IOP Conference Series: Materials Science and Engineering

PAPER • **OPEN ACCESS**

Impact of cyber risk on the safety of the MilliAmpere2 Autonomous Passenger Ship

Impact of cyber risk on the safety of the MilliAmpere2 Autonomous Passenger Ship

Ahmed Amro[1], Georgios Kavallieratos[1], Konstantinos Louzis[2] and Christoph A. Thieme[3]

[1]Department of Information Security and Communication Technology (IIK), University of Science and Technology (NTNU), Gjøvik, Norway
[2]Laboratory for Maritime Transport, School of Naval Architecture and Marine Engineering, National Technical University of Athens, Greece
[3]Department of Marine Technology (IMT), NTNU, Trondheim, Norway
E-mail: ahmed.amro@ntnu.no, georgios.kavallieratos@ntnu.no, klouzis@mail.ntua.gr, christoph.thieme@ntnu.no

Abstract. The digitalization of the maritime sector is continuously growing, leading to increased automation, such as, the development of autonomous vessels. The Autonomous Passenger Ship (APS) is a characteristic instantiation of this development, aiming to transport people on urban waterways. Although emerging technologies deployed in such APS aim to facilitate the functions and operations of the navigation and communication systems, various safety and security risks are inherent to the communication infrastructure due to their interconnectivity. The aim of this work is to study the safety and cyber security of the communication system of an APS, namely the MilliAmpere2 APS. The six step model (SSM) is utilized to facilitate the joint analysis. The application of the SSM enables, among others, the capturing of relationships between cyber attacks and component failures, the assessment of safety and cyber security countermeasures, as well as, the synergies between them. It has been found that most countermeasures in both categories are reinforcing or are conditionally dependent on each other, while few antagonize each another. These findings will allow for improved design and implementation of integrated safety and security management solutions.

1. Introduction

The emergence of the contemporary and interconnected Cyber Physical Systems (CPSs) in the maritime domain and particularly in the autonomous vessels infrastructure, such as, the Autonomous Passenger Ship (APS), is rapid and continuous. To this end, the safety and security analysis of such systems is needed to ensure the vessel's normal and safe operations. Safety and security are interrelated concepts that may face both commonalities and differences in the analysis process since the former is concerned with accidental events while the latter mainly consider malicious actions taken by adversaries [1]. Particularly, security is concerned with the risks originating from the environment impacting the system and typically addresses malicious risks. Whereas safety deals with risks arising from the system that may affect the environment and addresses purely accidental risks. Safety analysis aims to reduce the risks related to systems, humans, and the environment [2] to an acceptable level.

Security analysis aims to minimize the risk related to confidentiality, integrity, and availability of the operational and functional requirements and therefore the data, information, and services of the system [2]. An extended security analysis may also consider the properties of possession or control, authenticity, utility, and non-repudiation. Hazards can be defined as conditions or states that may cause harm [3]. The risk associated with the hazards is a measure of uncertainty with respect to outcomes and may be described through risk sources, events and their consequences [4]. From a security point of view, vulnerabilities are system or software flaws that could threaten the system. Vulnerabilities could be also considered as system weaknesses [3].

The aim of this work is to identify weaknesses related to safety and security of a communication architecture proposed for safe and secure navigation for an APS [5] in order to remove them or reduce the risk associated with them. We apply the Six Step Model (SSM) to analyse security and safety risks and study the implications that security poses to safety. Particularly, leveraging the multidimensional matrices provided in the SSM, the functions, structure, failures, safety countermeasures, cyber attacks, and security countermeasures are identified for the communication, navigation and control systems of the APS. Although various approaches exist in the literature for security and safety co-analysis, the SSM has been chosen as the most appropriate for the case of the APS, due to its holistic approach to assess interdependencies. The complexity of the communication systems and the novel technology used in the communication infrastructure can be appropriately studied by the graphical models of the SSM. Further, the SSM facilitates the collaboration of both safety and security experts towards a more comprehensive safety and security analysis. The SSM and its application to the MilliAmper2 is described in detail in Section 4. The methods being employed in this article and previous works have been carried out as initial steps of a risk management process that is part of the Autoferry project [6]. The risk management process is aligned with the guidelines proposed by the International Maritime Organization (IMO) regarding the inclusion of cyber risk management within the Safety Management Systems (SMS) [7].

2. Related Work

Many safety and security methods that have been developed, do not directly consider each other. However, the combination of security and safety analysis is expected to result in identifying synergies regarding interactions, events and conflicting countermeasures. Various works in the literature examined the interrelation between safety and cyber security [2, 8]. Particularly, Lisova et al. [8] conducted a systematic literature review for safety and security co-analysis and thirty- three approaches have been identified. Further, Kavallieratos et al. in [2] conducted a survey in co-engineering approaches for safety and cyber security in cyber physical systems. Various systematic approaches have been proposed in the literature to analyse safety and security. The System-Theoretic Process Analysis (STPA), is developed to facilitate the safety analysis of complex systems considering the control structure of the targeted systems. The STPA is extended to accommodate security considerations, called STPA-Sec [9]. Further, SafeSec Tropos [10] is a co-engineering methodology for safety and security requirements elicitation in CPSs based on STPA and the Secure Tropos methods from safety and security domain respectively.

