Journal of
Marine Science and Engineering

MDPI

Article

Managing Cyber Security Risks of the Cyber-Enabled Ship

Georgios Kavallieratos * and Sokratis Katsikas *

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 2815 Gjøvik, Norway

* Correspondence: georgios.kavallieratos@ntnu.no (G.K.); sokratis.katsikas@ntnu.no (S.K.)

Received: 12 September 2020; Accepted: 28 September 2020; Published: 30 September 2020

Abstract: One aspect of the digital transformation process in the shipping industry, a process often referred to as Shipping 4.0, is the increased digitization of on board systems that goes along with increased automation in and autonomy of the vessel. This is happening by integrating Information Technology with Operation Technology systems that results in Cyber Physical Systems on which the safe operations and sailing of contemporary and future vessels depend. Unavoidably, such highly interconnected and interdependent systems increase the exposure of the vessel's digital infrastructure to cyber attacks and cyber security risks. In this paper, we leverage the STRIDE and DREAD methodologies to qualitatively and quantitatively assess the cyber risk of Cyber Physical Systems on board digitalized contemporary and future ships. Further, we propose appropriate cyber security baseline controls to mitigate such risks, by applying a systematic approach using a set of criteria that take into account the security requirements; the cyber risks; the possible attacks; and the possibly already existing controls, to select from the list of controls provided in the Industrial Control Systems (ICS) overlay of the NIST Guide to ICS Security. The results are expected to support the decision-making and the design of a security architecture for the cyber-enabled ship.

Keywords: cyber-enabled ship; cyber risk assessment; cyber security controls selection; cyber physical systems

1. Introduction

Despite the fact that today almost all ships are to some extent digitalized, the shipping industry addresses the digital transformation challenge, including the emergence of crew-less vessels [1]. Such vessels come in two broad categories, namely the remotely operated vessel and the autonomous vessel; both kinds are referred to as *cyber-enabled ships (C-ES)* [2]. The C-ES is a cyber physical ecosystem which consists of the vessel itself, a Shore Control Center (SCC) that controls and handles the C-ES, the communication links between the vessel and the SCC, and other ships in the vicinity.

The integration of Information Technology (IT) and Operation Technology (OT) to form *Cyber Physical Systems (CPS)*, which constitute a central element of the digital transformation process in many application domains is unavoidably accompanied by an increase and a diversification of the cyber risks that the domain is facing. This is mainly due to the fact that whereas traditional operations were designed with no need for cyber security in mind, modern IT-enabled operations are allowed to be accessed and controlled by outward-facing information systems, through interfaces that are rarely adequately secure [3].

The C-ES is no exception. Although most of the C-ES CPSs are parts of today's conventional ships, their exposure to contemporary technologies, aiming to be controlled and monitored remotely, increases the attack surface and makes them more vulnerable to cyber-attacks. Indeed, research on the cyber security risks of autonomous and unmanned vessels [2,4] has revealed an increased attack surface and several vulnerable systems. Thus, ship-side cyber security incidents, such as, for example, the ones reported in Reference [5–7] , have already occurred; in fact, such incidents have been increasing at an alarming rate over the last three years [8]. Such incidents may also impact the safety of humans, operations, and cargo.

In the light of these findings, of the increased financial value of the sector [9], and of the multitude of potential attackers, including such with advanced capabilities, the promotion of cyber security and safety of the C-ES ecosystem becomes very important [10]. The first step towards strengthening the cyber security posture of an ecosystem is to understand, analyze, and manage the cyber risks that it faces; this will eventually drive the design of a security architecture that includes appropriate cyber security controls that will mitigate the risks.

Risk is defined as "the effect of uncertainty on objectives" [11]. Cyber Security risk is associated with the potential that threats will exploit vulnerabilities of an asset or group of assets and thereby cause harm to an organization. Cyber risk is assessed in terms of the likelihood of a *threat*[1] occurring, the extent of the *vulnerabilities*[2] to the threat, and the magnitude of the *impact*[3]; these constitute the *elements* of cyber risk.

The risk management process as specified in ISO 31000 [13] comprises five sub-processes [11], as shown in Figure 1:

1. The external and internal context for cyber security risk management should be established, which involves setting the basic criteria necessary for cyber security risk management, defining the scope and boundaries, and establishing an appropriate organization operating the cyber security risk management.
2. Risks should be assessed, i.e., identified, quantified or qualitatively described, and prioritized against risk evaluation criteria and objectives relevant to the organization.
3. Controls to reduce, retain, avoid, or share the risks should be selected and a risk treatment plan defined.
4. Information about risk should be exchanged and/or shared between the decision-makers and other stakeholders.
5. Risks and their elements should be monitored and reviewed to identify any changes at an early stage and to maintain an overview of the complete risk picture. This is why, as Figure 1 illustrates, the cyber security risk management process can be iterative for risk assessment and/or risk treatment activities.

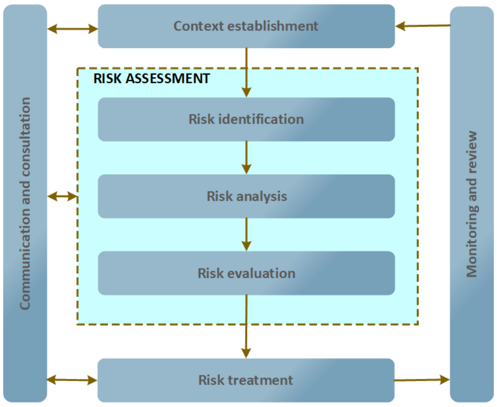

Figure 1. Risk management process.

[1] A threat is the potential cause of an unwanted incident, which may result in harm to a system or organization [12].
[2] A vulnerability is a weakness of an asset or control that can be exploited by one or more threats [12].
[3] Impact or consequence is the outcome of an event affecting objectives [12]

In this paper, we focus on the risk assessment and the risk treatment sub-processes. Risk assessment methods are quantitative, qualitative, or semi-quantitative. Quantitative risk assessment is based on using mathematical methods and rules and assigns a numerical value, often in the [1-x] range to each risk. The results are less subjective than those of the other two types, and therefore drive the process of control selection more effectively, but they cannot be easily communicated to non-technically oriented decision-makers. In contrast, qualitative risk assessment is based on applying non-numerical methods and assigns a level value to each risk, such as low, medium, and high. This type of assessment has a limited number of results, but these are more comprehensible to decision-makers. Finally, semi-quantitative risk assessment combines rules and methods for evaluating the risk by combining numeric values and levels; for example, the [1-x] range can easily be converted into qualitative expressions that help risk communication to decision-makers.

STRIDE and DREAD have been selected for the work described herein. These methods can effectively analyze highly interconnected CPSs comprising heterogeneous components [14], and they are most appropriate for analyzing systems under development. In such systems, the operational and functional requirements are not established yet. Alternative approaches need such requirements to produce valid results. In contrast, STRIDE and DREAD facilitate the analysis of conceptual systems by answering questions regarding the security objectives of the targeted ecosystem. Moreover, the combination of qualitative and quantitative methods to analyze the cyber risk provides a holistic view, not captured by other methods. Further, this hybrid approach facilitates the communication of the results to relevant stakeholders while allowing the representation of cyber risk in numeric form, thus facilitating the assessment of the effectiveness of controls at later stages of the risk treatment process. Finally, both STRIDE and DREAD are being widely used in both academia and industry [15].

