International Journal of Information Security (2023) 22:249–288
https://doi.org/10.1007/s10207-022-00638-y

REGULAR CONTRIBUTION

Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth

Ahmed Amro[1] · **Vasileios Gkioulos**[1]

Published online: 23 November 2022

Abstract
Recent innovations in the smart city domain have led to the proposition of a new mode of transportation utilizing Autonomous Passenger Ships (APS) or ferries in inland waterways. The novelty of the APS concept influenced the cyber risk paradigm and led to different considerations regarding attack objectives, techniques as well as risk management approaches. The main factor that has led to this is the autoremote operational mode, which refers to autonomous operations and remote supervision and control in case of emergency. The autoremote operational mode influences the risk of cyber attacks due to the increased connectivity and reliance on technology for automating navigational functions. On the other hand, the presence of passengers without crew members imposes a safety risk factor in cyber attacks. In this paper, we propose a new cyber risk management approach for managing the cyber risks against cyber physical systems in general and Autonomous Passenger Ships in particular. Our proposed approach aims to improve the Defense-in-Depth risk management strategy with additional components from the Threat-Informed Defense strategy allowing for more evolved cyber risk management capabilities. Moreover, we have utilized the proposed cyber risk management approach for the proposition of a cybersecurity architecture for managing the cyber risks against an APS use case named milliAmpere2. Additionally, we present our results after conducting a Systematic Literature Review (SLR) in cybersecurity evaluation in the maritime domain. Then, the findings of the SLR were utilized for a suitable evaluation of the proposed risk management approach. Our findings suggest that our proposed risk management approach named Threat-Informed Defense-in-Depth is capable of enriching several risk management activities across different stages in the system development life cycle. Additionally, a comprehensive evaluation of the cybersecurity posture of milliAmpere2 has been conducted using several approaches including risk evaluation, simulation, checklist, and adversary emulation. Our evaluation has uncovered several limitations in the current cybersecurity posture and proposed actions for improvement.

Keywords Autonomous Passenger Ship · Cybersecurity architecture · $ATT\&CK$ · Defense-in-Depth · Cyber risk Management

1 Introduction

In a constantly evolving globe, technological advances improve every aspect of modern life. In the maritime domain, automation and digitalization are constantly evolving leading to drastic changes in business models, processes, as well as technology [1]. The impact of the current pandemic has been observed clearly in the maritime transportation sector in the form of a drastic decrease in passengers in 2020 compared to 2019 [2]. At the same time, to adjust to the post-pandemic normal, the development of innovative technologies and services for the transportation community has been proposed. It is already undergoing in the maritime industry to make it greener, cheaper, and more efficient. The pandemic has even emphasized that role [3]. Also, the US Bureau of Transportation Statistics has argued that the increasing demand for extending the capacity and flexibility of transportation systems has fueled the development of innovative technologies and services [4].

Recent innovations in maritime logistics when meeting activities related to smart city development have led to the creation of innovation in the field of inland passenger transportation through the proposition of Autonomous Passenger

✉ Ahmed Amro
ahmed.amro@ntnu.no

Vasileios Gkioulos
vasileios.gkioulos@ntnu.no

[1] Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway

Ships (APS) (i.e., ferries). Domestic water transportation in Norway has witnessed the largest increase in passengers during the period between 2015 and 2019 [5]. In that direction, multiple projects have been recently initiated toward the development of autonomous passenger ferries in three regions in Norway [6]. Among these projects is a project named Autoferry which aims to develop an all-electric APS for inland water transport in the city of Trondheim [7]. The work presented in this paper originated from and is part of the Autoferry project. The targeted APS is planned to be autonomous with remote control and monitoring capabilities leading to an unconventional mode of operation in the maritime domain which is referred to as "autoremote" [8]. Although the new operational mode is expected to improve the provisioning of navigational services, it introduced a range of cyber threats with potential safety impacts. Toward addressing such issues, several system-specific requirements have been established during the authors' earlier work [9]. The established requirements were communicated by the identified APS stakeholders with a prime focus on communication reliability and cybersecurity toward safe operations. Toward addressing these requirements, a communication architecture for the APS has been proposed to satisfy the communication-related requirements [10]. This paper on the other hand addresses the cybersecurity requirements through the development of a cybersecurity architecture complementing the previously proposed communication architecture.

The identified stakeholders' requirements and concerns related to cybersecurity can be addressed by a cybersecurity architecture that provides risk management functions, including risk analysis, treatment, and monitoring. Moreover, autonomous ships are expected to include a group of industrial control systems (ICS) and cyber physical systems (CPS) participating in the provisioning of autonomous and remote control and monitoring functions. For this, the concept of layered defenses; formally known as Defense-in-Depth (DiD) is a proposed security strategy for risk management in critical systems [11] and in autonomous and remotely controlled vessels [8, §11]. Despite that, some concerns have been raised regarding the ability of DiD to withstand sophisticated attacks [12] as well as its lack of a Cyber Threat Intelligence (CTI) component that allows organizations to continuously enhance their defenses to match the ever-changing threat landscape [13]. At the same time, CTI is one of the components of another cybersecurity strategy named Threat-Informed Defense [14]. In this paper, we investigate the utility of combined implementation of the Threat-Informed Defense and DiD as a risk management strategy in a maritime use case that is the APS.

The contributions in this paper can be summarized as follows:

- We propose a new risk management approach named Threat- Informed Defense-in-Depth that combines components from two cybersecurity strategies, namely Threat-Informed Defense and Defense-in-Depth.
- We present a cybersecurity architecture for APS that is an outcome of the Threat-Informed Defense-in-Depth approach.
- We present the results of our SLR regarding cybersecurity evaluation in the maritime domain highlighting different aspects and approaches.
- We present the results of the conducted cybersecurity evaluation processes for an operational ferry that is a prototype implementation of APS.
- We discuss the observed challenges in carrying cyber risk management functions in the context of the autoremote operational mode.

2 Background

2.1 Maritime cyber risk management

The International Maritime Organization (IMO) has issued resolution MSC. 428(98) [15] regarding the consideration of cyber risk management within the safety management systems of the different entities in the maritime industry. In this direction, IMO issued guidelines for cyber risk management [16]. The guidelines suggest several relevant frameworks and resources including the Framework for Improving Critical Infrastructure Cybersecurity by the National Institute of Standards and Technology (NIST) [17]. Additionally, several entities in the maritime domain have discussed approaches to cyber risk management, BIMCO; a global organization for shipowners, charterers, ship brokers, and agents, and DNV; a member of the maritime classification society. The concept of layered defenses known as the Defense-in-Depth (DiD) is the agreed-upon and encouraged strategy among these institutions.

DiD is defined by NIST as an "Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization" [18]. A survey of cyber reference architectures and frameworks conducted by Savold et al [19] highlighted that DiD as a security design pattern that is observed in several security frameworks such as the Cisco SAFE [20], Oracle Reference Architectures [21], and Northrop Grumman Fan. [22]. Nevertheless, different DiD implementations focused more on Information Technology (IT) systems with the tendency to overlook Operational Technology (OT) systems. For that sake, the department of homeland security in the united states has issued a document for recommended practice as guidance for developing a DiD security program for environments with

industrial control systems (ICS) [23]. The document provides a detailed description of the DiD strategy from several viewpoints referred to as defense layers. Also, BIMCO provided guidelines for cyber risk management on board ships and discussed the strategy of DiD as well as Defense-in-Breadth (DiB); referring to the consideration of different technology domains, namely IT and OT in the cyber risk management. BIMCO proposed a risk management approach including a group of defense layers [24]. Additionally, DNV has suggested the adoption of a DiD strategy for the cybersecurity of autonomous and remotely controlled vessels and discussed several components of a cybersecurity management system that can be adapted to support the strategy [8, §11].

After surveying the literature regarding cyber risk management approaches in the maritime domain, the adoption of layered defenses has been observed. To mention a few, Svilicic et al [25] proposed and conducted a novel cyber risk assessment on board a vessel. The authors surveyed the vessel cybersecurity management system consisting of several defense layers including, physical access, patching, access control, and others. Grigoriadis et al [26] proposed a group of defenses for improving the cybersecurity of ports including vulnerability assessment, communication authenticity, weak password protection, and binary protection. Kavallieratos et al [27] leveraged the STRIDE and DREAD risk analysis techniques to assess cyber risks in cyber-enabled ships, which include autonomous and remotely controlled ships. The authors then followed the ISO 31000 risk management process [28] to propose baseline controls to mitigate the identified risks. The authors relied on the controls suggested by the Guide to industrial control systems (ICS) security [29].

Rajaram et al [30] have proposed guidelines for cyber risk management for shipboard systems with more focus on operational technology. The authors proposed a checklist approach for determining the cyber hygiene of vessels. The approach introduced the concept of security tiers which are aligned with risk priority levels, specifically, low, medium, and high. The concept of security tiers reflects the necessity for implementing security controls to address certain levels of risk.

However, the observed works lacked a clear implementation of the DiD strategy for ensuring that all layers of defenses are systematically considered. Therefore, in this paper, we utilize the DiD as an architecture framework during cybersecurity architecture development. The defense layers are collected from several sources including the DiD guidelines for ICS in [23], DNV [31], and BIMCO [24]. Additionally, some works in the literature provide valuable artifacts including candidate non-developmental items (NDIs), architectural elements' properties, features as well as their interconnections.

2.2 The *ATT&CK* framework

The Adversarial Tactics, Techniques, and Common Knowledge from MITRE, shortly known as the $ATT\&CK$ framework [32], is a recent, widely adopted framework in both academia and the cybersecurity industry. Currently, it encompasses three technology domains which are referred to as matrices, namely enterprise, mobile, and industrial control systems (ICS). The enterprise matrix covers Information Technology (IT) systems observed in enterprise networks. The mobile matrix covers handheld or mobile devices with Android or IOS. The ICS matrix covers networks and systems with Operational Technology (OT). This inclusion of several technology domains makes $ATT\&CK$ suitable in a wide range of use cases including the composition of these technologies. Additionally, the $ATT\&CK$ terminologies are utilized for mapping adversarial activities by many organizations such as the European Union Agency for Cybersecurity (ENISA) in their annual threat landscape report [33]. Moreover, the $ATT\&CK$ terminologies are integrated within several Security Incidents and Event Management (SIEM) systems [34,35] and cybersecurity testing frameworks such as Atomic Red Team [36] aiding the cybersecurity personnel in monitoring, detecting, and emulating adversarial activities in their network. Our risk management approach aims to integrate the $ATT\&CK$ framework within the different risk management processes, starting from the risk assessment process, during the cybersecurity architecture development up until the evaluation of the proposed architecture. We argue that this provides a clearer description and traceability of the risks of the organizations as the identified risks in the risk assessment are mapped with the security controls intended to mitigate them and evaluated during the architecture evaluation.

In this direction, a risk assessment approach for the cyber physical system has been proposed in our earlier work [37]. The approach is based on a design-level Failure Modes Effects and Criticality Analysis (FMECA) [38] which utilizes the common knowledge encoded within the $ATT\&CK$ framework. The $ATT\&CK$ framework was chosen due to its comprehensive and low-level abstraction of adversarial tactics and techniques compared to other high-level models observed in the literature such as STRIDE [39] and the cyber Kill Chain [40]. Provided with a system description and stakeholders' risk thresholds, the approach begins with identifying the possible failure mechanisms (i.e., cyber threat) for each system component. Then, the likelihood of these failure mechanisms is estimated utilizing the Common Vulnerability Scoring System (CVSS) [41]. The likelihood estimation also considers the existing mitigation methods. Afterward, the impact of the possible failure modes is estimated for each system component considering the occurrence of the failure mechanism. The $ATT\&CK$ framework provides the logical

mapping of failure mechanisms and failure modes within its threat model. The estimation of the impact relies on a group of metrics including ones that utilize the concept of centrality from graph theory which aids in reducing the effect of biased estimation [42]. These metrics are calculated using a graph of the system. Then, the detectability is calculated which refers to the degree to which the risk of the identified attacks is reduced by the existing controls. Finally, a risk priority number (RPN) is calculated considering the likelihood of failure mechanisms, the impact of the failure mode, and the existing risk reduction measures. The risk is later characterized according to the stakeholders' risk thresholds. In addition to calculating the risks, this approach utilized $ATT\&CK$ for suggesting suitable risk mitigation methods for each threat against each system component. These mitigation methods are later forwarded for developing a suitable cybersecurity architecture. The reader may refer to our original work [37] for more information regarding the risk assessment approach.

2.3 Evaluation of cybersecurity controls in the maritime domain

In this paper, we investigate the state of the art of cybersecurity control evaluation in the maritime industry considering the perspectives of both the academic community and relevant organizations including the classification society. The perspective of the academic community is captured through a Systematic Literature Review (SLR) which is discussed in Sect. 3.2.3. On the other hand, the perspective of the relevant organizations is captured through the collection and analysis of their publications regarding cybersecurity. The organizations were chosen based on the references in the literature. This includes, IMO, BIMCO, ENISA, and DNV.

The International Maritime Organization (IMO) guidelines for cyber risk management [15] refer to the need for evaluating a cyber risk management regime using effective feedback mechanisms without further description.

BIMCO guidelines [24] refer to the evaluation of cybersecurity controls within the risk assessment process through the assessment of residual risk when considering the existence of security controls. Also, the document refers to the third-party risk assessment process as means of performing accurate risk assessments by identifying whether the defense level matches the accepted level established in the cybersecurity strategy. The document refers mainly to penetration testing as a common approach but argued that it can be intrusive, risky, largely expensive, and requires an understanding of networks and assets. Therefore, other alternative approaches are proposed including asset discovery and inventory, auditing network architecture and design as well as vulnerability assessments.

DNV, another classification society in the maritime industry, refers in their class guidance for cybersecure systems to the evaluation and assessment of security controls during the acceptance stage for newly built and alteration projects [31]. They highlighted the roles of different stakeholders involved in the cybersecurity system testing and assessment of controls during the different system development stages.

Another documentation by DNV discusses resilience management of systems onboard ships and mobile offshore units [43]. The document discusses three approaches for assessing the cybersecurity of a system, namely high-level assessment, focused assessment, and comprehensive, in-depth assessment. The document refers to cybersecurity controls as barriers or safeguards. Comparing the current safeguards with the target is conducted through detailed checklists used in interviews with experts and relevant staff and users. After the assessment stage, a verification and validation process is needed to clear any discrepancy between the expected state and the actual state. The document suggests monitoring and testing the barriers at the level of the individual components as well as the system level. The discussed approaches include vulnerability assessment, technical verification such as load testing, network storm simulation (i.e. flooding), fuzz testing, actively provoking failures, and passive measurements. Penetration testing is discussed as a possible approach to systematically employ different methods. Moreover, the document discusses the verification of the information security management system by accredited third parties through audits and suggests a direction toward certification.

ENISA has published a report regarding cyber risk management for ports [44]. The report refers to assessing the maturity of cybersecurity posture following the maturity levels approach. Each maturity level is described, and the organizations are left to self-assess their position within different levels according to their own risk assessment.

In summary, the evidence collected from the published material by different relevant organizations suggests the existence of well-established and flexible methods and approaches for the evaluations of cybersecurity controls. Penetration testing is a commonly suggested approach, yet its discussed challenges pave the way for other possible approaches. However, the increased reliance on the human element within the evaluation process is observed, either through interviews, surveys, or relying on human evaluators. We argue that in autonomous vessels, human involvement is going to be reduced. This motivates the development and integration of automated processes for the evaluation of cybersecurity controls within different cyber assets involved in the autonomous vessels. In this work, we will investigate the suitability of the identified methods in the literature for the evaluation of cybersecurity architecture for an APS. Moreover, the increased reliance on sensor data supporting systems employing machine learning and artificial intelligence algorithms in the navigation functions exposes

the autonomous vessels to new threats such as adversarial machine learning. None of the studied literature or documents from different organizations have tackled this issue. This suggests the need for future efforts to investigate it.

3 Methodology

3.1 Cyber risk management strategy

The first question in this paper is, "What is a suitable strategy for managing the cyber risks of an autonomous passenger ship?". For this, a comprehensive literature survey was conducted to capture the state of the art in cyber risk management in the maritime domain. The perspectives of both the classification society and academia were considered. For this, academic databases, namely Scopus and Google Scholar, were queried for academic resources while the websites of relevant stakeholders were utilized for extracting documents relevant to maritime cyber risk management. As discussed in Sect. 2.1, the concept of layer defenses formalized as the DiD is the observed approach in maritime risk management. However, its effectiveness against sophisticated attacks has been questioned [12]. Based on that, we are proposing a new cyber risk management approach in this paper. Our proposed approach is described in Sect. 4.

3.2 Cybersecurity architecture development

The second question is "How a cybersecurity architecture can be developed to support the cyber risk management strategy?". There is a lack of discussion in the literature regarding this topic in the maritime domain. Therefore, we followed a standard system engineering process for the development of the cybersecurity architecture. It is based on a pre-specified set of requirements and concerns. It addresses the analyzed risks and includes components that allow updated risk monitoring and treatment capabilities. To realize this architecture, the system development followed the ISO 15288:2015 technical processes for defining an architecture and its design. Later, the developed design is subject to different system analysis processes to evaluate it. Figure 1 depicts an overview of the methodology followed for the development of the cybersecurity architecture as a system of systems (SoS). Moreover, guidelines from ISO 42010:2011[45] are utilized for the description of the architecture. The figure also reflects the input artifacts as well as the output for each process. Further details are discussed in the following sections.

