Bolbot, Victor; Basnet, Sunil; Zhao, Hanning; Valdez Banda, Osiris; Silverajan, Bilhanan

Investigating a novel approach for cybersecurity risk analysis with application to remote pilotage operations

Published in:
Proceedings of the MARESEC 2022

DOI:
10.5281/zenodo.7143998

Published: 04/10/2022

Document Version
Publisher's PDF, also known as Version of record

Investigating a novel approach for cybersecurity risk analysis with application to remote pilotage operations

Victor Bolbot*, Sunil Basnet*, Hanning Zhao †, Osiris Valdez Banda*, Bilhanan Silverajan†
*Aalto University, Espoo, Finland
{victor.bolbot@aalto.fi
†Tampere University, Tampere, Finland
{hanning.zhao@tuni.fi

***Abstract*—Remote pilotage constitutes a novel type of service aiming at reduction of operational costs and safety improvement. However, the increased inter-connectivity of remote pilotage renders it vulnerable to cyberattacks. In this paper, we investigate a novel approach to cybersecurity risk analysis, which integrates System-Theoretic Process Analysis method, Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) method, SysML, MITRE ATT&CK, and ranking method. To integrate the methods, we apply a series of relevant adjustments and amendments. As a result, we are able to investigate multiple facets of cyber risk, identify the most critical issues and propose relevant risk control measures. For the remote pilotage, the most important STRIDE attacks involve Spoofing, Tampering, and Denial of Service attacks, whilst the most critical MITRE ATT&CK attack techniques are the use of default credentials, the exploitation of public-facing applications, and replication through removable media, if general hacker profile is considered for the attack.**

***Index Terms*—Remote pilotage; Cyber-attacks; System-Theoretic Process Analysis; STRIDE; MITRE ATT&CK; SysML; CYRA-MS; Risk analysis**

I. Introduction

We live in an age, when novel systems are being developed and novel services are being offered, exploiting the advancements of the Information and Communication Technologies (ICT). An example of such service under development is the remote pilotage for ships [1]. It is expected that the remote pilotage will ease the navigation of ships in congested waters and reduce the costs, simultaneously guaranteeing accessibility to jobs associated with maritime for vulnerable groups [2], [3]. However, effective use of advancements in the ICT requires overcoming technological, regulatory, organizational, and societal challenges [4]. One of the important challenges is associated with cybersecurity aspects, as cyber-attacks can exploit vulnerabilities in the communication networks to get access or control over sensitive functions and information [5] or disturb safety-critical operations. Therefore, it is crucial to ensure that the novel systems and services are impenetrable to critical cyberattacks.

II. Related Work

A plethora of methods has been proposed to support the identification and risk assessment of cyberattacks. Some of the popular methods include Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privileges (STRIDE) [6], MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) [7] , Process for Attack Simulation and Threat Analysis [8], Attack Trees [9], and many others [10]. Several of the cybersecurity methods are based on safety analysis methods such as Failure Modes, Vulnerabilities, and Effects Analysis [11], Cyber Preliminary Hazard Analysis [10], CYRA-MS [5], Cyber Hazard and Operability study [10], allowing simultaneous identification and analysis of safety and cybersecurity-related problems.

The use of System-Theoretic Process Analysis (STPA) [12] for cybersecurity analysis has gained popularity in the last decade. The STPA as a method has been demonstrated to be supportive in the identification of hazards associated with software and organizational failures, but also of cybersecurity-related issues [13] [14]. STPA has also been applied in combination with other cybersecurity methods such as STRIDE [15], attack trees [16], formal models [17], diagrammatic representations of systems [18], Tropos method [19], as well as numerous safety methods such as Fault Trees [20], Bayesian Networks [21].

Multiple research studies have investigated the cybersecurity issues in remotely controlled ships [22], [23], [5], [24], but remote pilotage operations are different from remotely controlled operations since there is a crew present on the ship. Some of the research studies have dealt with the analysis of cybersecurity issues in remote pilotage by using MITRE ATT&CK [25], [26], [27], [28], [29]. However, these studies did not consider linking the results to STPA results and conducting a more detailed risk analysis. Also, none of the previous studies considered the use of SysML [30] to support the identification and analysis of cybersecurity scenarios in combination with STPA and MITRE ATT&CK. Furthermore, the ranking of identified attacks has not been included in the previous studies combining STPA with cybersecurity analysis.