Risk treatment is the process followed to modify risk [11]. A risk can be treated by :

- *modifying* its level, by introducing controls;
- *retaining* it, with no further action taken;
- *avoiding* it, by avoiding the activity or condition that gives rise to the particular risk;
- *sharing* it with other party or parties, for example, by means of insurance and/or risk financing.

The four options for risk treatment are not mutually exclusive. Sometimes a combination of options, such as modifying risks and sharing or retaining any residual risks, can be beneficial.

Individual elements of the cyber risk of, as well as *attacks*[4] against individual CPSs in the C-ES, have been studied, and proposals for risk assessment approaches have appeared in the literature. However, to the best of our knowledge, a holistic assessment of the cyber risks of the whole CPS part of the C-ES ecosystem, comprising all of the aforementioned types of risk assessment methods, which leads to concrete proposals for cyber security controls and can also be used by non-technical decision-makers, has not been made available.

In this paper:

- we extend our previous work in Reference [2] on qualitative risk assessment of CPSs on board the C-ES to all CPSs identified in Reference [16];
- we provide a quantitative risk assessment for all C-ES CPSs identified in Reference [16];
- we propose an approach for systematically selecting appropriate cyber security controls to mitigate the cyber risks; and
- we demonstrate the workings of the approach by applying it to select cyber security controls for the most vulnerable CPSs on board the C-ES.

The remainder of the paper is structured as follows: In Section 2, we review the relevant literature. In Section 3, we use the STRIDE method [17] as modified in Reference [2] to analyze the threats and the

[4] An attack is an attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an asset [12]. An attack is a particular way of a threat to exploit one or more vulnerabilities.

attack scenarios for the CPSs of the C-ES that have been identified in Reference [16] and to qualitatively assess the related risks. In Section 4, we turn our attention to quantitatively assessing the risks, by leveraging a variant of the DREAD method [18] adapted for use in CPSs. Our proposed approach for systematically selecting cyber security controls is presented in Section 5, where also its workings are demonstrated by means of applying it to select controls for the three most vulnerable on-board CPSs of the C-ES. Finally, Section 6 summarizes our conclusions and indicates directions for future research.

2. Related Work

A wealth of cyber risk assessment methods applicable to general purpose IT systems exists. Whilst these can be and have been applied to IT systems in the maritime domain, they cannot accurately assess cyber risks related to CPSs [19]. Cyber risk assessment methods for CPSs more often than not are domain specific, as they need to take into account safety as an impact factor additional to the "traditional" impact factors of confidentiality, integrity, and availability [3]. In the maritime domain, a review of cyber security risk assessment methods appeared in Reference [20]. Rødseth et al. in Reference [21] proposed a risk assessment method for the unmanned merchant ship. Although the method aims to identify both safety and security risks, particular focus is given on hazard identification and to the accordant risks, with cyber security left largely unaddressed. Tam et al. in Reference [4] proposed the MaCRA model-based framework for maritime cyber-risk assessment and applied it to a number of example scenarios [22]. However, the aim of MaCRA is not to assess the risks or flaws of specific systems, but rather to facilitate the understanding of cyber risks in the maritime domain. B. Svilicic et al. in Reference [23] proposed a framework for assessing cyber risks in ships and applied it to the case of the Electronic Chart Display and Information System (ECDIS).

Several works in the literature have analyzed security threats and risks for specific systems used in specific types of autonomous and remotely controlled vessels. Among these, Bolbot et al. in Reference [24] identified and analyzed safety related cyber-attacks in an autonomous inland ferry; their analysis covers safety aspects regarding the navigational and propulsion system of the ferry. Silverajan et al. in Reference [25] explored security issues and cyber attacks targeting systems of smart ships. Awan et al. in Reference [26] have analyzed 59 documented accidents to better understand the vulnerabilities of Integrated Bridge System (IBS) components. Svilicic et al. in Reference [27] present a study on the cyber security resilience of a shipboard Integrated Navigational System (INS) installed on a RoPax ship engaged in international trade. Wang et al. in Reference [28] propose a secure relative integrated navigation method to counteract injected fault measurement attacks. Balduzzi et al. in Reference [29] presented a security evaluation of the Automatic Identification System (AIS), by introducing threats affecting both the implementation in online providers and the protocol specification. Lund et al. in Reference [30] described a proof-of-concept attack on an INS and its integrated ECDIS, and demonstrated the attack on a vessel. Kavallieratos et al. in Reference [2] identified potential cyber attack scenarios and qualitatively evaluated the accordant risks for a number of CPSs of the C-ES ecosystem, both on-board and in the SCC.

Systematic methods for selecting security controls for IT systems either view the problem of control selection as an investment problem and apply management tools and financial analysis to optimize the selection [31], or in the context of responding to an intrusion, i.e., when a specific attack has been already detected as taking place [32]. A combinatorial optimization model to efficiently select security controls was proposed in Reference [31]. However, security control selection is still largely performed empirically, particularly for CPSs. In the maritime domain, potential cyber security controls for systems on board autonomous and remote controlled vessels have also been proposed. Bothur et al. in Reference [33] discussed the security vulnerabilities that smart ships face, and described security countermeasures, particularly procedural and technical solutions, by following a defense in depth approach. Silverajan et al. in Reference [25] analyzed the main systems of an unmanned smart ship and proposed defense strategies against previously discussed cyber attacks and threats. Bolbot et al. in Reference [24] analyzed safety-related cyber attacks for the navigational and propulsion systems, evaluated the accordant risks and proposed general security recommendations. Sahay et al. in Reference [34] proposed an SDN framework to mitigate cyber attacks and improve the resilience in the smart ship's communication network. None of the above works followed a systematic, risk-based process for selecting the controls. Further, the aforementioned analyses focused on defense strategies and controls that are not system-specific.

3. Qualitative Risk Assessment

3.1. STRIDE

STRIDE is an acronym formed by the initials of six security threats: *S*poofing, *T*ampering, *R*epudiation, *I*nformation disclosure, *D*enial of Service, and *E*levation of privileges. Spoofing is the capability of an adversary to pretend that they are someone or something else. Tampering is the alteration or disruption of aasset of the system, e.g., disk, network, or memory. Repudiation is someone's allegation that they did not do something which influences the system's operation or were not responsible for the results of their actions. Information disclosure reveals confidential information to unauthorized entities. Denial of Service reduces the availability of the system by, e.g., exhausting system resources. Elevation of Privilege is an adversary's ability to assume privileges that allow them to execute unauthorized actions.

The method was developed by Loren Kohnfelder and Praerit Garg in 1999 and is described in detail by A. Shostack in Reference [17]. Security threats are analyzed and attack scenarios are developed in light of the security objectives of *Authenticity, Integrity, Non-repudiation, Confidentiality, Availability, and Authorization*. STRIDE can be used to discover potential threats and vulnerabilities as early as the design phase. Therefore, it enables the analysis of systems that are under development, thus facilitating the requirements engineering elimination process and adherence to security-by-design principles [35]. STRIDE has been used in ecosystem environments similar to the C-ES, where CPSs are prominent [14,36,37].