3.2.1 Architecture definition process

The DiD strategy (section 2.1) is utilized as an architecture framework guiding the development of required defense

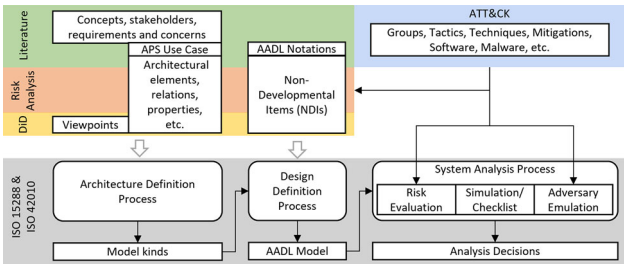

Fig. 1 Overview of the cybersecurity architecture development methodology

layers also known as viewpoints. The defense layers were defined after studying the documents issued by department of homeland security [23], DNV [31], and BIMCO [24] regarding implementing a DiD risk management approach. Later, and following a top-down approach, the system context, interfaces, and interactions with external entities are defined (Sect. 6.1). Then, the architectural entities and their relationships toward the satisfaction of stakeholders' requirements are defined. Afterward, each architectural entity is allocated relevant properties, concepts, etc. For this sake, a use case of the APS is presented to facilitate the description of the aforementioned concepts (Sect. 5). Then, a detailed description of architectural entities including any required system decomposition is conducted, depicting the interfaces and interactions between the different system elements. The aforementioned resources for DiD guidelines, the literature, and our conducted risk analysis [37] were consulted for useful artifacts during this stage. The outcome of these activities is discussed in detail in section 6. The modeling techniques utilized during these activities are preliminary data flow diagrams and adjacency matrices.

3.2.2 Design definition process

Architecture modeling is utilized to allocate system requirements to system elements (Appendix B), establish the structure of system elements (system, process, connection, etc.), defining interfaces among them as well as among external enabling systems. The later activities are achieved through the formalization of a model developed using Architecture Analysis and Design Language (AADL) [46] and OSATE, an open-source tool that supports it [47]. AADL is utilized to facilitate the architecture description and analysis considering that the underlying communication architecture is modeled using the same modeling language [10]. Moreover, AADL which can extend SysML has been utilized for analyzing critical systems due to its ability to describe information related to hardware, operating system, and code, allowing it to be applied at different stages during system development life-cycle [48,49]. Afterward, the assessment of possible NDIs is performed toward the selection of the

preferred solutions. The literature including DiD guidelines and our conducted risk analysis [37] were consulted regarding the possible NDIs to be integrated. Finally, the model is completed, and this paper completes the description of the architecture and its design describing the rationale for the different design decisions (Sect. 6).

3.2.3 System analysis process

The last question is "How the developed architecture can be evaluated ?". For this, a Systematic Literature Review (SLR) was conducted following the guidelines for conducting an SLR as proposed by Okoli and Schabram (2010) [50]. The proposed process consists mainly of four phases, planning, selection, extraction, and execution.

During the planning phase, the purpose of the review is defined. In this paper, the aim is to capture the state of the art in evaluating cybersecurity controls in the maritime transport domain, focusing on objectives, approaches, and relevant variables. The study aimed also to identify the relevant safety considerations as well as considerations related to the autonomous mode of operations.

Afterward, the selection phase entails the establishment of the parameters and criteria used to search the literature and filter the results. The following search query was used across three digital libraries, IEEE Xplore, and Scopus (with the appropriate syntax):(ship OR vessel OR maritime) AND (cyber OR "information security") AND (risk OR threat) AND (evaluate OR assess OR validate). The results were filtered to only include works after 2011, English as a language, and only considering documents of types (Conference Paper, article). The choice to only include works that were published in the last 10 years was based on the desire to stay updated. In total, 33 articles were identified. A clear criterion has been established for deciding either to include or exclude articles from further steps. The inclusion criterion is to only include works that targeted the evaluation, testing, assessment, or validation of cybersecurity controls in a system that is part of the maritime transport infrastructure.

Later, the extraction phase entails a deeper understanding of the resulted works to perform a quality appraisal and extract relevant data including other relevant articles. The results included a broad range of articles related to the evaluation of cybersecurity in maritime and other relevant domains. The main objective of this work is to identify works that have addressed the evaluation of cybersecurity controls in a maritime transport system. Other works that target systems outside this scope such as marine renewable energy systems were dropped. Additionally, works that targeted the analysis or assessment of the cybersecurity of certain systems without considering the evaluation of security controls were also dropped. The final list of articles proceeded for the next step was 18. Cybersecurity control evaluation is approached in this paper as a system analysis process. Therefore, the data extraction step relies on the ISO 15288 standard to map the observed artifacts in the literature to the relevant aspects in the system analysis process in the standard. For each screened work, the following aspects were captured: the process, approach, method, analysis questions, relevant stakeholders, scope, objectives, enabling systems, assumptions, quality and validity, discussion of corrective actions, and the venues for communication of results.

Finally, the SLR is executed through an overall synthesis of the found literature in addition to discussing and documenting the results and findings. The extracted artifacts from the studies during the data extraction stage are utilized for the identification and classification of evaluation approaches in order to identify those which are suitable for adoption in the evaluation of the cybersecurity controls in the APS. Then, the generation of the final document that is this paper is to be leveraged as a source of knowledge reflecting the current state of the art in the declared scope.

4 Threat-informed defense-in-depth

Although DiD is a widely adopted strategy and its usefulness against unsophisticated attacks has been demonstrated, critical discussions have been raised regarding its ineffectiveness against targeted sophisticated attacks [12]. This can be linked to the lack of a Cyber Threat Intelligence (CTI) program, one of the missing elements of DiD [13]. CTI enables defenders to constantly tune their defenses to manage the risks targeting their assets considering the current threat landscape [51]. CTI is one of the three main pillars of the Threat-Informed Defense strategy in addition to defensive engagement of the threat and focused sharing and collaboration [52]. The three pillars interact together to provide the $ATT\&CK$ framework [32] which can be used as an up-to-date resource for encoded common knowledge regarding adversarial behavior. We argue that aligning the $ATT\&CK$ framework and DiD layers would allow more evolved cyber risk management capabilities. So, in this paper, we propose a cyber risk management approach that integrates elements from the two strategies, namely the Threat-Informed Defense from MITRE [14] (i.e., Threat-Based Defense [52]), and Defense-in-Depth [23]. In the remainder of the paper, we will refer to cyber risk management simply as risk management. The approach is aligned with the risk management process in ISO 15288:2015 [53] as shown in Fig. 2 including four stages, planning, managing risk profile, analyzing the risks, and risk treatment and monitoring.

During the planning stage, the scope of the risk management process is defined. This entails the provisioning of a detailed system description including its operational context, stakeholders, requirements, components, their properties,

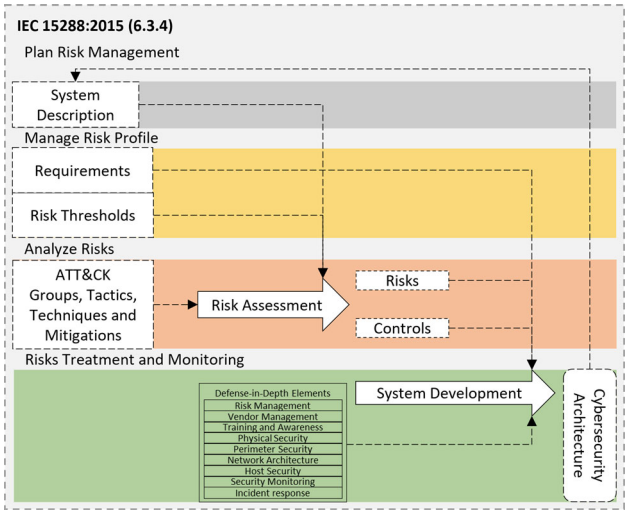

Fig. 2 Threat-Informed Defense-in-Depth risk management approach

and connections. Then, the stakeholders' risk thresholds are derived and established from their concerns and requirements. Additionally, results of earlier risk analysis and assessments are to be maintained in the risk profile. After that, the risks in the system are analyzed and assessed to identify the required risk controls. For this step, we propose the utilization of the $ATT\&CK$ framework [32] for facilitating the risk assessment process. $ATT\&CK$ is an integral component in the Threat-Informed Defense strategy as it provides a common knowledge repository for adversarial tactics and techniques drawn from several CTI sources. Additionally, $ATT\&CK$ suggests tailored defensive mechanisms for each technique. Such an approach is demonstrated in our previous work in which we proposed an FMECA-based risk assessment approach utilizing $ATT\&CK$ [37]. Based on a system description and risk thresholds, the risk assessment process identifies risks and proposes the required controls to mitigate them. Later, a cybersecurity architecture for supporting the risk management approach is developed. The architecture development relies on the proposed controls from the risk assessment process in addition to the stakeholders' requirements.

The DiD elements form architectural viewpoints for guiding a systematic architecture development process. For this, a mapping between the security controls suggested by $ATT\&CK$ and the DiD viewpoints is needed. The proposed mapping is depicted and discussed in Appendix A. The system development follows the ISO 15288:2015 technical processes for defining an architecture and its design. Later, the developed design is subject to different system analysis processes to evaluate it.

At the design stage, a suitable analysis process is a model-based risk evaluation. Several works have been observed to implement a similar approach [54,55]. The risk assessment process is conducted in several iterations against the system model considering different possible defensive strategies. The overall risk reduction (i.e., residual risk) for each defensive strategy is calculated in order to choose the optimal one. First, the cumulative risk of all the identified risks is aggregated and then the ratio of risks of each defense strategy compared to the base strategy (no controls) is calculated. To facilitate this analysis process, we have developed a defense strategy comparison algorithm. The algorithm extends the risk assessment algorithm proposed in our earlier work [37] for comparing the risk reduction in different defensive strategies. The strategy comparison algorithm is shown in Algorithm 1. A defense strategy is modeled using a mapping between the $ATT\&CK$ controls and the architectural components which are within the scope of the control function.

Algorithm 1 Strategy Comparison Algorithm (SCA)

```
procedure SCA(Threat information, Components information, Mitigation measures information.)
    for each defense strategy do
        for each component do
            AttackList ← IdentifyRelevantAttacks
            for each attack in AttackList do
                Likelihood ← Cal.AttackLikelihood
                Impact ← Cal.AttackImpact
                Detectability ← Calc.Attack Detectability
                RPN ← Likelihood × Impact × Detectability
                MitigationList ← GetAttackMitigation
            end for
        end for
        StrategyOverallRisk ← Sum.ofAllRPNs
    end for
    return RiskReduction, AttackLists, RPNs and MitigationLists for each defense strategy
end procedure
```

In order to demonstrate our approach, we will utilize a use case of an APS during different system development stages, namely an APS model which has been developed in our earlier work [10] as well as an implemented APS prototype named milliAmpere2.

5 Use case: autonomous passenger ship

The Autoferry project [7] aims to develop an APS use case named the milliAmpere2; An autonomous ferry capable of carrying 12 passengers across the Trondheim city canal proposed as an alternative to a high-cost bridge [56]. The ferry is designed to operate autonomously with human supervision. Supervision is carried from a Remote Control Center (RCC) encompassing monitoring APS operations and having the ability to intervene at any moment. The operation of the APS relies heavily on its communication architecture. Many stakeholders are involved in the design, development, and expected operations of the APS. The requirements for secure and reliable communication architecture have

Fig. 3 MilliAmpere2 ferry with an illustration of its main cyber components

been collected and adopted from each stakeholder's perspective [9]. The requirements for reliable communication included aspects related to redundancy for high availability, resiliency, network segregation, and others. The communication requirements have been addressed in the design and development of the communication architecture presented in [10]. On the other hand, the requirements related to the cybersecurity of the APS are addressed in this paper with the milliAmpere2 as a use case. A photograph of the milliAmpere2 ferry during a test run is shown in Fig. 3 including an illustration of its main cyber components.

A sufficient level of understanding of the communication architecture is needed to understand the needs and methods for implementing the security practices. An overview of the APS communication architecture in Fig. 4 shows the different architectural components and their interconnections. The proposed architecture connects the APS with its operational context through several communication channels. The entities in the operational context include a Remote Control Center (RCC), an Emergency Control Team (ECT), other ships, Vessel Traffic Services (VTS), and others (more details in [9], [10]). The APS communicates externally through several communication modules. A Mobile Communication Module (MCM) connects the APS to the internet through a mobile network using suitable technology (e.g., 5 G). The APS-RCC module provides direct point-to-point communication between the RCC and the APS through a suitable technology such as long-range Wi-Fi or mobile communication through a different service provider. The traffic module is required for ship-to-ship communication by broadcasting and receiving broadcast navigation messages such as ships' positions, speed, headings, etc. Automatic Identification System (AIS) is a candidate for implementation for the traffic module. Two modules for emergency purposes are integrated into the architecture. One is responsible for providing emergency navigation and control capabilities by the ECT while the other is to transmit emergency signals when passengers press on an emergency push button in case of incidents (e.g., passenger falling from the APS). Finally, the last group of modules is related to positioning and timing. Two Global Navigation Satellite System (GNSS) receivers are implemented one is connected to the traffic module and the other is connected to the GNSS system. Additionally, a single Real-time kinematic (RTK) receiver is connected to the GNSS system providing data for positioning correction.

The internal network of the APS connects different systems needed to carry out the expected functions including navigation, machinery systems, and others. The navigation system is responsible for collecting navigation data from arrays of sensors as well as the GNSS system for determining safe routes through an Autonomous Navigation System (ANS). The Machinery system is responsible for the ship's movement through active thrusters and a Dynamic Positioning (DP) system which is managed through an Autonomous Engine Monitoring and Control (AEMC). All the aforementioned components in the different systems are interconnected through an Ethernet network consisting mainly of Layer-3 switches. A compatible arrangement is proposed on the RCC to facilitate communication with the APS network. The three communication modules, namely MCM, APS-RCC, and traffic modules are expected to be similar to their pairs on board the APS. Also, a Remote Navigation System (RNS) supports the APS navigation system, in addition to a Remote Engine Monitoring and Control (REMC) for steering the ship.

The architecture model has been input to the developed defense strategy comparison algorithm (Sect. 4). Table 1 depicts the outcome of the algorithm for calculating the risk reduction percentage for each considered defense strategy. The strategy that provides the highest risk reduction is Strategy 5 which is based on BIMCO guidelines. However, the results suggest that it might be avoided in case of a reduced budget since Strategy 3 addresses a large portion of the identified risks with a lower amount of controls. Another aspect to consider is if satisfying the stakeholders' requirements is pursued, then Strategy 4 provides the optimal choice. It addresses the requirements as well as the identified risks while achieving a competing risk reduction score compared to other strategies. Therefore, the architecture development in the following section shall address controls based on Strategy 4. It is worth mentioning that the financial aspect of the

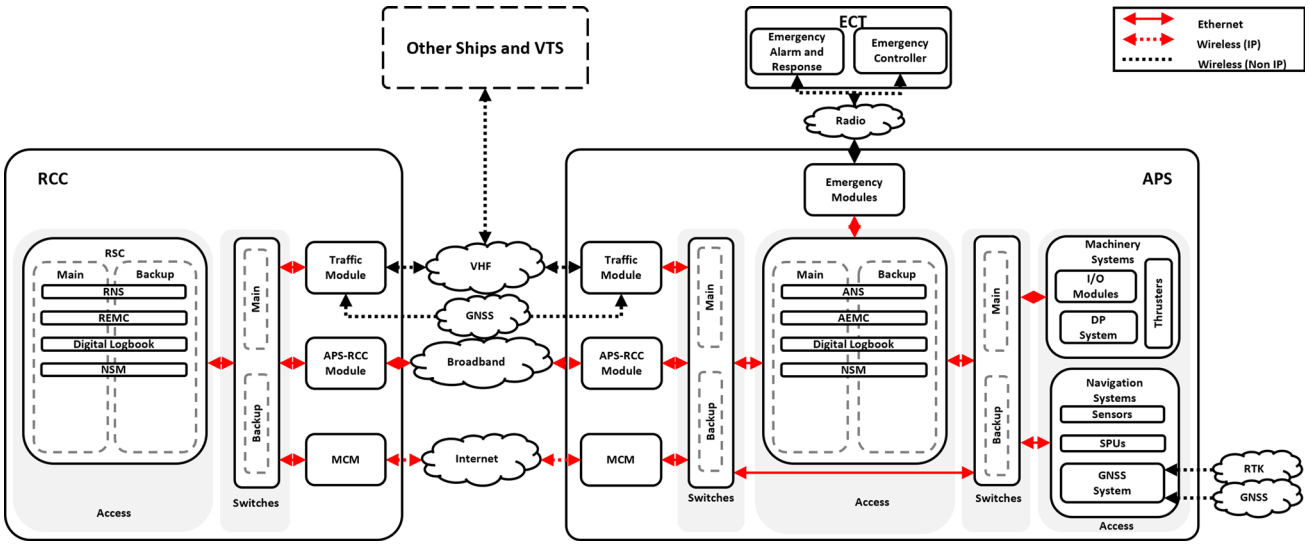

Fig. 4 Overview of the APS communication architecture (adapted from[10])

Table 1 Risk reduction in different defense strategies

Strategy	Risk reduction (%)	Description
1	0,84	The included controls in the current system model
2	80,22	The suggested or mandated controls in the stakeholders' requirements
3	69,72	The controls suggested after the risk assessment process while considering the current system model
4	81,94	The controls suggested after the risk assessment process while considering the stakeholders' requirements as bases for defense
5	85,35	The controls suggested in the BIMCO guidelines [24]
6	69,26	The controls suggested in the ICS DiD guidelines [23]
7	65,74	The controls suggested in the DNV guidelines [31]

strategy comparison is outside the scope of this paper and can be an item of future work.