Safety related cyber attacks for autonomous inland ships are identified and assessed by Bolbot et al. [11]. In particular, by leveraging from a Cyber preliminary hazard analysis (PHA) method and existing systems vulnerabilities, potential cyber attacks that may compromise the vessel's safety along with a set of general countermeasures are examined. Further, Baˇckalov [12] studied the safety of autonomous inland vessels. Namely, the key characteristics of the autonomous inland vessels are analyzed considering the corresponding legislation and standards related to the safety of sea-going ships and inland vessels. Kavallieratos et al. [10] analyzed the safety and security of a cyber-enabled ship that could be either autonomous or remotely controlled. By the application of the SafeSec Tropos method, they identified the necessary security and safety requirements for such vessels.

3. Background

This section summarizes the background on the MilliAmpere2 passenger ferry, an instantiation of an APS which is under development as part of the Autoferry project [6].

3.1 System description and context of operation

The MilliAmpere2 is designed to carry up to 12 passengers over the harbor channel in Trondheim, Norway. The APS is characterized by a high degree of autonomy where the navigational and operational requirements are fulfilled by the APS. A supervisor in a land-based control centre (during the first year located on site) is responsible for actions needed in case of emergencies. Autonomous functions include navigation, docking, passenger registration, charging. Therefore, the communication of navigational and status data to the land-based control centre is vital [6].

3.2 Communication architecture

The communication architecture of the APS enables the communication with the environment through a heterogeneous group of different technologies. There are six main communication gateways in the APS. Particularly, two IP based gateways aim to establish ship-to-shore communication links with the RCC by leveraging several implementation solutions such as mobile communication (4G/LTE/5G) and Wireless Local Area Networks (WLAN) technologies. The third gateway is intended for ship-to-ship communication to enable the vessels in the area to communicate with the APS. Automatic Identification System (AIS) is proposed for the implementation of this module. The fourth gateway is intended to carry emergency communications for the control and navigation of the APS in case of lost communication with the Remote Control Center (RCC) while the fifth and sixth gateways are utilized to receive signals for real time kinematic (RTK) and global navigation satellite system (GNSS).

The internal network architecture of the APS is designed to include redundant communication paths, segregated sub-network, and secure communication. A centralized monitoring and controlling group of servers called the Autonomous Ship Controller (ASC) is interfaced with two network traffic Core and Distribution tiers (C/D), each consisting of main and backup switches with IP routing capabilities. The former tier (C/D A) connects the external gateways with the servers in the ASC, while the latter (C/D B) connects the secondary (i.e., backup) servers in the ASC with the internally segregated sub-networks. Moreover, a centralized component named the connectivity manager is responsible for performing network management functions by configuring and monitoring the network devices in addition to additional functions related to security. The detailed communication architecture along with the corresponding functions are described by Amro et al. in [5].

3.3 Navigation and Machinery Systems

The navigation system is comprised of components able to collect environmental data, establish situational awareness based on the sensing data, and determine safe navigation routes. The navigation system components are arrays of sensors of different types (EO cameras, video cameras, Lidars, and Radars), in addition to RTK GNSS. All these components send their data through the ship internal network to the Autonomous Navigation System (ANS) that hosts the logic to perform autonomous navigation functions, as well, as support remote navigation by the RCC. Moreover, a machinery system implements maneuvers according to the determined route from the ANS. The machinery system consists of a Dynamic Positioning (DP) system, and thrusters, interfaced through Input/Output (I/O) cards. The machinery system is controlled by an Autonomous Engine Monitoring and Control (AEMC) system which host the logic to monitor engine data and determine the appropriate control parameters. Both the ANS and AEMC are hosted in the ASC servers zone.