3.2. STRIDE for the CPSs of the C-ES Ecosystem

STRIDE is a threat modeling method. In our previous work [2] we proposed a modified version of STRIDE and used it to model threats, to develop cyber attack scenarios, and to qualitatively assess the accordant risks for fourteen CPSs of the C-ES ecosystem, namely the Engine Automation System (EAS), the Bridge Automation System (BAS), the Shore Control Center (SCC), the Autonomous Engine Monitoring and Control System (AEMC), the Engine Efficiency System (EES), the Maintenance Interaction System (MIS), the Navigation Systems (NavS), the Autonomous Ship Controller (ASC), the Human-Machine Interface (HMI), the Remote Maneuvering Support System (RMSS), the Emergency Handling system (EmH), the Automatic Identification System (AIS), the Electronic Chart Display and Information System (ECDIS), and the Global Maritime Distress and Safety System (GMDSS). A reference architecture for the C-ES was proposed in Reference [16], in which five CPSs additional to those in the architecture proposed in Reference [2] were identified, namely the Collision Avoidance (C.A.), Radar, CCTV, Advanced Sensor Module (ASM), and Auto Pilot (AP) systems.

The results of the application of the modified STRIDE of Reference [2] to these systems, as well as to the Voyage Data Recorder (VDR), Cargo Management, and Engine Data Logger (EDL) systems that, due to space limitations, were not reported in Reference [2] are presented in Tables A1–A8 in the Appendix A. In these tables "I" stands for "Impact", "L" stands for "Likelihood" and "R" stands for "Risk". Three distinct values have been assigned to the impact and the risk: Low (L), Medium (M), and High (H). The possible values for the likelihood of a cyber attack are: Very Likely (VL), Moderate (M), and Rare (R). These values have been assigned by applying the criteria that are described in Tables 1 and 2, and in Figure 2 of Reference [2], and are summarized in Table 1. The values have been determined by both consulting the literature and by leveraging the authors' own expertise.

Table 1. Impact and likelihood criteria.

Impact Criteria	
High	Significant financial damage to the shipping company; or physical damage to the infrastructure; or loss of human life.
Medium	Financial damage to the shipping company; or disruption of operations; or legal sanctions; or breach of the confidentiality, integrity or availability of information.
Low	Delay of non-critical operations; or breach of the confidentiality, integrity or availability of non-sensitive information.
Likelihood Criteria	
Very Likely	Existence of highly motivated and capable attackers and no controls in place; or wide availability of exploits; or high exposure of the system to the internet.
Moderate	Existence of highly motivated and capable attackers and inadequate controls in place; or wide availability of exploits that require physical access; indirect exposure of the system to the internet.
Rare	Absence of highly motivated and capable attackers; or adequate controls in place; no exposure of the system to the internet.

4. Quantitative Risk Assessment

4.1. DREAD

DREAD [18] stands for *D*amage, *R*eproducibility, *E*xploitability, *A*ffected users/systems, and *D*iscoverability. *Damage* represents the damage that a cyber attack may inflict to the system; along with the *Affected Users/Systems*, it represents the *Impact* of the attack. *Reproducibility* represents the ability of the attacker to reproduce the attack, whilst *Exploitability* their ability to exploit the system's vulnerabilities and to carry out the attack. *Discoverability* represents the capacity of the adversary to identify system's vulnerabilities. The sum of Reproducibility, Exploitability, and Discoverability represents the *Likelihood* of the cyber attack.

STRIDE and DREAD are interrelated and provide a systematic analysis of novel systems to ensure the security of such systems early in the design phase. The former facilitates the qualitative security analysis of the system by considering six security threats that violate the corresponding security objectives. The latter quantifies the identified risks that result by the attack scenarios developed with STRIDE.

4.2. DREAD for the CPSs of the C-ES Ecosystem

Quantitative risk analysis aims to assign meaningful numbers to elements of risk analysis; impact and likelihood are such elements. Assessing the cyber risk by considering the probability of an attack occurring results in rating numbers and values that can cause confusion and disagreement among stakeholders in the risk management process [18]. DREAD aims to overcome such limitations by quantifying specific aspects (Damage potential, Reproducibility, Exploitability, Affected systems, and Discoverability) of security threats and attacks to assign meaningful numbers to the elements of risk by means of Formulas (1) and (2).

Building upon the analysis of the security threats and the corresponding attack scenarios for the CPSs of the C-ES as reported in Reference [2] and in Section 3.2 above, DREAD is used to produce quantitative estimates of the risks of the identified attack scenarios. The risk value is calculated by using the following formulas:

$$Impact = \frac{\sum(Damage, Affectedsystems)}{2}, \tag{1}$$

$$Likelihood = \frac{\sum(Reproducibility, Exploitability, Discoverability)}{3}, \tag{2}$$

$$Risk = \frac{(Impact + Likelihood)}{2}. \tag{3}$$

The values for the DREAD components are determined according to the criteria shown in Table 2, which have been adapted from Reference [18] so as to include CPSs aspects. These criteria are analyzed in Reference [38].

Table 2. DREAD (*D*amage, *R*eproducibility, *E*xploitability, *A*ffected users/systems, and *D*iscoverability) criteria [38].

	High (3)	**Medium (2)**	**Low (1)**
D	The adversary is able to bypass security mechanisms; get administrator access; upload/modify the CPS content.	Leakage of confidential information of the CPSs (functions/source code); cause partial malfunction/disruption of the system.	Leaking non-sensitive information; the attack is not possible to extend to the other CPSs on-board.
R	The cyber-attack can be reproduced anytime to the targeted CPS.	The adversary is able to reproduce the attack but under specific risk conditions.	Although the attacker knows the CPS's vulnerabilities/faults, s/he is unable to perform the cyber-attack.
E	The cyber-attack can be performed by a novice adversary in a short time.	A skilled adversary may launch the attack.	The attack requires an extremely skilled person and in-depth knowledge of the targeted CPS.
A	All CPSs are affected	Partial users/systems, non-default configuration	The attack affects only the targeted CPS.
D	The CPS's vulnerabilities are well known and the attacker is able to get access to the relevant information to exploit them.	The CPS's vulnerabilities/faults are not well known and the adversary needs to get access to the CPS.	The threat has been identified and the vulnerabilities have been patched.

Tables 3 and 4 depict the resulting risk value of each CPS for each STRIDE threat, calculated according to the Formulas (1)–(3), and by both consulting the literature, and by leveraging the authors' own expertise.

Table 3. Cyber risks in engine and Shore Control Center (SCC) Cyber Physical Systems (CPSs).

	EAS	**AEMC**	**EDL**	**ASM**	**EES**	**MIS**	**SCC**	**RMSS**	**HMI**
S	1.33	1.75	1.5	2.25	2	1.5	2.05	1.75	2.16
T	1.67	1.5	1.25	1.28	1.75	2.25	1.67	1.5	2.16
R	1.25	1.25	1.25	1.25	1	1.25	1.42	1.25	1.25
I	1.42	1	1.25	1.66	1.25	1.5	1.42	1.75	2
D	2	1.5	1.25	2	1.75	1.75	2.05	1.75	2.16
E	1.26	1.25	1.25	1.25	1.5	1.5	1.25	1.5	1.5

Table 4. Cyber-risks in bridge CPSs.