6 Cybersecurity architecture

In this section, a cybersecurity architecture is presented which is an outcome of our risk management approach. It describes the different cybersecurity functions carried by different architectural components across the APS operational context, namely the ferry, the RCC, and the ECT. The architecture is modeled using AADL [46], thus enabling an extended analysis on the one hand and design modifications in the future on the other. The model code can be accessed through an online repository [57]. It presents the architecture through a group of views encompassing the entire System-of-Systems (SoS) layout (i.e., facilities), the logical view (i.e., service), and the structure view (i.e., system elements). The following sections discuss different views and present the outcome of the architecture development processes mentioned in Sect. 3 by providing the rationale behind the different architectural and design decisions as well as attempts to provide a sufficient level of traceability among different viewpoints, system elements, stakeholders, concerns and requirements.

6.1 Context view

The objective of the cybersecurity architecture is to address stakeholders' concerns regarding managing the risks against the APS systems [10]. An overview of the Narrowest system of interest (NSoI) is depicted in Fig. 5. We will refer to the NSoI throughout the paper as the APS ecosystem. This view captures the highest level of abstraction concerning different

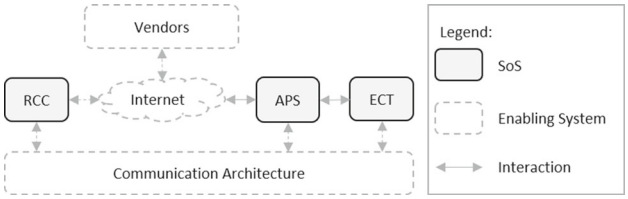

Fig. 5 Overview of the Narrowest system of interest

architectural components. It captures the System of Systems (SoS) in the operational context that collectively addresses the system objectives. Each SoS is hosted in a dedicated facility, APS SoS is hosted onboard the autonomous ship, RCC SoS is hosted in a Remote Control Center, and ECT SoS is hosted in a nearby boat carrying an emergency control team. Each SoS integrates additional components or utilizes components within the pre-defined communication architecture discussed in Sect. 5. Additionally, the APS and RCC are expected to utilize enabling systems hosted in remote locations accessed through the internet (e.g., updates). This view aids the understanding of various interacting entities in the context of the cybersecurity architecture; explicit details related to each architecture viewpoint and its relevant system components in the operational context are discussed in the following subsections.

6.2 Risk management

After January 1, 2021, all ship owners must address cyber risk management in their safety management systems for compliance under the ISM code [58]. To aid the efforts toward compliance with these regulations, the need for an Integrated Security, Safety, and Ship Management System (IS3MS) that applies an up-to-date risk management framework has been proposed in our earlier work [9]. Several cyber risk management approaches or frameworks have been cited in the literature, including DNV class guidelines [31], BIMCO guidelines [24], and ICS DiD guidelines in [23]. However, the discussed frameworks are generic and pose no restrictions on the applied methods. So, our proposed risk management approach (Sect. 4) includes activities that are aligned with all of them as shown in Table 2. Moreover, our proposed approach does not replace organizations' risk management processes. It can be utilized to complement them by identifying existing gaps to rectify them.

The scope of the IS3MS extends the scope of the cybersecurity architecture to include safety-related functions including monitoring and alerting. The development of an IS3MS architecture is a target study for future work. The concept includes the provisioning of different risk management functions by a centralized component. In the scope of this paper, the IS3MS is expected to include the following sub-components each addressing specific requirements or concerns:

6.2.1 Asset and user inventory

A regularly updated inventory of system users and components is required for the planning stage to define the scope of the risk management process. For the APS, at the design stage, this inventory includes an architecture model. During advanced stages in the development life cycle, this inventory can be conducted through other architecture scanning techniques. Additionally, a User Account Management (UAM) component is included in the architecture to support user inventory activities (more details in Sect. 6.6.4).

6.2.2 Risk assessment

Periodic risk analysis and assessment activities are required for maritime risk management proposed by the International Maritime Organization (IMO) in Resolution MSC. 428(98) [15] and constitutes an established requirement from the regulators' perspective in the APS system. This component is proposed to facilitate the conducting of this periodic process. It can be utilized to maintain the risk profile, aid in the identification of threats, assesses their risks, and propose controls. Our developed algorithm that supports risk assessment for cyber physical systems [37] has been integrated into this module. Our algorithm provides an assessment of the current threat landscape utilizing feeds from active Cyber Threat Intelligence programs delivered through the $ATT\&CK$ framework. This adds to the architecture the capability to identify weak points as well as directions for improvement. As mentioned in Sect. 4, we extended the algorithm in this paper to facilitate the comparison of different defensive strategies.

6.2.3 Policies and procedures

The establishment of policies and procedures is a common practice related to cyber risk management with varying focus areas. DNV's guidelines refer to policies related to personnel security, information classification, change management, and removable media [31]. BIMCO refers to crews' personal devices, use of administrative privileges, and equipment disposal. DiD guidelines in [23] focus on policies and procedures that are related to the human element.

Table 2 An alignment of our risk management approach with existing relevant approaches proposed by DNV [31], BIMCO [24], and DiD guidelines in [23]

IEC 15288 (6.3.4) [53]	Our approach	DNV [31]	ICS DiD [23]	BIMO [24]
Plan risk management	Specify assets		Inventory assets	
			Categorize asset criticality	
Manage risk profile	Specify risk thresholds			
Analyze risks	Identify failure modes	Identify risks	Identify security risks	Identify threats
	Identify controls			
	Identify effects of failure modes	Analyze risks	Determine potential impact	
	Identify failure causes			Identify vulnerabilities
	Estimate likelihood of failure causes			
	Evaluate risk	Evaluate risks		Assess risk exposure
	Identify Actions		Identify and tailor controls	
Risks treatment and monitoring	Develop cybersecurity architecture	Treat risks	Implement security controls	Develop protection and detection measures
			Monitor and adjust	Establish response plans
				Respond to and recover from incidents

6.3 Physical security

Controlling physical access to the facilities and components is an agreed-upon defense layer. However, no communicated cybersecurity requirements related to it were identified. In our previous work [9], the requirements were elicited by reviewing stakeholders' publications and documents with a focus on cybersecurity and communication requirements. Physical security is discussed within the realm of safety and security conditions [59, §2.2.2] and access control [8, §4.2.3.2] and [8, §6.4.4]. This suggests that physical security is outside the scope of the cybersecurity architecture of the APS, yet, it is a very important element that is required as an enabling system.

6.4 Training and awareness

The autoremote operational mode will change the traditional human role in maritime. The need for training regarding cybersecurity policies for APS personnel is a communicated concern and is a common defense layer. This includes personnel who are stationed in the RCC, among the ECT, or any other personnel that may access the APS system including service providers. Moreover, the risk analysis process has identified a group of threats that can be mitigated with cybersecurity training for both system developers and operators as well as the attack techniques that leverage user actions. Special considerations should be described regarding the implementation of security procedures in ICS to protect mission-critical systems. Training personnel and increasing their awareness regarding IT and OT security threats is an integral aspect to limit opportunities for compromising the systems and enabling the personnel to identify signs of compromise. This component aggregates the management of the aforementioned activities.

6.5 Network architecture

The segmentation and segregation of the APS network are an established requirement. The network has been designed with segmentation in mind to satisfy a segmentation policy related to communication reliability [9]. Nevertheless, security segmentation considers a different perspective. A network architecture for ICS is proposed in DiD guidelines in [23]. The architecture is described through different zones and levels. The proposed zoning architecture divides the network into six network levels across three zones each connecting a group of components with a specific set of functions.

The zones are the enterprise security zone, the manufacturing security zone, and the Demilitarized Zones (DMZ). The enterprise security zone hosts mostly IT systems that are expected to communicate with external entities. The manufacturing security zone on the other hand hosts mostly OT systems responsible for local or remote control and processing components as well as sensors and field devices. Furthermore, several network security levels reside within each security zone. Table 3 depicts the proposed distribution of components across different security zones.

Table 3 Proposed network architecture by DiD guidelines in [23]

Security zone	Security level	Systems description	Example (APS use case)
Enterprise	5	Perform communication and security management with a required overlook over the entire local network and communication with external entities	Intrusion Detection System, Security Incident and Event Monitoring
	4	Perform mostly functions related to internal system management such as DNS and data backup	Backup Server, User Access Management, Asset and User Inventory
DMZ		Systems with expected external access (e.g., internet access)	Jump Server
Manufacturing	3	Perform central processing and control operations	Navigation and Machinery monitoring and control
	2	Perform local control over systems in the same segmented network	Dynamic Positioning System
	1	Perform translation of commands coming from systems in level 2 to the end devices or expected to receive data from lower-level devices and forward processed data to systems at higher levels	Sensor Processing Units, I/O cards
	0	Data flow sources or sinks	Sensors, and Thrusters

Remote access is expected and has been identified as a possible risk; therefore, a secure network architecture should consider the external communications links arriving at the network through insecure networks (e.g., mobile network or wireless medium). For this sake, a DMZ within the APS network is considered to host servers with expected external access (e.g., internet access) including the jump server. Access to the DMZ should be secured using Access Control Lists (ACL). No requirement for a DMZ at the RCC has been identified at this stage. Systems in level 3 are considered among the biggest targets for intruders aiming at affecting a critical infrastructure system according to a "peel-the-onion" analysis due to the ability to control and oversee the control systems residing in lower levels as well as the ability to suppress potential alarms rising from their malicious actions [23]. A similar conclusion has been drawn from the conducted risk analysis [37]. The remote functions in the APS create additional challenges to the security in level 3 systems. Several systems outside the ship are involved in time-critical processing and control operations on the RCC facility, such as remote navigation and machinery monitoring and control. Such systems are not expected to have external access according to DiD guidelines in [23] nor is this operational mode addressed in the guidelines by DNV or BIMCO. Nevertheless, these systems provide crucial functions for safety and regulatory reasons [9]. Therefore, an additional layer of protection is expected between level 3 systems in different facilities. A proposed solution using VPN tunnels is discussed in Sect. 6.6.3.

Multiple VLANs are suggested to realize the expected network zones with appropriate Inter-VLAN routing and ACL rules. These configurations can be implemented at the network switches to route traffic between the appropriate zones securely and reliably. The switches act as security domain authorities enforcing the security policies of each security zone.

6.6 Network perimeter security

Additional measures should be put in place to secure communications between different network security zones in different facilities, namely the APS, the RCC, and the ECT. Achieving this can be accomplished by including both physical and logical controls. The physical controls are related to physical security which is outside of the scope of this paper. On the other hand, logical controls can be considered concerning the communication boundaries which are represented by the network gateways. Each gateway should be monitored by a firewall or another security barrier enforcing a security policy for securing the perimeter. The discussed focus areas for perimeter security are discussed in the subsequent sections.

6.6.1 Firewalls

A group of firewalls is placed at the edge of each network security zone in each facility to establish domain separation. Two dedicated network firewall devices are proposed, at the APS and the RCC, respectively, to handle external connections passing through two IP-based gateways (MCM and APS-RCC Module) such as connections with vendors over the Internet. Additional firewall capabilities for internal

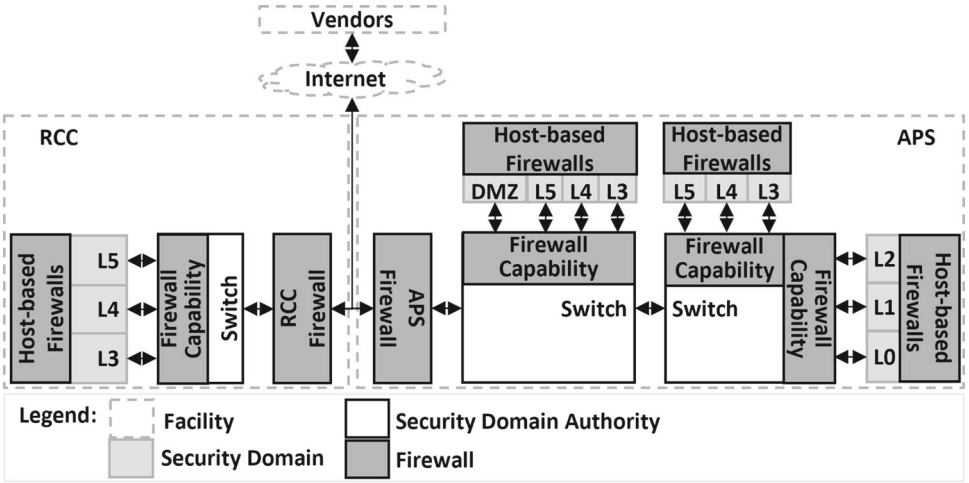

Fig. 6 Distribution of firewall functionality in the APS network

networks can be achieved through ACL implemented in the Layer 3 switches. Moreover, utilizing host-based firewalls can extend the borderline of perimeter security by extending the network firewall functionality to the hosts which strengthen the ability to protect the network from malicious intruders [23]. An illustration of the firewalls architecture is shown in Fig. 6. This suggested architecture dictates that no component can contact another component within or outside its network security domain unless authorized by a security domain authority.

6.6.2 Non-IP communication

Regarding non-IP traffic carried across the remaining gateways, perimeter security is discussed through a group of security solutions distributed among different gateways. The first gateway, (Traffic Module), carries data related to ships' traffic management (AIS messages). AIS is known for several vulnerabilities including ones that invade passengers' privacy and launch collision attacks [60]. Additionally, jamming or denial of service, and spoofing have been identified as possible risks during the risk assessment [37]. The proposed mitigation techniques against AIS attacks are not implemented at the firewall since the external interface of the traffic module employs VHF communication. But, the internal interface can encapsulate AIS messages using an IP-based protocol (e.g., TCP). The suggested mitigation methods in the literature include the use of cryptography [60–63] and anomaly analysis [64–66]. Therefore, solutions for AIS security are considered for future work. The second gateway is the emergency gateway that connects the backup navigation system with the emergency controller in the ECT and carries non-IP traffic for navigating the APS during emergencies. A proposed solution to the security of this link is to establish "Communication Authenticity" so that only authenticated devices can establish communication over this link. A solution using security monitoring is proposed in Sect. 6.8. The third and fourth gateways are the RTK and GNSS modules. The GNSS and RTK receivers provide the system with data needed for positioning measurements. RTK signals are not known to be a medium for attacks. GNSS signals on the other hand are susceptible to several known attacks. GNSS jamming and spoofing have been identified among the threats against the APS operations and the existing mitigation methods are classified by the conducted risk analysis as insufficient. Jamming attacks are proposed to be mitigated in the APS use case through redundant functional components such as other sensors (e.g., lidars, video, etc.) and backup GNSS systems. This has been considered and discussed in the conducted risk assessment [37]. Several solutions have been observed in the literature relying on anomaly detection using machine learning [67], and specification-based detection [68,69]. We have addressed this issue in our other work in which we have conducted an anomaly analysis and proposed detection rules for detecting simple and sophisticated attacks against GNSS systems communicating using the NMEA protocol (National Marine Electronics Association) [69]. The development of a dedicated anomaly detection solution is an item for future work.

6.6.3 VPN

The risk assessment process identified an important mitigation method through the encryption of sensitive information in transit. Moreover, Virtual Private Network (VPN) tunnels are suggested by DiD strategy to be implemented between systems in the same security level in different facilities for maintaining perimeter security [23]. For instance, the autonomous navigation component in L3 in the APS is expected to communicate navigational information to the remote navigation system in L3 in the RCC; this communication passes insecure mobile and/or broadband networks

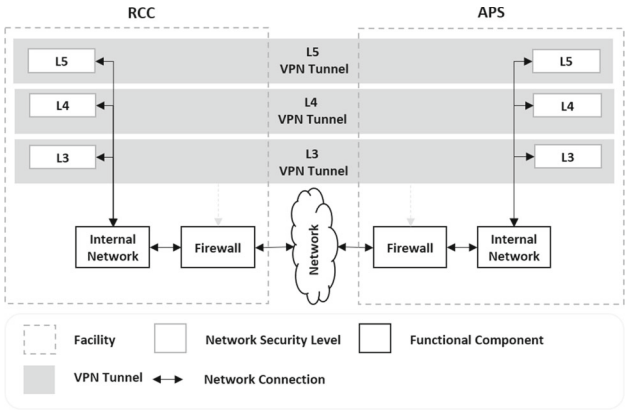

Fig. 7 Overview of the proposed VPN tunnels

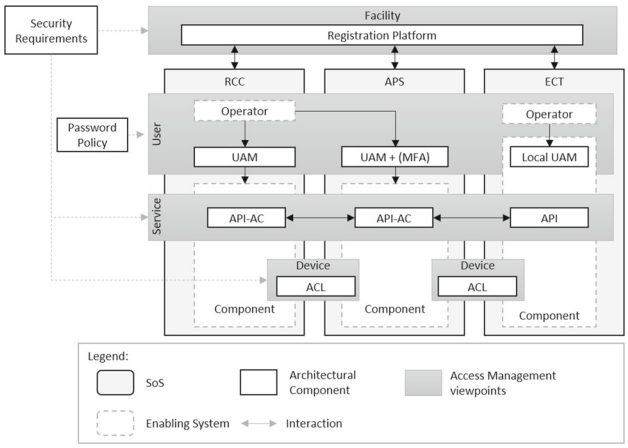

Fig. 8 Overview of the access management services

and may contain passenger-related data (e.g., video stream). Therefore, VPN is suggested to be implemented to secure these communication flows. As shown in Fig. 7, VPN tunnels are proposed to be integrated into the APS and RCC dedicated firewalls using router-based IPSec protocol [70] to reduce firewall management. Otherwise, client-based firewalls using PPTP (Point-to-Point Tunneling Protocol) [71] provide another implementation option.

6.6.4 Access management

The conducted risk analysis process has proposed considerations to be integrated into the access management components including a password policy, multi-factor authentication, and software and device authentication techniques. An overview of the access management services in the APS architecture is depicted in Fig. 8. At the higher level of abstraction, the facilities hosting different SoSs are expected to be registered on a common platform. This is a communicated requirement for having a ship registry component within the system operational context. Moreover, within the same facility (e.g., RCC), the operator can access components through a User Access Management (UAM) component that implements a password policy. User access to components in another facility requires a multi-factor authentication process (MFA) integrated with the UAM component. Hardware component-to-component access is controlled by ACL while software component-to-component access is controlled by a functionality integrated into different Application Programming Interfaces (API) which we refer to as API Access Control (API-AC). A group of security requirements is expected to be communicated to the providers of the enabling systems regarding the access management solutions such as the implementation of secure protocols related to Authentication, Authorization, and Accounting (AAA).

