Journal of
Marine Science and Engineering

Article

Cyber–Physical Security Assessment for Maritime Vessels: Study on Drillship DP System Using American Petroleum Institute Security Risk Analysis and Bow-Tie Analysis

Iosif Progoulakis [1,*], Ioannis K. Dagkinis [1], Anastasia Dimakopoulou [2], Theodoros Lilas [1], Nikitas Nikitakos [1] and Panagiotis M. Psomas [3]

[1] Department of Shipping Trade and Transport, University of the Aegean, Korai 2a, 82132 Chios, Greece; idag@aegean.gr (I.K.D.); lilas@aegean.gr (T.L.); nnik@aegean.gr (N.N.)
[2] Department of Computer Science, Democritus University of Thrace, 65404 Kavala, Greece; axdimak@cs.duth.gr
[3] Department of Financial and Management Engineering, University of the Aegean, Kountouriotou 41, 82132 Chios, Greece; ppsomas@aegean.gr
* Correspondence: i.progoulakis@aegean.gr

Abstract: The maritime industry's increasing integration of IT/OT systems into vessel operations has significantly elevated its exposure to cyber–physical threats, making the development of effective cyber risk management strategies a necessity. This paper provides an outlook of the current landscape of cyber security threats and vulnerabilities for the maritime sector and vessels. An outline of the relevant governmental and industry directives, standards, and guidelines for cyber security in maritime vessels is given. Considering maritime vessels as critical elements of the maritime critical infrastructure sector, a number of relevant cyber–physical security assessment methods are presented. Bridging cyber–physical security, process safety, and security, API SRA (American Petroleum Institute Security Risk Analysis) and BTA (Bow-Tie Analysis) are presented as the most applicable cyber–physical security assessment methods for complex maritime vessels, such as an offshore oil and gas drillship. The scenario of a cyber-attack on the Dynamic Positioning (DP) system of a drillship is presented with the use of API SRA and BTA. The difficulties in the implementation of NIST CSF v2.0 and IACS UR E26 and UR E27 in the maritime sector are also discussed. The need for intensified research on and the formulation of bespoke cyber security measures to mitigate the evolving cyber threats within the maritime domain is highlighted. The need for the allocation of training and resources for the reinforcement of the capacity of a maritime vessel's crew in the mitigation of cyber threats and safe maritime operations is emphasized.

Keywords: maritime cyber security; cyber–physical security; maritime transportation sector; critical infrastructure; cyber–physical security assessment; API STD 780; security risk assessment (SRA); bow-tie analysis (BTA); operational technology (OT); drillship; dynamic positioning (DP) system; cyber-attack; malware; industrial control systems (ICSs); NIST CSF v2.0; IACS UR E26; IACS UR E27

Citation: Progoulakis, I.; Dagkinis, I.K.; Dimakopoulou, A.; Lilas, T.; Nikitakos, N.; Psomas, P.M. Cyber–Physical Security Assessment for Maritime Vessels: Study on Drillship DP System Using American Petroleum Institute Security Risk Analysis and Bow-Tie Analysis. *J. Mar. Sci. Eng.* **2024**, *12*, 1757. https://doi.org/10.3390/jmse12101757

Academic Editor: Mohamed Benbouzid

Received: 18 August 2024
Revised: 13 September 2024
Accepted: 27 September 2024
Published: 4 October 2024

1. Introduction

In the contemporary maritime industry, the integration of digital systems that control automatons of vessel operations has significantly increased the susceptibility of ships to cyber threats. The International Maritime Organization (IMO) Resolution MSC.428(98) underscores the importance for heightened cyber risk awareness and the incorporation of cyber risk management into Safety Management Systems (SMSs), as stipulated by the International Safety Management (ISM) Code. This resolution is important for all maritime stakeholders, as it reiterates the necessity for reinforcements of the maritime transportation sector as a vital part of the general critical infrastructure against the wide spectrum of cyber threats and vulnerabilities.

Cyber-attacks specifically targeting maritime vessels have been documented and analyzed to an extent [1–3]. There have been reports of mass GPS spoofing attacks against over 20 vessels in the Black Sea [4,5]. There have been cases of ECDIS screens displaying false ship locations, whose data were received through forged AIS messages [6]. A vessel's engine system was targeted by remote cyber attackers [7]. A vessel's network was infected by malware affecting all IT systems [8]. Tanker ships were attacked through combined GPS spoofing and remote hacking of systems, while operating near the bunkering port of Fujairah in the United Arab Emirates [9,10]. A covert cyber-attack was carried out against a military vessel targeting its communication systems [11,12]. Other attacks have been simulated and validated in a lab environment [13–16], replicating actual cyber-attack incidents that have or are suspected to have occurred.

While direct cyber-attacks against ships are not as common or as frequent as those made against port facilities or shipping companies it is observed that their documentation is limited and not thoroughly studied. Attacks against ships may not be common or frequent, but they are probable and possible, and when confirmed, the repercussions to the maritime transportation sector or other linked critical infrastructure sectors can be detrimental. As has been highlighted by researchers and industry providers of cyber security services [17,18], a targeted manipulation of a vessel's OT and navigation systems, while transitioning critical maritime transit points, can lead to catastrophic events that include force majeure, blockage, supply disruptions, ship collisions, and environmental disasters. Similarly, in critical infrastructure sectors such as the upstream oil and gas sector, a cyber-attack on a specialized maritime vessel can lead to disruptions of upstream operations and the downstream fuel supply chain; the damage or destruction of oil and gas assets; injuries or fatalities; and, of course, major environmental disasters.

Structure and Methodology

This paper evaluates the cyber–physical security assessment and theory for maritime vessels by providing an overview of relevant assessment methodologies. The focus of this paper is the application of cyber–physical security assessment methods for maritime vessels as elements of the maritime and energy critical infrastructure sectors. A case study of an attack at an offshore oil and gas drillship is presented to show the applicability and effectiveness of security assessment methods of the oil and gas and process safety sectors for cyber–physical systems. The reason an offshore oil and gas drillship was selected for analysis in this paper is because it is considered a specialized vessel with an extensive OT infrastructure and a target of low probability for an attack but high-impact consequences.

This paper is structured as follows. The current landscape of cyber security threats and vulnerabilities for the maritime sector is discussed in Section 2. Section 2 also provides an outlook of relevant governmental and industry directives, standards, and guidelines for cyber security in maritime vessels. Section 3 presents thorough literature review of a number of cyber–physical security assessment methods that relate to the maritime critical infrastructure sector and maritime vessels. API SRA (American Petroleum Institute Security Risk Analysis) and BTA (Bow-Tie Analysis) are presented as the most applicable cyber–physical security assessment methods for complex maritime vessels, such as an offshore drillship, where cyber security and process safety are required. The reason for selecting these methods is described in more detail in Section 3. Section 4 presents the application of the API SRA and BTA cyber–physical security assessment methods for a scenario involving a cyber security breach of the Dynamic Positioning system of an offshore drillship. Important conclusions and discussion points in the application of cyber–physical security assessment methods in maritime vessels and, specifically, an offshore drillship, are presented in Sections 5 and 6.

2. Cyber Security in the Maritime Domain

2.1. Landscape and Regulatory Framework of Maritime Cyber-Security Threats

The maritime industry is increasingly interconnected and reliant on digital systems and industrial control systems (ICSs) [19], making it a prime target for cyber threats. The European Union Agency for Cybersecurity (ENISA) [20,21] reported a significant shift in the cyber risk profile of the maritime sector, with a rise in cyber security incidents at ports and on vessels. The United States Coast Guard (USCG) [22] and ENISA [20] reported an increase in a variety of cyber threats, including advanced persistent threats; phishing attacks; and ransomware cases affecting the maritime transportation sector, maritime shipping companies, and the assets involved, with significant consequences for global trade and security.

Politically and financially motivated attacks against IT and OT systems in maritime vessels and shipping companies also expose the involvement of state actors as the originators of attacks [21], creating a more complex threat environment, where covert military operations are convoluted with cyber-criminal operations, creating a composite and continually evolving threat landscape, with attackers becoming more sophisticated. All stakeholders involved in the maritime sector should, therefore, remain vigilant and implement robust cyber security measures to mitigate these risks, considering their assets, operational and technical characteristics, and requirements, while acknowledging the overlap of the maritime transportation sector with other critical infrastructure sectors.

BIMCO [23] also categorized the types of cyber threats faced by the maritime sector in untargeted and targeted categories, as also depicted in Table 1.

Table 1. Types of cyber threats faced by the maritime industry.

Type of Attack	**Threat**	**Description**
Untargeted Attacks	Malware	Includes trojans, ransomware, spyware, viruses, and worms that exploit unpatched software vulnerabilities. Ransomware encrypts data until a ransom is paid.
	Water Holing	Creating or compromising websites to exploit visitors, affecting crew members accessing the internet at sea.
	Scanning	Conducting random searches across the internet for exploitable vulnerabilities in a vessel's systems.
	Typosquatting	Exploiting typographical errors made by crew members when entering website addresses, leading them to malicious sites.
Targeted Attacks	Social Engineering	Manipulation of crew members into breaking security protocols, often through social media or other communication channels.
	Brute Force Attacks	Attempting to guess passwords to gain unauthorized access to vessel systems.
	Credential Stuffing	Using previously compromised credentials to access systems aboard the vessel.
	DoS and DDoS	Overwhelming the vessel's network with data to prevent legitimate access, potentially disrupting navigation and communication systems.
	Phishing and Spear Phishing	Sending emails to crew members with the intent of stealing sensitive information or delivering malware, including malicious attachments or links to fake websites.
	Supply Chain Attacks	Compromising equipment, software, or services delivered to the vessel, which could be used as a vector for a cyber-attack.

From known cyber security incidents in the maritime as well as other critical infrastructure sectors, such as the industrial and oil and gas domains, the following types of cyber adversaries are noted:

(a) Cybercriminals: these are hackers, organized criminals, etc., seeking financial gain through the use of stolen digital data or the manipulation of physical assets.
(b) State adversaries: these are hostile states seeking political advantage, espionage, the destruction of digital assets (physical assets, systems, or infrastructure), sabotage, etc.
(c) Insiders: these are dissatisfied employees seeking personal gain through the targeted theft of digital information, the destruction of digital assets, sabotage, etc., or careless employees causing unwanted incidents [23,24].
(d) Cyber terrorists [23,24]: these are terrorist groups seeking the sabotage or destruction of physical assets, and they exploit cyber and physical vulnerabilities for political or ideological reasons.
(e) Cyber activists: these comprise hacktivists and activist groups causing sabotage to cyber infrastructure through targeted cyber-attacks for political or ideological purposes.

