Graphical Abstract

SafeSec Tropos: Joint security and safety requirements elicitation

Georgios Kavallieratos ,Sokratis Katsikas ,Vasileios Gkioulos

figs/grabs.pdf

Highlights

SafeSec Tropos: Joint security and safety requirements elicitation

Georgios Kavallieratos ,Sokratis Katsikas ,Vasileios Gkioulos

- Novel method for the joint elicitation of security and safety requirements of Cyber Physical Systems.
- Safety and security objectives and goals for the Cyber-Enabled Ship ecosystem.
- Security and safety requirements of Cyber Physical Systems onboard a Cyber-Enabled Ship.

SafeSec Tropos: Joint security and safety requirements elicitation

Georgios Kavallieratos [a,*], Sokratis Katsikas [a,b,*] and Vasileios Gkioulos [a]

[a]Norwegian University of Science and Technology, Department of Information Security and Communications Technology, Gjøvik, Norway
[b]Open University of Cyprus, School of Pure and Applied Sciences, Latsia, Nicosia, Cyprus

ARTICLE INFO

Keywords:
security
safety
cyber physical systems
requirements elicitation
maritime ecosystem

ABSTRACT

The growing convergence of information technology with operational technology and the accordant proliferation of interconnected cyber-physical systems (CPSs) has given rise to several security and safety challenges. One of these refers to systematically identifying coherent, consistent, and non-conflicting security and safety requirements. This paper proposes an integrated method for safety and security requirements engineering for CPSs at the design stage of the system lifecycle. The method identifies security and safety objectives, it systematically elicits a comprehensive list of requirements, and it links these requirements to objectives, thus facilitating the process of resolving conflicts. To provide insight into the operations of the method, we demonstrate its use to the most vulnerable CPSs on board the Cyber-Enabled Ship (C-ES). By utilizing the proposed method, the safety and security objectives of these systems were defined, and their safety and security requirements were identified.

1. Introduction

Due to the close intertwining of the cyber and physical components, both safety and security are essential for the reliable operation of cyber-physical systems (CPSs). Safety aims to protect systems from unintentional actions while security implies protection from both intentional and unintentional threats. The associations between safety and security have extensively been analyzed in the literature [25, 51, 55].

Requirements engineering (RE) is a vital element of the CPS development process. As such, it is incorporated in both the safety [19] and the security [22] lifecycles and it is described in both safety and security standards. Several standards on the security and safety of cyber physical systems are discussed in [2, 57]. These include the ISO 27k family; NEC's CIP family of standards; and the ISA IEC IEC-62443 series. Also relevant are standards on software security requirements (such as e.g. ECSS-Q-ST-80 C, IEEE 830-1998, ISO/IEC 25010, ISO/IEC 27034-1, and ISO/IEC 27034-3). From the safety point of view, various standards exist for safety in the maritime domain. Such standards have been developed by ISO/TC 8/SC 1 and the International Maritime Organization (IMO). Additionally, various standards have been surveyed in [37] regarding the functional safety and security of industrial control systems. The incorporation of safety and security aspects is discussed in IEC 62859 for nuclear power plants. However, standards regarding the co-analysis of safety and security or even security alone in the maritime domain have not yet been developed. RE is incorporated in both the safety [19] and the security [22] lifecycles. As a weak combination of safety and security requirements may result in poor system design and development and possibly to damages to the CPS ecosystem, jointly analyzing and eliciting requirements for security and safety is necessitated. This is particularly so in cases where increasingly complex and interconnected CPSs are utilized, such as the Cyber-Enabled ship (C-ES) case. The C-ES is a variant of the autonomous or remotely controlled vessel. Its operational and functional activities are described considering Autonomy Levels (AL) 1-3, of the International Maritime Organization (IMO) classification [21]. As discussed in detail in Section 2, various security and safety requirements engineering methodologies have appeared in the literature. However, several impediments are associated with the co-analysis of security and safety in complex systems [55]. Most of the existing studies fall short of eliciting requirements that ensure both the satisfaction of safety constraints and the protection of information security attributes and are therefore not readily applicable to the security and safety co-analysis of CPSs within the C-ES ecosystem.

This work proposes an integrated method for the joint elicitation of security and safety requirements early during system design. The introduced method examines the safety and the security of the targeted system by analyzing the

[*]Corresponding author

georgios.kavallieratos@ntnu.no (G.K.); sokratis.katsikas@ntnu.no (S.K.); vasileios.gkioulos@ntnu.no (V.G.)
ORCID(s): 0000-0003-1278-1943 (G.K.); 0000-0003-2966-9683 (S.K.); 0000-0001-7304-3835 (V.G.)

corresponding objectives. This process enables the identification of requirements early in the system's design phase, and facilitates the resolution of potential conflicts between safety and security requirements. In particular, the evaluation and selection of the identified objectives, and the consideration of the relevant standards [19, 22], legislation, and stakeholders, facilitate the requirements elicitation process, where the safety and the security objectives are translated to corresponding requirements. Moreover, the elicitation of the safety and security requirements is not performed in isolation; this is a common weakness of other integrated methodologies [37]. The method analyzes both safety and security objectives evenly, by integrating two well established systematic approaches, namely the Secure Tropos [42] and the Systems Theoretic Process Approach (STPA) [33]. The analysis follows a top-down approach and allows the extraction of results without the need to consider the detailed design of the system under analysis. Thus, the proposed method enables the analysis of systems whose detailed specifications are not yet available. We then apply the proposed method to the use case of the C-ES to identify safety and security requirements for the most vulnerable onboard CPS, namely the Automatic Identification System (AIS), the Electronic Chart Display System (ECDIS), and the Global Maritime Distress and Safety System (GMDSS). The contribution of this work is threefold:

- a novel method for the joint elicitation of security and safety requirements of CPSs has been developed based on the Secure Tropos and STPA methods from the security and the safety domain respectively;
- a set of security and safety objectives for the C-ES ecosystem has been defined. The security objectives are based on the Parkerian Hexad with the addition of Non-Repudiation. To the best of our knowledge, this work is a first attempt to define safety objectives for the CPSs of the C-ES's ecosystem;
- the security and safety requirements of the most vulnerable navigational CPSs onboard a C-ES (AIS, ECDIS, GMDSS have been identified.

The remainder of this paper is structured as follows: Section 2 reviews the related work. Section 3 provides an overview of the Secure Tropos and the STPA methods. Section 4 discusses the limitations of the existing approaches and describes the proposed SafeSec Tropos method. Section 5 presents the application of the proposed method to the C-ES case. Section 6 discusses the results as well as limitations of the proposed method. Finally, 7 summarizes our conclusions and discusses challenges to be addressed in future research.

2. Related Work

The joint analysis of safety and security has received considerable attention. As a result, several relevant works exist in the literature, as well as reviews and surveys. A systematic literature review of safety and security co-analysis methods appeared in [35]; risk assessment approaches for security and safety of CPSs are surveyed in [38]; approaches combining security and safety for industrial control systems are surveyed in [31]; and safety and security co-engineering methods are surveyed in [47]. C. Raspotnig et al. in [53] surveyed risk analysis methods for safety and security and compared the surveyed techniques considering twelve criteria. The survey concluded that there is a need for a tighter integration of the requirements elicitation activities with safety and security aspects.

Two approaches regarding the co-analysis of safety and security are identified: (1) Integrated approach, and (2) Unified approach. An integrated approach analyzes safety and security separately and then integrates the results, while a unified approach analyzes safety and security jointly [35]. The former reduces the insight of the analysis leading to incomplete results, while the latter provides more rigorous results, with better understanding of potential conflicts between safety and security [12]. The existing methods have different characteristics depending on their approach towards analyzing the security and safety of the targeted system (unified/integrated); the phase of system lifecycle when the method can be applied (Development/Operational); the approach towards identifying the requirements (Qualitative/Quantitative); and the way safety and security properties influence each other (safety informed security/ security informed safety/ combined safety and security) [35, 31].