III. Aim and Objectives

The aim of the present study is to implement risk analysis of the cybersecurity aspects in remote pilotage based on SysML,

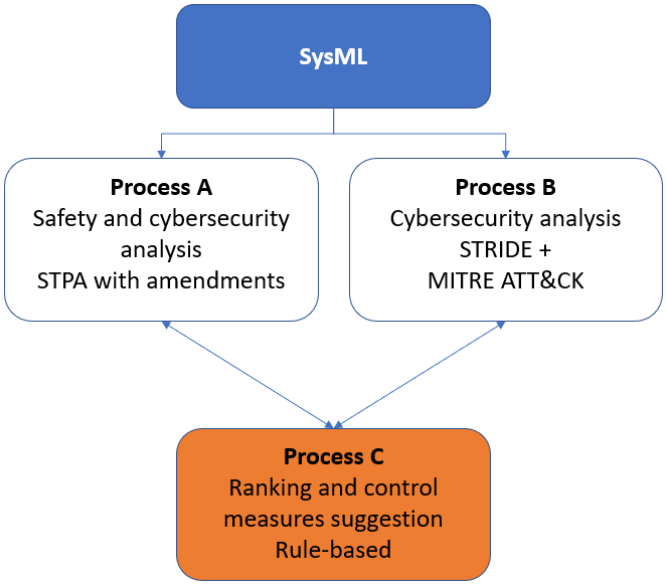

Figure 1. An overview of methodology followed in this study.

STPA, STRIDE and MITRE ATT&CK to identify the most critical cyber-attack scenarios in remote pilotage. The novelty of this research is as follows:

- Integrating STPA-Sec, STRIDE and MITRE ATT&CK for cybersecurity analysis
- Ranking of identified scenarios with STPA and MITRE ATT&CK
- Applying the developed methodology to remote pilotage operation to identify potential attacks.

IV. Methodology

The overview of the methodology followed in this study is shown in Figure 1.The methodology of the study follows the classical steps of the STPA but incorporates additional steps related to cybersecurity based on MITRE ATT&CK and STRIDE. These supplementary steps are applied after the initial STPA results have been generated by exploiting the SysML diagrams. This is necessary since STPA can support identification of control failures and has limited capacity for the identification of cybersecurity-related causes. STRIDE instead can support understanding where some high-level attacks can occur and MITRE ATT&CK can support identifying what type of techniques can be employed to achieve these attack types. The ranking is used to identify the critical scenarios, which require additional treatment or analysis. Based on the study results, some risk control measures are recommended.

A. System Modeling Language (SysML)

SysML is a visual modeling language supporting the specification, analysis, design, verification, and validation of complex systems[31]. The SysML diagrams provide detailed information of the system, such as component functions, interactions, sequence of events,and requirements[31]. In this study, SysML diagrams are used to support the STPA hazard analysis and STRIDE, as explained in next section.

B. STPA

STPA is a hazard analysis method based on the principles of the Systems-Theoretic Accident Model (STAMP), where losses are treated as an outcome of ineffective control rather than system failure [32]. In this study, the steps of STPA are extended for identifying the scenarios related to cybersecurity. The steps of STPA applied in this study are as follows[12]:

1) Defining the purpose of the analysis by identifying the losses, system-level hazards, and system constraints, also including cybersecurity-related events.
2) Modeling the hierarchical control structure of the system under assessment, which is composed of feedback and control loops between system components. In addition, we also depict the communication protocols to support the identification of vulnerabilities. The system components, controls and feedback are extracted from the SysML block definition diagrams and SysML activity diagrams.
3) Identifying Unsafe and Unsecured Control actions (UCAs) that could lead to a hazardous state due to inadequate control. As the SysML activity diagrams present the interactions of components and users to perform system activities (functions), these diagrams support the brainstorming session to identify the UCAs.
4) Identifying causal factors that can lead to each of the UCAs. These are more safety rather than security related as cybersecurity-related factors are identified by STRIDE and MITRE ATT&CK.

