Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework

AHMED AMRO, VASILEIOS GKIOULOS, and SOKRATIS KATSIKAS, Norwegian University of Science and Technology, Norway

Autonomous transport is receiving increasing attention, with research and development activities already providing prototype implementations. In this article we focus on **Autonomous Passenger Ships (APS)**, which are being considered as a solution for passenger transport across urban waterways. The ambition of the authors has been to examine the safety and security implications of such a **Cyber Physical System (CPS)**, particularly focusing on threats that endanger the passengers and the operational environment of the APS. Accordingly, the article presents a new risk assessment approach based on a **Failure Modes Effects and Criticality Analysis (FMECA)** that is enriched with selected semantics and components of the MITRE ATT&CK framework, in order to utilize the encoded common knowledge and facilitate the expression of attacks. Then, the proposed approach is demonstrated through conducting a risk assessment for a communication architecture tailored to the requirements of APSs that were proposed in earlier work. Moreover, we propose a group of graph theory-based metrics for estimating the impact of the identified risks. The use of this method has resulted in the identification of risks and their corresponding countermeasures, in addition to identifying risks with limited existing mitigation mechanisms. The benefits of the proposed approach are the comprehensive, atomic, and descriptive nature of the identified threats, which reduce the need for expert judgment, and the granular impact estimation metrics that reduce the impact of bias. All these features are provided in a semi-automated approach to reduce the required effort and collectively are argued to enrich the design-level risk assessment processes with an updatable industry threat model standard, namely ATT&CK.

CCS Concepts: • **Security and privacy** → **Systems security;**

Additional Key Words and Phrases: Risk assessment, safety and security, Cyber-Physical System, autonomous ship, MITRE ATT&CK, FMECA

ACM Reference format:
Ahmed Amro, Vasileios Gkioulos, and Sokratis Katsikas. 2023. Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework. *ACM Trans. Priv. Sec.* 26, 2, Article 22 (March 2023), 33 pages.
https://doi.org/10.1145/3571733

1 INTRODUCTION

Interest in automated and autonomous ships has increased in the last years with many ongoing projects in this domain, driving the industry into a major transformation [21]. An instance of this trend is the project targeting the development of an **Autonomous Ferry (Autoferry)** for transporting passengers autonomously across the Trondheim city canal in Norway. We classified the Autoferry earlier as an **Autonomous Passenger Ship (APS)** in [7], and the reader can find

Authors' address: A. Amro, V. Gkioulos, and S. Katsikas, Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway; emails: {ahmed.amro, vasileios.gkioulos, sokratis.katsikas}@ntnu.no.

2471-2566/2023/03-ART22 $15.00
https://doi.org/10.1145/3571733

detailed information about the project in [46]. This APS is expected to be fully autonomous, with remote navigation and control capabilities enabled by a heterogeneous communication architecture which we specified earlier [8]. This communication architecture fully supports the autonomous operation of e-navigation, which is defined by the **International Maritime Organization (IMO)** as "*the harmonized collection, integration, exchange, presentation and analysis of maritime information onboard and ashore by electronic means to enhance berth to berth navigation and related services, for safety and security at sea and protection of the marine environment*" for which the reader can find more information in [19]. However, introducing automation along with e-navigation increases the likelihood of cyber attacks because of the required increased connectivity and decreased human supervision.

Broadly, cyber attacks that target the maritime domain are increasing both in numbers and severity, also enabled by the aforementioned ongoing digital transformation. Such attacks target all the segments of maritime infrastructure, including the ships, ports, and shipping companies. Some notable and well-known examples of such incidents include the attack against the COSCO shipping company [2], the Austal naval shipbuilder [3], and the notoriously disruptive attack against the Maersk shipping company [25]. Ships themselves have also been targets of attacks, since, arguably, attacks against them are of comparatively low complexity [53], and past incidents targeting their **Global Positioning System (GPS)** [28] and communication technologies [63] are indicative of both their feasibility and potential impact.

In the case of the APS, its security risks can directly or indirectly endanger the safety of the passengers and affect the operational environment. Potential risks can arise if the ship's remote control capabilities are hijacked, and the ship is directed towards a collision with the surrounding environment or other ships. Therefore, risk management of the APS communication architecture must be implemented in order to increase the trustworthiness, security, and resilience of the integrated systems. Risk management comprises several processes with risk assessment at the core, as discussed in ISO 31010 [16] and ISO 27005 [23]. Furthermore, the relationship between safety and security in the risk management of **Cyber-Physical Systems (CPS)** like autonomous ships requires additional attention in order to ensure the safety of people and the systems themselves.

In this paper, the **Failure Modes Effects and Criticality Analysis (FMECA)** [15] has been chosen for conducting a risk assessment for the APS communication architecture. FMECA was conducted to identify risks and suggest mitigation methods to support the efforts towards developing a security architecture for the APS. In order to overcome limitations in existing risk assessment methods (discussed in Section 2), we propose an approach for utilizing the common knowledge encoded within the MITRE ATT&CK framework [58] within the FMECA process. Additionally, we introduce a group of impact estimation metrics that can be calculated from the target system model by utilizing concepts from graph theory [62]. The results reflect the comprehensive nature of the proposed approach in addition to the utility of the suggested metrics in reducing the effect of biased analysis and the need for expert judgment. Finally, several risks have been identified and considerations for mitigation methods have been proposed.

The remainder of this paper is structured as follows. In Section 2, our rationale for the proposition of the risk assessment approach is discussed, in addition to a comparison with relevant works. Additionally, a brief description of an **Autonomous Passenger Ship (APS)** is provided. The APS constitutes a CPS use case that is utilized to evaluate the proposed approach. Further, Section 2 includes a description of the ATT&CK framework and graph theory to facilitate later discussions throughout the paper. Then, Section 3 describes a group of related risk analysis works that influenced or that are comparable to the work in this paper. After that, Section 4 presents the proposed risk assessment approach for CPS and Section 5 presents an evaluation of the proposed approach using the case of the APS. Section 6 then presents the results of the conducted risk assessment of the APS, highlighting the benefits of the proposed approach. In Section 7 we discuss certain limitations and give recommendations for future work. Finally, Section 8 summarizes our conclusions.

2 BACKGROUND

2.1 Motivation and Comparison with Existing Approaches

The work in this paper is motivated by the need to introduce cyber risk management activities into the maritime domain and specifically the MilliAmpere2 APS use case described in Section 2.2 toward the proposition of a suitable cybersecurity architecture. IMO urged the different maritime industry stakeholders to include cyber risk management into their safety management systems. The resolution suggested some guidelines and requirements for cyber risk assessment and management [18]. This includes the consideration of different cyber technology domains such as IT and OT (Sections 2.1.1 and 2.1.2 in [18]), the consideration of operational, safety and security impacts (Section 1.1 in [18]), and the need for continuous risk assessment and management (Sections 3.3 and 3.5 in [18]). Because of the different technology domains found in the maritime environment, we considered the application of ATT&CK (more details in Section 2.3). ATT&CK includes different technology domains within its threat model, specifically, enterprise, mobile, and **industrial control systems (ICS)**. All were found to be relevant to the APS use case.

Regarding impact estimation for risk calculation, as shown in Table 1, several approaches for estimating the impact of cyber attacks in CPS were observed in the literature. The majority of the studied literature estimated the impact severity through the four elements described in the SAE J3061 Ground Vehicle Standard [17], namely, safety, financial, operational, and privacy/legislative. Other works considered the impact from the perspective of the breached security goals, namely, confidentiality, integrity, and availability, similar to the **Common Vulnerability Scoring System (CVSS)** criteria. Macher and Armengaud [37] utilized the DREAD impact model, Bolbot et al. [12] utilized three impact elements, namely, safety, environmental, and financial, while Tam and Jones [60] employed a novel model named MaCRA. However, we argue that the observed impact estimation approaches fail to clearly capture the impact of all observed adversarial tactics and techniques in ATT&CK including command and control, defense evasion, discovery, initial access, lateral movement, persistence, and credential access. Therefore, we considered utilizing the impact model proposed in the SAE J3061 standard and extending it to capture the security-related impact that is not captured in the other approaches.

The continuous risk assessment and management requirement has motivated us to reduce the efforts associated with conducting the risk assessment process. Table 1 reflects the sources of knowledge that are utilized in the different survey approaches. Expert judgment constitutes the main source for threat identification, risk calculation, and the proposition of mitigation methods. In this regard, our approach employs the concept of curated knowledge and utilizing available threat-related information in the ATT&CK repository. Similarly, Sheehan et al. [54] employed the **National Vulnerability Database (NVD)** as a source for updatable software-related threat identification methods. However, we argue that the ATT&CK threat model is more appropriate in the design phase in comparison to NVD which relies on specific software and hardware information for the identification of relevant vulnerabilities.

In addition to the requirements communicated by IMO in [18] we argue that the observed risk analysis approaches in the literature are not comprehensive enough in their consideration of threats. As depicted in Table 1, the most observed threat identification method in the studied literature is **STRIDE; Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation** of privileges [55]. Monteuuis et al. [44] however, have extended the STRIDE approach to include two additional threat categories, namely, linkability (which violates privacy) and confusion (which violates trustworthiness). In this regard, we considered the utilization of the ATT&CK framework which provides additional attack description information that STRIDE simply does not provide.

STRIDE-based methods consider only six threat categories, some extended them to eight. On the other hand, ATT&CK suggests more than 600 attack techniques across the several technology domains. Therefore, our threat identification approach is more descriptive and comprehensive. In addition to that, ATT&CK is constantly updated, thus providing an updatable feature to our risk assessment approach.

Still, ATT&CK is not a risk assessment framework. Therefore, we have considered several approaches toward the proposition of the most suitable risk assessment method. We referred to the IEC 31010:2019 [16] standard for risk assessment techniques. The standard provides detailed descriptions and comparisons among the most observed techniques employed within the different risk assessment steps. In our quest, we considered the scope, time horizon, requirements for specialist expertise, and the amount of effort required to apply the risk assessment techniques. Our scope of the risk assessment in CPS such as the APS includes components, equipment, and processes. The time horizon should be flexible, also the need for specialist expertise and amount of effort required should be at most moderate, to support the satisfaction of the requirement for continuous risk assessment and management as well as to reduce the effect of biased assessment associated with expert judgments. The aforementioned criteria have led us to FMECA. Moreover, the standard highlights the applicability of FMECA in the different steps in the risk assessment process, namely, risk identification, consequence, likelihood, risk estimation and risk evaluation. Afterwards, in each step of the FMECA process, we aimed to integrate the most suitable technique, while considering the requirements for the risk assessment process mentioned previously and by utilizing relevant artifacts from the literature. We suggested the utilization of a **Preliminary Hazard Analysis (PHA)** or a **hazard and operability study (HAZOP)** for the estimation of safety and financial impact based on the previous works by Bolbot et al. [12] and Thieme et al. [61]. Both works utilized these approaches for estimating the safety impacts of cyber attacks in different maritime use cases. Also, we suggested the utilization of the CVSS exploitability metrics for likelihood estimation based on its common adoption in the literature as depicted in Table 1 (more details in Section 4.6) and its suitability for our approach.

2.2 Communication Architecture of an Autonomous Passenger Ship

The Autoferry project [46] aims to develop an APS prototype 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 [29]. The ferry will operate autonomously with a human operator in a **Remote Control Centre (RCC)** monitoring its operations and with the capability to intervene at any moment.

We have designed a communication architecture for the APS [8] that enables it to communicate with its operational context. The architecture enables the APS to carry out a group of functions, including autonomous and remote navigation and control. Navigation functions rely on collecting sensing information from the surrounding environment through arrays of sensors including lidars, radars, Infra-Red, and video cameras which interface using several **Sensor Processing Units (SPU)** and sensor switches. Then, an **Autonomous Navigation System (ANS)** achieves situational awareness by leveraging sensor data to determine safe routes.

Additionally, the APS relies on real-time kinematics and the **Global Navigation Satellite System (GNSS)** for positioning. Moreover, the APS has the ability to carry control functions and maneuvers using a machinery system that includes a **Dynamic Positioning (DP)** system and active thrusters interfaced through Input/Output cards. The machinery system is supervised by an **Autonomous Engine Monitoring and Control (AEMC)** system. The APS is also equipped

Table 1. Comparison between our Approach and the Surveyed Works

Work	Technology Domains	Threat Identification			Risk Calculation Model		Risk Calculation	Knowledge Source			Attack Sequence Approach
		Attacker Profile Model	Threat Categories	Attack Categories	Impact	Likelihood		Mitigation Proposition	Threat Identification	Risk Calculation	
Our approach	IT/OT/ Mobile	ATT&CK Groups*	ATT&CK Tactics	ATT&CK Techniques	SAE J3061 (1) + Staging	CVSS Exploitability	Risk Priority Number + Risk criteria	ATT&CK Mitigations	ATT&CK Tactics and Techniques	Graph Theory + Expert Judgment	*
[44]	IT/OT	Knowledge, Expertise, Equipment	STRIDE + LC	Alter, Listen, Disable, Forge	SAE J3061 (1) + Controllability	Capability, elapsed time, opportunity	Risk Matrix	Expert Judgment	Expert Judgment	Expert Judgment	Attack tree
[37]	IT/OT	-	STRIDE + HARA (2)	-	DREAD (3)	Knowledge, resources	Risk Matrix	Expert Judgment	Expert Judgment	Expert Judgment	-
[31]	OT	-	STRIDE	-	SAE J3061 (1)	Expertise, knowledge, opportunity, equipment	Risk Matrix	Expert Judgment	Threat report: Microsoft Threat Modelling Tool 2014	Expert Judgment	-
[10]	OT	-	STRIDE	-	SAE J3061 (1)	Model 1: expertise, knowledge, opportunity, equipment, Model 2: CVSS Exploitability	Bayesian Network	Expert Judgment	Expert Judgment	Expert Judgment	-
[54]	IT/OT	-	Software vulns. in NVD	-	CVSS impact: Confidentiality, Integrity, Availability	CVSS Exploitability	CVSS Base Score + Risk Matrix	Expert Judgment	NVD	NVD + Expert Judgment	-
[33]	OT	-	STRIDE	-	Predefined criteria similar to SAE J3061 (1)	Predefined criteria considering capability, motivation, controls, available exploits, reachability, vulns., knowledge, authentication	Risk Matrix	Expert Judgment	Expert Judgment	Expert Judgment	-
[38]	IT/OT	-	STRIDE	-	CVSS Impact	CVSS Exploitability	CVSS Base Score	Expert Judgment	Expert Judgment	Expert Judgment	Attack tree
[12]	IT/OT	Technological level, Ease-of-exploit (EoE)	Predefined list	Predefined list	Safety, environmental, financial	Technological level, activity level, interest level, EoE, exposure level, vulns. level, frequency index	Risk Matrix	Expert Judgment	Expert Judgment	Expert Judgment	-
[60]	OT	EoE	MaCRA	Damage, theft, denial of service, misdirect, obfuscate	MaCRA (Vulns.+Ease of Exploit+Reward) Vulns: Attack vector, vulns. effects Ease of Exploit: Attack agent, type, target type, resources, controls Reward: Attack agent type, target type, attacker goal, target effect		MaCRA	Expert Judgment	Expert Judgment	Expert Judgment	-

(1) SAE J3061 impact elements: Safety, Privacy, Financial, Operational
(3) DREAD Impact elements: Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability
(2) HARA: Hazard Analysis and Risk Assessment
* Not included in the current work but planned in future work. Check Section 7 for more details.