DiD guidelines [23] suggest implementation options for the UAM and APIs. Regarding UAM, centralized access management for each facility is favorable over a distributed approach. Lightweight Active Directory Protocol (LDAP) is a possible protocol for implementation as it can provide Role-Based Access Control (RBAC) which is the recommended approach proposed according to the conducted risk analysis. Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System (TACACS) are both valid implementation options for the UAM [23]. However, the centralized approach introduces a risk if the authentication server gets compromised therefore, strict security controls should be applied to protect this server as well as establish redundancy. Also, remote connectivity is required for maintenance due to unmanned operations and jump servers hosted in the DMZ are proposed for this sake. Remote access to the jump server should be secure and MFA is proposed for that. Regarding APIs, they are widely popular in ICS and suffer from a wide range of security issues [23]. Therefore, great attention should be spent on the development of the API-AC component. This observation will be forwarded to other project members responsible for the development of APIs.

Further complications regarding access control and authentication are expected in ICS networks due to the provisioning of systems by different manufacturers not necessarily implementing the same authentication mechanisms. Therefore, local authentication and authorization policies and procedures should exist in these components.

6.7 Host security

Considering the viewpoint of host security, several aspects of interest have been identified through implementing the DiD strategy as well as the learned from the conducted risk analysis. These aspects are detailed in subsequent sections.

6.7.1 Patch and vulnerability management

Keeping up-to-date software with security patches is a strong countermeasure to many cyber threats. Integration of components for patch and vulnerability management (PVM) is an agreed-upon mitigation method according to the conducted risk analysis process and different DiD strategies. Moreover, a PVM component supports the satisfaction of established requirements regarding updates and security analysis. At the same time, the impact of a system patch should be evaluated before implementing the patch on the operating APS to ensure ongoing operations, especially regarding the operation of critical components.

6.7.2 Malware protection

The integration of the endpoint malware protection component within the APS architecture is a communicated requirement. Additionally, DiD guidelines suggest malware protection tools for supporting host security. Moreover, the risk assessment process has identified anti-malware among the required risk mitigation measure. Therefore, malware protection software is to be integrated into the relevant architectural components.

6.7.3 Application isolation and sandboxing

Identified as a risk mitigation method through the conducted risk assessment to mitigate against high risk imposed by scripting threat. The utilization of virtual machines, docker containers, and other forms of application and component separation is encouraged. Nevertheless, each implementation imposes different security threats and therefore, relevant security controls should be integrated. DiD strategies suggest considerations for the application of virtualized host components. This risk mitigation method is of particular relevance to centralized components hosting autonomous and remote control and navigation functions as well as other components for system and network management and security. The application of virtualization has been proposed in the architecture design earlier [10] and is also adopted in the scope of this cybersecurity architecture.

6.7.4 Backup

Data backup has been identified as the most important risk mitigation method during the conducted risk analysis to mitigate several attack techniques such as defacement attacks and loss of availability [37]. Also, a specific requirement exists concerning the availability of backup facilities for protection and recovery functions following a backup policy. Moreover, remote backup facilities have also been suggested during the risk analysis and the RCC is proposed to host such facilities. For this purpose, two backup servers are proposed, a server on board the APS and another hosted in the RCC. Regarding the APS backup server, the requirement dictates that an early alert indicating storage capacity exhaustion should be implemented and the ability to transfer the data to shore should be made available [9].

6.7.5 System hardening

Referred to by BIMCO as "Secure configuration of hardware and software" [24], this component is proposed to address a group of concerns identified through the risk analysis process. It is a required activity to perform several tasks as risk mitigation measures against the high, medium, and low risks including scripting, system timer attacks, and block reporting messages attacks. This component is expected to manage such operations including static network configuration, restrict file and directory permissions, and others.

6.8 Security monitoring

Intruders are expected to gain access somehow as observed in many attacks against highly secured industrial control systems [72,73]. A specific requirement exists to integrate monitoring capabilities to detect unusual activities within the network and hosts. Proposed solutions according to different DiD guidelines and the risk analysis are the application of Intrusion Detection and Prevention Systems, security information and event management (SIEM) systems as well as security audit logging.

6.8.1 Intrusion detection and prevention systems

Intrusion Detection Systems (IDS) and or Intrusion Prevention Systems (IPS) are vital elements for maintaining the security of the APS network. Similar to a typical ICS network, the network traffic within the APS network is predictable, the communicating hosts, IP and MAC addresses, ports, protocols, etc should be known. Strong rules to detect unusual traffic should be feasible, but care must be paid when utilizing IPS since they may stop ongoing vital time-critical operations. Therefore, passive IDS are more favorable than IPS. At the same time, IPS can be utilized to take action against events with high confidence malicious ratings, especially during autonomous operations to reduce human involvement.

IDS are commonly utilized in vehicular systems including maritime vessels as indicated in a survey conducted by Loukas et al. [74]. However, the focus of such systems is mainly on GNSS spoofing and anomalies related to CAN bus protocol. The placement of IDS/IPS according to the DiD strategy is advised to be located in high traffic locations (i.e., connected to network switches) or between security bound-

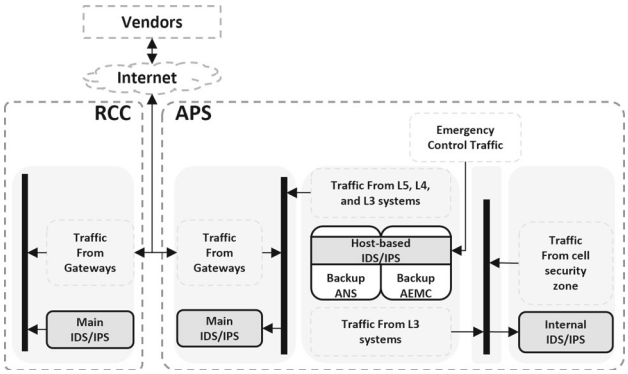

Fig. 9 proposed IDS/IPS architecture in the APS network

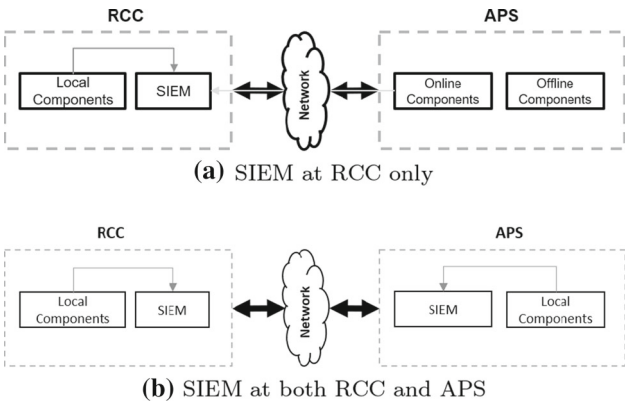

Fig. 10 Options for SIEM placement

aries (i.e., connected to a firewall) [75]. Figure 9 depicts a proposed arrangement of IDS in the APS ecosystem. In the APS network, all traffic between the cell security zone (i.e., L2, L1, and L0) and L3 should be sent to the internal IDS/IPS with the main focus on inter-system traffic that should be predictable to some extent. Additionally, the conducted risk analysis has identified the need for special host-based IDS/IPS units hosted on the backup ANS and the backup AEMC to monitor traffic from the emergency controller onboard the ECT. Moreover, a main IDS/IPS on each of the APS and the RCC is expected to monitor and possibly control the traffic received from the gateways connected to the enterprise security zone. The IDS/IPS is expected to include capabilities for mitigating a group of identified threats. Such capabilities include Data Loss Prevention (DLP), Endpoint Denial of Service, Restrict Web-Based Content, and others.

6.8.2 Security incident and event monitoring

Logging and monitoring of security-related events are an integral aspect to detect and identify malicious attacks and is among the communicated requirements. Therefore, it is important to enable the logging feature on all the devices within the APS network and facilitate the collection of this information for processing through host-based agents. This feature can be used as one of the data sources for centralized Security Incident and Event Monitoring (SIEM) components. The role of each SIEM component includes but is not limited to monitoring and logging; it can even include detection and post-incident preparation [76]. The centralized SIEM can also receive IDS/IPS data to correlate with other data sources for the detection of possible security events. A possible implementation option is through the utilization of open source Elastic stack instruments [77]. Elastic stack has been proposed in the literature for providing SIEM functionality and more [78,79].

During the system analysis process, we have evaluated different possible placements of the SIEM component within the APS ecosystem. The first considered option as shown in Fig. 10a, is one node at the RCC overseeing the APS network. This option, although it provides a single management location and reduced SIEM cost, has several shortcomings. First, all data collected from the host-based agents at the APS will need to be transferred over the network to the RCC which will consume valuable bandwidth required for critical functions. Second, some components within the APS are not expected to have external connectivity and therefore will not be managed by the SIEM at the RCC. Finally, the APS can be managed by different RCCs at different times; this setup will require re-configuration whenever the RCC in command is changed. The other option is shown in Fig. 10a, a dedicated SIEM at each of the APS and the RCC. Both nodes are configured to collect all the required information from the other components within their respective network through the host-based agents. This option limits the occupancy of the communication link for SIEM data require no re-configuration at changing the RCC, and offline components are still managed by the local SIEM. At the same time, the shortcomings of this option are the increased management locations as well as increased SIEM cost.

Moreover, the APS is expected to host several components that are maritime-specific such as the AIS, NMEA speaking components, etc. The inclusion of such components within the coverage of the SIEM component would require various adaptations and domain-specific rules and alerts. This is proposed as an item for future work.

6.9 Vendor management

Considerations regarding vendor management have been communicated in our previous work [9]. In the same direction, several policies and procedures are proposed by different DiD guidelines including security in supply chain management, outsourcing, and leveraging cloud services. Establishing security requirements at early stages during the procurement process is proposed to be conducted to control

the provisioning of services by third parties [23]. For example, a set of requirements could be specified when purchasing gateways to provide VPN capabilities, firewall capabilities as well as anti-spoofing capabilities. Additionally, several procedures are proposed through the conducted risk analysis to manage the risk in this direction. Such procedures include application vetting, updating software, audit, code signing, vulnerability scanning, and boot integrity. This component is proposed to aggregate the management of these activities.

6.10 Incident response

The formulation of Incident response plans is a communicated requirement for the APS. Additionally, several DiD guidelines suggest activities related to incident response such as establishing contingency plans [24,31], and data recovery [24]. Moreover, the conducted risk analysis has identified the utility of out-of-band communication channels as backup channels during incident response or in case of communication failure. This component is proposed to manage different activities and aspects related to incident response such as the provisioning of appropriate incident response plans.

7 Cybersecurity evaluation

The conducted SLR has captured the state of the art for the evaluation of cybersecurity controls in the maritime domain. We have identified existing approaches, aspects, scopes, and objectives. In this section, we will summarize our findings and utilize the observed approaches and aspects for evaluating the proposed risk management approach and its produced cybersecurity architecture.

7.1 Evaluation approaches

Several approaches have been observed with a distinct scope and varying levels of rigor. Table 4 depicts the observed approaches and evaluation environments. Commonly, approaches are combined for improving the evaluation process. Surveys through checklists and questionnaires are the most common method. Surveys focus on aspects including market research; quality and cost of controls [54], stakeholder engagement [26], usability and quality of risk assessment frameworks [80,81], existence, revision and awareness of controls [25]. Risk evaluation including risk and residual risk estimation and assessment is usually combined with another approach such as assessing the risks in scenarios using a game-based approach [82] or through questionnaires [54,81]. Some works evaluate the performance of target systems to assess their security or the impact of security controls on their operation. This is observed to be achieved through emulating the behavior of adversaries (i.e., adversary emulation) [66,83] or testing the functionality of a specific functional unit (i.e., unit testing) [26,82,84,85]. Other works target the exiting vulnerabilities in the system as an indicator of the efficiency of its security posture [25,86]. Kuhn et al [87] carried out an exercise for assessing the risk perception of participants for evaluating their decision-making capabilities in cyber incident response. McCready et al [88] researched relevant standards and regulations for evaluating the utility, feasibility, and aspects of a maritime compliance regime as an organizational control for improving the cybersecurity posture of organizations in the maritime domain. The authors also indicated the importance of record-keeping for the evaluation of the cybersecurity posture for audit purposes.

Moreover, the approaches vary based on the system development life cycle of the target system of evaluation. This is reflected in the environment used for evaluation. Some works addressing high-level controls such as compliance regimes [88], and risk assessment frameworks [80,86] utilize abstract descriptions of the target systems including relevant organizations, facilities, and utilized technologies for qualitative evaluation. Other model-based approaches tend to be theoretical with the capacity for simulation [54,55]. On the other hand, in more advanced system development phases, approaches tend to consider more realistic settings reaching the ability to evaluate the real target system [25,26] and on some occasions simulating certain elements in the environment [89,90]. Additionally, some works address the software source code, middleware and hosting operating system for evaluating its security [82,84,85].

All the observed approaches rely on a specific threat model encompassing several elements such as target system, threat or attack, mitigation methods, and others. Some approaches are more defensive as they mostly address the established risk mitigation measures or the existence of vulnerabilities in the target system [25], in other words, blue team activities. Other approaches are more offensive as they aim to evaluate the behavior of the target system against specific adversarial activities [66,83], in other words, red team activities. Other approaches consider both perspectives [54], similar to the concept of purple teaming, aiming to establish a wider view of the cybersecurity posture of the target system and its risk management capabilities.

7.2 Aspects, scopes, and test objectives

A wide range of aspects has been observed encompassing security, privacy, functional, cost, and governance aspects. Table 5 depicts a summary of the observed aspects, their scope, and the test objectives of the system analysis. Regarding the scope, some works have addressed the entire security posture of the organization including the organization, stakeholders, systems, and services. Other works target a certain

Table 4 Evaluation approaches and environments

Method	References	Environment	References
Risk evaluation	[54,55,81,89]	Simulation/system model	[54,55,83,87]
Survey	[25,26,54,80,81]	Real system	[25,26]
Vulnerability scanning and assessment	[25,86]	SW	[82,84,85]
Performance evaluation	[26,82,84,85,90]	Simulation/real systems	[66,89,90]
Unit testing	[26,82,84,85]	Abstract	[80,81,86,88]
Exersize	[87]		
Gamefication	[87,89]		
Research	[88]		
Record keeping	[88]		
Adversary emulation	[66,83]		

system such as a ship or the navigation system with or without knowledge of the included security controls. Others target specific security controls such as incident response, policies, and procedures. Regarding the targeted aspects of evaluation, several security aspects are observed including effectiveness, existence, awareness, and revision of controls, the existence of vulnerabilities, requirement satisfaction, and recommendations. Testing the effectiveness of controls is the main goal of evaluation with varying objectives. Some works targeted quantitative metrics such as detection quality, number of vulnerabilities over time, and successful logins. Others targeted qualitative aspects such as the effect of experience on incident response, or how the security control would respond to attacks. Also, evaluating the satisfaction of the stakeholders' requirements related to security and privacy is a common objective. Additionally, the functional aspect is addressed by several works focusing on the behavior of the system under attack, the integration of controls within the system, and the usability, feasibility, and applicability of the security controls assessed by the system stakeholders. Moreover, the financial and operational cost of controls during different system development life cycles is also addressed. Finally, aspects related to governance such as roles and responsibilities, the obligation of application, penalties of non-compliance, and assessment frequency have also been investigated.

7.3 Cybersecurity evaluation of the APS use case

Considering the current technology readiness level of the APS use case, there are several aspects and test objectives that are relevant for evaluation. The scope of the evaluation extends to the proposed risk management strategy (Sect. 3), and the security architecture produced after its application (Sect. 6).

Proper evaluation of the risk management strategy can be conducted over time by observing the efficiency of the developed cybersecurity architecture. However, its feasibility and usability have been evaluated. The risk management process was initially conducted against a system model of the APS; this has led to the development of the security architecture in Sect. 6. Moreover, another iteration of the process was conducted against the implemented prototype which is the milliAmpere2. The risk assessment process identified a group of risks and required controls that were later integrated into the ferry and the RCC. This reflects the suitability of the process for applications in different system life cycle stages.

The next subject of evaluation is the proposed cybersecurity architecture. The evaluation was conducted again for the developed model as well as the implemented ferry. The evaluation was conducted using several methods, namely risk evaluation, simulation and checklist, and adversary emulation.

7.3.1 Risk evaluation

We have implemented our proposed risk assessment approach [37] for the estimation of residual risk before and after the integration of the security controls. The risk evaluation was conducted for two system definitions. The first one is the model of the APS communication architecture discussed in Sect. 5. The other one is for a model of the implemented milliAmpere2 ferry. The cybersecurity architecture can improve the risk reduction from 0.84 to 81.94% for the APS communication architecture model, and from 58.37 to 85.72% for the milliAmpere2 ferry. The deficiency in the risk reduction value is mostly related to risks with no existing or limited controls such as resource hijacking and radio jamming; this is inferred from the fact that the $ATT\&CK$ framework designated such risks to have no or limited existing controls. The risk reduction in the milliAmpere2 before the cybersecurity architecture is due to the existence of controls such as network segmentation, physical security, firewalls, and several others. However, the existing controls weren't sufficient for addressing critical to medium risks.