The increasing number of cyber aggressors and the evolving threats and attack tactics call for the maritime industry to adapt to these changes by enhancing cyber security protocols and situational awareness about the latest cyber threats and vulnerabilities. This also entails the enforcement of existing cyber security directives and the creation of new ways to tackle the emerging threat landscape. The current initiatives for maritime cyber security in the form of standards, regulations, guidelines, and directives from industry and governmental organizations have been extensively reviewed in various academic publications [25–29], but this paper identifies the most prominent ones, specifically, those related to maritime cyber security, as shown in Table 2. These were derived from a review process using the available web-based IHS Markit database and governmental webpages. Main key words used for this review were “maritime cyber security” and “maritime cyber physical security”.

Table 2. Summary of governmental and industry initiatives related to maritime cyber security. Information elaborated on by the authors.

Category	Originator	Title
Standards	NIST	NIST Special Publications 800-30, 800-37, 800-82, NIST Cybersecurity Framework (CSF) 2.0.
	ASTM	ASTM F3286-17, ASTM F3449-20
	ISO/IEC	ISO/IEC 27001 [30], IEC-62443-4-2 [31], IEC 62443-3-3 [32], ISO/IEC 21827 [33], ISO/IEC 15408-1 [34], ISO/IEC 18045 [35], and ISO/IEC 27032 [36]
Industry Organizations	IMO	IMO Resolution MSC.428(98), IMO Guidance MSC-FAL.1/ Circ.3
	BIMCO	The Guidelines on Cyber Security Onboard Ships
	IACS	UR E26—Cyber resilience of vessels; UR E26—Cyber resilience of onboard systems and equipment
Government	IET, DSTL, and UK Department of Transport	Code of Practice Cyber Security for Ships
	USCG	NVIC 01-20; Vessel Cyber Risk Management Work Instruction CVC-WI-027 (2021)
	US Congress	Bill S. 4023 “Enhancing Maritime Cybersecurity Act of 2020”
	European Union	2008/114/EC, 2013/30/EU, 2016/1148/EU, 2019/881/EU, EU Cybersecurity strategy JOIN/2013/01, ENISA report 2016
	Danish Maritime Cybersecurity Unit	Cyber and Information Security Strategy for the Maritime Sector
	MPA Singapore	Shipping Circular No. 15 (2020)

Table 2. *Cont.*

Category	Originator	Title
Maritime Classification Societies	ABS	ABS "Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations—ABS CyberSafety Vol. 1", September 2016; ABS "Guide for Cybersecurity Implementation for the Marine and Offshore Industries—ABS CyberSafety Vol. 2", June 2018 (revised); ABS "Guidance Notes on Data Integrity for Marine and Offshore Operations—ABS CyberSafety Vo. 3", September 2016; ABS "Guide for Software Systems Verification—ABS CyberSafety Vol. 4", September 2016; ABS "Guidance Notes on Software Provider Conformity Program—ABS CyberSafety Vol. 5", September 2016.
	DNV GL	DNVGL-RP-G108 (2017), DNVGL-RP-G 496 (2016), DNVGL-CP-0231 (2018)
	Lloyd's Register (LR)	Lloyd's Register Guidance Note: Cyber-enabled ships—Deploying information and communications technology in shipping—Lloyd's Register's approach to assurance, 2016; Lloyd's Register Guidance Note: Cyber-enabled ships—ShipRight procedure—autonomous ships, 2016; Lloyd's Register Guidance Note: Cyber-enabled ships—Type Approval of Cyber Enabled Systems Components, 2016.
	Class NK	Class NK, "Guidelines for Designing Cyber Security Onboard Ships", 2nd Ed., July 2020; Class NK, "Cyber Security Management Systems for Ships", 1st Ed., April 2019.
	Russian Maritime Register of Shipping	Guidelines on Cyber Safety
	Croatian Register of Shipping (CRS)	ISM Code Statutory Newsletter Number 03.08.2020
	Indian Register of Shipping (IRCLASS)	Maritime Cyber Safety Guidelines (IRS-G-SAF-02—2018); Guidelines on Certification of Software for Computer Based Control Systems (IRS-G-DES-01—2019)
	International Registries and Maritime Administrator of The Republic of the Marshall Islands	Marine Guideline No. 2-11-16 (2018); Ship Security Advisory No. 13-20 (2020)
	Bureau Veritas	Rule Note NR 642 (2018), Rule Note NR 659 (2020)

From the above, it is worth evaluating the most recent developments in directives, as introduced to the industry. Specifically, the National Institute of Standards and Technology Cyber Security Framework version 2.0 (NIST CSF v2.0) [37], released in 2024, has expanded its scope to address cyber security risk management across various sectors, including the maritime industry. With the addition of the 'Govern' function to the existing suite of Identify, Protect, Detect, Respond, and Recover, this framework emphasizes the critical role of integrating cyber security into organizational governance.

In addition, the International Association of Classification Societies (IACS) introduced the Unified Requirements UR E26 [38] and E27 [39] to enhance the cyber security of ships. IACS prioritizes the reliability of critical onboard computer systems. UR E26 ensures the secure integration of OT and IT systems throughout a ship's lifecycle, from design to operation, treating the vessel as a unified cyber system.

2.2. Cyber Vulnerabilities of Maritime Vessels

With respect to the cyber vulnerabilities of maritime vessels, these relate to security gaps and potential weaknesses in a vessel's digital systems that can be exploited by cyber attackers [40–43]. These vulnerabilities can affect various functions that take place on board and are controlled or executed by commands from integrated IT systems. Especially in autonomous modern vessels, cyber vulnerabilities lead to potential risks to operational efficiency, safety, and security [44,45]. The main areas where risks from cyber-attacks can potentially occur are the following [46,47], as also shown in Figure 1:

- Navigation systems are at risk, as GPS signals can potentially be manipulated with spoofing, so that with misleading signals, the information can be altered, causing a possible diversion of the ship's course; access to the systems can be gained; or malware can be spread. Or, by tampering with AISs (Automatic Identification Systems), the data can be manipulated by giving false information about the position, speed, or identity of a vessel.
- Communication systems, which include satellite communication systems and the VHF radio, are at risk. Cyber-attacks on SATCOM systems are carried out by exploiting weak points in order to intercept or manipulate communications, while jamming VHF communications is aimed at disrupting coordination and security communications.
- Operational Technology (OT) systems that support the operations of a ship's equipment, such as its propulsion engines, electric motors, steam boilers, rudders, and other auxiliary machinery in the engine room, are at risk. Also, cargo management OT systems where sensors and digitally processed information are used to maintain the cargo in the desired condition during transport, as happens in ships carrying liquefied natural gas, in tankers carrying heated oil cargoes, in container ships managing the arrangement of containers, etc., are at risk. Much of their operation is based on the digital engine control technologies found on modern ships. These collect information from the engine load, performance, and temperature data from operations, which are then processed by advanced software to give commands to keep the engine running, supply fuel, etc. Gaining unauthorized access to the ship's engine control systems can cause a possible loss of propulsion, endangering the safety of the ship. Gaining unwanted access from a cyber-attack to steering systems can cause unwanted changes in the direction of a ship, which is particularly dangerous when a ship passes through channels and river areas with heavy ship traffic and when approaching ports, etc. Accordingly, interference with systems that manage cargo operations could lead to improper stowage or the mishandling of hazardous materials.
- Information technology (IT) systems, including network security and remote access control, are also at risk. Hacking embedded networks has the risk of accessing sensitive data or installing malware. Accordingly, interfering with remote access by exploiting the weakness of protocols results in gaining control of a ship's systems.
- With respect to human factors, targeting crew members with phishing emails can gain access to ship systems. Also, through social engineering, crew members can be manipulated into revealing confidential information or granting unauthorized access.

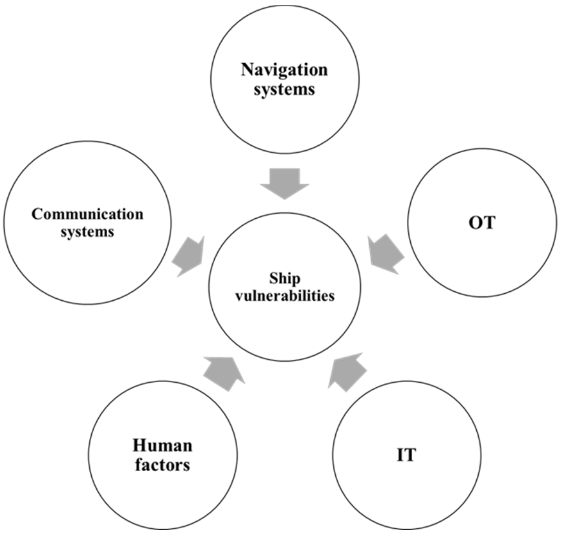

Figure 1. Cyber vulnerabilities of maritime vessels.

3. Cyber–Physical Security Assessment in the Maritime Domain

3.1. Cyber–Physical Security Assessment Methods

Cyber–physical systems can generally be defined as those that combine IT (Information Technology) and OT (Operational Technology) and human operations [25]. A security assessment can be generally defined as the evaluation process of an asset's characteristics through the security parameters of threat, risk, and vulnerabilities. A cyber–physical security assessment is essentially an assessment of the cyber security risks of Operational Technology (OT) systems and components along with related IT systems which connect to process safety and security. Cyber–physical security is particularly relevant to industrial and critical infrastructure assets due to their complex and multi-disciplinary technical and operational parameters.

Considering ships as integral components of the maritime transportation sector, we see them as being part of the critical infrastructure sector as well. Maritime vessels need to be seen as maritime industrial assets which play a key role in the maritime transportation sector. As maritime industrial assets, they comprise industrial control systems (ICSs) and, in general, OT and IT systems, equipment, and components, which enable maritime operations at a technical level. In order to assess security threats in the maritime cyber domain, it is necessary to seek methodologies that are relevant to both the maritime dimension of ships as well as their characteristics of industrial and critical infrastructure elements.

Based on a literature review, a number of relevant qualitative and quantitative cyber–physical security assessment methods for critical infrastructure (and the maritime transportation sector and its elements) are presented in Table 3. For the literature review, the databases of Science Direct; Google Scholar; Wiley Online Library; IEEE Xplore Digital Library; ProQuest; www.researchgate.net; www.academia.edu; and the most common world wide web search engines (Google, Yahoo, and MSN) were used to source information. Various combinations of search key words were used, which were selected in order to maximize the gathered data that were filtered for relativity and use. The most notable key word combinations used included the following: "maritime security", "oil and gas + maritime + cyber security", "offshore maritime security", "CIP and cyber security + oil and gas", "CIP + maritime + oil and gas", and "offshore oil and gas security". From the identified search results, the most relevant were identified through a review of their content and were utilized in the write-up of this paper, as presented and referenced in Table 3.

Table 3. List of cyber–physical security assessment methods.