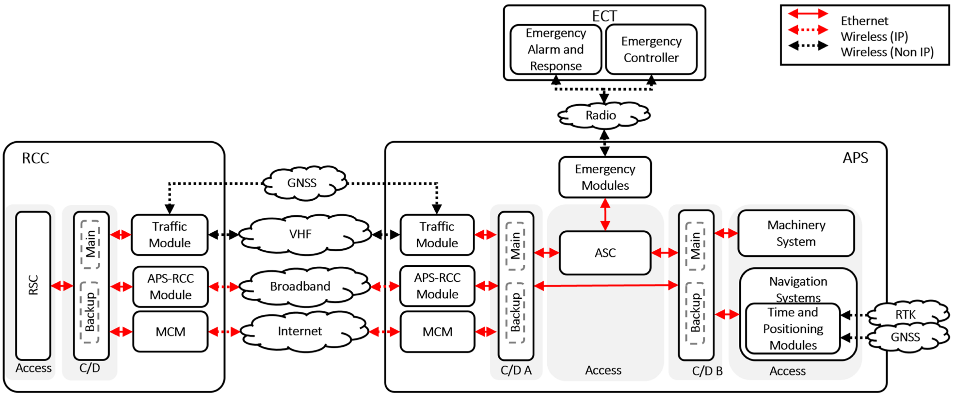


Fig. 1. APS Communication architecture, inspired from [8].

with an emergency push-button for initiating the emergency protocol, according to which a nearby **Emergency Control Team (ECT)** is expected to intervene when needed.

Moreover, a set of heterogeneous communication modules and components are proposed and integrated within the onboard network as shown in Figure 1, to satisfy the communication requirements of various stakeholders, as discussed in [7]. Additionally, the architecture supports carrying out the autonomous and remote functions through a group of communication functions including ship-to-shore, ship-to-ship, internal, and emergency communications. Ship-to-shore communication enables the APS to communicate with the RCC through two IP-based redundant communication modules: the **Mobile Communication Module (MCM)** and the APS-RCC Module. The technologies for implementing these modules are expected to be LTE/4G/5G and Wi-Fi, respectively. Ship-to-ship communication is facilitated through a traffic module such as an **Automatic Identification System (AIS)**, while internal communication is enabled through two **Core/Distribution** tiers (**C/D** part A and part B) each implemented using two redundant layer-3 switches. Emergency communication relies on two modules. The first emergency module (Emergency module 1) facilitates communicating with the ECT to perform emergency navigation functions, while the other module (Emergency module 2) is used to transmit emergency signals to the ECT when the emergency push button is pressed by a passenger. Finally, an intelligent entity named Connectivity Manager performs autonomous and remote network management functions.

A centralized component named **Autonomous Ship Controller (ASC)** resides in the center of the APS network which hosts the primary and backup servers hosting the ANS, AEMC, Connectivity Manager, as well as other components for the system, network, and security management.

A group of systems resides in the RCC network for remote navigation functions, control functions, and additional ship-to-shore communication functions. The network modules and devices are equivalent to the ones on board the APS. On the other hand, the **Remote Ship Controller (RSC)** hosts the **Remote Navigation System (RNS)** and **Remote Engine Monitoring and Control System (REMS)**, in addition to other components for the remote system, network, and security management. More details regarding the communication architecture can be found in [8].

In this paper, a risk assessment approach is first presented through the application of a FMECA enriched with the MITRE ATT&CK framework. Then, the proposed approach is evaluated using the communication architecture of the APS.

2.3 MITRE ATT&CK Framework

An increase in adopting the ATT&CK framework proposed by MITRE [5, 58] is observed in both academia and industry. **ATT&CK**, which stands for **Adversarial Tactics, Techniques, and**

Common Knowledge, is a curated knowledge base that models the behavior of cyber adversaries. It provides a common taxonomy in describing the different phases of the adversary attack life-cycle. Among the most important features of ATT&CK, that distinguishes it from other threat models, is the abstraction level in describing adversarial tactics and techniques. High-level models observed in the literature such as STRIDE [55] and the cyber Kill Chain [40], fail to effectively reflect the granularity of actions that adversaries can take, how they relate to one another, their consequences related to adversarial objectives, their correlation with mitigation methods and data sources, and their targeted platforms and systems [58]. We argue that these particular features qualify ATT&CK as an appropriate engine for conducting comprehensive and logically sound risk assessment, utilizing the systematically encoded expert knowledge to reduce effort and inconsistencies during risk estimation. The ATT&CK adversarial model comprises, among others, a group of essential terms, Tactics, Techniques, and Procedures. Tactics represent the adversarial objective of the attack, techniques represent the adversarial method for realizing an objective, while procedures represent the actual software utilized to run the technique to realize the tactic. The framework is organized as a group of matrices for different technology domains, enterprise, mobile, ICS, containers and adversarial machine learning. Each matrix holds the relationships between tactics, techniques, procedures, mitigation methods, and others.

In the context of the APS, since it comprises a collection of **Information Technology (IT)** and **Operational Technology (OT)** components, the comprehensive nature of ATT&CK was of particular utility to identify relevant threats for APS's heterogeneous components. Moreover, the well-established relationships in ATT&CK were found to be logically compatible with FMECA. A detailed discussion on applying ATT&CK in the FMECA process is presented in Section 4.

2.4 Graph Theory

Several works have highlighted the utility of graph theory [62] in analysing interconnected infrastructures [4, 35, 57]. Graphs are mathematical structures used to model the relationships between distinct objects [62], while the abstraction of graphs enables them to model a wide range of relationships including networked systems [4], connected organizational structures [35], and other types of related objects. A graph consists of nodes, each representing an object that is involved in a relationship with other objects, while these relationships are represented with edges connecting the related nodes. A group of formal measures has been proposed to analyze the graph, including the centrality measures. These measures can be utilized to estimate the relative influence of a node in the graph. Several centrality measures exist such as closeness centrality, degree centrality, Eigenvector centrality, and many others [57]. The aggregation of all centrality measures has been found to identify nodes with the highest influence over the graph [57]. On the other hand, the **Outbound Degree Centrality (ODC)** (i.e., out-degree centrality) of a node reflects the number of its neighbors. Nodes with the highest ODC within a graph are called "cascade initiating nodes" [36] and must be prioritized when examining mitigation controls [57]. In this paper, we rely on ODC and the semantics of the combined centrality measures proposed by Stergiopoulos et al. [57] during the estimation of the operational and the security related impacts (Section 4.4) for the examined use case.

3 RELATED WORK

In this section, we will discuss, in detail, related works that share considerable similarities with our approach. In the automotive domain, Islam et al. [31] argued that a risk assessment be performed in the requirements elicitation phase of the development life-cycle, in order to guide countermeasure integration in the design and development phase. The authors proposed a risk assessment framework that is aligned with known automotive processes related to functional safety and usability. The authors proposed a novel approach to calculate semi-quantitative risk by applying STRIDE for threat modeling, attacker expertise, required knowledge, equipment and window of opportunity for likelihood estimation, and the common impact elements safety, privacy, financial, and operation. The authors proposed the application of weights to adjust the impact estimates based on the organization's needs. In this paper, we utilize the concept of weights (i.e., factors) from the framework of [31] to adjust the impact assessment of risks according to the followed risk management strategy. Sheehan et al. [54] proposed a risk classification framework based on Bayesian networks to evaluate the security level of connected and autonomous vehicles. The authors utilized the software vulnerabilities in the **National Vulnerability Database (NVD)** for an updatable threat identification approach. Then, they employ Bayesian networks for estimating the likelihood and impact of threats, following the CVSS approach toward calculating the risk. Expert judgment is integrated into the proposed framework for deriving the structure of the Bayesian networks and estimating several risk variables. Our proposed approach in this paper shares similar features with [54] regarding the utilization of CVSS, the integration of expert judgment, the updatability of risk scores as well as the accommodation of existing mitigation techniques into the risk calculation. In contrast, we consider more comprehensive attack techniques and granular impact estimation parameters.

Compared to the domain of autonomous cars, fewer works have addressed risk assessment for autonomous ships. Kavallieratos et al. [33], proposed a multilayer architecture for the information and communication technology systems in cyber-enabled ships which include autonomous ships. The authors then applied the STRIDE threat modeling method to identify potential threats. Then the associated risks were assessed using risk matrices following risk estimation criteria inferred from the work by Jelacic et al. [32]. The risk estimation criteria consider safety, operations, economic, information leakage, and reputation impact elements. Moreover, the criteria consider attackers' capability, motivation, and knowledge, in addition to existing countermeasures and exploits as well as component reachability. Additionally, Tam and Jones [59] proposed a model-based risk assessment framework called MaCRA [60] and applied it on three futuristic ships with different applications and levels of autonomy. The process started with applying the MaCRA threat assessment framework and then the risk assessment process. The threat assessment considered the different attackers' profiles, their goals, and available resources. Moreover, the ships' vulnerabilities related to the expected technologies and the expected impact of the vulnerabilities have been considered. In the risk assessment process, five-tier values were applied to quantify the risks associated with the identified threats and the risk level was presented through two values, namely Ease of Exploitation (Likelihood) and Attackers reward (Impact). Bolbot et al. [12] proposed a cyber risk assessment method for ship systems based on a Cyber-Preliminary Hazard Analysis. The method was applied for conducting a risk assessment and providing design enhancement of the navigation and propulsion systems of inland waterways autonomous vessels. The risk assessment considers attacker groups, system vulnerabilities, attack likelihood, consequences, and existing barriers. The likelihood estimation considers component reachability (i.e., connectivity), attack complexity, attacker group motivation, capabilities, activity level, ease of exploitation, and the absence of barriers. The impact estimation considers safety, environmental, and financial consequences.

An application of ATT&CK in the risk analysis of digital substations is presented by Khodabakhsh et al. [34]. The authors utilized the ICS matrix in ATT&CK to identify possible attack paths in a system of digital substations, assessed their potential impact regarding **confidentiality, integrity, and availability (CIA)**, and finally, proposed a group of suitable countermeasures.

In contrast to the related works presented in this section, we propose a comprehensive and systematic approach for identifying relevant attacks against components in CPS architectures, considering three technology domains in ATT&CK, namely ICS, enterprise, and mobile. Additionally,

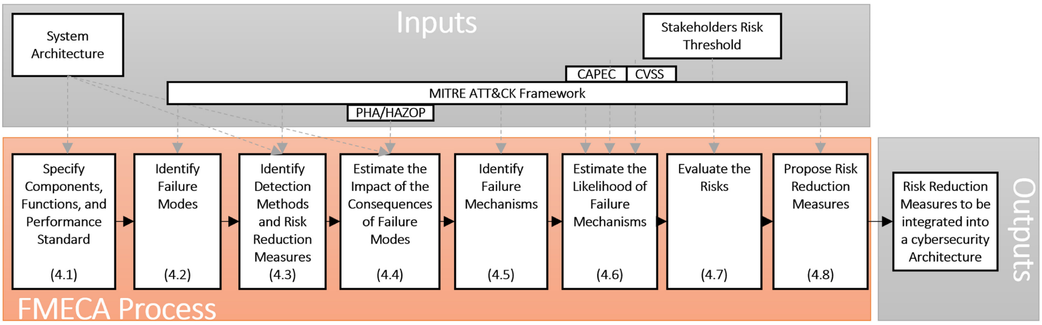

Inputs
System Architecture
Stakeholders Risk Threshold
CAPEC
CVSS
MITRE ATT&CK Framework
PHA/HAZOP
Specify Components, Functions, and Performance Standard (4.1)
Identify Failure Modes (4.2)
Identify Detection Methods and Risk Reduction Measures (4.3)
Estimate the Impact of the Consequences of Failure Modes (4.4)
Identify Failure Mechanisms (4.5)
Estimate the Likelihood of Failure Mechanisms (4.6)
Evaluate the Risks (4.7)
Propose Risk Reduction Measures (4.8)
FMECA Process
Risk Reduction Measures to be integrated into a cybersecurity Architecture
Outputs

Fig. 2. Overview of the proposed FMECA-based approach showing the integrated information sources.

Table 2. Components Classifications

Class.	Description
IT	Components that are hosted on a traditional IT system such as multipurpose computers or network devices.
OT	Components that are involved in monitoring and controlling functions.
Wireless	Components that are connected to a mobile network or communicate with an external infrastructure such as Aids to Navigation to acquire location-related information in the maritime domain.
IT/OT	Dual-homed components that are hosted on a traditional IT system and are involved in monitoring and controlling functions.
IT/OT/Wireless	Components that are classified as IT/OT and are connected to a mobile network or communicate with an external infrastructure.

we propose a granular and comprehensive impact estimation approach considering operational, safety, financial, and system and information security-related impacts.

