Future of maritime autonomy: cybersecurity, trust and mariner's situational awareness

Palbar Misas, JD

10.1080/20464177.2024.2330176
Journal of Marine Engineering & Technology
Informa UK Limited

Future of Maritime Autonomy: Cybersecurity, Trust and Mariner's Situational Awareness

J D Palbar [a*], R Hopcraft [a], K Tam [a], K Jones [a]

[a] *University of Plymouth, United Kingdom*

*Corresponding author. Email: juan.palbarmisas@plymouth.ac.uk

Synopsis

As technology evolves, the level of automation in the maritime industry also grows. Given the extensive benefits they offer, the industry will continue to develop its digital capabilities in order to improve. One key example of this is the industry currently striving for fully autonomous vessels. Current crew-based maritime operations on board rely on a mixture of automated simplistic processes, human decision-making, and human interventions. The future autonomy suggests the removal of the mariner physically on board. The remote nature of these operations will subject mariners and vessels to new operational risks, such as a potential reduction in Situational Awareness (SA) and/or cyber threats. In this research, authors engaged with navigators with a range of traditional operational experiences to extend previous discussions conducted with cadets on the importance of SA in maritime operations, and the potential challenges facing this when engaging in remote operations. This was done using tabletops, questionnaires and full bridge simulator exercises. Through this engagement, authors found that future navigators will need training to be equipped with new skills to interact with digital systems during different modes of human operation (such as remote monitoring, supervision and intervention) to overcome perceived challenges including cyber incident management.

Keywords: Autonomy; Trust; Maritime Cybersecurity; Situational Awareness; Human Element

1 Introduction

In 1964 the International Maritime Organization (IMO) first discussed automation and its ability to reduce, or remove, human intervention in commercial shipping (IMO, 1964; Chae et al., 2020). It took over half a century before the IMO considered the development of a regulatory framework for exploring the impacts of including Maritime Autonomous Surface Ships (MASS) in the world's fleet. Through a Regulatory Scoping Exercise (RSE), the IMO identified challenges to remote controlled and fully autonomous vessels and argued that the human element will continue to play an important role in these operations (IMO, 2021). This work, started by the IMO's Maritime Safety Committee (MSC) in November 2022, provides a table identifying preferred options to address the key deficiencies within IMO documentation that inhibits MASS operations. These deficiencies include the role and competencies required for MASS masters and crews, as well as the meaning of Remote Operator (RO) and Remote Operations Centres (ROC) which continues to be an ongoing work. Similar to the IMO's regulatory strategy to achieve zero emissions by 2050, the IMO will first adopt a non-mandatory MASS Code by 2025 that will be followed by a more prescriptive mandatory MASS Code in 2028 (IMO, 2022, 2023).

Currently, a number of different commercial and academic MASS projects are in progress such as: Maritime Unmanned Navigation through Intelligence in Network (MUNIN); Advance Autonomous Waterborne Applications (AAWA); Yara Birkeland; DNV-GL Revolt, Kongsberg maritime autonomous shipping, Korea Autonomous ship project; and NYK Maritime Autonomous Surface Ships Trials. To achieve remote and fully autonomous shipping, organizations are developing and adopting new technologies and digital capabilities. However, implementing these without a holistic socio-technical view for implementation from all industry stakeholders (e.g. ship owners, operators, class societies, technology developers, customers) could introduce new risks in operations (Issa et al., 2022; IMO, 2021). For example, many organisations do not align their innovation strategies to their machine-operator work processes when developing new technologies (Chae et al., 2020; Zongo, 2017). Instead, advancements are typically driven by profits, or their perceived positive impact on the environment (Digitalisation World, 2020). However, as demonstrated through early MASS trials, due to the fragmentation of organisational structure and heavy responsibility on ROCs, new roles may need to be introduced to ensure the safety of operations (Størkersen, 2021; Mallam et al., 2020).

Authors' Biographies

Juan Dorje Palbar Misas is a PhD Candidate in Navigation and Maritime Cybersecurity and an Associate Lecturer at the University of Plymouth. Prior to this, he was working as a Research Assistant on the EU Horizons Cyber-MAR project.

Dr Rory Hopcraft is a Lecturer in Cyber Security at the University of Plymouth, working within Cyber-SHIP Lab. Dr Hopcraft's research interests include maritime cyber security governance and the role of the human element in the safety and security of maritime operations.

Dr Kimberly Tam is an associate professor at the University of Plymouth and the Theme Lead for Marine and Maritime in the Data-Centric Engineering Programme at The Alan Turing Institute.

Prof Kevin Jones is the Deputy Vice-Chancellor - Research and Innovation at the University of Plymouth, and is PI for Cyber-SHIP Lab and the head of the maritime cyber threats research group.

Automation	Description	Type
Degree One	Ship with automated processes and decision support	Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated and at times be unsupervised but with seafarers on board ready to take control.
Degree Two	Remotely controlled ship with seafarers on board	Ship is operated from another location. Seafarers are available on board to take control and operate the shipboard systems and functions.
Degree Three	Remotely controlled ship without seafarers on board	The ship is controlled and operated from another location. There are no seafarers on board.
Degree Four	Fully autonomous ship	The operating system of the ship is able to make decisions and determine actions by itself.

Table 1: Degrees of Ship Autonomy and Extent of Human Involvement (IMO, 2018)

The incorporation of crew in ROCs will also require a higher level of Human-Autonomy Teaming (HAT) as there will be shared control of responsibility between the autonomous system and human operators. However, navigators will remain the ultimate agent responsible for operations at a remote location (Rieth and Hagemann, 2022; Chan et al., 2023b; Johansen and Utne, 2024; Xu and Gao, 2024). For this, the use of ship simulators to testbed and design human-centred applications, including Artificial Intelligence (AI) applications, will be essential to enhance operators' Situational Awareness (SA) and algorithms for the understanding of new methods of ensuring the safety of operations and remote crew's ability to respond to incidents (Endsley, 2023; Vagale et al., 2022). Therefore, not incorporating this could lead to critical safety failings of SA endangering crew, passengers, infrastructure, and the environment (Gutzwiller et al., 2020; Endsley, 2015). SA from a safety perspective refers to "being aware of what is happening around you in terms of, where you are, where you are supposed to be, and whether anyone or anything around you is a threat to your safety" (Health and Safety Executive, 2012). In terms of maritime safety operations, the same SA is required for a physically crewed and operated vessel, and has been included in the UK's Maritime Coastguard Agencies human factors "Deadly Dozen" since 2016 (Maritime and Coastguard Agency, 2016). However, in remote operations the perception of the environment is gained from digital data presented, for example, video footage from around the ship displayed on screens rather than from a crew member on watch. SA for fully autonomous vessels is based upon the provided digital data and tools (like algorithms) to make the appropriate decision (Hammernes, 2022; IMO, 2018). This study analyses the challenges of maintaining that mission-critical SA in remote maritime operations, and the importance of cybersecurity awareness in increasingly digitalised operational environments. Secondly, it identifies the skills ROs may require to undertake the new roles and responsibilities brought about by autonomy. To better understand the impact of automation within maritime operations, the authors engaged with a variety of operators with a range of experience, including a serving marine pilot, senior navigators, junior officers of the watch and cadets to extend previous research which was solely conducted with cadets as participants (Misas et al., 2022). The navigator's responses to various exercises were recorded and used to inform the discussions hereafter. The paper concludes by discussing how current, and future, autonomy affects SA and cybersecurity, and how this should inform the development of future HAT training in Autonomous and Remote Surface Vessel Operations (ARSVO) and ROC organisational structure design.

2 Background

Unchanged since 1964, the IMO broadly states that an autonomous ship is "... a ship which, to a varying degree, can operate independently of human interaction" (IMO, 1964, 2021). To narrow the focus of the RSE, the IMO settled on four degrees of automation, which describe the level of human involvement (see Table 1) (IMO, 2018). As it is estimated that 75%-96% of all accidents in the maritime sector are due to human error (Cardiff University and Allianz, 2012), it has been argued that autonomous ships could reduce errors, whilst providing other benefits including: a reduction in annual operation costs, and increases in safety and fuel efficiency (Ziajka-Poznańska and Montewka, 2021). However, the advantages of autonomy are not always weighed with the potential challenges of moving to ARSVO. The remainder of this section will explore these challenges.