Method Description	Author/Source
Commercial supply chain risk management as part of CIP	Häyhtiö, M., & Zaerens, K. (2017) [48]
Fuzzy RAMCAP	Alidoosti, A., et al. (2012) [49]
All-hazards catastrophe analysis framework, based on network science and normal accident theory	Lewis, T.G., et al. (2011) [50]
All-hazards assessment for cross-functional cyber and physical components, systems, and operations	Pollet J., et al. (2009) [51]
Threat, vulnerability, and consequence analysis using operations research, prospect theory, network science, and normal accident theory	Taquechel, E.F. & Lewis, T.G. (2017) [52]
Attack-modelling method for the assessment of vulnerabilities and risk exposure of information, communication, and industrial control systems	Ivanc, B., & Klobucar, T. (2014) [53]
Generic risk-based Criticality Analysis methodology for CIP	Theoharidou, M., et al. (2009) [54]
Limited Memory Influence Diagram (LIMID) using Bayesian Networks	Misuri, A., et al. (2019) [55]
Process control system (PCS) security for SCADA systems in CIP	Ryu, D.H., et al. (2009) [56]
Bilevel and trilevel optimization model analysis for CIP using attacker–defender models	Brown, G., et al. (2006) [57]
Defender–Attacker–Defender (DAD) sequential model analysis for CIP	Alderson, D.L., et al. (2011) [58]
Vulnerability assessment methodology for CIP using risk matrix analysis and systems taxonomy	Baker, G.H. (2005) [59]
Vulnerability analysis method for interdependent infrastructure systems in CIP	Ouyang, M. (2016) [60]
Criticality assessment method for critical energy infrastructure	Augutis, J., et al. (2016) [61]
Deterrence quantification method for CIP using game theory and probabilistic utility functions	Taquechel, E.F., et al. (2012) [62]
Security analysis using the Collaborative Security Management (CYSM) System method for Critical Information Infrastructure (CII) and maritime CIP	Karantjias, A., et al. (2014) [63]
Model-Based Risk Analysis (MBRA) for CIP and modelling terrorist transfer threat networks	Lewis, T.G., et al. (2012) [64] and Taquechel, E. (2010) [65]
Model-Based Vulnerability Assessment (MBVA) for the protection of interdependent critical infrastructure	Valencia, V.V., et al. (2012) [66]
Model-Based Risk Analysis (MBRA) for CIP of digital instrumentation and control subsystems	Gran, B.A., et al. (2007) [67]
Attack-strength-degradation model	Wu, B., et al., (2016) [68]
Cyber Risk Assessment for Ships (CRASH): a qualitative risk analysis method using severity, probability, and criticality ratings	Oruc, a, et al. (2024) [69]
CYber-Risk Assessment for Marine Systems (CYRA-MS): a modified Cyber Preliminary Hazard Analysis (CPHA) to IEC 62433 parameters.	Bolbot, V. et al. (2020) [46]
CRAMMTS (Cyber Risk Analysis Method for Maritime Transportation Systems): a survey-based quantitative risk analysis method that modifies the ISRAM (Information Security Risk Analysis Method) risk analysis method, considering IMP criteria and industry stakeholder feedback	Tatar, U. et al. (2024) [70]
Qualitative risk analysis method using a risk matrix customized to ship OT systems' parameters	Rajaram, P. et al. (2022) [71]
Maritime Vessel-Hierarchical Attack Representation Model (MV-HARM): a graphical security model for maritime vessels, considering probabilistic events, vulnerabilities, and network configurations of vessel components	Enoch S.Y. et al. (2021) [72]
Qualitative vulnerability assessment method for port and ship ecosystem components, implementing a System-of-Systems cyber risk analysis approach	Kapalidis, C. et al. (2022) [73]

Table 3. *Cont.*

Method Description	Author/Source
Security Vulnerability Assessment, Prevention, and Prediction (SVAPP): A safety barrier assessment methodology adapted for industrial assets for physical and cyber-attack scenarios	van Staalduinen, M. et al. (2016) [74]
Cyber PHA (Process Hazard Analysis): a safety-oriented cyber security risk assessment methodology for industrial control systems (ICSs) and safety instrumented systems (SISs), based upon ISA 62443-3-2, ISA TR84.00.09, ISO/IEC 27005:2018, ISO 31000:2009, and the NIST Special Publication (SP) 800-39.	Marszal, E.M., et al. (2019) [75] and Ginter, A. (2023) [76]
Rings Of Protection Analysis (ROPA): a adapted version of the Layer of Protection Analysis (LOPA) method for the cyber security of process control systems	Baybutt, P. (2004) [77]

In general, it was observed that while a number of cyber security risk analysis tools and methods exist and have been compared [78–80], these primarily relate to ICS or IT systems only, without taking into account the special operational and technical characteristics of ships or their mission-specific operational requirements or parameters. Similarly, by acknowledging the cyber–physical dimension of maritime vessels as critical infrastructure elements, a review of the methods presented in Table 2 indicated that very few methods tackle both the ICS technical and maritime operational functions of ships. The special operational and technical characteristics of ships and, specifically, drillships, include the following:

Maritime operations: these include operating at different sea state conditions, operating in remote locations away from shore technical support, mooring operations, DP operations, ship-to-ship fuel operations, OSV (offshore support vessel) to drillship operations.

Upstream oil and gas operations: these include drilling operations; well servicing, work overs, completion, and abandonment; oil, gas, mud, and water handling and storage; and artificial lift operations.

For maritime operations, a maritime vessel's propulsion, navigation, and other systems are used, which also involve the operation of necessary industrial control systems and IT/OT systems. For upstream oil and gas operations, the necessary control systems for the operation of specialized equipment are used, such as the following: pumps, motorized valves, cranes, heating systems, mixing devices/agitators, degasifiers, manifolds, reservoirs, rig electric drive controls, blowout preventers, turbine bottom-hole engines, etc. From a review of the publications presented in Table 3, it was determined that these works either deal entirely with shore-based or ship-related industrial control systems. None of these appear to tackle process safety and security as well as distinct upstream oil and gas operations.

3.2. Cyber–Physical Security Assessment Methods for Maritime and Oil and Gas Process Safety and Security Applications

If we consider the mission-specific requirements of specialized maritime vessels, such as those in the upstream offshore oil and gas sector, it is evident that a few of the methods presented in Table 3 could be deployed in the field. With respect to this paper specifically, considering the specific type of vessel chosen for analysis, an offshore drillship, it is necessary to apply methods that are specifically relevant to the oil and gas sector and its maritime assets while considering process safety and security.

Such a method is the American Petroleum Institute (API) Security Risk Assessment (SRA) methodology. SRA is an expert-based qualitative method, developed for assessing security risks at petroleum and petrochemical facilities [81]. It is applicable to a wide spectrum of physical and cyber security issues and for a broad variety of both fixed and mobile applications. The Security Risk Assessment (SRA) method described in API (American Petroleum Institute) standard (STD) 780 [81] includes the following five (5) process steps: (1) Asset characterization, (2) Threat assessment, (3) Vulnerability Assessment, (4) Risk evaluation, and (5) Risk treatment. The implementation of API SRA can assist in the compliance with the US Department of Homeland Security's Chemical Facility Anti-Terrorism Standards (CFATS) [82], 6 CFR Part 27, which mandate identifying and reporting cyber security incidents for oil and gas assets, among other directives. As per API standard 780, the SRA [81] is carried out by technical and corporate stakeholders of the asset, which represent security, risk management, operations, engineering, safety, environmental regulatory compliance, logistics, legal, IT and OT security, as well as any other relevant, contractors.

Another method is the Bow-Tie Analysis (BTA), which is a qualitative method utilized in Process Safety Management (PSM) for the oil and gas as well as chemical and processing industries [83]. The BTA is used for a review of safety- and security-related incidents, either proactively, during safety/security review processes, or reactively, after an incident has occurred. The Bow-Tie Analysis is used for the definition of risks, hazards, and consequences of safety and security incidents in systems, equipment, processes, and operations. The Bow-Tie Analysis is applicable in the maritime sector, as it can examine the interconnection of marine equipment, systems, and processes in vessels and other maritime assets in the case of safety and security incidents. Specifically in cyber–physical security, the Bow-Tie Analysis can identify the applicable security barriers and mitigation measures for IT/OT assets and processes at the micro (components, equipment, sub-assemblies, and instruments) and macro (assemblies, assets, equipment, and operations) scales.

The applicability of SRA and BTA in cyber–physical security assessments for maritime and oil and gas assets has been proved in various academic publications [25,26,84–90]. Furthermore, from an industry-wide survey related to cyber security in the oil and gas sector [91], API SRA was found to be one of the most prominent cyber security risk assessment and management methods [91]. The BTA is also considered to be one of most widely used process safety and security analysis methods in the oil and gas industry [83,92]. For these reasons, these methods were chosen to be applied in an analysis of a cyber security breach in this paper.

4. Cyber–Physical Security Assessment for an Offshore Drillship

4.1. Cyber–Physical Security Scenario

The cyber–physical security scenario to be examined in this paper involves a cyber breach incident in the Dynamic Positioning of an offshore drillship. This scenario was selected after an examination of other possible targets on maritime vessels and considering publications on the possibility of such cyber security breach incidents [93–99].

This drillship is a self-propelled floating offshore drilling unit that has a ship hull, which is capable of drilling exploratory wells in deep remote waters [100]. This drillship combines industrial equipment and processes supported by sophisticated and complex IT and OT systems for upstream (oil and gas exploratory) and maritime operations.

The Dynamic Positioning (DP) system enables a floating vessel to maintain its position over a location by varying the power of its propulsion units mounted along the vessel's hull, without deploying a conventional mooring or anchoring system. A propulsion system power is directed by a system of telemetry signals from a series of sensors, including beacons on the sea floor; satellite information (GPS, GNSS, and GLONASS); wind sensors; a gyro compass; motion reference units; vertical reference units; hydro acoustic sensors; or the angular movement of a taut wire [100]. DP systems can be found on a variety of specialized vessels, such as offshore support vessels (OSVs), cable-laying ships, drillships, shuttle tankers, etc. Based on the type and complexity of the maritime vessel and operations, DP systems are separated into different categories (DPS 0, DPS 1, DPS2, and DPS3), as per IMO Guidelines, IMO MSC.1/Circ. 1580 [101] and IMO MSC/Circ. 645 [102], which allow for different levels of station-keeping capabilities, reliability, and redundancy capacities and the use of a variety of sensors, systems, and DP control stations [103].

The selected cyber–physical security assessment methodology is the API standard 780 Security Risk Assessment (SRA) methodology, as it was found to be widely recognized and used in the oil and gas and maritime industry [25,26,91], and it provides a detailed analysis of maritime vessels, identified cyber vulnerabilities, and proposed cyber security countermeasures, considering the cyber-attack attractiveness of the targeted areas. The Process Safety Management method that was used is the Bow-Tie-Analysis (BTA) method, which can effectively assess the cyber security barriers deployed prior to and after a potential security breach scenario. The BTA also provides a visual presentation and a detailed analysis of all the consequences of threats and cyber security incidents, considering the deployment of specific cyber security countermeasures aiming to prevent incidents of cyber security breaches as well as to decrease residual risks and consequences after such an incident.