4 THE PROPOSED RISK ASSESSMENT APPROACH

The proposed risk assessment approach is based on a design-level FMECA [15]. A bottom-up approach is suggested that requires knowledge of low-level components. A FMECA process consists of three main phases, namely planning the analysis, performing it, and finally documenting it. The overall risk assessment process highlighting the utilized information sources is depicted in Figure 2. In the planning phase, the objectives and scope of analysis, as well as the considered scenarios, are identified. The ATT&CK framework aids the FMECA process by describing attack techniques and tactics in a manner that can be used to induce failure scenarios [5]; this feature is of particular utility to the analysis and communication of the identified risks. Additionally, the criteria for the treatment of failure modes should be defined according to the followed risk management strategy. Afterwards, the analysis is performed, and the detailed steps for performing an FMECA utilizing ATT&CK are presented in the subsequent sections. Finally, an FMECA report is generated, which gives detail on the analysis process.

4.1 Specify Components, Functions, and Performance Standard

An architecture model describing the different architectural components, their functions, and interconnections is a vital element of the risk assessment process. The components addressed in this analysis are the functional components, including software and hardware elements. The components are classified as Information Technology (IT), Operational Technology (OT), Wireless, and/or a combination of multiple categories. Wireless components include mobile devices and/or devices with wireless services. The classification of components is conducted based on the criteria shown in Table 2. Additionally, operational modes are proposed to be identified and considered to improve the analysis, particularly when they inflict a change in the system state (set of components and their connections). Moreover, the performance standard for each component function should be specified, to define what constitutes a component failure.

Table 3. Malicious Failure Modes According to ATT&CK

Class	Failure Mode	Failure effect
IT, OT, and Wireless	Initial Access	entry to the network.
	Collection	gathering data of interest.
	Command and Control	communicating with other compromised components in the network to control them.
	Defense Evasion	avoiding detection.
	Discovery	discovering the environment.
	Execution	running malicious code.
	Impact	impacting the data and/or components.
	Lateral Movement	moving between components within the environment.
	Persistence	maintaining a foothold in the environment.
IT and Wireless	Privilege Escalation	increasing privilege.
	Credential Access	discovering account names and passwords.
	Exfiltration	stealing data.
OT	Impair Process Control	impacting the control processes.
	Inhibit Response Function	impacting the safety, protection, and monitoring functions from responding.
Wireless	Network Effect	impacting the network traffic.
	Remote Service Effect	impacting components remotely.

4.2 Identify Failure Modes

A failure mode is defined as a manner in which a failure occurs [15]. In this study, the security of CPSs is analyzed. So, the security failure modes are considered. In system security engineering, a system security failure is defined as "not meeting the security-relevant requirements, objectives, and performance measures, to include exhibiting unspecified behavior, exhibiting unspecified interactions, or producing unspecified outcomes, where there is security-relevance" [51]. Earlier works have discussed security failure modes considering the CIA triad [9] and [34]. We propose to go beyond that and consider, for each component, a broader range of security failure modes. For this, we utilized the ATT&CK framework. We argue that the failure modes which are referred to as Tactics in ATT&CK (i.e., kill chain phases) are more comprehensive than the high-level failure modes classification according to the CIA triad since the tactics in ATT&CK involve failing more than one of the CIA attributes or none. The considered security failure modes for each component class are depicted in Table 3.

4.3 Identify Detection Methods and Risk Reduction Measures

In this step, the existing detection and risk reduction measures (i.e., controls) are identified and analyzed. These controls affect the *Detectability* estimation value when estimating the risks of failures. This value constitutes the probability of the attack being detected or mitigated. The calculation of this value is conducted as follows:

4.3.1 *The Failure-Mitigation Table (FMT).*

The FMT is constructed, which captures the possible mitigation methods for each considered failure mechanism as well as their expected efficiency. The ATT&CK framework was consulted for this purpose. A list of all techniques in the different ATT&CK matrices in the first and second column and their suggested mitigation methods in the third column were pulled from the online repository to populate the FMT. The fourth column captures the efficiency of the mitigation method (M) against that failure mechanism (FM) ($Efficiency_{FM,M}$); this value does not exist in the current ATT&CK knowledge base and therefore should be estimated. A typical measurement scale for detectability rating is provided in the FMECA standard [15]; the example is for a wind turbine. A sample of the FMT is depicted in Table 4. In the complete version of the FMT, a single technique could be mitigated by several mitigation methods. Similarly, a single mitigation method could be used to mitigate several techniques.

aka, a many-to-many relationship

4.3.2 *The Component-Mitigation Table (CMT).*

The Component-Mitigation Table (CMT) is constructed, which captures the coverage of mitigation methods for each component. For this, the CMT is populated with the mitigation methods in ATT&CK and their coverage for the existing components in the architecture. What is specifically meant by "coverage" is different from one

Table 4. An FMT Sample Reflecting Some Techniques, their Suggested Mitigation Methods, and their Estimated Efficiency

Matrix	Technique	Mitigation	Efficiency
ICS	Change Program State	Access Management	0.5
Enterprise	Commonly Used Port	Network Intrusion Prevention	0.5
Mobile	Remote File Copy	Application Vetting	0.5

Table 5. A CMT Sample Reflecting the Coverage of Some Components by the Mitigation Methods

Op-Mode	Mitigation	Component A	Component B
All	Access Management	0	1
All	Network Segmentation	1	0

mitigation method to another. But, in this paper, a component is said to be influenced by a mitigation method if the component in the proposed architecture is subject to an architectural decision that enforces the mitigation method. For instance, if the architecture is designed with network segmentation, all components in the isolated network segments are said to be covered by the network segmentation mitigation method. The CMT structure consists of the operational modes in the first column, the mitigation methods in the second, while the architectural components are spread across the remaining columns, and the coverage of the mitigation methods (M) for each component (C) (covered:1 or not:0) as the values ($Covarage_{M,C}$). A sample of the CMT is depicted in Table 5.

4.3.3 Calculating the Detectability. The value of $Detectability$ for each failure mechanism of a specific component is calculated based on whether or not the component is covered by a mitigation method suggested for the specific failure mechanism (as indicated in the CMT) and its mitigation efficiency (as indicated in the FMT). The $Detectability$ of the failure mechanism (FM) for a component (C) when considering the coverage of mitigation method (M) is calculated using Equation (1).

$$Detectability_{FM,C,M} = Covarage_{M,C} \times Efficiency_{FM,M} \quad (1)$$

4.4 Estimate the Impact of the Consequences of Failure Modes

The tactics in ATT&CK are terms that describe the desired outcome of attacks by attackers. This terminology allows the utilization of ATT&CK tactics as a classification of consequences for their corresponding techniques. Additionally, certain techniques have unique consequences; these techniques are grouped for each matrix within special tactic categories, namely, impact, network effect, or remote service effects. In our approach, we propose the consideration of all the tactics across all the relevant matrices in addition to the techniques under the special tactic categories. The impacts of these tactics and techniques are estimated based on the four most observed elements of impact of threats against CPS, namely, safety, financial, operational, and information criticality (e.g., privacy) [10, 31, 33, 44]. Nevertheless, some tactics have no impact according to the observed impact model in the literature; they rather have a security related impact that affects the security of connected nodes. For instance, a single successful technique aiming to achieve defensive evasion, which is the most observed ATT&CK tactic in 2019 [26] and second-most in 2020 [48], has no immediate impact on safety, privacy, financial or operations. But, it will support the attacker's efforts to stage future attacks. Therefore, we propose a fifth impact element named "Staging" to capture the impact of techniques that facilitate the staging of future attacks. The proposed process for estimating the impact of consequences is as follows:

Table 6. Mapping of Failure Modes and their Consequences in the FMCT

Mobile failure modes	O	S	I	F	ST	IT failure modes	O	S	I	F	ST	ICS failure modes	O	S	I	F	ST
Collection			1			Collection			1			Collection			1		
Command and Control					1	Command and Control					1	Command and Control					1
Defense Evasion					1	Defense Evasion					1	Defense Evasion					1
Discovery					1	Discovery					1	Discovery					1
Execution	1			1	1	Execution	1			1	1	Execution	1	1		1	1
Exfiltration			1		1	Exfiltration			1		1	Theft of Operational Information			1		1
Initial Access					1	Initial Access					1	Initial Access					1
Lateral Movement					1	Lateral Movement					1	Lateral Movement					1
Persistence					1	Persistence					1	Persistence					1
Credential Access					1	Credential Access					1	Damage to Property	1	1	1	1	
Data Encrypted for Impact	1	1	1	1	1	Data Encrypted for Impact	1	1	1	1	1	Denial of Control	1	1			
Privilege Escalation					1	Privilege Escalation					1	Denial of View	1	1		1	1
Carrier Billing Fraud				1		Account Access Removal	1	1		1	1	Impair Process Control	1	1		1	
Clipboard Modification	1					Data Destruction	1	1	1	1		Inhibit Response Function	1	1		1	
Delete Device Data	1		1	1		Data Manipulation	1	1	1	1		Loss of Availability	1	1	1	1	1
Device Lockout	1					Defacement	1	1	1	1	1	Loss of Control	1	1		1	
Downgrade to Insecure Protocols	1		1		1	Disk Wipe	1	1	1	1		Loss of Productivity and Revenue	1	1		1	
Eavesdrop on Insecure Network Communication			1		1	Endpoint Denial of Service	1	1		1		Loss of Safety	1	1		1	
Exploit SS7 to Redirect Phone Calls/SMS	1					Firmware Corruption	1	1		1		Loss of View	1	1		1	1
Exploit SS7 to Track Device Location			1			Inhibit System Recovery	1	1		1		Manipulation of Control	1	1		1	
Generate Fraudulent Advertising Revenue						Network Denial of Service	1	1		1		Manipulation of View	1	1		1	1
Input Injection	1					Resource Hijacking	1	1		1	1						
Jamming or Denial of Service	1	1		1		Service Stop	1	1		1							
Manipulate App Store Rankings or Ratings						System Shutdown/Reboot	1	1		1							
Manipulate Device Communication	1	1	1	1													
Modify System Partition	1																
Obtain Device Cloud Backups			1		1												
Remotely Track Device Without Authorization			1														
Remotely Wipe Data Without Authorization	1	1	1	1													
Rogue Cellular Base Station	1				1												
Rogue Wi-Fi Access Points	1				1												
SIM Card Swap	1				1												
SMS Control	1				1												
O: Operational || S: Safety || I: Information Criticality || F: Financial || ST: Staging																	

4.4.1 *Failure-Mode-Consequences Table (FMCT).*

The FMCT is constructed. It captures the mapping between each failure mode and its expected consequences across the entire system, expressed through the five impact elements. The FMCT can differ among different target systems. A sample FMCT is depicted in Table 6. For each matrix in ATT&CK, each failure mode was analyzed and the related impact elements were determined. For instance, all techniques under the collection tactic aim to collect information from the compromised target. The consequences of this attack can be assessed with relevance to the information criticality of the component with regards to the hosted process (i.e., intellectual property), information (i.e., confidentiality and privacy), and location information; therefore, an attack enabling collection will only impact information criticality of the component. As another example, the consequences of a successful attack with a "Loss of Control" failure mode will impact the ICS operations. The impact value can be estimated with relevance to the criticality of the component to the control functions it is involved with, in addition to the possible safety and financial impacts. Based on this mapping, five values are specified for each failure mode, namely **Safety Factor (SF)**, **Financial Factor (FF)**, **Information Criticality Factor (ICF)**,

Table 7. SC and FC Estimation Criteria [61]

Safety Criticality (SC)	Description	Financial Criticality (FC)	Description
None	No injuries	None	No damage to equipment or other property.
Minor (0.25)	Single and/or minor injuries	Minor (0.25)	Local equipment damage, small damage to other property, or minor loss of income.
Significant (0.5)	Multiple minor injuries and/or severe injury	Significant (0.5)	Damage to CPS, to other property, or significant loss of income.
Severe (0.75)	Single fatality and/or multiple severe injuries	Severe (0.75)	Severe damage to CPS, other properties, or loss of income equivalent to several days of operation.
Catastrophic (1)	Multiple fatalities and severe injuries	Catastrophic (1)	Loss of CPS or other properties.

Operational Factor (OF), and **Staging Factor (StF)**. A zero value reflects that no consequence is expected, while a positive value reflects the magnitude of the consequences. The implementation of this approach was influenced by the work of Islam et al. [31]. Based on the risk management strategy, the factor values can be controlled to reflect the priority of impact elements on the final risk value. For instance, the stakeholder concerns may prioritize safety as the greatest concern while considering privacy the lowest. In this case, the values of SF and ICF could be controlled to reflect that priority by increasing SF and decreasing ICF with appropriate proportions, based on the stakeholders' concerns.

4.4.2 The Component-Criticality-Scores Table (CCST). The CCST is constructed. It captures the impact scores for each component that correspond to the previously identified impact elements. The estimation criteria for each score are explained below:

- **Safety and Financial criticality (SC and FC):** safety and financial impact scores for each component can be elicited through a **Preliminary Hazard Analysis (PHA)** or a **hazard and operability study (HAZOP)**. An example of a set of estimation criteria is depicted in Table 7. The concept of this approach has been observed in hazardous waste management; a hazardous waste index is assigned to waste reflecting the level of safety procedures that are required in its handling, storage, transportation, and treatment [27]. The maximum possible safety and financial consequence values deduced from the PHA or HAZOP analysis for each component are recorded as the corresponding safety and financial criticality. For instance, if a component failure has been estimated to cause a catastrophic safety and financial consequence, the safety and financial impact scores for that component will be the maximum, (i.e., 1). After the analysis of the failure modes in ATT&CK, the nature of possible safety impacts is all similar, possibly leading to a life-threatening incident. On the other hand, the nature of financial impact was found to be different for a single failure mode, namely, Carrier Billing Fraud, a technique in the mobile matrix that could cause a financial impact in the form of unexpected billing for SMS-enabled devices should they exist within the CPS.
- **Operational criticality (OC):** for assessing the operational impacts, several architectural views are created, to calculate several impact values utilizing metrics from graph theory and multidimensional networks [20]. The ORA software [6, 13] is an example of existing software that can be utilized to draft the architecture views and provide metrics that are used to calculate the different OC metrics.

