Human Factors in Cybersecurity, Vol. 91, 2023, 10–19
https://doi.org/10.54941/ahfe1003715

Keeping the Human Element to Secure Autonomous Shipping Operations

Per Håkon Meland[1], Dag Atle Nesheim[2], and Ørnulf Jan Rødseth[2]

[1]SINTEF Digital, Software Engineering, Safety and Security, Trondheim, Norway
[2]SINTEF Ocean, Energy and Transport, Oslo/Trondheim, Norway

ABSTRACT

Autonomous shipping operations are becoming economically and technically feasible, but this development also requires new human roles and responsibilities onshore for managing cyber events. The goal of this paper is to present a methodology for describing autonomous shipping operations and risks caused by potential cyber-attacks, focusing on critical situations to the interplay between the automation and human operators. We have applied our methodology on a case study for planned autonomous operations in European waterways. Our results show that the reliance on new technologies such as sensors, computer vision and AI reasoning onboard the autonomous ships or cranes opens to new types of attacks that the industry has little experience with as of now. Unmanned systems should therefore be designed with assurance methods that can bring the human into the loop, providing situational awareness and control. At the same time, human resource exhaustion is a potential attack goal against remote operations. We could see from our threat likelihood estimation that attacks related to deny- and injure-motivations have the highest values in all mission phase patterns. This is in accordance with the general attack trends within the maritime domain and many other sectors, where financially motivated attackers will try to demand a ransom to stop business disruption.

Keywords: Cybersecurity, Human factors, Autonomous systems, Maritime operations, Remote control, Risk factors, Unified modeling language

INTRODUCTION

The introduction of autonomous operations in shipping creates a new cyber-physical attack surface that cannot be mitigated by technical means alone. With only a few or no sailors onboard the vessel itself, there is a need for new human roles and responsibilities onshore for managing cyber events that could potentially lead to damage to life, goods, economy or the environment. Especially the handover between the automation and human remote control represents intricate challenges which must be understood and properly assessed. When should the human be involved and relieved? What kind of situational awareness can a remote operator obtain? How can the required level of attention and reaction times be dynamically adjusted according to different mission phases and changing environment (e.g., weather, traffic, threats)? What can go wrong and how/why would an attacker provoke an incident? Since shipping is a highly competitive playing field, we also need to

make sure that the human and technical measures we invest in are affordable and proportional to the actual risks they are meant to manage.

The goal of this paper is to present a methodology for describing autonomous shipping operations and risks caused by cyber-attacks. This includes different levels of autonomy and human operator control, system components and people involved, mission phase patterns and operating conditions. We apply the *Unified Modeling language* (UML) to formally describe the concept of operations and extend these models with misuse case diagrams representing threat actors and threat goals, which are drilled down to sequence diagrams to show attack scenarios.

The next section describes characteristics of autonomous shipping operations, including terms, challenges and opportunities. We then present the need for cyber risk management in shipping before giving an overview of our methodology. An example case study from a real-life automation effort in the Trondheimsfjord area is then used to exemplify a security assessment, before we conclude the paper.

CHARACTERISTICS OF AUTONOMOUS SHIPPING OPERATIONS

The international interest in autonomous shipping operations started in 2012 with the MUNIN project (Burmeister *et al.*, 2014). Developments since then have been slow but steady and the *International Maritime Organization* (IMO) is currently working on a new code for autonomous ships in international trade with a target completion year of 2025 (IMO, 2022). The realization of an autonomous ship system can take many forms and the community has not even agreed on a common definition of a *Maritime Autonomous Surface Ship* (MASS) (IMO, 2022). However, it is understood that autonomous ships differ from other autonomous vehicles such as cars or aerial vehicles in many ways. Ships are much more costly, move more slowly, and operates in environments that generally has fewer obstacles than cars (Rødseth *et al.*, 2021). This also gives opportunities: Ships are costly enough to make the use of remote supervision and intervention cost effective compared to developing full autonomy for the ships. A fully uncrewed ship sails with an *autonomous onboard controller* (AOC) that can operate the ship without human assistance most of the time, while a manned *Remote Control Centre* (RCC) will intervene at the request of the AOC to handle situations beyond the AOC's capabilities (Rødseth, Wennersberg and Nordahl, 2021). This requires that the AOC can issue warnings in time for the operator to gain sufficient situational awareness to take safe actions. This is called *constrained autonomy* (Rødseth *et al.*, 2021), which enables a new and more efficient type of cooperation between human and automation. However, constrained autonomy will also create new possibilities for cyber-attacks as coordination between AOC and crew becomes critical. Thus, the handover of control between human and automation via a communication link becomes important. The AOC will also need to define fallback functions and states in cases where the *operational envelope* (Rødseth, Lien Wennersberg and Nordahl, 2022) is exceeded. This includes cases when the crew fails to take over control after an alert from the AOC. If the fallback states are too

simplistic, e.g., just stopping the ship in all cases of communication loss, simple jamming of the communication link can effectively stop the ship from doing anything useful. Thus, the definition of fallback states must also be seen in conjunction with new possibilities for cyber-attacks.