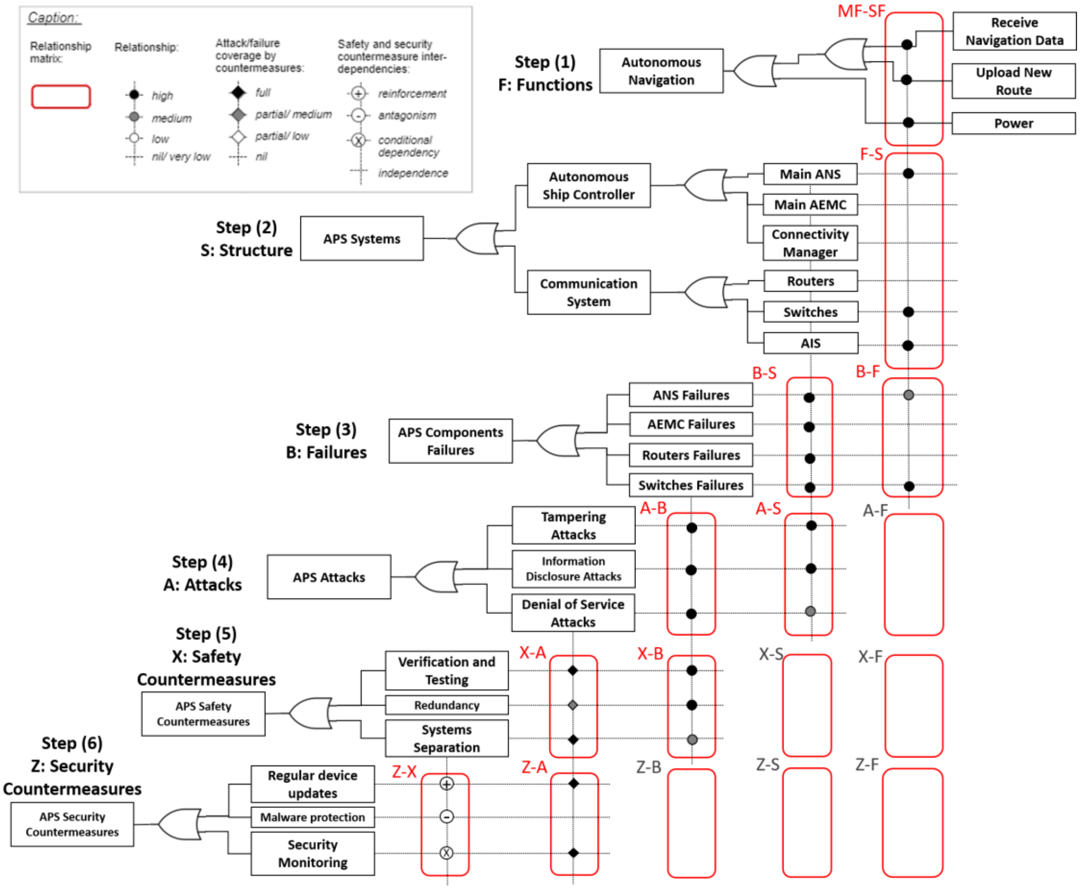

Figure 1. Overview of the applied Six Step Model steps (Adapted from [15])

3.4 Preliminary Hazard Analysis

A PHA for the MilliAmpere2 is presented in [13]. A PHA is a structured hazard identification method, which is guided through keywords that represent possible hazards and their sources [3]. The PHA for the APS was conducted in two sessions with the participation of several experts from several relevant domains. This analysis builds the foundation for identification of safety related issues in this article.

4. The six-step model

This Section summarizes the adopted six-step model (SSM) for the safety and security analysis of the communication, navigation and control systems of the APS. The SSM was proposed by Sabaliauskaite et al. [14] to analyze, both, safety and security aspects of CPS. Furthermore, the applicability of the SSM to and security issues of an autonomous vehicle is examined in [15]. An overview of the SSM that is followed in this work, is depicted in Figure 1. The six steps of the SSM model were performed disregarding some matrices, since their analysis was not considered relevant for the scope of the target analysis.

4.1 Step 1: Functions

The first step of the SSM describes the system's functions. Main and supporting functions are differentiated and their relationships are established. The main functions are cross referenced with the supporting, secondary functions of the system in the MF-SF matrix (Main-functions, Supporting Functions). The matrix provides the basis for further system analysis. Four types of relationships are distinguished, high, medium, low, very low/ none. The relationships description is adopted from [16]. High relationships characterize high dependency of the main function on the supporting function for proper operation. Medium means that the main functions might be dependent on the supporting functions to operate properly in some operational modes while low relationship means that the main functions are rarely dependent on the supporting functions. Finally, nil/ very low relationships mean that no dependencies on the supporting functions are identified.

4.2 Step 2: Structure

The second step identifies the relationships between the APS components and the APS functions in the S-F matrix (structure: functions). The APS components are identified by decomposing the systems to the appropriate level of analysis. This includes main and supporting systems. This analysis is necessary to determine the relationships between function failures and physical component failures in step 3 (Section 4.3). The rating scheme includes high, medium, low, and nil/ very low levels. A high relationship indicates that the component is highly important for the realization of the function under analysis. A medium relationship indicates that the component might be needed to realize the function in certain operational modes. A low relationship indicates that the component might be needed to realize the function in very specific and rare cases. Nil/ very low is assigned to pairs that have no relationship with each other.

