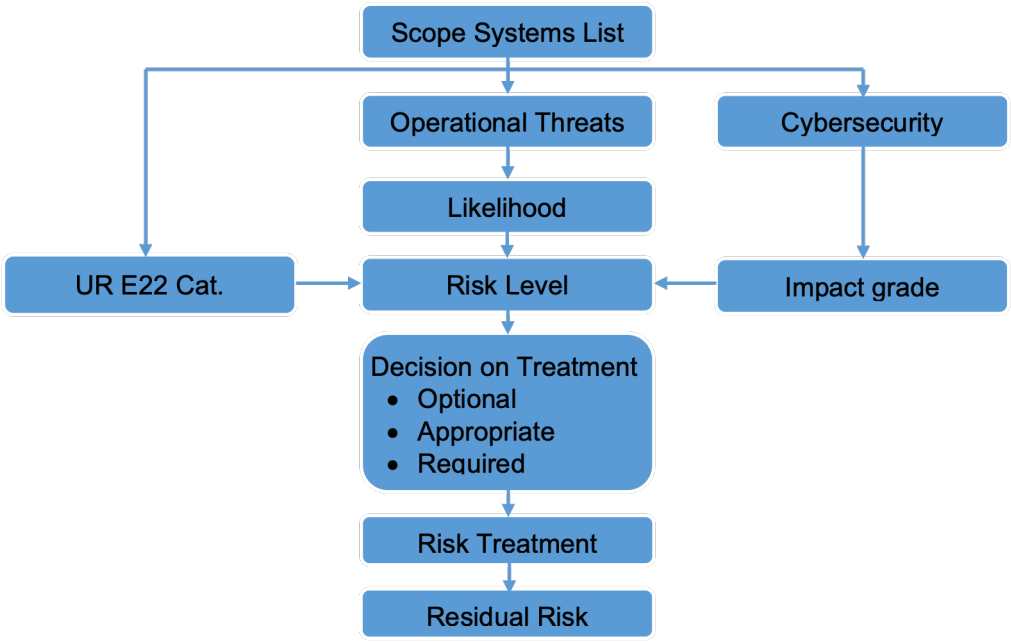
Central to Rec.171 is its detailed risk assessment framework (see Fig. 1), which helps stakeholders identify, evaluate, and mitigate risks associated with cyber threats to critical systems. The process begins with a thorough scoping and information-gathering phase, where details about systems, equipment, and their interconnections are collected. This includes understanding how onboard and external networks interact. The second phase involves assessing risk levels for individual systems, which is determined by three key factors: impact, likelihood, and system categorisation. Impact is graded on a five-point scale, ranging from negligible to catastrophic, depending on the consequences for availability, confidentiality, integrity, and traceability. Likelihood, on the other hand, incorporates factors such as the complexity of the system, its connectivity, human involvement, and the potential sophistication of attackers. These elements are combined with system categorisation, based on IACS UR E22 definitions, to calculate a precise risk level. The detailed presentation of the risk assessment process is illustrated in Figure 1 and detailed in the Section below.

The risk assessment process outlined in Rec. 171 is a comprehensive and methodical approach designed to protect maritime systems from cyber threats. It begins with the critical step of gathering information (i.e. defining the Scope of the Risk Assessment) to form what they refer to as the Scope Systems List, which includes identifying key systems (IT and/or OT), equipment, and their interconnections.

Once the scope is defined, the assessment focuses on three key parameters: impact, likelihood, and the UR E22 category. These parameters are carefully estimated to paint a complete picture of the risks that each system faces, that is the 'Risk Level' assessment of the system.

