TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 19
Number 2
June 2025
DOI: 10.12716/1001.19.02.35

Developing Human-Autonomy Teaming Strategies for Maritime Cyber Security Resilience in Uncrewed Autonomous and Remote Surface Vessel Operations

J.D. Palbar Misas, K. Tam & K. Jones
University of Plymouth, Plymouth, United Kingdom

ABSTRACT: The development of new technologies and digital capabilities for Uncrewed Autonomous and Remote Surface Vessel Operations (UARSVO) is driven by various industry stakeholders. This evolution impacts the maritime industry's human role, transforming from Human-Autonomy Hybrid (HAH) to Human-Autonomy Teaming (HAT). Human-Autonomy Collaboration (HAC) is vital for maritime safety, security, and sustainability, particularly in light of increasing cyber incidents in remote operations, which necessitates greater cyber resilience due to technology at sea and ashore. This paper aims to provide a holistic socio-technical approach to investigate and present an overview of the current state-of-the-art research, focusing on the human perspective in maritime cyber resilience for UARSVO. The view is developed using 76 semi-structured interviews with participants from various stakeholder groups across the Maritime Autonomous Surface Vessel (MASS) industry worldwide. Findings provide unique, holistic, and human-centred operational strategies for maritime cyber resilience, as well as the perceived training required to enhance these operations.

1 INTRODUCTION

The International Maritime Organization (IMO) Maritime Autonomous Surface Ship (MASS) Joint Maritime Safety Committee (MSC) - Legal Committee (LEG) - Facilitation Committee (FAL) Working Group on the 109th session stated within the principles of the MASS Code draft that "There should be a human master responsible for a MASS, regardless of mode of operation; regardless of mode of operation, the master of a MASS should have the means to intervene when necessary" [1]. These principles should continue unchanged as per current IMO's vision of adopting a non-mandatory MASS Code by 2026 and a mandatory MASS Code in 2032 [1]. This means that for a fully autonomous ship, a human master will remain in command, ultimately responsible for the safety of the MASS vessel. This person will delegate and share responsibility with an Autonomous Navigation System (ANS) for the conduct of a MASS vessel. Therefore, even for fully autonomous ships, humans will still be mandated to be in the loop, operating in monitoring or supervising mode. In addition, individual masters may oversee one or more MASS vessels at any given time, remotely viewing or controlling vessels from a Remote Operations Centre (ROC) to "intervene when necessary" in case the ANS makes an incorrect decision [2, 3].

The above demonstrates that regulations, standards, competences and certification for Remote Operator (RO) and ROC personnel will be as crucial as technical regulations and standards developed for MASS [4, 5]. The share of responsibilities during the hand-over between a RO to an ANS for the conduct of the ship and vice versa will require Human-Autonomy Teaming (HAT) to perform Uncrewed Autonomous and Remote Surface Operations (UARSVO) [6]. HAT is

the interdependence of human(s) and autonomous agent(s) working collaboratively but, with separate roles, to attain a common goal [7-9]. Thus, clear roles and responsibilities for all agents must be established to attain seamless, safe, secure and sustainable operations for future MASS vessels, especially when engaged in international commercial voyages [10].

Due to the increase in connectivity and complicated software, no part of the industry is, nor will be, immune to cyber threats. As demonstrated with real-world maritime autonomous systems in [11], multiple attacks can be performed utilising Adversarial Artificial Intelligence (AAI) to confuse MASS- running AI without HAT. When considering more general cyber threats in the maritime industry, from October 2023 to October 2024 31% of maritime professionals reported a cyber-attack, indicating a rise of 14% over the previous five years [12]. As completely cyber-secure maritime systems are not practically feasible, a key success for future operations is cyber resilience. Providing resilience is key to enabling autonomous systems and operators to reduce and minimise cyber-attacks but also continue operating safely during an active attack. Cyber resilience can be enhanced by developing proactive strategies including response procedures during cyber incidents. While it is difficult to train for this during a real incident, with the use of response plan scenarios played out (for example in a simulator), training cyber resilience becomes more feasible [13].

To achieve a maritime cyber resilient workforce, stakeholders and Maritime Education and Training Institutes (METIs) should collaborate and develop the appropriate training requirements for UARSVO. This would expand and introduce new and essential social-technical skills and behavioural markers [14, 15]. As this training is meant for people, using methods like the Human Centred Design (HCD) process when developing training can increase understanding of the operational needs of ROC operators (i.e. end-users). Moreover, to achieve a balance between the innovation technology developed and operational safety, ROC's top management level will need to serve as a link for the UARSVO stakeholder ecosystem so that technology developers (software and hardware manufacturers) can receive ROs (end-user) feedback on products before and after implementing technology [16].

UARSVO requires interdisciplinary collaboration to integrate technical and operational skills within a cooperative feedback loop to foster a shared vision of operations across organisations and enhance the resilience of proactive organisations [17]. As an example of a holistic solution, [18] uses HCD combined with the Desing Research Methodology (DRM), as a business and technical approach which includes the user need, to develop and conduct maritime cyber resilience training for crewed operated vessels with the participation of several maritime stakeholders' and operators. That said, that previous study focuses on crewed operations, differs significantly to this study, which focuses purely on uncrewed.

This study explores which training strategies could best enhance HAT in maritime cyber security resilience for UARSVO. To achieve this, 76 semi-structured interviews were held with participants from multiple stakeholder groups across the MASS industry, including international organisations, research and academia, national organisations, industrialists and resource providers, shipping companies, and members of the future workforce. This large, multi-disciplinary engagement provided a never-before-attempted holistic socio-technical view towards the future development of a HAT training framework in maritime cyber security resilience for UARSVO. The remainder of this paper follows the following structure: Section 1 introduces the context and draws the research objectives. Section 2 provides a literature review of HAT for UARSVO, HAT for maritime cyber security resilience and HAT maritime cyber security resilience training in UARSVO. Section 3 states the qualitative methodology and methods used for research as well as ethical considerations. Section 4 presents the results obtained per stakeholder group, and the findings are discussed in Section 5.

Section 6 outlines the limitations of the research and future work. Section 7 summarised key findings for the conclusion.

2 BACKGROUND

2.1 *HAT for UARSVO Overview*

The autonomy of a maritime vessel is classified by the degree it makes decisions and executes actions by itself. It must also, critically, perform these actions at the appropriate time without human intervention [19, 20]. As defined by [21], autonomy is considered a process as both autonomy and automation are somewhat overlapping terms that some use interchangeably. In this paper, if a machine or a computer performs operations without human control, this is referred to as automation. This means that sophisticated automation could overlap with the term autonomy [21, 22]. Although people seem to perceive "autonomy" as taking humans out of the loop, sometimes implying technology is superior to humans, the irony of automation is that if technology fails, humans will always be needed to take over [23]. Additionally, if technology acts unexpectedly for the user, causing a dangerous situation, this could be named as automation surprise [24]. The incident report findings provided by the National Transportation Safety Board (NTSB) in 2018 demonstrate the concept of automation surprise as there was a perceived loss of steering by the crew and subsequent mishandling of steering controls during the transfer of control. This caused the USS John S McCain in the Singapore Strait to veer off course and consequently collide with the tanker Alnic MC. This incident, which tragically led to the loss of life of seafarers aboard the USS John S McCain, highlighted the need for improved training when systems are perceived to malfunction [25].

However, a malfunction and a cyber attack are different. This paper builds on this with the hope that research in cyber resilience training can help prevent tragic incidents involving autonomy and cyber- attacks instead of being implemented after a tragedy.

From a socio-technical approach, and as seen with the incident case above, complex systems must be designed so that the technical and human elements can work in unison to achieve safe and effective operations

[26]. This means that systems are designed to enhance the adaptability human performance brings to dynamic and critical environments when oversight is required [27]. For this, there are three paradigms to the overall Human-Autonomy Relationship (HAR): Human-Autonomy Collaboration (HAC), Human-Autonomy Teaming (HAT) and Human-Autonomy Hybrid (HAH). At a strategic level, HAC encompasses any collaborative cooperation between humans and autonomy to achieve a common goal; at a tactical level, HAT significates that there is partial human authority as human and autonomy work as a unit with distinct roles each; at an operational level HAH autonomy works complementary and interdependently as an integrated unit with the human having the full authority in decision making and autonomy for decision-support [28, 29]. In the maritime industry for MASS vessels, the amount of control the systems have within the Operational Design Domain (ODD) and established performance capabilities and limits within the Operational Envelop (OE) is determined by the IMO's degree of autonomy (as shown in Table 1) which sets the boundaries for each agent [30]. From the human perspective, the degree of autonomy helps define ROC operators' competences and certification needed for UARSVO [4, 5, 31].

Table 1. Compilation of different Degrees of Autonomy (DOA) based on [32] and [33].

DOA	IMO	Bureau Veritas	DNV	ONE SEA	SARUMS	Lloyd's Register
D-0	N/A	System operated by a human.	Manually operated function.	Basic operation.	Crewed	Manual steering.
D-1	Ship with automated processes and decision support.	Systems directed by a human.	System decision supported function.	Assisted operation.	Operated	On-board decision support.
D-2	Remotely controlled ship with seafarers on board.	Systems delegated by a human.	System decision supported function with conditional system execution capabilities.	Partial automation.	Directed	On and off-board decision support.
D-3	Remotely controlled ship without seafarers onboard.	Systems supervised by a human.	Self-controlled function with human in the loop.	Conditional automation.	Delegated	"Active" human in the loop.
D-4	Fully autonomous ship.	Fully automated systems that only require human intervention in case of emergency.	Autonomous function without human intervention.	High automation.	Monitored	Human in the loop.
D-5				Autonomous.	Autonomous	Autonomous.
D-6						Fully Autonomous.

Frameworks by [34], [35], [36], [37], [33], [38].

2.2 *HAT Maritime Cyber Security Resilience for UARSVO*

Between the loss scenarios and causal factors identified in autonomous ships on the EU H2020 MOSES project, 43% of the causal factors of a loss scenario were attributed to cyber-attacks or connectivity issues [39]. This demonstrated that cyber resilience for UARSVO is a major concern and a crucial area of improvements as a continuous iterative process. In a survey conducted by DNV with maritime expert professionals, 95% of roughly 500 participants, stated that further collaboration is needed within the maritime industry to protect critical infrastructure from a cyber incident [40].

Within the current maritime international standards, the Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems has been adopted by the IMO's MSC in 2017 and entered into force in 2021. This resolution mandates that currently operating ships must assess cyber risks in their company's Safety Management System (SMS) as per the International Safety Management (ISM) Code [41]. To further provide guidance for maritime cyber resilience operations, the IMO in 2022 released the Guidelines on maritime cyber risk management under the MSC-FAL.1- Circ.3-Rev2. The document's intent is to embed cyber resilience principles for operations as states a high-level perspective of maritime cyber risk management and adopts the National Institute of Standards and Technology (NIST) framework with Identify, Protect, Detect, Respond and Recover as the elements of maritime cyber management [42]. Both technological resources (e.g. hardware and software) and workforce resources (e.g. ROC operators) are considered crucial for organisations' ability to achieve cyber resilience [43, 44].

From the workforce resource perspective, achieving UARSVO-related competences (Knowledge, Skills, Abilities and Behaviours) for maritime cyber security will be required for ROs as well as for UARSVO companies to maintain cyber security standards [33, 45]. At the international level, RO competences can be seen within the 2022 standard DNV-ST-0324 competence of ROC operators which introduces cyber security and cyber-attack competences under the emergency handling section [5]. Further clarification of competence standards for MASS RO was provided by the MASSPeople working group's submitted document for the IMO Intersessional Working Group on MASS in September 2023. This document includes cybersecurity competences at the (1) support level for implementing cyber-protection measures, (2) operational level for operating cyber-protection measures and responding to abnormal and emergency scenarios (including a cyber-attack), and (3) management level for managing cyber-protection measures [46]. Academically, [47] demonstrated a potential solution to develop standardised cyber security competences with the use of the NIST cyber security framework, which works with IMO's interest in NIST. However, for those RO competences to be developed, effective training must be implemented with the use of appropriate methods. As highlighted in the recommended practice by DNV [4], periodical training is also an essential part of continuous development as well as ROs competence retention. As

an example, the training course program created by [48] with the use of a survey provides a proposal on how MASS could be integrated within METIs and highlights the identification, prevention and mitigation of cyber-attacks within the main four competences. Moreover, their course guide proposal indicated in the course timetable proposal that 35% of the total hours were specified to be dedicated to cyber security and data management. However, that training course programme was created only using a questionnaire, and there was no participation from maritime cyber security experts or international maritime Subject Matter Experts (SMEs). This paper fills in the research gap for the development of more thorough maritime cybersecurity competences that could serve as a foundation for constructing a training framework focused on maritime cybersecurity resilience for RO.