	BAS	**AIS**	**ECDIS**	**GMDSS**	**ASC**	**ANS**	**EmH**	**C.A.**	**Radar**	**VDR**	**Cargo**	**CCTV**	**AP**
S	1.83	2.33	2.42	2.25	2.17	1.92	1.25	1.91	2.25	1.5	1.5	2.16	1.5
T	1.67	2.42	2.17	2.5	2.5	1.92	1.25	2.08	2.08	1.5	1.5	1.83	1.75
R	1.25	2.33	1.25	1.5	1.75	1.5	1	1.25	1.66	1.25	1.5	1.5	1.25
I	1.83	2.33	2.33	2.25	1.75	1.75	1.25	1.41	1	1.5	1.75	1.91	1.5
D	2	2	2.5	2.5	2.58	1.92	1.5	1.91	2	1.5	1.25	1.91	1.75
E	1.25	1.92	2.33	2.17	2	2.17	1	1.25	1.5	1.5	1.5	1.75	1.5

4.3. Discussion

As already mentioned in the introduction, a semi-quantitative risk assessment facilitates the communication of risks to non-technical decision-makers. In this case, expressing the results of the quantitative risk assessment in Section 4.2 will also allow comparisons to be made between these and those of the qualitative risk assessment in Section 3.2. To this end, the risk values in Tables 3 and 4 can be converted to qualitative risk levels as follows:

Low: DREAD risk ≤ 1
Medium: $1 <$ DREAD risk ≤ 2
High: $2 <$ DREAD risk ≤ 3

Table 3 suggests that Spoofing and Denial of Service are the most critical threats both among the engine room and the SCC systems. Similarly, Table 4 suggests that the Spoofing, Tampering, and Denial of Service threats present the highest risk levels among the bridge systems of the C-ES. Tampering and Information disclosure are medium risk threats, and Repudiation and Elevation of privileges are low risk threats.

Moreover, a single risk value for each examined system can be assigned, equal to the largest among the risk values for the same system. Table 5 depicts these numerical values, as well as the results of the quantitative risk assessment converted to qualitative according to the rules above and those of the qualitative risk assessment.

Table 5. Quantitative versus qualitative risks.

CPS	DREAD	Quantitative Risk Analysis	Qualitative Risk Analysis
ECDIS	2.5	High	High
GMDSS	2.5	High	High
ASC	2.5	High	High
AIS	2.42	High	High
MIS	2.25	High	Medium
ASM	2.25	High	Medium
Radar	2.25	High	Medium
ANS	2.17	High	High
HMI	2.16	High	High
CCTV	2.16	High	Medium
C.A.	2.08	High	Medium
SCC	2.05	High	Medium
EES	2	Medium	Medium
BAS	2	Medium	Medium
EAS	2	Medium	Medium
RMSS	1.75	Medium	Medium
AEMC	1.75	Medium	Medium
CaMa	1.75	Medium	Medium
EmH	1.5	Medium	Medium
VDR	1.5	Medium	Medium
EDL	1.5	Medium	Medium
AP	1.75	Medium	Medium

It can be noticed that none of the studied CPSs faces low risk, and that the risk levels determined by the qualitative and the quantitative risk assessment methods for most of these systems are similar; deviations should be attributed to the increased subjectivity of the qualitative risk assessment. Despite the deviations, both approaches suggest that the navigational systems are among the most vulnerable on-board CPSs of the C-ES.

In previous work [16], we analyzed the interconnections and interdependencies among the CPSs of the C-ES. By leveraging these results along with the quantitative risks depicted in Tables 3 and 4, the propagation of risks among the CPSs can be examined. Note, for example, which the AIS is interconnected and interdependent with the ECDIS, the Radar, and the ASM, systems that also face the highest risk values. This is because systems which are interconnected and interdependent share similar security risks, because they inherit the vulnerabilities of the most vulnerable CPSs which can be used as intermediate stepping stones for launching attacks [38].

5. Cyber Risk Treatment

The ISO27005 risk management approach aims at identifying risk treatment strategies rather than designing the security architecture of the system under study. A necessary prerequisite for designing such an architecture for the C-ES is to select appropriate controls for each individual component, and to consolidate these into a coherent and consistent whole that will take into account not only the risks, but also the requirements stemming from the C-ES's environment. Accordingly, we propose an approach for managing the risks of the C-ES, as depicted in Figure 2, where six sub-processes are specified, along with their inputs and outputs. The Environmental Analysis sub-process for the C-ES has been carried out in Reference [16]; the Threat Analysis sub-process has been carried out in Reference [2]; and the Security Requirements Elicitation sub-process has been carried out in Reference [39]. In this work we focus on the Cyber Risk Assessment sub-process (Sections 3 and 4) and on the Control Selection sub-process (Section 5.1). The Security Architecture Design sub-process is the subject of future work.

5.1. Control Selection

This activity includes the initial selection of a set of minimum security controls to protect the system based on a set of criteria that take into account the security requirements; the cyber risks; the possible attacks; and the possibly already existing controls. This set will ensure baseline protection of the system; the baseline controls are the starting point for the design of the overall security architecture, which will derive from the application of tailoring to the set of security control baselines to account for peculiarities of the system and of the organization that owns or operates the system. In the sequel our approach for selecting the set of baseline controls is described.

A number of sources (e.g., Reference [40–42]) provide sets of security controls from which a selection can be made. All of these sources pertain to information systems rather than cyber-physical systems; hence their applicability in the case under study is limited. However, Appendix G of the NISTGuide to Industrial Control Systems (ICS) Security [43] provides the *ICS overlay*, which is a partial tailoring of the controls and control baselines in Reference [41,42], which adds supplementary guidance specific to ICS. We will be using this source to select controls from, according to the following set of criteria, adapted from Reference [44]:

C1: Kind of CPS that needs to be protected;
C2: Security aspects that need to be protected.
C3: Threats that need to be eliminated.
C4: Potential control alternatives.
C5: The value of the CPS to protect, according to its importance. This has been assessed within the process of attack path analysis, performed in Reference [38].
C6: The likelihood of threat occurrence. This derives from the threat analysis performed within the risk assessment process of Sections 3 and 4.
C7: Risk coverage provided by alternative controls.

As an example, the values of the control selection criteria for the spoofing threat against AIS are as follows:

C1: Navigational CPS;
C2: Integrity and availability. These are derived from the security requirements that have been established in Reference [39].
C3: Spoofing/Tampering/DoS. These derive from the threat analysis results performed in Reference [2] and in Sections 3 and 4.
C4: Encryption/Tamperproof hardware.
C5: High. This has been assessed within the process of attack path analysis, performed in Reference [38].
C6: Very likely. This derives from the threat analysis performed within the risk assessment process of Sections 3 and 4.
C7: Low. No alternative controls are already in place.

and lead to selecting the IA-3 control category of Reference [43]. An example of a control that belongs to this category is the establishment and use of an authentication infrastructure for such devices, such as, e.g., the one proposed in Reference [45,46].