Figure 1

The risk assessment process per IACS Req. 171



Source: IACS (2022)

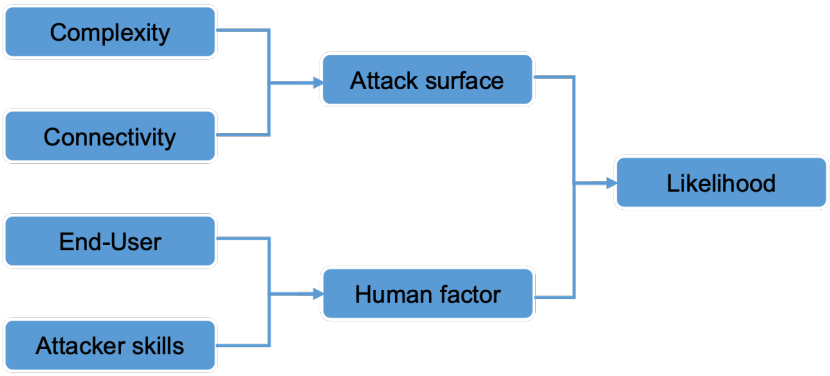
The **impact assessment** examines the potential consequences of a cyber incident. Systems are graded on a five-point scale ranging from negligible (P1) to catastrophic (P5). These categorise events from 'Negligible', when the *"system could be shut down without any significant effect",* or "No human or environmental impacts involved", to 'Catastrophic', where the impact could be the destruction of the physical systems (e.g. due to fire or explosion), loss of the vessel (e.g. due to collision or grounding), or the shipowner's bankruptcy.

This assessment considers various dimensions, such as system availability, data confidentiality, operational integrity, and the traceability of actions within the system. Per the provided definitions, 'Availability' of a system or equipment is the probability that it is not in a failed state at a point in time, 'Confidentiality' is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes, and 'Data integrity' is related to the maintenance of, and the assurance of, data accuracy and consistency.

The **likelihood assessment** evaluates the probability of a cyber threat materializing. Several factors influence this probability, including the level of system connectivity (CY) and complexity (CX) as part of the so-called 'attach surface'), and human factors; see Fig. 2 for more.

Figure 2

The likelihood assessment process per IACS Req. 171



Source: IACS (2022)

Connectivity, following a five-point scale, ranges from isolated systems (CY1) with minimal risk to open systems (CY5) defined as *"any system with an external link to a public network access, or without knowledge of special protection"* that interact with external networks, posing greater threats. Complexity is assessed on a three-point scale, based on system architecture, from 'low maintenance' systems (CX1) to distributed ones (CX3).

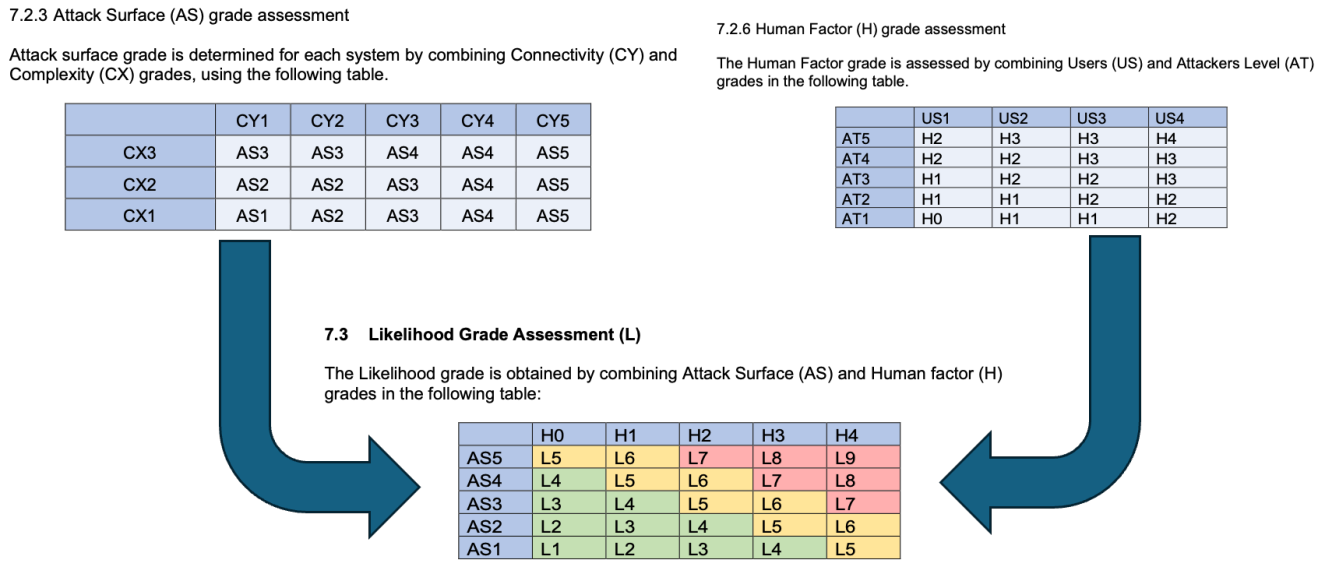
Human factors, such as crew training and attacker capabilities, also play a significant role in determining how vulnerable a system might be to cyber threats. The four-point 'grade of the end-users' (US) ranges from US1 ('aware user' to US4 ('any user') taking into account relevant crew (those who actually use the system/equipment) level of training/awareness, and the accessibility conditions of the system. A low level grade reduces the probability of a cyberattack, as 'aware users' systems are less vulnerable.