2.3 *Training for Maritime Cyber Security Resilience UARSVO*

In 2015, a collision in the River Humber (UK) between a pure car carrier and a RoPax ferry occurred as the pilot experienced disorientation due to "relative motion illusion" as well as visual constraints (caused by the limitations of bridge design), which led him to take incorrect actions [49]. This accident serves as an example of how spatial disorientation can affect navigators in crewed and remotely operated vessels perceiving motion in a direction that is perpendicular to the actual true motion. This could also cause automation surprise if the RO perceives the instrumentation performing unexpectedly when compared to their own visual cues [50]. As shown by the accident and examples in [51], MASS can be highly susceptible to cyber-attacks and that the complexity of operations could increase if a cyber incident (as defined in Table 2) was the causal factor. An example of this can be seen with the experienced mariners' response towards different cyber incident scenarios onboard traditional ships replicated on a full bridge ship simulator using different types of cyber-attacks. Some public scenarios of cyber-attacks include Global Navigation Satellite Systems (GNSS) spoofing and jamming, jamming of rudder and engine controls, ransomware attack, taking control of the Ballast Water Management System (BWMS) and Automatic Identification System (AIS) spoofing [13, 52-56].

Currently, for the cyber incidents shown above, there have been some cyber incident management response plan procedures developed for crewed commercial vessels, such as detailed best practice checklists for detecting and responding to a cyber incident by [57] and the Cyber Emergency Response Procedure (CERP) by [58]. These provide different steps to follow with the use of a flow chart. Additionally, the CERP framework demonstrates that there are three clear types of iterations that can followed in the face of a cyber incident, and each one requires a different maritime stakeholder involved to either recover the vessel with normal operation or maintain the ship's operation in a reduced mode [58].

The Maritime Cyber Security (Marcy) training program involved different maritime stakeholders for crewed vessels has been developed and evaluated [59, 60]. The Cyber-SHIP lab also provides different types of multi-disciplinary maritime cyber security training for a wide range of participants [61]. However, while current cyber resilience management and cyber resilience training have been developed for crewed vessels, there is a unique gap to be addressed when mariners are transferred to operate vessels remotely for UARSVO. This is due to a reduction in Situational Awareness (SA) as ROs are solely reliant on data, technology, and connectivity when operating from an ROC. Moreover, a further reduction in SA that ROs can occur when facing a cyber incident as there may be no physical crew onboard to witness or respond to these incidents directly (e.g. for manual control). This paper attempts to address this need for existing mariner training on cyber security to be expanded and adapted to ensure ROs are equipped with the required competences to interact with digital systems for effective HAT in maritime cyber security resilience for UARSVO [13].

Table 2. Definitions for cyber-related terms within MASS are based on [3].

Term	Definition
Cyber Security	The security of digital systems, software, and the data/information they hold across the autonomous ships themselves and related infrastructure such as Remote Control Centers (ROCs).
Cyber Resilience	Resilience of MASS and ROC systems ensures that key operations can safely continue despite an active cyber attack affecting systems and/or data.
Cyber Defense	Digital defenses for MASS and ROC are solutions that prevent a cyber attack from happening, entirely or partially, such as firewalls.
Cyber Physical	For the robotics and operational technology (OT) aspect of MASS, cyber physical refers to the risk of physical impacts (e.g., delay, physical damage, loss of cargo) due to a cyber- related incident.
Cyber Attack	A cyber attack for MASS in this chapter will by default imply cyber physical attacks. If an attack is Information Technology (IT) only, it will be stated as an IT cyber attack. This implies an attacker and excludes error.
Cyber Incident	An active cyber attack, passive attack, or error involving digital assets (e.g. the latency of messages, and the contest of messages or connectivity availability between ROC and the MASS vessel)

3 METHODOLOGY

For this research, an inductive approach (or "bottom-up") qualitative methodology was used as it allows an analyst to identify patterns of why a phenomenon is happening through data [62-64]. This approach provided flexibility, developing themes within the data. It also added credibility and validity to the research outcomes without using pre-existing coding framework constraints [65-67]. With this approach, this paper examines which strategies could best enhance HAT in maritime cyber security resilience for UARSVO from both an end-user and an interdisciplinary perspective. This contributes to the proposed hybrid Design Research Methodology (DRM) and Human Centre Design (HCD) (International Organisation for Standardization (ISO) standard 9241-210:2019) iterative approach for the development of a HAT training framework in maritime cyber security resilience for UARSVO [68, 69]. DRM performs as the primary expansive methodological framework for design research in this research, which can be applied to a variety of research disciplines. DRM methodology provides an effective rigorous approach and an

efficient measurable criterion throughout the different stages of this methodology to answer and assess the development of each research question [68]. However, as DRM is not end-user focused, HCD methodology has been integrated to embed the user in the design, development, testing and evaluation iterations between activities so that the user, the user tasks, and the environment can be explicitly understood. The operator's involvement in activities with all stakeholders (within UARSVO) through all research stages will help provide the whole user experience, as well as multidisciplinary perspectives and skills [69].

3.1 *Selection and Sampling of Interview Participants*

The selection of interview participants for this research used purposive sampling, a commonly used qualitative research analysis for selecting a specific sample of participants from the overall population [70-72]. This method helped attain rich and in-depth data on this paper's research topic from 76 representatives across key stakeholders. All participants selected were Subject Matter Experts (SMEs) from different maritime organisations across the MASS industry, as shown in Table 3 [73]. Although all participants currently work in the maritime (except one in the space industry), some participants had previous experience in the aviation (n=3), space (n=2) and automotive (n=2) industries and maritime cyber security (n=18). This can be seen in Table 4, within participants' varied experiences, 21 participants were former mariners holding a Certificate of Competency (COC) as either a Deck (17 participants), Engine (3 participants) or Electronic Technical (1 participant) Officer occupying a key position/role within different maritime organisations. Participants' experiences as a group (experience participants had accumulated within maritime and/or other industries) varied, as shown in Table 4, with 43% of them having more than 15 years of experience as a group. Moreover, as shown in Figure 1, the participants' occupational location was from 16 different nations across Europe, Asia, North America and Oceania.

Given the diversity of specialised groups that needed to be included, it was not possible to do this research with less than ten interviews from only one key MASS stakeholder. To best capture opinions across many topics and from many stakeholders, the snowball sampling method was used to gain a novel, holistic, view [74]. However, unlike previous research, which snowballed for one topic, this was an iterative process where several topics were snowballed. Interviews continued until data saturation was achieved, with fewer new themes or data emerging. This showed that homogeneity amongst participant data, as well as consistency in findings from the different stakeholder groups, could be achieved [75, 76]. It was found that, for the umbrella topic of ROC cyber security training, 76 interviews were needed to fully explore and identify the diverse perspectives and shared themes across multiple international and interdisciplinary stakeholder groups (as well as unique group- specific insight) to obtain data saturation [77].

Table 3. Interview participant's demographics (source: author).

Key Group of MASS Stakeholders	Response N per Group	MASS Stakeholders	Response N
International Organisations	11	Non-Governmental Organisations (NGO)	5
		Classification Societies	4
		Insurance	2
Research & Academia	15	Maritime Cyber Security	6
		Unmanned Aerial Vehicles	1
		Maritime IoT and Mobile Networks	2
		MASS	3
		Maritime Business and Supply Chain	1
		Maritime Regulation and Policy	1
		Marine Biology	1
National and Regional	15	Government	2
		Coastal Administration	1
		Accident Investigation	2
		Hydrographic Office	1
		Military Navy	4
		Port Authorities	2
		Pilotage Service	3
Industrialists and Resource Providers	14	Technology Provider	5
		Ship Builders	3
		Maritime Cyber Security Service	3
		CoC Training Provider	1
		RO MASS Training Provider	2
Shipping Companies and Future Workforce	20	Shipping Companies	5
		MASS Shipping Companies	3
		Deck Cadets	12
		Total N of Participants	76

Table 4. Interview Participant's demographics (source: author).

Demographics	Variable	Response N	Response Proportion %
Merchant Navy Certificate of Competency (CoC) holders and Candidates	Deck Officer or above	17	22.37
	Engineer Officer or above	3	3.95
	Electronic Technical Officer	1	1.32
	Deck Officer Cadets	12	15.78
	None CoC Holders or Candidates	43	56.58
Experiences as Group Represented (in Years)	0-1 year	10	13.16
	2-5 years	8	10.53
	6-10 years	7	9.21
	11-15 years	18	23.68
	Above 15 years	33	43.42

Figure 1. Countries covered according to participants occupational location (source: author).

3.2 *Data Collection and Ethics*

Semi-structured interviews, also known as moderately structured interviews were our primary means of data collection [78]. This fostered an opportunity to address

questions from a clear list of thematic issues with flexibility in exploring new issues as they arose dynamically [79, 80]. It gave the interviewees an opportunity to develop ideas and provide open-ended answers so that participants could elaborate on points of interest through personal experiences [63, 81]. To ensure that during the investigation, all perspectives were sufficiently covered, an interview guide was used (see topics in Table 5) [81]. This has been developed using previous research by [13] on training for ROs in maritime cyber resilience for UARSVO so that the method used was in line with the DRM and HCD methodologies' iterative processes [68, 69]. During the interview, a Microsoft PowerPoint was shared to introduce IMO's vision for the development of the MASS Code, responsibilities for MASS, and degree levels of autonomy as per IMO and interview guide questions. This ensured a common base of knowledge for all participants before starting.

Prior to starting each semi-structured interview, participants obtained via email in English, the established working language for this study:

1. A participant information sheet (with research aims and objectives; contact details of the research investigator and director of studies), semi-structured interview questions guide (for participation involvement);
2. Consent form (with rights to withdrawal, confidentiality and anonymisation) and verbal confirmation were asked to acknowledge that all documents were understood as well as to clarify any concerns or questions [65, 82].

With consent, data in the form of audio and video recordings were collected for each interview. Recordings were automatically transcribed via Microsoft Teams, used for both online (57) and in-person (19) interviews. All these interviews occurred between April 2024 and October 2024. The interviews lasted from 26 minutes to 2 hours and 50 minutes, with a mean of 54 minutes. The total time accumulated performing all interviews was 68 hours and 40 minutes (2.86 days).

Due to confidentiality, interviewees' responses were not given by any identifying details or pseudonyms. To prevent any identification, response comments were provided as a group and gender neutral for General Data Protection Rights (GDPR) to make results public [83].

Table 5. Semi-Structures Interview Guide Questions.

Theme	Questions
1. Opening Questions	1.1 Before we start, do you have any questions regarding the consent form and/or information sheet? Or any questions or comments regarding this research? 1.2 When and why did you begin your career in the Maritime Industry? What made you start a career pursue a career in the maritime industry? 1.3 What is your current Expertise? How is a normal day at your current job? 1.4 Experience (years/months)? Type of ships (age/flag) or companies you have worked on?
2. HAT Relationship for UARSVO	2.1 What do you think the human role and responsibilities will be for navigation officers in Autonomous and Remote Vessel Operations? Which parts will remain the same, or be different, and why? 2.2 What challenges do you foresee for operators of remote-controlled vessels (e.g. trust and reliance on navigation equipment information from sensors to safely navigate)? What type of standards and training do you consider vital for safe navigation when operating from a Remote Operations Centre? 2.3 What is your view on the Human-Autonomy Teaming relationship for Autonomous and Remote Surface Vessel Operations (e.g. decision-making process for different modes of human operation such as monitoring, supervision and remote control)? Are there particular operations that will be affected more? If so which ones and why?
3. HAT for Maritime Cyber Security Resilience	3.1 What types of cyber threats could an autonomous vessel be vulnerable to (e.g. GPS Spoofing)? What catastrophic events could this cause? 3.2 How could this attack be detected, reported, contained or eradicated by a Navigator at a Remote Operations Centre? 3.3 How do you think Human-Autonomy Teaming can enhance maritime cyber security resilience (e.g. strategies to resolve a potential machine error and/or reduce the magnitude of the incident)? 3.4 What type of training and procedures could help the operator to enhance maritime cyber security resilience? Would this training involve personnel across all levels of the organisation with external organisations (e.g. during cyber incident management)?
4. Debrief and Future Research Engagement	4.1 Thank you for your participation. Do you have any questions or comments regarding this research? 4.2 Would it be possible please to keep your name and contact details to be contacted to participate in the next stage of this research?