Despite the diversity, most of the existing works on the joint analysis of safety and security tackle security only as a peripheral or constituent of safety, largely neglecting the necessity for ensuring the fulfilment of its distinct objectives. Further, a recurring problem with existing work on joint security and safety analysis is that it more often than not results in identifying conflicting requirements. A framework to detect conflicts between safety and security requirements early in the development phase was proposed in [59]. The mechanism relies on negotiating changes in the requirements among safety and security engineers. A conflict resolution policy within the context of an approach based on the IEC 15408 and IEC 61508 standards was proposed in [45]. However, the proposed approach requires a formal description of the system under study, thus its applicability in practice is questionable. An approach to combine security and safety constraints by leveraging the NIST SP 800-30 standard and the Systems Theoretic Process Analysis (STPA) method

-discussed in the next section- was proposed in [50], where potential conflicts among the requirements are resolved by either redefining the system or refining the requirements. However, to the best of our knowledge, a method that would jointly analyze safety and security, and allow the resolution of possible conflicts by means of prioritizing the objectives that generated each conflicting requirement has not been proposed.

The Cyber Risk Assesment Framework (CRAF) was proposed in [5] and was applied analyze the security and safety of a vessel. An STPA-based approach to enhance the co-analysis of security and safety and its application to a semi-autonomous vessel was presented in [16]. A method to combine security and safety during the risk analysis process of the collision avoidance function of an autonomous surface vessel was proposed in [17]. Safety-related cyber-attacks against the navigation and propulsion systems of an inland autonomous vessel were identified in [8]. Three safety and security co-analysis approaches using an autonomous boat as a case study were compared in [60]. Safety and security issues for the crewless merchant vessel, developed within the EU project MUNIN, are examined in [29, 30]. However, a systematic analysis of safety and security requirements of the C-ES ecosystem and its constituent CPSs has not been undertaken.

3. Background

Secure Tropos is a model-based method for security requirements engineering [42]. It facilitates the analysis of the system's environment, along with complex and distributed computerized systems, by using a graphical language. It encompasses four models, namely: the security reference model; the security constraint model; the security entities model; and the secure capability model. The method follows four stages: (1) The early requirements elicitation, where the actors, goals, assets, and resources of the whole ecosystem are identified. The outcome of this phase is an actor diagram and a number of goal diagrams. (2) The late requirements elicitation, where the actor diagram of the previous stage is extended with the introduction of the system under study as an actor that has a number of dependencies with the rest of the actors. (3) The architectural design where a global architecture of the system is defined. (4) The detailed design. These stages facilitate the security analysis of the targeted system by identifying the relevant stakeholders, system goals, processes, and activities. The use of the method is supported by a software tool (SecTro Tool) [48]. Secure Tropos has been applied in various domains. Although Secure Tropos is a well accepted method for security requirements elicitation, it does not provide for considering safety-related objectives; therefore it cannot support the elicitation of safety constraints and requirements. Additionally, unsafe control actions and safety constraints cannot be identified, since the methodology supports only the security analysis of the targeted system.

STPA [34] is a systemic approach for safety analysis, focusing on the control actions of each system. STPA is based on system theory and facilitates the analysis of the targeted ecosystem by considering system and software interdependencies. The goal of STPA is to prevent losses. The method identifies potential causes of accidents by considering safety as a system control (constraint) problem. P. Asare et al. in [4] discussed the fitness of the STPA for analyzing the safety of CPSs, since the method analyzes components which are cyber and physical with social boundaries. The STPA analysis starts with the identification of accident and loss events, followed by the definition of hazardous system states that are responsible for possible accidents. These hazards are refined as system safety constraints, aiming to prevent accidents from occurring. STPA is carried out in four steps: (1) Define the purpose of the analysis; (2) Model the control structure; (3) Identify Unsafe Control Actions; and (4) Identify loss scenarios. The identification of the safety constraints can be achieved by following the four STPA principles: (i) A control action required for safety is not provided or not followed; (ii) An unsafe control action is provided; (iii) A potential safe control action is provided too early or too late; and (iv) A control action required for safety is stopped too soon or applied for too long. These principles are depicted in STPA tables, where the safety constraints along with the unsafe control actions and their consequences are described. STPA is a hazard analysis technique based on system theory; thus, certain cyber security threats, such as e.g. threats against confidentiality or repudiation, are not analyzed, since such threats cannot influence the system's safety. Although various extensions of STPA aiming to address security aspects have been proposed [14, 64], they come with some limitations [56, 12]. In particular, STPA-Sec is not able to capture and analyze information disclosure issues, hence it cannot be used to study confidentiality aspects of the targeted system. Even though a new approach, called STPA-SafeSec, overcomes some of the limitations of STPA-Sec, it is a unified safety and security analysis method; as such, it can lead to incomplete analysis [37].

Various reviews and surveys for security requirements engineering exist in the literature [44, 39, 43]. Secure Tropos is suggested for security requirements elicitation in [40, 43]. Further, Secure Tropos has been applied in different critical infrastructure domains to analyze cybersecurity aspects [52, 41]. As regards safety, various safety analysis techniques have been surveyed in [9, 53]. The survey concluded that the pros of the STPA are the wider perspective it provides on the system hazards; its ability to capture the control structure; and its coverage of conflicting actions in CPSs. An important advantage of STPA as compared to other safety analysis methods is that it considers the interactions among the system's components and it identifies safety constraints for such components [58]. This enables the analysis of more abstract systems whose technical and operational details have not been defined yet. Further, system hazards are identified in a more comprehensive way, based on the system's control structure [60]. Additionally, both Secure Tropos and STPA are top down approaches and facilitate the systemic analysis of the targeted system, early in the development phase. Accorddingly, Secure Tropos and STPA are chosen as the appropriate methods to combine in order to jointly study safety and security issues for CPSs.

This work proposes a method that addresses some of the identified limitations of existing alternatives:

- **Objectives-driven method:** To the best of our knowledge, none of the existing approaches analyzes a system and elicits requirements based on safety and security objectives. Doing so facilitates the *prioritization* of requirements, *communicating* them to relevant stakeholders, and *resolving conflicts* between safety and security requirements.

- **System models:** Security system models and safety system models can differ greatly, leading developers to take different views of the system, despite the fact that the underlying system is the same [12]. SafeSec Tropos allows the same model to be used for both safety and security analysis.

- **Documentation:** The documentation of the analyses can differ greatly between safety and security, thus making it difficult to find and compare requirements [12]. SafeSec Tropos provides similar documentation structures for both safety and security requirements, thus allowing easier identification of conflicts.

- **Conflict resolution:** The goal-oriented nature of SafeSec Tropos facilitates the resolution of potential conflicts between the safety and security requirements, as each requirement can be traced back to the objectives and goals that generated it.

- **Representation of complex systems:** SafeSec Tropos combines the graphical concepts of the Secure Tropos methodology and the systemic perspective of the STPA. This combination enables the representation and analysis of complex and interdependent systems such as those of the C-ES.

4. The SafeSecTropos method

Security and Safety *objectives* describe system features which ensure the system's security and safety. An essential step of the proposed method is the identification of these objectives for each system under analysis. *Constraint* is a restriction related to security/safety objectives which can influence the safety and security analysis and design of a CPS. A security/safety *dependency* introduces security/safety constraint(s) that must be realized to satisfy the corresponding dependency. A security/safety *entity* is a security/safety goal, a security/safety task, or a security/safety resource. A *safety goal* describes the requirement to ensure freedom from accidents/losses. *Safety constraints* are the restrictions in achieving the safety goals. Last, *safety tasks and resources* are the actions needed to achieve the safety goals, and information needed to perform the safety task, respectively. The proposed method integrates the elicitation of security and safety requirements by analyzing the system security and safety constraints in four phases, presented below. In doing so, it encompasses procedural elements of both SecureTropos and STPA. Specifically, it integrates Stage 2 of Secure Tropos with Steps 2 and 3 of STPA, and Stages 3 and 4 of Secure Tropos with Step 4 of STPA, as shown in Figure 1. In particular, during Stage 2, the control diagram has already been developed, and by following Steps 2 and 3 of STPA the safety constraints/objectives for each system are identified. Subsequently, the safety objectives are added to the existing Secure Tropos model, together with the security objectives. Finally, the final architecture of the targeted system along with its detailed design can be developed (Stages 2 and 3 of Secure Tropos), taking into account the causal factors that could lead to an unsafe action (Step 4 of STPA). The integration of the two approaches is depicted in Figure 2.