2.1 Trust in autonomous systems

Although trust in autonomous systems is yet to be fully explored, it is important to note that there are challenges remaining in promoting the sector's level of trust in such systems specially by integrating ecological interface design on interface design for ARSVO (Lee and See, 2004). The transit of goods through the global supply chain requires a degree of trust between stakeholders such as ship owners, operators, customers, class societies, technology developers and freight forwarders as well as their implied trust in the digital systems used to ensure the safe

passage of goods (e.g. navigation equipment, cargo tracking systems and digital certificates). Any acceptance of autonomous systems as the norm within this sector requires developing trust in the accuracy, reliability, safety and security of these existing systems as well as any new systems implemented to replace the human element. As an example, remote operations require the transfer of data pertaining to the ship's internal (e.g. systems that control the movement of the ship) and external (e.g. systems that aid collision avoidance, navigation and communications) environments with the ROC. Research demonstrates that the communication links used for this transfer are potentially not secure allowing this data to be manipulated by a third party (Cho et al., 2022), raising concerns regarding the trust placed in these systems and the data they transfer. However, a recent study by Longo et al. (2023a) proposed a solution using encryption and authentication to secure channels of communication between the ship and remote centre. These solutions can help develop the required level of trust over time as the accuracy of the information can be positively verified as systems are operating (Sharma et al., 2021; Lynch et al., 2022).

Achieving acceptable levels of trust is, and will, continue to be a challenge within commercial MASS projects. Currently, as Castro et al. (2022) demonstrated with the use of a questionnaire, the trust values of traditional navigators in automation seem similar and relatively high across navigators' responses. If sufficient training and supervision are provided, navigators are likely to be more willing to place trust in autonomy while adapting to new modes of operation from ROC such as remote monitoring, supervision, intervention (e.g., assisted control, direct control) and fleet mission management (Chan et al., 2023a; Veitch and Andreas Alsos, 2022). Thus, factors that influence navigators' levels of human-autonomy trust will remain essential for successful ARSVO as navigators are and they will be an integral part of operations to ensure and verify the accuracy of information regardless of degree of autonomy (Hoff and Bashir, 2015; Rodseth et al., 2022; IMO, 2023).

2.2 Situational Awareness challenges

Sometimes referred to as the automation conundrum (Zongo, 2017) or "human-in-the-loop" challenge, the inclusion of autonomy has its proposed benefits (see above), but can significantly reduce the human operator's SA. As the industry moves towards fully autonomous ships, crewed vessels may be required to intermingle with autonomous vessels, and in some situations, a human operator may be needed to intervene and take manual control of an otherwise autonomous vessel. Without maintaining good SA, these situations could lead to safety issues. This was demonstrated in 2018 with the grounding of Priscilla, a general cargo vessel, where the navigating officer during sole lookout at night due to automation complacency lost SA. In this case, the navigator failed the critical task of monitoring the ship's passage due to fatigue and boredom. Without proper use of digital aids, this led to late recognition of the dangerous position of the vessel and subsequent grounding (MAIB, 2019).

Another grounding in 2016 of the general cargo vessel Nova Cura was attributed to user assumptions and over-reliance on information from the Electronic Chart Display and Information System (ECDIS) which demonstrated the fallout of old skills in digital navigation (Dutch Safety Board, 2016). Moreover, the same fallout of old skills in digital navigation was seen in 2023 with the grounding and subsequent oil spillage of the Ro/Pax Ferry Marco Polo off the coast of Sweden when the vessel gradually deviated from course due to over-reliance on a faulty GPS by the Captain and an officer (Independent Online, 2023). Although operators make errors, humans are still often able to adapt to unpredictable situations by using creative problem-solving, something computers still struggle to do (Ahvenjärvi, 2016). Thus, highlighting how essential an operator's response and problem-solving can be for the safety and security of all operations including remote.

The IMO RSE concluded that no passenger transport will occur without seafarers on board (IMO, 2021). Even if all cargo ships become fully autonomous, passenger ships will still require trained personnel on-board. This further illustrates that seafarers will continue to have critical roles monitoring, supervising and intervening with safety critical systems (Mallam et al., 2020; Mehta et al., 2021), regardless of the perceived benefits (Rice, 2019). Until autonomous systems can fully replace human capabilities and are trustworthy, including being cyber-secure, maritime transportation will require a human-in-the-loop (Ahvenjärvi, 2016). Therefore, it is critical that mariners are provided with the training and technical support they need to maintain SA for both operational and cyber safety in an increasingly digitalised sector.

2.3 Remote Operation Training

The human-machine relationship in the maritime industry has a long history of innovation to meet numerous new challenges. The development of digital navigation aids, such as ECDIS, led to new training for mariners being developed. As technology changes, there is a need to re-evaluate seafarer training to address these new demands. The current regulatory framework somewhat allows for this. However, technological innovations often out-pace this process, creating socio-technical issues such as the lack of transparency in technological processes making it harder for the end user to understand, interact and collaborate with digital data.

Under Article 94 of the United Nations Convention on the Law of the Sea, each vessel must have a master who possesses appropriate qualifications (United Nations, 1982). This mariner must comply with regulatory obli-

gations, including those under the Convention on the International Regulations for Preventing Collisions at Sea 1972 (COLREGS) and the International Convention for the Safety of Life at Sea (SOLAS) (IMO, 2020, 2003). The physicality of removing the master from the vessel brings into question their specific roles and competencies (Ghaderi, 2019; Vojković and Milenković, 2020). Although the RSE started to identify preferred options when considering the master within remote operations some questions remain unanswered. For example, what elements of maritime training needed to be introduced, or changed, to ensure remote masters possess and maintain the required navigational or communication skills to maintain SA and operate safely? For this the IMO's MASS Joint MSC-Legal Committee (LEG)-Facilitation Committee (FAL) Working Group on the MSC 107 started to consider and discuss the International Convention Standards of Training, Certification and Watchkeeping for Seafarers (STCW) for MASS masters' and crews' qualification and skills if they were designated as seafarers (IMO, 2023).

In a recent incident involving an Unmanned Aerial Vehicle (UAV) the RO's inexperience in handling abnormal situations was blamed for the crash (Lynch et al., 2022a). While not maritime-specific, the incident highlights the need for organisations to consider the type of training they need to offer ROs, and how this might differ for more traditional crews. The UAV example highlights the importance of ensuring crew has the appropriate skills and knowledge to maintain SA and respond to sudden and unpredictable changes in the operational environment. As demonstrated by Tam et al. (2023) losing SA due to a cyber-physical attack could mean a significant econometric loss with an immense impact on numerous stakeholders.

In some incidents, as seen with Global Navigation Satellite System (GNSS) spoofing in the Black Sea (Jones, 2017) or the Straits of Hormuz (Cozzens, 2019), cyber-attacks can also degrade operator trust in the accuracy of critical systems. Thus, enhancing seafarer competencies to maintain SA in remote operations must include the ability to identify, protect, detect, respond and recover to mitigate cyber incidents. This can not only help maintain the safety of operations but also improve the allocation of trust in systems to understand, interact and collaborate (Endsley, 2017). As demonstrated by Castro et al. (2022) who used ship simulator scenarios exercises for GNSS spoofing and jamming detection with pilotage teams the best-performing teams during exercises fell somewhat in the middle among values of trust in automation when compared with questionnaire results. Moreover, the key success factor for resilience among those teams was attributed to compliance with structured response procedures during incident management. An example of a Cyber Emergency Response Procedure (CERP) is provided by Erstad et al. (2023b) which utilises three scenarios to demonstrate that both internal and external (from shoreside) support are needed during traditional cyber incident handling. Consequently, highlights the need for a standardised framework for cyber incident responses and a better understanding of these frameworks at an organisational level for both crewed and uncrewed surface vessels.

3 Methodology

To better understand the impacts of autonomy and cybersecurity on a seafarer's SA, the authors initially engaged with a group of 75 navigational cadets enrolled on their final year of BSc (Hons) Navigation and Maritime Science at a British university for a one-day workshop. Within the group, over 60% had some professional sea-based training experience and 37% of them were at the early stage of their sea time experience. To ensure a diversity in experience the authors ran a second workshop which engaged with a group of serving navigators including a British marine pilot, and several younger-generation navigators with a mixed service record. This second group would have increased the 12+ month demographic to roughly 30%. All participants demonstrated and shared their thoughts and opinions on what a future autonomous maritime sector could look like, and how they saw their roles and responsibilities changing to meet these developments. This section will present the adopted methodological approach, whilst Section 4 will provide a more detailed analysis. The following methods were used to collect both quantitative and qualitative data:

- Maritime cyber awareness questionnaire
- Future of remote operation tabletop exercises
- Full bridge cyber-attack simulation exercises

3.1 Questionnaire

Prior to the workshop, participants were provided with a questionnaire, to determine the group's baseline understanding and knowledge of autonomy and cybersecurity. The questionnaire was divided into two parts. The first included ten maritime cyber awareness questions, in which the majority of answers were quantitative (e.g. yes/no, scale of agree to disagree). The second part incorporated qualitative questions, asking for their opinions or details, for example, the type/flag of the ship they served on (see questionnaire results in Section 4).