The components are prioritized for threat modeling in Step 4 (Section 4.4) according to their highest effect on the main system functions, considering the relationships studied in Step 2. The scores of the components under analysis are calculated for all the APS's components, taking into account the assigned relationships of each component with the specified system functions following Equation 1. The number of high relationships with systems functions is denoted as ”h”. Further, the number of medium and low relationships are denoted as ”m” and ”l” respectively. The components that gathered scores above the average are considered for analysis.

$$Score = 5h + 3m + l \qquad (1)$$

4.3 Step 3: Failures

The aim of the third step is twofold; firstly the system failures of main components are identified and secondly the failures' impact on the system's functions are determined. In this step, the B-S matrix (failure: structure) is created. In this matrix, component failures were identified and assessed from the available PHA report [13]. The failures were generalized and the results from the report were used as input to rate the dependencies. The failures are assessed in relation to the system's functions in order to assess the severity of failures on the system's function execution. The information is recorded in the B-F matrix (failures: functions). The rating scheme used for the B-S and B-F matrices included high, medium, low, and nil/very low levels. These indicate the strength of the impact of a failure to either the operation of a component or the implementation of a system function. For instance, a high relationship between a failure and a component means that the latter will most probably not be able to operate, whereas the same level between a failure and a function means that the latter will be potentially severely impaired.

By leveraging the PHA [13] the Function Failure Impact Factor (FFIF) is determined. The FFIF represents the expected impact on the execution of a function that is weighted by potential consequences of the failures. The loss of each function was associated with potential consequence categories that included the following in ascending order of severity: loss of operational/ performance data, loss of remote monitoring and control, and loss of control/ drifting/ grounding/ collision/ injuries/ fatalities. Having calculated the failures' relationships with the system functions (Relationshipi,j (Failurei, Functionj)), the overall impact score for each component failure (i) is calculated using equation 2 where N represents the total number of system functions. Failures with Impact score above the average have been forwarded for analysis in Step 4 (Section 4.4).

$$Impact_i = \sum_{j=1}^{N} Relationship_{i,j} * FFIF_j \qquad (2)$$

4.4 Step 4: Attacks

The assessment of cyber attacks is performed in Step 4 by utilizing the STRIDE method. STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege [17]. The method enables the analysis of complex systems and environments similar to the APS [18, 19].

Potential security threats along with the corresponding attack scenarios are identified and analyzed for the APS's components considering STRIDE. The security analysis takes into account external and internal attackers. The former are able to conduct the attack remotely while the latter perform the attack by infecting system components. Further, malicious passengers are considered as potential adversaries that may attack the APS. The following relationship matrices are generated; matrix A-B (attacks: failures), and matrix A-S (attacks: structure).

The A-S matrix is analyzed through the application of STRIDE. The attacks considered in matrix A-B are a subset of the attacks that are analyzed in the A-S matrix. Using the analysis performed in step 2 (Section 4.2) only attacks against components with most effect on the system's functions have been considered. Therefore, the attacks that are characterized by the highest impact on the main system functions are identified. Further, the A-B matrix includes attack scenarios that violate the security objectives of authenticity, integrity, non-repudiation, confidentiality, availability, and authorization. These objectives aim to ensure the security of the components in the maritime environment [10] and therefore of the APS's infrastructure. The most critical security objectives related to the functions of the APS are integrity, confidentiality, and availability. These ensure the security and reliability of the communication systems.

The A-B matrix reflects the relationships between the prioritized attacks and prioritized failures. The relationships are categorized as high, medium, low, or nil/ very low. A high relationship means that the attack is expected to directly lead to the failure with high possibility. A medium relationship means that the attack triggers the failure with moderate possibility. A low relationship means that the attack may lead to the failure with low probability, while a nil/ very low relationship is considered if no connection between between the attack/ failure pair can be identified.

4.5 Step 5: Safety Countermeasures

Safety countermeasures are identified considering the failures and the attacks in the fifth step. The reasoning for identifying the potential safety countermeasures is based on a high- level consideration for the system design and development process, and strategies to mitigate potential risks. The safety countermeasures include measures that need to be designed into the system (e.g., integrity checks, error handling), measures during commissioning (i.e., testing and verification), and operational measures (e.g., maintenance policies for hardware and software components, minimum risk condition). The matrices assessed in this step are matrix X-B (safety countermeasures: failures), and matrix X-A (Safety countermeasures: Attacks). The X-A matrix enables the identification of synergies between safety and security issues. For X-B and X-A the assessment considered four distinct degrees; full, partial medium, partial low, and nil. A full degree removes the failure or attack and its associated consequences to a large degree or completely. A safety measure assessed as partial medium eliminates the consequences or reduce the consequences to a large degree. A partial low assessment implies conversely a minor reduction in the frequency of occurrence or a minor reduction in the expected consequences. Nil degree describes that no improvement from this measure is expected, or that it has been already implemented.