The Attacker's level (AT) ranges from AT1 to AT5, depending on the level of competence expected from an attacker on the contemplated system. These range from 'AT1: Unintentional Attacker' when, for instance, crew members have "unintentionally and accidentally introduced on board a common, not targeted virus or malware", to state-backed attacks (AT5: Cyber warfare Attacker).

By combining these factors into a matrix (see Fig. 3), systems are assigned a likelihood grade, ranging from low to high probability; see the IACS Rec. 171 (IACS, 2022) for a detailed description of the various components of the AS and H grade assessment.

Figure 3

Combining the Attack surface and Human Factors to estimate the likelihood per IACS Req. 171



	CY1	CY2	CY3	CY4	CY5
CX3	AS3	AS3	AS4	AS4	AS5
CX2	AS2	AS2	AS3	AS4	AS5
CX1	AS1	AS2	AS3	AS4	AS5

	US1	US2	US3	US4
AT5	H2	H3	H3	H4
AT4	H2	H2	H3	H3
AT3	H1	H2	H2	H3
AT2	H1	H1	H2	H2
AT1	H0	H1	H1	H2

	H0	H1	H2	H3	H4
AS5	L5	L6	L7	L8	L9
AS4	L4	L5	L6	L7	L8
AS3	L3	L4	L5	L6	L7
AS2	L2	L3	L4	L5	L6
AS1	L1	L2	L3	L4	L5

Source: Adapted from IACS (2022)

The third component, we will call this **criticality** —although in the framework it is denoted as the system category— is defined using the UR E22 classification system, which ranks systems based on their importance to safety and environmental protection. System categories are assigned based on their effects on system functionality; there are 3 categories: Cat. I for those systems, failure will not lead to dangerous situations for *"human safety, the safety of the vessel, and/or threat to the environment"*, Cat. II for failures that could eventually lead to danger, and Cat. III for those that could immediately lead to dangerous situations.

These three parameters—impact (P), likelihood (L), and criticality (Cat)—are then combined to calculate a Risk Level (RL) using the formula:

$$RL = 2\,(Cat + L + P - 4) \tag{1}$$

As zero risk does not exist (according to the framework), if the risk level is less than 1 (that includes negative values) then it is assigned a value of 1. This formula ensures a balanced assessment of all contributing factors.

Now, depending on the resulting RL, decisions are to be made about risk treatment. Low-risk systems (RL < 4) may not require immediate action ('optional risk treatment'), while medium-risk systems (RL between 4 and 12) warrant appropriate mitigation. High-risk systems (RL > 12) demand urgent intervention, i.e. *"risk treatment is required"*.

Once the risk level is established, the next step involves deciding on mitigation measures. When risk treatment is “appropriate” or “required”, mitigation measures are to be considered. The purpose of these mitigation measures is to reduce the Risk Level to an acceptable level assumed by the shipowner, called “Residual Risk Level”.

Mitigation strategies can include non-technical measures, technical measures, or a combination of both, depending on the level of risk and system criticality. Non-technical measures focus on human and procedural aspects, such as training crew members to enhance cybersecurity awareness and developing comprehensive procedures for monitoring systems and responding to incidents. Conversely, technical measures involve deploying advanced technologies, such as intrusion detection systems, real-time threat detection tools, and cybersecurity hardening solutions like firewalls and data diodes.