3.2 Tabletop

During the second half of the workshop, participants were split into groups of five or six. This was due to both expected watchkeeping crew sizes during presented scenarios and the size of the simulator. Each group completed a 50-minute tabletop discussion on what they perceived to be the impact of autonomous operations on their SA, and how this could affect their safety and security. To seed discussions, all participants were given the questions below, and were encouraged to draw on their own experiences of maritime operations, their everyday use of technology, and wider knowledge regardless of their sea-time experience to help better understand the long-term benefits of secure-by-design training and cyber security culture:

1. Will the roles and responsibilities of a navigational officer change with remote control?
2. What challenges do you foresee?
3. To what extent do you trust autonomous ships?
4. How would being physically removed from the ship affect SA?
5. What new skills would you require to operate safely?

All questions above referred to autonomous degrees 2-4. To aid their collaboration, each group was provided with large sheets of paper and pens to collate their thoughts.

3.3 Simulations

Each group was taken through two different simulation exercises by rotating the same teams to different stations. The operational requirements of both scenarios require extra manning on the bridge which is aligned with the number of participants in each group. Additionally, as some participants had less sea time experience than others team sizes provided a more inclusive environment for them and it also provided an acceptable combined team knowledge. Each exercise consisted of a 5-minute briefing/familiarization period, a 10-minute Watchkeeping section, during which a simulated cyber-incident occurs, and a 10-minute group discussion. During both simulations, participants were given 5 minutes to familiarize themselves with the 393m containership model, and the physical simulator. During this initial period, participants were given a handover that included standard information (voyage departure and destination locations, ship type characteristics, position, course, route, speed, time, weather conditions and exercise main tasks).

All exercise scenarios were designed to test the participants' SA in different ways as a response to incidents when the ship's navigational systems had been compromised. Using the full-bridge simulator brought a level of realism through the use of an appropriately represented scenario, allowing the participants to suspend disbelief ensuring the highest possible levels of SA in a simulated setting (Lateef, 2010; Salas et al., 1998). Therefore, any issues with participant SA were more likely to be attributed to the cyber-attack within the scenario, instead of simulation quality.

The first scenario as shown in Figure 1 introduced a GNSS drift of 300 metres every 2 minutes to the east of their position, simulating a spoofing attack as the ship transits the UK Land's End Traffic Separation Scheme (TSS) under restricted visibility (transiting various fog banks). On average it took cadets and mid-experience navigators 8 minutes after the first manipulation to spot the error, which meant a significant course offset of 1.2km for that period. On the contrary, for senior experienced mariners, the identification was almost instant. Even when response time was less ($<$3 minutes) cadets struggled to comprehend the direction spoofing had occurred. The position error could have been apparent if have had turned on the radar overlay which could have shown instant discrepancy between the radar overlay and coastline on the ECDIS display. However, as will be discussed later, participants tended to trust the information they were presented and when they did not, they expressed concerns as they did not know how to validate the information. For experienced mariners, it took 15 seconds from identification to validation, to communicating that there was GNSS manipulation occurring. Within 8 minutes of the incident starting, the experienced navigators had implemented Parallel Index (PI) lines on the radar, and taken manual position fixes on ECDIS (with range and bearing from the radar). Thus, allowing them to recover the SA of the ship's position at the end of the exercise.

The second scenario as shown in Figure 2 involved a more dramatic and sudden incident with a direct impact on the safety of the crew, vessel and environment. Using the cyber incident demonstrated in Tam et al. (2022), this scenario involved the jamming of the rudder full to port and engine full ahead during an inbound passage to the port of Valencia (Spain). Even with fast detection (within seconds), and mitigation actions in place, the scenario was designed so that the ship's momentum (high rate of turn and speed) and limited time (2 minutes and 40 seconds) meant grounding with rock pier and blockage of the port entrance was assured. During the simulation, participants were timed to see how quickly they would detect the loss of rudder and engine control, and the

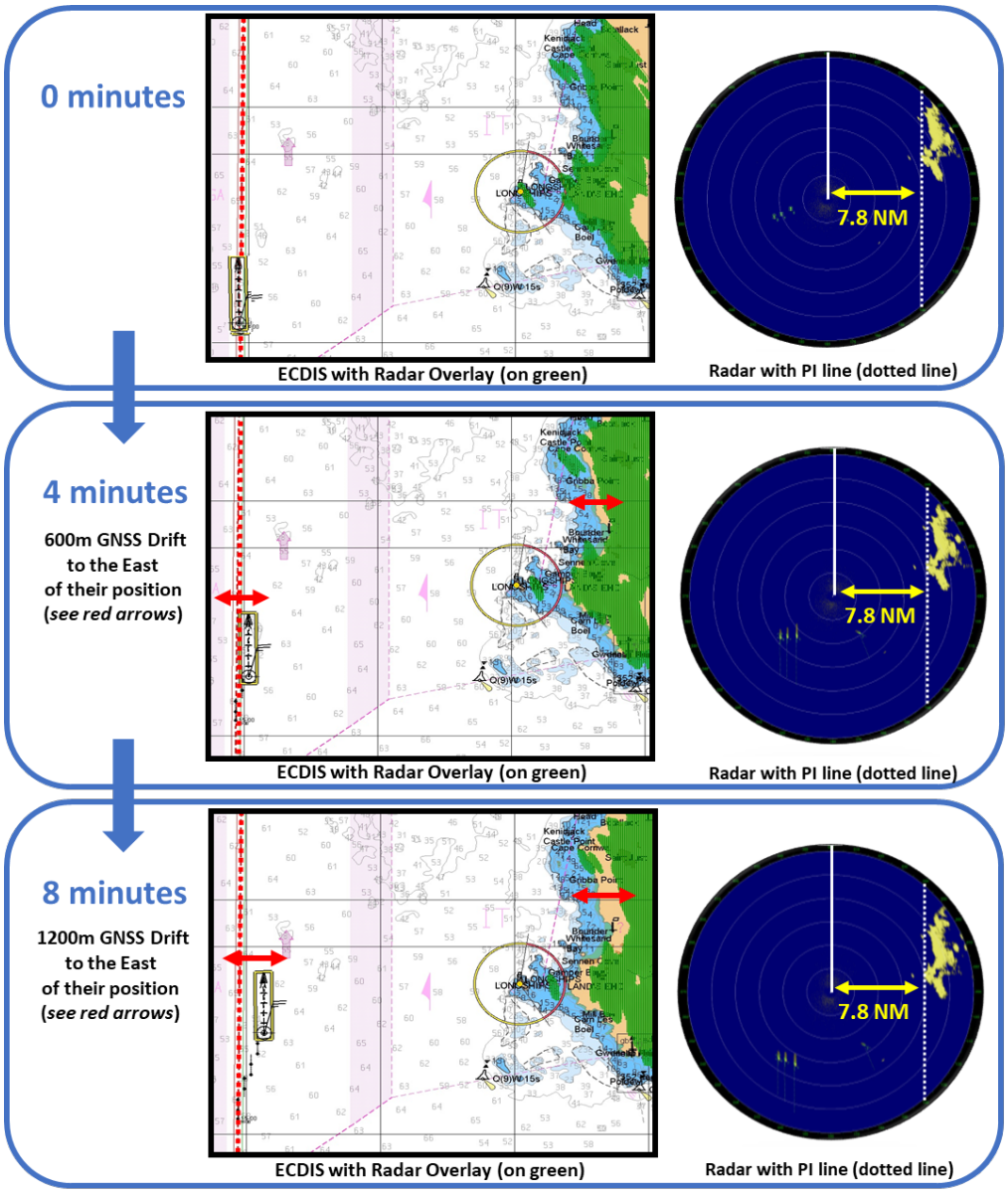

Figure 1: Demonstration of the first scenario GNSS drift at UK Land's End Traffic Separation Scheme (TSS) under restricted visibility. ECDIS with radar overlay indicating increased GNSS drift (on the left side) and radar with Parallel Index (PI) line not moving from headland indicating vessel on track at all times (on the right side)

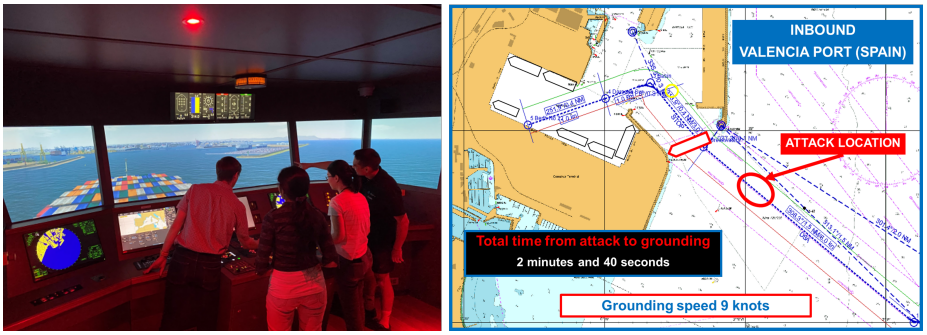

Figure 2: Demonstration of the second scenario jamming of the rudder full to port and engine full ahead inbound to the port of Valencia (Spain). A group of participants in the full bridge ship simulator at the start of the exercise (on the left side) and ECDIS display (with additional information) at the end of the exercise (on the right side)

subsequent emergency actions taken to try and prevent and minimize the incident's impacts. All participants detected the rudder and engine jamming within seconds of the incident occurring. However, there was a period on average of 40 seconds where participants hesitated before initiating an emergency response. These observed responses included the attempted use of the engines and rudder, and passing instructions to the tugboats. After a minute when realising that there was no response from the engine (ship's speed continuing to increase) and rudder (rudder remained hard to port) participants started to implement contingency measures including, sounding the general emergency alarm, dropping anchors, using bow thrusters, initiating manual operations of the rudder and closing watertight doors in order to minimize the incident impact.

