Journal of
*Marine Science
and Engineering*

MDPI

Article

Cyber Physical Systems Security for Maritime Assets

Iosif Progoulakis [1],*, Paul Rohmeyer [2] and Nikitas Nikitakos [1]

[1] Department of Shipping Trade and Transport, University of the Aegean, Korais St. 2A, GR 82132 Chios, Greece; nnik@aegean.gr
[2] School of Business, Stevens Institute of Technology, 1 Castle Point on the Hudson, Hoboken, NJ 07030, USA; prohmeye@stevens.edu
* Correspondence: iprogoulakis@aegean.gr

Abstract: The integration of IT, OT, and human factor elements in maritime assets is critical for their efficient and safe operation and performance. This integration defines cyber physical systems and involves a number of IT and OT components, systems, and functions that involve multiple and diverse communication paths that are technologically and operationally evolving along with credible cyber security threats. These cyber security threats and risks as well as a number of known security breach scenarios are described in this paper to highlight the evolution of cyber physical systems in the maritime domain and their emerging cyber vulnerabilities. Current industry and governmental standards and directives related to cyber security in the maritime domain attempt to enforce the regulatory compliance and reinforce asset cyber security integrity for optimum and safe performance with limited focus, however, in the existing OT infrastructure and systems. The use of outside-of-the-maritime industry security risk assessment tools and processes, such the API STD 780 Security Risk Assessment (SRA) and the Bow Tie Analysis methodologies, can assist the asset owner to assess its IT and OT infrastructure for cyber and physical security vulnerabilities and allocate proper mitigation measures assuming their similarities to ICS infrastructure. The application of cyber security controls deriving from the adaptation of the NIST CSF and the MITRE ATT&CK Threat Model can further increase the cyber security integrity of maritime assets, assuming they are periodically evaluated for their effectiveness and applicability. Finally, the improvement in communication among stakeholders, the increase in operational and technical cyber and physical security resiliency, and the increase in operational cyber security awareness would be further increased for maritime assets by the convergence of the distinct physical and cyber security functions as well as onshore- and offshore-based cyber infrastructure of maritime companies and asset owners.

Keywords: cyber security; cyber physical systems; IT; OT; maritime assets; cyber and physical security convergence; API STD 780; Security Risk Assessment (SRA); Bow Tie Analysis

check for updates

Citation: Progoulakis, I.; Rohmeyer, P.; Nikitakos, N. Cyber Physical Systems Security for Maritime Assets. *J. Mar. Sci. Eng.* **2021**, *9*, 1384. https://doi.org/10.3390/jmse9121384

Academic Editor: Zaili Yang

Received: 1 October 2021
Accepted: 2 December 2021
Published: 5 December 2021

1. Introduction

This paper explores the cyber physical concepts of cyber security for maritime assets, both onshore and offshore. Cyber physical systems in the maritime sector constitute a complex field that involves the integration of IT (information technology) and OT (operational technology) systems and the interface with human element parameters. This integration, as depicted in Figure 1, defines the concept of cyber physical systems and represents the majority of systems onboard maritime assets. Figure 2 provides a simplified illustration of the communication paths between shore-based and vessel-based stakeholders and IT/OT platforms to illustrate the interconnection of IT- and OT-based communication interactions. Maritime assets operated by humans contain an IT and OT interface that links together processes, systems, components, and the technical and operational performance. A naval vessel is considered a platform of systems of systems, containing IT and OT devices. A vessel's crew represents the operator of these components and processes and is responsible for the operational and performance integrity of the vessel as a whole. In parallel, shipping companies have an IT interface that supports naval vessels at a technical and operational level. Again, the human element is present as the operator of IT platforms which are tools to achieve performance and financially oriented tasks to support the maritime operations. Ports interface with naval vessels on a shore-to-ship and ship-to-shore operational level, either receiving from or loading the maritime commercial goods into naval vessels. In this case, for a port to carry out these loading and offloading tasks, a combination of IT and OT platforms is utilized. From cargo management platforms and cranes to utilities' support systems, IT and OT platforms are used for the support of maritime assets at a technical and operational level. The human element is present as the operator, configurator, and moderator in all cyber physical systems. The maintenance of OT devices and systems is carried out on a physical interface or remotely. The monitoring and configuration of key performance indicators of a vessel's systems is conducted mostly remotely. In all cases, the human element plays an important role as the operational lead.

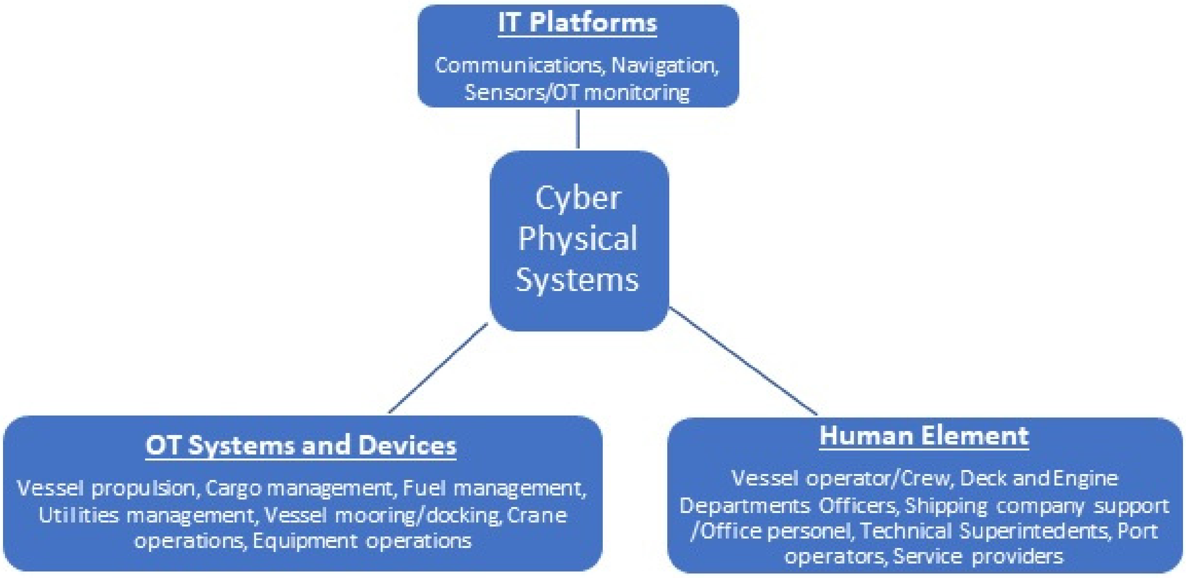
IT Platforms
Communications, Navigation, Sensors/OT monitoring
Cyber Physical Systems
OT Systems and Devices
Vessel propulsion, Cargo management, Fuel management, Utilities management, Vessel mooring/docking, Crane operations, Equipment operations
Human Element
Vessel operator/Crew, Deck and Engine Departments Officers, Shipping company support /Office personel, Technical Superintedents, Port operators, Service providers

Figure 1. IT, OT, and human element interface in cyber physical systems.

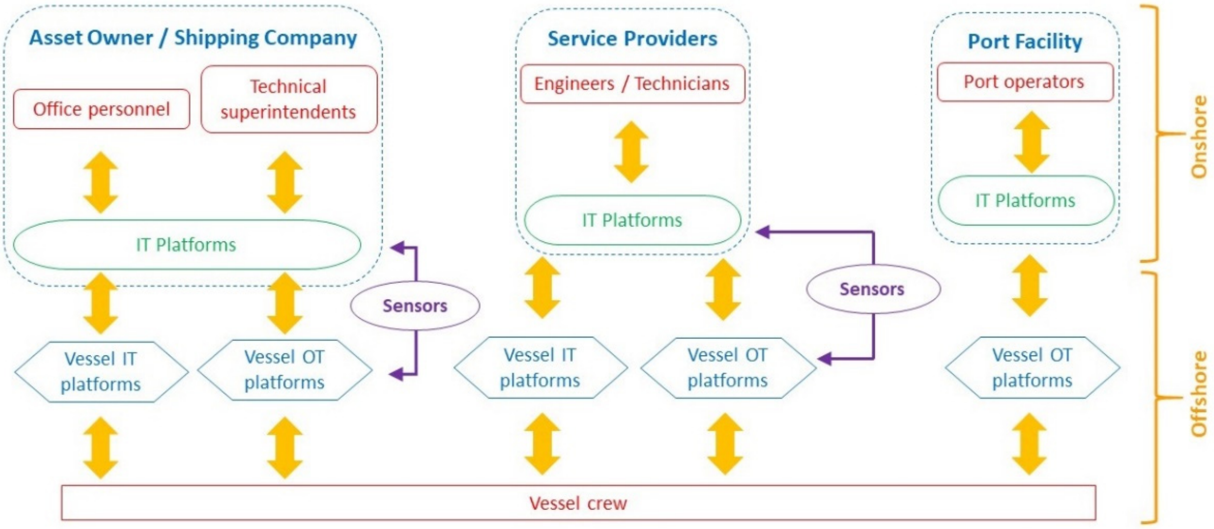

Figure 2. Communication paths of shore-based and vessel-based stakeholders and IT/OT platforms.

Research Methodology and Article Structure

This paper assesses the cyber physical concepts of cyber security for maritime assets, by presenting a comprehensive review of existing industry and governmental policies, directives, and standards that cover the subject of cyber security for maritime assets including cyber physical systems and operations. The main aspects of cyber physical security for the maritime sector in general are discussed in Section 2. The different security threats faced and known vulnerabilities, a brief overview of notable cyber incidents, and the emerging risk factors of maritime assets and their cyber physical systems and functions are discussed in Section 3. An overview of existing industry and governmental initiatives are presented in Section 4 and cover maritime industry organizations, industry standardization organizations, maritime classification societies, government agencies, marine insurance, and P&I clubs. This paper also discusses, in Section 5, two risk assessment methods deriving from different industry sectors and which could be applied in the maritime industry and specifically for the cyber security risk analysis for cyber physical systems. Section 5 also gives some examples of these methods, outlining important conclusions in cyber physical security assessment. The risk treatment process involving the design of cyber security controls for cyber physical systems and functions in maritime assets is discussed in Section 6. Important notes deriving from the review of the presented literature review in Section 4 are discussed in Section 7. Finally, key conclusions are presented in Section 8 along with a discussion on the scientific contribution of this paper and future research.

2. Cyber Physical Security Aspects for the Maritime Sector

The nature and complexities of IT and OT in maritime environments can be analyzed by considering the technical characteristics of vessels, ports, terminals, offshore oil and gas rigs, and other dimensions of maritime asset architecture. Each presents unique attributes and cyber physical risk challenges.

The maritime industry today relies on global communications and would be substantially crippled if communications became unavailable. The sector relies on complex, interconnected, global cyber architectures that contain both IT and OT systems in support of complex process functions. Technology is deployed to achieve greater efficiencies and optimization. Maritime system architectures are undergoing a substantial evolution that includes the rapid, global introduction of a variety of emerging technologies. This includes integration of capabilities associated with Industry 4.0, including the Internet of Things (IoT), distributed cloud computing, data analytics, robotics, embedded software, and other advances that combine to form the emergent systems landscape [1].