3.3 *Data Analysis and Fieldwork*

The data from the semi-structured interviews was examined with thematic analysis, as per [75] 's six- step process. This allowed us to identify and organise patterns in content and meaning [84, 85].

Familiarisation of data began by checking the transcribed transcripts saved as unique documents alongside the audio recordings. These transcripts were made available to participants for review, and the process was further supported by written field notes to ensure the quality and reliability of transcriptions [86]. Secondly, the anonymised and reviewed transcriptions were uploaded to NVivo software for the Generation of Codes, Combining Codes Into Themes, Reviewing Themes, Determine Significance of Themes and Reporting of Findings [112]. The gathered data was analysed descriptively (focused on what the data shows) and interpreted inductively (focused on why the patterns exist) [66, 75, 87]. On completion of the data analysis, four main themes arose in conjunction with sub- themes as presented in the contextual model in Section 4 below, which serves as the foundation for presenting the results obtained.

4 RESULTS AND ANALYSIS

The interview themes that emerged when discussing HAT strategies for maritime cyber security resilience in UARSVO, as shown in Figure 2, were used to divide this research into four topics: "UARSVO" overview, "Maritime Legislation for UARSVO", "Maritime Cyber Security Resilience in UARSVO" and "Maritime Cyber Security Training for UARSVO". Additionally, a graph demonstrating the occurrence difference between key groups of MASS stakeholders is shown for each theme (as per Figure 3) and for sub-themes within each theme

section (as per Figures 4, 6, 8 and 9). However, the "other industries" group was omitted from the graphs due to a low number of participants. Results from this group were embedded as occurrences within the table of total occurrence for each theme and sub-theme (which is below the graph) in each Figure. As shown in Figure 3, of the main four themes within the table of total occurrences, "UARSVO overview" was discussed the most, with 1,016 occurrences; on the other hand, "Maritime Cyber Security Training for UARSVO" was discussed the least, with 411 occurrences. Furthermore, amongst key groups of MASS stakeholders, "Maritime Legislation for UARSVO" was discussed the highest by national and regional organisations, with 247 occurrences, whereas "Maritime Cyber Security Training for UARSVO" was discussed the least by international organisations, with 41 occurrences.

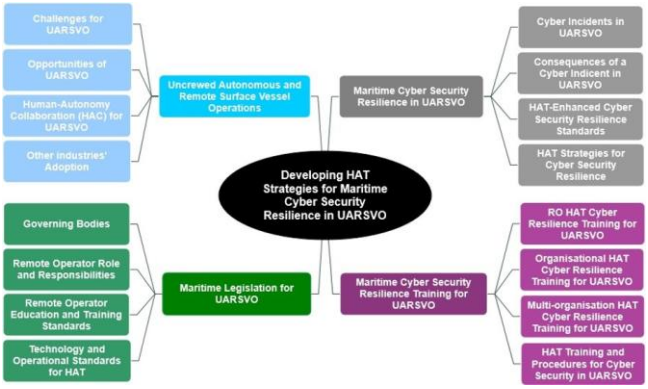
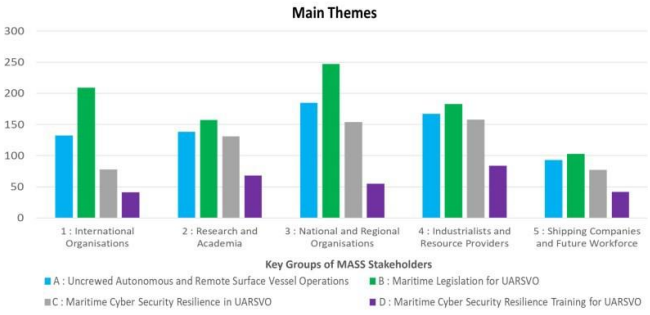


Figure 2. Emerged main themes and sub-themes with the use of NVivo from performed semi- structured interviews (Source: Author).



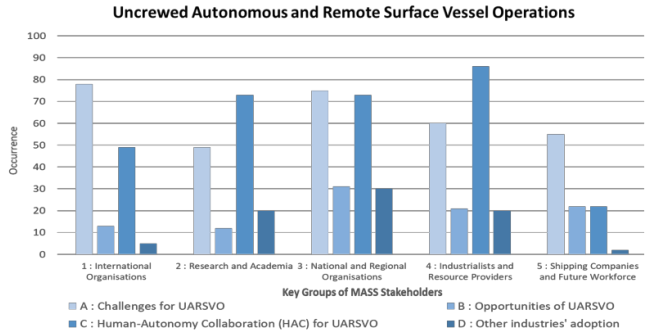
Main Themes

Theme	Occurrence	Description
Uncrewed Autonomous and Remote Surface Vessel Operations (UARSVO)	1016	Outlines an overall overview of participants' perspectives towards UARSVO and its introduction
Maritime Legislation for UARSVO	1384	Outlines participants views on the maritime legislation required for remote operators in UARSVO as well as governing bodies
Maritime Cyber Security Resilience in UARSVO	981	Describes maritime cyber security resilience overview and approaches provided by participants for UARSVO
Maritime Cyber Security Resilience Training for UARSVO	411	Outlines and details of maritime cyber security resilience training at different levels of analysis from participants' perspectives for UARSVO

Figure 3. Main themes identified with the use of NVivo from semi-structured interviews performed (Source: Author).

4.1 *Uncrewed Autonomous and Remote Surface Vessel Operations*

Figure 4 demonstrates that of the four sub-themes within "UARSVO", "HAC for UARSVO" was discussed the most, with 408 occurrences. Conversely, "Other industries' adoption" was discussed the least, with 103 occurrences. Furthermore, amongst key groups of MASS stakeholders, "HAC for UARSVO" was discussed the most by industrialists and resource providers, with 86 occurrences, whereas "Other industries' adoption" was discussed the least by shipping companies and future workforce, with 2 occurrences.



Uncrewed Autonomous and Remote Surface Vessel Operations (UARSVO)

Theme	Occurrence	Description
Challenges for UARSVO	388	Identifies participants' overall main challenges perceived for UARSVO
Opportunities of UARSVO	117	Identifies participants' overall main opportunities perceived for UARSVO
Human-Autonomy Collaboration (HAC) for UARSVO	408	Describes HAC from participants' perspective towards UARSVO
Other industries' adoption	103	Outlines the adoption of other industries' approaches for UARSVO identified by participants'

Figure 4. Main sub-themes emerged from the theme Uncrewed Autonomous and Remote Surface Vessel Operations (Source: Author).

4.1.1 *Challenges for UARSVO*

56 participants (73.69%) were mainly concerned about operational challenges for MASS, especially for coastal waters and port arrival/departure operations such as pilotage operations. The primary reasons were concerns about MASS performing safe passage through heavy traffic in different points around the globe, while being in compliance with the Convention on the International Regulations for Preventing Collisions at Sea 1972 (COLREGS). In addition, there were concerns between crewed and uncrewed vessels in conjunction with complex vessel manoeuvres such as leaving anchorage (e.g., Singapore Strait), narrow channels for vessels in head-on interactions, mooring operations, and adverse weather conditions [88]. Participants expressed concerns about communications with the MASS vessel from ROC and the MASS vessel communicating with other vessels, Vessel Traffic Service (VTS) and other entities. Additionally, significant challenges for the existence of uncrewed vessels included the vessels' constant maintenance requirements during international voyages.

Human factors and lack of HCD when developing systems were ranked second among challenges as operators may experience a loss of realism due to digitisation of operations, physical detachment, and loss of situational awareness. Participants also discussed MASS technology readiness challenges in sensor discrepancy for data received or lost, as well as latency or connectivity availability of the MASS vessel. As per participants' views, the challenges of technology readiness extended to trust and reliance on automation and navigation equipment and information from sensors. Additionally, the lack of workforce readiness (future workforce shortage and unqualified workforce) and infrastructure supporting these operations were agreed upon as the maritime industry is slowly keeping up with technology. Moreover, participants perceived that the maritime industry is not yet mature in cyber security, operational law and contractual law, MASS technology readiness costs (including economic consequences due to loss of MASS), and the industry stakeholder shift (such as the product and service provider becoming the new ship owner of MASS).

4.1.2 *Opportunities for UARSVO*

Participants spoke of major opportunities that could be available with the operational application of UARSVO, highlighting that these opportunities will depend on vessel type, operation, location, weather and traffic. Individuals indicated that, based on the relevant experience, opportunities have risen for smaller ships in size, such as ferries, survey vessels and cargo vessels operating in or near coastal waters with better connectivity, lower maintenance required, and more redundancies (to physically intervene whether it is to repair or hot swap the vessel). It was also highlighted that, globally, zones for UARSVO could include coastal waters and open seas, as these were seen as less risky environments, especially for the parts of the voyage where the autopilot onboard a vessel is already being used. The second most referenced topic was the opportunity to make safer and more efficient operations. Many participants discussed how autonomy could reduce human error with situational awareness optimisation, vessel predictive maintenance, reduction in vessel operational costs and crew costs, as well as more sustainable operations due to vessel optimisation. An additional suggestion was opportunities to create dedicated shipping lanes and/or vessel lights and shapes (as per COLREGS) for MASS vessels when operating remotely or autonomously for safer operations in a mixed environment with crewed vessels.

4.1.3 *Human-Autonomy Collaboration (HAC) for UARSVO*

In this sub-theme, the most frequently referenced topic was the significance of the HAT symbiotic relationship. Participants stated that the ANS would carry out 99% of the tasks according to the goals and parameters set by humans, with just 1% reserved for critical decision-making by humans in situations where the ANS is too limited to make a safe decision. Individuals stated that this 1% was as valuable as the 99%, as the human in the loop could prevent large catastrophic scenarios with a single intervention. For this, it was stated that gradual trust in technology increases as technology readiness and maturity levels are proven with performed safety and security reliability records as well as communication transparency of decision-making from ANS to ROs at ROC and vice versa.

From the participants' perspective, this maturity level could help to attain clarification in liabilities for insurance coverage when ANS is with the conduct of the vessel and an accident occurs due to automation surprise. Additionally, individuals stated that clear alarms and indications from the ANS to the RO for seamless handovers when transitioning between degrees of autonomy could help overcome these challenges.

As shown in Figure 5 within HAC, according to IMO degrees of autonomy (as shown in Table 1), participants expressed that at degree 0 should be added as there is no autonomy in direct control (e.g. manual control). Participants stated that degrees 1 to 3 should be classified as HAH as the navigator has the conduct of the ship and could have ANS for decision support. In degree 4, it was stated that it should be classified as HAT due to ANS becoming similar to a junior Officer of the Watch (OOW) with the conduct of the vessel with oversight by the Master and RO. The RO oversight was stated as standby (availability at ROC), monitoring (assessing ANS) and supervision (verification of ANS and assisting with decision-making). Additionally, per IMO's definition for degrees 3 and 4, from participants' perspectives, this was defined as uncrewed rather than unmanned, as a passenger ferry could operate autonomously without crew onboard but transporting passengers.

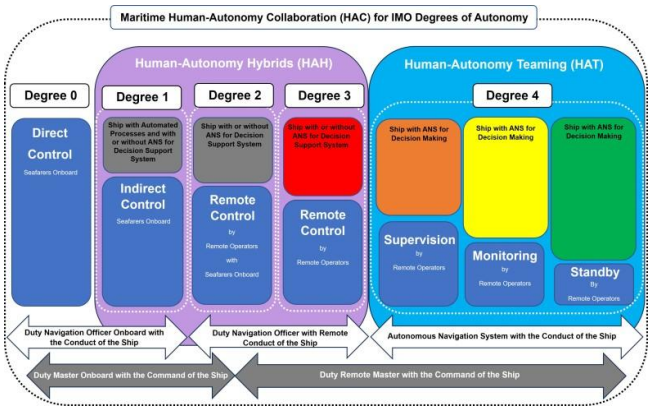


Figure 5. Maritime Human-Autonomy Collaboration (HAC) framework according to the IMO degrees of Autonomy (Source: Author).