C. STRIDE and MITRE ATT&CK

STRIDE belongs to an extensively used method for the identification of potential high-level cyberattacks . It is based on the use of some keywords and data flow diagrams [6]. In our analysis, instead of using data flow diagrams, we consider using the updated STPA control structure and SysML diagrams to comprehend the information flow in the remote pilotage.

MITRE ATT&CK is a globally-accessible knowledge base of techniques and adversary tactics utilized in cyber-attacks and it is based on all real-world base observations [7]. It is commonly applied as a basis for developing specific threat models. By using MITRE ATT&CK, professionals can effectively prevent or defend their system from cyber threats and risks. The current matrix representing tactics and techniques is geared towards a wide range of software systems, including Windows, macOS, Linux, cloud, and mobile devices, etc.

In addition to offering Enterprise related attacks, MITRE ATT&CK has also been adapted to Industrial Control Systems (ICS) by shifting the focus of analyzing attack surfaces from IT systems to the Operational Technology (OT) environment [33]. Considering the cyber security challenges in OT technology, ATT&CK for ICS is abstracted to handle diverse industrial systems, it focuses more on function levels and asset

classes tied to services. The knowledge database provided in [33] also provides some safety control measures.

D. Ranking

The ranking is implemented to support more effective risk management. First, the identified unsafe/unsecure control actions are identified and ranked based on the severity of their most probable consequences. To that mean, the matrix of Table I from [34] is used. We also consider the accident statistics provided to us by the Finnish pilots for the ranking of the UCAs.

For ranking of MITRE ATT&CK techniques, the methodology presented in [5] is being used. This method uses some parameters, such as the attacker's technological level, system exposure, attack frequency, attacker motivation, the number of resources required for the attack and the presence of cyber security control barriers. In addition, the relevance of various MITRE ATT&CK techniques to the critical UCAs caused by specific STRIDE attacks is assessed with the support of the Table II, coupling the MITRE ATT&CK techniques with the STPA method results.

Then for the most critical MITRE ATT&CK techniques, the relevant control measures are being suggested to minimize the risk of cyberattacks. For that, the existing library of MITRE ATT&CK is extensively used.

Table I
DESCRIPTION OF SEVERITY FOR THE UCAS

Ranking (SI)	Safety	Env*	Financial	Rep*
5-Catastrophic	Multiple fatalities	Major air/oil pollution	$ 80 mil	International impact
4-Severe	Single fatality	Serious air/oil pollution	$ 8 mil	Nation wide impact
3-Significant	Multiple non severe injuries	Limited air/oil pollution	$ 800k	Regional impact
2-Minor	One or more first-aid injury	Limited to no air/oil pollution	$ 80k	Local impact
1-Negligible	Minor first-aid injury	Negligible air/oil pollution	$ 8k	Local awareness

*Env=Environmental, Rep=Reputational

Table II
ASSESSMENT OF RELEVANCE TO CRITICAL UCAS

Influence on UCA	Rank	Probability
Strong	4	1
Medium	3	0.1
Small	2	0.01
Very small	1	0.001

V. CASE STUDY

Pilotage is defined in the Finnish pilotage act as "operations related to the navigation of ships in which the pilot acts as an advisor to the master of the ship and as an expert on the local waters and their navigation"[35]. With the advancements in port digitalization, and potential risks and cost reduction, the feasibility of remote pilotage is currently under-assessment in Finland [36], [37]. While the current pilots need to board the vessel to assist the crew in maneuvering, the remote pilot will assist from the shore control center. To enable this remote assistance, all the necessary data for pilotage, such as ship dynamics data, ship systems data, and situational awareness, will be transferred to shore.