Phase 1 - Define the scope: The scope of the analysis is defined considering both system and environment characteristics. The involved stakeholders are identified, along with the pertinent legislation and standards. Further, their functions and operations are clarified as a step towards the development of the organizational model. The outcome of this phase is the analysis of the targeted ecosystem's background.

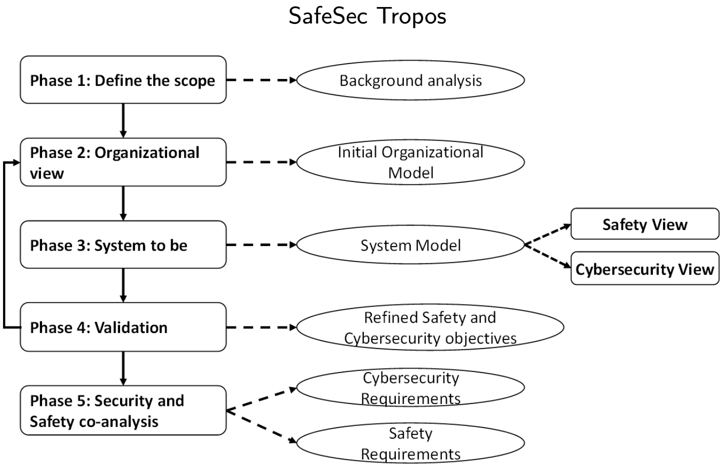

SafeSec Tropos
Phase 1: Define the scope
Background analysis
Phase 2: Organizational view
Initial Organizational Model
Phase 3: System to be
System Model
Safety View
Cybersecurity View
Phase 4: Validation
Refined Safety and Cybersecurity objectives
Phase 5: Security and Safety co-analysis
Cybersecurity Requirements
Safety Requirements

Figure 1: The SafeSecTropos Method

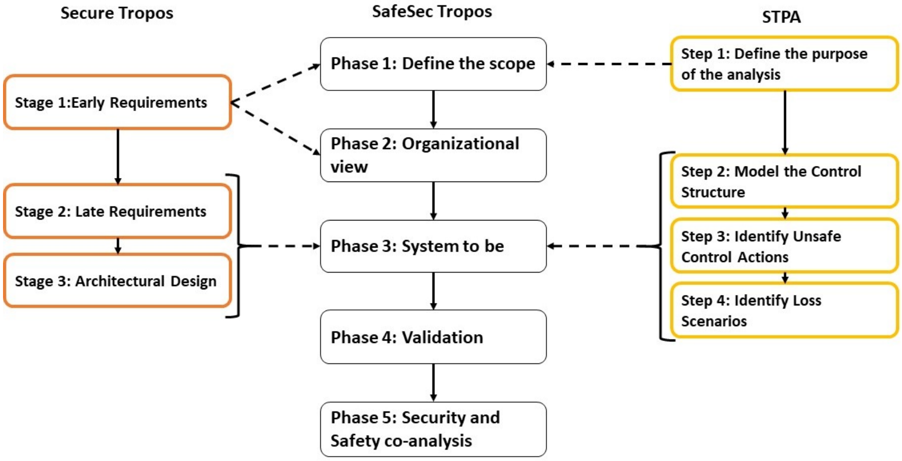

Secure Tropos
SafeSec Tropos
STPA
Stage 1:Early Requirements
Stage 2: Late Requirements
Stage 3: Architectural Design
Phase 1: Define the scope
Phase 2: Organizational view
Phase 3: System to be
Phase 4: Validation
Phase 5: Security and Safety co-analysis
Step 1: Define the purpose of the analysis
Step 2: Model the Control Structure
Step 3: Identify Unsafe Control Actions
Step 4: Identify Loss Scenarios

Figure 2: The SafeSecTropos Method

Phase 2 - Organizational View: The organizational model of the ecosystem is developed by considering the outcome of Phase 1. In this phase the stakeholders are modelled as actors, and their entities are identified. Such entities can be stakeholder's goals, plans, and resources, along with connections/ interconnections, and dependencies/ interdependencies.

Phase 3 - System-to-be: Modeling and description of the system-to-be. The system under analysis is modelled as an actor and its security and safety objectives are identified. In particular, the system's goals, entities, and processes are identified. Two distinct views are modelled, the safety view and the security view. The former represents system-level hazards and accidents, controller responsibilities, unsafe control actions, causal factors, and safety constraints. The latter depicts system-level vulnerabilities and threats, security entities, goals, and security constraints.

Phase 4 - Validation: The developed models are validated by considering the pertinent legislation, standards, and stakeholders. The outcome is a refined set of safety and security objectives.

Phase 5 - Security and Safety co-analysis: The security analysis for the target system is performed following the SecureTropos process, and the safety analysis following the STPA approach. The outcome of this phase is the set of the security requirements and the set of safety requirements. The prioritization of the security and safety requirements should be performed based on specific criteria. These criteria depend on the operational requirements of the system under study, the system architecture, and the validation that relevant stakeholders will perform. According to IEC 63069 [20] the resolution of possible conflicts between safety and security requirements should be performed by relevant stakeholders from both domains. This process is greatly facilitated by the fact that each requirement can be traced back to the objectve(s) that generated it.

5. The case of the C-ES

The CPSs of the C-ES have been selected as the use case of the proposed method because autonomous and remotely controlled vessels are already being extensively developed, and their safety and security requirements have not yet been well studied, in contrast to other domains such as e.g. autonomous vehicles. Furthermore, identifying such requirements is a stepping stone towards designing a secure architecture for such vessels, which will tackle both safety and security issues.

5.1. The C-ES ecosystem

The ICT components and the cyber-physical systems of the C-ES have been identified and analyzed in [26], where also a threat and risk analysis of such systems was carried out, and the most vulnerable onboard CPSs were identified. The most vulnerable onboard systems are the Automatic Identification System (AIS), the Electronic Chart Display System (ECDIS), and the Global Maritime Distress and Safety System (GMDSS) [26]. These are systems responsible for the safe and secure vessel operations.

- The *AIS* is an automated tracking system which facilitates vessel identification, monitoring, and locating. In addition, enhance the collision avoidance capabilities of the vessel. AIS transmits dynamic, voyage, static, and safety data to other vessel systems and to maritime authorities; such data are used to ensure the vessel's safety.
- The *ECDIS* is an information system that supports navigation by providing digital nautical charts, continuously determining the ship's position and unseen hazards. It transmits voyage, dynamic, and static data to facilitate the vessel's voyage and operations.
- The *GMDSS* aims to ensure the availability of the safety-related communication. By leveraging GMDSS the vessel communicates with the shore based station continuously, from any location. GMDSS consists of a set of systems and processes to handle emergencies.

These systems' interconnections, dependencies, and interdependencies were identified in [27] as a step towards eliciting the accordant security requirements in [3].

The stakeholders are the C-ES, the Shore Control Center (SCC), and Other Ships in the vicinity. The identified stakeholders are modelled as actors by leveraging the SecTro Tool. Further, the identification of their goals along with the interconnections, dependencies and interdependencies is performed. As legislation and standards for the autonomous/remotely controlled ships are still under development [28], in our analysis we considered the corresponding ones for conventional ships and systems. The analysis results in the initial organizational model of the targeted ecosystem as depicted in Figure 3. The C-ES includes the Bridge Automation system – BAS, and the Engine Automation System - EAS along with their subsystems.