Table 5 Aspects, scopes, and test objectives

Category	Aspect	Scope	Test objective
Security	Effectiveness	Cybersecurity posture [88]	Number of vulnerabilities over time [88]
		Control [25,26,54,55,85,87,89,90]	Flatness, successful logins [26]
		Control and host system [55,66,82,83]	Defense strategy and risk level [55,82,89]
			Will the controls work [26,90]
			How does the controls work [87]
			How experience affects the control [87]
			Level of confidentiality, integrity, and availability [90]
			Detection quality [90]
			Accuracy, precession, recall, F1-score [85]
			Deterrence [54]
			Can attacks be mitigated [83]
			Real time defense [54]
			Restoration [54]
	Existence of controls	Controls [25]	Incident handling and reporting [25]
	Controls awareness		Policies and procedures [25]
	Controls revision		
	Vulnerabilities	Host system [25,83]	What vulnerabilities exist [25,83,84]
		Host system and Controls [86]	What errors and defects exist [86]
		Application SW [84]	
	Requirements satisfaction	controls [26]	Are the security requirements satisfied [26,84,86]
		Application SW, Middleware, OS [84]	
		Host system and Controls [86]	
	Recommendations	Controls [26]	e.g., cryptographic strength

Table 5 continued

Category	Aspect	Scope	Test objective
Privacy	Requirements satisfaction	Controls [26]	Are the privacy requirements satisfied [26]
Functional	Behavior	Host system [83]	How would the system behave under attack [83]
	Integration	Controls [26]	Are the control properly integrated [26,84]
		Application SW, Middleware, OS [84]	
	Usability	Controls [26,80]	User acceptance testing [26,80]
	Feasibility and applicability	Control [80,88]	Compliance regime [88]
			Risk assessment framework [80]
Cost	Financial	Controls [54,81]	Cost of implementation [54,81]
			Cost saved by reducing risk [81]
	Operational	Against host system (i.e., safety) [26,54,90]	Execution Time [26,85]
		Controls [26,85,90]	Packet loss, delay [54]
			Overhead [26]
			Harmlessness and Data lost [90]
	Lifecycle	Control [54]	Future developmnet costs [54]
Governance	Responsibility	Compliance regime [88]	Enforcement, auditing and reporting [88]
		Assessment Organization [86]	Assessment [86]
	Obligation	Compliance regime [88]	Mandatory or voluntary [88]
	Penalties		What are the penalties for non-compliance [88]
	Assessment frequency		What is the period between audits [88]

7.3.2 Simulation and checklist

An observed method for evaluating the cybersecurity architecture is to check its satisfaction with the cybersecurity requirements. Yi and Kim [84] discussed the evaluation of naval ship combat software against a set of specified technical requirements related to accuracy and adequacy. Additionally, Grigoriadis et al [26] reached out to stakeholders for evaluating their risk assessment process against security, privacy, operational, and usability requirements. As mentioned before, we have identified a group of cybersecurity requirements for the APS [9]. These requirements are then utilized for evaluating the security architecture based on the verification criteria defined during the architecture design (Sect. 3.2.1). The evaluation was conducted against two system definitions, namely a simulated cybersecurity architecture, and the implemented milliAmpere2 ferry.

In this paper, simulation is utilized to verify the feasibility of integrating the cybersecurity architecture within the underlying communication architecture and to facilitate later security analysis. A prototype implementation of the IP-based components is provided using the GNS3 simulator [91]. GNS3 (Graphical Network Simulator-3) is a platform for emulating appliances (network, endpoints, etc.) using virtualized images. It enables the configuration, testing, and development of networks with flexibility and lower cost [91]. Later, cybersecurity controls proposed in the cybersecurity architecture in Sect. 6 were integrated using a variety of open-source and off-the-shelf controls to evaluate their feasibility and suitability for the autoremote operational mode. Later, the simulated architecture is evaluated for its satisfaction with the requirements. A summary of the verification process including the design-level and implementation-level verification criterion as well as details regarding the supporting components and conducted processes is shown in Table 7 in Appendix B. Detailed description of the simulated network, integrated controls, and attack trees used for evaluation is presented in Appendix D. Access to our simulated network can be provided upon request.

The design-level verification is of low fidelity and only intended to verify the feasibility of the cybersecurity architecture in the APS design model and simulated implementation. It demonstrated the feasibility of the model for implementation and shed some light on the considerations regarding the provisioning of risk management functions within the autoremote operational mode. More details are discussed in Sect. 8.

On the other hand, the implementation-level verification has shown some limitations in the cybersecurity posture of the milliAmpere2 ferry. Due to the involvement of several technology and service vendors, some cybersecurity controls have implementation gaps and limited information regarding their details. The most critical issue observed is related to regular software updates. A high-priority requirement exists to enforce regular software updates for components in the APS network. However, our evaluation uncovered that some components have outdated software versions and no existing process for updating them. Another issue that has been identified is related to the lack of training exercises related to cybersecurity. Efforts are planned in this regard and are expected to be items for future work. Moreover, the inclusion of some security controls has been found to be not feasible in the current implementation. Some components are protected from manipulation through agreements with vendors which limited the ability to install agent software for a dedicated SIEM and HIDS software. Therefore, reliance on NIDS is considered an alternative. Furthermore, a requirement exists related to the network topology to avoid including components used for navigation and control in the same network. However, it was found that this requirement is not satisfied.

In summary, the simulation was useful in reducing the cost of implementation at the real ferry as well as for trying out several implementing options at a lower cost. However, contextual information such as access limitations to some components was not considered during the simulation. The checklist approach uncovered several limitations in the implemented cybersecurity architecture of the ferry allowing for future improvements.

7.3.3 Adversary emulation

Having access to the implemented ferry allows for conducting hands-on adversary emulation; a security assessment process applying realistic attack scenarios which emulate the capabilities of real threat actors [32]. Several works in the literature have applied it in demonstrating and evaluating the security of maritime systems. Balduzzi [66] conducted various attacks against AIS protocol and some of its implementation to evaluate its security. Also, Hemminghaus [83] proposed a tool for automating several attacks against integrated bridge systems to evaluate the established security controls. Adversary emulation is another instrument of the Threat-Informed Defense strategy that utilizes the $ATT\&CK$ framework for mapping the adversarial behavior of a specific set of Advanced Persistent Threat (APT) groups. Conducting adversary emulation against the implemented ferry is intended as an evaluation process for the implemented cybersecurity architecture. Additionally, we aimed to understand the impact of the autoremote operational mode on cybersecurity functions and how would they withstand realistic cyber attack techniques. Based on that, we define a group of tests consisting of different $ATT\&CK$ tactics (i.e., kill chain phase) and techniques against different components for achieving a comprehensive evaluation.

The tests are intended to be comprehensive, covering all the attackers' objectives (i.e., tactics) proposed in the

$ATT\&CK$ framework and a wide range of techniques and software to implement them. For each tactic, at least one test was planned and developed. The tests were prioritized based on those identified as critical to medium risks and those which are technically feasible for testing. A summary of the planned and conducted tests is depicted in Table 8 in Appendix C. Several tests were not allowed to be carried out due to access limitations by the network vendors. The conducted tests have yielded useful information that will be used for improving the cybersecurity posture of the ferry ecosystem. This includes the discovery of critical vulnerabilities and a large number of open network services. Utilizing the $ATT\&CK$ framework enriched the adversary emulation process by enabling the development of atomic tests in a systematic manner. Still, a wide range of tests is needed to evaluate the entire architecture.

The utility of the adversary emulation process has been demonstrated. Conducting it at several iterations is needed to maintain accurate risk awareness. However, it comes with a high cost in time and resources. Therefore, efforts to automate some of the tests and expand their scope are items for future work.

8 Discussion

In this section, we present our reflections after conducting the different research activities presented in this paper. We discuss the challenges and limitations observed in different applied approaches. Also, we present our observations regarding the provisioning of risk management functions within the autoremote operational mode.

Starting with the risk management strategies. The DiD and the Threat-Informed Defense as risk management strategies are evaluated in this work through the integration of different elements in the strategies toward the development of the cybersecurity architecture of the APS. The DiD has been challenged previously for its ineffectiveness against sophisticated attacks [12]. These findings are confirmed in this work when discussing protocol-specific controls related to Non-IP communication in Sect. 6.6.2. We have identified the need for a dedicated anomaly detection solution for the NMEA protocol since traditional IDS systems are not tuned to detect anomalies for this specific protocol. This supports the argument that a DiD approach that relies on stacking up controls without proper evaluation of the threat landscape would risk the protected system against sophisticated attacks. Additionally, using simulation we have evaluated and demonstrated the utility of the proposed cybersecurity architecture in withstanding several cyber attacks. We have observed limited discussion regarding system hardening activities in several DiD guidelines while several suggestions in this direction are provided by the $ATT\&CK$-based risk assessment. Additionally, the Threat-Informed Defense strategy provided several instruments that enriched the risk management process and aided the development of the cybersecurity architecture. These instruments include the $ATT\&CK$ framework, and the defensive engagement of threats using adversary emulation. Both instruments are constantly updated from CTI feeds which allows the architecture to constantly evolve in order to match the latest threat landscape. However, some limitations are observed in the defensive functions proposed in $ATT\&CK$ such as the lack of clear interfaces between threats and incident response functions as well as the lack of high-level risk management elements such as roles and responsibilities. These findings indicate that our proposed Threat-Informed Defense-in-Depth risk management approach does provide improved risk management capabilities by combining both strategies.

Regarding the cybersecurity evaluation. The difference in the evaluation results between different evaluation methods highlights the importance of diversifying evaluation processes. Some approaches are less costly to implement (e.g., risk-based evaluation); however, their fidelity and accuracy have been questioned. An instance of this has been observed in this work. The risk evaluation assumes that if a mitigation method exists, it is sufficient to reduce the risk. However, the adversary emulation process has uncovered several discrepancies. For instance, a password policy exists regarding default credentials, during the risk assessment this information has rendered all relevant threats to be of negligible risks. During the adversary emulation process, 2 devices with default credentials were found. Hence, inaccurate risk assessment. This issue showcases a usability issue of the risk assessment process; it requires a lot of information that is not easily and readily available, such as the correct status of cybersecurity control coverage for all components in the network. Without active adversary emulation, knowing this with high confidence is not possible for all threats.

The simulated cybersecurity architecture implemented during the system analysis stage has highlighted several challenges in conducting the security functions in the context of the autoremote operational mode. The systems onboard the APS will need to be managed remotely due to the crew-less nature of the APS. This dictates the need to enable a remote management solution. One example is implemented through the installation of a remote desktop service for all components to facilitate their maintenance. This has been observed to be the case in the implemented milliAmper2 ferry. Another solution may include the utilization of Secure Shell Protocol (SSH). However, these particular solutions make the APS susceptible to remote attacks if the proposed cybersecurity architecture is not adopted. From the perspective of the security solutions, it has been observed that solutions that only function through a graphical user interface (GUI) are challenging to manage when integrated within the APS network.

So, solutions that provide Command Line Interface (CLI) are more suitable to facilitate their automation and remote management. Additionally, the proposed network architecture by DiD is challenged in the context of the autoremote operational mode (refer to Sect. 6.5). Therefore, we proposed the utilization of VPN tunnels to extend the perimeter of network security levels to span across different facilities. Further analysis of the impact of this proposition on the control and monitoring functions in the APS is within the scope of future work. Moreover, the GNS3 has provided very useful capabilities to demonstrate the feasibility of implementing and integrating different components. However, we have observed drastic network latency and packet loss which is linked to the nested virtualization capabilities. This drawback has led us to consider migrating the implementation to another platform for future work.

Finally, we acknowledge the following limitations in our proposed approaches and their application:

- Defense strategy comparison algorithm: The comparison is only based on the risk reduction without considering the cost of implementation. Also, the calculation relies on the controls in the $ATT\&CK$ framework. Some controls in DiD do not map to a clear control in the $ATT\&CK$ framework. Therefore, some controls do not account for a risk reduction such as "Establish contingency plans" (Other examples are found in Table 6).
- Cybersecurity evaluation: The simulation of the cybersecurity architecture relied on a group of commonly used open-source or free tools. Some tools are referenced in the literature such as the elastic stack for the SIEM component while others were chosen only for practical and compatibility reasons. On the other hand, the adversary emulation processes were restricted to allowed and feasible tests against the ferry which is only a small subset of the required tests for effective and comprehensive evaluation. Future works can investigate solutions to such limitations.

9 Conclusion

The ongoing digital transformation in the maritime domain has produced novel technologies and modes of operation. An instance of this is the proposition of Autonomous Passenger Ships (APS) for inland transportation. The APS technology is projected to operate under autoremote operational mode, autonomous when possible, remotely controlled when needed. With the recent calls for introducing cyber risk management capabilities in the maritime domain, investigating suitable means for the provisioning of cyber risk management functions for APS is a raising need. This paper investigates cyber risk management for the APS technology. Our research methodology follows a system engineering approach for the application of risk management functions during different system development phases. The approach relies on both the perspective of the classification society in the maritime domain and academia. The Defense-in-Depth (DiD) is observed to be an agreed-upon strategy for providing risk management capabilities. However, some limitations regarding its implementation for defending critical systems have been communicated. Therefore, we proposed a new risk management approach combining DiD with another risk management strategy named Threat-Informed Defense. Our proposed approach has been demonstrated to expand the provisioning of risk management functions using those proposed in the $ATT\&CK$ framework. Our approach is demonstrated through the development of a cybersecurity architecture for an APS use case. Afterward, a Systematic Literature Review (SLR) for cybersecurity evaluation in the maritime domain has been conducted and its results are presented. Observed approaches and artifacts from the SLR are then utilized for the evaluation of the proposed cybersecurity architecture for the APS. The evaluation has been conducted utilizing a system model as well as a real implemented prototype of an APS named milliAmper2. Several evaluation approaches have been deemed relevant to the current technology readiness level of the APS technology, namely risk-based evaluation, simulation and checklist, and adversary emulation. Risk evaluation reflects that the risk reduction in the proposed architecture is close to the optimal score considering it addresses the requirements as well as the identified risks, rendering other controls suggested in certain guidelines as non-critical. The adversary emulation and checklist evaluation approaches have identified vulnerabilities and unaddressed risks which have been observed to be a metric of successful risk management strategy. The simulation has uncovered challenges and considerations regarding the provisioning of risk management in the autoremote operational mode. This includes network segmentation, the reliance on non-IP communication, as well as the placement of SIEM components.

Moreover, the risk assessment process, which is an integral component of the proposed risk management approach, has identified new threats with varying level of sophistication. The proposed cybersecurity architecture has been tuned toward addressing such threats. For instance, a technology-specific intrusion detection system has been proposed and investigated in another work based on the work in this paper. This suggests that the communicated concerns regarding the limitations of DiD in defending against sophisticated attacks are addressed in the proposed architecture.

Several items have been identified suggesting the need for future work. Considering that autonomous vessels rely on machine learning and artificial intelligence, there is a lack of discussion related to the threat of adversarial machine learn-

ing in the maritime domain, also including other aspects in the strategy comparison algorithm such as the financial aspect for improved strategy analysis. Additionally, the inter-relations between safety and cybersecurity functions within the context of the APS require additional attention. Finally, additional work is needed relating to the adoption and automation of cybersecurity evaluation methods toward reducing the involvement of the human element.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital) Not applicable.

Data availability An implementation of the strategy comparison algorithm (Sect. 4) with the data used to generate the results in this paper can be found at the author's online repository [92].

Declarations

Conflict of interest Ahmed Amro declares that he has no conflict of interest. Vasileios Gkioulos declares that he has no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

A Mapping between *ATT&CK* and DiD elements

In this section, we discuss our developed mapping between the $ATT\&CK$ controls and DiD elements. This mapping is intended to facilitate the structured architecture development process in order to allocate the controls which are proposed from the risk assessment process and consider them during the architecture development. The mapping is done based on the description of the controls in the $ATT\&CK$ framework and the DiD element description. Table 6 depicts the outcome of our mapping efforts. The table reflects that the controls in $ATT\&CK$ do not support all the DiD elements, and others do not map to any DiD element. This indicates that aligning both would broaden the defensive capabilities of the target system.

Additionally, Table 6 reflects the sources discussing different DiD elements. The stakeholders' requirements that are related to cybersecurity span across all defense layers except physical security. Additionally, the variance of controls and DiD elements discussed in different sources demonstrates the need for continuous improvements in the risk management capabilities as no single source has considered all possible controls.

B Verification of requirements

A detailed analysis of the cybersecurity requirements verification has been conducted and is depicted in Table 7 to demonstrate the satisfaction of the communicated requirements by the proposed architecture. The table details the addressed requirements, their priority, the required verification criteria, the relevant architectural components, and efforts made to verify as well as evaluate the satisfaction of the requirements. The requirements are labeled using a three-level coding scheme (a-b-c). The first level (a) refers to the domain (S for Cybersecurity). The second level (b) refers to the sub-domain which are i) identification (I), ii) protection (P), iii) detection (D), iv) response, and v) recovery (R). Finally, the third level (C) refers to the number of the serial number of the requirement within its sub-domain.

Regarding the requirements priority, this property conveys the exact necessity level of each requirement as communicated by the stakeholders. Using the metrics in the MoSCoW requirement prioritization technique, most of the communicated requirements are "should" except two that are "must". The requirements with a priority "should" as communicated by one of the stakeholders suggests guidelines describing recommended processes to maintain equivalence with conventional designs [8]. In our previous work [9], we adopted these requirements with their indicated priority to propose a feasible architecture that is needed at the current project phase.

C Adversary emulation process

A summary of the adversary emulation process conducted against the milliAmpere2 ferry is shown in Table 8. Due to space limitations, the table presents only selected tests of the complete required set of tests. The shown tests cover all the attackers' objectives (i.e., tactics) proposed in the $ATT\&CK$ framework and a wide range of techniques and software to implement them. For each tactic, the relevant techniques, the test method, results, and proposed corrective action are presented.