MANAGING CYBER RISKS IN SHIPPING

Risk can generally be defined as the product of the assumed occurrence frequency or likelihood and the impact or consequence of hazardous incidents. Though the shipping industry has had a long tradition of considering risks from a safety perspective, the cyber security elements are often insufficiently considered (Cimpean *et al.*, 2011). One can argue that the hazards and the consequences generally are the same for both safety and cyber security related risk, but that the likelihood or frequency distribution is the main difference. As cyber-attacks often have a conscious and antagonistic motivation behind them, one cannot use general probability distributions based on historical occurrences. Instead, we have to follow the principle defined by Anderson (2020) that "we assume a hostile opponent who can cause some of the components of our system to fail at the least convenient time and in the most damaging way possible". In order to evaluate and rank for autonomous shipping operations, Meland et al. (2022) argue that we need to identify and assess threats based on the best data available. This paper also provides an overview of risk management frameworks for the maritime domain, similarly to Svilicic *et al.* (2019), Mraković and Vojinović (2019), Bolbot *et al.* (2020), Tusher *et al.* (2022), Grigoriadis *et al.* (2022) and Park *et al.* (2023). As pointed out by Tam and Jones (2018), many of the existing framework do not adequately address cyberthreats for autonomous vessels. Therefore, our methodology builds upon the concept of assessing *storyless systems* (Meland, 2021) to address the novelty of autonomous shipping.

METHODOLOGY OVERVIEW

The goal of the methodology is to formally describe the *Concept of Operation* (CONOPS) of an autonomous ship system. Figure 1 shows the framework of the methodology.

The *mission* is defined as the overall operation that the ship system executes, which may for instance be a certain voyage with port calls and cargo

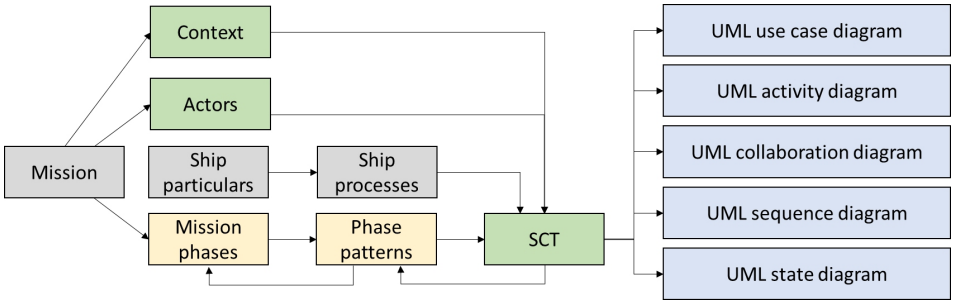

Figure 1: Framework of the methodology.

operations. Further, more details are added by defining the *context* (the external entities and systems that the ship system cannot control), the internal *actors* of the ship system, and also the various *mission phases* that the mission consists of. Examples of mission phases are automatic sailing, supervised sailing, cargo operation, port navigation, berthing and deberthing. Also, some of the *ship particulars* (information about the ship, e.g., size, speed, equipment and sensors) must be described to be able to further cover the actual *ship processes* that the autonomous ship system must handle. Examples of ship processes are navigation, cargo handling and energy production. To decrease model complexity, similar mission phases should be generalized into a mission *phase pattern*. This may be an iterative process, meaning that the initial definition of the mission phase may need to be changed after the mission phase pattern has been defined (the arrow from Phase patterns to Mission phases in Figure 1).

When the patterns have been defined, the *system control tasks* (SCT) and their prose definitions can be developed, again with a possibility for revising the patterns. SCTs are defined as "process control tasks, implemented by automation and/or humans, that are required to sustainably operate the autonomous ship system within its operational envelope" (ISO, 2022). The SCT also needs to consider the actors and context to determine how authority is shared between the automation and humans. In this methodology, we have a particular focus on the hand-over between the *Remote Control Center* (RCC) operator and the *autonomous onboard controller* (AOC) both operating the ship.