- An *accident* is the undesired and unplanned event that results in a loss. For the C-ES ecosystem, the accidents [62, 63, 11, 7] are depicted in Table 1.
- A *hazard* is a system state or set of conditions that could lead to an accident (loss). By considering the accident list, the hazards that could lead to these accidents are listed in Table 1.

5.2. Safety and security objectives

The identification of the security and safety objectives facilitates the identification of the security and safety constraints. These objectives are leveraged in modeling the system-to-be towards the elicitation of the system's requirements. The security objectives are based on the *Parkerian Hexad* with the addition of *Non-Repudiation*, which reflects the system nature of the analysis. Although the Parkerian Hexad is based on the CIA model, the added objectives provide a more comprehensive way to study cybersecurity and data security [49]. Security is better ensured and more efficient countermeasures are designed when all of these six objectives are considered rather than just the CIA triad [54], [46]. These are adapted to fit the maritime domain. All objectives are determined taking into account the operational environment -hence the operational requirements- of each system under study.

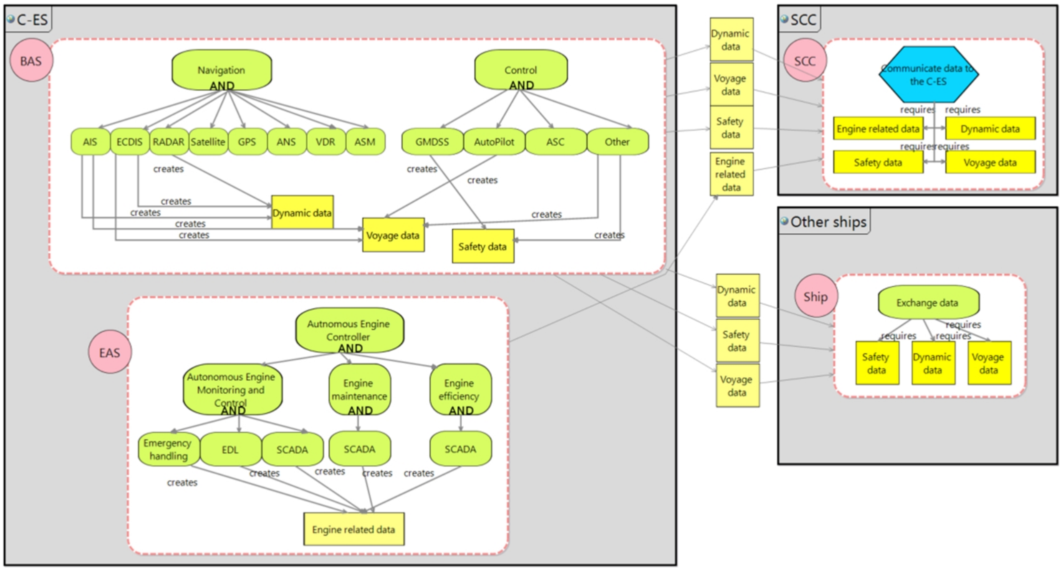


Figure 3: C-ES ecosystem: Organizational view

C-ES Accidents

A	Description
A1	Loss of human life or injury.
A2	Damage in the ship's infrastructure.
A3	Wide energy loss.
A4	Loss of ship's position.
A5	Loss of ship's control
A6	Loss of the communication links.
A7	Loss of cargo.
A8	Loss of the engine control.
A9	Loss of the control/monitoring of the propulsion/steering system.
A10	Loss of Navigational capabilities.
A11	Loss of ship's stability.
A12	Collision of the vessel with other human made or natural objects.
A13	Fire on board.
A14	Flooding/sinking
A15	Grounding
A16	Environment contaminated

C-ES Hazards

H	Description	Accidents
H1	Object detection sensor error.	A(1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16)
H2	Software failure.	All
H3	Technical fault (e.g. mechanical fault).	All
H4	Inability to handle harsh weather/sea conditions.	A(1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 14, 15, 16)
H5	Position reference equipment failure.	A(2, 4, 5, 6, 9, 12, 15)
H6	Overloading of the vessel.	A(1, 2, 5, 7, 10, 11, 14, 15, 16)
H7	Shifting of weights.	A(1, 2, 5, 10, 11, 13, 14, 15, 16)
H8	Ignition of electrical equipment or wiring.	All
H9	Passenger starting a fire.	All
H10	Unintended falling overboard.	A(1)
H11	Intended jumping overboard.	A(1)
H12	People getting injured/medical condition.	A(1)

Table 1
C-ES Accidents and Hazards

- **Confidentiality:** Information exchanged, and communication links between CPSs and services offered by CPSs should be protected against unauthorized access.
- **Integrity:** Information exchanged, services, CPSs, and communication links should be protected against unauthorized modifications or manipulations.
- **Availability:** Information exchanged, services, CPSs, and communication links should be available to authorized entities when requested by such entities.
- **Authenticity:** The management, the configuration, and operation of the onboard CPSs and services offered by

CPSs should be performed by authorized entities.

- **Possession and Control:** Information exchanged and communication links between CPSs and services offered by CPSs should be protected against the possibility that confidential data be possessed or controlled by unauthorized entities.
- **Utility:** Information exchanged and communication links between CPSs and services offered by CPSs should be useful.
- **Non-Repudiation:** CPSs should not refute responsibility.

Maritime safety is analyzed in [13] as part of transport and safety at sea. Maritime safety aims to protect life, health and property against environmental and operational risks. The safety objectives should ensure that hazards associated with each CPS are identified, tracked, evaluated, and eliminated through the entire system life cycle [24]. Industrial Control Systems attributes described in [32] and performance and security requirements described in [1] are also considered in identifying the maritime safety objectives. The following safety objectives apply.

- **Controllability:** The ability to bring a CPS's/vessel's process into a desired state and handle hazardous events during vessel's operations.
- **Observability:** CPSs should be able to determine their state to enhance the situational awareness of the SCC.
- **Operability:** The CPSs should be able to operate within the constraints imposed by the vessel's state.
- **Resilience:** The CPS's ability to absorb any disturbance caused by faults.
- **Survivability:** The CPS's ability to maintain the vessel's operations at some pre-defined acceptable level.
- **Graceful Degradation:** The CPSs should be able to maintain possibly limited but still safe functionality.
- **Quality of Service:** CPS's data should arrive in time and serve their purpose to perform the necessary safety functions and produce the safety messages that are needed.
- **Availability:** Capability of the CPS to provide a stated function if demanded under given conditions over its defined lifetime.
- **Redundancy:** The systems architecture of the C-ES should be redundant (CPSs, equipment, part, and data redundancy).
- **Fault tolerance:** The CPS of the C-ES should be operational without any interruption from system or software failure.
- **Integrity**: The vessel's CPSs and functions should be durable/stable.

5.3. Applying the SafeSecTropos method to onboard systems

The analysis of the ecosystem in the previous section facilitates the understanding of the systems under study, by providing potential accidents, hazards and the causes of these hazards. The vessel's ecosystem as depicted in Fig. 3 defines the stakeholders along with their interconnections and dependencies with the onboard systems. These remain the same for each individual onboard system under study. The analysis proceeds with the mapping of the identified accidents and hazards to the systems under study; these are used as an input to the STPA analysis. In order to illustrate the workings of the proposed method, we applied it to the AIS, the ECDIS and the GMDSS, these being the most vulnerable onboard systems. The resulting safety and security requirements are presented in Section 5.4. In the interest of saving space, the details of the intermediate steps of the method are presented only for the AIS.

Phase 1: The AIS provides static, dynamic, voyage and safety data, and helps authorities and other ships to monitor sea traffic. The involved stakeholders and their functions and operations are depicted in Fig. 3. Its interactions with other onboard systems and the environment are depicted in Fig. 4.

Phase 2: The organizational view of the AIS is depicted in Fig. 4. The SCC and Other Ships in the vicinity are modelled as system's stakeholders, as in Fig. 3. The onboard subsystems are depicted as separate actors which influence the operation of the AIS, according to their entities (operational and functional requirements). Control flows are exchanged between the AIS, the ECDIS, the Autonomous Navigation System (ANS), and the Collision avoidance system [27]. Therefore, three different control structures result, namely AIS-ANS; AIS-Collision Avoidance; and AIS-ECDIS. Again, in the interest of saving space, only the AIS-ANS control structure is discussed here, shown in Figure 5(a).