4.6 Step 6: Security Countermeasures

In this step, the relationship matrices being analyzed are matrix Z-X (Security countermeasures: safety countermeasures) and matrix Z-A (security countermeasures: attacks). The remaining matrices, Z-B (security countermeasures: failures), Z-S (security countermeasures: structure), and Z-F (security countermeasures: functions) were not analyzed. The identification of security countermeasures is needed for the analysis in this step. The considered countermeasures are based on previously established cyber security requirements for the communication architecture [20].

The Z-A matrix described the effectiveness of a countermeasure in mitigating cyber attacks. To this end, three relationship categories; 1) the countermeasure leads to fully mitigating the attack (f), 2) partial mitigation(p), 3) nil (no mitigation or not relevant). By applying equation 3 a score is calculated for each countermeasure to indicate the effectiveness against the attacks based on the analysed relationship.

$$Score = 5f + p \tag{3}$$

The Z-X matrix captures the dependencies between safety and security countermeasures, which is crucial to the study of the synergies between these different sets of countermeasures. In particular, the effects that the security countermeasures may have on the safety countermeasures are represented through four types of relationship as defined in [14]. These are: 1) Reinforcement,
2) Antagonism, 3) Conditional dependency, and 4) Independent.

5. Results

5.1 Step 1: Functional analysis

The proposed communication architecture enables the MilliAmpere2 to perform several functions related to navigation, control, communication, and safety. Figure 2 shows an overview of the functions supported by the communication architecture and reflects their relations with the APS components previously discussed in Section 3 as well as among themselves. These relations highly influenced the analysis in Step 1 and 2 in the SSM model. The main navigation functions provide the situational awareness of the APS for the determination of safe routes. The ”Engine Monitoring and Control” functions describe the monitoring and control of the APS’s thrusters. Furthermore, autonomous functions are performed by the APS. Remote functions are carried out by the RCC, and emergency functions are executed by the Emergency Control Team (ECT). Further functions are needed to initiate emergency signals by passengers referred to as ”Passenger Safety” functions. They are needed to indicate the occurrence of safety-critical events (e.g., passenger falling overboard). Therefore, these functions will only be found in APS or manned autonomous ships, and not in unmanned autonomous ships, since they will not be required. For the purpose of this paper, only emergency functions with respect to passenger communication with the RCC and the emergency services are considered, due to the focus on the communication system. The main communication functions are categorized considering their individual role. The ”Ship-to-shore communication” function provides the required connectivity between the ship and the RCC. The ”Internal communication” functions provide the needed connectivity between the different components onboard the ship. The ”Emergency communication” functions provide the needed connectivity with the ECT. These functions depend on several supporting functions such as power, security, and network system management (NSM).

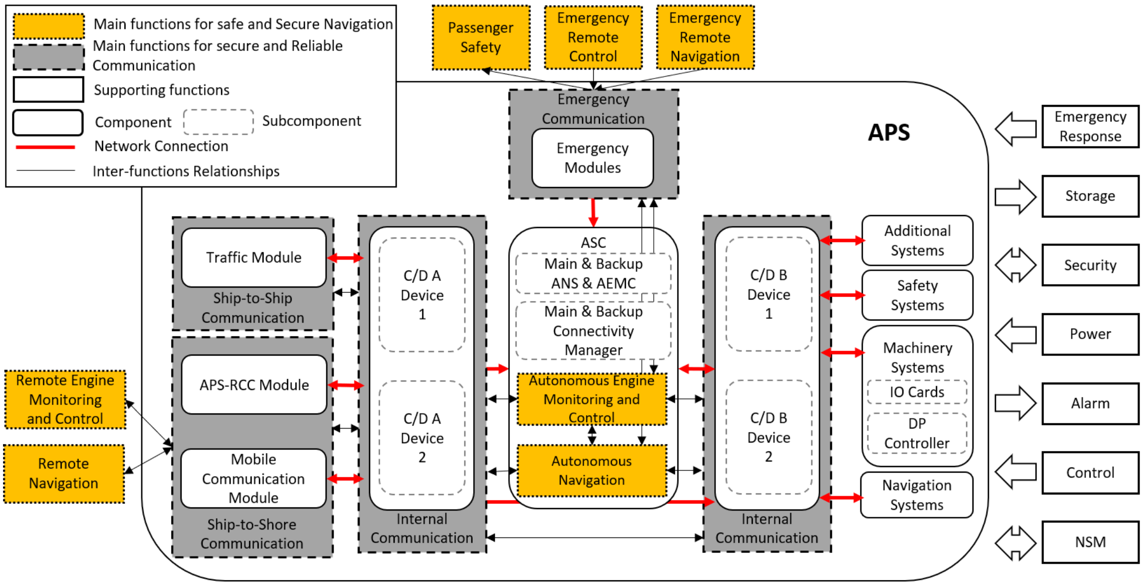

Figure 2. Overview of the relationships between the communication architecture functions and structure (Adapted from [5])

5.2 Step 2: Component assessment

The aforementioned scoring scheme in Step 4.2 was used to identify the components with the highest influence on the system. The components and the number of identified high, medium and low relationships with system functions are shown in Table 1. It can be observed that the components related to communication related have a relatively higher effect over system functions which is logical since they are responsible for the information exchange needed for most functions.