Ports facilitate automated operations and processes on a continuous basis. This includes the loading and unloading of cargo, financial transactions, contract management, exchanging supply chain information, environmental monitoring, and other functions. They also need to provide physical security and interact with law enforcement, military, and other regulatory bodies as needed. The move to intelligent, or “smart port”, architectures is underway and features the use of data analytics to drive improved decision making, streamline processes, optimize traffic management, and provide enhanced monitoring of essentially all port operations. Vessels, rigs, and other maritime assets address similar functional requirements. In the case of vessels, navigational requirements produce additional system requirements and architectures [2].

The complexity of maritime systems can be further illustrated by considering them “systems of systems” (SoS), with varying degrees of centralization, control, and ownership of the sub-set, constituent systems that comprise the SoS [3]. The SoS context suggests variability in the coordination and alignment of standards, process design, and other aspects of system governance.

Cyber security challenges are presented in all aspects of the maritime cyber physical architecture. Achieving the core cyber security objectives of confidentiality, integrity, and availability throughout the system and its components presents substantial difficulties that continuously evolve. The challenges are notable in ensuring cyber security with respect to

IT and OT systems assets that store, transit, or process operational, financial, personnel, navigation, and other data.

3. Cyber Security Threats and Vulnerabilities

Cyber security risk in all industries reflects threats to the confidentiality, integrity, and availability of systems and data and is a manifestation of the ever-present vulnerabilities in systems and architectural components. We can consider historical breach activity in maritime as well as other industries to illustrate the nature of specific threats and vulnerabilities. Examination of other industries can be useful for identifying threats and vulnerability characteristics that may not have yet been visible in past maritime cyber breach events.

Maritime operations, by nature, have been international and sometimes global for centuries. However, globalization in the present era creates technology risks due to the varying levels of technical sophistication and standards of preparedness across jurisdictions. There can be wide variety in the vintage of onboard and shoreside systems that are increasingly integrated. On a single voyage, a commercial vessel may need to accommodate data transfer in a wide variety of mechanisms including USB flash drives, direct connection of endpoint computers brought on-board by local port authorities, wired connections, and of course wireless of various vintages and security. Technical risk is present in all individual technologies, and new types of risk result from increased interdependency and interconnection.

In general, the identified cyber threats for maritime assets and their cyber physical interface can be classified as internal, external, or colluded [4]. This classification is similar to the physical threats faced. An insider threat can be a vessel crew member or port operator who unintentionally or intentionally allows the penetration of cyber security barriers (in this case IT platforms and tools) by operating in the cyber–physical domain without proper cyber security practices. From the use of a virus-infected USB device to the opening of an unsolicited email infected with malware, external threats can be a number of common cyber criminals, hackers, hacktivists or even state adversaries or terrorists using sophisticated methods to manipulate, degrade, or take control of IT and OT systems. The colluded threats are a combination of internal threat actors acting with the guidance of external sources.

3.1. Maritime Breach Incidents

Examination of recent maritime cyber breach events highlights important characteristics to inform risk assessment, control design, and loss expectations. Breach consequences include various forms of disruption to the mission of providing confidentiality, integrity, and availability to maritime systems. The impact of cyber breaches on maritime can be considered similar to cyber incident experiences across all industries; however, the maritime context does present unique characteristics in breach impact.

Maritime ransomware incidents have been notable. Perhaps the worst maritime cyber event, the NotPetya ransomware event, resulted in losses measured in over hundreds of millions of dollars for Moller–Maersk. The disruption caused by NotPetya caused global disruptions for weeks [5]. The event began with the infection of a single user workstation and took only seven minutes to widely propagate, according to the Maersk Chief Information Security Officer [6]. The Port of San Diego was significantly impacted by Ransomware as well, in a 2019 attack. The breach affected primarily IT systems as well as the San Diego Harbor police systems [7]. Clarksons, the British shipping services company, was victimized in a breach where the perpetrators sought ransom in exchange for the promise of not releasing sensitive information including personal data. Clarksons was not operationally disrupted and refused to pay the ransom [8]. The extent of the resulting data leakage, however, is unclear.

In regard to maritime assets, an attack against a US-flagged, ultra-large container ship using the Emonet malware was noted to have debilitated all operational systems of the vessel [9]. Vessel navigational system malfunctions due to the fact of GPS spoofing have also been reported [10]. Remote cyber-attacks utilizing vulnerabilities in wireless keyboards and printers have also been known [11] to have affected vessel IT and OT systems. Finally, cyber-attacks from state adversaries have also been reported in multiple vessels, resulting in the loss of propulsion and steering [12].

Attacks on industrial control systems (ICS), by nature, clearly illustrate the potential consequences of cyber-attacks on cyber physical systems. In 2019 the US Coast Guard released information about a Ryuk ransomware attack on a facility that was apparently the result of a phishing email. The malware had a sizeable impact on IT but also propagated into the ICS used for facility monitoring and cargo movement [13]. The impact of cyber security attacks on ICS and SCADA (Supervisory Control and Data Acquisition) systems has long been a point of concern despite the relatively lower number of reported breach incidents compared to attacks on IT networks. The recent Colonial Pipeline attack, however, provided a clear demonstration of the potential consequences including widespread disruption throughout integrated supply chains. The nature of attacks on ICS are significantly different than attacks on IT assets. As described by ICS cyber security researcher Joe Weiss, "The scary fact that almost any person in an organization that clicks on a "poison" attachment could cause a problem of the magnitude of what happened with Colonial Pipelines should give everyone pause for thought. The more I dug into the problem, the more complicated it became." [14].

3.2. Emerging Risk Factors

Cyber physical maritime system architecture is rapidly evolving and should be expected to produce or highlight novel risk scenarios. The study of past breaches is invaluable in forecasting risk dimensions in all systems. However, the ongoing infusion of new technology should be anticipated to produce previously unknown risk considerations. Therefore, examination of risk should ideally combine analysis of relevant historical events as well as new largely theoretical insights into potential vulnerabilities, attacker motives, consequences, and other factors.

Industrial Internet of Things (IIoT) reflects the increased integration of IoT into cyber physical system architectures, where we can expect the individual risk dimensions of IoT devices will manifest, in some cases, as substantial system risks. Risk should be anticipated due to the lack of standardization across device designs and protocols, and the expectation that new IoT components will be linked with legacy systems of varying sophistication, vintage, and security. Desires to control early costs in IIoT may contribute to concerning levels of risk acceptance [15]. Additionally, new exposures should be expected within the network communications architectures that will support new IIoT.

Greater process integration is typically expected to result from increased system interconnection. However, a wide base systems development and engineering research revealed the shortcomings of automating legacy processes without considering new capabilities and limitations introduced by the new technology [16]. Integration of artificial intelligence and robotics can similarly present "people and process risk" by removing historically important quality control benefits of manual oversight [17].

Process integration is expected in both horizontal and vertical integration strategies and is recognized as a goal of Industry 4.0 in the maritime industry [1]. Horizontal integrations seek to combine the strengths of entities operating at the same level of a value chain, such as multiple producers of the same component, while strategies of vertical implementation anticipate upstream and/or downstream coordination and, therefore, system connectivity. Human factors can create risk as well. Many cyber physical environments can be considered socio-technical systems, where technology and people interact and may produce substantial risk challenges. This includes personnel vulnerability aspects related to human operators throughout the system and process architecture.

The physical dimension presents unique vulnerability characteristics, as threat actors can take actions that are initially physical intrusions with an ultimate goal of a cyber breach. Physical breaches to systems and information, such as the theft of equipment or perhaps intruders undertaking cyber-attack actions from ship or terminal-based endpoints that are inside the trusted physical and cyber perimeters, and typically signed-in with accounts that possess escalated privileges. Therefore, a sequential physical-to-cyber-attack path represents an important potential threat vector in maritime environments, particularly considering the challenges in physical protection of vessels and rigs, where physical attackers may be motivated to ultimately breach systems on board as well as gain access to remote company and/or government systems.

4. Cyber Security Initiatives for the Maritime Sector

The cyber–physical aspects of security and cyber security in the maritime domain, in general, are covered by numerous publications, directives, guidelines, and standards from the industry and government. These are described in the subsequent subsections with the list not being conclusive.

4.1. Maritime Industry Organizations

Regarding international industry organizations, the International Maritime Organization (IMO) released in 2017 Resolution MSC.428(98) [18] and IMO Guidance MSC-FAL.1/Circ.3 [19]. These address the implementation of maritime risk management in vessels' safety management systems (SMSs) in accordance with the ISM (International Safety Management) Code objectives and requirements. MSC.428(98) and MSC-FAL.1/Circ.3. complement the IMO ISPS (International Ship and Port Facility Security) code for vessels dealing with cyber and physical security issues.

BIMCO (Baltic and International Maritime Council), The International Association for Classification Societies (IACS), The International Association of Independent Tanker Owners (INTERTANKO) along with other industry partners have issued the Guidelines on Cyber Security Onboard Ships [20] (2021) aimed at the implementation of cyber risk management strategies in accordance with relevant industry regulations and best practices on board a ship with a focus on operational and technical processes, equipment, personnel training, and the response to cyber incidents and the subsequent operational recovery.

4.2. Industry Standardization Organizations

The US National Institute of Standards and Technology (NIST) has developed the Cyber Security Framework [21] which is used worldwide in the maritime and general industrial sectors. The NIST series of standards captures the operational and technical cyber security requirements of general industrial and maritime assets. The NIST Cyber Security Framework consists of five functions: (1) cyber security risk identification for systems, assets, data and operations; (2) the implementation of cyber security protection safeguards for assets; (3) cyber security incident detection; (4) cyber security incident response; (5) cyber security incident recovery. The NIST Cyber Security Framework is complemented by NIST Special Publications 800-30 [22], 800-37 [23], and 800-82 [24], which relate to Industrial Control Systems (ICS) and their cyber security risk assessment and management. Specifically, for cyber physical systems, NIST also published Special Publications 1500-201 [25], 1500-202 [26], and 1500-203 [27], which, in three volumes, comprise the NIST Framework for Cyber–Physical Systems. The NIST Framework for Cyber–Physical Systems is derived from industry and academia and applies to various IT and OT systems in industry sectors including transportation and maritime. It also explores the interaction of systems and components within a cyber infrastructure, and it defines the SoS state of IT and OT assets and provides a comprehensive tool for the analysis and description of cyber physical systems.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have published a number of standards applicable to cyber security, which also cover IT and OT systems and ICS in operation in the maritime domain. ISO/IEC 27001 [28] is applicable for the maritime sector and it provides a structured framework for the identification, assessment, and mitigation of cyber security risks. IEC-62443 is a series of standards on industrial communication networks and security of IT systems and networks that cover both technical- and process-related industrial cyber security. From the IEC-62443 series, IEC-62443-4-2 [29] provides the technical requirements for components of Industrial Automation and Control Systems (IACS) and describes mitigation measures for cyber security vulnerabilities. IEC 62443-3-3 [30] describes the requirements of technical control systems and the security levels of their control system capability. ISO/IEC 21827 [31] presents practices used in the industry and describes the Systems Security Engineering—Capability Maturity Model® (SSE-CMM®), outlining the process for organizational security engineering for companies and assets. ISO/IEC 18045 [32] provides guidelines for the evaluation of systems and their IT security. ISO/IEC 15408-1 [33] provides the structure and basic concepts for the cyber security evaluation of IT products, defining the concept of a target of evaluation (TOE) and the context of evaluation of IT systems and components. ISO/IEC 27032 [34] covers the subject of security for information, networks, internet, and critical information infrastructure protection, providing guidance for cyber security improvement.