For high-risk systems, a blended approach that combines both technical and non-technical measures is often essential to ensure comprehensive risk mitigation. Human-centred measures, such as training and awareness programs, can reduce the risk level by one point, while organizational measures, including robust policies and protocols, can reduce it by three points. Technical solutions, like network security monitoring software and intrusion prevention systems, provide a more substantial reduction of six points. When a combined approach is implemented, it can achieve a maximum risk reduction of nine points, providing an effective strategy for managing critical vulnerabilities. See Rec. 171 (IACS, 2022) for more on the risk reduction for each measure category.

IACS Recommendation 166 on cyber resilience provides guidance for mitigating the risks related to events affecting onboard computer-based systems and presents a number of measures that can be used to address risk. The interested reader is referred to this document for a complete list of measures that can be implemented to mitigate risk.

After mitigation measures are applied, the residual risk is reassessed to ensure it falls within acceptable limits set by the shipowner. It is important to note that even with the most comprehensive measures, the residual risk cannot be reduced to zero, as no system is deemed to be entirely risk-free.

Rec. 171 also emphasizes the importance of continuous improvement. The risk assessment process is dynamic, requiring regular updates and reviews to address new threats and system changes. It highlights the adaptability of this methodology, allowing it to be tailored to different ship types and operational requirements.

3.2 Application of the Risk Assessment Approach: An illustrative example

Below are we present a rudimentary example to illustrate how IACS Recommendation 171 (Rec.171) can be applied in real-world scenarios.

Case Study: Bridge Navigation System (ECDIS)

System: ECDIS (Electronic Chart Geographic information system used for nautical navigation as Display and Information.

Scenario: A crude oil carrier (tanker vessel) uses an Electronic Chart Display and Information System (ECDIS) as its primary navigation tool. The risk assessment focuses on potential cyber threats to ECDIS during a transit in busy shipping lanes. We assume that the attack will be performed by an attacker with malicious intent using standard hacking techniques.

Step 1: Define Scope: The ECDIS is categorized as **Category III** under UR E22, as its failure could directly affect navigational safety.

Step 2: Impact Assessment (P)

Integrity: Corruption of data charts may considerably affect ship safety and security.

Availability: Loss of availability may seriously affect ship safety and security.

As both are considered to have a high impact, the impact is assessed to be high (**P4**); this is in line with the explicit assessment presented in Rec. 171.

Step 3: Likelihood Assessment (L)

Complexity (CX): The ECDIS software requires regular updates, graded as **CX2**.

Connectivity (CY): The system connects to shore for updates, graded as **CY4**.

Attack Surface (AS): Combining CX2 and CY4 results in **AS4**.

Human Factors (H): Any attacker (internal or external) with malicious intent using hacking tools and techniques is considered ‘AT3: Standard Attacker’. Here, we assume (a) that the crew is aware about cyber security, but poorly trained on cyber measures implementation, and (b) that default physical/logical access controls are applied to the system; we, thus, consider the End-Users (US) grade assessment of the system as 'US2: Controlled User'.