Table 6 A mapping between DiD layers, elements, and their relevant $ATT\&CK$ controls. In addition to indication of the sources that discussed their need

Defense layers	Elements	Requirement	DNV	ICS DiD	BIMCO	$ATT\&CK$
Cyber security and risk management	Policies and procedures		✓	✓	✓	Account use policies, password policies
	Standards/recommendations and system documentation		✓	✓		N/A
	Risk assessment		✓	✓	✓	Threat intelligence program
	Maintain asset inventory	✓		✓		N/A
	Management support		✓			N/A
	Roles and responsibilities		✓		✓	N/A
Physical security			✓	✓	✓	Limit hardware installation, limit access to resource over network
Training and awareness	Training, awareness and competence		✓	✓	✓	User Guidance, user training, application developer guidance
Network architecture	Network segmentation		✓	✓	✓	Network segmentation, limit access to resource over network
Perimeter security	Firewalls		✓	✓	✓	Filter network traffic, limit access to resource over network, network allowlists, SSL/TLS inspection
	Access management	✓	✓	✓	✓	Access management, account use policies, attestation, authorization enforcement, caution with device administrator access, communication authenticity, environment variable permissions, human user authentication, multi-factor authentication, operational information confidentiality, password policies, privileged account management, software process and device Authentication, user account control, user account management, minimize wireless signal propagation
	VPN			✓	✓	Communication authenticity, encrypt network traffic, encrypt sensitive Information, operational information confidentiality
	Satellite and radio communication	✓			✓	Communication authenticity, encrypt network traffic, encrypt sensitive information, operational information confidentiality
Host security	Patch and vulnerability management	✓	✓	✓	✓	Deploy compromised device detection method, security updates, update software, use recent OS version, vulnerability scanning
	Virtual machines			✓		Application isolation and sandboxing

Table 6 continued

Defense layers	Elements	Requirement	DNV	ICS DiD	BIMCO	*ATT&CK*
	Malware protection	✓	✓		✓	Antivirus/antimalware, behavior prevention on endpoint, execution prevention, exploit protection, privileged process integrity
	Secure configuration of hardware and software	✓			✓	Active directory configuration, credential access protection, disable or remove feature or program, environment variable permissions, execution prevention, exploit protection, limit hardware installation, limit software installation, lock bootloader, operating system configuration, privileged account management, restrict file and directory permissions, restrict library loading, restrict registry permissions, restrict web-based content, software configuration, static network configuration, system partition integrity, user account control
	Email and web browser protection				✓	N/A
Security monitoring	Intrusion detection systems	✓	✓	✓	✓	Audit, behavior prevention on endpoint, communication authenticity, data loss prevention, deploy compromised device detection method, exploit protection, network intrusion prevention, privileged process integrity, SSL/TLS inspection
	Security audit logging	✓		✓		Audit, behavior prevention on endpoint, data loss prevention, deploy compromised device Detection method, exploit protection, privileged process integrity, SSL/TLS inspection, vulnerability scanning
	Security incident and event monitoring	✓	✓	✓	✓	Audit, behavior prevention on endpoint, data loss prevention, deploy compromised device detection method, exploit protection, privileged process integrity, SSL/TLS inspection, vulnerability scanning
Vendor management		✓		✓	✓	Application vetting, boot integrity, code signing, supply chain management
Incident response	Establish contingency plans		✓		✓	N/A
	Data recovery	✓			✓	Data backup, remote data storage
	Investigating cyber incidents and effective response	✓			✓	N/A

Table 6 continued

Defense layers	Elements	Requirement	DNV	ICS DiD	BIMCO	*ATT&CK*
	Losses arising from a cyber incident				✓	Communication authenticity, encrypt network traffic, encrypt sensitive Information, operational information confidentiality
N/A						Watchdog timers, redundancy of service, safety instrumented s, mechanical protection layers

D IP network simulation

D.1 Development of simulation network

Simulation is a proposed system analysis method by the ISO 15288 standard [93], and it is an observed approach in the maritime domain. [54] utilized simulation for the evaluation of a specific set of security controls against a specific set of attacks against maritime systems. [66] and [83] utilized simulated environments for the evaluation of several maritime systems and protocols. In this paper, simulation is utilized to verify the feasibility of integrating the cybersecurity architecture within the underlying communication architecture and to facilitate later security analysis. A prototype implementation of the IP-based components is provided using the GNS3 simulator [91].

As shown in Fig. 11, two physically distinct facilities were implemented at two different locations, emulating both the APS and the RCC. At each location, a dedicated workstation is interfaced with a physical router (i.e., gateway). The rationale behind this is two folds. The first is intended to create a physical division for emulating the remote control and monitoring of the RCC over the APS toward identifying possible challenges in the provisioning of security functions under the autoremote operational mode. The second is related to performance management. The implementation consists of many virtualized components that collectively consume plenty of resources. Therefore, logically distributing these resources over two workstations aids toward an improved testing environment.

The gateways are both interfaced with the same network outside our control. Upon our request, two static IP addresses were reserved to the gateways using Dynamic Host Configuration Protocol (DHCP) to emulate a connection over the Internet from an Internet Service Provider (ISP). The gateways are implemented using Cisco RV042 routers. This model provides several of the required capabilities, namely firewall, VPN, and DMZ. The firewall capability implements the dedicated firewall component discussed in Sect. 6.6.1. The VPN capability implements the required VPN tunnels discussed in Sect. 6.6.3. Finally, the DMZ capability implements the required DMZ discussed in Sect. 6.5. On the other hand, each workstation hosts a group of virtualized components emulating either the APS or the RCC networks using the GNS3 simulator. The Core/ Distribution (C/D) switches (C/D at the RCC, C/D A, and C/D B at the APS) are simulated using a Cisco IOS image of a Layer-3 switch, while other components are simulated using different appliances including Windows, Ubuntu Desktop, Ubuntu Server, Kali, and Docker containers. GNS3 provides the capability to interface a simulated component with a physical network using a component called "cloud"; this allows the C/D switches to be interfaced with the RV042 routers emulating realistic networking. Several of the required components discussed in Sect. 6 were implemented toward satisfying the established requirements. In the following subsections, detailed discussions are provided for each implemented component grouped according to the DiD architecture viewpoints. We would like to highlight that our choices of tools for the implementation are based on commonly used open-source or free tools. These tools were only used to serve the purpose of the analysis which is feasibility and identification of possible challenges in the management of the cybersecurity risks in autonomous and remotely controlled systems.

D.1.1 Risk management

In this section, we discuss our implementation of the components that supports the risk management functions discussed in Sect. 6.2. A server with the GLPI software [94] is utilized to support the required asset and user inventory functions discussed in Sect. 6.2.1. Considering that GLPI is managed through a web interface, the server is implemented within the RCC network due to the crewless nature of the APS. Nevertheless, a group of agents using the FusionInventory software [95] are installed at each endpoint and server at both facilities to send inventory information to the GLPI server. This setup is similar to the SIEM setup in figure 10a and has the same shortcomings discussed in Sect. 6.8.2.

D.1.2 Network architecture

In this section, we discuss our implementations and the analysis for different components in the network architecture

Table 7 Cybersecurity requirements satisfaction checklist

Reference as in [9]	Requirement description	Priority*	Verification criteria	Verification check	Existing and simulated components	Verification criteria	Verification check	Implemented and existing components
			Design level	APS model		Implementation Level	MilliAmpere2	
Regulator perspective	Risk management	M	Components supporting risk management activities exist	YES	IS3MS 6.2 risk assessment process	Components supporting risk management activities are implemented	YES	IS3MS 6.2 Risk assessment process
Service provider perspective	Ship registry	S	Components supporting secure ship registration exists	YES	Access management 6.6.4	Components supporting secure ship registration are implemented	YES	Implemented based on the 5 G routers at each site. A registration platform is provided by the supplier. The ferry and the RCC are registered and monitored.
Service provider perspective	Secure service provisioning	S	Security controls for service providers should be planned	YES	Vendor management 6.9	Security controls for service providers are implemented	YES	Agreements with different providers exist regarding cybersecurity controls. VPN and 2FA for 5 G routers, non-disclosure agreements with network providers, and others.
S-I-1	Cybersecurity management framework	S	Components supporting activities in an up-to-date framework are proposed	YES	IS3MS 6.2 Risk assessment process	Components supporting activities in an up-to-date framework are implemented	YES	IS3MS 6.2 risk assessment process
S-I-2	Map of IT installation and network architecture	S	Asset inventory capabilities exist	YES	Asset and user inventory 6.2.1 GLPI software [94]	Detailed inventory of components and network architecture is performed	YES	Detailed and updated system and network diagrams exist.
S-I-3	Inventory of user accounts and privileges	S	Account inventory capability exists	YES	Access management 6.6.4 OpenLDAP [99]	Network user management capability is implemented	Partially	Distributed: some components have a local user management capability, while others don't.
S-P-1	User management	S	User management capability exists	YES	Access management 6.6.4 OpenLDAP [99]	User management capability is implemented with best practices in secure authentication	Partially	Some components have been observed to implement strong password requirements. On the other hand, some components were found to retain default credentials.

Table 7 continued

Reference as in [9]	Requirement description	Priority*	Verification criteria	Verification check	Existing and simulated components	Verification criteria	Verification check	Implemented and existing components
			Design level	APS model		Implementation Level	MilliAmpere2	
S-P-2	Regular Updates	M	Software updating capability exists	YES	Patch and vulnerability management 6.7.1 Wazuh [105]	Software updating according to an update policy is implemented	Partially	Some components have updating procedures while others don't.
S-P-3	Secure protocols	S	Secure protocols are proposed when applicable	YES	Network perimeter security 6.6 Cisco RV042 Router	Secure protocols are implemented when applicable	YES	Site-to-Site VPN was deemed an important controls and was implemented using OpenVPN cloud solution.
S-P-4	Malware protection	S	Malware protection capability exists	YES	Malware protection 6.7.2 ClamAV antivirus [102]	Malware protection capability is implemented	Unknown	Access to some components was restricted and no information was provided regarding the existence of malware protection.
S-P-5	Cybersecurity training	S	Relevant areas for training are proposed	YES	Training and awareness 6.4	Specific training exercises are proposed	NO	No training exercises have yet been proposed.
S-P-6	Regular software security analysis	S	Components supporting security analysis are proposed	YES	Patch and vulnerability management 6.7.1 Wazuh [105]	Software security analysis is conducted based on a suitable policy	Partially	Network vulnerability scanning was conducted. No information regarding software security analysis.
S-D-1	Monitoring capabilities	S	Monitoring capabilities should exist	YES	Security monitoring 6.8 Wazuh [105] and Snort [104]	Monitoring capabilities are implemented	Partially	A host-based intrusion detection exists for some components. Some components provide security alerting features.
S-R-1	Incident response plan	S	Components supporting incident response plans are proposed	YES	Incident response 6.10	Incident response plans are formulated and implemented when applicable	Partially	No plans specifically exist for cybersecurity related incidents. However, intervention plans exist in case of safety-related incidents. Emergency control team shall intervene.
S-R-2	Backup facilities	S	Backup facilities exist	YES	Backup 6.7.4 BorgBackup software [103]	Backup facilities are implemented with a suitable backup policy	Partially	A data backup service is implemented at RCC. No backup facilities exist at the ferry.

* MoSCoW rule (S: Should, M: Must)

Table 8 A summary of planned and executed tests in the adversary emulation process

ATT&CK tactic	Test objective	ATT&CK techniques	Test method	Results	Corrective action
Reconnaissance	Identify remotely open services	Gather victim host information (T1592), search open websites/domains (T1593)	Searching internet scanners (Shodan, Censys, and BinaryEdge) using the ferry's 5 G router's public IP address	Only shodan identified an open port for an IP camera at some time in the past. The port was not open at the time of the test	None
		Network service scanning (T1018), remote system discovery (T0846), active scanning (T1595)	Scanning the ferry's 5 G router's public IP address using Nmap	2 open ports for the router remote authentication and signaling services	None
	Learn ferry network topology	Remote system discovery (T0846), active scanning (T1595)	Using netdiscover to identify hosts and networks. This was only possible after gaining access to the network	2 local networks were identified. One by the 5 G router and another by a network switch. In total, 13 hosts were discovered	NIDS tuning to detect network scanning
	Discover vulnerabilities	Search open technical databases (T1596)	Using the national vulnerability database (NVD) to search for vulnerabilities in the network components	Several vulnerabilities were found for one critical component in the network. One vulnerability has a 9.8 CVSS rating	Updating the component to latest version
Initial access	Gain access to the ferry network	Transient cyber asset (T0864), hardware additions (T1200)	Insert a Raspberry Pi into the network	Sufficient controls exist providing physical security to mitigate this threat. However, permission to insert the Pi was granted to allow further tests	NIDS tuning to detect newly installed devices in the network
	Remotely access the 5 G network	Valid accounts (T0859), default credentials (T0812)	Assuming the attacker acquired the user credentials of the 5 G network management platform. Using the stolen credentials to access the network	The platform implements a 2FA service associated with an authenticator mobile application	None

Table 8 continued

ATT&CK tactic	Test objective	ATT&CK techniques	Test method	Results	Corrective action
Collection	Sniff network traffic	Network sniffing (T0842 or T1040)	Using Wireshark to sniff network traffic. Identify and collect navigation messages for planning further attacks	Network traffic is captured at several intervals including NMEA messages emitted from the GPS and broadcasted within the network	Limit access to resource over network
		Adversary-in-the-middle: ARP cache poisoning (T1557.002)	Using ettercap to run ARP spoofing attack to sniff unicast traffic between different hosts in the network	Only ICMP messages between hosts were collected	NIDS tuning to detect ARP spoofing
Execution	Run a script with several commands to collect host information	Hardware additions (T1200), system information discovery (T1082)	Using a USB stick with customized autorun function	No permission was granted from the network vendor to run this test	None*
Exfiltration	Transfer captured network traffic to a remote location	Automated exfiltration (T1020), exfiltration over web service (T1567)	Transferring the captured network traffic from the Raspberry Pi to a remote location	Was conducted on several occasions without any obstruction	Data loss prevention solution
Discovery	Identify hosts and networks	Remote system discovery (T0846), active scanning (T1595)	Using netdiscover to identify hosts and networks	2 local networks were identified. One by the 5 G router and another by a network switch. In total, 13 hosts were discovered	NIDS tuning to detect network scanning
	Identify open services in the network	Network service scanning (T1018), remote system discovery (T0846), active scanning (T1595)	Using Nmap to identify network services	A lot of open services were discovered ranging from HTTP, HTTPS, FTP, SSH,RDP, telnet, and NFS	NIDS tuning to detect network scanning

Table 8 continued

ATT&CK tactic	Test objective	ATT&CK techniques	Test method	Results	Corrective action
Lateral movement	Identify remote services that can allow lateral movement		Using Nmap to identify remote desktop services	The majority of components have open ports for well-known remote desktop software and network sharing service	Updating the component to the latest version and enforcing a password policy
	Remotely access a host from another	Remote services: remote desktop protocol (T1021.001)	Using the identified RDP software, attempt to access other devices	No permission was granted from the network vendor to run this test	None*
	Using default credentials to access other components	Valid accounts (T0859), default credentials (T0812)	Using default credentials found online for accessing network devices	2 devices were found to operate with the default credentials for the HTTP interface	Enforcing a password policy
Command & control	Establish C&C channel between a victim and a remote C&C server	Encrypted channel (T1573)	Using a covert channel software (e.g., Recub) run a client on a host in the network and run the server on a remote location	No permission was granted from the network vendor to run this test	None*
Credential access	Identify default or weak passwords	Brute force (T1110)	Using metasploit to brute force open network services	No permission was granted from the network vendor to run this test	
	Sniff credentials	Network sniffing (T0842 or T1040)	Using wireshark to sniff network traffic. Identify and collect credentials	No credentials were identified. Several display filters were used. However, no network traffic was found for known remotely accessible services	None**
Persistence	Access other hosts in the network to maintain a foothold	Remote services: remote desktop protocol (T1021.001)	Using the identified RDP software, attempt to access other devices	No permission was granted from the network vendor to run this test	None*

Table 8 continued

ATT&CK tactic	Test objective	ATT&CK techniques	Test method	Results	Corrective action
Defense evasion	Will the network scanning be detected	Network service scanning (T1018), remote system discovery (T0846), active scanning (T1595)	Using Nmap to scan the network with different configurations ranging from aggressive to polite scans	Aggressive scans were detected and stopped. Polite scans were not stopped. The status of the detection is unknown	NIDS tuning to detect network scanning
	Changing the IP address	Fallback channels (T1008)	Manually configuring the IP address of the Pi	When the scans were stopped, the Pi lost access to the network. However, access was regained after manually changing the IP address	NIDS tuning to detect IP changes in the network
Privilege escalation	Gain administrative privileges using operating system vulnerabilities	Abuse elevation control mechanism (T1548)	Run a pre-built malware	No permission was granted from the network vendor to run this test	None*
Impair process control	Modify control parameters	Manipulation of control (T0831)	Using ettercap, manipulate control commands in the network		
Inhibit response function	Drop navigation messages	Denial of view (T0815)	Using ettercap filters to drop some navigation messages (NMEA)	Attack did not succeed	None**
Network effect	Manipulate network traffic	Manipulation of view (T0832)	Using Ettercap, manipulate some navigation messages (NMEA)	Attack did not succeed	
	Jamming GPS data	Denial of view (T0815), network denial of service (T1464)	Using GPS jammer to impact positioning data collection	Future work	
Remote service effect	Obtain device backups stored remotely	Obtain device cloud backups (T1470)	Obtain online stored configurations of hosts	The configuration files of the 5G routers are secure with 2FA authentication	None
Impact	Manipulate network traffic	Manipulation of view (T0832)	Using Ettercap, manipulate some navigation messages (NMEA)	Attack did not succeed	None**
	Stealing operational information	Theft of operational information (T0882)	Identifying proprietary information from the network traffic	Proprietary information was identified in the network traffic related to the vendor's navigation system	Limit access to resource over network