  After the analysis of the failure modes in ATT&CK, we have observed that certain failure modes could affect the overall performance of CPS, others could only affect the control or monitoring functions. Therefore, three operational impact metrics are calculated for each element. A description of each impact metric is given below:

  - **Overall operational impact (OOI):** The aggregated centrality measures of the components in the entire network structure are calculated and scaled by creating a graph representing the expected connectivity between the architectural components and their operational context. Each node represents a component (hardware, or software), while each edge

  represents a network connection (wired or wireless) as well as an expected application-level connection.
  - **Impact to the control functions (I2CF):** for each system state (refer to Section 4.1), a graph is created to represent the connectivity between components involved in the control functions. The aggregated centrality measures are then calculated and scaled for each component.
  - **Impact to the monitoring functions (I2MF):** similar to previous, but for the monitoring functions.

  Finally, the value of the OC metric is calculated differently, based on the considered failure mode. *OC = I2CF* for the Manipulation of Control, Loss of Control, Denial of Control, and Impair Process Control failure modes, *OC = I2MF* for the Denial of View, Loss of View, and Manipulation of View failure modes, while *OC = OOI* for all other failure modes.

- **Information criticality (IC):** this metric captures the criticality of the component concerning possible privacy or/and confidentiality violations. The confidentiality of data stored, processed, or communicated within the CPS network could involve location information. Also, concerns could exist to preserve the intellectual property of processes hosted within the CPS components. After the analysis of the ATT&CK failure modes, three possible impacts have been identified related to information criticality, namely, the attackers might be able to collect sensitive data (e.g., violates users privacy), to collect data that violate the intellectual property, or to collect location information. Therefore, three possible metrics could be estimated based on the failure mode:
  - **Data Criticality (DC):** this metric captures the importance of data hosted or processed in a component. It is measured for each component according to its involvement in the processing and storage of sensitive data.
  - **Intellectual Property Criticality (IPC):** this metric captures the component criticality regarding the hosting of processes with intellectual value.
  - **Location Information Criticality (LIC):** this metric captures the component criticality regarding the involvement with location information and the sensitivity of such information. If the system under analysis is involved in a location-sensitive use case, this metric could be of value and should be estimated according to the use case specifications. Two failure modes can be estimated using this metric, namely, Exploit SS7 to Track Device Location, and Remotely Track Device Without Authorization.

  Based on the risk management strategy, the importance of each metric could differ. Therefore, three factors are proposed to control the prioritization of the information criticality metrics, namely, DC_F, $IPC_{F,}$ and LIC_F; the values of these factors range from 0 to 1. Finally, the information criticality (IC) of component (C) is calculated using Equation (2). It has been found that in only a single failure mode, namely the Collection failure mode, all three metrics could be of relevance. The values of these metrics for each component can be estimated through the implementation of an early Privacy Impact Assessment [14] or a Data Protection Impact Assessment [11].

$$IC_C = \frac{(DC_F \times DC_C) + (IPC_F \times IPC_C + (LIC_F \times LIC_C))}{(DC_F + IPC_F + LIC_F)} \tag{2}$$

- **Staging Criticality (StC)**: this metric captures the impact of a failure mode that enables the staging of future attacks. We have observed that the impact of some of the considered failure modes is not captured using the previously mentioned impact elements. These failure modes include command and control, defensive evasion, discovery, initial access, lateral movement, persistence, privilege escalation, and credential access (refer to Table 6). Yet, these failure modes are critical to the security status of a system. Other security impact elements such as confidentiality, integrity, and availability are captured directly or indirectly in other impact elements. For instance, the confidentiality impact is captured directly in the information criticality, while the integrity and availability impacts, should they exist, are captured indirectly in several impact elements: if the integrity and/or availability of information or process are not preserved, information, safety, financial, and operational impacts might occur. We propose that the StC metric can be estimated using two metrics, namely **Outbound Degree Centrality (ODC)** and **Overall Component Criticality (OCC)**. Details regarding both metrics are presented below:

- Outbound Degree Centrality (ODC): Some failure modes, if materialized, enable the attacker to move to or communicate with other components in the network; the impact of this ability increases with higher ODC of the component. The more connected the node to its neighbors the higher the staging impact. Moreover, regarding the credential access failure mode, the discovered credentials can be utilized in other components not connected to the compromised component, even outside the compromised network. The impact of this case is not captured in this specific metric. Nevertheless, we argue that this metric provides a logical estimate of the impact of this failure mode within the compromised network.
- Overall Component Criticality (OCC): the persistence, defense evasion, and privilege escalation failure modes do not directly impact the attacked node or other nodes. So, we propose the utilization of the combined impact metrics to capture the staging impact of these three failure modes. We argue that the impact of a successful attack aiming to inflict these failure modes can be measured by the combined criticality (OC, SC, IC, FC) of the attacked component, using Equation (3). In a study of adversarial behavior, a Unified Kill Chain similar to the ATT&CK framework was studied [50], which showed that persistence, defense evasion, and privilege escalation, occur most frequently among the observed attack paths. Therefore, it is highly likely that attackers applying techniques aiming to achieve these failure modes are aiming to inflict additional impact to the network. Since the future impact cannot be known, a reasonable estimate can be reached by considering all possible impact elements in the estimation.

$$OCC_C = \frac{OC_C + SC_C + IC_C + FC_C}{4} \tag{3}$$

Finally, the value of the StC metric is calculated based on the considered failure mode. $StC = OCC$ for the persistence, defense evasion, and privilege escalation failure modes while $StC = ODC$ for the other failure modes.

The CCST should include scores for each component in the different operational modes. Some scores may not change across the different operational modes such as the IC, while others such as the I2CF, and I2MF, are more likely to change.

4.4.3 The Failure-Mode-Metric Table (FMMT). The FMMT is constructed specifying the metrics used to estimate the impact of each failure mode. A sample of the FMMT is depicted in Table 8. The FMMT reflects the mapping in the FMCT with additional information reflecting the metrics utilized to estimate the impact elements. For instance, the FMCT shown in Table 6 specifies that the Denial of Control failure mode is expected to cause only operational and safety consequences with impact factor of 1 for both; then the FMMT specifies that the operational and safety impacts are estimated using the I2CF and SC metrics, respectively.

Table 8. An FMMT Sample Reflecting Some Failure Modes and their Proposed Impact Estimation Metrics

Matrix	Failure Mode	OC	SC	IC	FC	StC
Mobile	Data Encrypted for Impact	OOI	SC	IC	FC	ODC
Mobile	Persistence					OCC
Mobile	Exploit SS7 to Track Device Location			LIC		
ICS	Denial of Control	I2CF	SC			
ICS	Denial of View	I2MF	SC		FC	ODC
ICS	Damage to Property	OOI	SC	IC	FC	
Enterprise	Privilege Escalation					OCC
Enterprise	Defense Evasion					OCC

4.4.4 Impact Calculation. Finally, the impact of the failure mode (F) for a component (C) is calculated using Equation (4). The impact factors for the failure mode are retrieved from the FMCT. The metrics utilized to indicate the impact estimation for that failure mode are retrieved from the FMMT , while the impact scores for each metric for the component are retrieved from the CCST.

$$Impact_{F,C} = (SF_F \times SC_C) + (FF_F \times FC_C) + (ICF_F \times IC_C) + (OF_F \times OC_C) + (StF_F \times StC_C) \quad (4)$$

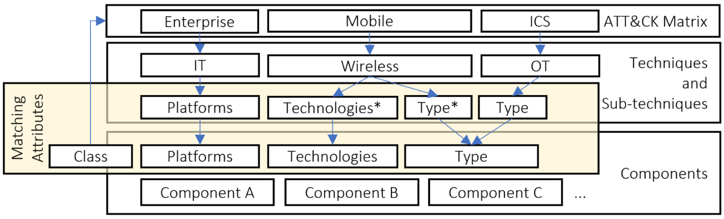
Considering the well-established relationship between the failure modes (i.e., tactics) and failure mechanisms (i.e., techniques) in ATT&CK, the estimated impact of each failure mode is considered the same for all failure mechanisms that could cause it. For instance, the collection failure mode could be achieved using more than 17 failure mechanisms (e.g., Automated Collection and Data from Information Repositories). The impact of all of them for the same component is considered the same at the design stage. In future stages in the development life cycle, when a more detailed classification of the hosted information on each component is made available, more granular impact estimation for each failure mechanism would be possible.

4.5 Identify Failure Mechanisms

A failure mechanism is defined as a process that leads to failure [15]. In this paper, the security failure mechanisms are considered. In the remainder of this paper, we refer to failure mechanisms as cyber attacks or techniques interchangeably. The identification of relevant attacks during the risk assessment through the utilization of checklists, classifications, and taxonomies is considered a comprehensive approach, in addition to promoting a common understanding of risk and reducing the need for special expertise [16]. For these reasons, we relied on the ATT&CK framework as the approach for the identifying attacks.

Due to the heterogeneous nature of CPSs, the nature of cyber-attacks is expected to be different. Accordingly, we utilized the $Techniques$ and $sub-techniques$ in the multiple matrices of ATT&CK, namely, the Enterprise matrix for the IT components, the Mobile matrix for wireless components, and the ICS matrix for OT components. Certain components can be classified as a combination of multiple classifications, therefore the attack surface for such components is expected to be broader. The relevant attacks are derived from multiple relevant matrices. For instance, a data historian component is expected to be hosted in industrial control systems, such a system is classified as a dual-homed data historian in ATT&CK, which means that it is both an IT and OT component. This means that the data historian component can be susceptible to both IT-based attacks in the Enterprise matrix as well as to OT-based attacks in the ICS-matrix. The process for identifying relevant attacks for each component is highlighted in Figure 3.

Initially, the **Techniques-Description Table (TDT)** is constructed. All techniques and sub techniques from the relevant matrices are pulled from the official MITRE ATT&CK online repository [41]. The technique-specific attributes utilized from ATT&CK that are relevant in this step are the platform, for the enterprise techniques; and the type for the ICS techniques. The mobile matrix was developed mainly for mobile devices operating Android or IOS. We have studied the techniques in



*:additions/changes were introduced to the official ATT&CK attributes

Fig. 3. Identification of relevant techniques per component from the ATT&CK matrices.

Table 9. TDT Samples Reflecting Some Techniques and their Attributes

<table>
<tr><td>Enterprise</td><td>Technique</td><td colspan="2">Platform</td><td>Tactics</td><td>CVSS</td><td>PR</td><td>AC</td><td>UI</td><td>AV</td></tr>
<tr><td>TDT</td><td>Network Device CLI</td><td colspan="2">Network</td><td>Execution</td><td>1.835</td><td>0.62</td><td>0.77</td><td>0.85</td><td>0.55</td></tr>
<tr><td>ICS</td><td>Technique</td><td colspan="2">Type</td><td>Tactics</td><td>CVSS</td><td>PR</td><td>AC</td><td>UI</td><td>AV</td></tr>
<tr><td>TDT</td><td>Alarm Suppression</td><td colspan="2">Field Controller/RTU/PLC/IED</td><td>Inhibit Response Function</td><td>2.221</td><td>0.85</td><td>0.44</td><td>0.85</td><td>0.85</td></tr>
<tr><td>Mobile</td><td>Technique</td><td>Type</td><td>Technologies</td><td>Tactics</td><td>CVSS</td><td>PR</td><td>AC</td><td>UI</td><td>AV</td></tr>
<tr><td>TDT</td><td>Jamming or Denial of Service</td><td>Any</td><td>Cellular, Wi-Fi</td><td>Network Effects</td><td>3.887</td><td>0.85</td><td>0.77</td><td>0.85</td><td>0.85</td></tr>
</table>

Table 10. A CDT Sample Reflecting Some Components and their Attributes

Name	Class	Type	Platform	MobileType	Technologies
Component A	OT/IT	Engineering Workstation	Linux	N/A	N/A
Component B	Mobile	Network	N/A	Non-App	Cell
Component C	OT/IT /Mobile	Network	Network	App-Based	Cell

the mobile matrix and we argue that they can be applied to wireless components hosted in CPSs. To this end, we propose modifications to the mobile matrix to enable the description of attacks outside the scope of traditional mobile devices, by defining the "type" and "technologies" attributes. Additional attributes in the TDT which will be utilized in later steps such as the "**Permission Required (PR)**", "Kill Chain Phase (Tactics)", and others are retrieved from ATT&CK. Samples of the TDTs are depicted in Table 9.

Secondly, the **Component-Description Table (CDT)** is constructed from the architecture description. All components in the architecture are tagged with appropriate attributes that allow accurate matching with the relevant attacks. The component-specific attributes are the "Name", "Class", "Platform", "type", "MobileType", and "technologies". The "Class" attribute specifies the component classification (following the criteria specified in Table 2) to enable its matching with techniques from relevant matrices. The "MobileType" attribute specifies the type of mobile device ("Application-based", or not), while the "technologies" attribute specifies the attached technologies with the component (e.g., Wi-Fi, Cellular, Bluetooth, etc.). The "type" and "platform" attributes specify the type corresponding to the ICS asset classification and the platform corresponding to the enterprise platform attribute, respectively. A sample of the CDT is depicted in Table 10. We argue that identifying several failure mechanisms for each failure mode for each component would support the efforts toward the proposition of risk reduction measures. Since the same failure mode could be triggered in several manners, each has a different mitigation method.