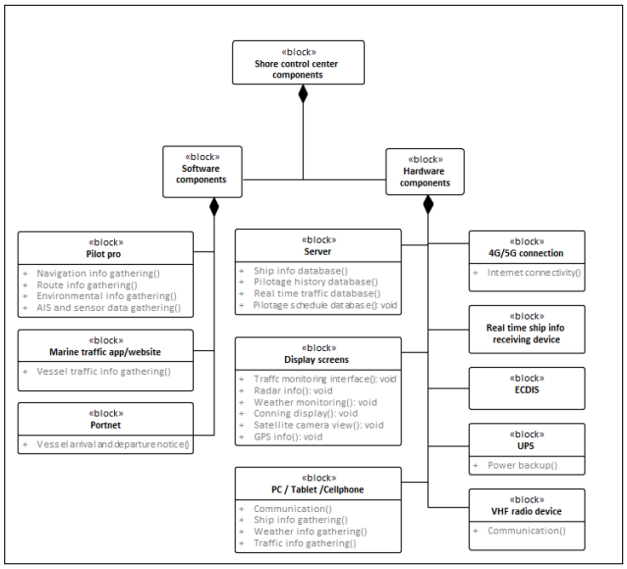

Figure 2. SysML Block definition diagram of remote pilotage components at shore control center

Herein, for MITRE ATT&CK techniques ranking we investigate only the cyberattack scenarios that can be potentially generated by a general hacker aiming at getting ransom as a reward for his attacks. The focus of the analysis is also on the shore control center of remote pilotage operations.

VI. RESULTS

A. SysML results

An example of a Block definition diagram and an Activity diagram in SysML are shown in Figure 2 and Figure 3, respectively. Figure 2 shows the information related to components such as Display screens, servers, and networks, to be installed at shore control center for remote pilotage. Figure 3 then shows an activity diagram of pilotage planning, where all the actors involved and their functions during pilotage planning are detailed. These diagrams are then used as input to create the remote pilotage control structure as well as during the brainstorming session to identify the UCAs and also to conduct STRIDE. Figure 4,

B. STPA and ranking results

Based on the analysis results, the updated list of accidents and hazards is provided in Table III and Table IV. The losses

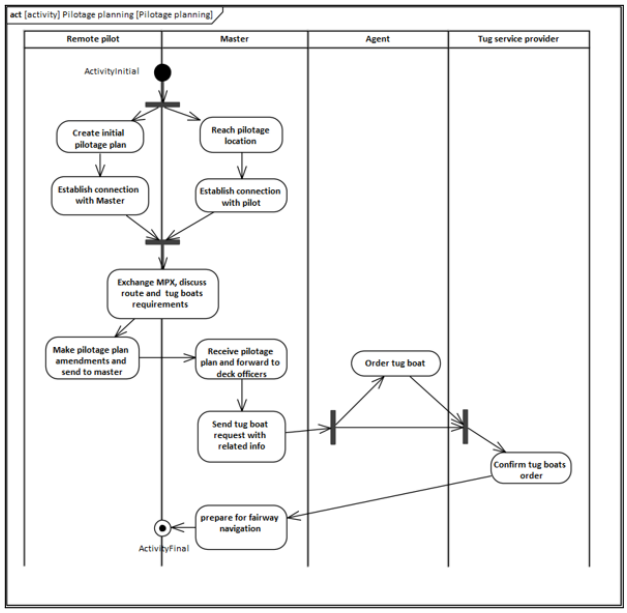

Figure 3. SysML activity diagram of remote pilotage planning

provided in Table III are extended to include the cybersecurity-related losses (losses from L-9 to L-11) since we apply a cybersecurity-enhanced version of STPA. Similarly the list of hazards includes additionally the cybersecurity hazards (such as H-6 and H-7). This obviously does not mean that the other hazards and losses cannot be caused by cyberattacks.