The aims and objectives of the presented analysis are the following:

- Identify the asset's systems and locations that are vulnerable to cyber breach incidents.
- Validate target attractiveness and vulnerabilities for the drillship's DP system.
- Apply the API SRA method to assess the asset's cyber vulnerabilities, target attractiveness, and cyber security posture through established security barriers.
- Apply the BTA to visualize and assess the cyber security barriers in the pre-event and post-event stages of the cyber breach incident.
- Validate the integrated use of the SRA and BTA in evaluating the proactive and reactive measures of security analysis and protection.

This analysis takes into account the maritime and industrial features of assets as well as their specific engineering and operational parameters. The technical information that was used for the analysis of a cyber security breach scenario included technical design drawings of the vessel, made available to the authors [104], as well as a DP system and IT network diagram created by the authors for the drillship, indicating the logical connectivity between the vessel server, IT equipment, and DP components. The selected DP system is of a level DPS 2 type and includes three bridge DP workstations and one portable one. The DP system diagram is shown in Figure 2.

4.2. Application of API SRA

For the validation of the API SRA method, the 5-step process described in API STD 780 was followed.

In Step 01 of the SRA process, an asset classification is carried out, aiming for the following:

- Identify the drillship's cyber-related components.
- Determine any interdependencies.
- Identify existing cyber security safeguards (internal and external).
- Determine consequences to human life, the environment, and business continuity.
- Allocate criticality, with grading being based on worst-case consequences.

Through a macroscopic evaluation of the available hazardous areas' classification drawing (see Figure 3), cyber critical areas and assets and their interdependencies within the drillship were identified. The hazardous areas' classification drawing (Figure 3) was derived from an engineering analysis based on IEC 60079-10-1 (Classification of areas—Explosive gas atmospheres). IEC 60079-10-1 identifies areas where flammable gas or vapor hazards may arise and can be used as a basis to the design, construction, operation, and maintenance of equipment for use in hazardous areas. The hazardous areas' classification drawing was used in the cyber–physical security analysis of the drillship in order to identify locations and systems for potential cyber breaches, which could lead to process safety incidents and cascaded effects. These cyber critical areas and assets are listed in Table 4 and cover three categories: (a) industrial (oil and gas) process areas and systems, (b) maritime process systems, and (c) IT systems. The cyber critical areas and assets were then rated based on the consequence parameters of casualties, the environment, replacements, businesses, and reputation, and an asset severity-ranking grade was allocated. Based on this severity ranking, the critical locations and cyber systems were prioritized.

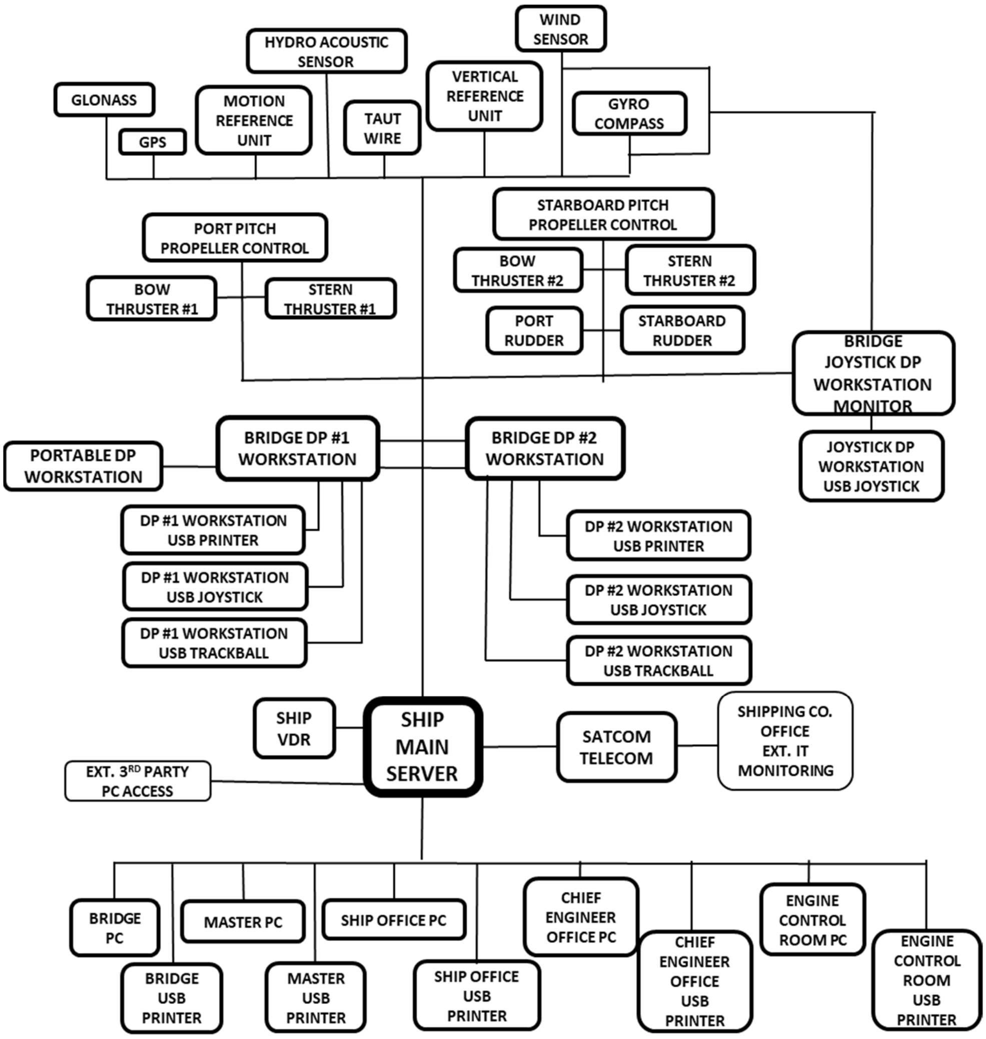

Figure 2. Diagram showing logical connections of the DP system and IT network of the drillship for the selected cyber breach scenario.

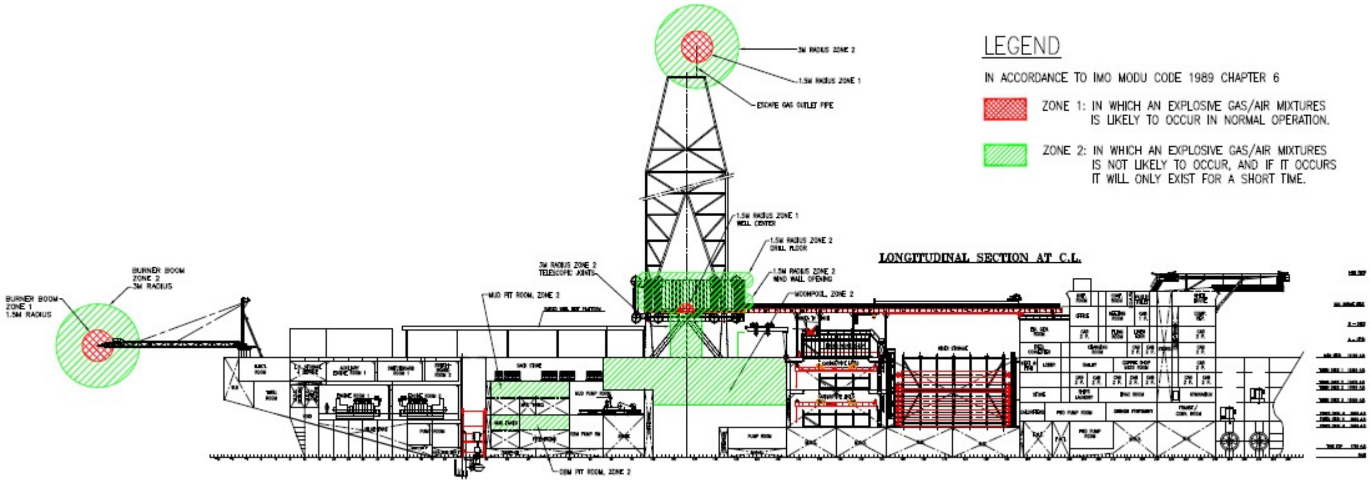
LEGEND
IN ACCORDANCE TO IMO MODU CODE 1989 CHAPTER 6
ZONE 1: IN WHICH AN EXPLOSIVE GAS/AIR MIXTURES IS LIKELY TO OCCUR IN NORMAL OPERATION.
ZONE 2: IN WHICH AN EXPLOSIVE GAS/AIR MIXTURES IS NOT LIKELY TO OCCUR, AND IF IT OCCURS IT WILL ONLY EXIST FOR A SHORT TIME.
LONGITUDINAL SECTION AT C.L.
3M RADIUS ZONE 2
1.5M RADIUS ZONE 1
ESCAPE GAS OUTLET PIPE
1.5M RADIUS ZONE 1 WELL CENTER
1.5M RADIUS ZONE 2 DRILL FLOOR
1.5M RADIUS ZONE 2 WIND WALL OPENING
MOONPOOL, ZONE 2
3M RADIUS ZONE 2 TELESCOPIC JOINTS
MUD PIT ROOM, ZONE 2
BURNER BOOM ZONE 2 3M RADIUS
BURNER BOOM ZONE 1 1.5M RADIUS
OBM PIT ROOM, ZONE 2

Figure 3. Hazardous areas' classification drawing of drillship [104].

Table 4. Identified cyber critical areas and assets within the drillship.

Identified Critical Areas of Asset		
Industrial (Oil and Gas) Process Areas and Systems	**Maritime Process Systems**	**IT Systems**
Engine rooms #1 and #2 (propulsion engines)	Bridge navigation systems	Drillship main server
Aux. engine room #1 (auxiliary propulsion engine)	AIS	Bridge DP workstation #1 + USB ports
Switch board rooms #1 and #2 (RTUs, PLCs, PIDs, etc.)	ECDIS	Bridge DP workstation #2 + USB ports
Well center area (well drilling control systems)	GPS/GLONASS	Shipping company office ext. IT monitoring
Drilling control room (drilling workstation and controls)	Engine control room	Bridge PC
Mud pump room (pump controls)	Bow thrusters	Master PC
Wheel house (ship controls)	Stern thrusters	Ship office PC
Emergency Gen room (backup generators and their controls)	Port pitch propeller control	Chief engineer PC
Frequency converter (converter and controls)	Starboard pitch propeller control	Engine control room PC
Transformer/converter room (transformer/converter and controls)	Port rudder	Bridge PC USB printer
FWD pump rooms #1 and #2 (pump controls)	Starboard rudder	Master PC USB printer
Pump room (pump controls)	VDR	Ship office PC USB printer
HVAC room (HVAC central controls)	SATCOM/TELECOM	Chief engineer PC USB printer
Backup control room (OT controls)	DP system	Engine control room PC USB printer
Emergency drilling room (drilling system controls)		Ext. 3rd-party PC
Electrical office (workstations and control equipment)		Personnel quarters (personal PC stations)
Backup HVAC room (central HVAC controls)		
Electrical equipment room (workstations and calibration equipment)		
Internal VHF radio (telecom systems)		
Transformer rooms (transformer and controls)		
Converter rooms (converters and controls)		
HRU (Hydrostatic Release Unit) rooms' THR-1 (Thruster 1) and THR-2 (Thruster 2) (HRU thruster controls)		
MCC (Motor Control Center) room (control systems)		

Through an assessment of the identified assets, locations, systems, components, etc., and considering the selected cyber security breach scenarios, the Dynamic Positioning (DP) system was validated and selected as a target location for further analysis. It was determined that the interreference or incapacitation of the DP system during a well drilling operation can lead to the loss of station keeping and possibly propulsion and power for the vessel and, subsequently, the disruption or complete halt of well drilling operations.

