Shipping 4.0: Security Requirements for the Cyber-Enabled Ship

Georgios Kavallieratos, Vasiliki Diamantopoulou, and Sokratis K. Katsikas

***Abstract*—The cyber-enabled ship (C-ES) is either an autonomous or a remotely controlled vessel which relies on interconnected cyber physical-systems for its operations. Such systems are not well protected against cyberattacks. Considering the criticality of the functions that such systems provide, it is important to address their security challenges, thereby ensuring the ship's safe voyage. In this article, we leverage the maritime architectural framework reference architecture to analyze and describe the environment of the C-ES. We then apply the Secure Tropos methodology to systematically elicit the security requirements of the three most vulnerable cyber–physical systems (CPSs) onboard a C-ES, namely the automatic identification system (AIS), the electronic chart display information system, and the global maritime distress and safety system. The outcome is a set of cyber-security requirements for the C-ES ecosystem in general and these systems in particular.**

***Index Terms*—Autonomous ships security, cyber-physical systems, cyber-security, security requirements engineering.**

I. Introduction

INDUSTRY 4.0 was initially coined to describe the trend toward automation and data exchange in manufacturing technologies and processes; nowadays, it encompasses areas which are not normally classified as an industry, such as smart cities, for instance, and describes the trend toward increasing automation and connectivity, by leveraging technologies such as the Internet of Things (IoT), artificial intelligence (AI), and Big data analytics, regardless of domain of application, leading to the appearance of terms such as *cities 4.0*. Accordingly, the term *Shipping 4.0* was coined in 2016 to describe the new developments in digitalization of shipping, to reflect the very similar developments in land-based industry which commonly goes under the name of Industry 4.0 [1].

In the maritime sector, despite the fact that nowadays almost all ships are automated in some way, the shipping industry is coming to alignment with Industry 4.0 with the emergence of crewless vessels [2]. 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). 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 C-ES ecosystem consists of both information technology (IT) and operational technology (OT) systems which are crucial for the vessel's secure and safe operations.

The integration of IT and OT that constitutes a central element of the digital transformation process in any application domain is unavoidably accompanied by an enlargement and diversification of the cyber risks that the domain is facing, with existing risks being increased and new risks being introduced. This is mainly due to the fact that, while traditional operations were designed with no need for cyber-security in mind, modern IT-enabled operations are allowed to be accessed and controlled by information systems connected to the internet, through interfaces that are rarely adequately secure.

The shipping industry and the C-ES in particular is no exception. Although most of the C-ES cyber–physical system (CPS) systems 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 cyberattacks. Indeed, research on the cyber-security risks of autonomous and unmanned vessels [3], [4] has revealed an increased attack surface and vulnerable systems. This enlarged attack surface has already made ship-side cyber-security incidents such as, for example, the ones reported in [5]–[7] possible.

In the light of these findings, the increased financial value of the sector [8], and the multitude of potential attackers, including such with advanced capabilities, the promotion of cyber-security and safety of the C-ES ecosystem is very important [9]. In order to strengthen the cyber-security posture of the ecosystem, it is necessary to define a security architecture. Acknowledging the fact that the C-ES ecosystem is characterized by high complexity and by the complex interconnections, dependencies, and interdependencies among its constituent CPSs, it follows that a systematic approach needs to be followed when

Manuscript received February 10, 2020; accepted February 11, 2020. Date of publication February 27, 2020; date of current version June 22, 2020. Paper no. TII-20-0670. *(Corresponding author: Georgios Kavallieratos.)*

Georgios Kavallieratos is with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik 2815, Norway (e-mail: georgios.kavallieratos@ntnu.no).

Vasiliki Diamantopoulou is with the Department of Information and Communication Systems Engineering, School of Engineering, University of the Aegean, 83200 Samos, Greece (e-mail: vdiamant@aegean.gr).

Sokratis K. Katsikas is with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik 2815, Norway, and also with the Faculty of Pure and Applied Sciences, Open University of Cyprus, Nicosia 2220, Cyprus (e-mail: sokratis.katsikas@ntnu.no).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2020.2976840

attempting to establish cyber-security requirements, both of the ecosystem as a whole and of each individual CPS in the ecosystem.

In this article, we first propose a security requirements elicitation process for the C-ES ecosystem. An architectural framework needs to be combined with a security requirements elicitation method to derive such requirements. The Secure Tropos methodology [10] and the maritime architectural framework (MAF) reference architecture [11] were identified as important elements for implementing the process. According to a threat analysis of onboard systems of the C-ES [3], a risk assessment of such systems [4], and the known vulnerabilities of such systems [12], the automatic identification system (AIS), the electronic chart display information system (ECDIS), and the global maritime distress and safety system (GMDSS) have been identified as the most vulnerable onboard systems of the C-ES. We then proceed with applying the process to the case of the C-ES ecosystem, and in particular to these systems. The outcome is a set of cyber-security requirements for these systems, checked for their validity against the criteria specified in [13].

The remainder of the article is structured as follows. Section II discusses related work. Section III describes our proposed security requirements elicitation process. Section IV presents the results of the application of the process to the C-ES case, and specifically the cyber-security requirements of the three most vulnerable CPSs among the C-ES systems. Finally, Section V concludes this article.