A simplified control structure of the remote pilotage operations is provided in Figure 4, whilst the distribution of ranked UCAs is provided in Figure 5. The elements of the control structure such as network (4G/5G), VHF, remote pilot display, and actors are also provided. From the identified UCAs, we expect that none should lead to catastrophic results involving multiple fatalities or complete ship loss. This ranking is suggested based on the available confidential accident statistics for conventional pilotage and we do not expect this to be violated in the remote pilotage operations. Also the critical UCAs were all safety-related or leading to some type of severe safety consequences. Example constitute such UCA as "Remote pilot does not provide deviation alert and advice when needed to the master during pilotage resulting into unsafe situation." or "Remote pilot provide wrong, missing or unclear advice on handling the deviations to the master during pilotage resulting into unsafe situation." All of the critical UCAs where relevant to the communication link between the remote pilotage and the under pilotage ship, as also depicted in Figure 4.

Very few unsecure control actions were added to the analysis and all of them were not considered as critical. This is attributed to the fact that the remote pilotage is related to safety critical operations and not to the handling of sensitive information, so even if the remote pilotage sends information to the wrong ship this was not considered as important as potential ship damage or ship crew injuries.

Table III
LOSSES

Losses Number	Losses description
L-1	Loss of life or injury to people (safety related)
L-2	Loss of or damage to own ship (financial related)
L-3	Loss of or damage to external objects (financial related)
L-4	Loss of mission (financial related)
L-5	Loss of availability (financial and safety related)
L-6	Negative publicity (reputational)
L-7	Environmental pollution (environment related)
L-8	Customer dissatisfaction (financial related)
L-9	Confidential loss (financial related)
L-10	Loss of data (financial related)
L-11	Loss of data/systems integrity (safety and financial related)

Table IV
SYSTEM LEVEL HAZARDS

Hazards Number	Hazard description
H-1	Ship violate minimum separation standards in route
H-2	Ship does not maintain safe under clear clearance
H-3	Ship leaves designated route
H-4	Lack of communication between remote pilotage stakeholders during remote pilotage
H-5	Lack of information sharing between remote pilotage stakeholders during remote pilotage
H-6	Unauthorized access to the ship systems/remote pilotage systems
H-7	Ship sending information to unauthorized persons

C. *STRIDE, MITRE ATT&CKs, and ranking results*

STRIDE is used here to identify the most relevant cyber attacks for critical UCAs. For instance, for the UCA: "Remote pilot does not provide deviation alert and advice when needed to the master during pilotage resulting into unsafe situation." the potential attack scenarios can include the Denial of service attack on the remote pilotage display or equipment during operation, or Denial of service attack of the ship navigational equipment or even on the fairway infrastructure. Similarly, Tampering attack on ship equipment or the remote pilotage equipment can cause misleading information being provided to remote pilot and, as a consequence, inappropriate guiding

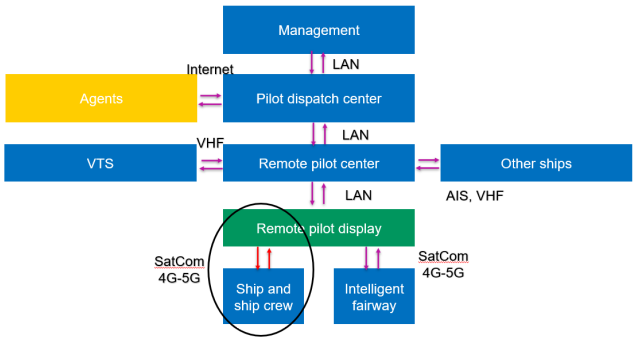

Figure 4. Remote pilotage control structure.

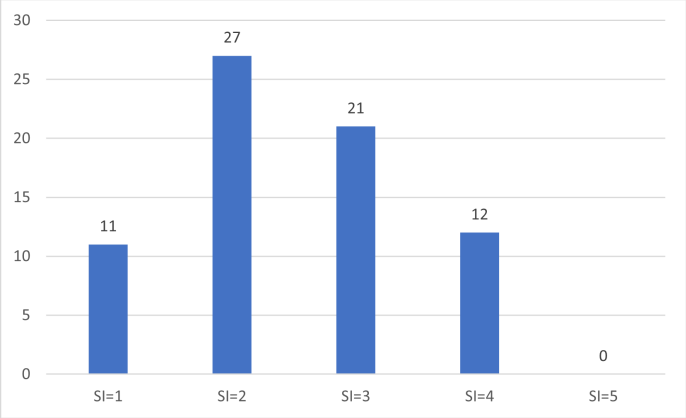

Figure 5. Distribution of the UCAs.

information being sent by the remote pilot. In our particular analysis, the Denial of Service, Tampering, and Spoofing attacks were considered of interest.