Phase 3: In this phase, the AIS goals (green boxes), entities, and resources (yellow boxes) are identified, along with the security and safety entities (red boxes), by considering Tables 1; these are depicted in Figure 5(a). The security and safety objectives described in Section 5 have been included in the organizational model derived in Phase 2, as shown in Figure 5(b).

Phase 4: The validation of the results derived from Phase 3 (safety and security views) is performed by domain (in

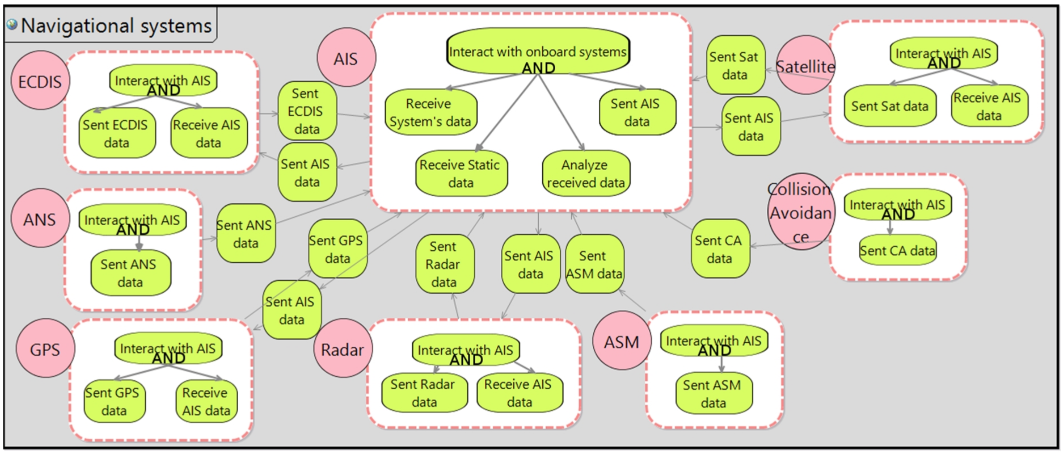
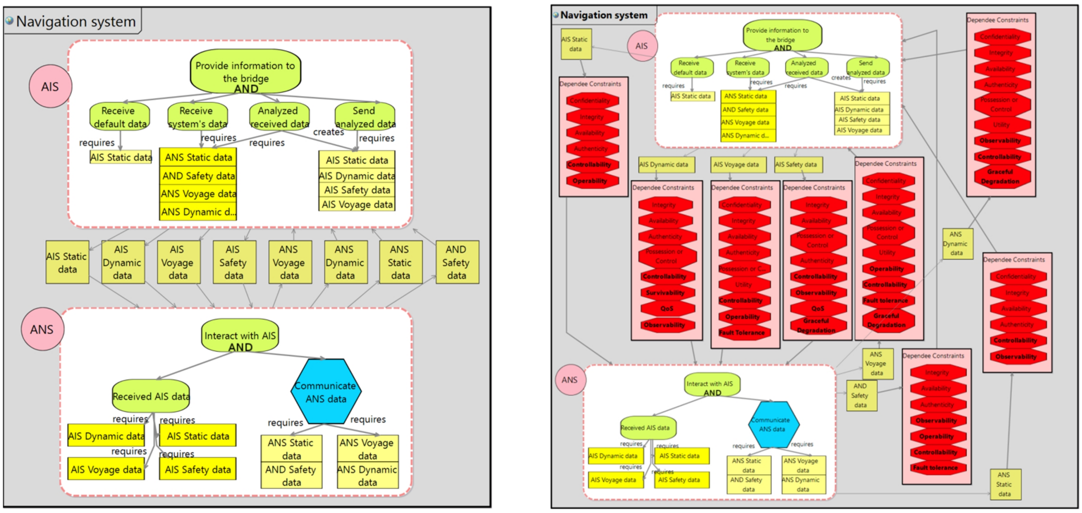


Figure 4: AIS organizational view



(a) Control structure/Safety View

(b) security and Safety objectives

Figure 5: AIS and ANS control structures

our case maritime) experts and relevant stakeholders, who are expected to consider the operational characteristics of autonomous systems, of which the analyst may have limited knowledge. These characteristics are the operational complexity, the environmental complexity, and the system complexity [61]. The former is related to system's deployment and how the system interacts with the surroundings. Environmental complexity captures the complexity of the mission and of the processes of the systems. The latter refers to the functional and operational complexity of the system itself. Both safety and security views should be equally analyzed to extract valid results. Particularly, system level hazards and threats should be identified at the same level of abstraction.

Phase 5: The security analysis of the AIS consists of the identification of the system's vulnerabilities, threats, security objectives, that lead to the identification of the security requirements. The security vulnerabilities for the AIS have been well examined in the literature [18, 6, 10]. Further, G. Kavallieratos et al. in [26] analyzed the security of the onboard ICT systems for the C-ES where potential attack scenarios have been developed by using the STRIDE method. Finally, the security objectives, together with the corresponding security requirements for the AIS, have been identified and analyzed in [3]. The STPA principles described in Section 3 are followed towards the safety analysis of the AIS. The identification of the safety goals and constraints requires the identification of AIS accidents and hazards;

AIS Accidents	
A1	Collision of the vessel
A2	Unable to control the vessel
A3	Unable to verify the ship's position
A4	Unable to verify the ship's identity

AIS Hazards	
H1	Software malfunction/error.
H2	Sensor malfunction/error
H3	High latency of the transmitting data
H4	Failure of AIS unit.

Table 2
AIS Accidents and Hazards

C1H1	No patched system.	C1H2	Wrong system's installation.
C2H1	Wrong system configuration.	C2H2	Sensors wrong readings.
C3H1	Lack of maintenance.	C3H2	Lack of sensors redundancy.
C1H3	Improper system configuration.	C1H4	Improper system configuration.
C2H3	Lack of sensors redundancy.	C2H4	Loss of power.
		C3H4	Software error.

Table 3
AIS Hazards Causes

these are depicted in Table 2. Furthermore, the potential causes of each hazard have been identified in Table 3 to analyze the safety environment of the targeted system and define the corresponding safety objectives.

AIS and ANS control structure: The Control Actions (CA) between the AIS and the ANS are depicted in Fig. 4. These are: CA1: Send AIS dynamic data to ANS; CA2: Send AIS static data to ANS; CA3: Send AIS voyage data to ANS; CA4: Send AIS safety data to ANS. Table 4 depicts the unsafe control actions between the AIS and the ANS, their consequences and the resulting system safety constraints. These lead to the following safety requirements for this control structure. The safety objectives that lead to each requirement follow the requirement in parentheses.

Safety requirements of the AIS-ANS control structure

- SafR1: AIS Dynamic data should be available to the ANS. (Availability, Controllability)
- SafR2: AIS Static data should be available to the ANS. (Availability, Controllability)
- SafR3: Voyage information such as destination port and ETA should be transmitted to the ANS.(Availability, Observability, Controllability, Operability, QoS)
- SafR4: Safety data should be sent to the ANS when needed. (Controllability, Observability, QoS)
- SafR5: The integrity of the transmitted data from the AIS to the ANS and vice versa should be ensured. (Integrity, Controllability, QoS)
- SafR6: Fire alerts should be sent within predefined time limits. (Availability, Survivability, Controllability)
- SafR7: Collision alerts should be transmitted to the ANS within specific time limits. (Availability, Survivability, Controllability)
- Safety alerts should follow a specific structure (eg. Fire/place/time/measures) (Integrity, Controllability, QoS)

5.4. Safety and security requirements of onboard systems

The safety requirements of each onboard system under study are identified by taking into account the safety constraints described in the STPA Tables (such as Table 4) for all relevant control structures. The requirements elicitation is performed by translating the identified safety constraints (e.g. Table 4) into requirements. For example *SafR9* aims to ensure the controllability, redundancy and observability of the AIS services and applications by providing redundancy of the installed sensors. This requirement aims to protect the system against loss of the vessel's control and loss of communication between the AIS and the systems that it interacts with, as a consequence of the Unsafe Control Action 1 - UCA1 depicted in Table 4. These are as follows:

5.4.1. AIS safety requirements

The list below describes the safety requirements of the AIS after the utilization of the SafeSec Tropos. The safety objectives that each requirement fulfills are shown in parenthesis. It can be seen that controllability and obervability are the most prominent objectives for the AIS.