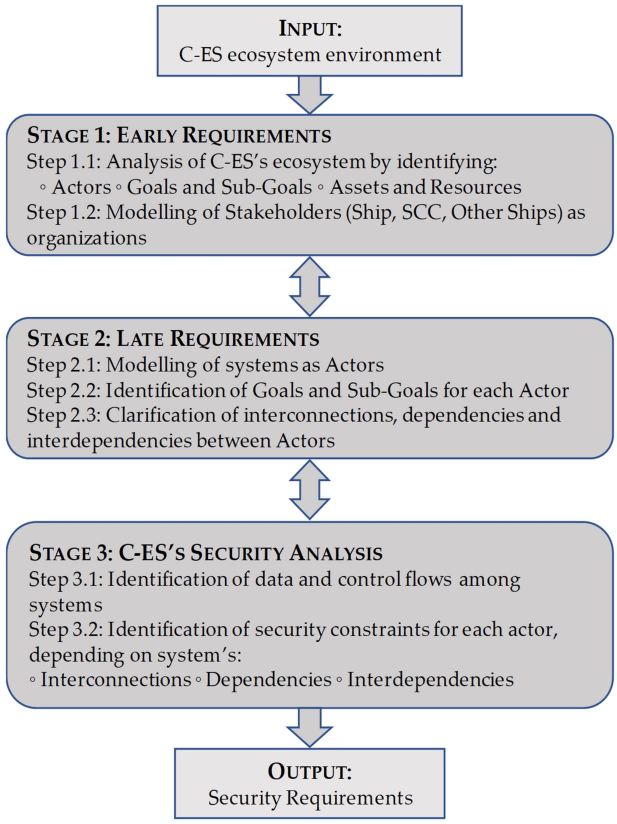

Fig. 1. Security requirements elicitation process.

II. Related Work

The security requirements of the autonomous vessels have only been scarcely and nonsystematically examined. The technical and nontechnical communication requirements for an autonomous merchant ship have been analyzed in [14]. However, the security requirements for such communications systems were not considered. The data requirements for wireless transmission of autonomous ships have been identified in [15]. Bureau Veritas [16] described the functional requirements of six main systems of the autonomous ship, but without considering the corresponding security requirements in detail. The security requirements of a vessel's control system components have been described in [17]. Although Ref. [17] provides a comprehensive analysis of the cyber-security requirements as they derive from relevant standards, only conventional vessels are considered. The IEC 61162-460 standard [18] describes the security requirements of the maritime navigation and radio communication equipment and systems onboard, for conventional ships. To the best of our knowledge, no previous work has addressed the problem of identifying the security requirements of the cyber-physical systems of the C-ES by leveraging a systematic approach.

A multitude of security requirements engineering methods exist and several works have compared methods, tools, and frameworks for security requirements elicitation [19]–[21]. Most of the reviews analyze the pros and cons of the reviewed methods and conclude with a recommendation on their appropriateness. Several of these, e.g., [22], [23] recommend the Secure Tropos methodology [10] as enjoying many of the desirable characteristics. The methodology has been used to extract security and privacy requirements in several cases, including the industrial IoTs [24], [25]. In addition, a framework which combines EBIOS, Secure Tropos, and PriS methods to extract security, privacy, and safety requirements for connected vehicles has been proposed in [26]. As privacy is not relevant to the CPS systems under study, because no personally identified data are involved with the operation of these systems, based on these findings, Secure Tropos was selected as the most appropriate methodology for the analysis of the complex C-ES ecosystem and for the elicitation of its security requirements.

The MAF [11] is a domain-specific architectural methodology designed to overcome the challenge to coordinate the development of new systems between technology issues, governance aspects, and users between existing architectures in the maritime sector. The MAF is derived from the successfully established architecture model in the energy domain named smart grid architecture model (SGAM) [27]. The main element of the MAF is the multidimensional cube, which combines different viewpoints to provide a graphical representation of the underlying maritime domain and the examined system architecture. The cube captures three dimensions, namely interoperability, hierarchical, and topological.

III. Security Requirements Elicitation Process

The proposed process of security requirements elicitation for the C-ES is based on and adapted from [25] and [28], and is depicted in Fig. 1. In the first stage, entitled "Early

TABLE I
C-ES ENVIRONMENTAL CONSTRAINTS

Constraint	Short description
Weather conditions	Heavy weather conditions, such as strong winds and heavy mist where the visibility is limited.
Legal	Sail in congested waters, such as ports using specific legal framework or SCC's directions.
Communication	Support a multitude of communication technologies.
Geographic	Islands, reefs, mountains which may influence the ship's operation, and protection of the sea life.
Cyber attacks	Since the C-ES is comprised of cyber-physical systems, the infrastructure may be exploited by physical/cyber attacks.
Traffic	Several other entities in the ship's vicinity, either physical or virtual.
Emergency	Search and rescue operations is compulsory according to International Maritime Organization (IMO) guidelines.
Restricted areas	Operating in Special Emission Control Area (SECA); ship reporting area or other restricted areas.
Harbors	Navigation in different harbors which are characterized by different architectures, port authorities, and legal frameworks.
Human factors	Ensure the safety of people and handle unpredictable incidents which derive from them.
Port systems	The interaction with the automated port systems is continuous and crucial for the security and monitoring of the cargo.

requirements," the C-ES ecosystem's actors, goals, assets, and resources are identified. The outcome of this phase is an actor diagram and a number of goal diagrams. In the next stage, entitled "late requirements," the actor diagram of the early requirements is extended with the introduction of the system as an actor that has a number of dependencies with the rest of the actors. In fact, these dependencies will be the functional and nonfunctional requirements of the system. In the third stage, entitled "security analysis," based on the system requirements and data and control flows among actors, a global architecture of the C-ES is defined, along with security constraints. The outcome of the overall process is the security requirements.

This process is implemented by leveraging the Secure Tropos methodology [10], initially designed as a security-aware software systems development methodology that combines requirements engineering concepts, such as "actor," "goal," and "plan," together with security engineering concepts such as "threat," "security constraint," and "security mechanism". Different ecosystem components, dependencies, inter-dependencies, connections, and interconnections among systems can be visually represented through this method as well as security-related arguments, such as security constraints, threats, vulnerabilities, and countermeasures. The application of the methodology is supported by the SecTro tool [28].

A. Environment Analysis

The first step in the process is the analysis of the environment of the system under examination. To this end, we leverage the MAF [11]. This framework enables the structured representation of the maritime domain, in terms of elements of the ecosystem, such as information assets, people, and technology used. The environment is represented by means of the MAF multidimensional cube, where three layers, namely the C-ES, the SCC, and the communication link between them and the ecosystem's elements are depicted. Essentially, the environment of the C-ES is represented by the actors of a ship's ecosystem, goals, and dependencies among actors and goals.