Finally, the SCT descriptions can be converted to *Unified Modelling language* (UML) diagrams, which are part of a language for system analysis and design stemming from the mid-1990s and managed by the *Object Management Group* (OMG) (Dobing and Parsons, 2006). These are also the basis for the security analysis. The advantage of this methodology is that it allows for a smooth transition from the autonomous ship system design phase to the assessment of the system using the same UML notation.

EXAMPLE CASE STUDY: TRONDHEIMSFJORD AREA

In this section we exemplify the methodology, using parts of a real-world use case covering autonomous transport of goods between Orkanger to Sandstad (for further transshipment) in the Trondheimsfjord area of Norway. Though the example is not complete, it shows how different UML diagrams can be used to formalize the description of the CONOPS and used in a security analysis. This mission is depicted in Figure 2 and the context can be described as sailing in an area with both leisure- and goods traffic of various sizes, hereunder motorized and non-motorized boats and ships. Since the fjord is relatively narrow with varying traffic situations, sailing in with a large container ships is not desirable. Instead, smaller autonomous container feeder vessels can do last mile delivery and retrieval of goods inside the fjord (e.g., Orkanger), while the larger ships dock at an outer island (Sandstad port at Hitra).

Figure 2: Mission: Voyage from Orkanger to Sandstad consists of 17 mission phases.

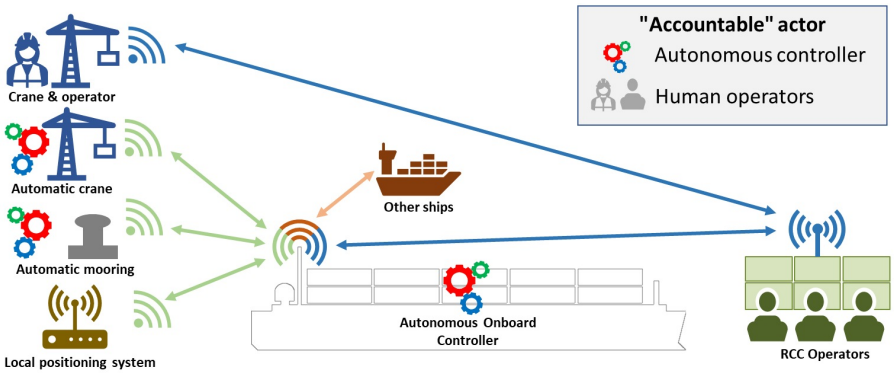

Figure 3: Central elements from the case study example.

Figure 3 illustrates central elements from context, actors and ship particulars that are used in this case study. The container feeder vessel is operated by an AOC with different levels of RCC attention. Communication and positioning systems are vital for avoiding static and dynamic objects surrounding the ship, as well as berthing/deberthing and cargo operations with manual/automatic cranes.

The most relevant ship process in this example is *navigation*, which again can be broken down into critical tasks such as (Rødseth, Lien Wennersberg and Nordahl, 2022):

- Situational awareness, that is, to verify the location, observe weather and sea, determine visibility, detect and classify objects and obstacles and assess own ship and the traffic situation.
- Maneuvering the ship, which is short term planning of safe operations. This includes keeping track, speed and course, avoiding static and dynamic obstacles, berthing and deberthing.

Table 1. Mission phases and mission phase patterns.

Phase	Description	Mission phase patterns	RCC Attention
1	Cargo operations in Orkanger (Manual)	Manual cargo operation	Direct
2	Deberth Orkanger	Deberthing	High
3	Departure Orkanger	Port navigation	Medium
4 – 9, 11–14	Sailing in low density waters towards Sandstad	Automatic sailing	Medium/low
10	Sailing in high traffic density/complexity area	Supervised sailing	High
15	Arrival Sandstad	Port navigation	Medium
16	Berthing Sandstad	Berthing	High
17	Cargo operations Sandstad (Automatic)	Automatic cargo operations	High
18	Deberth Sandstad	Deberthing	High
19	Departure Sandstad	Port navigation	Medium
20-23, 25–30	Sailing in low density waters towards Orkanger	Automatic sailing	Medium/low
24	Sailing in high traffic density/complexity area	Supervised sailing	High
31	Arrival Orkanger	Port navigation	Medium
32	Berthing Orkanger	Berthing	High

- Voyage management, which is planning and re-planning of the voyage done by the RCC operator, including acting on deviations that are not handled by the ship itself.
- Communication during voyage, that is, communication involving other ships, the RCC and *Vessel Traffic Services* (VTS).