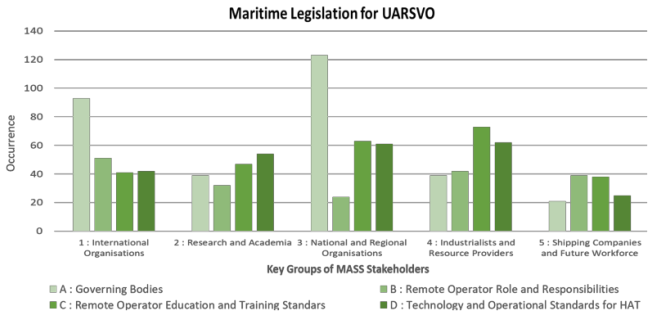
4.1.4 *Other Industries' Adoption*

Aviation was the industry most frequently mentioned among other industries' adoption, regarding air traffic control operations. In particular, individuals viewed their highly standardised communication, handover procedures implemented, and duration of shift rotations according to human cognitive ability as valuable practices to adopt within UARSVO for RO training. This extended towards aircraft pilots' training and refreshment training using scenarios and simulators. Second-ranked was the space industry, where some participants with relevant backgrounds stated that humans always remain in the loop for space operations. In regard to space training, the just-in-time approach to training adopted by the National Aeronautics and Space Administration (NASA) was suggested for UARSVO as it is focused on providing the specific training, information and resources when needed. Furthermore, from participant's perspective, RO training conducted for military operations for Unmanned Aerial Vehicles (UAV) offers approaches that could be effective for RO in UARSVO, such as the adopted specialised UAV operator training approach to acquire the required airmanship skills as UAV operators without previous experience as aircraft pilots.

4.2 *Maritime Legislation for UARSVO*

Figure 6 illustrates the four sub-themes discovered in this research within the theme "Maritime Legislation for UARVO". Of these four, "Governing Bodies" was discussed the most, with 474 occurrences; on the other hand, "Remote Operator Role and Responsibilities" was discussed the least, with 242 occurrences. Furthermore, amongst key groups of MASS stakeholders, "Governing Bodies" was discussed the most by national and regional organisations, with 123 occurrences, whereas "Remote Operator Roles and

Responsibilities" was discussed the least by national and regional organisations, with 21 occurrences.



Maritime Legislation for UARSVO		
Theme	Occurrence	Description
Governing Bodies	474	Describes the governing bodies at different levels of analysis and the interconnection between them from participants' viewpoint for UARSVO
Remote Operator Role and Responsibilities	242	Describes remote operators' roles and responsibilities identified by participants for UARSVO
Remote Operator Education and Training Standards	380	Describes participants' views on remote operators' education and training standards for UARSVO
Technology and Operational Standards for HAT	288	Describes participants' perspective towards required technology and operational standards for HAT in UARSVO

Figure 6. Main sub-themes emerged from the theme Maritime Legislation for UARSVO (Source: Author).

4.2.1 *Governing Bodies*

As shown in Figure 7, the following governing bodies were identified at macro, meso, and micro levels for UARSVO. The meso level received the most references concerning supporting organisations, indicating that port authorities should require the infrastructure and technology necessary to assume the risk of handling a MASS vessel for port operations. Participants also noted that Vessel Traffic Service (VTS) plays a crucial role in MASS surveillance within their designated controlled areas, relying on close collaboration with the ROC to ensure the safe coexistence of MASS with crewed vessels, alongside providing assistance in managing cyber incidents. Challenges regarding national organisations granting MASS clearance to enter territorial waters when operating in autonomous mode or under remote control from another country were identified. Participants emphasised the need for shipping companies to designate a ROC in the country where the vessel will primarily operate. Additionally, it was asserted that this could facilitate access for the National Accident Investigation Organisation (NAIO) to Voyage Data Recording (VDR) data at the ROC of that country. To support UARSVO accident investigations, adherence to ANS's standards for explainability in decision-making was deemed essential upon receipt of VDR data. For this scenario, participants highlighted the importance of close collaboration with technology providers and during operations with the ROC for troubleshooting purposes.

The second most referenced level was the macro. Individuals expressed that the IMO is leading the charge on international regulations with the MASS Code, emphasising the need for close collaboration with flag states, classification societies, and other entities. There was a call for a new section on MASS to be included in the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), similar to what was added for STCW for Fishing Vessel Personnel (STCW-F) [89]. Participants also raised concerns regarding the contract of carriage and insurance challenges that may arise if a software error from an ANS is detected after the MASS vessel is delivered from the shipyard to the ship owner. In this scenario, the vessel enters the owner's orbit, obligating them to exercise due diligence in ensuring the vessel's seaworthiness before and at the beginning of the voyage. From a micro-level perspective, pilots were regarded as essential for both arrival and departure during UARSVO, providing critical local port knowledge and preventing significant accidents (e.g. the pilot saved lives by contacting from the container ship Dali to halt traffic on the Francis Scott Key Bridge (Baltimore, USA) prior to a potential collision with the bridge) [90]. Participants also noted communication challenges due to the vessel's remote command by the master, suggesting that command of the vessel should be transferred to the pilot during pilotage waters.

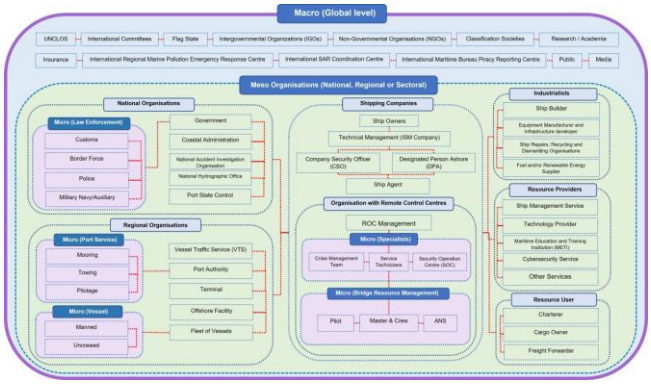


Figure 7. Operational Levels of Analysis for Uncrewed Autonomous and Remote Surface Vessel Operations (UARSVO) (Source: Author).

4.2.2 *Remote Operator Roles and Responsibilities*

The roles and responsibilities of RO most frequently mentioned by participants were emergency handling, passage planning, and cyber security for systems assurance as primary roles, with special emphasis on maintaining internal communication within ROC personnel and the company and external communication with other stakeholders. Other roles and responsibilities listed by the frequency of references included collision avoidance, preventive maintenance, cargo operations, ship stability, ship handling, and alternative fuel awareness. Participants noted that these roles and responsibilities could vary depending on the level of autonomy. It was also mentioned that these could depend on the capabilities of each shipping company's ROC, such as following the sun operations, manning of ROC personnel, vessel operation types, vessel types, the number of vessels operating from an ROC, and whether a specialist RO was created depending on the application.

The roles and responsibilities of the MASS Master were highlighted as likely to shift to a more specialised role with multi-vessel responsibilities for vessels operating in the open sea. Participants expressed the need to define the number of vessels a Master could be in command of, in which circumstances, and also the required backup Master(s) needed for redundancies. For operations in which the ANS is with the conduct of the MASS vessel, participants expressed that the Master should be responsible for the vessel but should not have full command responsibility as it may not be fully aware of the MASS vessel situation. Additionally, as the operation will be heavily reliant on technology, the Master was also seen as responsible for the performance of the systems and cyber security.

4.2.3 *Remote Operator Education and Training Standards*

Participants' most referenced topics within the RO education and training standard were the need for training standardisation around technology operated from ROC and cyber security of that technology as new education, training and awareness on digital systems. Additionally, special training was suggested for scenarios where latency and connectivity can be experienced from ROC, SA acquisition from navigational equipment operated from ROC, and system diagnosis for equipment fault. Along with this, participants stated the shift needed for RO candidates to attain training on electronic navigation equipment from the start and learn traditional negational methods as a backup. Individuals perceived that ROs would need similar training to VTS Officers as they will be required to have similar rational critical thinking, shared decision-making, cognitive ability to focus and duty duration. The importance of ROs' mental well-being was also highlighted concerning the risk of social life side effects when performing remote operations, as ROs will encounter shoreside social challenges (no longer working in isolation at sea). From the participants' perspective, training will be necessary to fulfil the roles and responsibilities listed in 4.2.2. Participants stated that METI's responsibility would be to equip ROs with transferable skills, enabling this workforce to become more employable, resourceful, and adaptable, as current mariner training was perceived to lack transferable skills ashore.

Concerning the training methods required for ROs, the most frequent response was the advantage of onboard mariner training for remote operations, as it imparts essential seamanship skills.

Participants deemed it safest to implement short- and medium-term ROs with sea time experience (mariners holding a CoC transitioning to become an RO). After a training maturity was attained and based on the experience gained from the training provided for those ROs, opportunities for RO training without sea time experience were deemed as an opportunity to be established in the long term. To achieve this, a strong emphasis was placed on establishing simulator-based training that could offer meaningful sea time in a safe environment for the roles and responsibilities required from ROs at the ROC. This includes reinforcement and refresher training for ROs, as well as a new type of training focused on how to interact with an ANS. Furthermore, individuals from company-based training viewed it as essential for organisations with an ROC to incorporate simulator-based training within their own ROC frameworks, providing a standardised familiarisation for ROs with the necessary time to develop remote situational awareness from the ROC. Alternatively, the use of Virtual Reality (VR) was mentioned to achieve a general experience and feel of real-world scenarios, but for limited periods of time, as some participants experienced nausea.

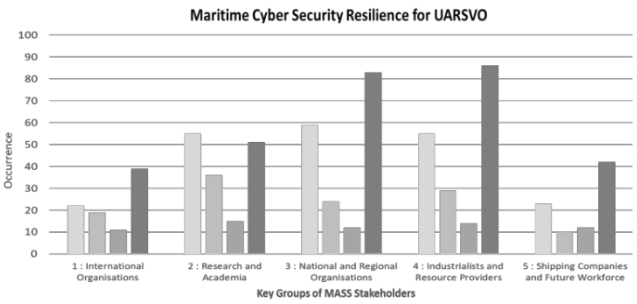
4.2.4 *Technology and Operational Standards for HAT*

The topic that received the most occurrence within this sub-theme was the standardisation and certification of safety assurance of autonomy and ROC. Individuals seem essential to attain a fail-safe mechanism for MASS when operating outside the operational design domain, such as dropping the anchor for emergency anchorage, stopping the vessel to hold position, assuming remote control by RO or performing a hot swap with another vessel. Additionally, redundancies for a backup ROC, communication channels and navigation equipment made by a manufacturer were stated. For this, participants perceived that a standardisation of ANS alarms and indications for RO would be needed to be created in combination with an agnostic ROC user interface for visuals (e.g. when multiple ROCs are operating the same vessel) and a bird's eye view set up from ROC (rather than traditional bridge ship view). This extended to the MASS safety and operational procedures with the need for a standardised risk assessment similar to the System Theoretic Process Analysis (STPA) approach or Risk Based Assessment Tool (RABAT) by the European Maritime Safety Agency (EMSA) [91, 92].

The second-most frequently discussed topic was the standardisation of industry best practices, such as seamless handovers for the command of a MASS vessel between ROCs on international operations, standardisation of communications, manning of ROCs for the different phases of the voyage, and minimum frequency of training for RO. Alternatively, new standards for expansion and clarification of the IMO degrees of autonomy were requested to define clear roles and responsibilities between humans and autonomy to acquire an international unified taxonomy and terminology for maritime autonomy.

4.3 *Maritime Cyber Security Resilience in UARSVO*

Figure 8 demonstrates that of the four sub-themes within the theme "Maritime Cyber Security Resilience in UARSVO", "HAT Strategies for Maritime Cyber Security Resilience" was discussed the most, with 444 occurrences; on the other hand, "HAT Enhanced Cyber Security Resilience Standards" was discussed the least, with 67 occurrences. Furthermore, amongst key groups of MASS stakeholders, "HAT Strategies for Maritime Cyber Security Resilience" was discussed the most by industrialists and resource providers, with 86 occurrences, whereas "Consequences of a Cyber Incident in UARSVO" was discussed the least by shipping companies and future workforce, with 10 occurrences.



Maritime Cyber Security Resilience in UARSVO		
Theme	Occurrence	Description
Cyber-Incidents in UARSVO	297	Describes the main cyber-incidents identified by participants for UARSVO
Consequences of a Cyber Incident in UARSVO	173	Outlines the overall consequences of a cyber incident perceived by participants for UARSVO
HAT Enhanced Cyber Security Resilience Standards	67	Describes participants' view towards standards to enhance cyber security resilience when using HAT technology for UARSVO
HAT Strategies for Cyber Security Resilience	444	Outlines main HAT strategies detailed by participants towards maritime cyber security resilience for UARSVO

Figure 8. Main sub-themes emerged from the theme Maritime Cyber Security Resilience in UARSVO (Source: Author).