Table 1. Relationships assessment of the components with the most effect on the main system functions

Component	Relationships		
	High	Medium	Low
C/D A Device 1 and 2	30	1	10
Mobile Communication Module	23	1	13
APS-RCC Module	23	1	13
Connectivity Manager	24	1	0
DP controller	9	19	1
C/D B Device 1 and 2	16	3	10
Backup Connectivity Manager	18	1	0
IO cards	10	14	0
Main ANS	15	4	1
Backup ANS	11	4	1
Emergency Module 1	11	1	10

5.3 Step 3: Assessment of failures

As an outcome of step 3, the failures having highest impact according to equation 2 were identified. The failures associated with the connectivity manager are found to have the highest impact score, with C/D part A devices next, and the DP system after them. We argue that the results are plausible since the failures with highest scores would indeed affect the entire APS. For instance, failures in the connectivity manager and network devices would lead to disruption in the information flow within the APS which would lead to total loss of certain functionalities. Additionally, the AEMC, DP, together with the I/O cards and the thrusters highly affect the APS, in case of a component failure Some may even lead to a blackout affecting the whole APS.

5.4 Step 4: Assessment of attacks

Through the application of the STRIDE methodology several attack scenarios were identified as well as their relevance to the system components. Those attacks were analyzed against the failures discussed in Section 5.3. The results reflect which attacks could cause additional failures, as well as, which failures increase the vulnerability of the system to cyber attacks. It was found that attacks against both, the main and backup, connectivity manager components could cause failures with highest impact, followed by the C/D switches. Additionally, it was observed that denial of service attacks cause higher impact failures than others, followed by tampering, while information disclosure attacks have much lower effect on failures. Moreover, susceptibility to cyber attacks is mostly enhanced by failures in the connectivity manager, ANS, and AEMC components.

5.5 Step 5: Assessment of safety measures

Eleven safety countermeasures were identified. The countermeasures are summarized and described in Table 2. Safety countermeasures were identified from the PHA [13] and common risk mitigation strategies, such as laid out in [3]. For the purpose and scope of the article, the safety countermeasures are generic in nature and the specific implementation for the components needs to be defined and described in the further design process.

Table 2. Identified safety countermeasures

ID	Mitigation measure	Description
CSaf1	Choice of communication protocol	Selecting protocols and bus systems that are robust and suitable for the purpose of communication between the components.
CSaf2	Verification and testing	The component should be tested and its function and behavior verified during different phases of the development process.
CSaf3	Monitoring and trouble shooting through shore operator	The shore operator monitors the system behavior and engages in problem trouble shooting if a problem with the ferry occurs. The ferry design needs to accommodate these trouble shooting abilities.
CSaf4	Component redundancy	A second similar component is introduced in the system design to take over functionalities in case of the failure occurring.
CSaf5	Separate hardware components	The component has its own dedicated computing hardware to run on.
CSaf6	Go to a safe state	A safe state is defined for a failure and will thereby mitigate the consequences of this failure. The ferry needs to be designed such that the safe state can be reached in the failure condition.
CSaf7	Self and status tests of the component	The component must be able to test for correct operation and functioning.
CSaf8	Choice of computing hardware	Sufficient powerful computing hardware needs to be chosen to fulfil the components purpose even under high load conditions.
CSaf9	Cross validation of data inputs for sensor data	The components using sensor data is crosschecked with other data for plausibility. Implausible and invalid data should be rejected.
CSaf10	Hardware maintenance and cleaning policy	A maintenance plan defining preventive and corrective maintenance, including cleaning for the hardware components.
CSaf11	Software maintenance policy	A maintenance policy for the software describing the policy for bug fixing and updating software, and associated tasks.

The assessment of the effectiveness of each safety countermeasure is based on its assumed degree of elimination or mitigation of a failure. However, due to the generic nature of these, their impact cannot be definitively assessed since the implementation of the measure for each component was not specified in detail. For the same reason, it cannot be assumed that all failures are removed from the system. The safety countermeasures address all the failures, as well as, most of the attack scenarios. Only hardware maintenance is not addressing any of the cyber attacks. Most failures and attacks can be addressed through testing and verification efforts (CSaf2) and Self and status tests (CSaf7). Monitoring through an operator (CSaf3) can assist to some degree in identifying safety and security related issues. However, adequate procedures need to be established in order to troubleshoot efficiently and react appropriately. Cross validation of data (CSaf9) and a hardware maintenance policy (CSaf10) is mainly relevant for the sensors and the actuators.