In Step 02 of the SRA process, the following are achieved:

- Identify and evaluate adversaries.

- Rank threats for each adversary.
- Apply security countermeasures.
- Analyze and assign an asset attractiveness ranking.

In Step 02 of the API STD 780 process, all threats (internal, external, and colluded) are separately assessed to capture all potential cyber threat and scenario rankings. The allocated threat ranking is based on a threat level scale of 1 (very low) to 5 (very high), considering factors such as the general history and nature of the threat, threat experience, the history of the asset, known capabilities and methods of the aggressors, and the potential actions and motivations of the threat actors. A target attractiveness evaluation of assets was conducted for the highest-ranking cyber threats for all assets or components, regardless of their ranking, in order to capture components/assets which can lead to cascaded effects or can influence maritime and upstream operations.

For cybercriminals and state adversaries targeting the drillship, both threats were ranked as high. Per API STD 780, this high ranking indicates that a credible threat exists against the asset, based on the aggressor's capability and intent to carry out an attack. This points to the following:

- Both are credible threats existing against the asset or similar assets.
- The threat demonstrates the capability and intent to launch a targeted cyber-attack.
- The identified asset or similar assets are targeted or attacked on a frequently recurring basis, based on historical information or credible assumptions.
- The frequency of a cyber-attack over the life of the asset or a similar asset is very high.

The case of an internal threat actor causing a cyber breach incident was ranked as a medium threat. Per API STD 780, a medium ranking indicates that there is a possible threat to the asset or similar assets, based on the threat actor's desire to compromise similar assets, but, currently, no specific and verified threat exists for the facility or asset. This scenario, however, is considered highly probable, considering the network interconnectivity of the drillship's systems and the history of similar insider-led security breach incidents in the past.

With regard to the target attractiveness of assets, it was determined that the DP system of the drillship is of potentially high interest to external threat actors (cybercriminals and state adversaries), and it has a higher value of preference in relation to other asset locations, as it would achieve their objective(s) and would provide the highest level of success. This determination considers the vulnerability of the identified locations and systems onboard the drillship (as presented in Table 4) and the detrimental effects of a process safety incident caused by a cyber–physical security incident. This target attractiveness can vary based on the aggressor's motivation, intent, and capabilities.

In Step 03 of the SRA process, the cyber vulnerability of an asset and its systems or locations are assessed, aiming for the following:

- Define the cyber security breach scenario and evaluate its consequences.
- Evaluate the scenario sequence and its consequences.
- Evaluate the effectiveness of existing cyber security barriers.
- Identify cyber vulnerabilities and their grade through a five-level ranking system (from 1 (very low) to 5 (very high)), considering recovery capabilities and the conditional probability of the success of an attack.
- Rank the severity of scenario-specific consequences.

In Step 03 of the SRA process, the residual risk for each cyber threat and scenario per asset is graded using a risk-ranking matrix, as defined by API STD 780. The assessment of vulnerabilities is carried out for all identified assets, components, systems, etc., within a drillship and for each type of cyber threat and scenario per threat. This process takes into account all possible cyber security barriers.

Through an analysis of this step, it was determined that the possible cyber security breach scenarios are the following:

(1) Cybercriminals aim at the disruption of well drill operations and possible ransomware attacks, carrying out targeted cyber-attacks to the drillship network via access to external IT monitoring, or through social engineering, phishing, and other techniques, of the vessel's PC stations, leading to a malfunction of the DP system.
(2) State adversaries, aiming at the disruption of well drill operations, carry out a combination of attacks to the vessel's OT systems (such as the engine room systems, propulsion systems, etc.) through OT-external network connections or remote software/firmware updates or interference with GPS/GLONASS systems; similar to cybercriminals' cyber-attacks to the DP system, this leads to a loss of the vessel's sea-keeping capabilities.
(3) A ship crew member gains access to the drillship network and intentionally or unintentionally plants malware using a portable USB device, causing an infection of the PC stations and, gradually, other network systems, thereby disrupting drilling and maritime operations and causing system failures.

Considering the three different security breach scenarios identified, the following countermeasures are proposed:

- Increase employee and DP operator security vetting and performance monitoring.
- Create a physical separation of the engine, propulsion, and DP control systems.
- Upgrade the IT/OT systems, HMI (Human–Machine Interface) equipment, and DP workstation firmware and software.
- Install firewalls and antivirus software for all systems and subsystems.
- Assign IT and OT experts onboard the vessel to mitigate potential incidents.
- Monitor and control access to communication (USB) ports for all systems.
- Upgrade training for use of the engine room and DP system operators.
- Create emergency protocols for IT/OT failures/malfunctions in propulsion and DP system operations.
- Build in redundancy systems for engine, propulsion, and DP system control and monitoring.
- Enable secure remote monitoring, control, and remediation from the corporate IT/OT support team.
- Establish new or reinforce existing standard operating procedures (SOPs) for preventive checks of equipment.
- Install alternate HMI systems for the propulsion and DP systems.
- Monitor and manage event and alarm notifications.
- Carry out localized propulsion and DP system performance data verifications.
- Network the segmentation and installation of second or multiple servers to segregate critical IT and OT systems.
- Use multiple position reference systems when operating the DP system to minimize risks of a GPS/GLONASS interference.
- Assert common mode failures when using multiple GPS systems.
- Calibrate motion and vertical reference unit systems regularly to monitor and reduce accuracy tolerances.

The above countermeasures are not suggested for prioritized, partial, or complete implementation, as this will depend on corporate decisions and the availability of technical and financial resources. It is understood that if more of these countermeasures are implemented, a better security posture can be achieved.

After the vulnerability assessment of the SRA method, Step 04, involving a risk evaluation, was carried out, aiming to achieve the following:

- An evaluation of the conditional likelihood of cyber breach scenario(s).
- An assignment of the initial risk of a cyber security threat.
- Risk prioritization.

For the three cyber security breach scenarios, the external cyber-attacks from cybercriminals and state adversaries were ranked with a high level of risk and likelihood to occur. The scenario where an insider-led cyber breach occurs was ranked at a medium level of risk, with high likelihood for it to occur. Risks and likelihoods are considered separate variables per API STD 780. The likelihood of a successful attack is calculated as a function of consequence and probability or the frequency of occurrence, considering the relative grade of risk to the asset in terms of the expected effect to each identified critical asset. For the determination of risk, a risk-ranking matrix was used, per API STD 780. In all three cases, risk was prioritized based on the selection and deployment of countermeasures and their potential effect. Also, countermeasure arrangement was evaluated based on the availability and effectiveness of technical, corporate/organizational, and financial resources.

Finally, in Step 05 of the SRA, the risk-treatment process is performed, where the following are achieved:

- An evaluation of the need for and subsequent recommendation for countermeasures.
- A re-calculation of the likelihood of an attack and the severity of consequences.
- A calculation of residual risks.
- A ranking of proposed countermeasures.

For the three cyber security breach scenarios, the countermeasures identified in Step 03 of the SRA remain valid for the reduction of vulnerabilities and residual risks. Their selective use depends on available resources and technical feasibility, as dictated by corporate management and technical stakeholders.

4.3. Application of BTA

The cyber–physical security breach scenarios involving malware contamination and interference to the drillship's DP system by external (cybercriminals and intestate adversaries) and internal (vessel crew members) threat actors are described below. These scenarios are based on the SRA carried out and the DP and network diagram in Figure 2. The combined Bow-Tie Analysis example for the identified cyber breach scenarios is shown in Figure 4.

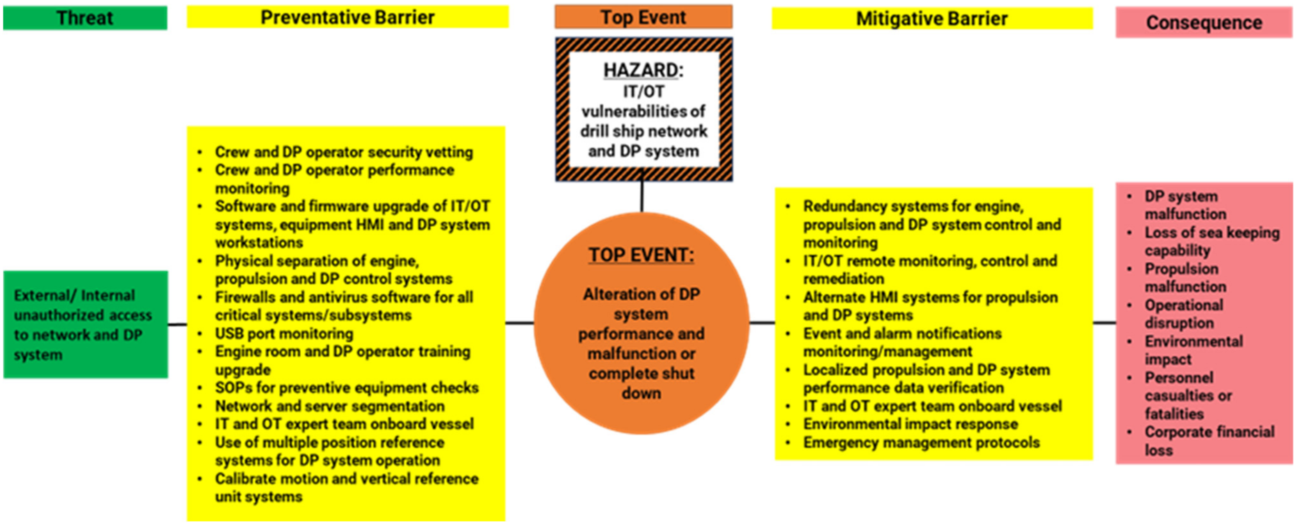
Threat
Preventative Barrier
Top Event
Mitigative Barrier
Consequence
HAZARD:
IT/OT vulnerabilities of drill ship network and DP system
External/ Internal unauthorized access to network and DP system
• Crew and DP operator security vetting
• Crew and DP operator performance monitoring
• Software and firmware upgrade of IT/OT systems, equipment HMI and DP system workstations
• Physical separation of engine, propulsion and DP control systems
• Firewalls and antivirus software for all critical systems/subsystems
• USB port monitoring
• Engine room and DP operator training upgrade
• SOPs for preventive equipment checks
• Network and server segmentation
• IT and OT expert team onboard vessel
• Use of multiple position reference systems for DP system operation
• Calibrate motion and vertical reference unit systems
TOP EVENT:
Alteration of DP system performance and malfunction or complete shut down
• Redundancy systems for engine, propulsion and DP system control and monitoring
• IT/OT remote monitoring, control and remediation
• Alternate HMI systems for propulsion and DP systems
• Event and alarm notifications monitoring/management
• Localized propulsion and DP system performance data verification
• IT and OT expert team onboard vessel
• Environmental impact response
• Emergency management protocols
• DP system malfunction
• Loss of sea keeping capability
• Propulsion malfunction
• Operational disruption
• Environmental impact
• Personnel casualties or fatalities
• Corporate financial loss

Figure 4. Bow-Tie Analysis for drillship's DP system cyber breach scenarios.