4 Analysis and Discussion

In this section, the qualitative and quantitative results from the questionnaire, tabletop, and simulated scenarios are used together to discuss the various SA challenges that the authors observed and that the participants identified.

4.1 SA Challenges During Remote Operations

Throughout the workshops and experience specially gained from simulator which represents a good analogous to ARSVO, participants expressed concerns (Table 2) about the quality of information they would need when carrying out their daily tasks remotely. Participants' main concern was that the sense of "realism" may be lowered if the remote control felt too game-like, whereby they feel too "safe" and physically and mentally detached from their environment and mistakes. The examples given were similar to the ones experienced in the simulator with difficulties in perception when completing tasks if cut off from physical senses (e.g. sound, smell and feel) and the physical ability to check systems, environment, engine, bow thrusters and cargo. Participants also noted that this sensorial deprivation would lead to lower levels of SA in certain situations like the master/pilot information exchange. Whilst in remote operations this exchange could occur via video call, it could lead to a weakening in the trusted relationship between crew and pilot within Bridge Resource Management (BRM), as well as a transfer of local knowledge. As Munir et al. (2022) states, sensory data forms a vital part of enhancing SA. Thus, adequate replacements would be needed for safe remote control. When asked to expand on this, many participants were not sure how accurate or trustworthy the technology used to "replace their senses" would be.

During the second simulation exercise, participants were able to maintain SA to the end. The response from cadets differed from mid to senior experience responses. This difference was clearly seen as "experiential learning" with the experienced crew using their knowledge to work within well-established organised communication processes. However, with this incident being unavoidable regardless of reaction time it raised interesting questions when considering the same scenario for MASS degree 3 with remote crew. In this case, arguably the simulator represents remote operations within an ROC. Was the response time positively or negatively affected (i.e. shortened/lengthened) as the crew were relying on only digital data for SA, not physically onboard? Moreover, if this vessel was fully autonomous and suddenly switched to manual control when the attack was triggered, what impact would this have on the remote crew? What training, or technologies, are needed to prevent these issues?

Degree of Automation	**Recommendations for skill requirements**	**Situational Awareness Challenges**
One	This entirely remains applicable	What we perceive today or current SA challenges
Two	Skills need to be amended to introduce new technology and/or automated processes	Maritime cyber awareness, reliance on navigation alarm response, emergency responses. Monitoring autonomous elements and using that information to inform decisions. Challenges include maintaining SA on individual tasks.
Three	Introduce the relationship between the remote and the seafarer on board	Multi-ship operations, maritime cyber awareness, reliance on navigation equipment, alarm response, emergency responses, not being able to physically sense and check systems. Challenges include maintaining SA on a higher ship-wide, multi-ship and sometimes fleet level.
Four	No seafarers on board	Challenges include maintaining SA on a higher ship-wide level, and sometimes a fleet-level over a long period of time as the vessel primarily makes decisions itself.

Table 2: SA challenges for each degree of automation, and RSE recommendations for skill requirements (IMO, 2021)

When discussed during the debrief navigators with more experience stated that adequate triangulation techniques, which are currently implemented for monitoring practices (such as PI line, radar overlay on ECDIS and manual position fixing) and that emergency response procedures, will need to be used with previously acquired maritime cybersecurity knowledge to handle cyber incidents and emergency situations.

Other main themes identified regarding degree 2-4 automation, were growing commercial pressures, and if office-based crews would then be responsible for multiple vessels (i.e. multi-ship management) (Tam et al., 2021). Being expected to maintain SA for multiple vessels, in a variety of situations, due to commercial pressures was a common concern. Similarly, there were reservations on how alarm response and emergency responses would be handled in such a scenario. Other general operational challenges included what COLREGS, regulations regarding pilotage, logbooks, and route planning, including weather conditions, would look like in a remotely controlled world. For this, some have started to suggest and introduce approaches such as operational envelopes for hand-over constraints with response times to react according to different operational scenarios (Fjortoft and Holte, 2022). Others have introduced technological approaches to aid operators in taking decisions such as the Quickly Getting Into the Loop Display (QGILD) which communicates deviations needed to help attain rapid SA (Porathe, 2022). However, these proactive approaches towards risk management for the interaction between humans and automation do not consider maritime cyber risks as part of those approaches.

4.2 Cybersecurity affecting SA

Another theme identified by the participants was the relationship between SA and cybersecurity. As part of the questionnaire, cadets were asked to indicate whether they were aware of IMO Resolution MSC428(98) (Maritime Cyber Risk Management in Safety Management Systems). Only 30% of the cadets responded "Yes", indicating a lack of awareness of the significant regulations affecting their operations. Interestingly, real-world experience seems to have had a positive effect on this as those who have had commercial operational experience were aware of this resolution as they have experienced some form of cyber risk management training on board. Moreover, all experienced navigators provided the correct order for the different stages of a cyber attack (survey, delivery, breach and pivot) compared to only 22.5% of cadets. The type of vessel participants served on did not seem to have a noticeable effect on this. However, it was stated by experienced navigators that response to a cyber incident may vary according to ship type due to operational training and Safety Management System (SMS) procedures. On a more positive note, during the simulation exercises, participants were acutely more aware of the link between cybersecurity and their operations if remotely over a digital link. One group commented that a remote crew may have less time to react to an incident due to latency in command-and-control communications due to weather patterns or geography.

During the questionnaire (as shown in Figure 3), participants did not consider insider cyber threats to be a large threat, with only 2.5% of cadets' responses indicating as such and none for experienced navigators. However, as Khan et al. (2021) illustrates the insider represents a credible threat to the sector. The more obvious options of criminals, terrorists and state-sponsored actors were all identified with a high rate (>82.5%) among cadets and almost 100% among experienced navigators. Interestingly, participants somewhat contradicted themselves

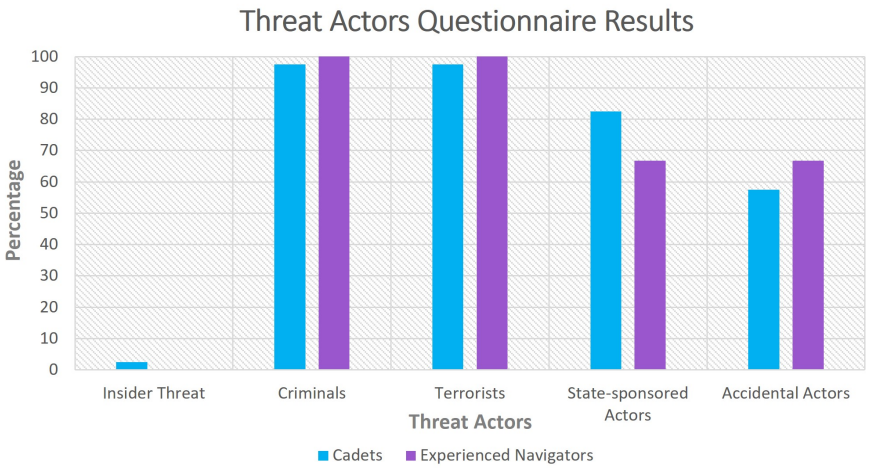

Figure 3: Questionnaire results on threat actors identified that could be responsible for a cyber attack affecting the maritime sector (by cadets and experienced navigators)

by considering the human element as an area of risk, with 57.5% of cadets' responses and 66.7% of experienced navigators indicating they considered accidental actors as a threat. This theme of human weakness was a core focus of several groups during the tabletop exercises as well, whereby topics of concentration, self-preservation, lack of training, legal issues and access to operation critical information, were deep concerns when considering maritime autonomy. Consequently, whilst navigators consider the human element as a risk during operations further needs to be done so that the relationship between the human element, cybersecurity and SA is assimilated.

4.3 Trust in digital systems

A significant challenge of maintaining remote control SA is whether the user trusts the system. Trust in an inaccurate system, and distrust in an accurate system, can both detrimentally influence user actions (Felski and Zwolak, 2020). In the questionnaire, 12.5% of cadets and 33.3% of experienced navigators indicated that they strongly trusted the systems they use to navigate, and 82.5% of cadets and 66.6% of experienced navigators noted they only slightly trusted their systems. However, during the first simulation exercise, it took on average 8 minutes for cadets and mid younger generation experience navigators to stop trusting a compromised system. This suggests that, while both groups of participants may be aware of untrustworthy (i.e. unsecured) systems, many are still subconsciously inclined to trust them during familiar operations.