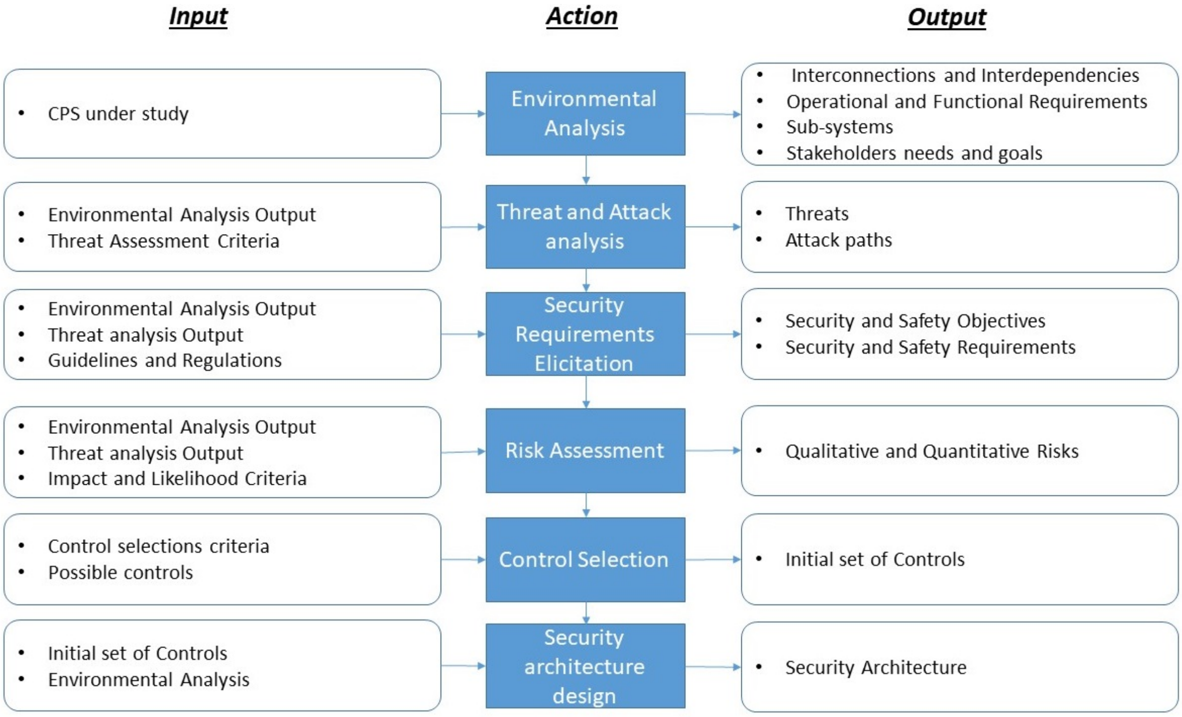
Input
Action
Output
CPS under study
Environmental Analysis
Interconnections and Interdependencies
Operational and Functional Requirements
Sub-systems
Stakeholders needs and goals
Environmental Analysis Output
Threat Assessment Criteria
Threat and Attack analysis
Threats
Attack paths
Environmental Analysis Output
Threat analysis Output
Guidelines and Regulations
Security Requirements Elicitation
Security and Safety Objectives
Security and Safety Requirements
Environmental Analysis Output
Threat analysis Output
Impact and Likelihood Criteria
Risk Assessment
Qualitative and Quantitative Risks
Control selections criteria
Possible controls
Control Selection
Initial set of Controls
Initial set of Controls
Environmental Analysis
Security architecture design
Security Architecture

Figure 2. Overall control selection approach.

5.2. Application to the Case of the AIS, the ECDIS, and the GMDSS

The results of the application of the process described above to the three most vulnerable on-board systems of the C-ES are shown in Tables 6–8.

Table 6. Control selection for the Automatic Identification System (AIS).

Threat	Risk	Requirement	Objective	Control Category
Spoofing	Medium	Reliable authentication mechanisms must be in place in order to uniquely identify the actors that read, modify, or transmit AIS data, as well as to authenticate the system itself and its services.	Authentication	Device Identification and Authentication (IA-3)
Tampering	High	The confidentiality and integrity of the data exchanged between internal (on board) systems and external actors (SCC or other vessel) should be ensured by appropriate mechanisms depending on the actors and the type of the data in transit.	Confidentiality/ Integrity	Port and I/O Device Access (SC-41), Software Firmware and Information Integrity (SI-7)
Repudiation	High	The AIS should implement the security services in order to protect the system from loss of control or possession of information.	Possession and Control, Non-repudiation	Device Identification and Authentication (IA-3), Physical Access Control (PE-3), Monitoring Physical Access (PE-6 (1)), Account Management (AC-2 (2),(3)), Non-repudiation (AU-10), Information System Component Inventory (CM-8 (4))
Information Disclosure	High	Voyage data, such as destination port or cargo related information, should be confidential to prevent potential leakage to adversaries.	Confidentiality, Integrity	Cryptographic Key Establishment and Management (SC-12 (1)), Cryptographic Protection (SC-13)
Denial of Service	Medium	The connectivity between system and external actors and between on board systems must be continuous.	Availability, Utility	Internal System Connections (CA-9), Information System Backup (CP-9 (1), (2), (3), (5)), Power Equipment and Cabling (PE-9), Denial of Service Protection (SC-5)
Elevation of Privileges	High	The AIS must be able to implement lock mechanisms (e.g., lock HMI screen) upon request by the administrator or after a configurable time of idleness.	Authenticity, Non- repudiation	Internal System Connections (CA-9), Monitoring Physical Access (PE-6)

Table 7. Control selection for the Electronic Chart Display and Information System (ECDIS).

Threat	Risk	Requirement	Objective	Control Category
Spoofing	High	The use of ECDIS must be restricted only to authorized and well trained personnel.	Authenticity, Integrity	Device Identification and Authentication (IA-3), Port and I/O Device Access (SC-41), Time Stamps (AU-8), Plan of Action and Milestones (CA-5)
Tampering	Medium	The ECDIS must be able to control the flows of voyage-related data sent to other ships and to the SCC.	Integrity, Authenticity	Device Identification and Authentication (IA-3), Audit Review Analysis and Reporting (AU-6 (3), (6)), Plan of Action and Milestones (CA-5)
Repudiation	Medium	The ECDIS should be able to audit sent and received data to external actors.	Integrity, Non repudiation	Internal System Connections (CA-9), Time Stamps (AU-8), Physical Access Control (PE-3), Monitoring Physical Access (PE-6 (1))
Information Disclosure	High	The confidentiality and integrity of the data exchanged between internal (on board systems and external actors (SCC or other vessel) should be ensured by appropriate mechanisms depending on the actors and the type of the data in transit.	Confidentiality	Cryptographic Protection (SC-13), Port and I/O Device Access (SC-41), Device Identification and Authentication (IA-3), Protection of Information at Rest (SC-28)
Denial of Service	High	The communication between the ECDIS and the satellite system should be continuously available.	Availability	Internal System Connections (CA-9), Incident Handling (IR-4 (4)), Denial of Service Protection (SC-5)
Elevation of Privileges	Low	The use of ECDIS must be restricted only to authorized and well trained personnel	Possession and Control	Device Identification and Authentication (IA-3), Unsuccessful Logon Attempts (AC-7)

Table 8. Control selection for the the Global Maritime Distress and Safety System (GMDSS).