4.6 Estimate the Likelihood of Failure Mechanisms

The likelihood estimation is proposed to be conducted by utilizing the exploitability score defined in the CVSS [30]. Several works have utilized CVSS during risk assessment to evaluate risks associated with threats rather than vulnerabilities [10, 38, 54]. We argue that this approach is of great value for the security-by-design approach, since the implementation-level vulnerabilities are unknown during the system design, but the designer should at some time during the development

Table 11. Exploitability Elements, their Values, and Description

Exploitability element	Metric	Value	Description
Attack Vector (AV)	Network	0.85	The attack can be carried out remotely and not bound to the local network, such as the internet. Also, if the attack does not require direct connectivity.
	Adjacent	0.62	The attack is bound to the network stack to logically adjacent topology. Such as local IP subnet, Bluetooth connection, or GNSS transmission.
	Local	0.55	The attack can be carried locally on the target component.
	Physical	0.2	The attack requires physical action upon the component.
Attack Complexity (AC)	Low	0.77	The attack requires a low level of combined skills and resources
	High	0.44	The attack requires a considerable level of skills and/or resources.
Privileges Required (PR)	None	0.85	The attack requires no authorization upon initialization to be successful.
	Low	0.62	The attack requires user-level privileges
	High	0.27	The attack requires high privileges (e.g., administrator)
User Interaction (UI)	None	0.85	No user interaction is needed to successfully launch the attack
	Required	0.62	The attack requires an action to be taken by the user.

life cycle consider the risk of such vulnerabilities and plan controls to mitigate the risk as early as possible to reduce the cost of remediation.

The base exploitability score in CVSS is calculated using four elements. A description of these elements and their values is depicted in Table 11. The official CVSS guidelines [22] describe the calculation of the exploitability score for vulnerabilities assuming some sort of online, physical, or logical access to the vulnerable component. In this paper, we have modified the description of the "Network" **Attack Vector (AV)** from the official CVSS guidelines [22] to enable the calculation of the exploitability score for off-line attacks existing in the ATT&CK framework, such as the supply chain compromise techniques, since such techniques could be performed way before the component is operational and no direct access to the component is required. Therefore, we propose that such group of attacks is assigned the highest AV value which corresponds to "Network" in the exploitability score. All the remaining descriptions are followed as the official CVSS guidelines suggest. The Scope metric proposed in the CVSS scheme is ignored since its effect is measured in the impact analysis conducted in this paper through the proposition of the "Staging" impact element. Finally, the likelihood value for each **Failure Mechanism (FM)** (i.e., attack) is calculated according to Equation (5). We decided to use the same equation for likelihood estimation as the one suggested for the exploitability score calculation in CVSS specified in [22], to make it compatible with this widely used approach to facilitate the analysis and the communication of results.

$$Likelihood_{FM} = 8.22 \times AV \times AC \times PR \times UI \tag{5}$$

The next step is to estimate the appropriate values of the exploitability elements for each attack in the ATT&CK framework and record the estimated values in the appropriator TDT (refer to Section 4.5). The number of analyzed attacks are 525, 86, and 81 in the enterprise, mobile, and ICS matrices, respectively. This step has been performed by analyzing the descriptions of the attacks with the provided attributes. The analysis went as follows:

- If the attack has a CAPEC [45] attack pattern associated with it, the available attributes in the CAPEC page are retrieved. Some attack patterns have a description of the typical likelihood, resources, and skills required. The missing attributes were estimated based on the provided description. If the attack has more than a single CAPEC pattern associated with it, the maximum likelihood is considered and recorded in the TDT.
- Some attacks have a **Common Vulnerabilities and Exposures (CVE)** entry associated with them; in this case, the attributes were retrieved from the CVE page. The exploitability value of the CVE version 3.0 was retrieved when available, otherwise the version 2.0 value was retrieved; this lacks the User Interaction metric. Also, when more than one CVE entry is associated with the attack, the highest exploitability score is considered and recorded in the TDT.

- The values for the Privileges Required are provided in the ATT&CK framework techniques headers as attributes. Some attacks have several possible required privileges based on the possible mechanisms to launch the attack; the lowest possible privilege is considered and recorded in the TDT.
- The values for the Attack Vector were estimated using the description and utilizing the data sources attribute in the techniques headers. For instance, an attack that can be detected using a "packet capture" data source was assumed to have at least an Adjacent AV. Moreover, if the technique has an attribute "Remote Support: Yes" this means that it has a Network AV. The estimated value is then recorded in the TDT.
- The values for the Attack complexity were estimated using the description of each technique and then recorded in the TDT.

The final state of the TDT for each technology domain (i.e., matrix) including the estimated likelihood values are provided in our GitHub repository for this work.[1] We provided comments when possible to highlight the assumptions behind the estimate and/or the source providing the estimate. We consider this as another contribution of this paper. Since these tables are architecture-independent, they can be considered as encoded knowledge that can be utilized in future risk assessment tasks for a wide range of CPSs, to reduce the efforts and required skills.

4.7 Evaluate the Risks

The risk value is acquired through the calculation of a **Risk Priority Number (RPN)** as suggested in the FMECA standard [15]. The calculation of RPN for each failure mechanism (FM) against a component (C) resulting in a certain failure mode (F) is performed according to Equation (6). A qualitative rating can then be elicited based on the distribution of the risk values. The distribution of the likelihood and the detectability value is always between (0.12–3.89) and (0–1), respectively. On the other hand, the distribution of the impact value depends on the criteria chosen for the impact factor values in Equation (4).

$$RPN_{FM,C,F} = Likelihood_{FM} \times Impact_{F,C} \times Detectability_{FM,C,M} \tag{6}$$

A tool has been developed in this work to aid the calculation of the RPNs for the attacks against CPS architectures and suggest relevant mitigation methods. The tool implements the **RPN Calculation and Mitigation Identification (RPNMI)** algorithm summarized in Algorithm 1. Initially, all the tables described previously should be constructed and made available as inputs in addition to a list with the operational modes. Then, for each component specified in the CDT the relevant attacks specified in the TDT are retrieved to populate an attack list specifying the list of attacks for each component (refer to Section 4.5). Then, the likelihood of each attack in the attack list is calculated from the TDT (refer to Section 4.6), its impact is calculated based on its associated tactic according to ATT&CK using the FMCT, CCST, and FMMT (refer to Section 4.4), its detectability is calculated using the FMT and CMT (refer to Section 4.3), its RPN is calculated using Equation (6), and its suggested mitigation methods are retrieved from the FMT. Finally, the tool produces all the components' attack lists in each operation mode with RPN and mitigation methods for each attack.

4.8 Propose Risk Reduction Measures

Finally, after the identification of risk values, the last step in the performing phase of an FMECA analysis is the proposition of risk reduction measures for each failure or failure mode. The

[1] https://github.com/ahmed-amro/APS-Communication_Architecture/tree/master/RPNMI.

ALGORITHM 1: RPN Calculation and mitigation identification (RPNMI) algorithm

```
procedure RPNMI( $OPModes, TDT, CDT, FMCT, CCST, FMMT, FMT, CMT$)
    for each component in CDT do
        AttackList ← $IdentifyRelevantAttacks(CDT, TDT)$
        for each Operational Mode in OPModes do
            for each attack in AttackList do
                Likelihood ← $CalculateAttackLikelihood(TDT)$
                Impact ← $CalculateAttackImpact(FMCT, CCST, FMMT)$
                Detectability ← $CalculateAttackDetectability(FMT, CMT)$
                RPN ← $Likelihood \times Impact \times Detectability$
                MitigationList ← $GetAttackMitigation(FMT)$
            end for
        end for
    end for
    return AttackLists, RPNs and MitigationLists
end procedure
```

ATT&CK framework provides a list of suggested mitigation and detection methods for each technique. Algorithm 1 produces a list of the mitigation methods for each identified attack against components with the risk information to facilitate later analysis to prioritize the integration of the mitigation methods into a security architecture.

5 RISK ASSESSMENT FOR AN AUTONOMOUS PASSENGER SHIP

In this section, we present the details of the tool-assisted application of the proposed approach for the APS use case. The main objective is to assess the risks of cyber threats against a communication architecture for an APS to aid the efforts in managing those risks through the development of a security architecture. The analysis aims to identify cyber risks considering scenarios with malicious intent causing failures in APS components. All scenarios are induced from the description of techniques and tactics in ATT&CK. Additionally, the criteria for the treatment of failure modes are based on the stakeholders' requirements. Safety and reliability are the main topics of concern. Additional topics of concern are the privacy of APS users, financial impact, and the security of the components and their communications. Afterwards, the analysis is performed, and the detailed steps for performing a FMECA utilizing ATT&CK are presented in the subsequent sections. Finally, an FMECA report is generated detailing the analysis process. This section constitutes a summarized report of the conducted FMECA process and is intended to demonstrate the utility of the proposed approach.

5.1 Specify Components, Functions, and Performance Standard

The targeted components are inferred from the developed model of the communication architecture developed using **Architecture Analysis and Design Language (AADL)** [1]. The components addressed in this analysis are the functional components that include software and hardware elements. The components are classified as Information Technology (IT), Operational Technology (OT), Wireless, and/or a combination of multiple categories. The classification of components is conducted based on the criteria shown in Table 2. A brief description of each element is presented in Section 2.2 while a detailed discussion on them can be found in [8].

The proposed architecture supports several main functions, including autonomous, remote, and emergency navigation and control, in addition to internal, Ship-to-Shore, Ship-to-Ship, and emergency communication. Each component is involved in one or more system functions. A mapping between the system elements and the system functions has been provided using the goal tree success tree approach [52] the results of which are presented in the communication architecture definition in [8]. Moreover, the **Operational Modes (OM)** of the APS have been considered during the risk assessment process. The proposed architecture of the APS supports four operational modes, namely, **Autonomous Execution (OM-AE)**, **Autonomous Control (OM-AC)**, **Remote Control (OM-RC)**, and **fail-to-safe (OM-F2S)**. Each component is utilized in one or more operational modes. It has been identified that the overall APS system structure can be in one of two states (set of components and their connections); the first state operates in the three operational modes (OM-AE, OM-AC, and OM-RC) while the second state operates in the fourth operational mode (OM-F2S). This allowed for a more granular risk assessment.

Nevertheless, for the use case employed in this work, the results reflect no considerable difference in the risk values when considering the operational modes. However, we argue that for more advanced systems in which the components' interconnections could differ considerably across different operational modes, considering risk assessment with an operational mode perspective could reveal unexpected risk values.

The performance standard is based on the system security engineering definition of security failure; any violation of one of the established requirements and/or objectives of for the APS components constitutes a system security failure.

5.2 Identify Failure Modes

All the failure modes in ATT&CK (refer to Section 4.2) were considered relevant and have been considered, except two from the mobile matrix, namely, Generate Fraudulent Advertising Revenue, and Manipulate App Store Rankings or Ratings. All the other failure modes; should they occur, violate one or more of the stakeholders' concerns communicated as requirements and objectives in our earlier work [7].

5.3 Identify Detection Methods and Risk Reduction Measures

Considering that the system under analysis is still under development, no detection methods have yet been integrated. On the other hand, some controls have been proposed and included in the architecture description to satisfy previously established requirements. These are: Out-of-Band Communications Channel, Network Segmentation, and Redundancy of Service. Based on this, the CMT (refer to Section 4.3) is constructed describing the coverage of the architectural components with regards to the mitigation methods.

5.4 Estimate the Impact of the Consequences of Failure Modes

The estimation of the impact values of failure modes for the APS architecture is conducted as follows:

5.4.1 The Failure-Mode-Consequences Table (FMCT). It is constructed for the APS use case considering the entire communication architecture as a System-of-Systems. The constructed FMCT is depicted in Table 6.

5.4.2 The Component-Criticality-Scores Table (CCST). It is constructed as follows:

- Safety and Financial criticality (SC and FC): safety and financial impact scores for each component were elicited from previously conducted Preliminary Hazard Analysis (PHA) for an APS use case [61].
- The different Operational Criticality (OC) scores, namely, the OOI, I2CF, and I2MF were calculated as described in Section 4.4. Three architecture views were developed using the ORA software. The OOI metric for each component is calculated using the combined centrality measures provided by the ORA software after modeling the entire APS network. The I2CF metric for each component is calculated in a similar manner, but only the components

Table 12. IPC and DC Estimation Criteria

Data Criticality (DC)	Description	Intellectual Property Criticality (IPC)	Description
None (0)	The component does not store or process sensitive passenger data (e.g., GNSS System).	None (0)	The component host processes with no intellectual property value.
Low (0.33)	The component only forwards encoded sensitive passenger data (e.g., network device).	Low (0.33)	The component host processes with low intellectual property value (Common proprietary software) (e.g., network devices).
Medium (0.66)	The component performs the processing of sensitive passenger data (e.g., video camera).	Medium (0.66)	The component host processes with medium intellectual property value (Rare proprietary software) (e.g., DP system).
High (0.99)	The component stores sensitive passenger data (e.g., data historian).	High (0.99)	The component host processes with high intellectual property value (Innovative proprietary software) (e.g., ANS).

involved in the control functions (Autonomous, remote, and emergency control, Section 5.1) were modeled. Finally, the I2MF metric for each component is similarly calculated, but only the components involved in the monitoring functions (Autonomous, remote, and emergency navigation, Section 5.1) were modeled.

- The Information Criticality (IC) scores were estimated based on the communicated stakeholders' concerns. A specific requirement has been established to protect passengers' privacy from tracking and surveillance [7]. Also, concerns related to the preservation of intellectual property of processes hosted within the ship components in the Autoferry project [46] have been expressed. The estimation criteria for the IPC and DC metrics are shown in Table 12. The location information has been deemed to be of no impact (zero value) because the APS is utilized for passenger transportation in a fixed operational area.
- The Staging Criticality (StC) scores were calculated as follows:
  - The ODC scores for each component were calculated by the ORA software after modeling the entire APS network.
  - The OCC scores for each component were calculated using all the previously estimated criticality scores according to Equation (3).

5.4.3 The Failure-Mode-Metric Table (FMMT). The FMMT is constructed reflecting the metrics that are needed to estimate each impact of each failure mode.