ASTM International, formerly known as the American Society for Testing and Materials, issued two standards that relate to cyber security in maritime assets. ASTM F3286-17 [35] relates to the organizational need to mitigate the likelihood of cyber security attacks and to reduce the extent of potential cyber incidents through the protection of sensitive data onboard vessels and offshore operations. ASTM F3286-17 also utilizes the NIST Cyber Security Framework for maritime assets and critical infrastructure. ASTM F3449-20 [36] provides guidance, information, and options to the maritime industry in order to incorporate technical and operational cyber elements into vessel safety management systems (SMS). The suggested guidelines are in compliance with the International Safety Management (ISM) Code and other national and international requirements as well as the IMO Resolution MSC.428(98).

4.3. Maritime Classification Societies

In the sector of maritime classification societies, the International Association for Classification Societies (IACS) has issued Recommendation No. 166 on Cyber Resilience, which provides technical requirements for the buildup of necessary cyber resilient infrastructure for vessels. IACS Recommendation No. 166 [37] supports IMO Resolution MSC.428(98) and IMO Guidance MSC-FAL.1/Circ.3.

The American Bureau of Shipping (ABS) published five cyber security-related guidance documents [38–42] that apply to vessel operators, owners as well as construction and integration companies. The ABS guidance documents provide best practices for the implementation of cyber security measures at the operational and technical levels. They also provide guidance on system data integrity and the application of mitigation measures for IT and OT systems for maritime assets.

DNV GL published recommended practices DNVGL-RP-G 496 (2016) [43] and DNVGL-CP-0231 (2018) [44]. These implement the guidelines of the International Electrotechnical Commission's IEC 62443 standard for the cyber security assessment of IT and OT systems and infrastructure as well as industrial automation and control systems onboard maritime assets. The aim of DNVGL-RP-G 496 (2016) and DNVGL-CP-0231 (2018) is the buildup of IT and OT system infrastructure resiliency against various cyber security threats.

Lloyd's Register (LR) issued three guidance notes (2016) [45–47]. These cover the deployment of IT and OT systems in maritime assets and autonomous ships. They also cover the type of approval of cyber-enabled components of vessel IT and OT systems as well as the LR Cyber Security Framework (CSF) for the Marine and Offshore sector, adopting IMO Resolution MSC.428(98) and IMO Guidance MSC-FAL.1/Circ.3.

The Japanese ship classification society Nippon Kaiji Kyokai or Class NK published two guideline documents that apply to cyber security elements for maritime vessels. The Class NK guideline documents "Guidelines for Designing Cyber Security Onboard Ships" (ClassNK 2020) [48] and "Cyber Security Management Systems for Ships" (Class

NK 2019) [49] deal with the implementation of operational and technical controls and measures against cyber threats for IT and OT systems on board vessels. They also cover cyber security management of IT and OT systems for companies and maritime assets and their implementation, maintenance, and improvement aiming for safe navigation.

The Croatian Register of Shipping (CRS) issued ISM Code Statutory Newsletter Number 03.08.2020 [50], which outlines the cyber risk management policies and procedures for maritime assets in accordance with the International Ship and Port Facility Security Code (ISPS Code), International Safety Management Code (ISM Code), IMO Resolution MSC.428(98), and IMO Guidance MSC-FAL.1/Circ.3.

The Indian Register of Shipping (IRCLASS) published the Maritime Cyber Safety Guidelines (IRS-G-SAF-02—2018) [51] that provide the requirements for evaluation and management of cyber risk in ships. In addition, the Guidelines on Certification of Software for Computer Based Control Systems (IRS-G-DES-01—2019) [52] were published. These guidelines outline the quality assurance certification requirements for software for computer-based control systems and their shipboard applications.

The Russian Maritime Register of Shipping published the Guidelines on Cyber Safety (ND No. 2-030101-040-E—2021) [53] which is based on IACS Recommendation No. 166 (Recommendation on Cyber Resilience) and implements the provisions of IMO Resolution MSC.428(98) and IMO Guidance MSC-FAL.1/Circ.3. These guidelines provide recommendations on the design, manufacture, maintenance, and testing of the shipboard computer-based systems as well as applicable recommendations for the vessel's safety management systems (SMS).

The International Registries and Maritime Administrator of The Republic of the Marshall Islands issued Marine Guideline No. 2-11-16 (2018) [54], which outlines the necessary resources for the establishment of policies and procedures for the mitigation of maritime cyber risks in accordance with IMO Resolution MSC.428(98) and IMO Guidance MSC-FAL.1/Circ.3. The aim of Marine Guideline No. 2-11-16 is for asset owners to develop the safeguards against cyber risks for Republic of the Marshall Islands (RMI)-flagged vessels. In addition, the Maritime Administrator of The Republic of the Marshall Islands issued Ship Security Advisory No. 13-20 (2020) [55], which recommends the use of the Guidelines on Cyber Security Onboard Ships from BIMCO as well as USCG Work Instruction CVC-WI-027 on Vessel Cyber Risk Management.

Bureau Veritas issued two Rule Note documents related to cyber security aspects in the maritime sector. Rule Note NR 642 (2018) [56] deals with cyber security related to manufacturing and technical requirements of components and systems to be utilized on board ships. Rule Note NR 659 (2020) [57] applies to the design, construction, commissioning, and maintenance of computer-based systems (CBS) and IT and OT systems to be utilized on board vessels and which are required to be certified as part of the classification of the maritime asset.

4.4. Government Agencies

In the governmental sector in the US, the US Congress (2020) issued Bill S. 4023 "Enhancing Maritime Cyber Security Act of 2020" [58]. Bill S. 4023 assigns to the US Cyber Security and Infrastructure Security Agency (CISA) and the Maritime Administration (MARAD), the implementation of cyber security strategies and measures. The US Coast Guard (2020) issued Navigation and Vessel Inspection Circular (NVIC) 01-20 [59], titled "Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities". NVIC 01-20 provides guidance to MTSA-regulated facilities for the assessment, documentation, and addressing of computer system and network cyber vulnerabilities in their assets. NVIC 01-20 covers maritime assets and facilities in the outer continental shelf and offshore operations and encourages the implementation of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cyber Security and NIST Special Publication 800-82. The USCG has also issued Vessel Cyber Risk Management Work Instruction CVC-WI-027 (rev.2, 2021) [60], which provides guidance for the assessment of vessels' cyber risks in order to avoid posing risk to the Marine Transportation System (MTS) in the case of a cyber breach scenario.

In the United Kingdom (UK), the Institution of Engineering and Technology (IET), the Department for Transport (DfT), and the Defense Science and Technology Laboratory (Dstl) issued the Code of Practice for Cyber Security for Ships (2017) [61]. This Code of Practice provides a management framework for the reduction of the risk of cyber incidents that could affect a ship's safety or security, its crew, passengers, or cargo. The UK DfT, the Defense Science and Technology Laboratory (Dstl), the National Cyber Security Centre (NCSC), and the Institution of Engineering and Technology (IET) also published a Good Practice Guide in Cyber Security for Ports and Port Systems (2020) [62]. This Good Practice Guide is applicable for port and port systems and facilities and is aimed at the integration of cyber security into their overall security planning.

In the European Union, cyber security for the maritime industry is addressed by the European Union Maritime Security Strategy (EUMSS) Action Plan (2018) [63] that aims to reinforce and enhance the EU's capabilities to mitigate security challenges and improve the protection and resilience of maritime systems and infrastructure. Regulation (EU) 2016/679 [64], called the General Data Protection Regulation (GDPR), protects the processing of personal data for all industry sectors, including the maritime sector. The cyber security of IT networks and the delegation of operational cyber security to the European Union Agency for Network and Information Security (ENISA), are addressed by directive 2016/1148/EU [65] and the EU Cyber security Act (2019/881/EU) [66]. The European Union's cyber security strategy JOIN/2013/01 [67] was also developed to strategically implement mitigation technologies and policies and to raise cyber resilience and security levels. ENISA also published reports related to cyber risk management for ports (2020) [68] and port cyber security (2019) [69].

Finally, in Singapore, the Maritime and Port Authority of Singapore published Shipping Circular No. 15 [70] on Maritime Cyber Risk Management. This Circular applies the requirements of IMO Resolution MSC.428(98) and IMO Guidance MSC-FAL.1/Circ.3.

4.5. Marine Insurance Companies and P&I Clubs

The financial loss and asset damage coverage due to the fact of a cyber-attack is a complex insurance issue that is addressed by marine insurers and P&I clubs in various ways. While marine insurance companies provide vessel structure and equipment coverage to asset owners and cargo coverage to cargo owners, P&I clubs cover third-party liabilities [71]. A cyber-attack breach, however, could potentially lead to a third-party liability that may or may not be covered by the insurance contract. Currently, maritime asset insurance includes the Institute Cyber Attack Exclusion Clause (CL 380) 10/11/2003. An Exclusion Clause (CL 380) is included in all marine insurance policies and covers liabilities for the failure of computer equipment and systems. It does not cover, however, losses, damages, or liabilities that are caused by computer systems or equipment when used as a means of aggression or attack.

The Institute Cyber Attack Exclusion Clause (CL 380) 10/11/2003 is incorporated into contract insurance clauses by the following marine insurers and P&I Clubs [71]:

- Exclusion Clause (CL 380) Exclusion Clause (CL 380) The International Group of Protection and Indemnity Clubs (IGPANDI) and every member of this Group (13 members);
- Gard P&I (Bermuda) Ltd.;
- The London Steam-Ship Owners' Mutual Insurance Association Limited';
- The Ship-owners Mutual Protection and Indemnity Association (Luxembourg);
- Assuranceforeningen Skuld;
- The West of England Ship Owners Mutual Insurance Association (Luxembourg);
- United Kingdom Mutual Steamship Assurance Association (Bermuda) Ltd;
- The Steamship Mutual Underwriting Association (Bermuda) Limited.

Similar to the above, The Japan Ship Owners' Mutual Protection and Indemnity Association does not cover insurance liabilities due to the fact of cyber risks, but it does not explicitly apply the Institute Cyber Attack Exclusion Clause (CL 380) 10/11/2003 [71]. The Standard Club Ltd. and Sveriges Ångfartygs Assurans Förening/The Swedish Club [72] exclude liabilities deriving from computer equipment, systems, or software.