- SafR1: The AIS should be able to send ship's positioning and speed data to the ECDIS. (Controllability, Ob-

	Control function is not provided	Unsafe control function is provided	Control function is provided in wrong time	Control function is provided for too short or too long
UCA1	AIS dynamic data are not provided to the ANS.	Wrong dynamic data are provided to the ANS.	The AIS dynamic data are provided too soon or too late to the ANS.	Not all AIS dynamic data are provided to the ANS.
UCA2	AIS static data are not provided to the ANS.	Wrong IMO number is provided to the ANS.	AIS static data are provided to the ANS after the entrance to a port.	
UCA3	1) The destination and ETA of the vessel are not provided to the ANS. 2) The ship's draught is not provided to the ANS. 3) The type of the cargo is not provided.	Wrong voyage related data are fed to the ANS.	The AIS voyage data are provided too late to the ANS.	
UCA4	Safety related messages are not sent to the ANS.	1) False fire alert is sent to the ANS. 2) False flooding alert is sent to the ANS. 3) False collision alert is sent to the ANS.	1) Fire alert is sent out of the predetermined time limits. 2) Collision alert is provided to the ANS after the collision.	Fire alert is provided without some details (e.g. missing location).
Conseq.				
CUCA1	1) The ANS is not able to control the vessel. 2) Loss of the communication between the AIS and the ANS. 3) The ANS cannot control the vessel's speed.	1) The ANS suggests the increase/decrease of the vessel's speed. 2) The ANS changes the vessel's heading (misdirection).	1) Loss of ship's position. 2) The ANS is not able to get the navigational status of the vessel.	The ANS cannot continuously communicate with the AIS.
CUCA2	The AIS cannot be authenticated to the ANS.	Insufficient vessel authentication to the ANS.	The ANS cannot control the navigation commands properly.	
CUCA3	The ANS is not able to provide navigational control commands to its sub systems.	Misdirection of the vessel.	1) The ship may enter to no go area. 2) Disruption of vessel's procedures. 3) Vessel's inability to reach port of destination in expected time	
CUCA4	The ANS is not able to provide the necessary functions to address emergencies.	Disruption of vessel's operations.	1) Damage to the ship's infrastructure. 2) Loss of life.	The ANS is not able to send the necessary commands to address the emergencies.

Table 4
AIS to ANS safety constraints

servability, QoS)

- SafR2: The AIS should be able to send vessel's identification data to the ECDIS. (Controllability, Accessibility, Observability)
- SafR3: The integrity of the charts should be ensured. (Controllability, QoS)
- SafR4: The data sent to ECDIS should be regularly updated. (Operability, Observability, Controllability)
- SafR5: Route and the destination port data of the vessels should be transmitted to the ECDIS. (Observability, Operability, Availability, Controllability)
- SafR6: The necessary AIS data should be provided to the ECDIS to avoid confusion of the system functions. (Observability, Controllability)
- SafR7: The AIS must be patched in case of system vulnerabilities or errors. (Observability, QoS, Controllability, Operability)
- SafR8: The installation and configuration of the AIS must be performed via well trained personnel. (Observability, QoS, Controllability)
- SafR9: The redundancy of the installed sensors should be ensured. (Controllability, Redundancy, Observability)
- SafR10: The power supply of the AIS should be continuous. (Availability, Operability, Controllability)

5.4.2. ECDIS safety requirements

By applying the proposed methodology for the ECDIS, the following safety requirements have been identified by considering the interaction of the targeted system with other onboard CPSs. We notice that availability and QoS are the most prominent safety objectives for the ECDIS.

- SafR1: The redundancy of the installed ECDIS sensors should be ensured. (Redundancy, Controllability, QoS)
- SafR2: Dynamic, Safety, and Voyage data transmitted to the Autonomous Ship Controller (ASC) should be available. (Availability, Observability)
- SafR3: The integrity of the Dynamic, Voyage and Safety data should be ensured. (Integrity, QoS)
- SafR4: Emergency procedures should be initiated when are needed. (Operability, Graceful Degradation)

- SafR5: ECDIS data should be transmitted to the ASC and the ANS in time. (Availability, QoS)
- SafR6: Static data should be provided to the ANS. (Controllability, Operability, Availability)
- SafR7: The authentication of the vessel to the ANS should be ensured. (QoS, Observability)
- SafR8: The integrity of the static data transmitted to ANS should be maintained. (Integrity, QoS)

5.4.3. GMDSS safety requirements

SafeSec Tropos identified the six safety requirements for the GMDSS listed below. Various safety objectives are fulfilled by the identified requirements, since GMDSS is an onboard system that aims to ensure safety during the voyage. As such, different objectives are met by fulfilling the safety requirements.

- SafR1: The availability of the distress signals should be ensured. (Availability, Operability)
- SafR2: The integrity of the transmitted distress signals should be ensured. (Integrity, Observability, Operability)
- SafR3: The Authenticity of the transmitted safety data should be ensured. (Controllability, Operability, Observability)
- SafR4: The redundancy of the communication links between ship to ship and ship to shore should be ensured. (Redundancy, Operability, Availability)
- SafR5: The controllability of the transmitted data and signals should be ensured. (Controllability, Operability, Observability)
- SafR6: The survivability and timeliness of the transmitted safety data should be ensured. (Survivability, Controllability, QoS)

The security requirements for the onboard systems of the C-ES have been identified in [3] by leveraging the Secure Tropos methodology. These are listed below.

5.4.4. AIS security requirements

- SecR1: The AIS should implement the security services in order to protect the system from loss of control or possession of information. (Confidentiality, Authenticity, Possession and Control)
- SecR2: Voyage data such as destination port or cargo related information should be confidential to prevent potential leakage to adversaries. (Confidentiality, Integrity)
- SecR3: The communication channel with the radar system should be redundant. (Availability, Utility)
- SecR4: Voyage related data transmitted to the SCC must be protected against tampering or damage. (Integrity, Availability)
- SecR5: 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. (Authenticity, Utility, Non-Repudiation)
- SecR6: 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. (Confidentiality, Authenticity, Possession and Control, Utility)
- SecR7: The freshness of the dynamic, voyage and safety data should be established. (Availability, Utility)
- SecR8: The configuration and installation of the AIS must be performed by authorized personnel. (Confidentiality, Integrity, Possession and Control, Authenticity)
- SecR9: A suitable amount of AIS sensors should be installed considering the operational mission of the vessel to ensure the redundancy of the AIS. (Availability, Utility)

5.4.5. ECDIS security requirements

- SecR1: The ECDIS administrator must be trained and able to distinguish rogue data packets.(Integrity, Authenticity, Utility)
- SecR2: The use of ECDIS must be restricted only to authorized and well trained personnel. Confidentiality, Integrity, Authenticity, Possession and Control
- SecR3: The ECDIS must be able to control the flows of voyage-related data sent to other ships and to the SCC. (Integrity, Possession and Control, Utility)
- SecR4: The ECDIS should be able to audit sent and received data to external actors. (Integrity, Authenticity, Possession and Control, Utility)
- SecR5: Safety-related information transmitted by the ECDIS must be authenticated. (Integrity, Authenticity, Non-repudiation)

- SecR6: The communication between the ECDIS and the satellite system should be continuously available. (Availability, Utility)