Threat	Risk	Requirement	Objective	Control Category
Spoofing	High	Distress signals transmitted through the GMDSS must be verified by external actors, such as SCC and other ship's subsystems, such as the Autonomous Engine Monitoring and Control (AEMC) and Navigation systems	Confidentiality, Authenticity	Continuous Monitoring (CA-7 (1)), Time Stamps (AU-8)
Tampering	High	The signals transmitted to external actors or subsystems must be appropriately encrypted	Integrity	Cryptographic Protection (SC-13)

Table 8. *Cont.*

Threat	Risk	Requirement	Objective	Control Category
Repudiation	Medium	The authenticity of the transmitted GMDSS signals and data in transit to the Autonomous Ship Controller (ASC), to other subsystems, and to the SCC must be ensured	Authenticity, Non repudiation	Physical Access Control (PE-3), Access Control for Output Devices (PE-5), Unsuccessful Log on Attempts (AC-7)
Information Disclosure	High	The measures to protect the confidentiality and integrity of data should not downgrade their utility	Confidentiality	Continuous Monitoring (CA-7(1))
Denial of Service	Medium	Safety signals transmitted through the GMDSS to other on board systems and external actors must be continuously available.	Availability	Internal System Connections (CA-9), Incident Handling (IR-4 (4)), Contingency Plan (CP-2), Denial of Service Protection (SC-5)
Elevation of privileges	Medium	The ASC must be able to provide security, safety, and dynamic data to the GMDSS, when needed	Authenticity, Possession and Control	Device Identification and Authentication (IA-3)

Table 9 depicts the consolidated controls per studied CPS.

Table 9. Baseline controls.

CPS	Baseline Controls
AIS	Device Identification and Authentication (IA-3), Port and I/O Device Access (SC-41), Software Firmware and Information Integrity (SI-7 (1)), Cryptographic Protection (SC-13), Tamper Protection (PE-3(5)), Physical Access Control (PE-3), Monitoring Physical Access (PE-6 (1)), Account Management (AC-2 (2),(3)), Non-repudiation (AU-10), Information System Component Inventory (CM-8 (4)), Cryptographic Key Establishment and Management (SC-12 (1)), Internal System Connections (CA-9), Information System Backup (CP-9 (1), (2), (3), (5)), Power Equipment and Cabling (PE-9), Denial of Service Protection (SC-5)
ECDIS	Device Identification and Authentication (IA-3), Port and I/O Device Access (SC-41), Time Stamps (AU-8), Plan of Action and Milestones (CA-5), Audit Review Analysis and Reporting (AU-6 (3), (6)), Internal System Connections (CA-9), Physical Access Control (PE-3), Monitoring Physical Access (PE-6 (1)), Cryptographic Protection (SC-13), Protection of Information at Rest (SC-28), Incident Handling (IR-4 (4)), Denial of Service Protection (SC-5), Unsuccessful Logon Attempts (AC-7)
GMDSS	Continuous Monitoring (CA-7 (1)), Time Stamps (AU-8), Cryptographic Protection (SC-13), Physical Access Control (PE-3), Access Control for Output Devices (PE-5), Unsuccessful Log on Attempts (AC-7) , Internal System Connections (CA-9), Incident Handling (IR-4 (4)), Contingency Plan (CP-2), Denial of Service Protection (SC-5), Device Identification and Authentication (IA-3).

Some of these controls are recommended for all systems (Device Identification and Authentication (IA-3), Cryptographic Protection (SC-13), Denial of Service Protection (SC-5), Physical Access Control (PE-3), Internal System Connections (CA-9)), whilst others are recommended for two or for only one of the studied systems. During the security architecture design phase, the controls identified for all systems will need to be re-considered, consolidated, checked for applicability in the specific environment, conformance to guidelines, compliance to standards etc.

As is typical with risk treatment strategies, the application of security controls does modify (reduce) the risk but does not eradicate it. To complete the risk treatment process one needs to assess the effectiveness of the applied controls, to consider the residual risk within the specific environmental and organizational context and to possibly repeat the process until the residual risk falls below the accepted risk level. This process can be effectively performed when the whole security architecture of the C-ES has been determined; accordingly, this is an item for future work.

One of the distinctive characteristics of CPSs is their ability to interconnect dynamically, sometimes to address scope beyond the originally intended one. This often results in emergent, hence unpredictable, behavior. In order to effectively secure CPSs in such situations, dynamic assessment of cyber risk is recommended. The proposed methodology, as it now stands, cannot capture such behavior. However, it can be extended, along the lines followed in Reference [36].

6. Conclusions

We systematically analyzed the cyber security risks of the CPSs of the C-ES. Both a qualitative and a quantitative assessment of these risks was undertaken, by using the STRIDE and DREAD methods respectively. By leveraging the results of both assessments and applying a systematic structured approach, we identified appropriate baseline cyber security controls for each of the three more vulnerable on-board CPSs. As future work, we intend to build on these results to design the security architecture of instances of the C-ES.

Author Contributions: Conceptualization, G.K. and S.K.; methodology, G.K.; investigation, G.K.; writing—original draft preparation, G.K.; writing—review and editing, S.K. and G.K.; supervision, S.K.; project administration, S.K.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

Appendix A. STRIDE Tables

Table A1. Collision Avoidance—C.A.

T	Collision Avoidance—C.A.	I	L	R
S	An adversary may spoof the existence of another ship in the vicinity, thereby causing the vessel to change its route.	H	M	H
T	Tampering of sensor data may cause the vessel to collide with other ships/human made obstacles/environmental obstacles.	H	M	H
R	The repudiation of actions of the collision avoidance system is unacceptable since all such actions are clearly defined and assigned to the necessary equipment.	M	R	L
I	The leakage of information exchanged via the collision avoidance system may reveal information regarding the position of the vessel and its voyage.	L	M	M
D	A disruption of the operation of the collision avoidance system may cause physical damage.	H	M	H
E	An adversary with high privileges may disrupt the normal operation of the system.	H	R	M

Table A2. Radar.

T	Radar	I	L	R
S	An attacker may spoof the identity of a ship in the vicinity and confuse the ANS to deviate from the intended route.	M	VL	H
T	An attacker may violate the integrity of the dynamic data of the Radar (positioning data) and cause physical damage to the vessel.	M	M	M
R	The dynamic data sent by the Radar can be spoofed, rendering other systems unable to identify the source of the data.	M	R	L
I	No confidential or sensitive data are transmitted through Radar.	L	R	L
D	A signal jamming of the Radar may cause disruption on the services and confusion to the other systems regarding the position and the speed of the vessel.	M	VL	H
E	An attacker with high administrative access is able to turn off the Radar or alter the transmitted data.	M	R	L

Table A3. CCTV.