The North of England P&I Association recognizes the cyber security threats faced by the maritime sector as well as the existing operational and technical vulnerabilities and has issued a number of publications, briefings and circulars [71–75], for their customers. They also recommend customer compliance to IMO Resolution MSC.428(98) and IMO Guidance MSC-FAL.1/Circ.3 as well as the BIMCO Guidelines on Cyber Security Onboard Ships (2021) (Loss Prevention Briefing, 2016). The use of a cloud-based software platform for their customers is also available and recommended for them in order to carry out assessments of their organizational, operational and technical cyber capabilities and vulnerabilities (Circular 2020/02). In the case of a cyber breach due to the fact of a computer virus (and the subsequent non-existence of suitable IT system antivirus protection), however, there is no coverage for losses, liabilities, or costs suffered (Circular 2021/06).

Finally, the Institute Cyber Attack Exclusion Clause (CL 380) 10 November 2003 is not applied by The American Steamship Owners Mutual Protection and Indemnity Association, Inc.; The Britannia Steam Ship Insurance Association Limited; Sveriges Ångfartygs Assurans Förening/The Swedish Club [71].

5. Risk Analysis Methods for Cyber Physical Security

5.1. API STD 780 SRA (Security Risk Assessment)

The Security Risk Assessment (SRA) methodology was developed for primary use in the oil and gas, chemical, and industrial sectors. SRA is described by API (American Petroleum Institute) standard (STD) 780 (2013) [76] and was developed to be applied in a wide spectrum of applications in the security risk assessment of facilities and assets. API STD 780 SRA can be used to assess security risks from various physical security threats, such as terrorism, piracy, theft, sabotage, for fixed and mobile assets/facilities. The application of SRA can cover both localized areas and functions of assets as well as greater assemblies of facilities/assets at a macroscopic scale. This makes SRA applicable to cyber physical security applications, as it can capture both the physical aspect of security breaches and vulnerabilities as well as the interface of assets with IT/OT systems and infrastructure.

The API STD 780 SRA methodology assesses and allows for the management of security risks through a risk-based, performance-oriented management process aimed at the protection and security of assets, people, and the environment. The SRA is a five-step process as shown in Figure 3.

Application of the API STD 780 SRA Method in a Maritime Asset

In order to prove the case that the API STD 780 SRA can be applied in cyber physical security applications for a maritime asset, an FPSO (floating production storage and offloading) vessel was analyzed in different security incidents. For this analysis, the main maritime features and functions of the vessel were analyzed, excluding the complex processing systems used in the upstream oil and gas sector. For the implementation of the API STD 780 SRA, the available vessel's technical designs and PIDs (process Instrumentation diagrams) were studied.

The five steps of the security assessment described in API STD 780 were followed in order to analyze the asset components, its threats, vulnerabilities, and credible security risks and to propose risk mitigation measures.

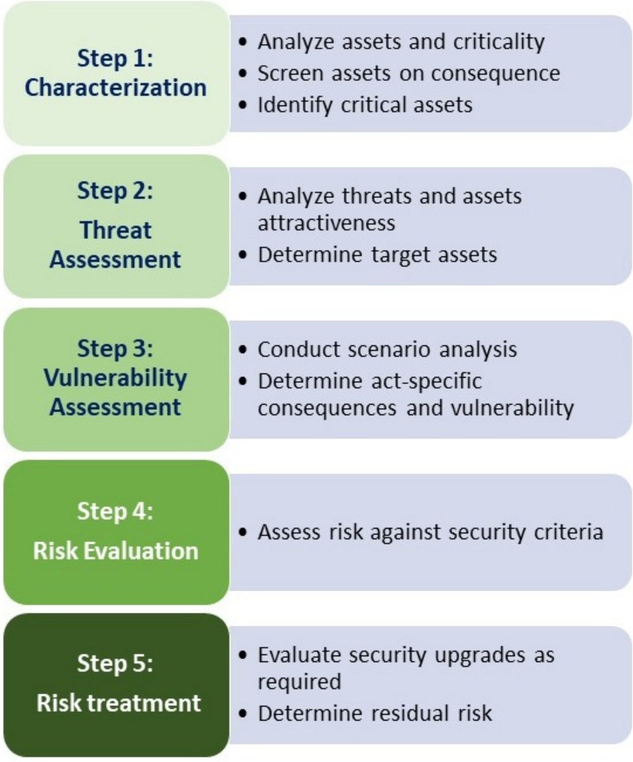
Step 1:
Characterization
• Analyze assets and criticality
• Screen assets on consequence
• Identify critical assets
Step 2:
Threat
Assessment
• Analyze threats and assets attractiveness
• Determine target assets
Step 3:
Vulnerability
Assessment
• Conduct scenario analysis
• Determine act-specific consequences and vulnerability
Step 4:
Risk Evaluation
• Assess risk against security criteria
Step 5:
Risk treatment
• Evaluate security upgrades as required
• Determine residual risk

Figure 3. API SRA process (source: [76], with information elaborated by authors).

In Step 1 of the SRA process, the following occur:

i. FPSO vessel asset components are identified;
ii. Interdependencies of the assets are determined;
iii. Existing security safeguards (internal and external) are identified;
iv. Consequences to human life, environment, and business continuity are determined;
v. Criticality ranking based on severe consequences is assigned.

Critical assets that have been identified include vessel engine room, electrical switch board rooms, emergency generators, electrical frequency converters, HVAC equipment, radio/communication equipment, bow and aft thrusters, main propulsion systems, and motor control centers (MCCs). These have been ranked based on their criticality in vessel operational performance, security, and safety. Existing cyber-related measures that have been identified include the physical cyber-separation in some vessel systems and the existing schedule for system software upgrades.

In Step 2 of the SRA process, the following are carried out:

i. Adversaries are identified and evaluated;
ii. Threat ranking for each adversary is assigned;
iii. Security countermeasures are applied;
iv. Identified assets' attractiveness ranking is analyzed and assigned.

The adversaries identified include criminals, interstate adversaries, disgruntled employees, and terrorists. The potential security breach scenario was identified as the planting of malware into control systems and a direct remote cyber-attack to vessel OT and IT systems. Asset attractiveness was assigned based on asset, component, and process interconnections.

In Step 3 of the SRA process, the following are accomplished:

i. Security breach scenarios are defined, and their consequences are evaluated;
ii. Security breach scenario sequence and consequences are evaluated;
iii. Effectiveness of existing security barriers are evaluated;
iv. Vulnerabilities are identified, considering recovery capability and estimating vulnerability degree;

v. Severity ranking of scenario-specific consequences is allocated.

The two main security breach scenarios identified are: (a) the intentional remote planting of malware, corruptive software virus, etc.; (b) the unintentional introduction of malware through a remote USB device. Both scenarios result in the disruption of operations and cause system failure. The main vulnerabilities for IT/OT and control systems identified are (a) the remote connectivity of controls with company's maintenance hub; (b) the existence of obsolete or vulnerable hardware or software that can lead to cyber contamination of the network and vessel systems.

In Step 4 of the SRA process, the following tasks are completed:

i. Conditional likelihood of scenarios is evaluated;
ii. Initial risk ranking is assigned;
iii. Risk is prioritized.

Considering the existing history of cyber breach incidents of maritime assets, the scenarios of intentional remote cyber-attacks and cyber contamination from an external adversary, such as a criminal and a vessel crew member, received a higher risk ranking. The unintentional cyber contamination of IT/OT systems from a vessel crew member was ranked equally in risk level.

Finally, in Step 5 of the SRA process, the following are achieved:

i. The necessity for countermeasures is evaluated along with the recommendations for specific assets;
ii. Likelihood of attack and severity of scenario consequences are recalculated;
iii. Residual risk is determined;
iv. Recommended measures are prioritized.

The main countermeasures determined against the identified cyber security breach scenarios included (a) upgrading the electronic/IT protection systems; (b) installation of firewalls for all segmented systems and subsystems; (c) assignment of an on-board IT expert, as the likelihood of an intentional or unintentional cyber breach scenario from an external (i.e., criminal) or internal (i.e., vessel crew member) threat still ranked high. The implementation of a rigorous IT and OT software and hardware upgrade, the execution of a cybersecurity training program for vessel crew members and the allocation of a specialized IT technician on board the vessel were considered high priority. The residual risk for cyber breach scenarios remained, however, due to the following reasons:

- The anticipated difficulty in the implementation of the recommended measures due to the presence of financial and technical constraints;
- The continuously evolving sophistication and ingenuity of cyber-attacks.

From the above, it can be determined that while the API STD 780 SRA method applied was not evaluated in-depth for all technical cyber physical systems, since it was applied at a macroscopic level, it is obvious that it is a capable tool that assists in the security analysis of complex industrial as well as maritime assets such as those found on an FPSO vessel.

5.2. Bow Tie Analysis (BTA)

Bow Tie Analysis (BTA) is a qualitative Process Safety Management (PSM) method primarily used in the oil and gas, chemical, and processing sectors for the proactive and reactive review of safety incidents. Bow Tie Analysis is used for the definition of risks, hazards, and consequences of safety incidents in systems, equipment, processes, and operations. Bow Tie Analysis is also applicable in the maritime sector, as it can be used to analyze the interconnection of marine equipment, systems, and processes in vessels and other maritime assets in the case of safety incidents. For physical and cyber security applications, Bow Tie Analysis can be used to identify the applicable security barriers and mitigation measures for IT/OT assets and processes at the micro- and macro-scales.

- Micro: components, equipment, sub-assemblies, and instruments;
- Macro: assemblies, assets, larger equipment, and operations.

The bow tie diagram, as shown in Figure 4, has the following elements [77]:

- Hazard: a condition that can potentially cause damage;
- Top Event: The event that can occur due to the loss of control of the hazard;
- Threats (depicted on the left side of the bow tie diagram): events or scenarios that could cause the loss of control of a hazard and lead to a top event;
- Consequences (depicted on the right side of the bow tie diagram): unwanted harmful effects that can affect the assets, system, process, people, or the environment;
- Prevention Barriers (on the left side of the diagram): prevention barriers that stop threats from resulting in the top event;
- Mitigation Barriers (to the right of the top event): mitigation barriers that mitigate the top event (i.e., reduce the scale of and possibly stop undesired consequences);
- Degradation Factors: factors that can be applied to both prevention and mitigation barriers and can lead to damage or failure of the barrier to which they are attached;
- Degradation Controls: Control barriers that act to mitigate the degradation factors, assuring the function of the preventive or mitigation barriers. Barriers and degradation controls are illustrated to show these as fundamental elements of the safety management system. Altogether, the diagram provides a holistic picture of the risk management system.