5.4.4 Impact Calculation. The final impact values for each failure mode of each component are calculated by means of Equation (4), by utilizing the developed tool.

5.5 Identify Failure Mechanisms

The identification is conducted by utilizing the approach that identifies the relevant attacks for each component using attribute matching as described in Section 4.5. Initially, the TDT table is constructed by retrieving the techniques from the ATT&CK repository. Then the CDT is constructed by consulting the architecture description in [8]. Future work may attempt to perform automatic construction of the CDT table from a formal architecture description provided through an architecture description language such as AADL. Nevertheless, in this work, the CDT is manually constructed in a **Comma Separated Value (CSV)** format.

5.6 Estimate the Likelihood of Failure Mechanisms

The likelihood for each technique is calculated by means of Equation (5), using the available information in the TDT. The result is added to the TDT in the "CVSS" column (refer to Table 9).

5.7 Evaluate the Risks

Afterwards, the tool calculates the RPN of all attacks relevant to all components using the RPNMI algorithm described in Section 4.7. Since the impact factors (refer to Section 4.4) are all chosen to be 1, a qualitative rating of the RPN can be calculated according to the following criteria: low risk rating (0–4.86), medium risk rating (4.87–9.72), high risk rating (9.73–14.58), and critical risk rating (14.59–19.44).

5.8 Propose Risk Reduction Measures

The tool additionally provides the mitigation methods suggested for each technique, based on the FMT table (refer to Section 4.3). Therefore, the suggested mitigation methods for each failure mechanism were identified and collected to analyze the most needed mitigation methods to support the effort in the development of a security architecture for the APS.

6 RESULTS AND EVALUATION

In this section, a summary of the results of the risk assessment process are presented to demonstrate the granular and comprehensive outcome of the proposed approach. Additionally, we show the evaluation of the different elements of the approach.

After conducting a risk analysis of attacks against 39 different components in the APS architecture, we present an overview of the highest identified risks across the different failure modes, the most observed failure modes, failure mechanisms, and required mitigation methods. Concurrently, we discuss the utility of our approach regarding each outcome and the argued differences compared to other approaches. Then, an evaluation of the proposed metrics for estimating operational and staging impacts is presented.

Since no considerable difference has been identified in the risk values among the different operational modes, all the presented results are related to risks specifically identified for three operational modes, namely, OM-AE, OM-AC, and OM-RC; as they all maintain a unified system state, the risk values are the same among all of them.

The developed tool and the raw results can be found in our shared GitHub repository.[2] Additionally, we have shared the populated tables discussed throughout the paper. These tables were utilized for the risk assessment of the APS communication architecture.

6.1 Overview

The comprehensive outcome of our proposed approach is demonstrated in Figure 4. The figure depicts the identified techniques with the highest risks across the different failure modes or tactics. Firstly, the utility of the inclusion of the different ATT&CK matrices is demonstrated through the identification of different risks from all of them. For instance, the manipulation of communication is a risk against wireless technology suggested in the mobile matrix in ATT&CK. In the APS, an expected implementation of the traffic module is an AIS. The result seems consistent with what is observed in the literature since AIS has been deemed susceptible to spoofing attacks by several works [12, 33]. However, in our approach, this risk is identified without the need for expert judgment as it is encoded common knowledge. Similarly, the suggested mitigation methods are drawn from the encoded common knowledge in ATT&CK and are in alignment with an observed direction for improving the security of AIS through encryption as suggested by Goudossis and Katsikas [24]. Also, the consideration of 16 failure mode categories improves the risk and countermeasures description. For instance, Auditing is a proposed countermeasure for the “Modify parameter” technique to impair process control. This granular description of the threat also suggests another descriptive scope for auditing, which is to include technologies and processes that allow the investigation of the modification of parameters sent to the DP controller component. Figure 4 also highlights the logical identification and estimation of risks across the different tactics. For instance, considering the digital logbook for the collection of information is very reasonable as

[2] https://github.com/ahmed-amro/APS-Communication_Architecture/tree/master/RPNMI.

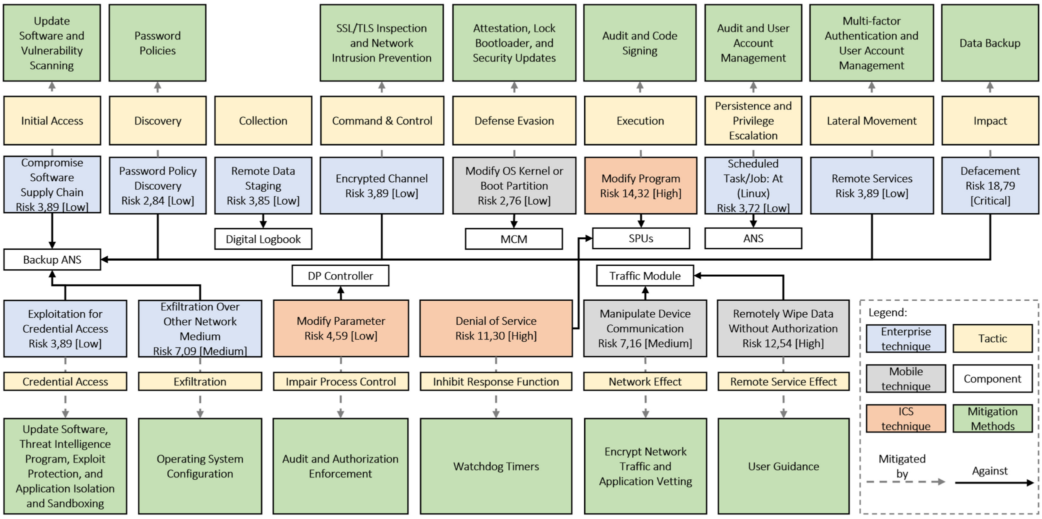

Update Software and Vulnerability Scanning
Password Policies
SSL/TLS Inspection and Network Intrusion Prevention
Attestation, Lock Bootloader, and Security Updates
Audit and Code Signing
Audit and User Account Management
Multi-factor Authentication and User Account Management
Data Backup
Initial Access
Discovery
Collection
Command & Control
Defense Evasion
Execution
Persistence and Privilege Escalation
Lateral Movement
Impact
Compromise Software Supply Chain Risk 3,89 [Low]
Password Policy Discovery Risk 2,84 [Low]
Remote Data Staging Risk 3,85 [Low]
Encrypted Channel Risk 3,89 [Low]
Modify OS Kernel or Boot Partition Risk 2,76 [Low]
Modify Program Risk 14,32 [High]
Scheduled Task/Job: At (Linux) Risk 3,72 [Low]
Remote Services Risk 3,89 [Low]
Defacement Risk 18,79 [Critical]
Digital Logbook
MCM
SPUs
ANS
Backup ANS
DP Controller
Traffic Module
Exploitation for Credential Access Risk 3,89 [Low]
Exfiltration Over Other Network Medium Risk 7,09 [Medium]
Modify Parameter Risk 4,59 [Low]
Denial of Service Risk 11,30 [High]
Manipulate Device Communication Risk 7,16 [Medium]
Remotely Wipe Data Without Authorization Risk 12,54 [High]
Credential Access
Exfiltration
Impair Process Control
Inhibit Response Function
Network Effect
Remote Service Effect
Update Software, Threat Intelligence Program, Exploit Protection, and Application Isolation and Sandboxing
Operating System Configuration
Audit and Authorization Enforcement
Watchdog Timers
Encrypt Network Traffic and Application Vetting
User Guidance
Legend:
Enterprise technique
Tactic
Mobile technique
Component
ICS technique
Mitigation Methods
Mitigated by
Against

Fig. 4. An overview of the identified highest risk techniques for each tactic, their calculated risk, targeted component, and suggested mitigation method.

it is the component with the highest information criticality; its function is to log and store information from most components, including passenger-related information. Still, the collection itself constitutes low risk since the collected information is still within the same component. Then, considering the Backup ANS for exfiltration through other network media is also very reasonable as it is a more connected component and is expected to include several communication technologies. Also, exfiltration does constitute a higher risk than collection since it also can affect other components if the exfiltration includs system credentials. Another example is the risks associated with the **Sensor Processing Units (SPU)**. These components are proposed to aggregate the different sources of sensor data before forwarding them to the **Autonomous Navigation System (ANS)**. The estimated risks of targeting this component through the execution of a modified program as well as denial of service are very reasonable. Since both would inhibit the monitoring functions of the APS and disable its ability to establish situational awareness which could lead to hazardous consequences (e.g., collision).

Overall, we argue that no other observed approach in the literature provides such a detailed level of risk identification, estimation, and proposition of countermeasures that can be utilized from the design stage. Also, the approach can be conducted in a semi-automated manner based on an updatable source such as ATT&CK, which results in reduced risk assessment effort.

6.2 Failure Modes

The risks associated with each failure mode have been analyzed. The results suggest that the most critical failure modes are related to adversaries aiming to inflict an impact, execute malicious software, remotely affect the APS services and inhibit the response functions of the APS. Additionally, exfiltration of sensitive passenger information or information with intellectual property as well as affecting the APS network constitute medium risks. The remaining failure modes constitute only low risks according to the followed risk management strategy.

The risks of some techniques such as Defense Evasion, Credential Access, Discovery, and the like, have been estimated "Low" due to the risk management strategy followed in the estimation of the impact of failure modes which is captured in the FMCT (refer to Section 4.4). The strategy considers all the elements of impact as equals; this rendered the impact of these failure modes as low as they only affect the staging impact element (see Table 6). A different security-focused risk strategy that increases the value of the staging factor (i.e., StF) in the impact estimation could have been adopted; such a strategy would generate different results and it is to be expected in future work.

Compared to other works, we argue that our risk assessment methodology provides a granular description of failure modes. Other methods provide a comparatively less meaningful description of the attackers' objectives in the assessed system. For instance, the persistence, command and control, and defense evasion failure modes are not straightforwardly mapped to the STRIDE threat categories or the CIA objectives. Considering the popularity of such failure modes in the current threat landscape, a methodology that addresses them is required. Moreover, the inclusion of failure modes from the different technology domains (i.e., ATT&CK matrices) provides meaningful context to the failure modes. For instance, the high risk identified due to the remote service effects failure mode highlights the risks associated with the inclusion of wireless technology while the inhibit response function highlights risks due to the inclusion of OT for monitoring functions. We argue that this provides an improved threat communication feature of our approach.

6.3 Failure Mechanisms

The Failure Mechanisms (i.e., techniques) with estimated critical and high risks belong to the "impact" failure mode. Regarding critical risks, an attacker could severely impact the entire APS and its operational area, possibly leading to damage and life-threatening hazard against passengers through the ANS and Backup ANS that are responsible for the navigation functions. Damage could occur through several forms, an example would be similar to the Polish teen incident in which he derailed the city tram system [56], an attacker controlling the main or backup ANS systems could enforce unsafe routes and/or drop the reporting of warnings to the operator to avoid intervention. Moreover, a surprising risk was identified: the possibility to inflict impact through a defacement attack. Defacement attacks usually target web applications by modifying the distributed content [42]. A possible implementation of the control and monitoring functions could be through web services [39, 49]. Therefore, a defacement technique could manipulate or impair the control and monitoring functions to a severe degree. Regarding high risks, a group of attacks has been identified, that aim to inflict impact through a group of denial of service techniques, namely, reflection amplification, direct network flood, service and OS exhalation flood, or endpoint and network denial of service. Additionally, other attacks could inflict impact through manipulation of transmitted date, scheduled execution, scripting, and project file infection. Two surprising techniques that are not common against ships are "Resource Hijacking", and "Remotely Wipe Data Without Authorization". Resource hijacking is a widely observed technique that attackers carry out to exploit system resources to validate transactions related to cryptocurrency networks [43]. Such a technique could impair the target system by reducing its performance, the effect could be amplified if the component is involved in time-critical functions which is the case for some of the APS components such as the **Autonomous Navigation System (ANS)**. Also, adversaries could Remotely Wipe Data Without Authorization for components involved in the control and monitoring functions; this attack could be in the form of ransomware. The **Mobile Communication Module (MCM)** components are expected to be routers that are not immune against ransomware attacks [47], while the traffic modules are expected to be **Automatic Identification Systems (AIS)**. Until the time of writing this paper, no ransomware attack has been found to attack this specific implementation solution but, at the design stage, the implementation solution is unknown, and therefore, such an attack could be of relevance and therefore should be considered.

Table 13. Snapshot from CCST Reflecting the Criticality Scores of the Highlighted Components

Op-Mode	Component	OC			SC	IC	FC	StC	
		OOI	I2CF	I2MF				ODC	OCC
OM-AE, OM-AC, and OM-RC	AEMC	0.95	1	0	1	0.49	1	0.88	0.86
	ANS	1	0.27	1	1	0.82	1	0.77	0.95
	Backup ANS	0.99	0.074	0.99	1	0.82	1	1	0.95
	GNSS IMU	0.45	0	0.56	1	0.16	1	0.11	0.65

Other attacks observed in the maritime domain such as jamming, data encryption for impact (i.e., ransomware), and exfiltration have been found to have a medium impact. These results were not surprising, for different reasons. Jamming attacks have been considered since the system concept definition phase in the Autoferry project; therefore, design solutions were introduced to mitigate their effect through redundant functional components such as other sensors. Thus, the operational effect of the jamming attack is reduced and this is reflected in the risk value. Furthermore, network segmentation is one of the mitigation methods against ransomware and exfiltration attacks. The APS network has been designed with network segmentation for most of the components. This affects the *Detectability* value of the risks against them and thus reduces their risk values. We argue that these results reflect the accuracy of our proposed process.