Combining AT3 and US2 results in H2 as illustrated in Figure 3

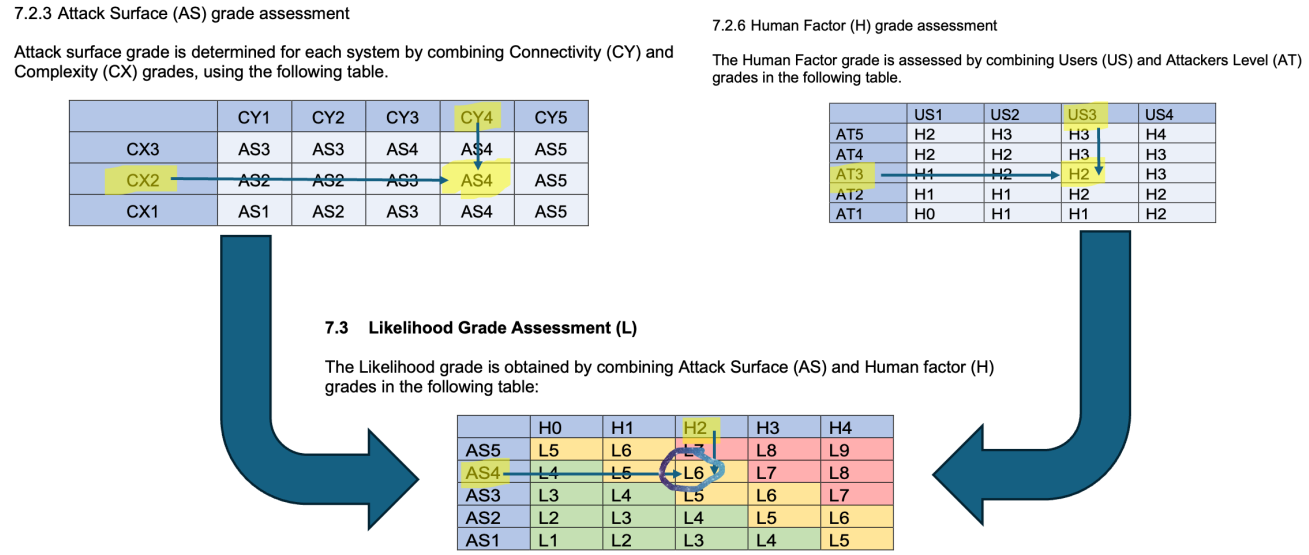
Figure 4 show the calculations of the ‘attack surface’ (AS) and the ‘human factor’ (H) elements of the likelihood of the threats to ECDIS; see Figure 3 and the relevant text in the Methodology Section on how these two are combined.

The likelihood can be then calculated (see Figure 3).

Likelihood Grade (L): Using AS4 and H2, the likelihood grade is **L6 (Medium)**.

Figure 4

Likelihood estimation for the ECDIS case-study



Source: Authors based on Figure 3.

Step 4: Risk Level Calculation (RL)

Based on the above estimations, ECDIS which is a category 3 system, has a likelihood of 6, and a high impact of 4. By using Eq. 1, the total risk level (RL) can be calculated as follows:

$$RL=2\times(3+6+4-4)=18$$

The risk level of 18 (which is above the threshold of 12) indicates that mitigation measures are **required**.

Step 5: Risk Treatment

Mitigation measures range from the simplest and easiest to implement (so-called "human-related" or "non-technical" measures) to the most elaborate "technical" measures. The desired level of effort depends on the Residual Risk Level to be achieved. In our case, the current risk is 18.

According to Rec. 171, when human-related mitigation measures are applied, the previous risk level can be reduced by 1. However, in our case, the residual risk level will still be too high. We believe this point needs further investigation, as a risk reduction of 1 seems too low. It is important not to underestimate the significance of raising crew awareness and vigilance regarding cybersecurity. For example, human supervision and checks of relevant data updates might, in our opinion, reduce the risk by more than one point.

Given the high risk level, several technical "monitoring" solutions should be implemented, as they can achieve significant risk reductions. To protect the ECDIS system, shipowners can implement a layered approach using various technical monitoring solutions. Real-time threat detection systems, such as Intrusion Detection and Prevention Systems (IDS/IPS), monitor for unauthorized access and malicious activity. Network security tools analyse traffic for anomalies, while Endpoint Detection and Response (EDR) focuses on securing connected devices. Vulnerability management and patching ensure the system stays updated, while threat intelligence platforms anticipate emerging threats.

More practical measures can be found in the IACS Rec. 155 'Recommendation on Cyber Resilience' (IACS, 2020), the NIST 2.0 framework (NIST, 2024), and BIMCO (2025) 'Cyber Security Workbook for On Board Ship Use' (BIMCO, 2025).

By implementing these technical "monitoring" solutions, as per Rec. 171, the risk level can be reduced by 6, bringing it down to 12, which we deem acceptable. Note that there is no universally acceptable risk level per Rec. 171 (except when the risk is equal to or below 4, in which case the risk treatment is considered "optional"). The acceptable level is determined by the shipowner, as they are the vessel's owner, decision-makers, and those who will assume any damages. This point warrants further academic and industry research to define an acceptable risk level or perhaps link it with ALARP (as low as reasonably practicable) and the cost-benefit step of the Formal Safety Assessment.