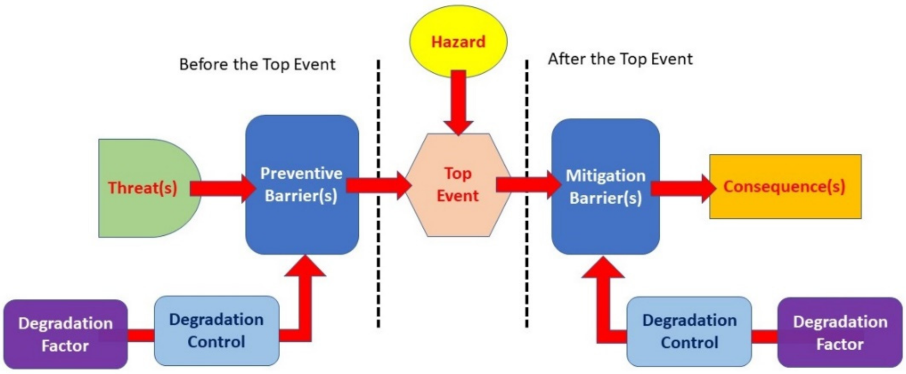

Figure 4. Bow Tie Analysis diagram.

Bow Tie Analysis is an effective methodology to assess and manage security hazards, risks, consequences, and their mitigation. In general, it has the following advantages [78]:

- Ease of use;
- Communicates to all levels of an organization, being highly visual and without excessive or complicated documentation;
- Forces the user to think in terms of risk assessment and barrier-based risk management from the outset;
- Builds system robustness in a logical, structured, and incremental manner;
- Enforces the importance of effective barrier and mitigation management;
- Easily identify areas of weakness in any system;
- Quickly prioritize safety and operational and business critical tasks and objectives;
- Readily integrates with existing management systems;
- Provides assurance via a visual link between bow tie and business processes;
- Promotes awareness of hazards, risks, and management methods;
- Supports brainstorming and hazard identification;
- Effective demonstration of hazard management;
- High-level hazard identification and risk assessment;
- Complements incident investigation and safety and risk regulations.

The application of the Bow Tie Analysis method in cyber security has been demonstrated in general industrial sectors by third-party engineering and cyber security consultants [79,80] and industry organizations [81]. While the usage of the Bow Tie Analysis method is not directly applied in the maritime sector, due to the complexity of the systems involved, it is determined as also being applicable for maritime assets. Considering the cyber physical systems found in maritime assets, Shuang-Hua et al. [82] developed a harmonizing methodology to analyze safety and security risks simultaneously for industrial applications and cyber physical systems. Their methodology incorporated the Bow Tie Analysis method and security assessment via examining preventive barriers. Similarly, Meland et al. [83] determined that the Bow Tie Analysis method is suitable for the analysis of security and safety of cyber and physical systems, identifying a wide range of proactive (preventive) and reactive mitigating barriers. Abdo et al. [84] developed another methodology that integrates the attack tree and Bow Tie Analysis methodologies for a combined safety and security industrial risk analysis including cyber security applications. Using this method, the representation of risk scenarios and quantification of likelihood provide the right control measures. Finally, Bernsmed et al. [85] use the Bow Tie Analysis method as a tool to analyze and visualize physical and cyber security risks and presented their approach using an example in the maritime sector involving navigational communication systems. In addition to the above, Bow Tie Analysis was proposed by DNVGL-RP-G496 [43] as an assessment tool of preventive and reactive security barriers of vessels and mobile offshore units' cyber systems. Similarly, ISO/IEC 31010 [86] mentions Bow Tie Analysis as a risk management tool for cyber systems and cyber security applications.

Application of the Bow Tie Analysis Method in a Maritime Cyber Physical Asset

In order to illustrate the applicability of Bow Tie Analysis as a methodology for risk assessment and management for cyber and physical security, an example involving the malware contamination of a vessel's engine human–machine interface (HMI) system is be described below. The scenario involves a typical IT–OT interface through network communication influenced by data transferred via external sources (network or external device) which leads to the malware contamination of the engine's HMI and the incorrect display of the engine's performance data. The IT–OT communication flow path through the vessel's ICS is shown in Figure 5.

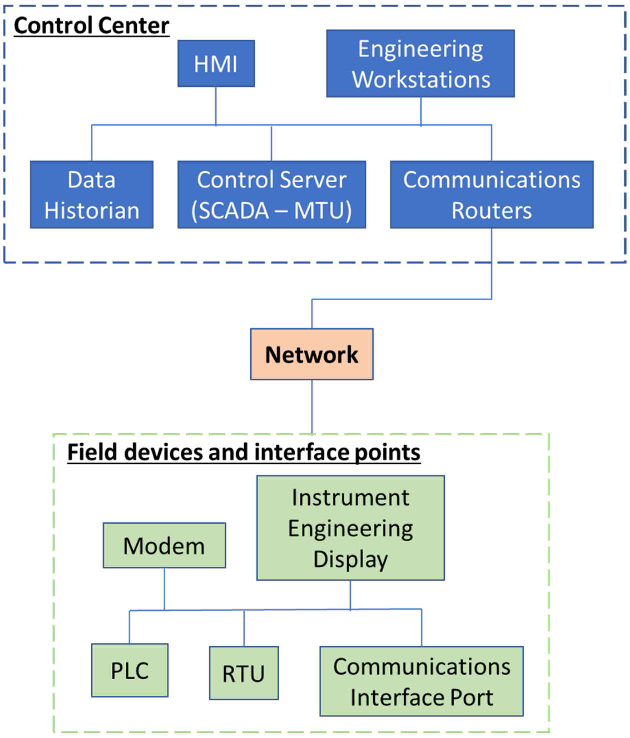
Control Center
HMI
Engineering Workstations
Data Historian
Control Server (SCADA – MTU)
Communications Routers
Network
Field devices and interface points
Modem
Instrument Engineering Display
PLC
RTU
Communications Interface Port

Figure 5. Vessel's ICS communication data flow.

Basically, the vessel's engine control center communicates to field devices through network data flow. The control center includes the HMI, engineering workstation(s), server data historian, control server, and communication routers and interface ports, among other systems. The field devices include interface ports, PLCs (Programmable Logic Controllers), RTUs (Remote Terminal Units), and Instrument Engineer Displays (IEDs). The Bow Tie Analysis example for this scenario is shown in Figure 6.

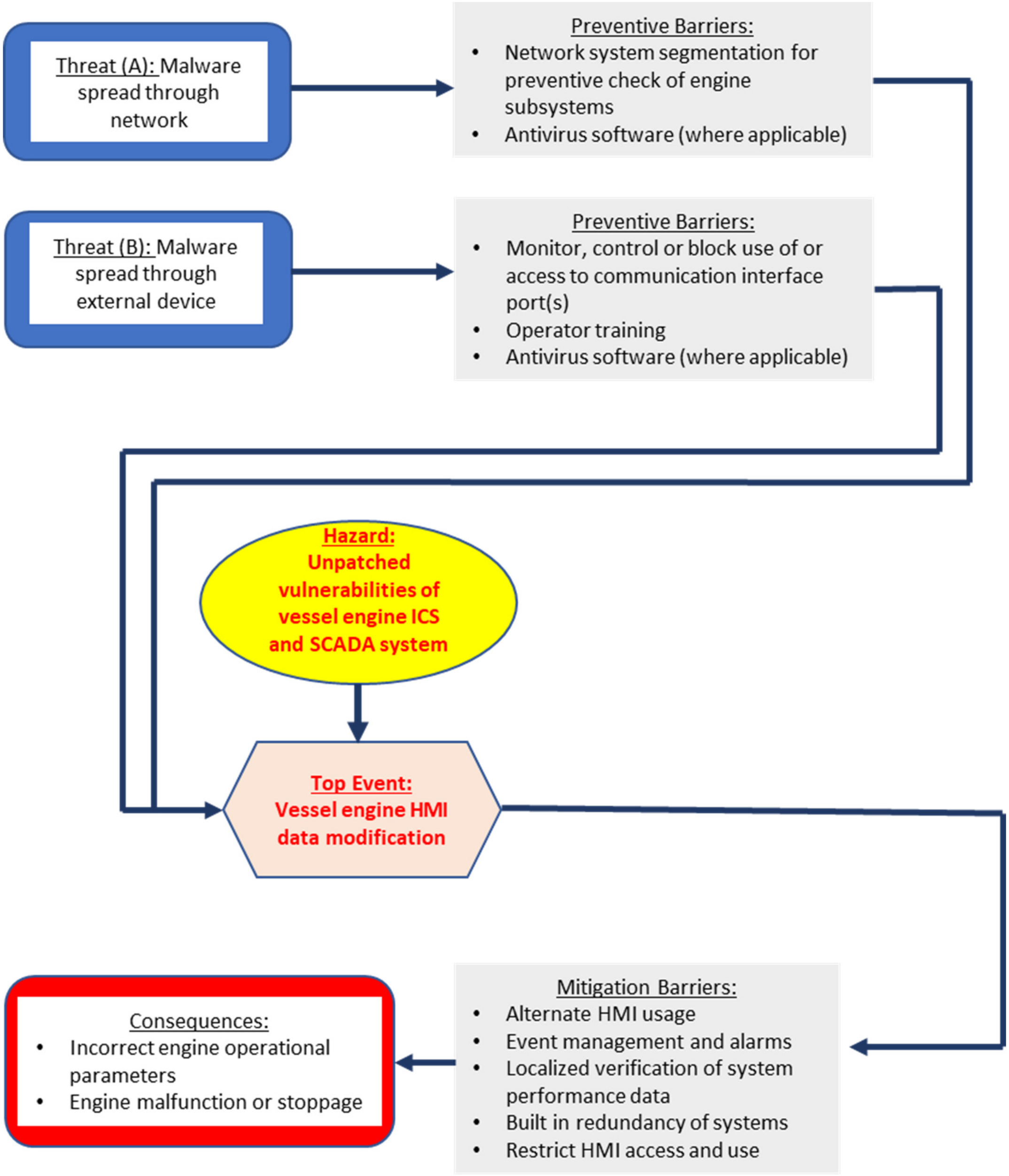
Threat (A): Malware spread through network
Preventive Barriers:
• Network system segmentation for preventive check of engine subsystems
• Antivirus software (where applicable)
Threat (B): Malware spread through external device
Preventive Barriers:
• Monitor, control or block use of or access to communication interface port(s)
• Operator training
• Antivirus software (where applicable)
Hazard: Unpatched vulnerabilities of vessel engine ICS and SCADA system
Top Event: Vessel engine HMI data modification
Mitigation Barriers:
• Alternate HMI usage
• Event management and alarms
• Localized verification of system performance data
• Built in redundancy of systems
• Restrict HMI access and use
Consequences:
• Incorrect engine operational parameters
• Engine malfunction or stoppage

Figure 6. Bow Tie Analysis for vessel engine HMI data modification due to the fact of malware contamination.