5.6 Step 6: Assessment of security measures

The analysis performed in the Z-A matrix is utilized to assess the countermeasures coverage of the identified attacks. By using equation 3, as depicted in Table 3 various countermeasures are found to mitigate either fully or partially several attacks, such as the application of secure network protocols, and the preparation of incident response plans. The analysis facilitates the prioritization of the countermeasures implementation. It can be observed that the implementation on secure network protocols such as Transport Layer Security (TLS) and Virtual Private Network (VPN) would be most effective for attack mitigation, followed by well planned incident response procedures, and security monitoring. Moreover, it was observed that cyber security training for operators is not of high priority which is logical due to the reduced human involvement in the direct operation of the APS. For the operation of the RCC, the cyber security training may still be of importance.

Table 3. Outcome of the assessment of cyber security countermeasures

ID		Att a cks mitigati on		
	Countermeasures	Fully	Partially	None
CSec1	Secure network protocols	14	2	2
CSec2	Incident response plans	7	10	1
CSec3	Security monitoring for detecting malicious and abnormal incidents	8	8	2
CSec4	User access management system	7	7	4
CSec5	Regular device updates	3	9	6
CSec6	Detailed map of IT and network equipment and software	3	8	7
CSec7	Cyber security management framework	2	9	7
CSec8	Regular software security analysis (penetration testing)	1	8	9
CSec9	Backup facilities	4	2	12
CSec10	Periodic inventory of user accounts and their associated privileges	2	5	11
CSec11	Malware protection	0	8	10
CSec12	Cyber security training	1	6	11

In this work the impact of security risk on safety is examined and analyzed. To this end, Table 4 depicts the relationship between the safety and security countermeasures. By leveraging the information depicted in Table 4 most of the security countermeasures are independent (60 relationships) while 40 relationships were assessed as enhancing the existing safety countermeasures. For instance, the cyber security management framework facilitates and strengthens the corresponding safety countermeasures. Additionally, twenty seven countermeasure relationships are characterized as conditionally dependent. Only five relationships between safety and security countermeasures are characterized as antagonism. Namely, the need to separate system components (CSaf5) and specify certain choices of hardware (CSaf8) for safety countermeasures may complicate the implementation of suitable security monitoring solutions (CSec3).

6. Discussion

The SSM analysis identifies the relationships between components and functions and provide a holistic view for the system under analysis. Therefore, the interplay of safety and security is examined in detail, considering the different viewpoints that are provided by the corresponding matrices. Overall the SSM provides an appropriate analysis of a system under development, in the initial steps of the design process where the functional and operational requirements are not defined in detail. Our analysis shows that the SSM provide results that may help to prioritize identified safety and security issues for more detailed analysis.

The analysis of an abstract system architecture is facilitated by leveraging the SSM. The method extracts rigorous and valid results in high organizational and operational levels. However, the SSM scales badly with increasing system complexity, due to the state-space growth in the SSM matrices. The SSM would benefit from additional guidance on how to represent and model the system and the dependencies among its components in a standardized way, similarly to how the STPA defines the safety control structure as a way to model the system. This would help in better determining, for example, common cause failures and assessing the impact of failures on the system structure and functionality. Additionally, further guidance on ranking the relationships described in each SSM matrix and steps for the failure and attack prioritization are needed. This may reduce the effect of subjective expert assessments that may not be justified in a transparent and reproducible manner.

Table 4. Relationships between safety and security countermeasures

Safety	Security											
	CSec7	CSec6	CSec10	CSec4	CSec5	CSec11	CSec1	CSec12	CSec8	CSec3	CSec2	CSec9
CSaf1	●	◑	○	◑	○	○	●	●	○	●	○	◑
CSaf2	●	●	◑	○	○	○	◑	○	●	○	○	○
CSaf3	●	●	◑	◑	●	●	●	●	●	●	●	●
CSaf4	●	○	○	○	○	○	○	○	○	○	◑	●
CSaf5	●	◑	○	◑	🔴	○	○	●	◑	🔴	○	○
CSaf6	●	◑	○	◑	○	○	◑	○	○	●	●	○
CSaf7	●	○	○	◑	◑	🔴	○	◑	◑	◑	○	○
CSaf8	●	○	○	○	◑	○	◑	○	○	🔴	🔴	●
CSaf9	●	●	○	○	◑	●	○	○	●	●	●	◑
CSaf10	◑	○	○	○	○	○	○	○	○	○	◑	○
CSaf11	●	○	●	●	●	○	○	●	●	●	◑	◑

Legend: ● Reinforcement, 🔴 Antagonism, ◑ Conditional dependency ○ Independent

Common cause failures, emerging system behavior, and multiple system failures are hard to include in the assessment. This may reduce the ability to identify interdependencies of failures. The identification of safety countermeasures is performed on a high level and detailed risk countermeasures could be developed early in the design phase.Applying the SSM process later, in the detailed design phases, the identified design changes and risk mitigation measures may come with a high cost. Guidelines on how safety and security measures may be identified with the SSM are also desirable.