6.4 Mitigation Methods

An outcome of our proposed approach is a list of the most needed mitigation methods, drawn from the suggested mitigation methods by ATT&CK for the identified risks. The mitigation methods against critical risks include data backup, mechanical protection layers, safety, instrumented systems, network allow lists, out-of-band communication channels, and redundancy of service. These controls are considered to be prioritized during the security architecture design. Two special categories of mitigation methods should receive additional focus, namely, “Mitigation Limited or Not Effective” and “Do Not Mitigate”. ATT&CK classifies the mitigation method for certain techniques as difficult to mitigate since they are based on the abuse of system features; yet, some of them have proposed suggestions for detection that should be considered in the security architecture design. The identified techniques with high and medium risks that belong to such category include Resource Hijacking, Account Access Removal, Automated Exfiltration, Jamming or Denial of Service, and System Shutdown or Reboot. Therefore, future efforts will be dedicated to suggesting mitigation methods for these techniques in the APS and integrating them within the security architecture. Moreover, two defense evasion techniques, namely Execution Guardrails, and Environmental Keying are proposed not to be mitigated, since the mitigation methods could lead to increasing the risk of compromise.

6.5 Evaluation for the Proposed Metrics

In this section, we present the results of the analysis conducted to evaluate the proposed staging and operational impact metrics. During the discussion in the coming sections, we will utilize the values in Table 13, which depicts a snapshot from the CCST (Section 4.4) holding the values of the impact metrics for the AEMC, ANS, Backup ANS, and GNSS components.

6.5.1 *The Granularity of Operational Impact Estimation.*

In this section, we highlight the results of our proposed application of the different operational criticality metrics, namely the **Overall Operational Impact (OOI)**, **Impact to the Control Functions (I2CF)**, and **Impact to the Monitoring Functions (I2MF)** (refer to Section 4.4). To demonstrate the effect of the application of these metrics on the risk estimation, Table 14 depicts the utilized metrics in the calculation of the impact score for three different failure modes against the ANS and AEMC components. According

Table 14. Estimation of Failure Mode Impact using Different OC Metrics

Failure Mode	OC Metric	Componet	OC			SC	IC	FC	StC	Impact Value
			OOI	I2CF	I2MF				ODC	
Impair Process Control	OOI	AEMC	0.950538225	-	-	1	-	1	-	2.950538225
	I2CF		-	1						3
	OOI	ANS	1	-						3
	I2CF		-	0.272978267						2.272978267
Manipulation of View	OOI	AEMC	0.950538225	-	-				0.8888889	3.839427125
	I2MF		-		0				-	2.8888889
	OOI	ANS	1		-				0.7777778	3.7777778
	I2MF		-		1				-	3.7777778
Resource Hijacking	OOI	AEMC	0.950538225		-				0.8888889	3.839427125
	OOI	ANS	1						0.7777778	3.7777778

to Table 6, the “Impair Process Control” failure mode has positive SF, FF, and OF, which means that it is only expected to cause incidents with safety, financial, and operational impacts. The **safety criticality (SC)** and **financial criticality (FC)** are all estimated using the same metrics for the three failure modes. The **operational criticality (OC)** on the other hand, can be estimated using either the OOI or the I2CF. Considering the two components, the impact of this failure mode when using the OOI metric has a negligible difference: 2.95, and 3 for the AEMC and the ANS, respectively. But, when using the I2CF the difference is noticeable: 3 and 2.27 for the AEMC and the ANS, respectively. Since the AEMC is heavily involved in the control functions while the ANS has less involvement, we argue that the I2CF metric reflects a more reasonable estimate of the operational impact than the OOI metric for this failure mode and similar ones involved in the control functions. The other failure mode, namely the “Manipulation of View”, has positive SC, FF, OC, and StC, meaning it can cause incidents with safety, financial, operational, and staging impacts. The OC metric can be estimated using either the OOI or the I2MF metrics. The difference in the impact values is negligible when using the OOI metric: 3.84, and 3.78 for the AEMC and the ANS, respectively. But, when using the I2MF metric, the difference is noticeable: 2.89, and 3.78 for the AEMC and the ANS, respectively. Since the ANS is heavily involved in the monitoring functions while the AEMC has much less involvement, we argue that the I2MF metric accounts for a more reasonable estimate of the operational impact than the OOI metric for this failure mode and similar ones involved in the monitoring functions. Finally, the “Resource Hijacking” failure mode could impact the entire system functions, certainly not only the control and monitoring functions. Considering that ANS and AEMC are centralized components involved in several functions other than monitoring and control and both have very similar combined centrality measures (0.95 and 1 for the AEMC and ANS, respectively), the OOI metric captures a reasonable estimate of the operational impact for this failure mode should it occur for any of these components.

The majority of observed risk assessment methods are qualitative as they utilize expert judgment for the estimation of the operational impact. This increases the required effort for conducting risk assessment and subjugates the assessment to bias. However, our proposed metrics reduce these shortcomings by relying on a graph-based model of the system for providing a more granular quantitative estimate of the operational impact.

6.5.2 The Granularity of Staging Impact Estimation. As discussed in Section 4.4, the staging impact element estimates the ability of the attacker to stage future attacks which are mainly influenced by the position and criticality of the attacked component in the system network. Table 15 shows the estimates of the impact value of the group of failure modes that do not have any other impact than the staging impact. Also, an example of a failure mechanism for each failure mode is presented. The Backup ANS component is among the most connected components in the network, having the highest **Outbound Degree Centrality (ODC)** measure. This provides attackers with several options for traversing the network for staging other attacks. Moreover, it is a critical

Table 15. Estimation of Failure Modes Impact using the StC Metrics

								Backup ANS	GNSS IMU
Failure Mechanism	Description	Failure Mode	StC Metric	OC	SC	IC	FC	Impact Value	Impact Value
VNC	Attackers may use this remote access software to access other components in the network	Lateral Movement	ODC	-				1	0.111
DNS	Attackers may communicate using DNS protocol to avoid detection	Command and Control							
Drive-by Compromise	Attackers may obtain initial access using a downloaded malicious payload (e.g., driver)	Initial Access							
ARP Cache Poisoning	Attackers may use this technique to collect and/or relay data such as credential	Credential Access							
Remote System Discovery	Attackers may discover connected systems in the network	Discovery							
Valid Accounts	Attackers may create new accounts or use existing ones to keep a foothold in the network	Persistance	OCC					0.956	0.654
Obfuscated Files or Information	Attackers may alter files in a manner to make them hard to discover	Defense Evasion							
At (Linux)	Attackers may exploit this scheduling tool to run a process using the privilege of a specified account	Privilege Escalation							

component, having among the highest **Overall Component Criticality (OCC)**. Failing to eliminate persistence, defense evasion and privilege escalation failure modes on this specific component could initiate critical future risks, thus the staging impact is higher. On the other hand, the GNSS IMU system is much less connected and has among the lowest ODC. This limits the attacker's ability to traverse the network. Also, its OCC measure is estimated to be less than that of the Backup ANS, as it is less involved in the overall operations and hosts less critical information. Therefore, its staging impact estimates for the failure mechanisms shown in Table 15 are also less. The results suggest that the ODC and OCC metric provides reasonable estimates of the proposed staging impact.

We argue that other risk assessment methods observed in the literature might overlook the impact of certain failure mechanisms in ATT&CK. For instance, using the legitimate VNC software for lateral movement is not expected to have any safety, financial, privacy, or operational impact on the target component, nor does it inflict an immediate impact on confidentiality, integrity, or availability. However, it aids attackers during the staging of cyber attacks and our approach provides a granular estimation of the impact of such activities. We argue that this impact element is of critical value to the cybersecurity posture as it aids the identification of the most critical risks related to the ability of adversaries to stage attacks.

7 LIMITATIONS, DISCUSSION AND FUTURE WORK

Below, limitations in the proposed approach are discussed with possible improvements to be addressed in future work:

- Traditional FMECA only enables the identification of single failure modes [16]. Nevertheless, the relationships between different failure modes are communicated through the kill chain concept embedded in ATT&CK. The latest version of ATT&CK provides detailed information regarding software (i.e., malware) and threat groups employing the different tactics and techniques. Specifically, 638 software and 129 threat groups are present in the enterprise and mobile matrices in addition to 19 software and nine groups in the ICS matrix. This information is expected to be utilized as models for propagating threats in the system under analysis. Additionally, the expected paths (i.e., links) in the network utilizing graph theory are also planned to be employed to achieve comprehensive coverage of threat propagation paths. However, the correlation between the different ATT&CK techniques across the different kill chain phases in addition to the suitable methods for estimating the collective likelihood and impact values are yet unresolved issues. Therefore, future work will focus on the correlation between attacks, causing different failure modes to generate attack scenarios composed of coherent steps similar to the concept of attack trees.

- The Checklist risk identification approach is said to lack the ability to identify new attacks [16]. We argue that the comprehensive nature of the tactics and techniques in ATT&CK reduces the effect of this limitation.
- Some components might be covered by multiple mitigation methods. In this paper, for simplicity, the detectability value is estimated based on whether a component is covered by (at least) one mitigation method or not. Future work can investigate how this value is affected when multiple mitigation methods contribute to the coverage.
- We relied on the literature for choosing the ODC to estimate the staging impact. Nevertheless, we have considered other centrality measures, such as the Authority Centrality, to estimate the staging impact. However, it is outside the scope of this paper to compare the utility of different centrality measures. In future work, a comparative study could be conducted to do so.
- The mapping between failure mode and consequence reflected in the FMCT (refer to Section 4.4) is constructed after manual analysis of the description of each failure mode in ATT&CK and as such, it is subject to bias and therefore should be reconstructed for other use cases with considerations for reducing biased judgment. The IEC 31010 standard [16] provides guidelines for eliciting stakeholders' and experts' views while reducing bias.
- The ODC metric in the staging impact estimation may overlook the fact that in some attacks, the attacker only requires a single point of access to stage future attacks (Low ODC value). However, we argue that the higher the possible points of access from a component to other components, the higher the impact value contributing to the risk.
- The proposed metrics for estimating safety and financial impacts require a prior PHA/HAZOP or similar analysis. Future work may attempt to provide more granular quantitative estimates induced from the architecture description.
- A comparative analysis of our proposed approach is suggested for future work. This includes the engagement of independent experts to isolate and prevent biases introduced by the authors, as well as considering several use cases that could help quantify performance limitations across the various methods.

7.1 Approach Adaptability

Our proposed approach can be applied in different CPS use cases. Also, it is capable of assessing new risks matching the up-to-date threat landscape due to its reliance on the ATT&CK framework. Figure 5 depicts a flowchart for applying the approach at different periods of time, in different use cases, or when the same use case is updated or modified.

When the approach is to be applied against a different system or a modified version of the same system, the system components are classified according to the criteria in Table 2. If some components cannot be classified (e.g., docker containers), the risks associated with them will not be assessed. Then, the relevant failure modes from Table 3 are identified. Then, the CMT is updated to map the relationships between the existing controls and the system components. However, the controls are limited to those in the ATT&CK framework. Therefore, use cases with some controls that do not exist in the ATT&CK framework (e.g., Email Protection) will suffer inaccurate results. Afterward, the FMCT is updated to map the relationships between the failure modes and the consequences according to the defined impact model. Consequently, the FMMT is updated to define the required metrics for the entries in the FMCT. After that, the CCST is updated to specify the criticality values of the components in the system. This is done by estimating the safety, financial, operational, information, and staging criticality metrics using their appropriate approaches discussed

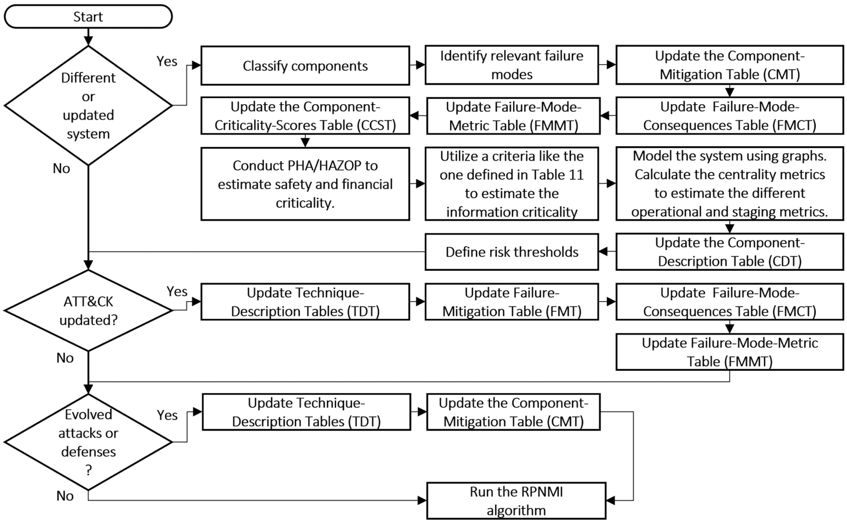

Start
Different or updated system
Yes
No
Classify components
Identify relevant failure modes
Update the Component-Mitigation Table (CMT)
Update Failure-Mode-Consequences Table (FMCT)
Update Failure-Mode-Metric Table (FMMT)
Update the Component-Criticality-Scores Table (CCST)
Conduct PHA/HAZOP to estimate safety and financial criticality.
Utilize a criteria like the one defined in Table 11 to estimate the information criticality
Model the system using graphs. Calculate the centrality metrics to estimate the different operational and staging metrics.
Update the Component-Description Table (CDT)
Define risk thresholds
ATT&CK updated?
Yes
No
Update Technique-Description Tables (TDT)
Update Failure-Mitigation Table (FMT)
Update Failure-Mode-Consequences Table (FMCT)
Update Failure-Mode-Metric Table (FMMT)
Evolved attacks or defenses ?
Yes
No
Update Technique-Description Tables (TDT)
Update the Component-Mitigation Table (CMT)
Run the RPNMI algorithm

Fig. 5. The procedure for applying the approach in different or updated systems and at different periods of times.

in Section 4.4.2. Later, the CDT is updated with the components properties, namely, classification, type, platform, mobile type, and technologies. Then, the risk threshold needs to be defined.

In the case of a new version or an update to ATT&CK is released, some tables needs to be updated. This can be done by updating the TDT by fetching the techniques' information from the ATT&CK online repository and updating their CVSS metrics. Then, updating the FMT by fetching the information of the techniques' mitigation methods from the online repository and updating the effectiveness estimation. Later, the FMCT is updated after identifying the new failure modes and defining their expected consequences according to the defined impact model. Consequently, the FMMT is updated to define the required metrics for the new entries in the FMCT.