Security requirements are most usefully defined as requirements for the operational and environmental constraints of the system under analysis [24]. Therefore, the detailed identification of such constraints is an important element of the security requirements elicitation process. The authors in [29] have already defined the operational constraints for the unmanned merchant ships [30] without, however, identifying constraints such as system vulnerabilities and potential cyberattacks. The environmental constraints are inexorably linked to the C-ES's operational constraints, as they restrict the various goals and plans the ship has and can be exploited by adversaries, thus raising security issues. As the SCC is also a crucial part of the C-ES's ecosystem, environmental constraints for the SCC should also be identified. The identified environmental constraints for the C-ES are depicted and shortly described in Table I, and those for the SCC in Table II.

B. Organizational Analysis

Stage 1 and Stage 2 of the security requirements elicitation process together constitute the organizational analysis of the ecosystem and of its elements. This is carried out by following Steps 1.1 through 2.3 as indicated in Fig. 1. The analysis is carried out both for the ecosystem as a whole and for each one of the individual systems considered, namely the AIS, the ECDIS, and the GMDSS.

1) Ecosystem Organizational Analysis: Fig. 2 depicts the organizational view of the C-ES ecosystem where three entities have been identified: the ship, the SCC, and other ships. Following the Secure Tropos methodology, these entities are represented as distinct organizations, by rectangles. Within the ship, the bridge and the engine systems have been identified as actors, and are represented by circles; these interact with the external actors, such as the human–machine interface (HMI) of the SCC and other ships in the vicinity. Actors' boundaries are represented by dashed rounded rectangles that contain the goals and the subgoals that the actors have to fulfill (represented by rounded rectangles), as well as the resources they require in order to satisfy those goals (represented by rectangles). The actors are defined based on their dependencies and interdepencencies, as depicted in Fig. 2. It should be noted that the organizational view of the ecosystem includes different types of data, depending on the actors these data derive from. For example, bridge systems communicate navigation, voyage, and safety-related data, while engine systems exchange engine-related data.

2) AIS Organizational Analysis: The AIS provides information intended to facilitate the monitoring of traffic, thus contributing to ensuring the ship's safety and to increasing the situational awareness. The AIS exchanges data with six different navigational subsystems and two external actors, namely the SCC and other ships in the vicinity. The transmitted data can be static, voyage, dynamic, and safety-related, depending on the

TABLE II
SCC ENVIRONMENTAL CONSTRAINTS

Contraint	Short description
Weather conditions	Harsh weather may cause malfunction to the external sensors or antennas of the SCC building and could affect the delay and latency of communication.
Legal	The SCC should follow the International maritime legislation and standards for the safe and secure ship's operation.
Communication	Loss of communication link or malfunction of the satellite provider may cause disruptions to the C-ES.
Geographic	The location of the SCC is essential for its smooth communication with both the vessel and the shipping company.
Cyber attacks	The SCC is comprised of cyber and physical systems, like the C-ES.
Natural disaster	Flood, fire or earthquakes may influence the environment of the SCC and its operation.
Different vendors	SCC systems developed by different vendors could cause interoperability issues.
Personnel	The environment of the SCC may be affected in case of a personnel leaving or dismissal.
Multi role environment	The SCC is an environment where humans with diverse professional expertise and roles co-exist and co-operate.
Port Authorities	The SCC should be able to effectively communicate and interact with port authorities
Stakeholders	The SCC communicates and interacts with stakeholders in order to ensure the vessel's operations.

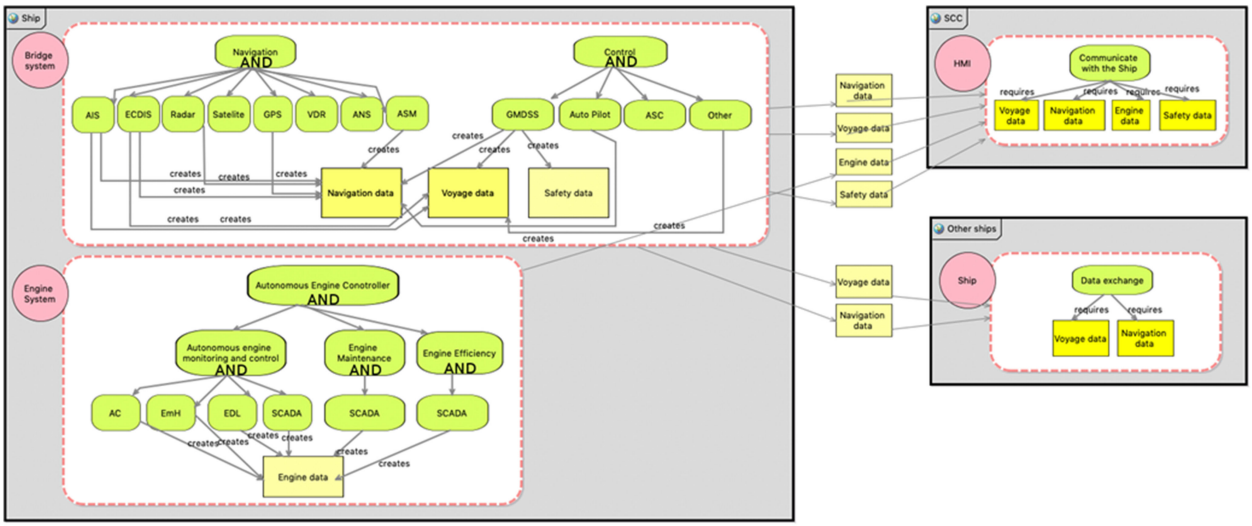

Fig. 2. General ecosystem representation.

system interconnections and interdependencies, as it is depicted in the full organizational view[1] of the AIS.

3) ECDIS Organizational Analysis: The ECDIS provides and transmits information regarding the ship's voyage. Its full organizational view[2] includes eight internal and two external actors. The internal actors are the subsystems of the navigation system and the external actors are the SCC and the ship controller. It is worth noting that although the ship controller is an onboard system, it has been characterized as an external actor because it is not a subsystem of the navigation system. The goals and the subgoals of each actor have been identified taking into account the corresponding resources, i.e., the exchange data among actors; these can be static, dynamic, voyage, and safety-related data.