Having the knowledge of that, the MITRE ATT&CK techniques are ranked based on their likelihood and relevance to the critical UCAs and the considered STRIDE attacks. The most critical techniques, along with control measures, are provided in Table V. These attack techniques have been considered based on their applicability to the remote pilotage center, even though the attacks on piloted ships are expected to be similar in terms of likelihood. These techniques are considered as critical, since their use is relatively simple and does not require a significant amount of resources, so they can be easily implemented by a general attacker. However, their contribution to the critical UCAs similar to the one previously mentioned can be limited, as causing UCA can be outside the motivation of the particular attacker group and most probably can be caused unintentionally, e.g. causing a denial of service of remote pilotage center during critical operation to request the ransom.

Table V
MITRE ATT&CK CONSIDERED TECHNIQUES AND CONTROL MEASURES

MITRE ATT&CK	Control measures
Default credential	Mitigation - Ensure embedded controls and network devices are protected through access management. Review vendor documents and security alerts for potentially unknown or overlooked default credentials within existing devices Detection - Use of Logon session and network traffic analysis
Exploit public-facing application	Mitigation - Application isolation and sandboxing, web application firewalls, network segmentation, privilege account management, establish procedures to rapidly patch systems and scan for vulnerabilities Detection - Use of Logon session and network traffic analysis
Replication through removable media	Mitigation - Disabling such features as Autorun, restricting USB ports on the remote pilotage communication and interaction systems, system hardening Detection - Drive controls, alarms in case of unauthorized file access and file creation, or process creation

VII. Discussion

In the present conference paper, we have investigated how completely independent methods (STPA, SysML, STRIDE, MITRE ATT&CK, and ranking method) can be integrated to offer more effective risk management. We could observe that such integration can be helpful in offering different perspectives of the cyber risk in the remote pilotage. SysML diagrams provided detailed system information such as components, actors, functions, and interactions, which eased the development of control structure. Furthermore, it helped in identification of UCAs in STPA and relevant attacks in STRIDE. STPA offered the understanding of safe and unsecure control actions. STRIDE then offered an understanding of which high level cyberattack scenarios and on which systems the safe and unsecure control actions could occur. Next, MITRE ATT&CK contributed in detailed understanding of how the cyber attack scenarios can occur and how they can be addressed by utilizing the available knowledge library. Ranking supported the prioritization of the analysis and resources allocation.

On the other hand, we could observe that there is an overlap between the SysML, STPA, STRIDE, and MITRE ATT&CK required and generated information which resulted in relevant adaptations. For instance the information provided in control structure of STPA and SysML diagrams partially overlaps with the information provided in Data Flow Diagrams required by STRIDE, so we considered replacing Data Flow Diagrams with the STPA control structure and SysML diagrams. Also we eliminated some of the MITRE ATT&CK techniques since we have already encountered them in the STRIDE or considered them as accidents in STPA. To interconnect the ranking method described in [5] we added a Table II. Thus, the integration between different techniques required a special treatment and adjustments.

We could observe also that MITRE ATT&CK has been lacking some cyber attack scenarios which are relevant for ship systems as identified in [5] for instance dazzling attacks for cameras, and attacks on GPS and AIS systems. However, by including this attack techniques in the analysis, this gap can be easily addressed. In our case these attack scenarios were not identified as critical and likely as the other attacks for the case of general hacker attacks.

VIII. Conclusions

In this paper, we presented an novel approach to cyber risk analysis integrating some state-of-the-art and novel techniques with application to remote pilotage operations.