4 Conclusions

Rec. 171 adopts a traditional risk management framework, emphasising that mitigation measures should be proportionate to the assessed level of risk. Future research could explore its alignment with the ALARP principle and examine the risk calculation methodology in greater detail. Comparisons with other risk definitions, such as those in the BIMCO Guidelines—where likelihood is defined as a combination of threat and vulnerability—could provide valuable insights and highlight areas for further refinement.

Low-risk scenarios may only require optional interventions, while higher-risk situations demand more robust strategies. These strategies are categorised into non-technical and technical measures, ranging from crew training and procedural enhancements to advanced technical solutions such as network segmentation and system hardening. Recognising that risk management is a dynamic process, the recommendation highlights the importance of continuous monitoring and adaptation as systems evolve and new threats emerge. The ultimate objective is to achieve an acceptable residual risk level that aligns with the shipowner's operational and safety goals.

Compared to other frameworks, Rec. 171 distinguishes itself with its specific focus on the maritime domain. While the BIMCO Guidelines offer practical and high-level recommendations for managing cyber risks, they lack the detailed, quantitative methodology provided by Rec. 171 (IACS, 2022). BIMCO (2020) emphasises operational aspects such as incident response and crew training, whereas Rec. 171 presents a structured risk assessment framework that integrates seamlessly into existing Safety Management Systems (SMS). Similarly, IT-centric standards such as ISO 27001 focus on general principles of information security, which, although comprehensive, do not address the unique challenges of maritime OT systems. By aligning with IMO mandates such as MSC.428(98) and MSC-FAL.1/Circ.3, Rec. 171 offers a regulatory-compliant approach tailored specifically for shipboard cybersecurity.

The benefits of a wider use and a potential incorporation of IACS Rec. 171 (IACS, 2022) in the IMO Guidelines are clear. Its maritime-specific focus ensures that cybersecurity risk management strategies are directly relevant to the complex interdependencies and operational priorities of shipboard systems. By incorporating both human and technical mitigation measures, the framework achieves a practical balance between ease of implementation and the sophistication needed to address modern cyber threats. Furthermore, its emphasis on continuous improvement ensures that systems remain resilient in the face of evolving technologies and threats.

In a time when digital threats are as consequential as physical ones, IACS Recommendation 171 fills a critical gap in maritime safety management. It equips shipowners, operators, and other stakeholders with the tools not only to meet international regulatory requirements but also to proactively protect their operations from an ever-changing cyber threat landscape. By embedding its principles into SMS, the maritime industry can strive towards a future that is secure both digitally and operationally.

Acknowledgments

Acknowledgements should be included in a separate headed section after the main text. Authors may acknowledge in this section support for the development of the study or research, or any contribution to the work done, including sponsorship and financial support.

References

BIMCO. (2016). *The guidelines on cyber security onboard ships* (1st ed.). BIMCO. Retrieved from https://www.bimco.org

BIMCO. (2020). *The guidelines on cyber security onboard ships* (4th ed.). Available at https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

BIMCO. (2025). *Cyber security workbook for onboard ship use* (6th ed.). Witherbys. ISBN: 9781917308083.

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection, 40*, 100571. https://doi.org/10.1016/j.ijcip.2022.100571

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. *Safety Science, 131*, 104908. https://doi.org/10.1016/j.ssci.2020.104908

Chang, C. H., Kontovas, C., Yu, Q., & Yang, Z. (2021). Risk assessment of the operations of maritime autonomous surface ships. *Reliability Engineering & System Safety, 207*, 107371. https://doi.org/10.1016/j.ress.2020.107371

Erbas, M., Khalil, S. M., & Tsiopoulos, L. (2024). Systematic literature review of threat modeling and risk assessment in ship cybersecurity. *Ocean Engineering, 306*, 118059. https://doi.org/10.1016/j.oceaneng.2023.118059