5.4.6. GMDSS security requirements

- SecR1: The authenticity of the transmitted GMDSS signals and data in transit to the ASC, to other subsystems, and to the SCC must be ensured. (Integrity, Authenticity, Non-repudiation)
- SecR2: Distress signals transmitted through the GMDSS must be verified by external actors such as the SCC and other ship's subsystems such as the Autonomous Engine Monitoring and Control (AEMC) and Navigation systems. (Authenticity, Integrity, Utility)
- SecR3: The ASC must be able to provide security, safety, and dynamic data to the GMDSS, when needed. (Availability, Utility)
- SecR4: Safety signals transmitted through the GMDSS to other on board systems and external actors must be continuously available. (Availability, Integrity, Utility)
- SecR5: The GMDSS must be able to detect whether the signal/data comes from a legitimate user/system or from a malicious user. (Confidentiality, Integrity, Authenticity, Non-repudiation)
- SecR6: The signals transmitted to external actors or subsystems must be appropriately encrypted. (Confidentiality, Integrity)
- SecR7: GMDSS antennas must be appropriately installed. (Availability, Utility)

6. Discussion - Challenges, Issues and Observations

Regarding the safety and security requirements derived through the application of SafeSec Tropos to the C-ES case, we note that:

- **Overlapping requirements:** Some safety requirements overlap with security requirements. For example, in the case of the AIS these are: (i) **Saf**R4 with **Sec**R7, (ii) **Saf**R8 with **Sec**R8, and (iii) **Saf**R9 with **Sec**R9. It is noteworthy that similarities can be found in requirements that derive from the availability, integrity, redundancy, and quality of service objectives. Further, the overlapping requirements share the same safety and security goals. The prioritization of the overlapping requirements should be done considering specific criteria described in Section 4.

- **Grouping requirements:** Several requirements, applicable to all systems, can be grouped together to form *Generic requirements*. The remaining requirements will form sets of *System-specific requirements*. This grouping facilitates the communication and the prioritization of the requirements during the architecture definition and implementation phase. Further, the safety and security measures to implement such requirements can follow the same classification; thus their management and implementation process is facilitated.

- **Conflicting requirements:** No obvious requirements conflicts have been identified. This may be attributed to the specificities of the system under study, but also to the careful, non-conflicting, selection of the safety and security objectives and goals that SafeCec Tropos allows.

- **Applicability to C-ES variants:** SafeSec Tropos can capture the differences between different autonomy levels, by modeling the interactions, dependencies and interdependencies of the model components of different vessel types (conventional, remote controlled, autonomous).

- **Validation:** The lack of standards and legislation for autonomous ships and for the joint analysis of safety and security, the validation of safety and security views in Phase 3 of SafeSec Tropos was performed by considering the relevant literature, and security [22] and safety standards [23]. The models derived from phase 3, were validated by considering the operational, environmental, and system complexity of the CPSs under study.

7. Conclusions

In this paper, an integrated approach for safety and security requirements engineering has been proposed. The proposed SafeSec Tropos method facilitates the joint analysis of safety and security by modeling the system for both purposes under the same model and providing documentation regarding the potential conflicts of the identified requirements. These conflicts can be resolved by tracing them back to the corresponding safety and security objectives. Further, complex systems can be analyzed by leveraging the modeling language of the Secure Tropos and the system perspective of the STPA. The safety and security objectives in the maritime domain have been identified towards the identification of cyber physical systems safety and security requirements. Due to the complex nature of such systems, a graphical-based model is proposed by leveraging the existing SecTro tool. The ecosystem of the Cyber-Enabled Ship is used to demonstrate the applicability of the proposed method. The three most vulnerable onboard systems, namely the AIS, the ECDIS, and the GMDSS have been analyzed and their safety and security requirements have been identified.

As future work we plan to define a safety and security architecture compliant to the identified requirements. Such an architecture would possibly include automated incident response mechanisms [36] to handle the critical incidents that may occur in the vessel's infrastructure. The identification and modelling of the appropriate security and safety measures will facilitate the design and the installation of safe and secure by design systems in critical infrastructures such as the C-ES. Furthermore, it is important to study and explore how potential changes in one set of requirements affects both sets and how this can be done in an iterative fashion. Additionally, in our future work we plan to verify the applicability and usefulness of the SafeSec Tropos along with its claimed advantages in other reference architectures and domains where the emerging technology of the cyber-physical systems also exists. Such domains could be autonomous vehicles, smart homes [15], and various fields within Industry 4.0 [41]. Finally, due to the increasing development of CPSs for the maritime domain to facilitate port, vessel, and many logistics operations, it is important to make concrete proposals for creating a standard for safety and security in the maritime domain, similar to e.g. IEC TR63069:2019 [20].

References

[1] C. Alcaraz and J. Lopez. Analysis of requirements for critical control systems. *International journal of critical infrastructure protection*, 5(3-4):137–145, 2012.

[2] S. Ali, T. Al Balushi, Z. Nadir, and O. K. Hussain. Standards for CPS. In *Cyber Security for Cyber Physical Systems*, pages 161–174. Springer, 2018.

[3] anonymized. under revision. 2019.

[4] P. Asare, J. Lach, and J. A. Stankovic. FSTPA-I: A formal approach to hazard identification via system theoretic process analysis. In *Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems*, pages 150–159. ACM, 2013.

[5] F. Asplund, J. McDermid, R. Oates, and J. Roberts. Rapid integration of CPS security and safety. *IEEE Embedded Systems Letters*, 11(4):111–114, 2019.

[6] M. Balduzzi. AIS Exposed Understanding Vulnerabilities Attacks 2.0. In *Blackhat, Asia, 2014*, page 44, 2014.

[7] O. A. V. Banda and S. Kannos. Hazard analysis process for autonomous vessels. Technical report, 2017.

[8] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos. Safety related cyber-attacks identification and assessment for autonomous inland ships. In *International Seminar on Safety and Security of Autonomous Vessels (ISSAV)*, September 2019.

[9] V. Bolbot, G. Theotokatos, L. M. Bujorianu, E. Boulougouris, and D. Vassalos. Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review. *Reliability Engineering System Safety*, 182:179 – 193, 2019.

[10] D. Bothur, G. Zheng, and C. Valli. A critical analysis of security vulnerabilities and countermeasures in a smart ship system. *In Proceedings of 15th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia. (pp.81-87)*, 2017.

[11] DNV-GL. Autonomous and remotely operated ships, class guideline. Technical report, 2018.

[12] D. P. Eames and J. Moffett. The integration of safety and security requirements. In *International Conference on Computer Safety, Reliability, and Security*, pages 468–480. Springer, 1999.

[13] K. Formela, A. Weintrit, and T. Neumann. Overview of definitions of maritime safety, safety at sea, navigational safety and safety in general. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 13, 2019.

[14] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer. STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*, 34:183 – 196, 2017.

[15] K. Ghirardello, C. Maple, D. Ng, and P. Kearney. Cyber security of smart homes: Development of a reference architecture for attack surface analysis. In *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, pages 1–10, March 2018.

[16] J. Glomsrud and J. Xie. A Structured STPA Safety and Security Co-analysis Framework for Autonomous Ships. *Safety and Reliability–Safe Societies in a Changing World. Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway*, 2019.

[17] N. H. C. Guzman, D. K. M. Kufoalor, I. Kozin, and M. A. Lundteigen. Combined safety and security risk analysis using the UFoI-E method: A case study of an autonomous surface vessel. In *29th European Safety and Reliability Conference*, pages 4099–4106, 2019.

[18] J. Hall, J. Lee, J. Benin, C. Armstrong, and H. Owen. IEEE 1609 Influenced Automatic Identification System (AIS). In *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, pages 1–5, 2015.

[19] International Electrotechnical Commission. Functional safety - Safety instrumented systems for the process industry sector, IEC 61511 . Technical report, 2016.

[20] International Electrotechnical Commission. Industrial-process measurement control and automation, Framework for functional safety and security IEC 63069:2019. Technical report, 2019.