4) GMDSS Organizational Analysis: The GMDSS ensures the rapid alerting of (no)shore authorities in the event of emergency. Its organizational view[3] includes the ship controller's subsystems, characterized as the internal actors. The external actors are the onboard systems and subsystems which GMDSS interacts with, and the SCC. The goals and subgoals of each actor have been defined considering the type of the signals and data that are transmitted; these indicate dependencies and interdependencies. Transmitted signals and data are the resources that are required for each actor to accomplish its goals. The GMDSS is interdependent with the onboard and onshore systems, the engine and navigation systems, and the SCC.

C. Security Requirements

The organizational view of the ecosystem, as depicted in Fig. 2, constitutes the C-ES system's general architecture. Based on the functionality and the technical characteristics of the systems under study, the data and control flows are identified, as required in Step 3.1 of the security requirements elicitation process. These are depicted in Figs. 3, 4, and 6. Step 3.2 requires the identification of the security constraints for each actor. In our case, these constraints are the elements of the *Parkerian Hexad*, i.e., *Confidentiality* – defined as limited observation and disclosure of knowledge; *Integrity* – defined as completeness, wholeness, and readability of information and quality being unchanged from a previous state; *Availability* – defined as usability of information for a purpose; *Possession* – defined as

[1][Online]. Available: https://drive.google.com/open?id=1uzLTvcqeGcVDS6BT4n8Oh7IwCcDGgNLE

[2][Online]. Available: https://drive.google.com/open?id=1bw3vvi1UseVI40TnVo0TwXRxz1Q_pYjG

[3][Online]. Available: https://drive.google.com/open?id=1pQGSxM57s13GQkTrk3KhH7RPEhuARqz1

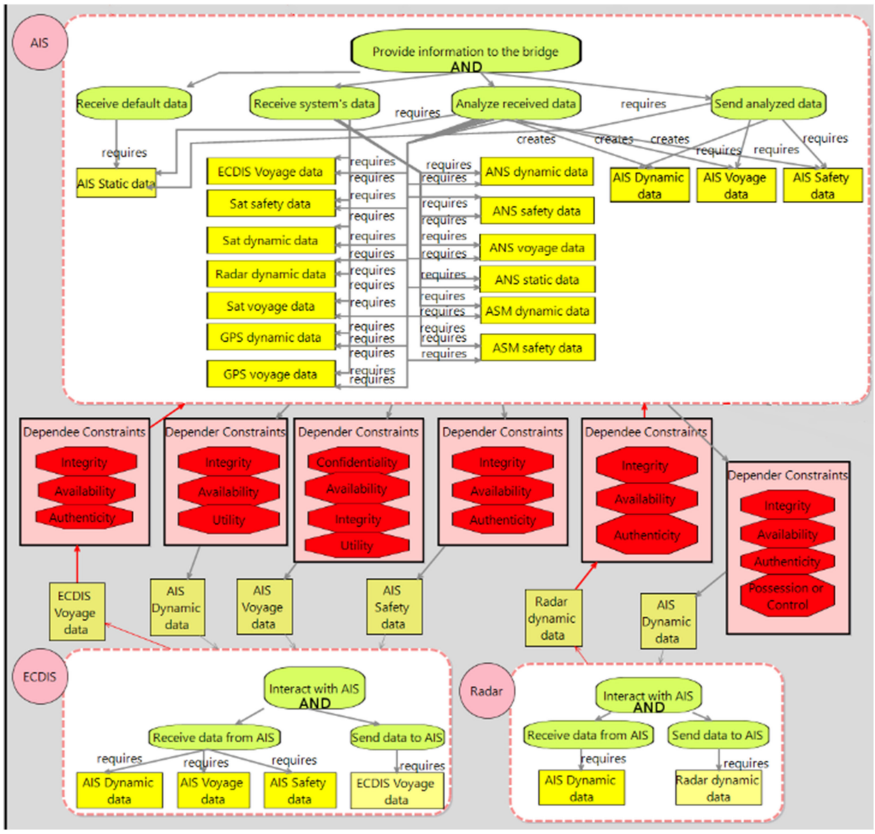

Fig. 3. AIS security requirements.

holding, controlling, and having the ability to use information; *Authenticity* – defined as validity, conformance, and genuineness of information; and *utility* – defined as usefulness of information for a purpose [31].

According to [28], when using the Secure Tropos methodology, the security constraints in the systems goal diagram are the security requirements of the targeted system. The identified system functional and operational requirements lead to identifying the system goals, as well as the processes and resources utilized to achieve the identified goals. The security constraints which will protect the identified processes and goals are identified by considering the Parkerian hexad. An example of this procedure follows. Two identified security requirements are as follows: the connectivity between system and external actors and between onboard systems must be continuous and voyage-related data transmitted to the SCC must be protected against tampering or damage. Considering the Secure Tropos method, first, we analyze the environment of the targeted system and we identify its operational and functional requirements which are Inform SCC about vessels speed and position and send voyage data to SCC, respectively. Then, the goals and subgoals that need to be achieved so as the system fulfills the operational and functional requirements are identified. These include 1) receive and analyze voyage data from ECDIS and Radar, and 2) send analyzed data to SCC. The resources to achieve these goals are the AIS voyage data. In order to design the system-to-be (in this case, a secure AIS system), the security constraints are identified. In this case, availability and integrity are identified as security constraints of the interconnections and interdependencies between the AIS and the SCC. Since a security requirement is the security constraint in the systems goal diagram, the resulting security requirements are as follows: the availability of the transmitted data between AIS and SCC should be ensured and the integrity of the processed and transmitted data must be protected. Considering the operational and functional requirements of the targeted system, and the potential threats to the AIS (denial of service, tampering) [4] that could violate the identified constraints (availability, integrity), a system-specific security requirement is that voyage-related data transmitted to the SCC must be protected against tampering or damage. Since the protection of availability of the transmitted data is a common requirement for the three targeted systems, the availability requirement is refined to "the connectivity between system and external actors and between onboard systems must be continuous." This requirement is allocated in the first group of requirements (common security requirements).