T	CCTV	I	L	R
S	An adversary may spoff the identity of a monitoring camera in the engine room and confuse the EAS's decision-making.	M	M	M
T	An attacker is able to alter the images depicted in the monitoring system and cause damage. The integrity of the data sent from CCTV is crucial since they contribute to the situational awareness of the C-ES.	M	M	M
R	Wrong data regarding the vessel's environment could be sent to the ANS. The ANS cannot perform any integrity check or identify the malicious source of the system's data.	M	R	L
I	Potential leakage of the data exchanged between CCTV and SCC may cause GDPR violations and hence financial and legal damages to the shipping company.	H	M	H
D	Any disruption of the system's services may lead to loss of the vessel's situational awareness.	H	M	H
E	An adversary with administrative access to the system may disable the cameras on-board or the access control systems and hence violate the authenticity and availability of information within the vessel.	H	R	M

Table A4. VDR.

T	VDR	I	L	R
S	An adversary may pretend the identity of the legitimate ECDIS and store wrong/malicious data to the VDR.	H	R	M
T	By leveraging the weak encryption of the stored data, the attacker may change voyage/dynamic/static data and confuse the decision-makers.	H	M	H
R	The data are stored automatically to the VDR by a well-defined process; such a threat is not applicable.	M	R	L
I	An attacker may gain access to unauthorized data by leveraging the weak encryption of the data and the absence of an access control mechanism.	H	M	H
D	The adversary may disrupt the storage of data service by sending data for storage continuously.	M	M	M
E	Potential access to the systems as an administrator could cause damage to the stored data, such as delete, alter, or leak confidential data.	H	R	M

Table A5. Cargo management.

T	Cargo Management	I	L	R
S	An adversary may spoof the identity of the cargo or ship owner and gain access to sensitive data regarding the type of the cargo or the destination port.	H	R	M
T	Tampering of the data derived from the cargo monitoring system may cause damage to the cargo.	H	M	H
R	An attacker may confuse the cargo management process by attacking the CCTV system and sending malicious data, such as fire on the deck, pirates on-board, etc.	H	R	M
I	The violation of the data confidentiality of the cargo management system may lead to GDPR violation and cause financial damage.	H	M	H
D	An adversary may disrupt the operation of the system by attacking the communication line between ship and shore, thus making the cargo handling service unavailable.	H	M	H
E	An attacker with administrative access to the cargo management system may cause damage to the cargo (cargo loss), financial damage to the shipping company, or damage to the reputation of the shipping company.	H	R	M

Table A6. Engine Data Logger—EDL.

T	EDL	I	L	R
S	An adversary may assume the identity of the captain/system administrator by logging in with the credentials of the administrator and gain access to the engine related data.	H	M	H
T	The attacker may alter the data stored in the EDL, such as the engine performance data and cause damage to the engine or confusion during the investigation of an accident.	H	M	H
R	An adversary may log wrong data to the EDL by leveraging the lack of control actions to properly track the logged-in users.	H	R	M
I	The information and data stored in EDL are not confidential; therefore a potential leakage cannot cause significant damage to the vessel.	L	M	L
D	The disruption of the system's operation may cause physical damage to the engine room by confusing the MIS to proceed with the actions foreseen in case of engine failure.	M	R	M
E	An attacker with high administrative rights may change the system's configuration and cause violations of data integrity and/or availability.	H	R	M

Table A7. Advanced Sensor Module—ASM.

T	Advanced Sensor Module—ASM	I	L	R
S	An adversary may gain access to the ASM by deploying a malware. By leveraging the malware, the attacker is authenticated as system administrator and therefore fault messages could be sent to other on board systems, such as navigation and engine monitoring systems. This scenario may cause damage to the ship and/or financial damage to the company.	H	M	H
T	An attacker may tamper the engine sensor data transmitted to ANS and provide fake measurements (e.g., temperature, engine oil).	H	R	M
R	The repudiation of the actions of the ASM is unacceptable since its functions are based on automated and well-defined process. Potential violation of the repudiation of the system may cause confusion in the decision-making process.	H	R	M
I	Potential data leakage of the ASM or potential disclosure of the sensor architecture facilitates the reconnaissance stage of a cyber-attack.	M	M	M
D	An adversary may flood the systems with fake data, thus affecting its ability to share the valid data with the engine and navigational systems. The disruption of the system's operation may cause significant damage to the vessel and/or financial damage to the shipping company since the vessel's situational awareness capability will be adversely affected.	H	M	H
E	Due to the weak access control in the ASM, an adversary may gain system access with high administrative rights and disrupt the ASM operation and/or services.	H	R	M

Table A8. Auto Pilot—AP.

T	Auto Pilot—AP	I	L	R
S	An attacker may spoof the identity of the Shore Control Center and provide wrong position coordinates to the AP.	M	M	M
T	The alteration of the AP data may lead to the grounding of the vessel and cause financial and physical damage.	H	R	M
R	If the source of the received data is spoofed, the AP will not be able to identify the system that sent the wrong data.	H	R	M
I	An adversary may gain access to information related to the vessel's position or the destination port. Financial damage may result due to the leakage of confidential information.	M	R	L
D	The attacker may send fake data continuously to the AP and hence disable its normal operation.	H	M	H
E	An attacker with administrative rights is able to change the vessel's route and cause financial damage.	H	R	M