[21] International Maritime Organization . IMO takes first steps to address autonomous ships. `http://www.imo.org/en/mediacentre/pressbriefings/pages/08-msc-99-mass-scoping.aspx`, 2018.

[22] International Organization for Standardization (ISO). Information technology — Security techniques — Information security management systems, ISO 27000 series. Technical report, 2016.

[23] International Organization for Standardization (ISO). Road vehicles — Functional safety, ISO 26262-1:2018. Technical report, 2018.

[24] Joint Software System Safety Committee. Software system safety handbook, a technical managerial team approach. Technical report, 1999.

[25] N. Karanikas. Revisiting the relationship between safety and security. *International journal of safety and security engineering*, 8(4):547–551, 2018.

[26] G. Kavallieratos, S. Katsikas, and V. Gkioulos. Cyber-attacks against the autonomous ship. In *Computer Security*, pages 20–36, Cham, 2019. Springer International Publishing.

[27] G. Kavallieratos, S. Katsikas, and V. Gkioulos. Modelling shipping 4.0: A reference architecture for the cyber-enabled ship. In *Proceedings of the 12th Asian Conference on Intelligent Information and Database Systems*, 2020.

[28] A. Komianos. The autonomous shipping era. operational, regulatory, and quality challenges. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 12, 2018.

[29] L. Kretschmann, Ø. J. Rødseth, B. S. Fuller, H. Noble, J. Horahan, and H. McDowell. MUNIN D9.3: Quantitative assessment. Technical report, 2015.

[30] L. Kretschmann, Ø. J. Rødseth, A. Tjora, B. S. Fuller, H. Noble, and J. Horahan. MUNIN D9.2: Qualitative assessment. Technical report, 2015.

[31] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand. A survey of approaches combining safety and security for industrial control systems. *Reliability engineering & system safety*, 139:156–178, 2015.

[32] M. Krotofil, K. Kursawe, and D. Gollmann. Securing industrial control systems. In *Security and Privacy Trends in the Industrial Internet of Things*, pages 3–27. 2019.

[33] N. Leveson. *Engineering a safer world: Systems thinking applied to safety*. MIT press, 2011.

[34] N. Leveson and J. Thomas. STPA handbook. 2018.

[35] E. Lisova, I. Šljivo, and A. Čaušević. Safety and security co-analyses: A systematic literature review. *IEEE Systems Journal*, 13(3):2189–2200, Sep. 2019.

[36] J. Lopez, C. Alcaraz, and R. Roman. Smart control of operational threats in control substations. *Computers & Security*, 38:14–27, 2013.

[37] M. A. Lundteigen and B. A. Gran. The need of improved methods to handle functional safety and cybersecurity in industrial control and safety systems.

[38] X. Lyu, Y. Ding, and S.-H. Yang. Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications*, 2019.

[39] N. R. Mead. How to compare the security quality requirements engineering (square) method with other methods. Technical report, Carnegie-Mellon University, 2007.

[40] D. Mellado, C. Blanco, L. E. Sánchez, and E. Fernández-Medina. A systematic review of security requirements engineering. *Computer Standards & Interfaces*, 32(4):153–165, 2010.

[41] H. Mouratidis and V. Diamantopoulou. A security analysis method for industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(9):4093–4100, 2018.

[42] H. Mouratidis and P. Giorgini. Secure tropos: a security-oriented extension of the tropos methodology. *International Journal of Software Engineering and Knowledge Engineering*, 17(02):285–309, 2007.

[43] 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 *International Conference on Availability, Reliability, and Security*, pages 79–93. Springer, 2014.

[44] A. Nhlabatsi, B. Nuseibeh, and Y. Yu. Security requirements engineering for evolving software systems: A survey. In *Security-aware systems applications and software development methods*, pages 108–128. IGI Global, 2012.

[45] T. Novak and A. Treytl. Functional safety and system security in automation systems-a life cycle model. In *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, pages 311–318. IEEE, 2008.

[46] D. B. Parker. Toward a new framework for information security? *Computer security handbook*, pages 3.1 – 3.23, 2012.

[47] S. Paul and L. Rioux. Recommendations for security and safety co-engineering (release n 2). *WIT Transactions on The Built Environment*, 151:335 – 349, 2015.

[48] M. Pavlidis, S. Islam, and H. Mouratidis. A case tool to support automated modelling and analysis of security requirements, based on secure tropos. In *International Conference on Advanced Information Systems Engineering*, pages 95–109. Springer, 2011.

[49] G. Pender-Bey. The parkerian hexad, master's thesis. Technical report, 2016.

[50] D. Pereira, C. Hirata, R. Pagliares, and S. Nadjm-Tehrani. Towards combined safety and security constraints analysis. In S. Tonetta, E. Schoitsch, and F. Bitsch, editors, *Computer Safety, Reliability, and Security*, pages 70–80, Cham, 2017. Springer International Publishing.

[51] L. Piètre-Cambacédès and M. Bouissou. Modeling safety and security interdependencies with bdmp (boolean logic driven markov processes). In *2010 IEEE International Conference on Systems, Man and Cybernetics*, pages 2852–2861. IEEE, 2010.

[52] N. Polatidis, M. Pavlidis, and H. Mouratidis. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*, 56:74–82, 2018.

[53] C. Raspotnig and A. Opdahl. Comparing risk identification techniques for safety and security requirements. *Journal of Systems and Software*, 86(4):1124 – 1151, 2013. SI : Software Engineering in Brazil: Retrospective and Prospective Views.

[54] R. C. Reid and A. H. Gilbert. Using the parkerian hexad to introduce security in an information literacy class. In *2010 Information Security Curriculum Development Conference*, pages 45–47, 2010.

[55] S. Sadvandi, N. Chapon, and L. Pietre-Cambacédes. Safety and security interdependencies in complex systems and SoS: Challenges and perspectives. In *Complex Systems Design & Management*, pages 229–241. Springer, 2012.

[56] M. Z. Schmittner, C. and P. Puschner. Limitation and improvement of STPA-Sec for safety and security co-analysis. In *Proceedings of the SAFECOMP 2016 Workshops*, LNCS 9923, pages 195 —- 209. Springer, 2016.

[57] L. Shan, B. Sangchoolie, P. Folkesson, J. Vinter, E. Schoitsch, and C. Loiseaux. A survey on the applicability of safety, security and privacy standards in developing dependable systems. In *International Conference on Computer Safety, Reliability, and Security*, pages 74–86. Springer, 2019.

[58] S. M. Sulaman, A. Beer, M. Felderer, and M. Höst. Comparison of the fmea and stpa safety analysis methods–a case study. *Software Quality Journal*, 27(1):349–387, 2019.

[59] M. Sun, S. Mohan, L. Sha, and C. Gunter. Addressing safety and security contradictions in cyber-physical systems. In *Proceedings of the 1st Workshop on Future Directions in Cyber-Physical Systems Security (CPSSW'09)*. Citeseer, 2009.

[60] E. N. Torkildson, J. Li, S. O. Johnsen, and J. A. Glomsrud. Empirical studies of methods for safety and security co-analysis of autonomous boat. *Safety and Reliability–Safe Societies in a Changing World. Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway*, 2018.

[61] I. B. Utne, A. J. Sørensen, and I. Schjølberg. Risk management of autonomous marine systems and operations. In *ASME 2017 36th International Conference on Ocean, Offshore and Arctic Engineering*. American Society of Mechanical Engineers Digital Collection, 2017.

[62] K. Wróbel, J. Montewka, and P. Kujala. System-theoretic approach to safety of remotely-controlled merchant vessel. *Ocean Engineering*, 152:334–345, 2018.

[63] K. Wróbel, J. Montewka, and P. Kujala. Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. *Reliability Engineering & System Safety*, 178:209–224, 2018.

[64] W. Young and N. Leveson. Systems thinking for safety and security. In *Proceedings of the 29th Annual Computer Security Applications Conference*, ACSAC '13, pages 1–8, New York, NY, USA, 2013. ACM.