4.3.1 *Cyber-incidents in UARSVO*

Within the sub-theme of cyber incidents in UARSVO, participants' most frequently referenced spoofing of the MASS vessel's Global Navigation Satellite System (GNSS) and jamming of GNSS. For the secondary category, the most mentioned is an incident caused accidentally due to personnel incompetence, ransomware and Automatic Identification System (AIS) spoofing. The third category encompassed Denial of Service (DDoS) attacks, man-in-the-middle attacks, adversarial AI, social engineering, and insider threats.

Participants noted that the primary threat actors they believed responsible for these cyber incidents were predominantly nation-states, owing to their access to resources and expertise in the maritime field, which enables sophisticated cyber operations. The next most mentioned actors were terrorists and pirates, who tend to engage in less sophisticated cyber activities. Others cited include activists, criminals, and those involved in business espionage. Participants indicated that the principal motivations behind these cyber incidents were likely financial gain and reputational damage.

4.3.2 *Consequences of a Cyber Incident in UARSVO*

All except for one participant indicated that the consequences of a cyber incident in UARSVO would be either the same or higher. Participants' major concern was that a cyber incident could affect critical infrastructure due to gaining control of the MASS vessel steering and propulsion system; such examples given were a MASS vessel colliding with another vessel or infrastructure, grounding, blocking a critical choke point, causing environmental damage, and supply chain disruptions. The secondary consequences were company data loss and loss of property, life, and reputation. Other less frequently mentioned were cyber incidents affecting port Operational Technology (OT) and national security. Amongst the higher consequence group, participants perceived that a cyber incident compromising ROC could affect an entire company's fleet and the worldwide economy due to the connectivity of operations. Conversely, only one participant opposed, arguing that the consequences are lower as there could be no loss of life or environmental damage scenarios, considering there may not be anyone onboard and that alternative fuel or electric batteries may already be in use.

4.3.3 *HAT-Enhanced Cyber Security Resilience Standards*

Among the standards and frameworks for maritime cyber resilience, the primary ones mentioned by participants for continuity were the Unified Requirements (UR) established by the International Association of Classification Societies (IACS) alongside the E26 (Guidelines for Cyber Resilience of Ships) and E27 (Guidelines for Cyber Resilience of On-board Systems and Equipment), which began to be applied to new ships from 1 January 2024. Additionally, the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 standard for Information Security Management Systems (ISMS) was noted, along with the NIST framework adopted by the IMO. Furthermore, participants indicated that greater emphasis should be placed on the standardisation of VDRs in UARSVO, as this would assist in investigating causal factors for cyber incidents.

Participants stated that training should be integrated from the beginning and embedded within the secure-by-design implementation for MASS as HAT-enhanced cyber security resilience standards. Participants perceive a need for the standardisation of training in maritime cyber security resilience at the international level, enabling nations to ratify and adopt international standards to their own national guidelines, thereby ensuring the safety and security of MASS vessels. To facilitate this, individuals believe that a gradual introduction is essential for progressively assimilating the new roles and responsibilities that come with maturity.

4.3.4 *HAT Strategies for Cyber Security Resilience*

The primary strategy highlighted by participants and analysed by the authors for HAT cyber security resilience in UARSVO was centred on system resilience, particularly through the provision of redundancies with other instruments during non-nominal operations when systems do not function as anticipated (such as using an Inertial Navigation System (INS) and the next generation of AIS which is VHF Data Exchange System (VDES)) [93, 94]. Sensor fusion was regarded as the most effective approach for achieving this, with the potential to employ an intrusion detection system integrated with AI to identify any cyber incidents, thereby minimising human error in such situations.

Participants also noted that a fail-safe mechanism should be established for MASS during a cyber incident, ensuring the redundancies mentioned earlier in 4.2.4 Technology and Operational Standards for HAT. Furthermore, individuals emphasised the necessity of new alert systems for cyber incidents regarding ROC, the ROC user interface, and the transparency of communication in decision- making from ANS to RO concerning the information gathered for SA and decision-making, which will be essential for verifying the integrity of systems and ensuring data quality. Additionally, individuals stated that a zero-trust architecture should be implemented for UARSVO, even though there are currently no ISO standards for this.

The second most significant strategy referenced was the Cyber Security Management System (CSMS) at the company level. The area most frequently identified as needing attention within the CSMS was the response procedure from the ROC during a cyber incident. This includes the procedure for assuming manual control of the MASS vessel, if necessary, during a work case scenario, as well as the decision-making process to follow in the event of a cyber incident. Participants also emphasised that a culture of cyber resilience should be embedded as part of organisational strategy, alongside risk assessments that incorporate multi-level safeguarding and a dedicated response system for cyber incidents to provide optimal assistance when required. Consequently, they emphasised the importance of having a checklist for work case cyber incident scenarios and conducting regular audits and assessments of these.

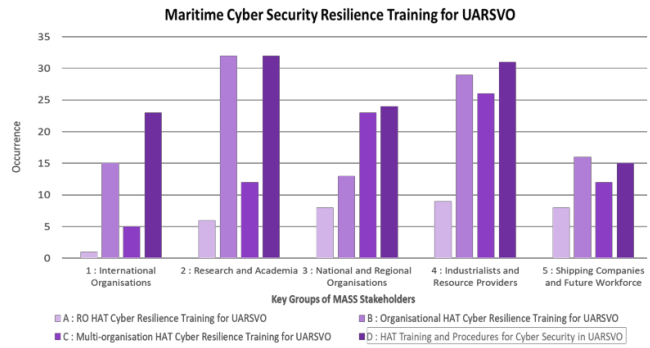
The third highest strategy mentioned was HAT training in maritime cyber security resilience for UARSVO, which is closely linked to the previous two. Individuals highlighted the importance of training in distinguishing between cyber-attacks and normal system failures (as this is currently a challenge faced within the maritime industry) and training for maximum cyber incident crisis scenarios. It was suggested that the development of these should be undertaken by flag states and classification societies but designed by the IMO. Additionally, the embedding of cyber-attacks as an emergency was proposed.

The fourth-mentioned strategy was a socio-technical systems approach from a multi-level perspective. Participants asserted that this could help strengthen the relationship between stakeholders during cyber incidents, such as exploring the best approaches in various scenarios to identify which team and individual are best suited to assume responsibility in a cyber incident.

Individuals noted that this could enhance information sharing and lessons learned across the maritime industry, such as developing a cohesive paperless report that is valuable across all technology suppliers and stakeholders, like the maritime single window established by the IMO from January 2024 for ships when entering a port but applied to cyber incidents [95].

4.4 *Maritime Cyber Security Resilience Training for UARSVO*

Figure 9 demonstrates that of the four sub-themes within the theme "Maritime Cyber Security Training for UARSVO", "HAT Training and Procedures for Cyber Security in UARSVO" was discussed the most, with 140 occurrences; on the other hand, "RO HAT Cyber Resilience Training for UARSVO" was discussed the least, with 38 occurrences. Furthermore, amongst key groups of MASS stakeholders, "Organisational HAT Cyber Resilience Training for UARSVO" and "HAT Training and Procedures for Cyber Security in UARSVO" were discussed the most by research and academia, with 32 occurrences, whereas "RO HAT Cyber Resilience Training for UARSVO" was discussed the least by international organisations, with 1 occurrence.



Maritime Cyber Security Resilience Training for UARSVO

Theme	Occurrence	Description
RO HAT Cyber Resilience Training for UARSVO	38	Describes RO cyber resilience training needed as perceived by participants for HAT in UARSVO
Organisational HAT Cyber Resilience Training for UARSVO	129	Describes organisations cyber resilience training needed as perceived by participants for HAT in UARSVO
Multi-Organisation HAT Cyber Resilience Training for UARSVO	104	Describes at a multi-organisational level the cyber resilience training needed as perceived by participants for HAT in UARSVO
HAT Training and Procedures for Cyber Security in UARSVO	140	Outlines participants' perception towards HAT training and procedures for cyber security in UARSVO

Figure 9. Main sub-themes emerged from the theme Maritime Cyber Security Resilience Training for UARSVO (Source: Author).

4.4.1 *RO HAT Cyber Resilience Training for UARSVO*

The most frequently reported topic within the RO HAT cyber resilience training was RO training on recognising and managing a cyber incident. Participants noted that these RO operators would play a crucial role, acting as the first human line of defence during a cyber incident, which may or may not involve additional collaboration with personnel from the ROC or external stakeholders. To address this, cyber awareness training and education were seen as needing different approaches for individuals with sea time experience (traditional mariners) transitioning to RO roles compared to those ROs lacking real sea time experience. Furthermore, participants indicated that ROs would need to learn cyber terminology to communicate with cyber analysts effectively and should grasp how systems operate to gain a foundational understanding that could assist the RO during a cyber incident.

4.4.2 *Organisational HAT Cyber Resilience Training for UARSVO*

Training at the operational level was the most frequent occurrence at the organisational level. There was a clear need among participants for a maritime cyber security expert or a technical operator who could work alongside or embedded within the navigation team in the ROC as individuals perceived challenges in combining the RO role with the cyber analyst. Moreover, participants emphasised that cyber analysts and the chief engineer of the MASS vessel will need to work closely with the RO and the ROC management during a cyber incident. Within the ROC for a cyber incident, two approaches were seen as viable for shipping companies with an ROC to adopt: either setting up a cyber crisis management team that constantly operates or key people among different departments forming the cyber crisis management team.

At the management level, participants believed that ROC management should require both operational and technical skills to effectively handle the responsibilities during a cyber incident, as previously mentioned. The ROC manager was viewed as closely collaborating with the organisation's fleet manager, Company Security Officer (CSO), and Designated Person Ashore (DPA). In some scenarios, as indicated by participants, the Security Operations Centre (SOC) (which could be within the ROC or third party) must feed that information to the ship owner and MASS Master. If it fails to, the SOC might determine that the MASS vessel is not seaworthy without the Master knowing it.

Therefore, the right information and training would need to be provided for the Master so that they can take the appropriate action when detecting a cyber-attack, as they are ultimately responsible for the command of the MASS vessel. Participants stated that in the UK, shipping companies are considered Operator of Essential Services (OES) under Network and Information Systems (NIS) regulation and that for incidents meeting the mandatory reporting thresholds, such as hampering the ability to deliver essential services (e.g. closing ports across the UK) should report to the Department for Transport (DfT) Cyber Compliance Team (CCT) no later than 72 hours (as per Part 3 of the Data Protection Act 2018) of the notifiable

incident has happened [96-98]. Consequently, individuals stated that it ultimately depends on the company's board-level culture whether the ship owner takes responsibility for addressing the cyber incident, which could potentially lead to micromanagement or whether this responsibility is delegated to technical management. If full trust is placed in the management team, the ship owner will be distanced from the cyber incident.

For this, training and standardised procedures to follow by the ROC team during a cyber incident were seen as essential, since the ability to quantify non-nominal operations uncertainty and how to act upon those uncertainties with tools such as checklists and up-to-date reporting records.

4.4.3 *Multi-organisation HAT Cyber Resilience Training for UARSVO*

Within multi-organisation HAT cyber resilience training, the meso level received the most occurrences, especially regarding technology suppliers. These organisations have encountered different challenges that could cause a cyber incident, incorrect system integration, improper use of equipment or another cause and perceived the need to receive a reported tracking back with how systems are operated and maintained. As vessels operate with many equipment manufacturers, they perceived that a single point of contact from all the Original Equipment Manufacturers (OEM) vendors would be needed for UARSVO to facilitate efficiency during cyber incident response collaboration with ROC. Other stakeholders were also regarded as directly involved during a cyber incident, such as the VTS, coastal authorities and port authorities intervening to help ensure the safety of the vessel in the vicinity of the designated area and providing backup assistance to the ROC operating the MASS vessel. Alternatively, NAIOs are seen as advantageous for collecting data on cyber incidents to provide the industry with valuable lessons from various scenarios, as in some cases, participants stated that NAIOs may be the first to identify that the cause of an accident was a cyber incident.

At the macro level, the insurance perspective for training during a cyber incident on UARSVO was seen as essential to proactively look at preventive measures, such as the provided identification of roles and responsibilities of the Company Financial Officer (CFO), negotiators, and lawyers during a cyber incident as well as coverage under the premium insurance for a cyber incident. Alongside this classification societies were seen as essential with the smart notations implemented for ships that use smart technology, which helps detect early any potential failure. At the micro level, participants stated that each micro-specialist during a cyber incident could assist in providing crucial information such as marine pilots, law enforcement entities and terminal operators. Consequently, individuals suggested the implementation of joint multi-disciplinary training exercises for cyber-incidents to help define roles and responsibilities internally and externally of the organisations and attain the needed joint experiential learning within ROC and UARSVO stakeholders.