Table 1 shows how the mission is divided into 32 discrete mission phases. This includes cargo operations, deberth and departure in Orkanger (phase 1-3), sailing outbound to Sandstad (phase 4-14) and arrival, berthing and cargo operations in Sandstad (phase 15-17). A similar phase organization is used towards Orkanger for the returning goods (phase 18-32). The mission phases have been mapped towards seven mission phase patterns to simplify the analysis. The reason why phase 1 has manual cargo operations, while phase 17 has automatic, is that Orkanger does not have autonomous crane equipment installed. The RCC attention column gives a rough indication of the need for operator attention during the different phases.

Direct means that the RCC operator must directly control the operation. *High* means that the operation is critical and continuous attention is needed, although operation will normally be automatic (e.g., mission phases 10 and 24 are in an area with frequent ferry crossings). *Medium* means that the operator may be called to intervene if the traffic situation becomes too complex for the automation and *low* means that the system will be able to handle the automatic operation by itself and that any deterioration of the situation will not happen suddenly.

At this point we have enough information to initiate the security analysis by considering the malicious intents for potential threat actors for each of the identified mission phase patterns. This is depicted as a high-level UML use case description in Figure 4. Intents and threat actors are selected and specialized from a pre-existing library for the maritime domain, and depicted using the *misuse case* notation by Sindre and Opdahl (2005).

The *system control tasks* (SCT) define the desired level of human intervention versus automation for the mission phase patterns. Special focus is on the hand-over between humans and automation systems, since we cannot expect that the autonomous ship will be capable of taking all decisions by itself. In such cases, the RCC must be alerted to take over the control of the ship. Further, we must take into consideration that communication systems between the ship and the RCC and other ship particulars are exposed to both technical errors and intentional attacks. Figure 5 shows two UML sequence diagrams related to the automatic sailing pattern. The left part shows the normal situation, where the RCC Operator will be in a monitoring state, and some time is needed to get situational awareness and transition to supervised sailing. The initiative for this transition can come from both the RCC and the AOC. In the right part of the figure, we have broken the *injure* intent from Figure 4 into more specific attack scenarios. Here, jamming of the AOC or RCC may stop the normal transition between automatic and supervised sailing. More advanced attack steps are feasible as well, where jamming is combined with

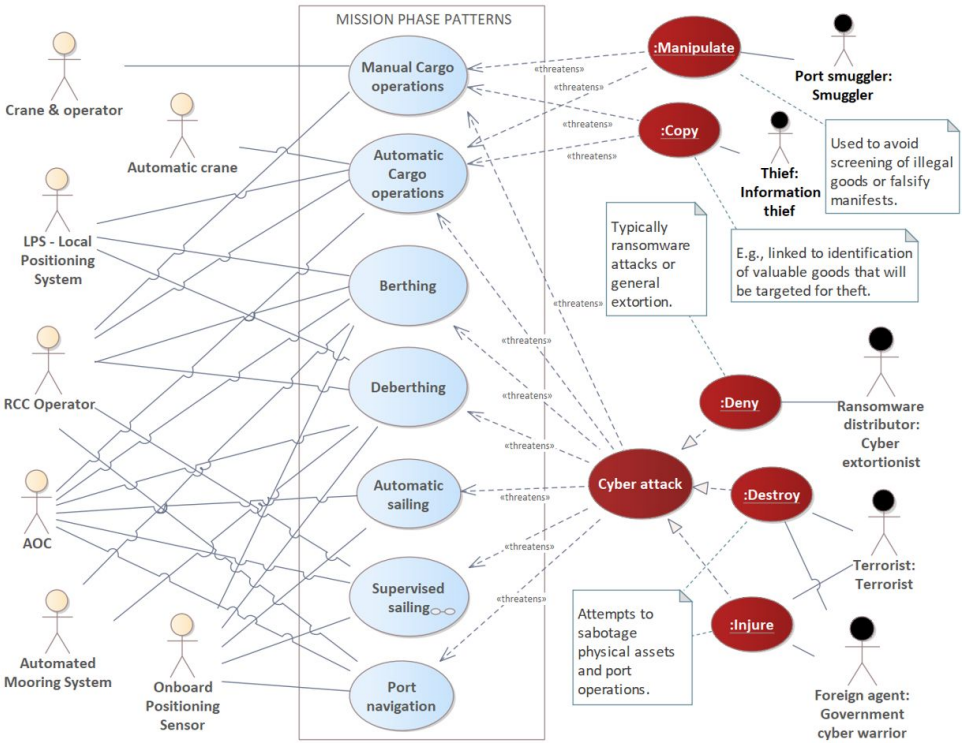

Figure 4: UML use case showing actors and mission phase patterns linked to misuse case activities and threat actors.