The identified preventive barriers for the selected cyber security breach scenarios are the following:

- Security vetting and performance monitoring of the drillship's crew and DP system operator.
- Software and firmware of IT and OT systems, equipment HMIs, and DP system.
- A physical separation (segregation) of the vessel engine, propulsion, and DP control systems.
- The installation of firewalls and antivirus software for all critical systems and subsystems.

- The monitoring of USB port usage in all IT and OT systems.
- Upgrade the training for use of the engine room and DP operators.
- SOPs for preventive equipment checks.
- Network and server segmentation.
- The placement of an IT and OT expert team onboard the vessel.
- The use of multiple position reference systems for DP system operations.
- The calibration of motion and vertical reference unit systems.

From the above barriers, insider-threat mitigation measures (employee vetting and performance monitoring) should be emphasized to prevent disgruntled employees from causing damage or sabotaging the IT/OT systems of the vessel. Also, the monitoring, control, or blockage of the use of or access to USB ports eliminate the intentional or unintentional transfer of malware to IT/OT systems. Operator training and emergency procedures, as part of this effort, also increase cyber awareness and establish cyber hygiene practices. The monitoring of critical operational parameters for propulsions and the DP system and interventions in the case of excessive deviations are also other barriers with great potential to mitigate the threat scenarios analyzed. The use of antivirus software and firewalls in systems would also eliminate the installation of malware, but their technical and operational feasibility will depend on the type and age of the IT and OT systems and software/firmware on board the vessel.

In the post-event side of the bow-tie diagram, the mitigation barriers that could be used are the following:

- Redundancy systems for the control and monitoring of the engine, propulsions, and DP system.
- The remote monitoring, control, and remediation of the IT/OT system.
- The alternate HMI systems for the propulsion and DP systems.
- The monitoring and management of event and alarm notifications.
- The verification of the performance data of the propulsions and DP system.
- The placement of an IT and OT expert team onboard the vessel.
- Responses to environmental impacts.
- Emergency management protocols.

The post-event barriers would include the installation of a redundant system to enable the operation of substitute systems, such as the bridge joystick DP workstation, which independently relies on the gyro compass and vertical reference unit, as indicated in Figure 2. This, of course, can be a solution to maintain some sea-keeping capabilities of the drillship, assuming it is not compromised by the malware attack through the IT/OT network. Event management and alarm notifications could also be included in the system, assuming there is no overlap or duplicate of such systems. A localized verification of the operational parameters of the vessel's engine, propulsions, and DP system would also be a reliable barrier to monitoring the system's overall performance and would act to prevent operational malfunctions or abnormalities. It would be assumed for such a method, however, that the operators possess the necessary in-depth knowledge of the system's performance and understand system data, which is something that could be fortified by upgrading their training. The utilization of an on-board IT and OT expert team of operators, along with possible remote (from corporate IT/OT experts or third-party experts) monitoring and control, could also prove crucial in the mitigation of malfunctions and shut downs of the vessel's engine and DP system. Emergency management protocols need to be set in place to tackle worst-case scenarios, such as a loss of sea-keeping capabilities and the power of the vessel and potential environmental impacts due to a disruption of well drilling operations.

Finally, it should be highlighted that operator use and the level or lack of knowledge of systems are degradation factors, as they can potentially reduce the effect of any preventive barriers applied, leading to negative consequences. The IT/OT system operators' roles are crucial in maintaining preventive and mitigating barriers.

5. Conclusions

Through the known cyber security attacks against maritime vessels, it is evident that these are targeted towards specific equipment and systems. It is, therefore, safe to assume that aggressors have a very good understanding of the technical aspects of maritime vessels, their industrial control systems, IT/OT infrastructure and systems, and maritime operations.

The evolving threat landscape indicates the necessity for increasing or reinforcing the cyber security posture and operational resilience of the maritime transport sector. This can only be achieved through the allocation of adequate resources from the industry stakeholders and corporate entities involved.

An examination of available industry and governmental directives and standards, presented in Table 2, concerning the cyber security aspects for maritime vessels, indicated that a majority of these do cover the subject; however, they do so mainly through guidelines to protect or reinforce existing IT or OT systems and infrastructures. A majority of these directives, guidelines, and standards remain generic documents, recommending improved practices for the reinforcement of the security posture of IT and OT systems without being specific about the critical systems, processes, or components deemed operationally or technically critical for specialized vessels, such as the selected drillship. Also, the implementation of existing maritime cyber security directives, policies, and standards needs to be reinforced by the industry stakeholders in order to maintain the necessary level of compliance and, in turn, cyber security posture.

A plethora of cyber–physical security assessment methods or frameworks are presented in Table 3, and, in most cases, these are used in "laboratory-" or "classroom-" based environments and are aimed at presenting technical features, the feasibility of usage, and assessment capabilities. These methods and frameworks do not seem to adequately tackle the problem of field validation and industry implementation, which consider technical and resource constraints.

The credibility of the cyber breach scenario involving the drillship's network and leading to a remote incapacitation of its DP system was validated through a cyber–physical security assessment carried out using the API SRA and BTA tools. The use of API SRA proved to be a valuable tool in assessing cyber–physical security threats, vulnerabilities, and target attractiveness for maritime vessels serving as elements in the maritime transportation and oil and gas critical infrastructure sectors. Similarly, the application of the BTA method proved to be a useful tool that visualizes the threat scenario path of events, highlighting the pre- and post-event stages and the preventive and mitigative barriers in place. The combined use of the API SRA and BTA validated the selected security breach scenarios through a confirmation of the preventive and mitigative countermeasures prior to and after the cyber security breach in the DP system of the drillship.

Human factors, the crew members of maritime vessels, play the most crucial role in the compliance with cyber security directives, the maintenance of the cyber security posture, and the implementation of emergency procedures for a cyber breach. They are the ones that need to balance maritime operations, cyber security hygiene, and vessel-system usage. It is, therefore, imperative that the necessary training and resources are allocated to reinforce their capacity in the mitigation of cyber threats and safe maritime operations.

6. Discussion

The implementation of the API SRA and BTA methods assumes the use of the technical drawings of a drillship; however, only a small number of drawings of the vessel's system were made available to the authors, due to confidentiality reasons. Similarly, the diagram of the network and DP system created by the authors is a typical configuration, as it was partially based on publicly available data. So, it may not capture all the technical parameters or system architectures of existing DP systems and IT/OT network diagrams of maritime vessels.

It is possible that standards, directives, or guidelines and policies related to maritime cyber security may have been omitted during the writing of this publication. Similarly, academic and research publications on the subject of maritime cyber–physical security may have been missed. This was not intentional but due the fact that the subject of this article can be expanded beyond the resources available to the authors and that some standards or publications may have been released after the submission of this article for publication.

With regard to the latest release of NIST CSF v2.0, it should be noted that it holds significant implications for OT professionals involved in the maritime sector. While NIST CSF v2.0 provides a comprehensive set of guidelines for managing cyber risks, its application to the maritime sector reveals a gap, particularly in the cyber security of Operational Technology (OT) systems. These systems, crucial for the control of physical operations on vessels and at ports, are closely connected to the maritime supply chain, and their disruption can have significant repercussions. A published research study [105] revealed critical gaps in how the maritime industry has implemented NIST CSF v2.0, pointing out that it is not being fully utilized for maritime cyber security. The study emphasizes the urgent need for a version of this framework, specifically adapted for maritime use, which could significantly improve cyber security resilience in this sector. Furthermore, there is a notable lack of research on cyber security in maritime supply chains, a vital area closely connected to Operational Technology (OT) systems on ships and the wider maritime sector. This identified gap underscores the necessity for increased research to strengthen cyber security across all aspects of maritime activities. In addition, the application of NIST CSF v2.0 does not account for the engineering approaches to the management of physical security due to cyber security threats of OT and IT systems in the industrial and general critical infrastructure sectors [76], leading to the ineffective implementation of cyber–physical security for such assets.

Finally, considering the recent release of the IACS Unified Requirements UR E26 [38] and E27 [39], it should be highlighted that their implementation in the maritime sector requires time and resource allocation. The implementation to maritime vessels may be constrained by the interpretation of UR E26 and UR E27 by shipping companies and maritime vessel owners or operators, due to the presumed financial and technical implications of new builds or recently deployed vessels. The industry may need some clarification and guidance on the implementation of UR E26 and E27, which would require the involvement of all industry stakeholders, including vessel classifications, maritime insurance, and governmental entities.

Author Contributions: I.P. conceived of the title, idea, and layout of the paper; wrote and edited the draft and final manuscript; and carried out the SRA and BTA analysis. I.K.D. and A.D. provided input to the title, vessel network, and DP system architecture, and cyber security threat landscape and vulnerabilities and reviewed and assisted in editing the manuscript. T.L. provided input to the cyber–physical security scenarios and reviewed and assisted in editing the manuscript. N.N. provided supervision and direction on the layout and structure of the paper and reviewed and assisted in editing the manuscript. P.M.P. provided input on the ship engine systems and reviewed and assisted in editing the 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.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to confidentiality reasons.