4.4.4 *HAT Training and Procedures for Cyber Security in UARSVO*

For this sub-theme, the implementation of cyber security resilience training in UARSVO has been the most frequently mentioned. Participants indicated that current training and education on the latest cyber threat landscape should be provided to the maritime workforce. Individuals believe that a foundational level of training and awareness on maritime cyber security has been delivered at all competency levels in recent years since the release of Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems [41]. However, specialised training that links the decision-making process across macro, meso, and micro hierarchy levels is necessary for high-risk cyber incident scenarios that escalate through various operational levels of analysis. Participants requested additional training focused on critically assessing information provided by systems, incorporating real-world scenarios, to establish an innovative training response framework that can be tested with maritime personnel to observe the differences in responses between those with and without maritime cyber security training. Participants also expressed that regular training would be essential to acquire the experience and knowledge required to respond to unforeseen cyber incident scenarios that may arise within UARSVO. The frequency of training was emphasised to be tailored to each organisation's needs to ensure cost efficiency. Furthermore, individuals noted that research and academia could be the initial implementers of this training, after which a third-party training company could expand and develop customised solutions suitable for organisations.

The most frequently referenced training methods for UARSVO were the use of simulators, which provide a safe environment for training, and tabletop exercises, as these are straightforward to conduct [99]. Either method was considered valuable depending on the ROC organisation and the type of vessel operation. In addition, participants with a procurement cycle perspective suggested an objective-based assessment approach for determining training requirements when introducing this training. Moreover, participants suggested using an objective-based approach to wargaming for this training, rather than one centred on procedural risks, to ensure it is goal-oriented instead of prescriptive about the procedures, as it offers flexibility for targeted outcomes.

5 DISCUSSION AND FINDINGS

The ongoing development of UARSVO requires multidisciplinary collaboration to address all perspectives essential for ensuring a successful transition when introducing new technology, as noted in Section 4.2.1. This has been evident through the engagement of key MASS stakeholders in this study, particularly among governing bodies. As discovered from Section 4.1.1 and 4.1.2, major advancements in this development have been seen across developed countries and regions where technology and infrastructure have been well established to facilitate these operations. Although a mandatory MASS Code is aimed to be implemented in 2032 by the IMO, MASS

vessel acceptance will be dependent on the above, as well as regulations established nationally and regionally, having the ability only to perform autonomous vessel navigation on dedicated sea areas [1, 100, 101]. This also correlates with the results provided in Figure 4, as a higher occurrence in the sub-theme challenges for UARSVO was received across international organisations, and in the sub-theme opportunities for UARVO, it was received across national organisations.

As stated by [102] and [103] due to the interrelatedness in definitions between the terms automation and autonomy, crucial awareness should be provided for these terminologies, as the autonomy of technology occurs when technology assumes responsibility and makes decisions on behalf of humans. This distinction is clearly illustrated in Section 4.1.3, obtained from participant contributions, and highlights the need for the IMO to define the terminology and taxology for this. Furthermore, the HAT within the HAC requires a relationship similar to that highlighted by participants and literature, viewing technology at the same level as human-to-human interactions rather than as mere tools [104, 105]. This correlates with the [6] and [106] statement that the role of the human element is perceived to evolve and transition towards a more supervisory one.

Participants noted with the use of the interview guide, as shown in Section 4.2.2, that RO roles and responsibilities must be specialised in emergency handling, passage planning, and cyber security for systems assurance. Additionally, in Section 4.2.3 on RO Education and Training Standards, training with technology operated from ROC and cyber security ranked among the two highest-referenced areas due to the necessity of systems assurance. In each case, a specialised RO role in these areas was seen as feasible, depending on the needs of the ROC organisation, as participants found it difficult to combine the RO role with that of the cyber analyst. This incorporation of cyber security for MASS has also been regarded as essential to include as a new topic within the maritime curricula for METIs, according to [107] which involved 70 participants from various stakeholder groups in the maritime sector. Furthermore, the review provided by [108] on the IMO Human Element, Training and Watchkeeping (HTW) 10th session in February 2024, stated the need for amendments to incorporate hands-on experience with simulations and practical exercises to enhance cyber security awareness and training among mariners within international maritime education and training for crewed vessels. However, this remains unaddressed as no amendments were made at the 11th HTW held in February 2025 [109].

Participants perceived the development of training on HAT for maritime cyber security resilience in UARSVO as vital as ROs will serve as a crucial line of defence in cyber incident management within ROC, collaborating with other internal and external personnel within and outside of the organisation. The proposed approach for the short-term development and implementation of this training was identified for mariners with sea time experience transitioning into an RO role, which will require future adaptation in the long-term if ROs without sea time experience become a reality in future UARSVO. Although HAT training for maritime cyber security resilience was ranked as the third strategy (see Table 5) by participants for HAT in maritime cyber security resilience for UARSVO, workforce training remains a vital organisational asset, as it interrelated to the first two strategies, system resilience and CSM in the event of a cyber incident.

Alternatively, the fourth most frequently mentioned strategy was the socio-technical system approach from a multi-level perspective during cyber incident management, aimed at improving safety in UARSVO [110, 111]. This also aligns, as highlighted in Section 4.4.4, with the necessity of providing holistic, specialised training that encompasses the connections within the decision-making process across macro, meso, and micro hierarchy levels during cyber incident management, which escalates through various operational levels analysis. [55] proposed future work to develop a maritime cyber risk management training framework specifically for crewed vessels, utilising the HCD process at a holistic macro level. However, within the maritime industry, the only standardised cyber incident response reporting procedure varies from country to country, and there is yet to be a standardised procedure at the international level [96-98].

Table 5. Strategies that could best enhance HAT in maritime cyber security resilience for UARSVO as per frequency received by participants (source: author).

Strategies	Sub-Strategies Developed Developed
System resilience	Redundancies with other instruments during non-nominal operations
	Sensor fusion
	Fail-safe mechanism
	Alert systems for cyber incidents regarding ROC
	Transparency of communication in decision-making from ANS to RO
	Zero trust architecture
Cyber Security Management System (CSMS)	Response procedure from the ROC during a cyber incident
	Culture of Cyber Resilience
	Risk assessments that incorporate multi- level safeguarding
	Dedicated response system for cyber incidents
	Checklist for work case cyber incident scenarios
HAT training in maritime cyber security resilience for UARSVO	Training in distinguishing between cyber- attacks and normal system failures
	Training for maximum cyber incident crisis scenarios
	Embedding of cyber-attacks as an emergency was proposed
Socio- technical systems approach from a multi- level perspective	Best approaches in various scenarios
	Identify which team and individual are best suited to assume responsibility in a cyber incident
	Enhance information sharing and lessons learned across the maritime industry

6 LIMITATION AND FUTURE WORK

The methodological implications of conducting semi-structured interviews for this research provided a holistic foundational knowledge and strategies for HAT in maritime cyber security resilience for UARSVO, building upon previous work that focused solely on mariners [13]. However, the methodology adopted rendered various challenges to obtaining the data for the conduct of this study. One of the main challenges was that the data acquisition from semi-structured interviews was highly time-consuming due to the time required to arrange interviews (which

included dropouts or the need to reschedule some interviews) and the process of verifying transcriptions and coding. The second main challenge was data quality assurance, as the questions given were open-ended, meaning that although this gave room to explore and develop new themes, there was room for proving generic answers. The answers from participants also depended on their willingness and knowledge to provide their perception and the order in which longer answers were given, especially for the first question set. Additionally, when interpreting the data, this was subjective to the interview guide. During this research, the interview process was stopped when data saturation and consistency from the different stakeholder groups were achieved. Other limitations extended to attaining confidential or classified information for each organisation. Although a participant with prior experience in VTS, a participant currently working in coastal administration, and experienced ROs were interviewed (including fieldwork with ROCs and discussions with currently operating ROs), a broader diversity of opinions would be achieved if currently active Vessel Traffic Service (VTS) officers, coastal authorities, and ROs could also have participated.

Future efforts could consider utilising the comprehensive, in-depth foundational qualitative data gathered from semi-structured interviews conducted with key MASS stakeholders. In combination with results obtained from [13], participant engagement could be extended (as stated above) to develop and validate a training framework for HAT in maritime cyber security resilience for UARSVO. The framework could then be tested and evaluated with key MASS stakeholders in a workshop completing the iteration steps from the hybrid DRM and HCD methodology adopted.

7 CONCLUSION

This research, based on semi-structured interviews with 76 participants, is the first of its kind due to the diversity of industry experts who participated from different key MASS industry stakeholder groups. The findings were unique as these address a comprehensive overview and foundational knowledge of UARSVO, maritime legislation surrounding UARSVO, maritime cyber security resilience related to UARSVO, and training in maritime cyber security resilience for UARSVO. Furthermore, the study developed key strategies that could effectively enhance HAT in maritime cyber security resilience for UARSVO based on thorough expertise that participated in this study from multi- disciplinary backgrounds within maritime autonomy.

The first ranked proposed strategy focused on systems resilience; the second emphasised Cyber Security Management Systems (CSMS) at the company level for ROCs; the third involved HAT training in maritime cyber security resilience for UARSVO with special focus on training to differentiate between cyber-attacks and normal system failures, along with training for maximum cyber incident crisis scenarios; the fourth adopted socio-technical systems approach from a multi-level perspective. Based on these findings, while HAT training in maritime cyber security resilience for UARSVO was the third most frequently mentioned strategy, it is the one that underpins the first two and the fourth during cyber incident management. Furthermore, it was identified that within HAT cyber resilience training for ROs will prioritise recognising and managing a cyber incident as a primary focus for training.

Results highlighted that future education and training standards would require ROs to integrate cyber security into METIs, as this would be one of the primary roles and responsibilities of these ROs, even though it is perceived to differ from that of a cyber security expert. Additionally, the results offer a comprehensive foundational knowledge that could inform the development of future training for ROs in HAT related to maritime cyber security resilience for UARSVO. This could then serve as an interim training framework under the IMO's sub-committee on HTW, enabling academia to develop training programmes on cyber resilience for UARSVO until mandatory instruments are established.

ACKNOWLEDGEMENTS

We would like to express our gratitude to all the interview participants for their crucial contributions to this study. Without them, the study could not have been conducted. We extend our gratitude to the sponsors of this research, Reardon Smith Nautical Trust and Cyber-SHIP lab, for enabling this research.

REFERENCES

[1] IMO. "MSC 109/WP.8 Development of a Goal-Based Instrument for Maritime Autonomous Surface Ships (MASS) - Report of the MSC-LEG-FAL Joint Working Group on Maritime Autonomous Surface Ships (MASS)." IMO. https://docs.imo.org/ (accessed 21/01/2025, 2025).

[2] T. Johansen and I. B. Utne, "Human-autonomy collaboration in supervisory risk control of autonomous ships," Journal of Marine Engineering & Technology, vol. 23, no. 2, pp. 135-153, 2024/03/03 2024, doi: 10.1080/20464177.2024.2319369.

[3] K. Tam, "MASS Cybersecurity," in Maritime Autonomous Surface Ships (MASS) - Regulation, Technology, and Policy: Three Dimensions of Effective Implementation, C.-J. Chae and R. Baumler Eds. Cham: Springer Nature Switzerland, 2024, pp. 165-180.

[4] DNV. "DNV-RP-0323 - Certification scheme for remote control centre operators." DNV. https://rules.dnv.com/ (accessed 21/01, 2025).

[5] DNV. "DNV-ST-0324 - Competence of remote control centre operators." DNV. https://rules.dnv.com/ (accessed 21/01, 2025).

[6] J. Chan, D. Golightly, R. Norman, and K. Pazouki, "Perception of Autonomy and the Role of Experience within the Maritime Industry," Journal of Marine Science and Engineering, vol. 11, no. 2, doi: 10.3390/jmse11020258.

[7] J. Y. C. Chen, A. R. Selkowitz, K. Stowers, S. G. Lakhmani, and M. J. Barnes, "Human-Autonomy Teaming and Agent Transparency," presented at the Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction, Vienna, Austria, 2017. [Online]. Available: https://doi.org/10.1145/3029798.3038339.