Figure 6 shows the malware contamination threat being analyzed involving two different sub-scenarios. In the first threat scenario, the malware spread is caused by network data flow. In this case, one of the preventive barriers for such a threat is network system segmentation, limiting or controlling data flow and allowing preventive checks of the engine's subsystems. The second threat scenario involves engine HMI malware contamination due to the fact of its connection to an external device. Such a device can be a technician's or engineer's laptop, or an external storage drive used to update ICS software during maintenance operations. One of the preventive barriers in this case would be the monitoring, control, or blockage of the use of or access to the communication interface ports. In this way, unintentional or intentional transfer of malware to systems is eliminated. Another preventive barrier would be operator training, which would raise cyber-awareness and cyber hygiene practices and improve the monitoring of critical operational parameters and intervention in the case of excessive deviations being noticed. The use of an antivirus software is also a useful tool and a preventive barrier for both cases, eliminating the installation of malware. Unfortunately, it is not always applicable to vessels' systems due to the varied type and age of IT and OT systems and software on board vessels.

In the post-event side of the bow tie diagram, the mitigation barriers that could be used after the HMI data modification would include the design and integration of redundant devices to enable the use of substitute systems such as an alternate HMI. Event management and alarm notifications could also be included in the system assuming they are integrated within and do not overlap or duplicate such existing systems. The localized verification of the operational parameters of engine systems would also be a reliable barrier to monitor the overall system performance and act against any noted operational malfunctions or abnormalities. For such a method, however, the operator's in-depth knowledge of system performance and operations would be necessary to ensure the proper interpretation of system data. The control and restriction of HMI access could also be implemented as a physical security method to ensure the unauthorized access to systems data is prevented. The ultimate consequence of the failure of all preventive and mitigating barriers would be the display of incorrect operational and performance data through the vessel's engine HMI, resulting in the vessel's engine malfunction, damage, and possible complete stoppage.

Finally, it should be emphasized that the example given highlights the human factor (HMI operator) to machine (OT systems and devices, e.g., HMI) interface and the deriving degradation factors. Human factors (operator use and knowledge of systems) can degrade any preventive or mitigating barriers applied, leading to destructive consequences. Human factors are at the center of the risk management process applied in IT/OT systems. IT/OT system operators and end users need to understand the importance of their roles in maintaining preventive and mitigating barriers. The Bow Tie Analysis method can be a valuable tool to prepare and educate IT/OT system operators and users to ensure cyber physical security breach scenarios are minimized, eliminated, or contained by the use of proper barriers.

6. Risk Treatment—Design of Cyber Security Controls

Substantial guidance exists to support the design of effective technical risk treatments and cyber security controls. This includes well-developed frameworks and other references from government and standards-setting bodies as well as a large base of industry best practices. While individual control requirements should be expected to present some degree of uniqueness in relation to unique risk characteristics, there can be substantial value achieved by the application of a standards-based approach to establish the majority of the controls architecture.

There has been substantial coalescence around the NIST cyber security standards across industries. The US Coast Guard (USCG) has collaborated with the US National Cyber Security Center of Excellence (NCCOE) to specifically address cyber concerns related to maritime, providing guidance related to many of the industry's dimensions described previously in this paper. This includes application of the NIST Cyber Security Framework (NIST CSF) to specific maritime challenges including maritime bulk liquids transfer, offshore operations, and passenger vessel operations [87].

NIST CSF incorporates technical and process dimensions to provide a basis for a comprehensive controls design that established major functional groupings of cyber security activities with subsequent decomposition into categories and subcategories. The first function, Identify, is intended to guide an enterprise to inventory all relevant assets including technologies, data, and personnel. Attention is then turned to the Protect function that includes the design of safeguards relevant to the identified asset base. Next is analysis of the Detect functions including automated monitoring and associated incident alerting. Detect activities then feed the Respond function, outlining the essential system and personnel reactions to observed events. Lastly, the functional requirements to Recover the organization and guide resumption of normal function are described. The result is a robust framework that interrelates ongoing controls design and operation along with necessary response steps when incidents are suspected [88].

NIST CSF describes how the controls design should ideally be guided by the organization's risk management processes and perspectives, which should be derived from the enterprise's risk management posture. Organizational factors, such as risk appetite, legal frameworks, and organizational business or process needs, combine to form the risk posture. NIST CSF illustrates the "notional information and decision flows within an organization", describing the interaction of operational, organizational management, and senior executives. These information and decision flows provide a basis to govern the degree of interaction between IT and OT systems [88].

A significant characteristic that adds complexities to control designs, however, is cyber physical systems, that by definition, reflect the convergence of the cyber and the physical. Therefore, unlike other contexts, the designer of cyber physical controls must consider the unique aspects of threat, vulnerability, and impact. For example, application of the NIST CSF to information systems often manifests as exercises in logging and alerting, whereas cyber physical controls will also potentially require incorporation of physical reactions such as ceasing forward motion, stopping the flow of materials, or ensuring physical aspects "fail closed" to prevent potentially disastrous physical outcomes. The NIST CSF and other industry-neutral cyber security standards do not reflect such risk dimensions.

Once implemented, the controls design requires ongoing oversight using continuous monitoring technologies as well as a robust program of audits and assessment. Technical monitoring control designs are also described in the NIST CSF and provide the basis for the deployment of Security Incident and Event Management (SIEM) architectures that can help the organization manage the continuous inflow of event data, which increasingly present as high-frequency data streams. Advances in artificial intelligence and machine learning technologies offer some promise for helping organizations navigate the substantial event data generated.

The application of available standards, such as the NIST CSF, establishes a framework for the design of adequate controls that will require periodic evaluation to ensure controls are operationally effective. This includes the completion of manual and automated controls testing and using techniques, such as penetration testing, to simulate adversary conduct. The periodic execution of controls effectiveness audits and tests is a staple in other industries and should be considered essential in the maritime context.

7. Discussion

The review of available industry and governmental directives and standards has proved the fact that cyber physical security in maritime assets and, in effect, OT cyber security, while although it is recognized as critical in the overall cyber security of assets, it is not covered adequately to provide solutions for the maritime industry. The majority of available standards and directives focus primarily on the IT side of systems and operations and fail to define mitigation measures and procedures that would guide asset owners and operators in confronting the credible threats faced. Those that do cover cyber physical security are either prescriptive or performance based and do not highlight the need for corporate policies and procedures that would apply to maritime assets both onshore and offshore.

Considering the physical security element involved for cyber systems, asset owners and operators need to realize the need for the actual physical protection and security required for such systems, components, and processes including portable and personal devices used for business or operations on board vessels. Vessel and facility physical security while enforced by the ISPS (International Ship and Port Facility Security) Code, remains partly applied to the physical security of critical cyber assets despite the cyber risk management imposed by the implementation of IMO Resolution MSC.428(98) and IMO Guidance MSC-FAL.1/Circ.3. The enforcement of IEC-62443 could provide mitigation measures and procedures that if followed by asset owners and operators, could provide superior protection of critical cyber systems and functions of assets. This could be through the establishment of complementary physical and cyber security policies that would address both physical and cyber security in the protection of maritime assets in the microscopic scale (systems, components, and processes on board vessels). The application of physical security controls and barriers for specific components or systems of a vessel or maritime facility could control and mitigate unauthorized access to protected assets. This could be further controlled and enforced by the provision of specific access and entry controls for each security barrier or control established.

The auditing of the cyber security and operations of critical components and processes of maritime assets should also be considered by asset owners and operators. This auditing should look into both the technical design and performance of as well as the service provision to maritime assets and their systems and components. This auditing process, if applied by asset owners and operators, could provide the following:

(a) Identification of remote access to the asset, its systems, and functions;
(b) The definition of the existing level of hardening of cyber systems and processes;
(c) The verification of performance and integrity of service providers to the maritime asset owner (shipping company) and operator (vessel crew);
(d) The suitability and adequacy of existing corporate contract documents for the provision of services considering cyber physical security requirements;
(e) The identification of critical systems and functions onboard the vessel and within the shipping company (asset owner);
(f) The asset posture for operational and technical resiliency;
(g) The existing system notification sequence and mechanisms in place that would alert the asset owner and operator in case of a cyber breach incident.

The above could be achieved by the use of security risk assessment methods from the industrial sectors such as the security risk assessment method from API STD 780 and the Bow Tie Analysis method. Considering the advancement of cyber physical security in the general industrial and oil and gas sectors for SCADA systems, the implementation of assessment tools outside the maritime industry could provide advanced capabilities for complex OT systems onboard vessels.

Similarly, the MITRE ATT&CK Threat Model [89] could be used to preemptively classify cyber-attacks and assess organizational risks [90]. It could assist in the understanding of the attack behavior, tactics, and techniques of cyber adversaries and allow for the proper organization of such data [91] for use by the corporate (shipping company or asset owner) chief information security officer (CISO) and cyber mitigation team. Due to the versatility of the MITRE ATT&CK Threat Model for the assessment of enterprise IT networks and cloud, mobile devices, and industrial control systems (ICS) [90], its use for the characterization and verification of post-compromise adversary behavior while operating within maritime asset IT and OT systems and infrastructure and networks could prove to be a useful vulnerability assessment tool.

The maritime industry, equally to other industries, also appears to tackle cyber physical security considering two distinct operational and technical functions, the physical security function, as dictated by the ISPS code, and the cyber security function. This division of cyber and physical security functions necessitates the distinct roles of a CISO and the "asset" physical security officer which, according to the ISPS code, entails the combination of a ship security officer (SSO), vessel security officer (VSO), port facility security officer (PFSO), and company security officer (CSO). This segmentation of duties includes the segmentation of security (cyber and physical) operational policies and procedures that basically lead to "siloed" security functions and, in turn, to hindered collaboration and visibility of interconnected cyber–physical assets and processes and the reduced capacity to tackle complex security threats (physical, cyber, or hybrid). The solution for this issue would be the convergence of security functions at a corporate and operational level as also suggested by CISA [92]. This convergence of cyber and physical security functions would lead to a fully integrated security perception at an operational and technical level, enhanced security of assets (components, systems, and operations), and reinforced organizational and operational security and awareness.

Similar to the segmentation of cyber and physical functions as described previously, the maritime industry also appears to address cyber security considering two distinct operational and technical entities: the shore-based infrastructure and the maritime-based asset infrastructure. The shore-based infrastructure, as described in Section 1, includes the infrastructure supporting the maritime asset and operations and focuses primarily on IT operations and systems. The maritime-based asset infrastructure consists of the vessel's cyber systems, components, and functions that enable, monitor, and control its maritime operations. This corporate approach to cyber segmentation leads to the deconstructed security approach between IT processes and systems ashore and the OT systems and processes onboard maritime assets offshore. This leads further to the diminished corporate understanding of IT and OT functions and vulnerabilities onboard maritime assets and the cyber and physical security threats faced. In this case, maritime asset owners need to invest in the general cyber awareness of their assets and operations by following a holistic approach that includes both OT and IT systems and functions for both their corporate organizations and their maritime assets.

Finally, considering the human element interface in cyber physical systems, as highlighted in Section 1, the reinforcement of cyber security skills for personnel active in the maritime domain should be considered of paramount importance and should be implemented accordingly. Significant investment in the training of maritime vessel operators (crew) and shipping company personnel should be dedicated. Training should be implemented for all personnel across the corporate hierarchy, from field personnel (vessel crew) to company executives. Cyber security-related training should be customized for specific maritime operational stakeholders such as all officers of the engine and deck departments as well as technical superintendents. These stakeholders should be educated to the level of the IT and OT systems utilized on board vessels so that they can contribute to the design, implementation, monitoring, and control of cyber physical security barriers and mitigation measures. As the cyber security threats and IT/OT technologies are evolving, the provided training needs to be revised and re-applied at a recurring rate.