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

References

1. Meland, P.H.; Bernsmed, K.; Wille, E.; Rødseth, Ø.J.; Nesheim, D.A. A retrospective analysis of maritime cyber security incidents. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2021**, *15*, 519–530. [CrossRef]
2. Ben Farah, M.A.; Ukwandu, E.; Hindy, H.; Brosset, D.; Bures, M.; Andonovic, I.; Bellekens, X. Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information* **2022**, *13*, 22. [CrossRef]
3. Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. Cybersecurity challenges in the maritime sector. *Network* **2022**, *2*, 123–138. [CrossRef]
4. Ubaleht, J. Importance of Positioning to MASS: The Effect of Jamming and Spoofing on Autonomous Vessel. Master's Thesis, Novia University of Applied Sciences, Vaasa, Finland, 2022.
5. Hambling, D. Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon. New Scientist; 10 August 2017. Available online: https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/ (accessed on 2 August 2024).
6. Leite Junior, W.C.; de Moraes, C.C.; de Albuquerque, C.E.; Machado, R.C.S.; de Sá, A.O. A triggering mechanism for cyber-attacks in naval sensors and systems. *Sensors* **2021**, *21*, 3195. [CrossRef]
7. Bolbot, V.; Methlouthi, O.; Banda, O.V.; Xiang, L.; Ding, Y.; Brunou, P. Identification of cyber-attack scenarios in a marine Dual-Fuel engine. In *Trends in Maritime Technology and Engineering*; CRC Press: Boca Raton, FL, USA, 2022; pp. 503–510.
8. Rundle, J. Coast Guard Details February Cyberattack on Ship. *WSJ. Wall Str. J.* **2019**, *26*. Available online: https://www.wsj.com/articles/coast-guard-details-february-cyberattack-on-ship-11564133401 (accessed on 1 August 2024).
9. Seanews Editor. Naval Dome CEO Itai Sela Comments on Attacks on Tankers Near Port of Fujairah—Sea News. Sea News—Global Maritime News. 16 May 2019. Available online: https://seanews.co.uk/shipping-news/naval-dome-ceo-itai-sela-comments-on-attacks-on-tankers-near-port-of-fujairah/ (accessed on 11 July 2024).
10. Cyber-Attacks on Maritime Oil Tankers. (n.d.). Available online: https://www.cybersecurityintelligence.com/blog/cyber-attacks-on-maritime-oil-tankers-4293.html (accessed on 1 August 2024).
11. Babb, C. US Cyberattack Hit 2 Iranian Military Ships in Red Sea. Voice of America; Voice of America (VOA News). 17 February 2024. Available online: https://www.voanews.com/a/us-cyberattack-hit-2-iranian-military-ships-in-red-sea-/7491503.html (accessed on 1 August 2024).
12. The Maritime Executive. Report: U.S. Carried Out Covert Cyberattack on Iranian Spy Ship. The Maritime Executive; The Maritime Executive. 15 February 2024. Available online: https://maritime-executive.com/article/report-u-s-carried-out-covert-cyberattack-on-iranian-spy-ship (accessed on 5 July 2024).
13. Svilicic, B.; Rudan, I.; Jugović, A.; Zec, D. A study on cyber security threats in a shipboard integrated navigational system. *J. Mar. Sci. Eng.* **2019**, *7*, 364. [CrossRef]
14. Tam, K.; Hopcraft, R.; Moara-Nkwe, K.; Misas, J.P.; Andrews, W.; Harish, A.V.; Gimienez, P.; Chrichton, T.; Jones, K. Case study of a cyber-physical attack affecting port and ship operational safety. *J. Transp. Technol.* **2021**, *12*, 1–27. [CrossRef]
15. Vu, L.; Nguyen, T.L.; Abdelrahman, M.S.; Vu, T.; Mohammed, O.A. A cyber-HIL for investigating control systems in ship cyber physical systems under communication issues and cyber attacks. *IEEE Trans. Ind. Appl.* **2023**, *60*, 2142–2152. [CrossRef]
16. Hassani, V.; Crasta, N.; Pascoal, A.M. Cyber security issues in navigation systems of marine vessels from a control perspective. In Proceedings of the International Conference on Offshore Mechanics and Arctic Engineering, Trondheim, Norway, 25–30 June 2017; p. V07BT06A029.
17. Dryad Global. Can a Cyber Attack Control a Ship? Dryad Global Ltd. 30 July 2024. Available online: https://channel16.dryadglobal.com/can-a-cyber-attack-control-a-ship (accessed on 5 August 2024).
18. Bush, D. Ethical Hacker Says Ships Are Wide Open to Cyber Attack. Lloyd's List. 27 May 2021. Available online: https://www.lloydslist.com/LL1136933/Ethical-hacker-says-ships-are-wide-open-to-cyber-attack (accessed on 1 August 2024).
19. The Danish Center for Cybersecurity. The Cyber Threat against Operational Systems on Ships. Centre for Cybersecurity. 2020. Available online: https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/-cyber_threat_against_operational_systems_on_ships-.pdf (accessed on 10 August 2024).
20. ENISA. *(European Union Agency for Cybersecurity) ENISA Threat Landscape: Transport Sector (January 2021 to October 2022)*; ENISA Publications Office: Attiki, Greece, 2023. Available online: https://data.europa.eu/doi/10.2824/553997 (accessed on 1 August 2024).
21. COMPU-VISION. Cyber Attacks on Shipping See Rapid Growth in Numbers. Roban Assafina. 2024. Available online: https://assafinaonline.com/news_details/en/20768/Cyber-attacks-on-shipping-see-rapid-growth-in-numbers (accessed on 1 August 2024).
22. United States Coast Guard (USCG); U.S. Coast Guard Cyber Command (CGCYBER). 2023 Cyber Trends and Insights in the Marine Environment Report. 22 April 2024. Available online: https://www.news.uscg.mil/maritime-commons/Article/3750095/2023-cyber-trends-and-insights-in-the-marine-environment-report/ (accessed on 4 August 2024).
23. The Guidelines on Cyber Security Onboard Ships. 2023. Available online: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships (accessed on 3 August 2024).
24. ENISA (European Union Agency for Cybersecurity) Foresight Cybersecurity Threats For 2030—Update 2024. ENISA. Available online: https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024 (accessed on 3 August 2024).

25. Progoulakis, I.; Rohmeyer, P.; Nikitakos, N. Cyber physical systems security for maritime assets. *J. Mar. Sci. Eng.* **2021**, *9*, 1384. [CrossRef]
26. Progoulakis, I.; Nikitakos, N.; Dalaklis, D.; Christodoulou, A.; Dalaklis, A.; Yaacob, R. Digitalization and cyber physical security aspects in maritime transportation and port infrastructure. In *Smart Ports and Robotic Systems: Navigating the Waves of Techno-Regulation and Governance*; Springer International Publishing: Cham, Switzerland, 2023; pp. 227–248.
27. Taherdoost, H. Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics* **2022**, *11*, 2181. [CrossRef]
28. Djebbar, F.; Nordström, K. A comparative analysis of industrial cybersecurity standards. *IEEE Access* **2023**, *11*, 85315–85332. [CrossRef]
29. Kalogeraki, E.M.; Polemi, N. A taxonomy for cybersecurity standards. *Secur. Saf.* **2024**, *5*, 95–115. [CrossRef]
30. *ISO/IEC 27001*; Information Technology-Security Techniques-Information Security Management Systems–Requirements. ISO/IEC: Geneva, Switzerland, 2013.
31. *IEC-62443-4-2*; Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components. IEC: Geneva, Switzerland, 2019.
32. *IEC 62443-3-3*; Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels. IEC: Geneva, Switzerland, 2013.
33. *ISO/IEC 21827*; Information Technology-Security Techniques-Systems Security Engineering-Capability Maturity Model® (SSE-CMM®). ISO/IEC: Geneva, Switzerland, 2008.
34. *ISO/IEC 15408-1*; Information Technology-Security Techniques-Evaluation Criteria for IT Security. ISO/IEC: Geneva, Switzerland, 2009.
35. *ISO/IEC 18045*; Information Technology-Security Techniques-Methodology for IT Security Evaluation. ISO/IEC: Geneva, Switzerland, 2008.
36. *ISO/IEC 27032*; Information Technology-Security Techniques-Guidelines for Cybersecurity. ISO/IEC: Geneva, Switzerland, 2012.
37. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0; Public Draft NIST.CSWP.29.ipd. 2024. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (accessed on 2 August 2024).
38. International Association of Classification Societies (IACS) UR E26 Cyber Resilience of Ships—Rev. 1 November 2023. Available online: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/02/04140503/UR-E26-Rev.1-Nov-2023-CR.pdf (accessed on 1 November 2023).
39. International Association of Classification Societies (IACS) UR E27 Cyber Resilience of On-Board Systems and Equipment—Rev.1 Sep 2023. Available online: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103853/UR-E27-Rev.1-Sep-2023-CLN.pdf (accessed on 2 August 2024).
40. Kavallieratos, G.; Katsikas, S. Managing cyber security risks of the cyber-enabled ship. *J. Mar. Sci. Eng.* **2020**, *8*, 768. [CrossRef]
41. Lagouvardou, S. *Maritime Cyber Security: Concepts, Problems and Models*; Department of Management Engineering: Kongens Lyngby, Copenhagen, 2018.
42. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing cyber challenges of maritime navigation. *J. Mar. Sci. Eng.* **2020**, *8*, 776. [CrossRef]
43. Miranda Silgado, D. Cyber-Attacks: A Digital Threat Reality Affecting the Maritime Industry. Ph.D. Thesis, World Maritime University, Malmö, Sweden, 11 April 2018.
44. Tusher, H.M.; Munim, Z.H.; Notteboom, T.E.; Kim, T.E.; Nazir, S. Cyber security risk assessment in autonomous shipping. *Marit. Econ. Logist.* **2022**, *24*, 208–227. [CrossRef]
45. Zhou, X.Y.; Liu, Z.J.; Wang, F.W.; Wu, Z.L. A system-theoretic approach to safety and security co-analysis of autonomous ships. *Ocean. Eng.* **2021**, *222*, 108569. [CrossRef]
46. Bolbot, V.; Theotokatos, G.; Boulougouris, E.; Vassalos, D. A novel cyber-risk assessment method for ship systems. *Saf. Sci.* **2020**, *131*, 104908. [CrossRef]
47. Melnyk, O.; Onyshchenko, S.; Onishchenko, O.; Lohinov, O.; Ocheretna, V. Integral approach to vulnerability assessment of ship's critical equipment and systems. *Trans. Marit. Sci.* **2023**, *12*, 1–10. [CrossRef]
48. Häyhtiö, M.; Zaerens, K. A comprehensive assessment model for critical infrastructure protection. *Manag. Prod. Eng. Rev.* **2017**, *8*, 42–53. [CrossRef]
49. Alidoosti, A.; Yazdani, M.; Fouladgar, M.M.; Basiri, M.H. Risk assessment of critical asset using fuzzy inference system. *Risk Manag.* **2012**, *14*, 77–91. [CrossRef]
50. Lewis, T.G.; Mackin, T.J.; Darken, R. Critical infrastructure as complex emergent systems. *Int. J. Cyber Warf. Terror. (IJCWT)* **2011**, *1*, 1–12. [CrossRef]
51. Pollet, J.; Cummins, J. All Hazards Approach for Assessing Readiness of Critical Infrastructure. In Proceedings of the IEEE Conference on Technologies for Homeland Security, Boston, MA, USA, 11–12 May 2009; pp. 366–372.
52. Taquechel, E.F.; Lewis, T.G. A Right-Brained Approach to Critical Infrastructure Protection Theory in support of Strategy and Education: Deterrence, Networks, Resilience, and "Antifragility". *Homel. Secur. Aff.* **2017**, *13*, 50–83.
53. Ivanc, B.; Klobucar, T. Attack Modeling in the Critical Infrastructure/Modeliranje napadov v kriticni infrastrukturi. *Elektrotehniski Vestn.* **2014**, *81*, 285.