[8] K. T. Wynne and J. B. Lyons, "An integrative model of autonomous agent teammate-likeness," Theoretical

Issues in Ergonomics Science, vol. 19, no. 3, pp. 353-374, 2018/05/04 2018, doi: 10.1080/1463922X.2016.1260181.
[9] T. O'Neill, N. McNeese, A. Barron, and B. Schelble, "Human–Autonomy Teaming: A Review and Analysis of the Empirical Literature," Human Factors, vol. 64, no. 5, pp. 904-938, 2022/08/01 2020, doi: 10.1177/0018720820960865.
[10] T.-E. Kim, L. P. Perera, M.-P. Sollid, B.-M. Batalden, and A. K. Sydnes, "Safety challenges related to autonomous ships in mixed navigational environments," WMU Journal of Maritime Affairs, vol. 21, no. 2, pp. 141-159, 2022, doi: 10.1007/s13437-022-00277-z.
[11] M. Walter, A. Barrett, D. Walker, and K. Tam, "Adversarial AI Testcases for Maritime Autonomous Systems," AI, Computer Science and Robotics Technology, vol. 2, 04/25 2023, doi: 10.5772/acrt.15.
[12] DNV. "Tackling a growing cybersecurity threat in an increasingly connected industry." DNV. https://www.dnv.com/expert-story/maritime-impact/tackling-a-growing-cybersecurity-threat-in-an-increasingly-connected-industry/#:~:text=Scale%20and%20frequency%20of%20cyber,over%20the%20previous%20five%20y ears. (accessed 21/01, 2025).
[13] J. D. Palbar Misas, R. Hopcraft, K. Tam, and K. Jones, "Future of maritime autonomy: cybersecurity, trust and mariner's situational awareness," Journal of Marine Engineering & Technology, pp. 1-12, 2024, doi: 10.1080/20464177.2024.2330176.
[14] V. Bolbot, K. Kulkarni, P. Brunou, O. V. Banda, and M. Musharraf, "Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis," International Journal of Critical Infrastructure Protection, vol. 39, p. 100571, 2022/12/01/ 2022, doi: https://doi.org/10.1016/j.ijcip.2022.100571.
[15] N. Tabish and T. Chaur-Luh, "Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives," IEEE Access, vol. 12, pp. 17114-17136, 2024, doi: 10.1109/ACCESS.2024.3357082.
[16] E. Veitch, A. Hynnekleiv, and M. Lützhöft, "The Operator's Stake in Shore Control Center Design: A Stakeholder Analysis for Autonomous Ships," International Conference on Human Factors 2020, 02/19 2020, doi: 10.3940/hf.20.5.
[17] A. Nuwan, M. Shukri, and A. Khatibi, "Managerial Strategies for Organisational Resilience in SME Sector," International Journal of Research and Scientific Innovation, vol. xi, pp. 384-404, 01/01 2024, doi: 10.51244/IJRSI.2024.1101030.
[18] E. Erstad, "Operational training for enhanced maritime cyber resilience: Bridging safety and security through maritime education and training," Doctoral theses, Department of Ocean Operations and Civil Engineering, NTNU, NTNU Open, 2024:109, 2024. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3125566
[19] Maritime Coastguard Agency. "Maritime Autonomy Regulation Lab (MARLab) Report." Gov.UK. https://www.gov.uk/government/publications/maritime-autonomy-regulation-lab-marlab- report (accessed 07/02, 2025).
[20] AUTOSHIP. "D3.1 - Autonomous ship design standards." European Comission. https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5da3b7aa6&appId=PPGMS (accessed 18/02, 2025).
[21] T. Relling, M. Lützhöft, R. Ostnes, and H. P. Hildre, "A Human Perspective on Maritime Autonomy," in Augmented Cognition: Users and Contexts, Cham, D. D. Schmorrow and C. M. Fidopiastis, Eds., 2018// 2018: Springer International Publishing, pp. 350-362.
[22] Cambridge Dictionary. "Definition of Automation." https://dictionary.cambridge.org/dictionary/english/automation (accessed 22/01, 2025).
[23] L. Bainbridge, "Ironies of automation," Automatica, vol. 19, no. 6, pp. 775-779, 1983/11/01/ 1983, doi: https://doi.org/10.1016/0005-1098(83)90046-8.
[24] N. Sarter, D. Woods, and C. Billings, "Automation surprises," vol. 2, 1997, pp. 1926-1943.
[25] National Transport Safety Board. "Collision between US Navy Destroyer John S McCain and Tanker Alnic MC Singapore Strait, 5 Miles Northeast of Horsburgh Lighthouse." National Transport Safety Board. https://www.ntsb.gov/investigations/accidentreports/reports/mar1901.pdf (accessed 23/01, 2025).
[26] J. Rasmussen, "Risk management in a dynamic society: a modelling problem," Safety Science, vol. 27, no. 2, pp. 183-213, 1997/11/01/ 1997, doi: https://doi.org/10.1016/S0925-7535(97)00052-0.
[27] J. Rasmussen, Information processing and human-machine interaction : an approach to cognitive engineering (North-Holland series in system science and engineering ; 12). New York: North-Holland, 1986.
[28] D.-T. Pham, H. Ali, K. Fennedy, M.-H. Hsieh, S. Alam, and V. Duong, "Human-AI Hybrid Paradigm for Collaborative Air Traffic Management Systems."
[29] D. H. Hagos, H. El Alami, and D. B. Rawat, AI-Driven Human-Autonomy Teaming in Tactical Operations: Proposed Framework, Challenges, and Future Directions. 2024.
[30] Ø. Rødseth, L. A. Wennersberg, and H. Nordahl, "Levels of autonomy for ships," Journal of Physics: Conference Series, vol. 2311, p. 012018, 07/01 2022, doi: 10.1088/1742-6596/2311/1/012018.
[31] European Maritime Safety Agency. "CMOROC Final Report - Identification of Competences for MASS Operators in Remote Operation Centres." https://www.emsa.europa.eu/publications/reports/item/5089-cmoroc-mass.html (accessed 23/01, 2025).
[32] Z. H. Munim, T. Notteboom, H. Haralambides, and H. Schøyen, "Key determinants for the commercial feasibility of maritime autonomous surface ships (MASS)," Marine Policy, vol. 172, p. 106482, 2025/02/01/ 2025, doi: https://doi.org/10.1016/j.marpol.2024.106482.
[33] Maritime UK. "Maritime Autonomous Ship Systems (MASS) UK Industry Conduct Principles and Code of Practice A Voluntary Code - Version 8 " The Society of Maritime Industries (SMI). https://www.maritimeindustries.org/application/files/9417/3375/8340/MASS_COP_2024_V8_pages_V1.1.pdf (accessed 14/02, 2025).
[34] (2018). Maritime Safety Committee - 100th Session, Agenda Item 5: Regulatory Scoping Exercise for the use of Maritime Autonomous Surface Ships (MASS).
[35] Bureau Veritas. "Guidelines for Autonomous Shipping." Bureau Veritas. https://erules.veristar.com/dy/data/bv/pdf/641-NI_2019-10.pdf (accessed 22/01, 2025).
[36] DNV. "DNVGL-CG-0264 Autonomous and remotely operated ships." DNV. https://www.smashroadmap.com/files/dnvgl-cg-.pdf (accessed 22/01, 2025).
[37] ONESEA. "AUTONOMOUS SHIPS TERMS OF REFERENCE FOR RULE DEVELOPMENT." ONEDEA. https://b307d3dfff.clvaw-cdnwnd.com/ac8e62b9b6e49d3c818fcd9770855fb0/200000069-3d56a3d56d/WHITEPAPER%202022_One%20Sea%20-%20Terminology%20and%20levels%20of%20automation.pdf?ph=b307d3dfff (accessed 22/01, 2025).
[38] Lloyds Register. "LR Code for Unmanned Marine Systems." Lloyd's Register.https://www.smashroadmap.com/files/LR_Code_for_Unmanned_Marine_Systems__February_20172_.pdf (accessed 22/01, 2025).

[39] N. P. Ventikos. "Determining the requirements for fail-safe design of autonomous ships: The MOSES Autonomous Tugboat Swarm." https://moses-h2020.eu/wp- content/uploads/2024/06/Autonomous-tugboats-failsafe-approach_v1.0.pdf (accessed 28/01, 2025).
[40] DNV. "Maritime Cyber Priority 2024/25: Managing cyber risk to enable innovation." https://www.dnv.com/cyber/insights/publications/download/thank-you-download-2024-maritime- cyber-priority/ (accessed 28/01, 2025).
[41] IMO. "Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems " IMO. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf (accessed 28/01, 2025).
[42] IMO. "MSC-FAL.1-Circ.3-Rev.2 - Guidelines On Maritime Cyber Risk Management." IMO. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3- Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf (accessed 29/01, 2025).
[43] P. Peng, X. Xie, C. Claramunt, F. Lu, F. Gong, and R. Yan, "Bibliometric analysis of maritime cybersecurity: Research status, focus, and perspectives," Transportation Research Part E: Logistics and Transportation Review, vol. 195, p. 103971, 2025/03/01/ 2025, doi: https://doi.org/10.1016/j.tre.2025.103971.
[44] NIST. "Cyber Resiliency Definition." https://csrc.nist.gov/glossary/term/cyber_resiliency (accessed 29/01, 2025).
[45] National Institutes of Health. "What are competencies?" NIH. https://hr.nih.gov/about/faq/working-nih/competencies/what-are-competencies#:~:text=Knowledge%20is%20information%20developed%20or,individual%20to%20a%20certain%20situation. (accessed 29/01, 2025).
[46] MASSPeople. "MSC/ISWG/MASS 2/3/1 Consideration of Proposals for Further Development of the Draft MASS Code. Bridging Competency Gaps for MASS Operators in Alignment with the STCW Framework." IMO. https://www.masspeople.org/imo-submission/msc-iswg-mass-2-3-1 (accessed 08- 03, 2025).
[47] R. Hopcraft, "Developing Maritime Digital Competencies," IEEE Communications Standards Magazine, vol. 5, no. 3, pp. 12-18, 2021, doi: 10.1109/MCOMSTD.101.2000073.
[48] C. Campos Toresano, M. L. Castells Sanabra, and C. Borén Altés, "Conceptualization of the era of autonomous shipping within maritime education and training framework," 2024 2024: Universitat Politècnica de Catalunya. Iniciativa Digital Politècnica, doi: 10.5821/mt.12808. [Online]. Available: https://dx.doi.org/10.5821/mt.12808
[49] MAIB. "Collision between pure car carrier City of Rotterdam and ro-ro freight ferry Primula Seaways." GOV.UK. https://www.gov.uk/maib-reports/collision-between-pure-car-carrier-city-of- rotterdam-and-ro-ro-freight-ferry-primula-seaways (accessed 29/01, 2025).
[50] A. Landman, E. L. Groen, M. M. van Paassen, A. W. Bronkhorst, and M. Mulder, "Dealing With Unexpected Events on the Flight Deck: A Conceptual Model of Startle and Surprise," Human Factors, vol. 59, no. 8, pp. 1161-1172, 2017/12/01 2017, doi: 10.1177/0018720817723428.
[51] S. Symes, E. Blanco-Davis, T. Graham, J. Wang, and E. Shaw, "The survivability of autonomous vessels from cyber-attacks," Journal of Marine Engineering & Technology, pp. 1-23, 2024, doi: 10.1080/20464177.2024.2428022.
[52] University of Plymouth. "Maritime-Cyber Ransomware Scenario." https://www.youtube.com/watch?v=WZvkWIp6sEQ (accessed 30/01, 2025).
[53] University of Plymouth. "False AIS Data in Cyber-Attack Scenario." https://www.youtube.com/watch?v=fTjCr0X0nRQ (accessed 30/01, 2025).
[54] NHL Stenden. "Maritime Cyber Incident Simulations." https://www.nhlstenden.com/en/maritime-cyber-incident-simulations (accessed 30/01, 2025).
[55] E. Erstad, R. Hopcraft, A. Vineetha Harish, and K. Tam, "A human-centred design approach for the development and conducting of maritime cyber resilience training," WMU Journal of Maritime Affairs, vol. 22, no. 2, pp. 241-266, 2023/06/01 2023, doi: 10.1007/s13437-023-00304-7.
[56] D. Santos Castro, V. Plácido Da Conceição, and S. Campaniço Cavaleiro, "PNT Resilience and the Impact of Satellite Radio Positioning Disruptions on Piloting Teams," Institute of Marine Engineering, Science and Technology (IMarEST), 2022.
[57] Whiterbys, Cyber Security Workbook for On Board Ship Use. London: Whiterbys, 2025, p. 238.
[58] E. Erstad, R. Hopcraft, J. D. Palbar, and K. Tam, "CERP: A Maritime Cyber Risk Decision Making Tool," TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, vol. 17, no. 2, pp. 269-279, 2023, doi: 10.12716/1001.17.02.02.
[59] A. Oruc, N. Chowdhury, and V. Gkioulos, "A modular cyber security training programme for the maritime domain," International Journal of Information Security, vol. 23, no. 2, pp. 1477-1512, 2024/04/01 2024, doi: 10.1007/s10207-023-00799-4.
[60] A. Oruc, N. Chowdhury, V. Gkioulos, and S. Katsikas, "Evaluation of Maritime Cyber Security (MarCy) Training Programme," TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, vol. 18, no. 4, pp. 743-763, 2024, doi: 10.12716/1001.18.04.01.
[61] A. Vineetha Harish, K. Tam, and K. Jones, "Generating training events for building cyber- physical security skills," The Computer Journal, p. bxae123, 2024, doi: 10.1093/comjnl/bxae123.
[62] S. M. Kim, "Inductive or deductive? Research by maxillofacial surgeons," Journal of the Korean Association of Oral and Maxillofacial Surgeons, vol. 47, no. 3, pp. 151-152, 2021, doi: 10.5125/jkaoms.2021.47.3.151.
[63] A. Bryman and E. Bell, Business Research Methods. Oxford: Oxford University Press, 2011.
[64] M. Saunders, P. Lewis, and A. Thornhill, Research Methods for Business Students, 7th Edition ed. Harlow: Pearson, 2016.
[65] J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Los Angeles: Sage, 2018.
[66] M. N. K. Saunders, P. Lewis, and A. Thornhill, Research Methods for Business Students, 8th Edition ed. New York: Pearson, 2019.
[67] W. M. Trochim and J. P. Donnelly, The Research Methods Knowledge Base, 3rd ed. Cincinnati, OH: Atomic Dog, 2006.
[68] L. T. M. Blessing and A. Chakrabarti, DRM, a Design Research Methodology. Springer London, 2009, pp. XVII, 397.
[69] ISO. "9241-210: 2019 Ergonomics of human-system interaction. Part 210: Human-Centred Design for Interactive Systems. ." ISO. https://www.iso.org/standard/77520.html (accessed.
[70] L. A. Palinkas, S. M. Horwitz, C. A. Green, J. P. Wisdom, N. Duan, and K. Hoagwood, "Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research," (in eng), Adm Policy Ment Health, vol. 42, no. 5, pp. 533-44, Sep 2015, doi: 10.1007/s10488-013-0528-y.
[71] S. Sarantakos, Social Research, 3rd ed. London: Palgrave Macmillan, 2005.
[72] C. Andrade, "The Inconvenient Truth About Convenience and Purposive Samples," Indian Journal of Psychological Medicine, vol. 43, no. 1, pp. 86-88, 2021/01/01 2020, doi: 10.1177/0253717620977000.