The implicit trust by the less experienced navigators could be in part due to the use of the simulator, which was set up by an instructor prior to the exercise starting. As this instructor is part of their daily academic training they are potentially viewed as an authority figure by the cadets. Cadets may accept that the instructor has set up devices correctly with the optimal information presented and not question it. However, this is not largely different from a new navigator during their familiarisation period on a new ship, they should be aware of the techniques they need but might not be aware of how to implement them on this particular device. Therefore, they could, and in real operations, they would seek guidance from a more experienced navigator. This also suggests that modern technology and/or cadets and junior officers rely more heavily on digital aids such as GNSS, promoting a high level of trust in them. This is not inherently bad, but rather a recognition that trainers should be aware of the trust navigators place in such systems. Thus, trainers should also equip them with the skills to interrogate, correlate, and validate digital information as well as the importance of an organisational culture that promotes early career and newly qualified personnel to perform operations and take risks in a controlled environment under supervision. This may also help prevent maritime accidents as the experience and knowledge would not be kept by top ranks within BRM, they will help promote resilience by speaking up about any system and human failures (such as single point of failure) benefiting the long-term high-quality service within the organisation.

In comparison senior, experienced, navigators during the first simulation exercise detected the GPS drift instantly and the decision to communicate the incident from happening was delayed by 15 seconds so that the information was better processed, analysed, and communicated with the right strategy for the bridge team to recover full SA. Moreover, their response, implementing redundancies, recovered the ship's position effectively. Furthermore, the group provided a good example of possible response procedures including the internal reporting mechanisms on the vessel (calling the Electronic Technical Officer (ETO) to investigate the cause of the error) as well as external (calling other ships in the vicinity, Vessel Traffic Service (VTS), company, manufacturer, next port of call port authority). Thus, demonstrated how operational experience may enhance a better response. Additionally, it was also noted that if this scenario was placed with a more subtle gradual drift or in the middle of other instructions (such as alteration of course) or with the radar image compromised so that it matched with GNSS signal (Longo et al., 2023b) or from shared experience when transiting high traffic areas such as the Malacca Strait this incident would not have been spotted. Furthermore, it was also stated that the response between seafarers may vary according to ship type operating and training procedures, as well as onboard organisational culture.

4.4 Roles and responsibilities for future remote operations

Participants broadly identified the following responsibilities as those likely to remain, just in a different guise, regardless of future levels of automation:

- Maintaining watch
- Communication responsibilities
- Collision avoidance
- Safe and efficient function
- Command hierarchies
- Maintenance

Of those listed, maintenance responsibilities are most likely to change considering the physical distance between crew and vessel. Participants also saw autonomy as an opportunity for companies to consolidate many of these responsibilities, for several ships, and place those responsibilities on smaller remote teams. While MASS prototypes, and their control, are still very much in their infancy, it is still important to consider the impact of commercial pressures on the human-in-the-loop and ROC. As per Zhang and Zhang (2023) ROs in ROC will process a lot of data, some of which will be mission/safety critical during incident response such as cyber-attacks to preserve SA, collaborate or communicate within ROC.

Consequently, a more adaptative and flexible approach to safety management tasks will be needed to strengthen the construction and operation of ROC (Mallam et al., 2020). As an example Dittmann et al. (2021) highlighted the use of the International Convention STCW as a basis to address the co-design of on-board systems in an ROC emphasising the importance of human assistance, information sharing and digestion between human and machine is and will remain to be crucial to maintain safe operations. Thus, these new practices need to be developed and gradually introduced into the management system (Luchenko et al., 2023). To achieve this organisations could make use of a Human-Centre Design (HCD) process (e.g. with the creation of a stakeholder map that highlights the importance of human factor issues of ROC operators in an organisational context) which needs to run simultaneously with the technology innovation so that designers can understand the business model of the organisation, the operational needs of the ROC operators, and technology developers and customers (Veitch et al., 2020).

When asked if a cyber-attack could cause a catastrophic event (e.g. collision, pollution, loss of life), 92.5% of cadets agreed it was possible to some degree, and 100% of experienced navigators strongly agreed especially as vessels operating at remote degrees 2-4 would be heavily reliant on technology and connectivity (not only meaning possible disruption, also delays when receiving digital data from screens). Thus, participants discussed changes in their responsibilities that could reduce the possibility of a catastrophic event through information verification, and better cybersecurity. Participants also stressed that good communication and team management skills would remain a key factor. It was also noted that the type of communication will evolve as their roles and responsibilities as an operator will be integrated within ROC's organisational structure and operation (Lynch et al., 2023). A multi-stakeholder environment was especially highlighted when dealing with cyber incidents as operators may need to work in parallel with a cybersecurity technical advisor or incident team (like Maritime-Security Operation Centres (M-SOC's) as explained in Nganga et al. (2022)) internally within ROC and externally with different organisations (such as in the UK for maritime the Joint Maritime Security Centre (JMSC)) to deal with situations similar to the one experienced in the full bridge simulator. Representative exercise scenarios have been used by Raimondi et al. (2022) to demonstrate and define that SOC analysts need specific skills and knowledge to operate in the maritime environment. Furthermore, Jacq et al. (2018) emphasised the complexity of attaining cyber situation awareness of maritime information systems at SOC. This demonstrates the need for a standardised joint cyber incident decision-making framework and training to create and enhance joint organisational learning strategies which could help sustain capabilities across organisations (Pöyhönen et al., 2021). Additionally, as stated by senior navigators there is a necessity to develop and provide further regulations in cybersecurity as part of these operations as currently, these are minimal.

Many of the cadets also wanted to maintain the seafarer lifestyle as it provided them with the experience of working in a multicultural environment as part of a team. Working in an office setting had less appeal for many. Although, preserving that aspect of culture may be essential now future ROC will provide more attractive aspects that will help ROs' and their families' well-being (Tam et al., 2021; Abila et al., 2023). This could include high-quality work-life balance, workforce long-term talent retention, higher quality of training more frequently, more inclusive hiring scope, and a high level of well-being support from personnel at ROC to operators during and after accident occurrence including access to medical help.

4.5 Training needed for future remote operations

Managing the transition to, and associated risks of, remote operations is vital to ensure the safety of those operations. Thus, it is vital to consider the training, qualifications and experience of operators as a way to reduce the risks posed by the human element (Berg, 2013). As Hopcraft et al. (2022) argue, training is only effective if it changes the behaviours of crew. When asked, 75% of cadets indicated that training would be needed to detect, report, and stop a cyber-attack on board a vessel (as shown in Figure 4). Of concern is that 20% were neutral and 5% disagreed that training would help. As these responses were collected prior to the simulation exercises several participants commented how their initial impression was wrong. Additionally, 100% of experienced navigators indicated that training would be needed for the above. Many cadets during the tabletop exercise identified multi-ship operations as a new skill set required for remote control operations. Experience navigators on this stated that this multi-ship operation will be similar to air traffic control stations or VTS when overseeing the fleet from ROC. However, during interventions and direct ship remote control, especially for congested water and port ar-

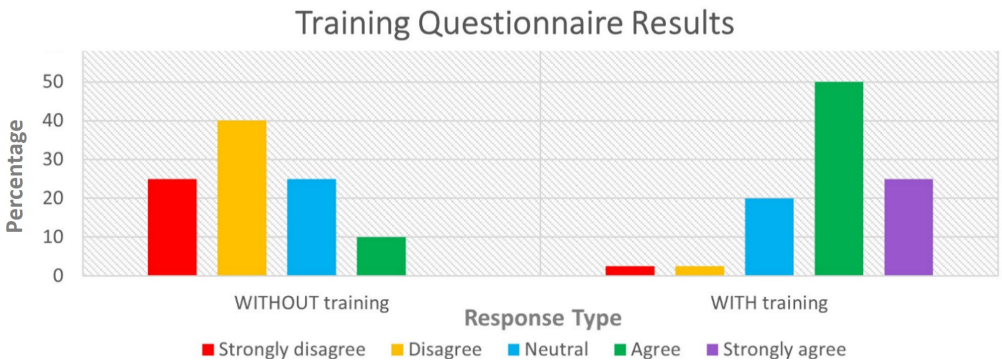

Figure 4: Questionnaire results when asked if a mariner could detect, report, contain or eradicate a cyber attack (by cadets)

rival/departure procedures would need to be done in isolation. Emergency response training for remote operations was rated highly among all participants, following the simulator exercises. It was also highlighted that there was a need to develop skills to validate information using the same practices with a deeper maritime cybersecurity awareness and knowledge as highlighted in Section 4.1. Additionally, the authors also noticed some disconnects between the written survey answers and the behaviours of cadets and mid-experience navigators. Particularly around the perception of insider vulnerabilities, and levels of actual trust in the systems. What participants said in a classroom setting did not always match their actions in the simulator, a gap in perception that can be mitigated with awareness training and cultural changes.