54. Theoharidou, M.; Kotzanikolaou, P.; Gritzalis, D. Towards a Criticality Analysis Methodology: Redefining Risk Analysis for Critical Infrastructure Protection. In Proceedings of the 3rd IFIP International Conference on Critical Infrastructure Protection, Hanover, NH, USA, 22–25 March 2009.
55. Misuri, A.; Khakzad, N.; Reniers, G.; Cozzani, V. A Bayesian network methodology for optimal security management of critical infrastructures. *Reliab. Eng. Syst. Saf.* **2019**, *191*, 106112. [CrossRef]
56. Ryu, D.H.; Kim, H.; Um, K. Reducing security vulnerabilities for critical infrastructure. *J. Loss Prev. Process Ind.* **2009**, *22*, 1020–1024. [CrossRef]
57. Brown, G.; Carlyle, M.; Salmerón, J.; Wood, K. Defending critical infrastructure. *Interfaces* **2006**, *36*, 530–544. [CrossRef]
58. Alderson, D.L.; Brown, G.G.; Carlyle, W.M.; Wood, R.K. *Solving Defender-Attacker-Defender Models for Infrastructure Defense*; Naval Postgraduate School Monterey CA, Dept of Operations Research: Monterey, CA, USA, 2011.
59. Baker, G.H. A vulnerability assessment methodology for critical infrastructure sites. In *DHS Symposium: R and D Partnerships in Homeland Security*; James Madison University: Harrisonburg, VA, USA, 2005.
60. Ouyang, M. Critical location identification and vulnerability analysis of interdependent infrastructure systems under spatially localized attacks. *Reliab. Eng. Syst. Saf.* **2016**, *154*, 106–116. [CrossRef]
61. Augutis, J.; Jokšas, B.; Krikštolaitis, R.; Urbonas, R. The assessment technology of energy critical infrastructure. *Appl. Energy* **2016**, *162*, 1494–1504. [CrossRef]
62. Taquechel, E.F.; Lewis, T.G. How to Quantify Deterrence and Reduce Critical Infrastructure Risk. *Homel. Secur. Aff.* **2012**, *8*, 1–28.
63. Karantjias, A.; Polemi, N.; Papastergiou, S. Advanced security management system for critical infrastructures. In Proceedings of the IISA 2014, The 5th International Conference on Information, Intelligence, Systems and Applications, Chania, Greece, 7–9 July 2014; pp. 291–297.
64. Lewis, T.G.; Darken, R.P.; Mackin, T.; Dudenhoeffer, D. Model-based risk analysis for critical infrastructures. *WIT Trans. State—Art Sci. Eng.* **2012**, *54*.
65. Taquechel, E. Layered defense: Modeling terrorist transfer threat networks and optimizing network risk reduction. *IEEE Network* **2010**, *24*, 30–35. [CrossRef]
66. Valencia, V.V.; Thal, A.E., Jr. Applying the Model-Based Vulnerability Assessment Technique to Interdependent Infrastructures. In Proceedings of the IIE Annual Conference, Orlando, FL, USA, 19–23 May 2012.
67. Gran, B.A.; Fredriksen, R.; Thunem, A.P.J. Addressing dependability by applying an approach for model-based risk assessment. *Reliab. Eng. Syst. Saf.* **2007**, *92*, 1492–1502. [CrossRef]
68. Wu, B.; Tang, A.; Wu, J. Modeling cascading failures in interdependent infrastructures under terrorist attacks. *Reliab. Eng. Syst. Saf.* **2016**, *147*, 1–8. [CrossRef]
69. Oruc, A.; Kavallieratos, G.; Gkioulos, V.; Katsikas, S. Cyber Risk Assessment for SHips (CRASH). *Int. J. Mar. Navig. Saf. Sea Transp.* **2023**, *18*, 115–124. [CrossRef]
70. Tatar, U.; Karabacak, B.; Keskin, O.F.; Foti, D.P. Charting New Waters with CRAMMTS: A Survey-Driven Cybersecurity Risk Analysis Method for Maritime Stakeholders. *Comput. Secur.* **2024**, *145*, 104015. [CrossRef]
71. Rajaram, P.; Goh, M.; Zhou, J. Guidelines for cyber risk management in shipboard operational technology systems. *J. Phys. Conf.* **2022**, *2311*, 012002. [CrossRef]
72. Enoch, S.Y.; Lee, J.S.; Kim, D.S. Novel security models, metrics and security assessment for maritime vessel networks. *Comput. Netw.* **2021**, *189*, 107934. [CrossRef]
73. Kapalidis, C.; Karamperidis, S.; Watson, T.; Koligiannis, G. A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships. *J. Mar. Sci. Eng.* **2022**, *10*, 1486. [CrossRef]
74. van Staalduinen, M.A.; Khan, F.; Gadag, V. SVAPP methodology: A predictive security vulnerability assessment modeling method. *J. Loss Prev. Process Ind.* **2016**, *43*, 397–413. [CrossRef]
75. Marszal, E.M.; McGlone, J. *Security PHA Review for Consequence-Based Cybersecurity*; International Society of Automation (ISA): Research Triangle Park, NC, USA, 2019.
76. Ginter, A. *Engineering-Grade OT Security: A Manager's Guide*; Abterra Technologies Inc.: Calgary, AB, Canada, 2023.
77. Baybutt, P. Cyber security risk analysis for process control systems using rings of protection analysis (ROPA). *Process Saf. Prog.* **2004**, *23*, 284–291. [CrossRef]
78. Roldán-Molina, G.; Almache-Cueva, M.; Silva-Rabadão, C.; Yevseyeva, I.; Basto-Fernandes, V. A comparison of cybersecurity risk analysis tools. *Procedia Comput. Sci.* **2017**, *121*, 568–575. [CrossRef]
79. Knowles, W.; Prince, D.; Hutchison, D.; Disso, J.F.P.; Jones, K. A survey of cyber security management in industrial control systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *9*, 52–80. [CrossRef]
80. Erbas, M.; Khalil, S.M.; Tsiopoulos, L. Systematic literature review of threat modeling and risk assessment in ship cybersecurity. *Ocean. Eng.* **2024**, *306*, 118059. [CrossRef]
81. American Petroleum Institute (API). *Standard (STD) 780: Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries*; API: Washington, DC, USA, 2013.
82. U.S. Department of Homeland Security (DHS); Cybersecurity and Infrastructure Security Agency (CISA). *Chemical Facility Anti-Terrorism Standards (CFATS)*; 2014. Available online: https://www.cisa.gov/chemical-facility-anti-terrorism-standards (accessed on 10 September 2024).

83. American Institute of Chemical Engineers. *Center for Chemical Process Safety. Bow Ties in Risk Management: A Concept Book for Process Safety*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2018.
84. DRAGOS Inc.; OSIsoft Inc. 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 2 August 2024).
85. aeBlogs: "The Benefits of Visualizing CyberPHAs Using Bowtie Diagrams". aeSolutions Inc. Available online: https://www.linkedin.com/pulse/benefits-visualizing-cyberphas-using-bowtie-diagrams-kramer-mba/ (accessed on 2 June 2024).
86. 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 22 May 2024).
87. Arnaboldi, L.; Aspinall, D. Towards interdependent safety security assessments using bowties. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Florence, Italy, 6–9 June 2022; Springer International Publishing: Cham, Switzerland, 2022; pp. 211–229.
88. Yang, S.H.; Cao, Y.; Wang, Y.; Zhou, C.; Yue, L.; Zhang, Y. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. *Process Saf. Environ. Prot.* **2021**, *148*, 1279–1291.
89. Meland, P.H.; Bernsmed, K.; Frøystad, C.; Li, J.; Sindre, G. An experimental evaluation of bow-tie analysis for security. *Inf. Comput. Secur.* **2018**, *26*, 536–561. [CrossRef]
90. 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]
91. 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.
92. Progoulakis, I.; Nikitakos, N.; Rohmeyer, P.; Bunin, B.; Dalaklis, D.; Karamperidis, S. Perspectives on cyber security for offshore oil and gas assets. *J. Mar. Sci. Eng.* **2021**, *9*, 112. [CrossRef]
93. Nolan, D.P. *Safety and Security Review for the Process Industries: Application of HAZOP, PHA, What-If and SVA Reviews*; Elsevier: Amsterdam, The Netherlands, 2015.
94. 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*; DNV GL: Oslo, Norway, 2016; Volume 5.
95. International Organization for Standardization/International Electrotechnical Commission standard ISO/IEC 31010. *Risk Management—Risk Assessment Techniques*; International Organization for Standardization: Geneva, Switzerland, 2019.
96. DP Ships Potentially at Risk from Cyber Attacks. Riviera. 2024. Available online: https://www.rivieramm.com/news-content-hub/news-content-hub/dp-ships-potentially-at-risk-from-cyber-attacks-37302 (accessed on 18 May 2024).
97. Hamill-Stewart, J. The Cyber Vulnerabilities of Dynamic Positioning Systems. The Maritime Executive. 6 March 2023. Available online: https://maritime-executive.com/editorials/the-cyber-vulnerabilities-of-dynamic-positioning-systems (accessed on 19 May 2024).
98. Hacking the Ship Scenario: An Offshore Supply Vessel's Dynamic Positioning System. ABS Group. 2015. Available online: https://www.abs-group.com/Knowledge-Center/Insights/Hacking-the-Ship-Scenario-An-Offshore-Supply-Vessels-Dynamic-Positioning-System/ (accessed on 18 May 2024).
99. United States Coast Guard (USCG). U.S. Coast Guard Inspections and Compliance Directorate, Marine Safety Alert 11-22: Dynamic Positioning Systems—Don't Overestimate Their Capabilities! 1 November 2022. Available online: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/USCGSA_1122.pdf?ver=3De_jhZjFj31ThdbAFE-Gg== (accessed on 4 August 2024).
100. Baker, B.J.; Call, I.F.R. *A Primer of Oilwell Drilling: A Basic Text of Oil and Gas Drilling*; Petroleum Extension Service, Continuing & Extended Education, University of Texas at Austin: Austin, TX, USA, 2001.
101. International Maritime Organization (IMO). *Resolution MSC.1/Circ. 1580, Guidelines for Vessels and Units with Dynamic Positioning*; IMO Publishing: London, UK, 2017.
102. International Maritime Organization (IMO). *Resolution MSC/Circ. 645 Guidelines for Vessels with Dynamic Positioning Systems*; IMO Publishing: London, UK, 1994.
103. American Bureau of Shipping (ABS). *Guide for Dynamic Positioning Systems*; ABS: Houston, TX, USA, 2024.
104. Teriakidis, G.; (Naval Architect, Athens, Greece). Personal communication, 29 June 2018.
105. Dimakopoulou, A.; Rantos, K. Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2. 0. *J. Mar. Sci. Eng.* **2024**, *12*, 919. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.