The outcome of Stage 3 of the security requirements elicitation process, guided and supported by the SecTro tool, is the security requirements. These are presented in the sequel, following the classification scheme in the ISO 27001:2013 [32] and ISO 27002:2013 [33] standards. Several standards on the security of cyber-physical systems are discussed in [34]. These include the ISO 27 k family; NECs CIP family of standards; and the ISA IEC IEC-62443 series. Also relevant are standards on software security requirements (such as, e.g.,

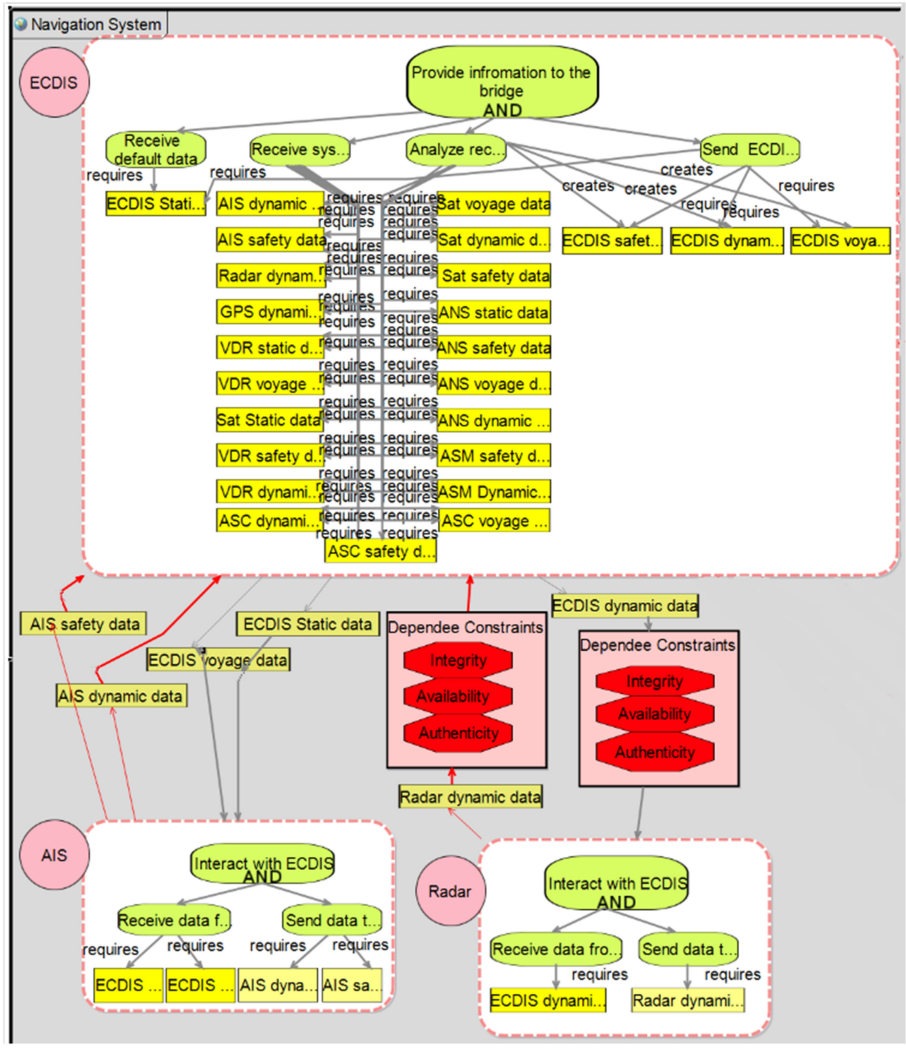

Fig. 4. ECDIS security requirements.

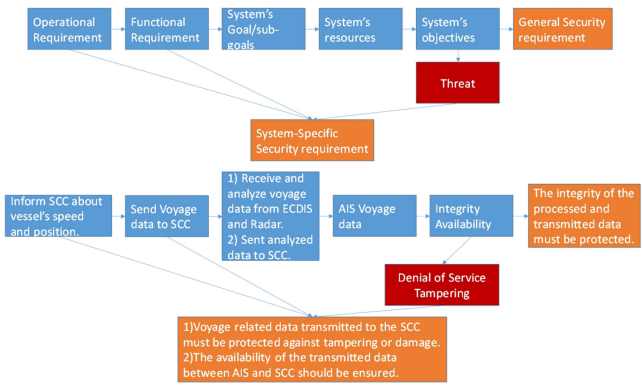

Fig. 5. Security requirements elicitation process.

ECSS-Q-ST-80 C, IEEE 830-1998, ISO/IEC 25010, ISO/IEC 27034-1, and ISO/IEC 27034-3). In the maritime domain, Ref. [17] provides a classification of cyber-security requirements. As the ultimate goal of this research is to propose cyber-security requirements for the whole C-ES ecosystem, we have decided to use the ISO 27001-27002 standards for presenting the requirements, as these pertain to organizations rather than isolated systems, be they software or otherwise. This will greatly facilitate their integration with additional requirements derived from other elements of the C-ES ecosystem. Using the classification in [17] could have been an alternative; however, we opted for a de jure standard rather than an industry proposal. Two groups of requirements are presented: common and system-specific. The former group includes requirements applicable to all three studied systems, whereas the latter includes requirements pertinent to each individual system.