References

1. Cross, J.; Meadow, G. Autonomous ships 101. *J. Ocean Technol.* **2017**, *12*, 23–27.
2. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Cyber-attacks against the autonomous ship. In *Proceedings of the SECPRE 2018, CyberICPS 2018. Lecture Notes in Computer Science, Vol 11387*; Springer Nature: Basel, Switzerland, 2018; pp. 20–36.
3. BIMCO and CLIA and ICS and INTERCARGO and INTERMANAGER and INTERTANKO and IUMI and OCIMF and WORLD SHIPPING COUNCIL. In *The Guidelines on Cyber Security Onboard Ships*; Technical Report; BIMCO: Bagsværd, Denmark, 2018.
4. Tam, K.; Jones, K. Cyber-risk assessment for autonomous ships. In Proceedings of the International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2018; pp. 1–8.
5. USCG. Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels. Available online: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf (accessed on 2 September 2020).
6. Jones, M. Spoofing in the Black Sea: What Really Happened? Available online: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/ (accessed on 2 September 2020).
7. MARAD. 2019-012-Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea-Threats to Commercial Vessels by Iran and Its Proxies. Available online: https://www.maritime.dot.gov/content/2019-012-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea-threats-commercial-vessels (accessed on 2 September 2020).
8. Cyber Attacks on Maritime OT Systems Increased 900% in Last Three Years. 2020. Available online: https://safety4sea.com/cyber-attacks-on-maritime-ot-systems-increased-900-in-last-three-years/#:~:text=Cyber%2Dattacks%20on%20the%20maritime,security%20firm%20Naval%20Dome%20reveals (accessed on 29 August 2020).
9. Kessler, G.; Craiger, J.; Haass, J. A Taxonomy Framework for Maritime Cyber Security: A Demonstration Using the Automatic Identification System. *Transnav Int. J. Mar. Navig. Saf. Sea Transp.* **2018**, *12*, 429. [CrossRef]
10. Katsikas, S.K. Cyber security of the autonomous ship. In Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, Abu Dhabi, UAE, 2 April 2017; pp. 55–56.
11. International Organization for Standardization, ISO. *ISO/IEC 27005:2018 Information Technology—Security Techniques—Information Security Risk Management*; ISO: Geneva, Switzerland, 2018.
12. International Organization for Standardization, ISO. *ISO/IEC 27000:2018(en) Information Technology—Security Techniques—Information Security Management Systems—Overview And Vocabulary*; ISO: Geneva, Switzerland, 2018.
13. International Organization for Standardization, ISO. *ISO 31000:2018 Risk management—Guidelines*; ISO: Geneva, Switzerland, 2018.
14. Kavallieratos, G.; Gkioulos, V.; Katsikas, S.K. Threat analysis in dynamic environments: The case of the smart home. In Proceedings of the 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; pp. 234–240.
15. Hussain, S.; Kamal, A.; Ahmad, S.; Rasool, G.; Iqbal, S. Threat modelling methodologies: A survey. *Sci. Int.* **2014**, *26*, 1607–1609.
16. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Modelling Shipping 4.0: A Reference Architecture for the Cyber-Enabled Ship. In Proceedings of the Asian Conference on Intelligent Information and Database Systems, Phuket, Thailand, 23–26 March 2020; pp. 202–217.
17. Shostack, A. *Threat Modeling: Designing for Security*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
18. Microsoft. Chapter 3—Threat Modeling. 2010. Available online: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN (accessed on 25 August 2020).
19. Ali, S.; Al Balushi, T.; Nadir, Z.; Hussain, O.K. Risk Management for CPS Security. In *Proceedings of Cyber Security for Cyber Physical Systems*; Springer International Publishing: Berlin/Heidelberg, Germany, 2018; pp. 11–34.
20. You, B.; Zhang, Y.; Cheng, L.C. Review on Cyber Security Risk Assessment and Evaluation and Their Approaches on Maritime Transportation. In Proceedings of the 30th Annual Conference of International Chinese Transportation Professionals Association, Houston, TX, USA, 19–21 May 2017.

21. Rødseth, Ø.J.; Burmeister, H.C. Risk assessment for an unmanned merchant ship. *Transnav Int. J. Mar. Navig. Saf. Sea Transp.* **2015**, *9*, 357–364. [CrossRef]
22. Tam, K.; Jones, K. MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU J. Marit. Aff.* **2019**, *18*, 129–163. [CrossRef]
23. Svilicic, B.; Kamahara, J.; Celic, J.; Bolmsten, J. Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU J. Marit. Aff.* **2019**, *18*, 509–520. [CrossRef]
24. Bolbot, V.; Theotokatos, G.; Boulougouris, E.; Vassalos, D. Safety related cyber-attacks identification and assessment for autonomous inland ships. In Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV), Aalto University, Espoo, Finland, 17–20 September 2019.
25. Silverajan, B.; Ocak, M.; Nagel, B. Cyber Security Attacks and Defences for Unmanned Smart Ships. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 15–20.
26. Awan, M.; Al Ghamdi, M. Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS). *J. Mar. Sci. Eng.* **2019**, *7*, 350. [CrossRef]
27. 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]
28. Wang, Y.; Wang, Y.; Feng, X. Ship Security Relative Integrated Navigation with Injected Fault Measurement Attack and Unknown Statistical Property Noises. *J. Mar. Sci. Eng.* **2020**, *8*, 305. [CrossRef]
29. Balduzzi, M.; Pasta, A.; Wilhoit, K. A Security Evaluation of AIS Automated Identification System. In Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC'14, Association for Computing Machinery, New York, NY, USA, 8–12 December 2014; pp. 436–445. [CrossRef]
30. Lund, M.; Hareide, O.; Jøsok, Ø. An Attack on an Integrated Navigation System. *J. Ocean Technol.* **2017**, *12*, 23–27.
31. Schilling, A.; Werners, B. Optimal selection of IT security safeguards from an existing knowledge base. *Eur. J. Oper. Res.* **2016**, *248*, 318–327. [CrossRef]
32. Nespoli, P.; Papamartzivanos, D.; Gómez Mármol, F.; Kambourakis, G. Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 1361–1396. [CrossRef]
33. Bothur, D.; Zheng, G.; Valli, C. A critical analysis of security vulnerabilities and countermeasures in a smart ship system. In Proceedings of the Australian Information Security Management Conference, Perth, Australia, 5–6 December 2017.
34. Sahay, R.; Sepulveda, D.; Meng, W.; Jensen, C.D.; Barfod, M.B. CyberShip: An SDN-based Autonomic Attack Mitigation Framework for Ship Systems. In Proceedings of the International Conference on Science of Cyber Security, Beijing, China, 14–16 August 2018; pp. 191–198.
35. Sandra Domenique Zinsmaier, H.L.; Waldvogel, M. A Practical Approach to Stakeholder-driven Determination of Security Requirements based on the GDPR and Common Criteria. In Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020), Valletta, Malta, 26 November 2020; pp. 473–480.
36. Kavallieratos, G.; Chowdhury, N.; Katsikas, S.; Gkioulos, V.; Wolthusen, S. Threat Analysis for Smart Homes. *Future Internet* **2019**, *11*, 207. [CrossRef]
37. Seifert, D.; Reza, H. A security analysis of cyber-physical systems architecture for healthcare. *Computers* **2016**, *5*, 27. [CrossRef]
38. Kavallieratos, G.; Katsikas, S. Attack Path Analysis for Cyber-Physical Systems. In Proceedings of the CyberICPS 2020, Guildford, UK, 12 July 2020.
39. Kavallieratos, G.; Diamantopoulou, V.; Katsikas, S. Shipping 4.0: Security requirements for the Cyber-Enabled Ship. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6617–6625. [CrossRef]
40. Federal Office for Information Security. *IT-Grundschutz-Catalogues*; 13th Version; Federal Office for Information Security: Bonn, Germany, 2013.
41. JOINT TASK FORCE. Security and Privacy Controls for Federal Information Systems and Organizations. *NIST Spec. Publ.* **2020**, *800*, 8–13.
42. JOINT TASK FORCE. Control Baselines for Information Systems and Organizations. *NIST Spec. Publ.* **2020**. [CrossRef]

43. Stouffer, K.; Pillitteri, V.; Marshall, A.; Hahn, A. Guide to industrial control systems (ICS) security. *NIST Spec. Publ.* **2015**, *800*, 247.
44. Government of Spain, Ministry of Finance and Public Administration. *MAGERIT—Version 3.0 Methodology for Information Systems Risk Analysis and Management*; Government of Spain, Ministry of Finance and Public Administration: Madrid, Spain, 2014; pp. 1–109.
45. Goudossis, A.; Katsikas, S.K. Towards a secure automatic identification system (AIS). *J. Mar. Sci. Technol.* **2019**, *24*, 410–423. [CrossRef]
46. Goudosis, A.; Katsikas, S. Secure AIS with Identity-Based Authentication and Encryption. *Transnav Int. J. Mar. Navig. Saf. Sea Transp.* **2020**, *14*, 287–298, doi:10.12716/1001.14.02.03. [CrossRef]