In the case that some attack techniques and defenses evolve effecting the CVSS or effectiveness estimations in the TDT or CMT, respectively, some tables needs to be updated. For instance, a new released exploit for an attack technique with different attack complexity. This changes the respective CVSS score of that attack.

Finally, when all the aforementioned conditions are considered and processed, the RPNMI algorithm can be launched to generate updated results.

8 CONCLUSION

A semi-quantitative risk assessment approach is proposed in this paper following a **Failure Modes Effects and Criticality Analysis (FMECA)** and utilizing the ATT&CK framework. This approach provides a comprehensive risk assessment while reducing the need for expert judgment. Additionally, the approach addresses the heterogeneous nature of CPSs and provides attack descriptions that are relevant for different categories of components. Further, the approach, in addition to identifying the required mitigation methods, can identify areas of concern which the system under analysis can be susceptible to and only limited mitigation methods are yet available. Moreover, the approach allows for the updatability of the risk values through updating input values to reflect the current threat landscape.

The proposed impact estimation metrics are demonstrated to provide a reasonable estimate of the different impact elements, namely operational, information criticality, and security-related impact. Additional efforts are required to provide metrics that are capable of estimating safety and financial impacts.

The approach has been evaluated through a tool implementing the **RPN Calculation and mitigation identification (RPNMI)** algorithm. The tool has been used for conducting a risk assessment for the APS. The results reflect the comprehensive and granular nature of the results as they provided a detailed description of the risks and suggested countermeasures. This provides useful suggestions to be included in later efforts for the development of a relevant security architecture.

Future efforts are needed to address the propagation of threats, improve safety and financial impact estimation, and the estimation of countermeasure effectiveness. Moreover, future applications of the approach are discussed, including the development of threat-informed security architectures, residual risk estimation, and supporting adversary emulation for security evaluation.

Regarding the APS, the need for data backup, network allow list, out-of-band communication channels, and redundancy of service have been identified to have the highest priority for integration within the security architecture. Moreover, the results suggest that additional work is needed to provide mitigation methods against certain threats, such as resource hijacking, account access removal, jamming, and denial of service.

REFERENCES

[1] [n.d.]. APS communication architecture AADL model. https://github.com/ahmed-amro/APS-Communication_Architecture.git. Accessed: 2021-02-16.

[2] 2018. COSCO Shipping Lines Falls Victim to Cyber Attack. https://bit.ly/COSCOAttack.

[3] 2018. Iranian hackers suspected in cyber breach and extortion attempt on Navy shipbuilder Austal. https://bit.ly/AustalAttack.

[4] Aida Akbarzadeh and Sokratis Katsikas. 2020. Identifying critical components in large scale cyber physical systems. In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*. 230–236.

[5] Otis Alexander, Misha Belisle, and Jacob Steele. 2020. MITRE ATT&CK® for industrial control systems: Design and philosophy. (2020).

[6] Neal Altman, Kathleen M. Carley, and Jeffrey Reminga. 2017. ORA User's Guide 2017. *Center for the Computational Analysis of Social and Organizational System CASOS Technical Report* (2017).

[7] Ahmed Amro, Vasileios Gkioulos, and Sokratis Katsikas. 2019. Connect and protect: Requirements for maritime autonomous surface ship in urban passenger transportation. In *Computer Security*. Springer, 69–85.

[8] Ahmed Amro, Vasileios Gkioulos, and Sokratis Katsikas. 2021. Communication architecture for autonomous passenger ship. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* (2021), 1748006X211002546.

[9] Arben Asllani, Alireza Lari, and Nasim Lari. 2018. Strengthening information technology security through the failure modes and effects analysis approach. *International Journal of Quality Innovation* 4, 1 (2018), 5.

[10] Ali Behfarnia and Ali Eslami. 2018. Risk assessment of autonomous vehicles using Bayesian defense graphs. In *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*. IEEE, 1–5.

[11] Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. 2016. A process for data protection impact assessment under the European general data protection regulation. In *Annual Privacy Forum*. Springer, 21–37.

[12] Victor Bolbot, Gerasimos Theotokatos, Evangelos Boulougouris, and Dracos Vassalos. 2020. A novel cyber-risk assessment method for ship systems. *Safety Science* 131 (2020), 104908.

[13] Kathleen M. Carley and Jürgen Pfeffer. 2012. Dynamic network analysis (DNA) and ORA. *Advances in Design for Cross-Cultural Activities Part I* (2012), 265–274.

[14] Roger Clarke. 2009. Privacy impact assessment: Its origins and development. *Computer Law & Security Review* 25, 2 (2009), 123–135.

[15] IEC 60812 Technical Committee et al. 2018. Analysis techniques for system reliability-procedure for failure mode and effects analysis (FMEA). (2018).

[16] IEC 31010 Technical Committee et al. 2019. 31010: Risk management–risk assessment techniques. (2019).

[17] SAE J3061 Vehicle Cybersecurity Systems Engineering Committee et al. 2016. Cybersecurity guidebook for cyber-physical vehicle systems. *SAE International* (2016).

[18] The Maritime Safety Committee. [n.d.]. Interim Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.1). https://cutt.ly/6R8wqjN.

[19] Mirko Čorić, Anita Gudelj, Zvonimir Lušić, and Sadko Mandžuka. 2019. E-navigation architecture overview and functional connection analysis. *NAŠE MORE: Znanstveno-stručni časopis za more i Pomorstvo* 66, 3 (2019), 120–129.

[20] Manlio De Domenico, Albert Solé-Ribalta, Elisa Omodei, Sergio Gómez, and Alex Arenas. 2015. Ranking in interconnected multilayer networks reveals versatile nodes. *Nature Communications* 6, 1 (2015), 1–6.

[21] Okan Duru. [n.d.]. The Future Shipping Company: Autonomous Shipping Fleet Operators. https://bit.ly/MaritimeFuture.

[22] FIRST. 2019. Common vulnerability scoring system version 3.1: Specification document. (2019).

[23] International Organization for Standardization. 2018. *Information Technology. Security Techniques. Information Security Risk Management: ISO/IEC 27005: 2018.* International Organization for Standardization.

[24] Athanassios Goudossis and Sokratis K. Katsikas. 2019. Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology* 24, 2 (2019), 410–423.

[25] Andy Greenberg. [n.d.]. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. https://bit.ly/MaerskAttack.

[26] INSIKT GROUP. 2020 (accessed December 2, 2020). *Defense Evasion Dominant in Top MITRE ATT&CK Tactics of 2019.* https://www.recordedfuture.com/mitre-attack-tactics/.

[27] J. P. Gupta and B. Suresh Babu. 1999. A new hazardous waste index. *Journal of Hazardous Materials* 67, 1 (1999), 1–7.

[28] David Hambling. 2017. Ships fooled in GPS spoofing attack suggest Russian cyberweapon. https://bit.ly/GPSAttack.

[29] Gina Havdal, Christina Torjussen Heggelund, and Charlotte Hjelmseth Larssen. 2017. *Design of a Small Autonomous Passenger Ferry.* Master's thesis. NTNU.

[30] Siv Hilde Houmb, Virginia N. L. Franqueira, and Erlend A. Engum. 2010. Quantifying security risk level from CVSS estimates of frequency and impact. *Journal of Systems and Software* 83, 9 (2010), 1622–1634.

[31] Mafijul Md. Islam, Aljoscha Lautenbach, Christian Sandberg, and Tomas Olovsson. 2016. A risk assessment framework for automotive embedded systems. In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security.* 3–14.

[32] Bojan Jelacic, Daniela Rosic, Imre Lendak, Marina Stanojevic, and Sebastijan Stoja. 2017. STRIDE to a secure smart grid in a hybrid cloud. In *Computer Security.* Springer, 77–90.

[33] Georgios Kavallieratos, Sokratis Katsikas, and Vasileios Gkioulos. 2018. Cyber-attacks against the autonomous ship. In *Computer Security.* Springer, 20–36.

[34] Athar Khodabakhsh, Sule Yildirim Yayilgan, Mohamed Abomhara, Maren Istad, and Nargis Hurzuk. 2020. Cyber-risk identification for a digital substation. In *Proceedings of the 15th International Conference on Availability, Reliability and Security.* 1–7.

[35] Carlos León. 2013. Authority centrality and hub centrality as metrics of systemic importance of financial market infrastructures. Available at *SSRN 2290271* (2013).

[36] Eric Luiijf, Albert Nieuwenhuijs, Marieke Klaver, Michel van Eeten, and Edite Cruz. 2008. Empirical findings on critical infrastructure dependencies in Europe. In *International Workshop on Critical Information Infrastructures Security.* Springer, 302–310.

[37] Georg Macher, Eric Armengaud, Eugen Brenner, and Christian Kreiner. 2016. Threat and risk assessment methodologies in the automotive domain. *Procedia Computer Science* 83 (2016), 1288–1294.

[38] Bharat B. Madan, Manoj Banik, and Doina Bein. 2019. Securing unmanned autonomous systems from cyber threats. *The Journal of Defense Modeling and Simulation* 16, 2 (2019), 119–136.

[39] Markus Mathes, Christoph Stoidner, Steffen Heinzl, and Bernd Freisleben. 2009. SOAP4PLC: Web services for programmable logic controllers. In *2009 17th Euromicro International Conference on Parallel, Distributed and Network-based Processing.* IEEE, 210–219.

[40] Ioan-Cosmin Mihai, Stefan Pruna, and Ionut-Daniel Barbu. 2014. Cyber kill chain analysis. *Int'l. J. Info. Sec. & Cybercrime* 3 (2014), 37.

[41] MITRE. 2020 (accessed December 2, 2020). *Cyber Threat Intelligence Repository Expressed in Stix 2.0.* https://github.com/mitre/cti.

[42] MITRE. 2020 (accessed December 8, 2020). *Defacement Technique.* https://attack.mitre.org/techniques/T1491/.

[43] MITRE. 2020 (accessed December 8, 2020). *Resource Hijacking.* https://attack.mitre.org/techniques/T1496/.

[44] Jean-Philippe Monteuuis, Aymen Boudguiga, Jun Zhang, Houda Labiod, Alain Servel, and Pascal Urien. 2018. Sara: Security automotive risk analysis method. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security.* 3–14.

[45] Thomas L. Nielsen, Jens Abildskov, Peter M. Harper, Irene Papaeconomou, and Rafiqul Gani. 2001. The CAPEC database. *Journal of Chemical & Engineering Data* 46, 5 (2001), 1041–1044.

[46] NTNU Autoferry. 2018. Autoferry - Autonomous all-electric passenger ferries for urban water transport. https://www.ntnu.edu/autoferry.

[47] Emmanuel Olaniyi. 2020 (accessed December 8, 2020). *Ransomware and Routers - Spectranet and Smile Ransomware Hit*. https://www.cybersecfill.com/ransomware-and-spectranet/.

[48] Charlie Osborne. 2020 (accessed December 2, 2020). *Code Execution, Defense Evasion are Top Tactics used in Critical Attacks Against Corporate Endpoints*. https://bit.ly/zdnet-DefenseEvasion.

[49] Punnuluk Phaithoonbuathong, Radmehr Monfared, Thomas Kirkham, Robert Harrison, and Andrew West. 2010. Web services-based automation for the control and monitoring of production systems. *International Journal of Computer Integrated Manufacturing* 23, 2 (2010), 126–145.

[50] Paul Pols and Jan van den Berg. 2017. The Unified Kill Chain. *CSA Thesis, Hague* (2017), 1–104.

[51] Ron Ross, Michael McEvilley, and Janet Oren. 2016. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. Technical Report. National Institute of Standards and Technology.

[52] G. Sabaliauskaite and S. Adepu. 2017. Integrating six-step model with information flow diagrams for comprehensive analysis of cyber-physical system safety and security. *Proceedings of IEEE Int. Symposium on High Assurance Systems Engineering* (2017), 41–48. https://doi.org/10.1109/HASE.2017.25

[53] Tara Seals. [n.d.]. Researcher: Not Hard for a Hacker to Capsize a Ship at Sea. https://threatpost.com/hacker-capsize-ship-sea/142077/.

[54] Barry Sheehan, Finbarr Murphy, Martin Mullins, and Cian Ryan. 2019. Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A: Policy and Practice* 124 (2019), 523–536.

[55] A. Shostack. 2014. *Threat Modeling: Designing for Security*. Vol. Wiley Publishing.

[56] Shelley Smith. 2020 (accessed December 8, 2020). *Teen Hacker in Poland Plays Trains and Derails City Tram System*. https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/.

[57] George Stergiopoulos, Marianthi Theocharidou, Panayiotis Kotzanikolaou, and Dimitris Gritzalis. 2015. Using centrality measures in dependency risk graphs for efficient risk mitigation. In *International Conference on Critical Infrastructure Protection*. Springer, 299–314.

[58] Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas. 2018. Mitre ATT&CK: Design and Philosophy. *Technical Report* (2018).

[59] Kimberly Tam and Kevin Jones. 2018. Cyber-risk assessment for autonomous ships. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE, 1–8.

[60] Kimberly Tam and Kevin Jones. 2019. MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs* 18, 1 (2019), 129–163.

[61] Christoph A. Thieme, Chuanqi Guo, Ingrid B. Utne, and Stein Haugen. 2019. Preliminary hazard analysis of a small harbor passenger ferry–results, challenges and further work. In *Journal of Physics: Conference Series*, Vol. 1357. IOP Publishing, 012024.

[62] Douglas Brent West et al. 1996. *Introduction to Graph Theory*, Vol. 2. Prentice Hall Upper Saddle River, NJ.

[63] Davey Winder. 2019. U.S. Coast Guard Issues Alert After Ship Heading Into Port of New York Hit By Cyberattack. https://bit.ly/USShipAttack.

Received 17 February 2021; revised 23 June 2022; accepted 11 November 2022