1) Common Security Requirements: Human resource security: i) the system administrator must be well trained and aware of system functional and nonfunctional requirements (e.g., AIS modes and communication capabilities). *Asset management*: i) data and signals must be identified and classified into protection levels; ii) a documentation of third-party components, versioning, and published system vulnerabilities must be maintained; *Access control*: i) a strong password policy must be enforced which will specify the length and the lifetime of each

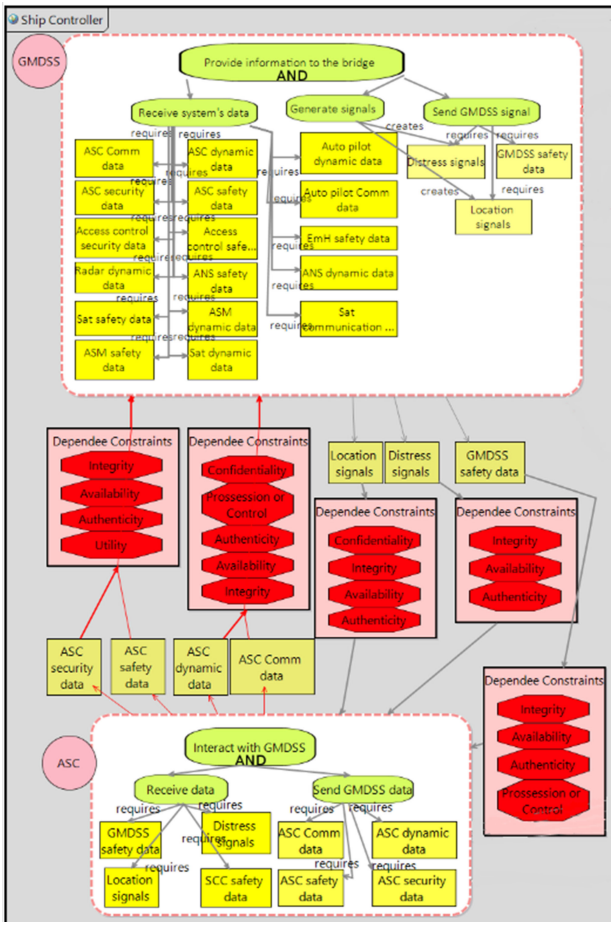

Fig. 6. GMDSS Security Requirements.

combination of the credentials (e.g., passwords to log in to the ECDIS should be regularly changed); ii) the nonrepudiation and traceability of actions performed either from the SCC or physically to the onboard system must be ensured with appropriate authentication mechanisms; iii) the system must be able to implement lock mechanisms when requested by the system administrator or after a configurable time of idleness; iv) the number of consecutive login attempts to the system must be specified; v) the system must support multifactor authentication; and vi) the system must accept inputs only from authorized entities, by authorized maritime actors. *Cryptography*: i) the system must support encryption algorithms able to promote data confidentiality and integrity, and to satisfy data transmission timing requirements during the voyage; ii) data transmitted to external and internal actors should be encrypted by using appropriate – in each case – cryptographic mechanisms [e.g., dynamic data sent from ECDIS to radar, global positioning system (GPS), and advanced sensor module (ASM) systems must be encrypted]; iii) stored data should be appropriately encrypted, the strength of the encryption mechanism depending on their type and the possible pertinence of maritime legal or regulatory requirements. *Physical and environmental security*: i) the physical integrity of the on board or SCC sensors must be protected; ii) the system must be installed so as to prevent physical damages, such as flooding or fire; and iii) all physical and virtual connection points of the system must be appropriately protected or blocked (e.g., USB ports or any other human interface device-HID). *Operations security*: i) both onboard and SCC systems must be able to operate under network stress situations such as a denial of service attack; ii) security mechanisms must be implemented in order to protect the system from malicious code; iii) frequent system data backup should be maintained (e.g., ECDIS voyage data should be backed up regularly to the VDR); iv) the system must be able to determine whether an action taken has been performed by a system onboard or by a human user remotely from the SCC; v) the integrity of the static, processed, and transmitted data must be protected; vi) the confidentiality of data in transit and in storage must be protected; vii) the freshness of data should be ensured; vii) the authenticity of services, transmitted data, and software sources must be ensured (e.g., AIS updates or ECDIS charts updates should be performed by authorized sources/vendors); viii) the utility of the dynamic and voyage data should be ensured; and ix) the measures to protect the confidentiality and integrity of data should not downgrade their utility. *Communication security*: i) the confidentiality and integrity of the data exchanged between internal (onboard 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; ii) the segregation of the onboard components in different trust levels must be ensured; iii) the connectivity between system and external actors and between onboard systems must be continuous; iv) onboard systems must be mutually authenticated; v) the traffic from and to the system must be monitored; vi) the systems should be able to control the sent data considering the actor and the type of the data in transit; vii) all external actors of the C-ES ecosystem must be able to determine the source of data flows originating from the onboard systems; viii) the data exchange between onboard systems should be established in a way such that their authenticity can be verified; ix) the systems must use transport layer security to protect the data in transit; x) the system should support mechanisms to detect rogue data packets; xi) the services between onboard systems and external actors (SCC/other vessel) must be authenticated; xii) there should be redundancy of communication channels between onboard systems; and xiii) the maximum allowable latency in system-to-system communication should conform to pertinent standards and to the systems' operational requirements. *System acquisition, development, and maintenance*: i) system development and deployment must be performed following pertinent cyber-security standards; ii) the update process must be protected against time-of-check vs. time-of-use attacks; iii) the source of the software must be authenticated; iv) both onboard and shore-based systems must be maintained regularly; v) the system should be properly installed, taking into account network segmentation and physical access; vi) system updates/upgrades must be performed only by authorized entities; vii) the integrity of the maintenance process must be ensured to prevent malicious intrusions, viii) system maintenance must be performed only by well-trained personnel; ix) the configuration and installation of the system must be performed by authorized personnel;

x) the vessel's infrastructure must be well designed and the corresponding systems appropriately installed according to the type of the ship; and xi) the system must not allow downgrading to old system software versions. *Supplier relationships*: i) appropriate mechanisms must be employed to validate hardware, software, and data from the suppliers; and ii) strict review of the security policies of the system's vendor must be undertaken. *Information security incident management*: i) the system must detect and produce an alert on abnormal numbers of requests, such as by a user or an external actor; ii) the system's functional and nonfunctional requirements should be maintained during a security incident such as, e.g., GMDSS signal jamming; and iii) the SCC must be notified when a system anomaly has been detected. *Information security aspects of business continuity management*: i) the continuity of system operations must be ensured; ii) the system onboard or on-shore must be able to operate using alternative power sources; iii) the system must be able to operate 24/7; and iv) redundant systems should be installed taking into account the operational complexity[4] of the C-ES and the system operations. *Compliance*: i) Formal certification of compliance with the pertinent legislative and regulatory requirements must be obtained.