[73] S. Campbell et al., "Purposive sampling: complex or simple? Research case examples," (in eng), J Res Nurs, vol. 25, no. 8, pp. 652-661, Dec 2020, doi: 10.1177/1744987120927206.
[74] G. R. Sadler, H. C. Lee, R. S. Lim, and J. Fullerton, "Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy," (in eng), Nurs Health Sci, vol. 12, no. 3, pp. 369-74, Sep 1 2010, doi: 10.1111/j.1442-2018.2010.00541.x.
[75] V. Braun and V. Clarke, Thematic Analysis A Practical Guide, First ed. London: SAGE, 2022.
[76] M. M. Hennink, B. N. Kaiser, and V. C. Marconi, "Code Saturation Versus Meaning Saturation:How Many Interviews Are Enough?," Qualitative Health Research, vol. 27, no. 4, pp. 591- 608, 2017, doi: 10.1177/1049732316665344.
[77] L. Nyanchoka, C. Tudur-Smith, R. Porcher, and D. Hren, "Key stakeholders' perspectives and experiences with defining, identifying and displaying gaps in health research: a qualitative study protocol," (in eng), BMJ Open, vol. 9, no. 8, p. e027926, Sep 3 2019, doi: 10.1136/bmjopen-2018- 027926.
[78] A. Galletta, Mastering the semi-structured interview and beyond: From research design to analysis and publication (Mastering the semi-structured interview and beyond: From research design to analysis and publication.). New York, NY, US: New York University Press, 2013, pp. xiii, 245-xiii, 245.
[79] N. King and C. Horrocks, Interviews in qualitative research. London: Sage, 2010.
[80] B. Dicicco-Bloom and B. F. Crabtree, "The qualitative research interview," (in eng), Med Educ, vol. 40, no. 4, pp. 314-21, Apr 2006, doi: 10.1111/j.1365-2929.2006.02418.x.
[81] M. DeJonckheere and L. M. Vaughn, "Semistructured interviewing in primary care research: a balance of relationship and rigour," (in eng), Fam Med Community Health, vol. 7, no. 2, p. e000057, 2019, doi: 10.1136/fmch-2018-000057.
[82] C. Willig, Introducing Qualitative Research in Psychology. McGraw-Hill Education., 2013.
[83] UK Data Service. "Anonymising qualitative data." https://ukdataservice.ac.uk/learning- hub/research-data-management/anonymisation/anonymising-qualitative-data/ (accessed 30-12,2024).
[84] M. Naeem, W. Ozuem, K. Howell, and S. Ranfagni, "A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research," International Journal of Qualitative Methods, vol. 22, p. 16094069231205789, 2023/10/01 2023, doi: 10.1177/16094069231205789.
[85] W. Xu and K. Zammit, "Applying Thematic Analysis to Education: A Hybrid Approach to Interpreting Data in Practitioner Research," International Journal of Qualitative Methods, vol. 19, p. 1609406920918810, 2020/01/01 2020, doi: 10.1177/1609406920918810.
[86] C. Davidson, "Transcription: Imperatives for Qualitative Research," International Journal of Qualitative Methods, vol. 8, no. 2, pp. 35-52, 2009/06/01 2009, doi: 10.1177/160940690900800206.
[87] L. S. Nowell, J. M. Norris, D. E. White, and N. J. Moules, "Thematic Analysis: Striving to Meet the Trustworthiness Criteria," International Journal of Qualitative Methods, vol. 16, no. 1, p.1609406917733847, 2017/12/01 2017, doi: 10.1177/1609406917733847.
[88] IMO. "Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs)." IMO. https://www.imo.org/en/About/Conventions/Pages/COLREG.aspx (accessed 2025, IMO).
[89] IMO. "International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978." IMO. https://www.imo.org/en/OurWork/HumanElement/Pages/STCW- Convention.aspx (accessed 08-03, 2025).
[90] National Transport Safety Board. "Contact of Containership Dali with Francis Scott Key Bridge and Subsequent Bridge Collapse." National Transport Safety Board. https://www.ntsb.gov/investigations/Pages/DCA24MM031.aspx (accessed 08-03, 2025).
[91] R. Sadeghi and F. Goerlandt, "A proposed validation framework for the system theoretic process analysis (STPA) technique," Safety Science, vol. 162, p. 106080, 2023/06/01/ 2023, doi: https://doi.org/10.1016/j.ssci.2023.106080.
[92] European Maritime Safety Agency. "Risk Based Assessment Tool (RBAT)." European Maritime Safety Agency. https://www.emsa.europa.eu/mass/rbat.html (accessed 08-03, 2025).
[93] N. El-Sheimy and A. Youssef, "Inertial sensors technologies for navigation applications: state of the art and future trends," Satellite Navigation, vol. 1, no. 1, p. 2, 2020/01/20 2020, doi: 10.1186/s43020-019-0001-5.
[94] F. Lázaro, R. Raulefs, W. Wang, F. Clazzer, and S. Plass, "VHF Data Exchange System (VDES): an enabling technology for maritime communications," CEAS Space Journal, vol. 11, no. 1, pp. 55-63, 2019/03/01 2019, doi: 10.1007/s12567-018-0214-8.
[95] IMO. "Maritime Single Window." IMO. https://www.imo.org/en/OurWork/Facilitation/Pages/MaritimeSingleWindow-default.aspx (accessed 08-03, 2025).
[96] UK Civil Aviation Authority. "Reporting a cyber security incident. Information and reporting procedures in the event of a cyber security incident." CAA. https://www.caa.co.uk/commercial- industry/cyber-security/reporting-a-cyber-security-incident/ (accessed 20/02, 2025).
[97] Gov.UK. "Guidance - Where to Report a Cyber Incident." Gov.UK. https://www.gov.uk/guidance/where-to-report-a-cyber-incident (accessed 20/02, 2025).
[98] Gov.UK. "Guidance - Implementing the Network and Information Systems Directive in the transport sector." Gov.UK. https://www.gov.uk/government/publications/implementing-the- network-and-information-systems-directive-in-the-transport-sector (accessed 20/02, 2025).
[99] M. Odéen, C. Sellberg, G. Praetorius, O. Lindwall, L. Englund, and A. Andersson, "Intelligent Learning Systems for Simulator-Based Professional Training: A Systematic Literature Review," in Integrating Emerging Technologies into Education and Training: Proceedings of the 2nd ETELT 2024 Workshop, Cham, T. E. Kim, M. Milrad, and I. Remolar, Eds., 2025// 2025: Springer Nature Switzerland, pp. 109-119.
[100] R. Thomas, Modern Law of Marine Insurance Volume Five, The (Maritime and Transport Law Library). London: Informa Law from Routledge, 2023, p. 372.
[101] H. Ringbom, Røsæg, E., & Solvang, T., Autonomous Ships and the Law London: Routledge, 2020, p. 318.
[102] R. Bo, "From Automatism to Autonomy," Conversations: The Journal of Cavellian Studies, no. 10, pp. 98-127, 2023, doi: 10.18192/cjcs.vi10.6615.
[103] S. Chiodo, "Human autonomy, technological automation (and reverse)," AI & SOCIETY, vol. 37, no. 1, pp. 39-48, 2022/03/01 2022, doi: 10.1007/s00146-021-01149-5.
[104] E. J. de Visser, R. Pak, and T. H. Shaw, "From 'automation' to 'autonomy': the importance of trust repair in human–machine interaction," Ergonomics, vol. 61, no. 10, pp. 1409-1427, 2018/10/03 2018, doi: 10.1080/00140139.2018.1457725.
[105] E. Veitch and O. Andreas Alsos, "A systematic review of human-AI interaction in autonomous ship systems," Safety Science, vol. 152, p. 105778, 2022/08/01/ 2022, doi: https://doi.org/10.1016/j.ssci.2022.105778.
[106] E. Veitch, O. A. Alsos, T. Cheng, K. Senderud, and I. B. Utne, "Human factor influences on supervisory control of remotely operated and autonomous vessels," Ocean Engineering, vol. 299, p. 117257, 2024/05/01/ 2024, doi: https://doi.org/10.1016/j.oceaneng.2024.117257.

[107] C. Campos, M. Castells-Sanabra, and C. Borén, "Maritime Stakeholders' Insights on Maritime Education and Training in the Autonomous Shipping Era. A Small-Scale Study in Spain " Scientific Journal of Maritime Research - Pomorstvo, vol. 39, pp. 80-91, 2025, doi: https://10.31217/p.39.1.7.
[108] S.-Y. Yi, M. Jung, and S.-I. Lee, "Adapting to change: International maritime education and training for future seafarers – focusing on the comprehensive review of the STCW convention and code of the 10th session of the IMO HTW," Journal of International Maritime Safety, Environmental Affairs, and Shipping, p. 2464486, 2025, doi: 10.1080/25725084.2025.2464486.
[109] IMO. "Sub-Committee on Human Element, Training and Watchkeeping, 11th session (HTW 11), 10 – 14 February 2025." IMO. https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/HTW-11th-session.aspx (accessed 24/02, 2025).
[110] A. Connor, "Methods for the investigation of work and human errors in rail engineering contexts," 07/15 2016.
[111] J. Wang, W. Fang, H. Qiu, and Y. Wang, "The Impact of Automation Failure on Unmanned Aircraft System Operators' Performance, Workload, and Trust in Automation," Drones, vol. 9, no. 3, doi: 10.3390/drones9030165.
[112] LUMIVERO. "NVIVO Qualitative Analysis Software." LUMIVERO. https://lumivero.com/products/nvivo/ (accessed 20/02, 2025).