7. Conclusion

In this work, a joint safety and security analysis of the MilliAmpere2 Autonomous Passenger Ship (APS) has been conducted. The Six-Step-Model (SSM) was applied to capture the different analysis viewpoints, namely, APS functions, structure, failures, cyber attacks, and safety and cyber security countermeasures. The main goal of the analysis was to infer the effect of cyber threats on safety, as well as, the interrelations between safety and security countermeasures, for design and implementation of integrated safety and security countermeasures.

Several conclusions can be drawn from the application of the SSM. It was found that the connectivity manager has most effect on the system functions. It could cause most failures, and is among the most susceptible to cyber threats. Secure network protocols, incident response plans and security monitoring were identified as the most important security countermeasures to be implemented. Moreover, safety and cyber security countermeasures have been found to be mostly compatible. Some measures are contradictory, which is very helpful to know during the design and implementation of both. Further work is needed to establish a security architecture for the APS that considers interrelations with safety. The outcome of this paper is expected to influence the design and implementation of security countermeasures to be adopted in the target security architecture as well as the undergoing design and implementation of the connectivity manager to mitigate it's discovered threats.

Acknowledgements
Thieme acknowledges the support by the Norwegian Research Council through the UNLOCK project, project number 274441.

References

[1] L. Pi`etre-Cambac´ed`es and C. Chaudet. The sema referential framework: Avoiding ambiguities in the terms “security” and “safety”. Int. Journal of Critical Infrastructure Protection, 3(2):55–66, 2010.

[2] G. Kavallieratos, S. Katsikas, and V. Gkioulos. Cybersecurity and safety co-engineering of cyberphysical systems—a comprehensive survey. Future Internet, 12(4):65, 2020.

[3] M. Rausand. Risk Assessment: Theory, Methods, and Applications. John Wiley & Sons, Hoboken, New Jersey, USA, 1st ed. edition, 2013.

[4] T. Aven and O. Renn. On risk defined as an event where the outcome is uncertain. Journal of Risk Research, 12(1):1–11, 2009.

[5] A. Amro, V. Gkioulos, and S. Katsikas. Communications architecture for autonomous passenger ship. Submitted for review to Journal of Risk and Reliability (JRR).

[6] NTNU Autoferry. Autoferry - Autonomous all-electric passenger ferries for urban water transport, 2018.

[7] The Maritime Safety Committee. International maritime organization (imo) (2017) guidelines on maritime cyber risk management. http://bit.ly/IMORiskManagement.

[8] E. Lisova, I. Sˇljivo, and A. Cˇauˇsevi´c. Safety and security co-analyses: A systematic literature review. IEEE

[9] Systems Journal, 13(3):2189–2200, 2018.

[10] W. Young and N. Leveson. Systems thinking for safety and security. In Proceedings of the 29th Annual Computer Security Applications Conference, pages 1–8, 2013.

[11] G. Kavallieratos, S. Katsikas, and V. Gkioulos. Safesec tropos: Joint security and safety requirements elicitation. Computer Standards & Interfaces, 70:103429, 2020.

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

[13] I. Baˇckalov. Safety of autonomous inland vessels: an analysis of regulatory barriers in the present technical standards in europe. Safety science, 128:104763, 2020.

[14] C. A. Thieme, C. Guo, I. B. Utne, and S. Haugen. Preliminary hazard analysis of a small harbor passenger ferry-results, challenges and further work, 2019.

[15] G. Sabaliauskaite, S. Adepu, and A. Mathur. A six-step model for safety and security analysis of cyber- physical systems. In Int. Conference on Critical Information Infrastructures Security, pages 189–200. Springer, 2016.

[16] G. Sabaliauskaite and Jin Cui. Integrating autonomous vehicle safety and security. In Proceedings of the 2nd Int. Conference on Cyber-Technologies and Cyber-Systems (CYBER 2017), Barcelona, Spain, pages 12–16, 2017.

[17] G. Sabaliauskaite and J. Cui. Integrating Autonomous Vehicle Safety and Security. CYBER 2017 : The Second Int. Conference on Cyber-Technologies and Cyber-Systems, (level 0):75–81, 2017.

[18] A. Shostack. Threat Modeling: Designing for Security, volume Wiley Publishing. 2014.

[19] G. Kavallieratos, S. Katsikas, and V. Gkioulos. Cyber-attacks against the autonomous ship. In Computer Security, pages 20–36. Springer, 2018.

[20] G. Kavallieratos, V. Gkioulos, and S. K Katsikas. Threat analysis in dynamic environments: The case of the smart home. In 15th Int. Conference on Distributed Computing in Sensor Systems (DCOSS), pages 234–240. IEEE, 2019.

[21] A. Amro, V. Gkioulos, and S. Katsikas. Connect and protect: Requirements for maritime autonomous surface ship in urban passenger transportation. In Computer Security, pages 69–85. Springer, 2019.