IACS. (2020). *Rec 155 – Recommendation on cyber resilience*. International Association of Classification Societies. Available at https://iacs.org.uk/resolutions/recommendations/141-160

IACS. (2022). *Rec 171 – Recommendation on incorporating cyber risk management into Safety Management Systems*. International Association of Classification Societies. Available at https://iacs.org.uk/resolutions/recommendations/161-180

IACS. (2023a). *UR E26 Cyber resilience of ships* (Rev. 1, Nov 2023). International Association of Classification Societies. Available at https://iacs.org.uk/resolutions/unified-requirements/ur-e

IACS. (2023b). *UR E27 Cyber resilience of onboard systems and equipment* (Rev. 1, Sep 2023). International Association of Classification Societies. Available at https://iacs.org.uk/resolutions/unified-requirements/ur-e

IMO. (2017a). *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3/Rev.1). International Maritime Organization. Available at https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

IMO. (2017b). *Maritime cyber risk management in safety management systems* (MSC.428(98)). International Maritime Organization. Available at https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

IMO. (2018). *Revised guidelines for formal safety assessment (FSA) for use in the IMO rule-making process* (MSC-MEPC.2/Circ.12/Rev.2). International Maritime Organization. Available at https://wwwcdn.imo.org/localresources/en/OurWork/HumanElement/Documents/MSC-MEPC.2-Circ.12-Rev.2.pdf

IMO. (2021). *The guide to maritime security and the ISPS code*. International Maritime Organization. Available at https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

IMO. (2022). *Guidelines on maritime cyber risk management* (Rev. 2, MSC-FAL.1/Circ.3/Rev.2). International Maritime Organization. Available at https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2.pdf

ISO. (2018). *ISO 31000:2018 – Risk management guidelines*. International Organization for Standardization. Available at https://www.iso.org/standard/65694.html

ISO. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity, and privacy protection*. International Organization for Standardization. Available at https://www.iso.org/standard/27001.html

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., & Chang, C. H. (2022). Maritime cybersecurity: Are onboard systems ready? *Maritime Policy & Management*, 1–19. https://doi.org/10.1080/03088839.2022.2124464

Kontovas, C. A., & Psaraftis, H. N. (2009). Formal safety assessment: A critical review. *Marine Technology, 46*(1), 45–59.

Kontovas, C. A., & Psaraftis, H. N. (2010). Carbon dioxide emissions valuation and its uses. *3rd International Symposium on Ship Operations, Management and Economics (SOME)*. SNAME Greek Section. Retrieved from https://orbit.dtu.dk/en/publications/carbon-dioxide-emissions-valuation-and-its-uses

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology. Retrieved from https://www.nist.gov/cyberframework/csf-11-archive

National Institute of Standards and Technology (NIST). (2024). *Framework for improving critical infrastructure cybersecurity* (Version 2.0). National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Park, C., Kontovas, C., Yang, Z., & Chang, C. H. (2023). A Bayesian network-driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management, 235*, 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

Park, C., Kontovas, C., Yang, Z., & Chang, C. H. (2024). Mmaritime Cybersecurity Risk Assessment Using Bow Tie Diagrams. Extended Abstract. 2025 Conference of the International Association of Maritime Economists, Valencia, Spain.

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber-physical systems security for maritime assets. *Journal of Marine Science and Engineering, 9*(12), 1384.

Sèbe, M., Kontovas, C. A., & Pendleton, L. (2019). A decision-making framework to reduce the risk of collisions between ships and whales. *Marine Policy, 109*, 103697. https://doi.org/10.1016/j.marpol.2019.103697

Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. *Journal of Cyber Policy, 3*(2), 147–164. https://doi.org/10.1080/23738871.2018.1513053

UNCTAD. (2024). *Review of maritime transport 2024*. United Nations Conference on Trade and Development. Retrieved from https://unctad.org/publication/review-maritime-transport-2024

Yang, Z., Wang, J., & Ng, A. K. (2016). Toward robust management of maritime risk and security. In P. T.-W. Lee & K. Cullinane (Eds.), *Dynamic shipping and port development in the globalized economy* (pp. 122–149). Palgrave Macmillan.