The main findings are as follows:

- The integration of STPA, SysML, STRIDE, MITRE ATT&CK, and ranking methods required adaptation in the methods steps to allow joint risk analysis.

- On the other hand, the integration of different methods allowed understanding of various risk facets by demonstrating link between safety and cybersecurity.
- The usage of SysML diagrams as input supported the development of the control structure and identifying UCAs in STPA and attacks in STRIDE.
- The MITRE ATT&CK attack techniques require enhancement to be applicable to ship related systems.
- The potential inadvertent consequences due to general cyberattack are not expected to be of catastrophic nature in remote pilotage operations.
- In the context of remote pilotage attention, should be paid to denial of service, spoofing, and tampering attacks.
- The most likely and critical MITRE ATT&CK techniques that needs to be addressed involve the use of default credentials, the exploitation of public facing applications, and replication through removable media.

The presented approach can support enhanced cyber risk analysis in maritime systems. Future research could focus on investigating the facilitation of its practical implementation.

IX. Acknowledgements

The authors gratefully acknowledge Business Finland for providing financial support through the Sea4Value research program and Finnish Pilots for support with data.

References

[1] O. DIMECC, "Sea4value/fairway program (s4vf)," *online], https://www. dimecc. com/dimecc-services/s4v*, 2020.

[2] D. M. Authority, "Technological assessment on the possibility of shore based pilotage in danish waters," 2014.

[3] T.-e. Kim, A. Sharma, A. H. Gausdal, and C.-j. Chae, "Impact of automation technology on gender parity in maritime industry," *WMU Journal of Maritime Affairs*, vol. 18, no. 4, pp. 579–593, 2019.

[4] E. Jokioinen, J. Poikonen, R. Jalonen, and J. Saarni, "Remote and autonomous ships-the next steps," *AAWA Position Paper, Rolls Royce plc, London*, 2016.

[5] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos, "A novel cyber-risk assessment method for ship systems," *Safety Science*, vol. 131, p. 104908, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925753520303052

[6] L. Kohnfelder and P. Garg, "The threats to our products (1999)," *URL: https://adam. shostack. org/microsoft/The-Threats-To-Our-Products. docx*, 2021.

[7] MITRE, "Mitre att/ck," [Online; accessed 28-June-2022]. [Online]. Available: https://attack.mitre.org/

[8] T. UcedaVelez and M. M. Morana, *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons, 2015.

[9] B. Schneier, "Attack trees," *Dr. Dobbâs journal*, vol. 24, no. 12, pp. 21–29, 1999.

[10] J.-M. Flaus, *Cybersecurity of industrial systems*. John Wiley & Sons, 2019.

[11] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security application of failure mode and effect analysis (fmea)," in *International conference on computer safety, reliability, and security*. Springer, 2014, pp. 310–325.

[12] N. G. Leveson and J. P. Thomas, *STPA Handbook*. The MIT Press, 2018.

[13] W. Young and N. Leveson, "Systems thinking for safety and security," in *Proceedings of the 29th Annual Computer Security Applications Conference*, 2013, pp. 1–8.

[14] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, "Stpa-safesec: Safety and security analysis for cyber-physical systems," *Journal of information security and applications*, vol. 34, pp. 183–196, 2017.

[15] N. P. De Souza, C. d. A. C. César, J. de Melo Bezerra, and C. M. Hirata, "Extending stpa with stride to identify cybersecurity loss scenarios," *Journal of Information Security and Applications*, vol. 55, p. 102620, 2020.

[16] J. Glomsrud and J. Xie, "A structured stpa safety and security co-analysis framework for autonomous ships," in *European Safety and Reliability conference, Germany, Hannover*, 2019.

[17] D. Dghaym, T. S. Hoang, S. R. Turnock, M. Butler, J. Downes, and B. Pritchard, "An stpa-based formal composition framework for trustworthy autonomous maritime systems," *Safety science*, vol. 136, p. 105139, 2021.

[18] N. H. Carreras Guzman, M. Wied, I. Kozine, and M. A. Lundteigen, "Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis," *Systems Engineering*, vol. 23, no. 2, pp. 189–210, 2020.