*None at the moment due to lack of information as a result of not allowing to run the tests**None at the moment due to lack of information as a result of insufficient testing. Additional testing in the future is needed

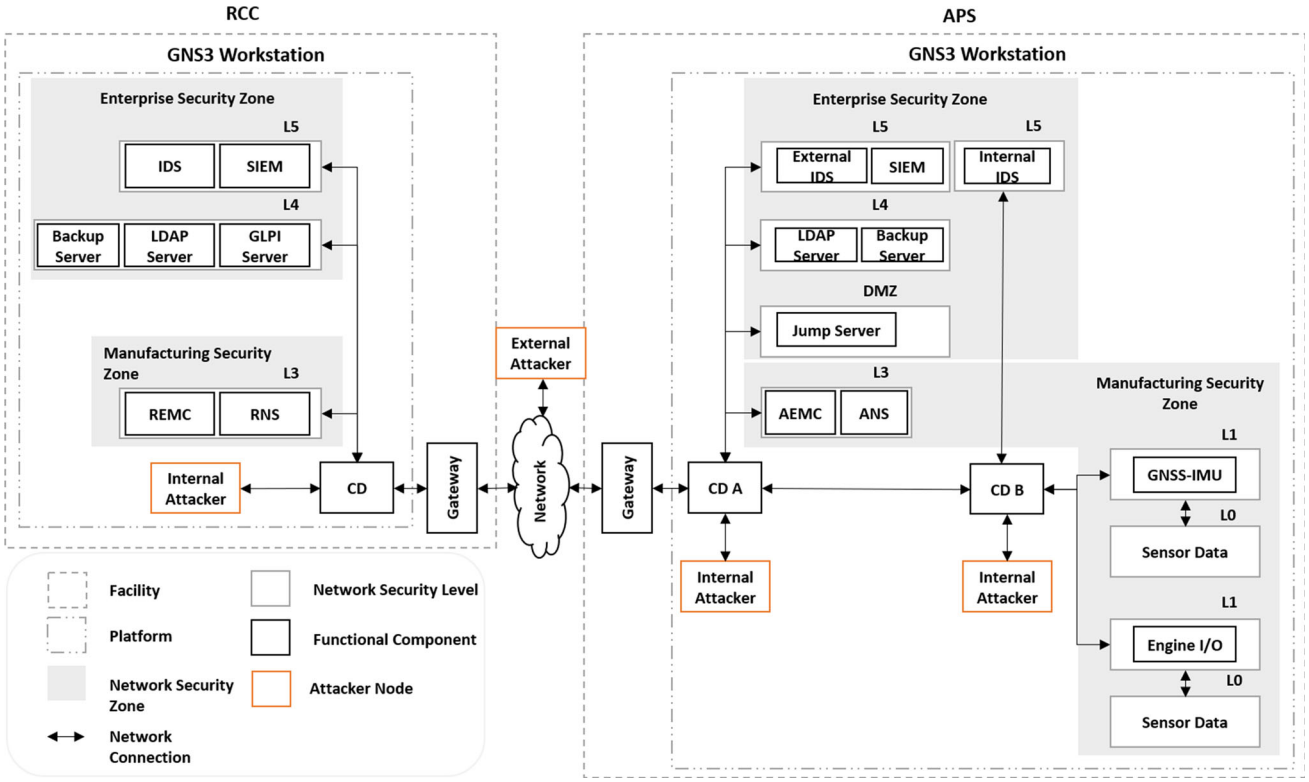

Fig. 11 Overview of the implemented architecture

discussed in Sect. 6.5, particularly the C/D switches, the DMZ, and the jump server. The C/D switches are already proposed in the communication architecture. They are utilized in the cybersecurity architecture to realize different network security zones and levels discussed in Sect. 6.5, the firewall capabilities discussed in Sect. 6.6.1 as well as the component-to-component access management discussed in Sect. 6.6.4. The security zones and levels are implemented using VLANs mapped to different network levels. The firewall capabilities, as well as the component-to-component access management, are implemented using ACL. For instance, the GNSS-IMU component is programmed to transmit sensor data to the ANS only. An ACL rule is created to allow this communication and deny any other component to be reached from the GNSS-IMU.

Regarding the DMZ, an IP address has been assigned to the jump server from the network that is outside our control which emulates the internet. The public IP address has been mapped to the local IP address using the one-to-one NAT technique configured at the APS gateway. Firewall rules were created to restrict inbound access from the server at the DMZ into the internal network to only RDP connections.

As discussed previously in Sect. 6.6.4, a jump server is required for remote maintenance. It is advised to be placed at the DMZ and access to it should be secure using 2FA. This has been implemented using a windows workstation placed at the DMZ. The 2FA is implemented using the free software from Cisco called "Duo" [96]. Duo has been installed at the jump server and is linked to a mobile phone and enforces a policy to approve any remote access using Remote Desktop Protocol (RDP) using the assigned mobile phone through a dedicated app.

D.1.3 Network perimeter security

In this section, we discuss our implementations and the analysis for different components in network perimeter security including the firewalls (Sect. 6.6.1), the VPN tunnels (Sect. 6.6.3), and Access Management (Sect. 6.6.4).

The main firewalls are implemented on the gateways. Additional firewall capabilities are implemented at the C/D switches for achieving the network architecture. Moreover, host-based firewalls are enabled with customized rules to allow the traffic for the required services such as the SIEM agents.

Regarding the implemented VPN tunnels. The implemented protocol is IPSec with strong encryption and policy-enforced complex shared key. We have utilized the iperf tool [97] for latency testing with the activation of VPN tunnels. The average latency was observed to be 1,94 ms for the link between the two workstations which exists outside the GNS3 implementation. This is well within the acceptable

latency for the ship to shore communication suggested by the MUNIN project which is one second [98]. However, we have observed very high latency in the GNS3 implementation which is related to the virtualization technology. For instance, the average latency at the bridged interface between the gateway and the C/D switch is 12,184 ms and it reaches 133,477 ms between the ANS and the RNS with 19% packet loss. This indicates that GNS3 is not suitable for the performance evaluation of the security controls.

An LDAP server running OpenLDAP [99], an open-source software implementing the Lightweight Directory Access Protocol [100] is implemented at each facility to realize the required User Access Management discussed in Sect. 6.6.4. A network domain was created as well as user accounts for different endpoints. Then, the endpoints are joined to the created domain. The open-source pGina plugin [101] is implemented to integrate the endpoints with the Windows operating system with the Linux LDAP server.

D.1.4 Host security

In this section, we discuss our implementations and the analysis for different components related to host security, particularly, malware protection, backup, as well as application isolation, and sandboxing.

The malware protection component has been implemented using the open-source ClamAV antivirus engine [102]. This capability realizes the required malware protection function discussed in Sect. 6.7.2.

Backup facilities have been implemented at both the APS and the RCC utilizing the open-source BorgBackup software [103]. A script was written to perform a daily backup of the APS and the RCC endpoints with encryption and compression of the archives.

The development of the APS navigational applications is outside the scope of this paper. Nevertheless, we have developed a group of scripts to receive or generate simulated sensor data and transmit them to the processing and control components in the ASC and the RSC. These scripts were developed as docker containers to realize the application isolation requirement.

D.1.5 Security monitoring

In this section, we discuss our implementations and the analysis for different components related to Security Monitoring, particularly, the IDS components, and the SIEM components.

Two types of IDS are implemented. Host-based IDS (HIDS) and Network-based IDS (NIDS). HIDSs are implemented using the Wazuh software. This component is installed on all devices including the backup ANS and backup AEMC as discussed in Sect. 6.8.1. This allows for customized rules for these endpoints particularly to monitor the out-of-band emergency communication channel with ECT. On the other hand, the NIDSs are implemented using Snort [104]. Three Snort appliances are implemented and connected to the networks at each facility: two at the APS and one at the RCC, to realize the required IDS capability discussed in Sect. 6.8.1 and shown in Fig. 9. This allows for customized rules at each Snort node focusing on a specific set of expected communication flows.

The SIEM components have been implemented using the open-source security platform Wazuh [105]. It is built on top of the elastic stack and provides a wide range of cybersecurity capabilities. With regards to the APS cybersecurity requirements, Wazuh provides several capabilities; among other things, monitoring and logging (Sect. 6.8), incident response (Sect. 6.10), system hardening (Sect. 6.7.5), and vulnerability management (Sect. 6.7.1). We implemented two SIEM nodes, one at the APS and another at the RCC as suggested in Sect. 6.8.2.

D.2 Adversary emulation

Having the simulated implementation in section D allows for conducting hands-on adversary emulation. Conducting adversary emulation against the simulated implementation aims to help in understanding the impact of the autoremote operational mode on cybersecurity functions and how would they withstand realistic cyber attack techniques. Based on that, we define a group of attack scenarios consisting of different $ATT\&CK$ tactics (i.e., kill chain phase) and techniques against different components in order to showcase the concept of layered defenses. Different attacks techniques applied in this section are a result of the conducted risk assessment process for the APS proposed in our earlier work [37] and discussed briefly in Sect. 2.2.

D.2.1 External attacker aiming to impact the APS operations

In this section, we will describe a fictional attack scenario to showcase the role of different mitigation methods at each defense layer. Although it is fictional, we have utilized the prototype implementation discussed in section D to emulate some of the attack techniques in order to obtain a realistic attack flow.

In this scenario, an external attacker aims to gain a foothold into the network toward impacting the APS operations in any way possible. The attack exploits the remote desktop feature in the APS which is enabled to allow remote maintenance due to the autoremote operational mode. Figure 12 depicts an attack tree for achieving the attacker objective. The figure also depicts the different stages of the attack, the attacked component as well as the mitigation methods that need to fail for this attack to succeed. A detailed description of the attack scenario is described below:

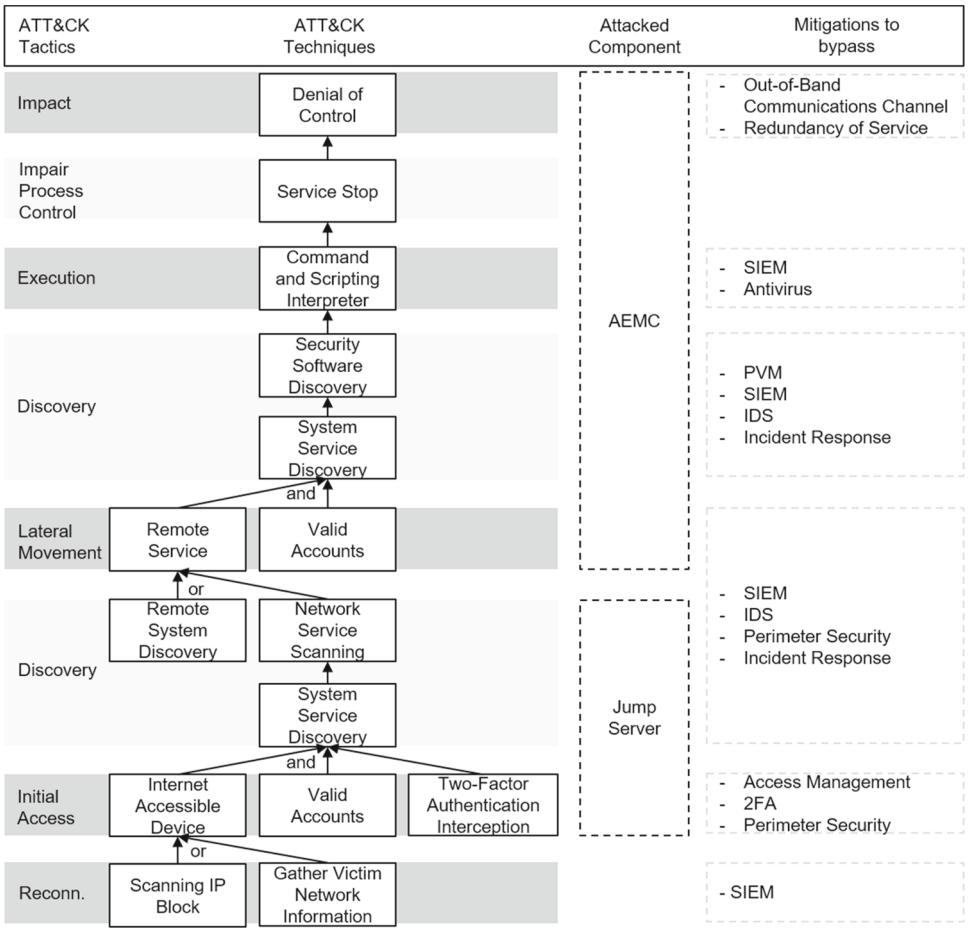

Fig. 12 An attack tree of a possible scenario

- *Reconnaissance*: no reconnaissance techniques have been considered during the risk evaluation considering that reconnaissance techniques occur outside the control of the cybersecurity architecture. Nevertheless, the attacker can perform "Scanning IP Blocks" or "Gather Victim Network Information" to learn more about the network and the services it provides. Assuming the attacker has previous knowledge of the public IP addresses of the target network, now the attacker can learn that the jump server at the DMZ is publicly open.
- *Initial Access*: to achieve a foothold into the network, the external attacker utilizes "Internet Accessible Device". In the simulated architecture, several devices are connected to the internet at both the RCC and the APS. One target can be the jump server using a remote desktop client. The attacker is initially faced with an authentication request to provide credentials to access the jump server (access management). Assuming the attacker can guess the credentials (i.e., default credentials), then the attacker gains initial access through "Valid Accounts". Then, the attacker faces the next security control which is the 2FA. Considering that this 2FA is configured to approve access to RDP connections to the jump server by a specific mobile phone outside the attacker's reach, the attack fails. Assuming the attacker can conduct "Two-Factor Authentication Interception" to bypass this security control; similar to the Chimera group [106]. Then the attacker can access the jump server and gain the initial foothold.
- *Discovery*: Assuming the attacker has access to the jump server. The next step is to understand the environment. Initially, the attacker performs "System Service Discovery" to understand the running services on the accessed machine. Considering it's a jump sever and no other important services are hosted on it. The attacker decides to locate a more critical target. So, the attacker performs "Network Service Scanning" or "Remote System Discovery" to discover the running services in the network in an attempt to discover vulnerabilities. Considering that the traffic to and from the DMZ is heavily filtered using ACLs, the attacker is unable to discover services other than the RDP to other hosts in the network. Therefore, the attacker needs to perform a technique to achieve "Lateral Movement" to move within the network to another location with more observability to the network. At the same time, the attacker is performing the activities at the discovery stage, the IDS and the SIEM have raised

indicators that some discovery activities are being conducted. If security personnel at the RCC is monitoring these logs and deem suspicious behavior is happening, incident response activities could be initiated. For the sake of this scenario, let's assume that the attacker is still undiscovered.

- *Lateral Movement*: The attacker performs lateral movement from the jump server through the available "Remote Services" (i.e., RDP) on the AEMC and pivots to that location using the same valid credentials used at the jump server.
- *Execution*: Assuming the attacker has access to the AEMC. The discovery phase is conducted again to understand the environment. Considering the critical role of AEMC in the control functions, the attacker is able to recognize an industrial control software using "System Service Discovery". Due to the PVM component, this software is patched, and the attacker is unable to discover a vulnerability to exploit. Assuming this software has a non-patched vulnerability that allows for a "Denial of Service" (DoS) attack and there is an available malware that is able to launch the exploit. To avoid detection, before running the malware, the attacker performs a "Security Software Discovery" and discovers the availability of the antivirus software which the attacker discovers is able to recognize the malware binary and prevents it from running as well as alert the RCC of a running attack. So, the attacker utilizes "Command and Scripting Interpreter" to build a custom exploit and execute it.
- *Impair Process Control*: Assuming the DoS attack is in the form of a "Service Stop" that impairs the AEMC from performing control functions of the thrusters.
- *Impact*: Assuming the attack succeeded, the passengers on the APS should feel something out of the ordinary. They can use the previously proposed emergency push button to inform the RCC and the ECT of a problem so they can initiate a suitable response plan. An existing response plane is to intervene using the Out-of-Band communication channels and utilize the redundant control system to navigate the APS to safety (Sect. 6.10).

D.2.2 Ship to shore communication eavesdropping

In this section, we will describe two attack scenarios in which the attackers aim to eavesdrop on the communication flows between the APS and the RCC. We utilized the prototype implementation to perform a defensive engagement of the threat to evaluate the proposed mitigation methods.

In the first attack, a passenger aims to gain initial access to the network by performing a "Hardware Additions" technique. The passenger inserts a computer into the "C/D tier A" switch and attempts to sniff the traffic. Assuming that no physical barriers are in place, the first security control that the attacker faces is the static network configuration which is a result of the system hardening discussed in Sect. 6.7.5. Assuming that the attacker has previous knowledge of different sub-nets and can assign a static IP address. Then, the attacker can perform the "Man-in-the-Middle: ARP Cache Poisoning" technique to be able to perform "Network Sniffing" of the traffic. Security events generated from these activities can be observed at the SIEM, if an operator on the RCC is monitoring these events, an incident response plan can be initiated.

In the second attack, an external attacker aims to eavesdrop on the ship to shore communication. Assuming the attacker has previous knowledge of the public IP addresses within the APS ecosystem. Then, the attacker employs "Network Service Scanning" using tools such as $NMAP$ [107] to discover the services from each host with public IP. Utilizing NMAP OS identification capability, the attacker can identify that two of the public IP addresses are assigned for the gateways (Cisco RV042 routers). Moreover, both routers have port 60443 open which indicates the possible existence of VPN tunnels. Scanning the third IP address discloses the RDP service on the jump server. The attacker then attempts to perform the "Man-in-the-Middle: ARP Cache Poisoning" technique to be able to perform "Network Sniffing" of the traffic, but the attack failed. The reason this attack failed is due to a requirement in the vendor management process (Sect. 6.9) to have a countermeasure for spoofing attacks, and indeed, the RV042 has such capability [108]. Assuming no such requirement exists, and the gateway doesn't have such capability. The traffic between the two gateways passes an external network that is outside the control of the cybersecurity architecture. Therefore, the implemented VPN tunnels implemented using the IPSec protocol shield the ship-to-shore communication from "Eavesdrop on Insecure Network Communication" techniques.