2) AIS-Specific Security Requirements: A part of the security requirements view of the AIS is depicted in Fig. 3. The full requirements view[5] is omitted in the interest of saving space.

Operations security: i) the AIS should implement the security services in order to protect the system from loss of control or possession of information; and ii) voyage data, such as destination port or cargo-related information, should be confidential to prevent potential leakage to adversaries. *Communications security*: i) the communication channel with the radar system should be redundant; and ii) voyage-related data transmitted to the SCC must be protected against tampering or damage. *Access control*: i) reliable authentication mechanisms must be in place in order to uniquely identify the actors reading, modifying, and transmitting AIS data, as well as to authenticate the system itself and its services; and ii) 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. *Cryptography*: i) the authenticity of AIS functions (e.g., request, read, process, and send) must be ensured by using security techniques such as digital signatures.

3) ECDIS-Specific Security Requirements: A part of the security requirements view of the ECDIS is depicted in Fig. 4. The full requirements view[6] is omitted in the interest of saving space.

Human resource security: i) The ECDIS administrator must be trained and able to distinguish rogue data packets. *Access control*: i) the use of ECDIS must be restricted only to authorized and well-trained personnel. Communication security: i) the ECDIS must be able to control the flows of voyage-related data sent to other ships and to the SCC; ii) the ECDIS should be able to audit sent and received data to external actors; iii) safety-related information transmitted by the ECDIS must be authenticated; and iv) the communication between the ECDIS and the satellite system should be continuously available.

4) GMDSS-Specific Security Requirements: A part of the security requirements view of the GMDSS is depicted in Fig. 6. The full requirements view[7] is omitted in the interest of saving space.

Information security policies: i) A policy for installing the GMDSS components in the vessel's network should exist. *Access control*: i) 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; and ii) sistress 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. *Operations security*: i) The ASC must be able to provide security, safety, and dynamic data to the GMDSS, when needed. *Communication security*: i) Safety signals transmitted through the GMDSS to other onboard systems and external actors must be continuously available; ii) the GMDSS must be able to detect whether the signal/data comes from a legitimate user/system or from a malicious user; and iii) the signals transmitted to external actors or subsystems must be appropriately encrypted. *System acquisition, development and maintenance*: i) GMDSS antennas must be appropriately installed.

IV. Conclusion

In this article, we proposed a process for eliciting the security requirements of the C-ES ecosystem, based on the Secure Tropos methodology and leveraging the MAF reference architecture as instantiated in the case of the C-ES. By applying the proposed process, we identified the security requirements for the three most vulnerable C-ES systems, namely the AIS, the ECDIS, and the GMDSS. As future work, we intend to address the issue of systematically deriving the security requirements of the C-ES viewed as a system-of-systems utilizing the requirements of each individual constituent system. Additionally, we intend to extend our work by allowing the combined elicitation of security and safety requirements.

References

[1] SINTEF, "Shipping 4.0 presented at singapore maritime week," [Online]. Available: https://www.sintef.no/en/latest-news/shipping-4.0-presented-at-singapore-maritime-week/

[2] J. Cross and G. Meadow, "Autonomous ships 101," *J. Ocean Technol.*, vol. 12, pp. 23–27, 2017.

[3] K. Tam and K. Jones, "Cyber-risk assessment for autonomous ships," in *Proc. IEEE Int. Conf. Cyber Secur. Protection Digital Services*, 2018, pp. 1–8.

[4] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cyber-attacks against the autonomous ship," in *SECPRE 2018, CyberICPS 2018. Lecture Notes in Computer Science*. Springer, 2018, vol. 11387, pp. 20–36.

[4]The C-ES's operational complexity depends on the mission and the environment of the vessel, as well as on its level of autonomy.

[5][Online]. Available: https://drive.google.com/open?id=127DIgy9QR4H1b5K3-40Kx3KfDVyYsGEy

[6][Online]. Available: https://drive.google.com/open?id=1VljM1uibsuT--u7DuiIcPGnq5Y8TgSps

[7][Online]. Available: https://drive.google.com/open?id=1errDRGKchm9UOZ_R0UCR-IRIbRrmAL9F