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

[20] V. Bolbot, G. Theotokatos, E. Boulougouris, G. Psarros, and R. Hamann, "A novel method for safety analysis of cyber-physical systems-application to a ship exhaust gas scrubber system," *Safety*, vol. 6, no. 2, p. 26, 2020.

[21] I. B. Utne, B. Rokseth, A. J. Sørensen, and J. E. Vinnem, "Towards supervisory risk control of autonomous ships," *Reliability Engineering & System Safety*, vol. 196, p. 106757, 2020.

[22] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cyber-attacks against the autonomous ship," in *Computer security*. Springer, 2018, pp. 20–36.

[23] A. Amro, G. Kavallieratos, K. Louzis, and C. A. Thieme, "Impact of cyber risk on the safety of the milliampere2 autonomous passenger ship," in *IOP Conference Series: Materials Science and Engineering*, vol. 929, no. 1. IOP Publishing, 2020, p. 012018.

[24] G. Kavallieratos, V. Diamantopoulou, and S. K. Katsikas, "Shipping 4.0: Security requirements for the cyber-enabled ship," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6617–6625, 2020.

[25] A. Hummelholm, J. Pöyhönen, T. Kovanen, and M. Lehto, "Cyber security analysis for ships in remote pilotage environment," in *ECCWS 2021 20th European Conference on Cyber Warfare and Security*. Academic Conferences Inter Ltd, 2021, p. 169.

[26] J. Pöyhönen, T. Kovanen, and M. Lehto, "Basic elements of cyber security for an automated remote piloting fairway system," in *Proceedings of the 16th International Conference on Cyber Warfare and Security ICCWS*, 2021, pp. 299–308.

[27] J. Pöyhönen and M. Lehto, "Assessment of cybersecurity risks: Maritime automated piloting process," in *The proceedings of the 17th international conference on cyber warfare and security*, vol. 17. Academic Conferences International Ltd, 2022.

[28] J. Pöyhönen, A. Hummelholm, and M. Lehto, "Cybersecurity risk assessment subjects in information flows," in *Proceedings of the European conference on cyber warfare and security*. Academic Conferences International Ltd, 2022.

[29] T. Kovanen, J. Pöyhönen, and M. Lehto, "Cyber-threat analysis in the remote pilotage system," in *ECCWS 2021 20th European Conference on Cyber Warfare and Security*. Academic Conferences Inter Ltd, 2021, p. 221.

[30] S. Friedenthal, A. Moore, and R. Steiner, "Omg systems modeling language (omg sysml) tutorial," in *INCOSE Intl. Symp*, vol. 9, 2006, pp. 65–67.

[31] M. Hause *et al.*, "The sysml modelling language," in *Fifteenth European Systems Engineering Conference*, vol. 9, 2006, pp. 1–12.

[32] N. G. Leveson, *Engineering a safer world: Systems thinking applied to safety*. The MIT Press, 2016.

[33] O. Alexander, M. Belisle, and J. Steele, "Mitre att&ck for industrial control systems: Design and philosophy," *The MITRE Corporation: Bedford, MA, USA*, 2020.

[34] V. Bolbot, G. Theotokatos, J. McCloskey, D. Vassalos, E. Boulougouris, and B. Twomey, "A methodology to define risk matrices â application to inland water ways autonomous ships," *International Journal of Naval Architecture and Ocean Engineering*, vol. 14, p. 100457, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2092678222000231

[35] M. of Transport and Communications, "Pilotage act 940/2003; amendments up to 1534/2019 included."

[36] S. Basnet, A. Bahootoroody, M. Chaal, O. A. V. Banda, J. Lahtinen, and P. Kujala, "A decision-making framework for selecting an mbse

language–a case study to ship pilotage," *Expert Systems with Applications*, vol. 193, p. 116451, 2022.
[37] J. Lahtinen, O. A. V. Banda, P. Kujala, and S. Hirdaris, "Remote piloting in an intelligent fairway–a paradigm for future pilotage," *Safety Science*, vol. 130, p. 104889, 2020.