To this end, Marit et al. (2022) explored the competency standards of ROs (including the analysis from (DNV, 2022) which also incorporates recommended practice) for the contribution and development of new training in the operational management of autonomous vessels. Results from this research demonstrated the essential need for the integration of both technical and non-technical skills into RO competencies for a successful training scheme with a special focus on mundane work and emergencies. Among the new skills and competencies both Ceylani et al. (2022) and Zagan et al. (2022) highlighted that is crucially important for ROCs to adopt a cybersecurity action plan so that operators have the ability to implement cybersecurity management measures. In this regard, Relling et al. (2021)'s approach to systems engineering (and Endlsey (2019) in aviation safety) combines Design Research Methodology (DRM), and Human-Centred Design (HCD) in the design phase. This allows system designers to understand the effects on, and between, the socio-technical system involving the end users (such as maritime pilots and navigators) for ROC. This process seems to be a necessity in the design and operations of an ROC as they are a highly multi-disciplinary working environment.

Effective cybersecurity training for remote operations will need to be implemented in combination with a connectivist and constructivist learning approach similar to Erstad et al. (2023a) with the use of an HCD process in maritime simulators. Moreover, it would be necessary to involve all members in cyber incident management from operators, incident management team, company fleet management and external organisations (such as VTS, Coastguard and port authorities). Consequently, a holistic joint training involving personnel at all levels within the organisation with other entities (within the ecosystem of ARSVO) would enhance organisations resilience and embed a shared response vision across organisations against cyber incident occurrence (Wróbel et al., 2020).

Accordingly, MASS level 3-4 operations are not yet fully introduced, therefore, it is difficult to specify the exact training needed for these operations, especially for cybersecurity. However, to improve the alignment between humans and autonomous technology, organisations will need a culture that promotes adaptability to changing conditions such as the adhocracy organisational culture which drives innovation, risk-taking and adaptability for the long-term effectiveness and innovation entrepreneurial orientation (Hartnell et al., 2011).

Moreover, a proactive re-evaluation of training may be required in addition to some re-evaluation around the design of remote-control autonomy technology. Such an adjustment for future remote operations will require either new legislation or amendments to existing requirements as per identified gaps by AutoShip (2023) like the process of including cyber risk management within the International Safety Management (ISM) Code and International Association of Classification Societies (IACS) with the Unified Requirements (UR) E26 and E27. One such amendment could be the creation of new competencies for remote operations within the STCW Convention.

5 Limitations and Future Research

Due to the need for physical access to the simulator the participant group comprised of cadets enrolled at the University and a small number of experienced navigators. To ensure the participants could engage effectively with

the given scenarios final year cadets were selected. However, 35% had no sea time experience, with a further 40% having less than a year. Thus, some participants lack real-world experiences of manual operations so their views on remote operations may be limited. Further research would benefit from a larger experienced group with an average age closer to the industry average of 34 (Bergeron, 2018). Similarly, a group with greater diversity in educational, national and cultural backgrounds would be a better representation (Janićijević, 2019).

The diversity of opinions within the discussions highlights that we need a range of experiences both culturally and operationally to be involved as they differ in risk perception or SA processes for decision-making. As highlighted by the senior experienced navigator every crew member, crew team, ship, operations and company are different. Therefore, whilst it might be impossible to get a perfect representation of experience in several small groups, ongoing work would use as many groups as possible with the widest range of experiences to help develop these findings further. Alongside the diversity of experiences impacting the responses to questions, further studies would suggest more specific questions in order to identify gaps needing to be filled by specified training approaches for ARSVO.

The diversity of opinions within the discussions highlights the need to include operators within the design phase of remote vessels, and control centres. This inclusion should be ongoing, and with remote operation projects still in their infancy, the opportunity remains available. However, with access to these groups, potentially limited further research could engage with more mature remote surface vessel organisations within commercial shipping already involved with large automation projects and other transport sectors remote organisations such as UAVs.

As discussed, the transition to a fully autonomous world fleet will continue to develop without completely removing the human element for monitoring, supervision and intervention for remote direct ship control. Therefore, as the sector adds more autonomy to systems, it must consider whether this has been done in such a way as to allow the human element to maintain an appropriate level of SA if that system fails. Therefore, technology must adjust to mariner needs as well as business and environmental needs. Further work could consider joint training across operational and management levels that an ROC could have, from the operator experiencing the information in the specific system(s) used to how this could be transferred across an incident team, fleet management level and externally (such as VTS, Coastguard, port authority and government) to deal with system failure emergency situations and understand how the different layers of departments adjust within the organisation structure for the safety and resilience of operations and perceived commercial benefits.

At this early stage of marine autonomy, there are many questions identified by this work that remain unanswered. Given the importance of commercial shipping to the world and the rise in both autonomy and cyber-threats, it is important to address these in future work building on these tabletop exercises, scenarios, and surveys. In addition to undertaking training and awareness sessions with more mariners across different sectors of the industry, future research could consider the following questions:

1. How do response practices for both imminent and non-imminent safety-critical situations need to be implemented when suspected cyber attack in a ROC?

2. What knowledge is needed by ROC operators to deal with maritime cybersecurity incidents? Would a training approach involving teams across the ROC internally or between ROCs externally? How would these drills and training exercises need to be implemented within ROC, how regularly and would it vary due to ship-type operations? How would the maritime cyber awareness subject be best introduced in Maritime Education and Training (MET) institutions for the benefit of the study?

3. Would the roles or responsibilities for ROs adjust to what appears to be with a different organisational structure within ROC?

4. How much training for remote operations would be based on simulation (Hwang et al., 2022)? How much training in remote simulator operations would be needed to obtain SA or "trusted relationship" of the vessel according to systems, manoeuvrability and operations? Could future simulation and remote operations be implemented similarly to UAV remote operations (Lynch et al., 2022)? Would sea time still be required (Karlis, 2018)? Would augmented reality and/or virtual reality be needed to be used to interact with other stakeholders for future remote operations (such as remote pilotage, VTS or incident management team with technical advisors) and/or training (Gernez et al., 2020; Arjoni et al., 2023)?

6 Conclusions

Based on the discussions and observations completed as part of this study, five main challenges for the future of maritime autonomy were identified:

1. Current cyber awareness in the maritime sector is low, which could have a long-term impact on SA such as over-trusting digital aids, coupled with a lack of skills to validate information.

2. What regulations and guidelines from the IMO and other entities such as classification societies need to be incorporated and/or changed in regards to training and education programmes, especially with the incorporation of autonomous technology the cyber-threat landscape changes, and how this should be adapted within future ROC organisations SMS for a long-term sustainable change?

3. How can critical decision-making be affected by trust in inaccurate data or distrust in an accurate system?

4. How can the overreliance on digital aids be reduced with different practices and awareness training?

5. How could being removed from the physical ship hinder an operator's ability to sense and check safety?

In conclusion, this study has considered some of the challenges in cybersecurity, trust and mariners SA as the maritime sector moves towards remote and fully autonomous operations. The ability of ROs to operate safely is contingent on their knowledge and skills. Primarily among those is the need to interact with digital systems, whereby operators need to be equipped with the appropriate knowledge, skills and experience to be able to do so safely. Through these findings, we believe that future mariner training needs to focus on providing these skills to operators whilst considering the new skills required for monitoring (e.g. multi-ship management), supervision and intervention with direct control (including communication skills for incident management across departments). As a result, this type of workshop helps increase the awareness of experienced navigators and also early career navigators. Feedback from these exercises implies that implementation of these types of exercises within MET institutions could help increase cyber awareness across the workforce in the future. Furthermore, this could also help in the creation of new amendments to competencies for MASS within the STCW Convention.

Acknowledgment

This paper is partly funded by the research efforts under Cyber-MAR and Reardon Smith Nautical Trust.

Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

The authors would also like to thank Tom Crichton, Tim Davies, Avanthika Vineetha Harish, Wesley Andrews, Luke Christison and all those who participated.

References

Abila, S., Kitada, M., Malecosio Jr, S., Tang, L., Subong-Espina, R., 2023. Empowering Seafarers as Agents of Their Mental Health: The Role of Information and Communication Technology in Seafarers' Well-Being. Inquiry: a journal of medical care organization, provision and financing 60, 469580231162752. doi:10.1177/00469580231162752.

Ahvenjärvi, S., 2016. The Human Element and Autonomous Ships. TransNav 10, 517–521. doi:10.12716/1001.10.03.18.

Arjoni, D.H., de Souza Rehder, I., Figueira, J.M.P., Villani, E., 2023. Augmented reality for training formation flights: An analysis of human factors. Heliyon 9, e14181. URL: https://doi.org/10.1016%2Fj.heliyon.2023.e14181, doi:10.1016/j.heliyon.2023.e14181.

AutoShip, 2023. D8.2 - Roadmap for Autonomous Ship Adoption and Development. URL: https://www.autoship-project.eu/wp-content/uploads/2023/03/Roadmap-for-Autonomous-ship-adoption-and-development.pdf.