[5] USCG, "Cyber incident exposes potential vulnerabilities onboard commercial vessels," [Online]. Available: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5~PC/INV/Alerts/0619.pdf
[6] M. Jones, "Spoofing in the black sea: What really happened?" [Online]. Available: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/
[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," [Online]. Available: https://www.maritime.dot.gov/content/2019-012-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea- threats-commercial-vessels
[8] G. Kessler, J. P. Craiger, and J. C. Haass, "A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system," *TransNav: Int. J. Marine Navigation Safety Sea Transp.*, vol. 12, no. 3, p. 429, 2018.
[9] S. Katsikas, "Cyber security of the autonomous ship," in *Proc. 3rd ACM Workshop Cyber-Physical Syst. Secur.*, ACM, 2017, pp. 55–56.
[10] H. Mouratidis and P. Giorgini, "Secure tropos: A security-oriented extension of the tropos methodology," *Int. J. Softw. Eng. Knowl. Eng.*, vol. 17, no. 2, pp. 285–309, 2007.
[11] B. Weinert, A. Hahn, and O. Norkus, "A domain-specific architecture framework for the maritime domain," in *Informatik 2016*, H. C. Mayr and M. Pinzger, Eds, Bonn, Germany: Gesellschaft für Informatik e.V., 2016, pp. 773–784.
[12] L. Kretschmann, Ø. J. Rødseth, B. S. Fuller, H. Noble, J. Horahan, and H. McDowell, "MUNIN D9.3: Quantitative assessment," 2015, p. 150.
[13] Body of Knowledge and Curriculum to Advance Systems Engineering Editorial Board, "The guide to the systems engineering body of knowledge (SEBoK), v. 2.0," [Online]. Available: www.sebokwiki.org.
[14] Ø. J. Rødseth, B. Kvamstad, T. Porathe, and H. Burmeister, "Communication architecture for an unmanned merchant ship," in *Proc. MTS/IEEE OCEANS – Bergen*, Norway, 2013, pp. 1–9.
[15] M. Höyhtyä, J. Huusko, M. Kiviranta, K. Solberg, and J. Rokka, "Connectivity for autonomous ships: Architecture, use cases, and research challenges," in *Proc. IEEE Int. Conf. Inf. Commun. Technol. Convergence*, 2017, pp. 345–350.
[16] Bureau Veritas, "Guidelines for autonomous shipping," Tech. Rep., 2017. [Online]. Available: https://www.bureauveritas.jp/news/pdf/641-NI_2017-12.pdf
[17] DNVGL, "Cyber security capabilities of control system components," Det Norske Veritas Germanischer Lloyd, Tech. Rep, 2018.
[18] International Electrotechnical Commission – IEC, "Maritime navigation and radiocommunication equipment and systems," NEK IEC 61162-460:2018, 2018, p. 152.
[19] N. Mead, "How to compare the security quality requirements engineering (SQUARE) method with other methods," Tech. Rep., Aug. 2017, [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a471104.pdf
[20] A. Nhlabatsi, B. Nuseibeh, and Y. Yu, "Security requirements engineering for evolving software systems: A survey," *Int. J. Syst. Syst. Eng.*, vol. 1, pp. 54–73, 2010.
[21] A. Pattakou, C. Kalloniatis, and S. Gritzalis, "Security and privacy requirements engineering methods for traditional and cloud-based systems: A review," *Cloud Comput.*, vol. 155, pp. 145–151, 2017.
[22] D. Mellado, C. Blanco, L. Sánchez, and E. Fernández-Medina, "A systematic review of security requirements engineering," *Comput. Standards Interfaces*, vol. 32, no. 4, pp. 153–165, 2010.
[23] D. Muñante, V. Chiprianov, L. Gallon, and P. Aniorté, "A review of security requirements engineering methods with respect to risk analysis and model-driven engineering," in *Proc. Int. Conf. Availability Rel. Secur.*, 2014, pp. 79–93.
[24] V. Diamantopoulou and H. Mouratidis, "Applying the physics of notation to the evaluation of a security and privacy requirements engineering methodology," *Inf. Comput. Secur.*, vol. 26, no. 4, pp. 382–400, 2018. doi:10.1108/ICS-12-2017-0087.
[25] H. Mouratidis and V. Diamantopoulou, "A security analysis method for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4093–4100, Sep. 2018.
[26] C. Kalloniatis *et al.*, "Towards the design of an assurance framework for increasing security and privacy in connected vehicles," *Int. J. Internet Things Cyber-Assurance*, 2019.
[27] CEN-CENELEC-ETSI Smart Grid Coordination Group, "CEN-CENELEC-ETSI smart grid coordination group smart grid reference architecture," Tech. Rep., Nov. 2012, p. 107.
[28] M. Pavlidis and S. Islam, and H. Mouratidis, "A CASE tool to support automated modelling and analysis of security requirements, based on secure tropos," in *Proc. Int. Conf. Adv. Inf. Syst. Eng.*, 2011, pp. 95–109.
[29] Ø. J. Rødseth and Å. Tjora, "A system architecture for an unmanned ship," in *Proc. 13th Int. Conf. Comput. IT Appl. Maritime Industries*, 2014, p. 13.
[30] "MUNIN maritime unmanned navigation through intelligence in networks," [Online]. Available: http://www.unmanned-ship.org/munin/
[31] D. B. Parker, "Toward a new framework for information security?" *Computer Security Handbook*, 6th ed., S. B. Michel and E. K. E. Whyne, Eds. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2012, ch. 3, pp. 3.1–3.23.
[32] International Organization for Standardization, ISO, "ISO/IEC 27001:2013 Information Technology Security Techniques Information Security Management Systems Requirements," Cham, Switzerland, Tech. Rep. ISO, 2013.
[33] International Organization for Standardization, ISO, "ISO/IEC 27002:2013 Information Technology Security Techniques Code of Practice for Information Security Controls," Cham, Switzerland, Tech. Rep. ISO, 2013.
[34] S. Ali, A. T. Balushi, Z. Nadir, and O. K. Hussain, "Standards for CPS," in *Cyber Security for Cyber Physical Systems*. Cham, Switzerland: Springer Nature, 2018, pp. 161–174.

Georgios Kavallieratos received the B.Sc. degree in computer science and the M.Sc. degree in digital systems security in 2016 and 2018, respectively, from the University of Piraeus, Piraeus, Greece. He is currently working toward the Ph.D. degree in security of the cyber-enabled ship with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway.

His research interests include cyber-physical systems security and maritime cyber-security.

Vasiliki Diamantopoulou received the Diploma in product and systems design engineering, the M.Sc. degree in management of information systems, and the Ph.D. degree in information systems and innovation from the Department of Information and Communication Systems Engineering, University of the Aegean, Lesvos, Greece.

She is currently an Adjunct Professor with the Department of Information and Communication Systems Engineering, University of the Aegean, and a Senior Researcher with the Department of Digital Systems, University of Piraeus, Piraeus, Greece. She was a Research Fellow with the School of Computing, Engineering and Mathematics, University of Brighton, U.K. Her research interests include privacy and security of information systems, eGovernment and interoperability frameworks, and eBusiness and innovation of information systems.

Sokratis K. Katsikas received the Diploma in electrical engineering from the Univeristy of Patras, Patras, Greece, in 1982, the M.Sc. degree in electrical and computer engineering from the Univeristy of Massachusetts Amherst, Amherst, MA, USA, in 1984, and the Ph.D. degree in computer engineering and informatics from the University of Patras, in 1987.

He is the Rector of the Open University of Cyprus, Latsia, Cyprus, and a Professor with the Center for Cyber and Information Security, Norwegian University of Science and Technology, Gjøvik, Norway. He has authored or coauthored more than 280 journals, book chapters, and conference proceedings, and has authored or edited 41 books. He has participated in more than 70 funded national and international R&D projects in the areas of his research interest, which focuses on the area of information and communication systems security.

Dr. Katsikas is on the editorial board of several scientific journals. He chaired or was on the technical program committee of more than 680 international scientific conferences.