8. Conclusions

The following key points and conclusions were derived from the analysis undertaken in this paper:

(a) The majority of available standards, policies, and directives focus primarily on the IT side of systems and operations and fail to tackle the interoperability and threats to OT systems and components in the maritime sector;

(b) The importance of the physical protection of IT and OT assets needs to be recognized by asset owners, operators, and integrators. The enforcement of physical protection and security of portable devices and critical IT/OT infrastructure onshore and offshore can mitigate imminent cyber threats;

(c) The auditing of cyber security and operations of critical components and processes of maritime assets should be realized by asset owners and operators, considering their technical design, performance, and service provisions. Auditing can expose unknown vulnerabilities in systems, processes, and infrastructure while also verifying the effectiveness and status of already in place corporate and technical measures and procedures;

(d) The use of "out-of-the-industry" security risk assessment methods should be examined. Existing security assessment methods, such as the API STD 780 SRA and the

Bow Tie Analysis methods, have shown their capability to tackle complex industrial systems in the processing and oil and gas industries, similar to the ones found onboard maritime assets;

(e) The convergence of shore-based and vessel-based cyber and physical security should be pursued by maritime asset owners and operators. This could enhance cyber and physical security policies' implementation and improve threat mitigation;

(f) Cyber security knowledge for maritime vessel operators (crew) and shipping company personnel should be further improved by the implementation of proper training. This can be achieved only through the allocation of adequate funding, corporate commitment, and the realization of a holistic stakeholder involvement and management process for cyber-related functions at a corporate and field level.

The submitted paper is considered novel in its concept and contributes to the scientific and academic fields because it focuses on IT/OT system interfaces and cyber physical security specifically for the maritime sector. The industry and governmental standards, policies, and directives reviewed make this paper a single source of information where academics and industry associates can educate themselves and understand the complexity of cyber physical and IT/OT systems in the maritime sector as well as the available directives that they ought to conform to. The presentation of two security risk assessment methods, the API STD 780 SRA and the Bow Tie Analysis methods, is also novel in its concept, because it presents "outside-the-box" thinking for sourcing risk assessment methods from the oil and gas and process safety sectors that can be applied in maritime cyber physical security applications. These methods have proved their usability for complex systems and assets and can handle the IT/OT system interface and complexity for maritime assets.

Finally, further research in the field of cyber physical security could expand in the use of other assessment methods from the accident investigation and security assessment sectors. The use of methods, such as STAMP (Systems-Theoretic Accident Model And Processes), ACCIMAP, Tripod Beta, CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability), RAMCAP (Risk Analysis and Management for Critical Asset Protection), or MBVA/MBRA (Model-Based Vulnerability Assessment/Model-Based Risk Assessment) could be compared to BTA and SRA in possible cyber physical security breach scenarios. Further analysis of more complex IT and OT systems used in maritime assets could be also carried out to identify the weaknesses in system architecture and possibly improve system design and operation.

Author Contributions: I.P. conceived the original title and layout of the paper and wrote and edited the draft and final manuscript; P.R. conceived the idea and revised title and contributed to the layout of the paper, co-wrote manuscript sections, and co-edited the draft and final manuscript. N.N. provided supervision, direction on the layout and structure of the paper, vessel operational information and reviewed the draft and final manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zarzuelo, I.; Soeane, M.; Bermudez, B. Industry 4.0 in the port and maritime industry: A literature review. *J. Ind. Inf. Integr.* **2020**, *20*, 100173.
2. Svilicic, B.; Rudan, I.; Jugovic, A.; Zec, D. A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. *J. Mar. Sci. Eng.* **2019**, *7*, 364. [CrossRef]
3. Dahman, J.S.; Baldwin, K.J. Understanding the current state of US defense systems of systems and the implications for systems engineering. In Proceedings of the 2nd Annual IEEE Systems Conference, Montreal, QC, Canada, 7–10 April 2008.
4. American Petroleum Institute (API). *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*; American Petroleum Institute: Washington, DC, USA, 2004.

5. Mathews, L. NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million. Available online: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/?sh=4a211fae4f9a.2017 (accessed on 10 June 2021).
6. Parizo, E. Maersk CISO Says NotPeyta Devastated Several Unnamed US Firms. Available online: https://www.darkreading.com/threat-intelligence/maersk-ciso-says-notpeyta-devastated-several-unnamed-us-firms/a/d-id/1336558.2019 (accessed on 10 June 2021).
7. Nguyen, A. Port of San Diego Hit with Ransomware; Hackers Demanded Payment in Bitcoin. 2019. Available online: https://www.nbcsandiego.com/local/port-of-san-diego-hit-with-ransomware-hackers-demanded-payment-in-bitcoin/50375/ (accessed on 10 June 2021).
8. Schuler, M. Clarkson Plc Reveals Details of 2017 Cyber Security Incident. 2018. Available online: https://gcaptain.com/clarkson-plc-reveals-details-of-2017-cyber-security-incident/ (accessed on 10 June 2021).
9. Rundle, J. Coast Guard Details February Cyberattack on Ship. Available online: https://www.wsj.com/articles/coast-guard-details-february-cyberattack-on-ship-11564133401 (accessed on 6 August 2021).
10. Goward, D. New GPS 'Circle Spoofing' Moves Ship Locations Thousands of Miles. Available online: https://www.gpsworld.com/new-gps-circle-spoofing-moves-ship-locations-thousands-of-miles/ (accessed on 15 June 2021).
11. Bush, D. Ethical Hacker Says Ships Are Wide Open to Cyber Attack. Available online: https://lloydslist.maritimeintelligence.informa.com/LL1136933/Ethical-hacker-says-ships-are-wide-open-to-cyber-attack (accessed on 20 August 2021).
12. Bebbington, T. Cyberattack or Coincidence? Available online: https://www.seatrade-maritime.com/opinions-analysis/cyberattack-or-coincidence (accessed on 6 August 2021).
13. USCG. Cyberattack Impacts MTSA Facility Operations. 2019. Available online: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf (accessed on 10 June 2021).
14. Weiss, J. The Colonial Pipeline Cyberattack—Did IT/OT Convergence Contribute to the Attack. 2021. Available online: https://www.controlglobal.com/blogs/unfettered/the-colonial-pipeline-cyberattack-did-itot-convergence-contribute-to-the-attack (accessed on 15 May 2021).
15. Gold, J. What is the Industrial Internet of Things? Essentials of IIoT. 2018. Available online: https://www.networkworld.com/article/3243928/what-is-the-industrial-internet-of-things-essentials-of-iiot.html (accessed on 6 June 2021).
16. Henshell, A. Taylorism and the History of Processes: 6 Key Thinkers You Should Know. 2018. Available online: https://www.process.st/taylorism/ (accessed on 15 June 2021).
17. Bhatti, B. 7 Types of AI Risk and How to Mitigate their Impact. 2020. Available online: https://towardsdatascience.com/7-types-of-ai-risk-and-how-to-mitigate-their-impact-36c086bfd732 (accessed on 5 June 2021).
18. International Maritime Organization (IMO) Resolution MSC. *Maritime Cyber Risk Management in Safety Management Systems*; International Maritime Organization: London, UK, 2017; Volume 428.
19. International Maritime Organization (IMO) Resolution MSC-FAL.1/Circ.3. *Guidelines on Maritime Cyber Risk Management*; International Maritime Organization: London, UK, 2017.
20. BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF AND IUMI, "The Guidelines on Cyber Security Onboard Ships", Version 3.0. 2021. Available online: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf (accessed on 15 August 2021).
21. National Institute of Standards and Technology (NIST) Cyber Security Framework. Available online: https://www.nist.gov/cyberframework (accessed on 25 May 2021).
22. National Institute of Standards and Technology (NIST) Special Publication 800-30. Guide for Conducting Risk Assessments. 2012. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (accessed on 13 May 2021).
23. National Institute of Standards and Technology (NIST) Special Publication 800-37. Risk Management Framework for Information Systems and Organizations—A System Life Cycle Approach for Security and Privacy. 2018. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (accessed on 23 May 2021).
24. National Institute of Standards and Technology (NIST) Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. 2015. Available online: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final (accessed on 20 May 2021).
25. National Institute of Standards and Technology (NIST) Special Publication 1500-201. Framework for Cyber-Physical Systems: Volume 1, Overview. 2017. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf (accessed on 25 May 2021).
26. National Institute of Standards and Technology (NIST) Special Publication 1500-202. Framework for Cyber-Physical Systems: Volume 2, Working Group Reports. 2017. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-202.pdf (accessed on 29 May 2021).
27. National Institute of Standards and Technology (NIST) Special Publication 1500-203. Framework for Cyber-Physical Systems: Volume 3, Timing Annex. 2017. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-203.pdf (accessed on 20 May 2021).
28. International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 27001. *Information Technology—Security Techniques—Information Security Management Systems—Requirements*; International Organization for Standardization: Geneva, Switzerland, 2013.