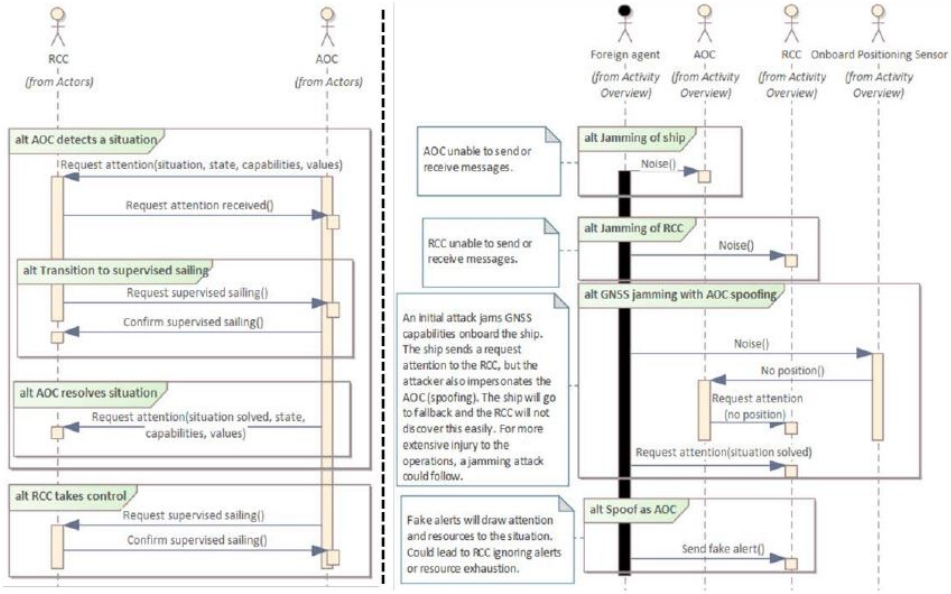

Figure 5: Expected behavior (left) and attack scenarios (right).

spoofing to make the RCC believe that a situation is solved when it is not, putting the AOC in an uncertain state. Also, sending fake alerts to the RCC could lead to resource exhaustion or security fatigue, which is another threat towards the operations.

In our case study we have similarly to the example in Figure 5 created attack scenarios for all the mission phase patterns and malicious intents. Together with subject-matter experts, we have estimated values for threat likelihoods based on the *size of the group* of potential threat actors identified in the UML models, the *opportunities* or favorable circumstances for an attack during the given mission phase patterns, the *means* the threat actors would require to perform the attacks as described in the attack scenarios and finally the *motivation* for the threat actors, which greatly depends on the expected reward in case of a successful attack. This is in accordance with the storyless system concept (Meland, 2021) and the axiom by Anderson (2020) that "One of the first things the security engineer needs to do when tackling a new problem is to identify the likely opponents" and "…what sort of capabilities will the adversaries have, and what motivation?".

Our results show that it is the deny- and injure-intents that have the highest likelihood values in all mission phase patterns. This is in accordance with the general attack trends within the maritime domain (Meland *et al.*, 2021; Park *et al.*, 2023) and other sectors, where financially motivated attackers will try to demand a ransom, typically through malware injections or denial-of-service attacks. Complex attacks can create more disturbance, but are also more expensive and complex to perform, thus requiring highly motivated threat agents. Berthing/deberthing and cargo operations have the strictest real-time requirements to communication and control. In these cases, the ship

is close to shore, and more alternative communication systems are available. This makes attacks more difficult, but it is also in these situations where inflicted damage could be greatest. In general, hand-over between AOC and RCC is a critical phase as the autonomous ship system needs to be sure who is the accountable party at every point in time. There are several ways in which an attacker could try to block or trigger hand-over unnecessarily, causing disruptions or delays in the operations. As a worst case, the attacker could gain control of the ship through supervised sailing.