References

1. Fruth, Markus, Teuteberg, Frank: Digitization in maritime logistics-what is there and what is missing. Cogent Bus. Manag. **4**(1), 1411066 (2017)
2. Sea passenger statistics 2020: Short sea routes. http://bit.ly/PassengerStatistics2020. Accessed 11 Oct 2021
3. Lam, Y.: Technology will help maritime transport navigate through the pandemic-and beyond. https://blogs.worldbank.org/transport/technology-will-help-maritime-transport-navigate-through-pandemic-and-beyond, November (2020). Accessed 05 Jan 2022
4. Transportation statistics annual report 2020. https://www.bts.gov/tsar, Dec (2020)
5. Domestic transport. https://www.ssb.no/en/transport-og-reiseliv/statistikker/transpinn. Accessed 11 Oct 2021
6. Nfas - norwegian projects. https://nfas.autonomous-ship.org/resources_page/projects-page/

7. NTNU Autoferry. Autoferry - Autonomous all-electric passenger ferries for urban water transport. https://www.ntnu.edu/autoferry, (2018)
8. DNV GL. Dnvgl-cg-0264: Autonomous and remotely operated ships. (2018)
9. Amro, Ahmed, Gkioulos, Vasileios, Katsikas, Sokratis: Connect and protect: Requirements for maritime autonomous surface ship in urban passenger transportation. In: Computer Security, pp. 69–85. Springer, (2019)
10. Amro, A., Gkioulos, V., Katsikas, S.: Communication architecture for autonomous passenger ship. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, p. 1748006X211002546, (2021)
11. Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., Hahn, A.: Nist special publication 800-82, revision 2: Guide to industrial control systems (ics) security. National Institute of Standards and Technology, (2014)
12. Fielder, A., Li, T., Hankin, C.: Defense-in-depth vs. critical component defense for industrial control systems. In: 4th International Symposium for ICS & SCADA Cyber Security Research 2016 4, pp. 1–10, (2016)
13. zvelo. Fight ransomware with defense in depth. https://zvelo.com/fight-ransomware-with-defense-in-depth/. Accessed 11 Oct 2021
14. MITRE. Threat-informed defense. https://www.mitre.org/news/focal-points/threat-informed-defense. Accessed 05.01.2022
15. The Maritime Safety Committee. International maritime organization (imo) (2017) guidelines on maritime cyber risk management. http://bit.ly/MSC428-98
16. The Maritime Safety Committee. Interim guidelines on maritime cyber risk management (msc-fal.1/circ.3/rev.1). https://cutt.ly/6R8wqjN
17. Barrett, M.P.: Framework for improving critical infrastructure cybersecurity. In: National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep, (2018)
18. Boyens, J., Paulsen, C., Moorthy, R., Bartol, N., Shankles, S.: Nist special publication 800-161: Supply chain risk management practices for federal in-formation systems and organizations. In: NIST. April, (2015)
19. Savold, R., Dagher, N., Frazier, P., McCallam, D.: Architecting cyber defense: A survey of the leading cyber reference architectures and frameworks. In: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 127–138. IEEE, (2017)
20. Americas Headquarters. Cisco safe reference guide. (2009)
21. Chappelle, D.: Security in depth reference architecture release 3.0. In: White paper, Oracle Corporation, Redwood Shores, (2013)
22. McCallam, D.: An analysis of cyber reference architectures. In: Presented at NATO 2012 Workshop with Industry on Cybersecurity Capabilities, (2012)
23. Fabro, M., Gorski, E., Spiers, N., Diedrich, J., Kuipers, D.: Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies. DHS Industrial Control Systems Cyber Emergency Response Team, (2016)
24. DK Rasmus Nord Jorgensen in Copenhagen. Bimco: The guidelines on cyber security onboard ships. https://iumi.com/news/blog/bimco-the-guidelines-on-cyber-security-onboard-ships
25. Svilicic, B., Kamahara, J., Rooks, M., Yano, Y.: Maritime cyber risk management: an experimental ship assessment. J. Navig. **72**(5), 1108–1120 (2019)
26. Grigoriadis, C., Papastergiou, S., Kotzanikolaou, P., Douligeris, C., Dionysiou, A., Elias, A., Bernsmed, K., Meland, P., Kamm, L.: Integrating and validating maritime transport security services: Initial results from the cs4eu demonstrator. In: 2021 Thirteenth International Conference on Contemporary Computing (IC3-2021), pp. 371–377, (2021)
27. Kavallieratos, G., Katsikas, S.: Managing cyber security risks of the cyber-enabled ship. J. Mar. Sci. Eng. **8**(10), 768 (2020)
28. ISO. Iso 31000:2018 risk management - guidelines, (2018)
29. Stouffer, Keith, Falco, Joe, Scarfone, Karen, et al.: Guide to industrial control systems (ics) security. NIST Spec. Publ. **800**(82), 16–16 (2011)
30. Rajaram, P., Goh, M., Zhou, J.: Guidelines for cyber risk management in shipboard operational technology systems. arXiv preprint arXiv:2203.04072, (2022)
31. DNV. Ddnvgl-cg-0325: Cyber secure class notation. https://rules.dnvgl.com/docs/pdf/DNVGL/CG/2020-10/DNVGL-CG-0325.pdf, (2020)
32. Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B.: Mitre att&ck: Design and philosophy. Tech. Rep. (2018)
33. Enisa threat landscape 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021, (2021)
34. How mitre attck alignment supercharges your siem. https://www.securonix.com/how-mitre-attack-alignment-supercharges-your-siem/, (2019)
35. Enhancing with mitre. https://documentation.wazuh.com/current/user-manual/ruleset/mitre.html, (2021)
36. Atomic red team. https://github.com/redcanaryco/atomic-red-team
37. Amro, A., Gkioulos, V., Katsikas, S.: Assessing cyber risk in cyber-physical systems using the attack framework. Submitted for review to ACM Transactions on Privacy and Security (TOPS), Association for Computing Machinery, New York, USA. https://doi.org/10.1145/3571733, (2022)
38. IEC 60812 Technical Committee et al. Analysis techniques for system reliability-procedure for failure mode and effects analysis (fmea). (2018)
39. Shostack, A.: Threat Modeling: Designing for Security, Wiley Publishing. 2014
40. Mihai, I.-C., Pruna, S., Barbu, I.-D.: Cyber kill chain analysis. Int. J. Info. Sec. Cybercrime **3**, 37 (2014)
41. Houmb, S.H., Franqueira, V.N.L., Engum, E.A.: Quantifying security risk level from cvss estimates of frequency and impact. J. Syst. Softw. **83**(9), 1622–1634 (2010)
42. Douglas, B.W. et al. Introduction to graph theory, vol. 2. Prentice hall Upper Saddle River, NJ, (1996)
43. Dnvgl-rp-0496 recommended practice: Cyber security resilience management for ships and mobile offshore units in operation. https://www.dnv.com/maritime/dnv-rp-0496-recommended-practice-cyber-security-download.html, (2021). Accessed on 16 Feb 2022
44. Drougkas, A., Sarri, A., Kyranoudi, P.: EU Agency for cybersecurity. Guidelines - cyber risk management for ports. https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports, 12 (2020)
45. IEC ISO. Ieee: Iso/iec/ieee 42010: 2011-systems and software engineering–architecture description. Proceedings of Technical Report, (2011)
46. Feiler, P.H., Gluch, D.P., Hudak, J.J.: The architecture analysis & design language (aadl): An introduction. Technical report, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, (2006)
47. SEI AADL Team et al. An extensible open source aadl tool environment (osate). In: Software Engineering Institute, 2006
48. de Saqui-Sannes, P., Hugues, J., et al.: Combining sysml and aadl for the design, validation and implementation of critical systems. In: ERTS 2012, (2012)
49. Kordon, F., Hugues, J., Canals, A., Dohet, A.: Embedded systems: analysis and Modeling with SysML, UML and AADL. John Wiley & Sons, (2013)

50. Okoli, C., Schabram, K.: A guide to conducting a systematic literature review of information systems research. (2010)
51. Mavroeidis, V., Bromander, S.: Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In: 2017 European Intelligence and Security Informatics Conference (EISIC), pp. 91–98. IEEE, (2017)
52. Threat-based defense. https://www.mitre.org/capabilities/cybersecurity/threat-based-defense
53. Iec, I.S.O., ieee 15288,: Systems and software engineering-Content of systems and software life cycle process information products (Documentation), p. 2015. Geneva, Switzerland, International Organization for Standardization/International Electrotechnical Commission (2015)
54. Babineau, G.L., Jones, R.A., Horowitz, B.: A system-aware cyber security method for shipboard control systems with a method described to evaluate cyber security solutions. In: 2012 IEEE Conference on Technologies for Homeland Security (HST), pp. 99–104. IEEE, (2012)
55. Enoch, S.Y., Lee, J.S., Kim, D.S.: Novel security models, metrics and security assessment for maritime vessel networks. Comput. Netw. **189**, 107934 (2021)
56. Havdal, G., Heggelund, C.T., Larssen, C.H.: Design of a small autonomous passenger ferry. Master's thesis, NTNU, (2017)
57. Aps communication architecture aadl model. https://github.com/ahmed-amro/APS-Communication_Architecture.git. Accessed: 10 June 2022
58. CORE Ramboll. Advokatfirma: Analysis of regulatory barriers to the use of autonomous ships: Final report. Danish Maritime Authority, Copenhagen, pp. 1374–1403, (2017)
59. Veritas, B.: Ni641 guidelines for autonomous shipping. (2019)
60. Goudossis, A., Katsikas, S.K.: Towards a secure automatic identification system (ais). J. Mar. Sci. Technol. **24**(2), 410–423 (2019)
61. Kessler, G.C.: Protected ais: a demonstration of capability scheme to provide authentication and message integrity. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 14(2), (2020)
62. Goudosis, A., Katsikas, S.K.: Secure ais with identity-based authentication and encryption. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 14(2), (2020)
63. Aziz, A., Tedeschi, P., Sciancalepore, S., Di Pietro, R.: Secureais-securing pairwise vessels communications. In: 2020 IEEE Conference on Communications and Network Security (CNS), pp. 1–9. IEEE, (2020)
64. Iphar, Clément., Ray, Cyril, Napoli, Aldo: Data integrity assessment for maritime anomaly detection. Expert Syst. Appl. **147**, 113219 (2020)
65. Blauwkamp, D., Nguyen, T.D., Xie, G.G.: Toward a deep learning approach to behavior-based ais traffic anomaly detection. In: Dynamic and Novel Advances in Machine Learning and Intelligent Cyber Security (DYNAMICS) Workshop, San Juan, PR. Retrieved from http://faculty.nps.edu/Xie/papers/ais_analysis_18.pdf, (2018)
66. Balduzzi, M., Pasta, A., Wilhoit, K.: A security evaluation of ais automated identification system. In: Proceedings of the 30th annual computer security applications conference, pp. 436–445, (2014)
67. Boudehenn, C., Jacq, O., Lannuzel, M., Cexus, J.-C., Boudraa, A.: Navigation anomaly detection: an added value for maritime cyber situational awareness. In: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1–4. IEEE, (2021)
68. Lee, D.-K., Miralles, D., Akos, D., Konovaltsev, A., Kurz, L., Lo, S., Nedelkov, F.: Detection of gnss spoofing using nmea messages. In: 2020 European Navigation Conference (ENC), pp. 1–10. IEEE, (2020)
69. Amro, A.: Oruc, Aybars, Gkioulos, Vasileios, Katsikas, Sokratis: navigation data anomaly analysis and detection. Information **13**(3), 104 (2022)
70. Joe, T., Eggert, L., Wang, Y.: Use of ipsec transport mode for dynamic routing. Request for Comments (RFC), 3884, 2004
71. Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., Zorn, G.: Point-to-point tunneling protocol (pptp), (1999)
72. Lee, R.M., Assante, M.J.: Analysis of the cyber attack on the ukraine power grid. In E-ISAC and SANS, White (2016)
73. Cherepanov, A.: Win32/industroyer: A new threat for industrial control systems, p. 2017. ESET (June, White paper (2017)
74. Loukas, G., Karapistoli, E., Panaousis, E., Sarigiannidis, P., Bezemskij, A., Vuong, T.: A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. Ad Hoc Netw. **84**, 124–147 (2019)
75. Ross, R., Viscuso, P., Guissanie, G., Dempsey, K., Riddle, M.: Protecting controlled unclassified information in nonfederal information systems and organizations. Technical report, National Institute of Standards and Technology (2016)
76. Ab Rahman, Nurul Hidayah, Choo, Kim-Kwang Raymond.: A survey of information security incident handling in the cloud. Comput. Secur. **49**, 45–69 (2015)
77. Elk stack: Elasticsearch, logstash, kibana. https://www.elastic.co/what-is/elk-stack. Accessed 11 Oct 2021
78. Kotenko, I., Kuleshov, A., Ushakov, I.: Aggregation of elastic stack instruments for collecting, storing and processing of security information and events. In 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), pp. 1–8. IEEE, (2017)
79. Nabil, M., Soukainat, S., Lakbabi, A., Ghizlane, O.: Siem selection criteria for an efficient contextual security. In: 2017 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1–6. IEEE, (2017)
80. Kimberly, T., Kevin, J.: Factors affecting cyber risk in maritime. In: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pp. 1–8. IEEE, 2019
81. Abkowitz, M.D., Camp, J.S.: An application of enterprise risk management in the marine transportation industry. WIT Trans. Built Environ. **119**, 221–232 (2011)
82. Kushal, T.R.B., Lai, K., Illindala, M.S.: Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system. IEEE Trans. Smart Grid **10**(5), 4741–4750 (2018)
83. Hemminghaus, C., Bauer, J., Padilla, E.: A bridge attack tool for cyber security assessments of maritime systems, Brat (2021)
84. Yi, C.-G., Kim, Y.-G.: Security testing for naval ship combat system software. IEEE Access **9**, 66839–66851 (2021)
85. Le, H.V., Nguyen, T.N., Nguyen, H.N., Le, L.: An efficient hybrid webshell detection method for webserver of marine transportation systems. IEEE Trans. Intell. Transp. Syst., (2021)
86. Daniel T., Jonathon M., Alexander, F.L.S.: A framework for cybersecurity assessments of critical port infrastructure. In: 2017 International Conference on Cyber Conflict (CyCon US), pp. 1–7. IEEE, (2017)
87. Kuhn, K., Bicakci, S., Shaikh, S.A.: Covid-19 digitization in maritime: understanding cyber risks. WMU Journal of Maritime Affairs, pages 1–22, (2021)
88. McCready, J.W., Callahan, W., Mayhew, D., Heckman, M.: Toward a maritime cyber security compliance regime. In: SNAME Maritime Convention. OnePetro, (2018)

89. Schauer, Stefan, Polemi, Nineta, Mouratidis, Haralambos: Mitigate: a dynamic supply chain cyber risk assessment methodology. J. Transp. Secur. **12**(1), 1–35 (2019)
90. Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., Simonin, J.: Detecting and hunting cyberthreats in a maritime environment: Specification and experimentation of a maritime cybersecurity operations centre. In 2018 2nd Cyber Security in Networking Conference (CSNet), pp. 1–8. IEEE, (2018)
91. Neumann, J.C.: The book of GNS3: build virtual network labs using Cisco, Juniper, and more. No Starch Press, (2015)
92. Strategy comparison algorithm. https://github.com/ahmed-amro/APS-Communication_Architecture/tree/master/RPNMI/Strategy_Comparison_Algorithm
93. Systems and Software Engineering - System Life Cycle Processes. Geneva, Switzerland: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers. ISO/IEC 15288:2015
94. Gestionnaire libre de parc informatique (glpi). https://glpi-project.org/. Accessed 11 Oct 2021
95. FusionInventory - the opensource it inventory solution. https://fusioninventory.org/. Accessed 11 Oct 2021
96. Duo security - two factor authentication. https://duo.com/. Accessed 11 Oct 2021
97. Ajay, T.: Iperf: The tcp/udp bandwidth measurement tool. http://dast.nlanr.net/Projects/Iperf/, 1999
98. Rødseth, Ø.: Munin deliverable 4.3: Evaluation of ship to shore communication links. http://www.unmanned-ship.org/munin/wp-content/uploads/2014/02/d4-3-eval-ship-shore-v11.pdf, (2012)
99. Chu, H.: LDAP. Washington, D.C., Dec (2006). USENIX Association
100. Wengyik, Y., Tim, H., Steve, K.: Lightweight directory access protocol. 1995
101. Nathan, Y.: pgina administration and users documentation. http://pgina.org/. Accessed 11 Oct 2021
102. Clamav an open-source antivirus engine. https://www.clamav.net/. Accessed: 11 Oct 2021
103. Borgbackup, deduplicating archiver with compression and encryption. https://www.borgbackup.org/. Accessed: 11 Oct 2021
104. Roesch, M., et al.: Snort: lightweight intrusion detection for networks. In Lisa **99**, 229–238 (1999)
105. Wazuh - the open source security platform. https://wazuh.com/. Accessed 11 Oct 2021
106. MITRE. Chimera, Group G0114, 2021 (accessed 11 May 2021). https://attack.mitre.org/groups/G0114/
107. Gordon, F.L.: Nmap network scanning: The official Nmap project guide to network discovery and security scanning. Insecure, Com LLC (US) (2008)
108. Cisco: RV0xx Series Routers, ADMINISTRATION GUIDE, (2021) (accessed 13 May 2021). http://bit.ly/RV042