29. International Electrotechnical Commission standard IEC-62443-4-2. *Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components*; International Organization for Standardization: Geneva, Switzerland, 2019.
30. International Electrotechnical Commission standard IEC 62443-3-3. *Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels*; International Organization for Standardization: Geneva, Switzerland, 2013.
31. International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 21827. *Information Technology—Security Techniques—Systems Security Engineering—Capability Maturity Model®(SSE-CMM®)*; International Organization for Standardization: Geneva, Switzerland, 2008.
32. International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 18045. *Information Technology—Security Techniques—Methodology for IT Security Evaluation*; International Organization for Standardization: Geneva, Switzerland, 2008.
33. International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 15408-1. *Information Technology—Security Techniques—Evaluation Criteria for IT Security*; International Organization for Standardization: Geneva, Switzerland, 2009.
34. International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 27032. *Information Technology—Security Techniques—Guidelines for Cybersecurity*; International Organization for Standardization: Geneva, Switzerland, 2012.
35. American Society for Testing and Materials standard ASTM F3286-17. *Standard Guide for Cybersecurity and Cyberattack Mitigation*; ASTM International: West Conshohocken, PA, USA, 2017.
36. American Society for Testing and Materials standard ASTM F3449-20. *Standard Guide for Inclusion of Cyber Risks into Maritime Safety Management Systems in Accordance with IMO Resolution MSC.428(98)—Cyber Risks and Challenges*; ASTM International: West Conshohocken, PA, USA, 2020.
37. International Association for Classification Societies (IACS) Recommendation No. 166: "Recommendation on Cyber Resilience". 2020. Available online: https://www.iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr1/ (accessed on 15 August 2021).
38. American Bureau of Shipping (ABS). *Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations—ABS CyberSafety*; American Bureau of Shipping (ABS): Houston, TX, USA, 2016; Volume 1.
39. American Bureau of Shipping (ABS). *Guide for Cybersecurity Implementation for the Marine and Offshore Industries—ABS CyberSafety*; American Bureau of Shipping (ABS): Houston, TX, USA, 2018; Volume 1.
40. American Bureau of Shipping (ABS). *Guidance Notes on Data Integrity for Marine and Offshore Operations—ABS CyberSafety*; American Bureau of Shipping (ABS): Houston, TX, USA, 2016; Volume 3.
41. American Bureau of Shipping (ABS). *Guide for Software Systems Verification—ABS CyberSafety*; American Bureau of Shipping (ABS): Houston, TX, USA, 2016; Volume 4.
42. American Bureau of Shipping (ABS). *Guidance Notes on Software Provider Conformity Program—ABS CyberSafety*; American Bureau of Shipping (ABS): Houston, TX, USA, 2016; Volume 5.
43. DNV GL. (Det Norske Veritas-Germanischer Lloyd) Recommended Practice DNVGL-RP-G496. In *Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation*; DNVGL-RP-0496; DNV GL: Oslo, Norway, 2016; Volume 5.
44. DNV GL. (Det Norske Veritas-Germanischer Lloyd) Class Programme Type Approval DNVGL-CP-0231. In *Cyber Security Capabilities of Control System Components*; DNVGL-RP-0496; DNV GL: Oslo, Norway, 2018.
45. Lloyd's Register Guidance Note. *Cyber-Enabled Ships—Deploying Information and Communications Technology in Shipping—Lloyd's Register's Approach to Assurance*; Lloyd's Register: London, UK, 2016.
46. Lloyd's Register Guidance Note. *Cyber-Enabled Ships—ShipRight Procedure—Autonomous Ships*; Lloyd's Register: London, UK, 2016.
47. Lloyd's Register Guidance Note. *Cyber-Enabled Ships—Type Approval of Cyber Enabled Systems Components*; Lloyd's Register: London, UK, 2016.
48. Class, N.K. *Guidelines for Designing Cyber Security Onboard Ships*, 2nd ed.; Class N.K.: Tokyo, Japan, 2020.
49. Class, N.K. *Cyber Security Management Systems for Ships*, 1st ed.; Class N.K.: Tokyo, Japan, 2019.
50. Croatian Register of Shipping (CRS) ISM Code Statutory Newsletter Number 03.08.202. *Maritime Cyber Security Risk Management*; Croatian Register of Shipping: Split, Croatia, 2020.
51. Indian Register of Shipping (IRCLASS) Guidelines IRS-G-SAF-02 -2018. *Maritime Cyber Safety*; Indian Register of Shipping: Mumbai, India, 2018.
52. Indian Register of Shipping (IRCLASS) Guidelines IRS-G-DES-01—2019. *Certification of Software for Computer Based Control Systems*; Indian Register of Shipping: Mumbai, India, 2019.
53. Russian Maritime Register of Shipping ND No. 2-030101-040-E—2021. *Guidelines on Cyber Safety*; Russian Maritime Register of Shipping: Saint Petersburg, Russia, 2021.
54. The International Registries and Maritime Administrator of The Republic of the Marshall Islands Marine Guideline No. 2-11-16. *Maritime Cyber Risk Management*; The International Registries and Maritime Administrator of The Republic of the Marshall Islands: Reston, VA, USA, 2018.

55. The International Registries and Maritime Administrator of The Republic of the Marshall Islands Ship Security Advisory No. 13-20. *Cyber Risk Management—Revised Industry Guidelines and United States Port State Control Measures*; The International Registries and Maritime Administrator of The Republic of the Marshall Islands: Reston, VA, USA, 2020.
56. Bureau Veritas, Rule Note NR 642 DT R00 E. *Cybersecurity Requirements for Products to be Installed On-Board Naval Ships*; Bureau Veritas: Neuilly-sur-Seine, France, 2018.
57. Bureau Veritas, Rule Note NR 659 DT R01. *Rules on Cyber Security for the Classification of Marine Units*; Bureau Veritas: Neuilly-sur-Seine, France, 2020.
58. U.S. Congress Bill. S. 4023 Enhancing Maritime Cybersecurity Act of 2020. 22 June 2020. Available online: https://www.govtrack.us/congress/bills/116/s4023/text (accessed on 19 May 2021).
59. U.S. Coast Guard; U.S. Department of Homeland Security. Navigation and Vessel Inspection Circular (NVIC) 01-20 Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities. 26 February 2020. Available online: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023 (accessed on 10 May 2021).
60. U.S. Coast Guard; U.S. Department of Homeland Security. Office of Commercial Vessel Compliance (CG-CVC) Mission Management System (MMS) Work Instruction (WI) CVC-WI-027 "Vessel Cyber Risk Management Work Instruction. 18 February 2021. Available online: https://www.dco.uscg.mil/Portals/9/CVC-WI-27%282%29.pdf (accessed on 23 May 2021).
61. UK Institution of Engineering and Technology (IET) Guidance Document. *Code of Practice: Cyber Security for Ships*; UK Institution of Engineering and Technology: London, UK, 2017.
62. UK Institution of Engineering and Technology (IET) Good Practice Guide. *Cyber Security for Ports and Port Systems*; UK Institution of Engineering and Technology: London, UK, 2020.
63. Council of the European Union, 10494/18. *Council Conclusions on the Revision of the European Union Maritime Security Strategy (EUMSS) Action Plan*; Council of the European Union: Brussels, Belgium, 2018.
64. European Union, Directive 2016/679/EU on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1599862836456&uri=CELEX:32016R0679 (accessed on 10 May 2021).
65. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. Available online: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed on 23 May 2021).
66. European Union, Directive 2019/881/EU on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Available online: https://eur-lex.europa.eu/eli/reg/2019/881/oj (accessed on 14 April 2021).
67. Joint Communication to The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Join/2013/01 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553779410177&uri=CELEX:52013JC0001 (accessed on 25 April 2021).
68. ENISA Report. Cyber Risk Management for Ports: Guidelines for Cybersecurity in the Maritime Sector. 2020. Available online: https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports (accessed on 27 May 2021).
69. ENISA Report. Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector. 2019. Available online: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector/at_download/fullReport (accessed on 28 May 2021).
70. Maritime and Port Authority of Singapore. *Shipping Circular No. 15 of 2020: Maritime Cyber Risk Management*; Maritime and Port Authority of Singapore: Singapore, 2020.
71. Alifragki, M.E. Cyber-Attacks: The new type of piracy in the Maritime World. Master's Thesis, Department of Maritime Studies, University of Piraeus, Pireas, Greece, 2019. Available online: https://dione.lib.unipi.gr/xmlui/handle/unipi/12503 (accessed on 15 May 2021).
72. The North of England P&I Association. Cyber Risks & P&I Cover. Available online: https://www.nepia.com/cyber-risks-pi-cover/ (accessed on 2 May 2021).
73. Circular 2021/06: Class War Risks—Renewals 2021/2022, The North of England P&I Association. 16 February 2021. Available online: https://www.nepia.com/circulars/class-war-risks-renewals-2021-2022/ (accessed on 11 May 2021).
74. Circular 2020/02: Cyber Security: Kick Start—New Member Benefit for Cyber Security Compliance, The North of England P&I Association. 10 January 2020. Available online: https://www.nepia.com/circulars/cyber-security-kick-start-new-member-benefit-for-cyber-security-compliance/ (accessed on 25 May 2021).
75. *Loss Prevention Briefing: Cyber Risks in Shipping*; North of England P&I Association: Newcastle upon Tyne, UK, 2016.
76. American Petroleum Institute (API), Standard (STD) 780. *Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries*; American Petroleum Institute: Washington, DC, USA, 2013.
77. Center for Chemical Process Safety (CCPS), The Energy Institute. *Bow Ties in Risk Management: A Concept Book for Process Safety*; John Wiley & Sons Inc.: Hoboken, NJ, USA, 2018.
78. American Bureau of Shipping (ABS). American Bureau of Shipping (ABS) Technical Report. In *Bowtie Applications for the Marine and Offshore Industries*; American Bureau of Shipping (ABS): Houston, TX, USA, 2013.

79. DRAGOS Inc and OSIsoft Inc White Paper: Using Bow Tie Risk Modeling for Industrial Cybersecurity. DRAGOS Inc., 2021. Available online: https://www.dragos.com/resource/using-bow-tie-risk-modeling-for-industrial-cybersecurity/ (accessed on 15 November 2021).
80. aeBlogs: The Benefits of Visualizing CyberPHAs Using Bowtie Diagrams. aeSolutions Inc. Available online: https://www.aesolutions.com/post/The-benefits-of-visualizing-cyberphas-using-bowtie-diagrams (accessed on 10 September 2021).
81. SANS Institute Information Security Reading Room White Paper: Evaluating Cyber Risk in Engineering Environments: A Proposed Framework and Methodology. Rebekah Mohr, 2016. Available online: https://www.sans.org/white-papers/37017/ (accessed on 10 September 2021).
82. Ji, Z.; Shuang-Hua, Y.; Yi-jia, C.; Yuchen, W.; Chenchen, Z.; Liang, Y.; Yinqiao, Z. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. *Process. Saf. Environ. Prot.* **2021**, *148*, 1279–1291. [CrossRef]
83. Meland, P.H.; Bernsmed, K.; Frøystad, C.; Li, J.; Sindre, G. An experimental evaluation of bow-tie analysis for security. *Inf. Comput. Secur.* **2019**, *26*, 536–561. [CrossRef]
84. Abdo, H.; Kaouk, M.; Flaus, J.; Masse, F. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie—combining new version of attack tree with bowtie analysis. *Comput. Secur.* **2018**, *72*, 175–195. [CrossRef]
85. Bernsmed, K.; Frøystad, C.; Meland, P.H.; Nesheim, D.A.; Rødseth, Ø.J. Visualizing Cyber Security Risks with Bow-Tie Diagrams. In *Graphical Models for Security, GraMSec 2017*; Lecture Notes in Computer, Science, Liu, P., Mauw, S., Stolen, K., Eds.; Springer: Cham, Switzerland, 2018; Volume 10744. [CrossRef]
86. International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 31010. *Risk Management—Risk Assessment Techniques*; International Organization for Standardization: Geneva, Switzerland, 2019.
87. Available online: https://www.nccoe.nist.gov/projects/use-cases/maritime-ong (accessed on 15 May 2021).
88. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed on 15 May 2021).
89. The MITRE Corporation. "MITRE ATT&CK®", The MITRE Corporation. 2016. Available online: https://attack.mitre.org/ (accessed on 4 June 2021).
90. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors* **2021**, *21*, 3267. [CrossRef] [PubMed]
91. MITRE Report MP180360R1. MITRE ATT&CK®: Design and Philosophy. 2020. Available online: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf (accessed on 4 June 2021).
92. US DHS CISA Cybersecurity and Physical Security Convergence Guide. Available online: https://www.cisa.gov/publication/cybersecurity-and-physical-security-convergence (accessed on 4 June 2021).