CONCLUSION

Autonomous shipping operations are in the process of being realized around the world. However, the human element is still vital in managing situations where the automation falls short. Furthermore, the reliance on new technologies, such as computer vision and AI reasoning onboard autonomous ships or cranes, opens for new attack types that the industry has little experience with as of now. Therefore, there is a need for a continued risk assessment based on the context, involved actors, ship particulars/processes and mission phases for the individual missions. Our methodology focuses on finding critical situations where cyber-attacks threaten these operations, especially related to the interplay between the automation and human operators. Further work intends to also apply the methodology on other specific missions, such as inland waterway missions in central Europe.

ACKNOWLEDGMENT

This work has been funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 859992 (AEGIS - Advanced, Efficient and Green Intermodal Systems). Many thanks to Egil Wille and Marianne Hagaseth for their valuable input to this work.

REFERENCES

Anderson, R. (2020) *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.

Bolbot, V. *et al.* (2020) 'A novel cyber-risk assessment method for ship systems', *Safety Science*, 131, p. 104908. Available at: https://doi.org/10.1016/j.ssci.2020.104908.

Burmeister, H.-C. *et al.* (2014) 'Autonomous unmanned merchant vessel and its contribution towards the e-Navigation implementation: The MUNIN perspective', *International Journal of e-Navigation and Maritime Economy*, 1, pp. 1–13.

Cimpean, D. *et al.* (2011) *Analysis of cyber security aspects in the maritime sector*. ENISA. Available at: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport.

Dobing, B. and Parsons, J. (2006) 'How UML is used', *Communications of the ACM*, 49(5), pp. 109–113.

Grigoriadis, C. *et al.* (2022) 'An Adaptive, Situation-Based Risk Assessment and Security Enforcement Framework for the Maritime Sector', *Sensors*, 22(1), p. 238. Available at: https://doi.org/10.3390/s22010238.

IMO (2022) *Maritime Safety Committee (MSC 106), 2–11 November 2022*. Available at: https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-106.aspx (Accessed: 25 January 2023).

ISO (2022) *ISO/TS 23860:2022 Ships and marine technology — Vocabulary related to autonomous ship systems*. Available at: https://www.iso.org/standard/77186.html (Accessed: 24 January 2023).

Meland, P. H. *et al.* (2021) 'A retrospective analysis of maritime cyber security incidents', *The International Journal on Marine Navigation and Safety of Sea Transportation*, 15(3). Available at: https://doi.org/10.12716/1001.15.03.04.

Meland, P. H. (2021) *Storyless cyber security: Modelling threats with economic incentives*. NTNU. Available at: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2825312.

Meland, P. H. *et al.* (2022) 'Assessing cyber threats for storyless systems', *Journal of Information Security and Applications*, 64, p. 103050.

Mraković, I. and Vojinović, R. (2019) 'Maritime cyber security analysis–how to reduce threats?', *Transactions on maritime science*, 8(01), pp. 132–139.

Park, C. *et al.* (2023) 'A BN driven FMEA approach to assess maritime cybersecurity risks', *Ocean & Coastal Management*, 235, p. 106480. Available at: https://doi.org/10.1016/j.ocecoaman.2023.106480.

Rødseth, Ø. J. *et al.* (2021) 'Operational Design Domain for Cars versus Operational Envelope for Ships: Handling Human Capabilities and Fallbacks', in *Proceedings of the 31st European Safety and Reliability Conference*.

Rødseth, Ø. J., Lien Wennersberg, L. A. and Nordahl, H. (2022) 'Towards approval of autonomous ship systems by their operational envelope', *Journal of Marine Science and Technology*, 27(1), pp. 67–76.

Rødseth, Ø. J., Wennersberg, L. A. L. and Nordahl, H. (2021) 'Improving safety of interactions between conventional and autonomous ships', in *1st International Conference on the Stability and Safety of Ships and Ocean Vehicles*, pp. 7–11.

Sindre, G. and Opdahl, A. L. (2005) 'Eliciting security requirements with misuse cases', *Requirements Engineering*, 10(1), pp. 34–44. Available at: https://doi.org/10.1007/s00766-004-0194-4.

Svilicic, B. *et al.* (2019) 'Maritime cyber risk management: An experimental ship assessment', *The Journal of Navigation*, 72(5), pp. 1108–1120.

Tam, K. and Jones, K. (2018) 'Cyber-Risk Assessment for Autonomous Ships', in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pp. 1–8. Available at: https://doi.org/10.1109/CyberSecPODS.2018.8560690.

Tusher, H. M. *et al.* (2022) 'Cyber security risk assessment in autonomous shipping', *Maritime Economics & Logistics*, 24(2), pp. 208–227. Available at: https://doi.org/10.1057/s41278-022-00214-0.