Berg, H.P., 2013. Human Factors and Safety Culture in Maritime Safety. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation 7, 343–353. doi:10.12716/1001.07.03.04.

Bergeron, S., 2018. Crewing demographic timebomb laid bare. Splash URL: https://splash247.com/crewing-demographic-timebomb-laid-bare/#:~:text=In%20the%20offshore%20industry%2C%20averages,55%20and%20older%20has%20grown.

Cardiff University and Allianz, 2012. Safety and Shipping 1912-2012: From Titanic to Costa Concordia. Report. URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review-2012.pdf.

Castro, D., Conceição, V., Campaniço Cavaleiro, S., 2022. PNT Resilience and the Impact of Satellite Radio Positioning Disruptions on Piloting Teams, in: Conference Proceedings of INEC. doi:10.24868/10697.

Ceylani, E., Kolcak, I., Solmaz, M., 2022. A Ranking of Critical Competencies for Future Seafarers in the Scope of Digital Transformation, in: The International Association of Maritime Universities (IAMU) Conference.

Chae, C.J., Kim, M., Kim, H.J., 2020. A Study on Identification of Development Status of MASS Technologies and Directions of Improvement. Applied Sciences 10, 4564. URL: https://dx.doi.org/10.3390/app10134564, doi:10.3390/app10134564.

Chan, J., Golightly, D., Norman, R., Pazouki, K., 2023a. Perception of Autonomy and the Role of Experience within the Maritime Industry. Journal of Marine Science and Engineering 11, 258. URL: https://dx.doi.org/10.3390/jmse11020258, doi:10.3390/jmse11020258.

Chan, J.P., Pazouki, K., Norman, R.A., 2023b. An experimental study into the fault recognition of onboard systems by navigational officers. Journal of Marine Engineering & Technology 22, 101–110. URL: https://dx.doi.org/10.1080/20464177.2022.2143312, doi:10.1080/20464177.2022.2143312.

Cho, S., Orye, E., Visky, G., Prates, V., 2022. Cybersecurity Considerations in Autonomous Ships. NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous_Ships.pdf.

Cozzens, T., 2019. Iran jams GPS on ships in Strait of Hormuz. URL: https://www.gpsworld.com/iran-jams-gps-on-ships-in-strait-of-hormuz/TracyCozzens.

Digitalisation World, 2020. Why Organisations Are Facing An Automation Conundrum. URL: https://m.digitalisationworld.com/blogs/55956/why-organisations-are-facing-an-automation-conundrum.

Dittmann, K., Hansen, P.N., Papageorgiou, D., Jensen, S., Lützen, M., Blanke, M., 2021. Autonomous Surface Vessel with Remote Human on the Loop: System Design for STCW Compliance, in: 13th IFAC Conference on Control Applications in Marine Systems, Robotics, and Vehicles CAMS 2021, Elsevier BV. pp. 224–231. URL: https://doi.org/10.1016%2Fj.ifacol.2021.10.097, doi:10.1016/j.ifacol.2021.10.097.

Dutch Safety Board, 2016. Marine Incidents: Grounding of "Nova Cura". URL: https://legacy.iho.int/mtg_docs/com_wg/NCWG/NCWG4/NCWG4-10.2%20-%20%20Incident%20Nova%20Cura.pdf.

Endlsey, M.R., 2019. Human factors & aviation, in: Hearing on Boeing 737-Max8 Crashes. URL: https://docs.house.gov/meetings/PW/PW00/20191211/110296/HHRG-116-PW00-Wstate-EndsleyM-20191211.pdf.

Endsley, M.R., 2015. Situation Awareness Misconceptions and Misunderstandings. Journal of Cognitive Engineering and Decision Making 9, 4–32. doi:10.1177/1555343415572631.

Endsley, M.R., 2017. From Here to Autonomy. Human Factors: The Journal of the Human Factors and Ergonomics Society 59, 5–27. URL: https://dx.doi.org/10.1177/0018720816681350, doi:10.1177/0018720816681350.

Endsley, M.R., 2023. Ironies of artificial intelligence. Ergonomics , 1–13URL: https://dx.doi.org/10.1080/00140139.2023.2243404, doi:10.1080/00140139.2023.2243404.

Erstad, E., Hopcraft, R., Harish, A.V., Tam, K., 2023a. A human-centred design approach for the development and conducting of maritime cyber resilience training. WMU Journal of Maritime Affairs URL: https://doi.org/10.1007%2Fs13437-023-00304-7, doi:10.1007/s13437-023-00304-7.

Erstad, E., Hopcraft, R., Palbar Misas, J.D., Tam, K., 2023b. CERP A Maritime Cyber Risk Decision Making Tool. TransNav the International Journal on Marine Navigation and Safety of Sea Transportation 17, 269. doi:10.12716/1001.17.02.02.

Felski, A., Zwolak, K., 2020. The Ocean-Going Autonomous Ship—Challenges and Threats. Journal of Marine Science and Engineering 8, 41. URL: https://dx.doi.org/10.3390/jmse8010041, doi:10.3390/jmse8010041.

Fjortoft, K., Holte, E., 2022. Implementing operational envelopes for improved resilience of autonomous maritime transport, in: Human Factors in Transportation. AHFE (2022) International Conference. URL: http://doi.org/10.54941/ahfe1002507.

Gernez, E., Nordby, K., Eikenes, J.O., Hareide, O.S., 2020. A review of augmented reality applications for ship bridges. NECESSE 5, 159–186.

Ghaderi, H., 2019. Autonomous technologies in short sea shipping: trends, feasibility and implications. Transport Reviews 39, 152–173. doi:10.1080/01441647.2018.1502834.

Gutzwiller, R., Dykstra, J., Payne, B., 2020. Gaps and Opportunities in Situational Awareness for Cybersecurity. Digital Threats 1. doi:10.1145/3384471.

Hammernes, A., 2022. SITUATIONAL AWARENESS - ENHANCING SAFETY AND EFFICIENCY. Kongsberg. URL: https://www.kongsberg.com/maritime/products/situational-awareness/.

Hartnell, C.A., Ou, A.Y., Kinicki, A., 2011. Organizational culture and organizational effectiveness: A meta-analytic investigation of the competing values framework's theoretical suppositions. Journal of Applied Psychology 96, 677–694. URL: https://doi.org/10.1037%2Fa0021987, doi:10.1037/a0021987.

Health and Safety Executive, 2012. Knowing what is going on around you (situational awareness). URL: https://www.hse.gov.uk/construction/lwit/assets/downloads/situational-awareness.pdf.

Hoff, K.A., Bashir, M., 2015. Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. Human Factors 57, 407–434. URL: https://doi.org/10.1177/0018720814547570, doi:10.1177/0018720814547570, arXiv:https://doi.org/10.1177/0018720814547570. pMID: 25875432.

Hopcraft, R., Tam, K., Dorje Palbar Misas, J., Moara-Nkwe, K., Jones, K., 2022. Developing a maritime cyber safety culture: Improving safety of operations. Maritime Technology and Research 5, 258750. URL: https://dx.doi.org/10.33175/mtr.2023.258750, doi:10.33175/mtr.2023.258750.

Hwang, H., Hwang, T., Youn, I.H., 2022. Effect of Onboard Training for Improvement of Navigation Skill under the Simulated Navigation Environment for Maritime Autonomous Surface Ship Operation Training. Applied Sciences 12, 9300. URL: https://doi.org/10.3390%2Fapp12189300, doi:10.3390/app12189300.

IMO, 1964. International Maritime Organization MSC VIII/11 - Automation in Ships.

IMO, 2003. Convention on the International Regulations for Preventing Collisions at Sea, 1972. IMO, IMO.

IMO, 2018. International Maritime Organization MSC100/20 add.1 - Report of the maritime safety committee on its 100th session.

IMO, 2020. Safety of Life at Sea Convention. IMO, IMO.

IMO, 2021. International Maritime Organization MSC.1/Circ.1638 - Outcome of the Regulatory Scoping Exercise for the use of Maritime Autonomous Surface Ships (MASS).

IMO, 2022. MSC 106/5 - Development of a Goal-Based Instrument for Maritime Autonomous Surface Ships - Report of the MSC-LEG-FAL Joint Working Group on MASS on its First Session.

IMO, 2023. MSC 107/5-1 - 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) on its Second Session.

Independent Online, 2023. A ferry that ran aground repeatedly off the swedish coast is leaking oil and is extensively damaged. URL: https://www.independent.co.uk/news/swedish-ap-baltic-sea-stockholm-marco-polo-b2438488.html.

Issa, M., Ilinca, A., Ibrahim, H., Rizk, P., 2022. Maritime Autonomous Surface Ships: Problems and Challenges Facing the Regulatory Process. Sustainability 14. URL: https://www.mdpi.com/2071-1050/14/23/15630, doi:10.3390/su142315630.

Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., Simonin, J., 2018. Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre, in: 2018 2nd Cyber Security in Networking Conference (CSNet), pp. 1–8. doi:10.1109/CSNET.2018.8602669.

Janićijević, N., 2019. The Impact of National Clture on Leadership. Economic Themes 57, 127–144. URL: https://dx.doi.org/10.2478/ethemes-2019-0008, doi:10.2478/ethemes-2019-0008.

Johansen, T., Utne, I.B., 2024. Human-autonomy collaboration in supervisory risk control of autonomous ships. Journal of Marine Engineering & Technology 0, 1–19. doi:10.1080/20464177.2024.2319369.

Jones, M., 2017. Spoofing in the Black Sea: What really happened? URL: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/.

Karlis, T., 2018. Maritime law issues related to the operation of unmanned autonomous cargo ships. WMU Journal of Maritime Affairs 17, 119–128. URL: https://doi.org/10.1007/s13437-018-0135-6, doi:10.1007/s13437-018-0135-6.

Khan, N., J. Houghton, R., Sharples, S., 2021. Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks. Cognition, Technology & Work URL: https://dx.doi.org/10.1007/s10111-021-00690-z, doi:10.1007/s10111-021-00690-z.

Lateef, F., 2010. Simulation-based learning: Just like the real thing. Journal of emergencies, trauma, and shock 3, 348–352. URL: https://pubmed.ncbi.nlm.nih.gov/21063557https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2966567/, doi:10.4103/0974-2700.70743.

Lee, J.D., See, K.A., 2004. Trust in Automation: Designing for Appropriate Reliance. Human Factors: The Journal of the Human Factors and Ergonomics Society 46, 50–80. URL: https://dx.doi.org/10.1518/hfes.46.1.50_30392, doi:10.1518/hfes.46.1.50_30392.

Longo, G., Orlich, A., Merlo, A., Russo, E., 2023a. Enabling Real-Time Remote Monitoring of Ships by Lossless Protocol Transformations. IEEE Transactions on Intelligent Transportation Systems 24, 7285–7295. doi:10.1109/TITS.2023.3258365.

Longo, G., Russo, E., Armando, A., Merlo, A., 2023b. Attacking (and defending) the maritime radar system. IEEE Transactions on Information Forensics and Security 18, 3575–3589. doi:10.1109/TIFS.2023.3282132.

Luchenko, D., Georgiievskyi, L., Bielikova, M., 2023. Challenges and Developments in the Public Administration of Autonomous Shipping. Lex Portus 9. URL: https://doi.org/10.26886%2F2524-101x.9.1.

2023.2, doi:10.26886/2524-101x.9.1.2023.2.

Lynch, K.M., Banks, V.A., Roberts, A.P.J., Downes, J., Radcliffe, S., Plant, K.L., 2023. The application of a system-based risk management framework and social network analysis to the Maritime Autonomous Surface Ship system: Who are the decision-makers in the wider system? Human Factors and Ergonomics in Manufacturing & Service Industries 33, 395–429. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/hfm.21000, doi:https://doi.org/10.1002/hfm.21000, arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/hfm.21000.

Lynch, K.M., Banks, V.A., Roberts, A.P.J., Radcliffe, S., Plant, K.L., 2022. What factors may influence decision-making in the operation of Maritime Autonomous Surface Ships? a systematic review. Theoretical Issues in Ergonomics Science 0, 1–36. doi:10.1080/1463922X.2022.2152900.

MAIB, 2019. Grounding of general cargo vessel Pircilla. URL: https://www.gov.uk/maib-reports/grounding-of-general-cargo-vessel-priscilla.

Mallam, S.C., Nazir, S., Sharma, A., 2020. The human element in future Maritime Operations – perceived impact of autonomous shipping. Ergonomics 63, 334–345. URL: https://dx.doi.org/10.1080/00140139.2019.1659995, doi:10.1080/00140139.2019.1659995.

Marit, W.A., t Knogsvik, Lamvik, G.M., 2022. Operational management of autonomous ships: A need for new competence and resilience skills., in: MARESEC 2022. Bremerhaven, Germany.

Maritime and Coastguard Agency, 2016. Marine Guidance Notice (MGN) 520 (m) human element guidance. URL: https://www.gov.uk/government/publications/mgn-520m-human-element-guidance.

Mehta, R., Winter, S.R., Rice, S., Edwards, M., 2021. Are passengers willing to ride on autonomous cruise-ships? Maritime Transport Research 2, 100014. URL: https://dx.doi.org/10.1016/j.martra.2021.100014, doi:10.1016/j.martra.2021.100014.

Misas, J., Hopcraft, R., Tam, K., 2022. Future of Maritime Autonomy: Cybersecurity, Trust and Mariner's Situational Awareness. URL: https://dx.doi.org/10.24868/10703, doi:10.24868/10703.

Munir, A., Aved, A., Blasch, E., 2022. Situational Awareness: Techniques, Challenges, and Prospects. AI 3, 55–77. doi:10.3390/ai3010005.

Nganga, A., Lutzhoft, M., Scanlan, J., Mallam, S., 2022. Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment, in: CYBER 2022: The Seventh International Conference on Cyber-Technologies and Cyber-Systems.

Porathe, T., 2022. Remote Monitoring ofAutonomous Ships: Quickly Getting into the Loop Display (QGILD), in: Human Factors in Transportation. AHFE (2022) International Conference. URL: http://doi.org/10.54941/ahfe1002506.

Pöyhönen, J., Kovanen, T., Lehto, M., 2021. Basic elements of cyber-security for an Automated Remote Piloting, in: 16th International Conference on Cyber Warfare and Security 2021. doi:10.34190/IWS.21.021.

Raimondi, M., Longo, G., Merlo, A., Armando, A., Russo, E., 2022. Training the Maritime Security Operations Centre Teams, in: 2022 IEEE International Conference on Cyber Security and Resilience (CSR), pp. 388–393. doi:10.1109/CSR54599.2022.9850324.

Relling, T., Lützhöft, M., Ostnes, R., Hildre, H.P., 2021. The contribution of Vessel Traffic Services to safe coexistence between automated and conventional vessels. Maritime Policy & Management 49, 990–1009. URL: https://doi.org/10.1080%2F03088839.2021.1937739, doi:10.1080/03088839.2021.1937739.

Rice, S., 2019. Would you Fly on a Plane Without a Human Pilot? URL: https://www.forbes.com/sites/stephenrice1/2019/01/07/would-you-fly-on-a-plane-without-a-human-pilot/?sh=7c6b84e32518.

Rieth, M., Hagemann, V., 2022. Automation as an equal team player for humans? – a view into the field and implications for research and practice. Applied Ergonomics 98, 103552. URL: https://www.sciencedirect.com/science/article/pii/S000368702100199X, doi:https://doi.org/10.1016/j.apergo.2021.103552.

Rodseth, O.J., Lien Wennersberg, L.A., Nordahl, H., 2022. Towards approval of autonomous ship systems by their operational envelope. Journal of Marine Science and Technology 27, 67–76. URL: https://doi.org/10.1007/s00773-021-00815-z, doi:10.1007/s00773-021-00815-z.

Salas, E., Bowers, C.A., Rhodenizer, L., 1998. It Is Not How Much You Have but How You Use It: Toward a Rational Use of Simulation to Support Aviation Training. The International Journal of Aviation Psychology 8, 197–208. URL: https://dx.doi.org/10.1207/s15327108ijap0803_2, doi:10.1207/s15327108ijap0803_2.

Sharma, A., Kim, T.E., Nazir, S., 2021. Implications of Automation and Digitalization for Maritime Education and Training, in: Carpenter, A., Johansson, T.M., Skinner, J.A. (Eds.), Sustainability in the Maritime Domain:

Towards Ocean Governance and Beyond. Springer, Cham, Switzerland. chapter 11, pp. 223–234.

Størkersen, K.V., 2021. Safety management in remotely controlled vessel operations. Marine Policy 130, 104349. doi:https://doi.org/10.1016/j.marpol.2020.104349.

Tam, K., Chang, B., Hopcraft, R., Moara-Nkwe, K., Jones, K., 2023. Quantifying the econometric loss of a cyber-physical attack on a seaport. Frontiers in Computer Science 4. URL: https://www.frontiersin.org/articles/10.3389/fcomp.2022.1057507, doi:10.3389/fcomp.2022.1057507.

Tam, K., Hopcraft, R., Crichton, T., Jones, K., 2021. The potential mental health effects of remote control in an autonomous maritime world. Journal of International Maritime Safety, Environmental Affairs, and Shipping 5, 40–55. URL: https://dx.doi.org/10.1080/25725084.2021.1922148, doi:10.1080/25725084.2021.1922148.

Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J.P., Andrews, W., Harish, A.V., Giménez, P., Crichton, T., Jones, K., 2022. Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. Journal of Transportation Technologies 12, 1–27. URL: https://dx.doi.org/10.4236/jtts.2022.121001, doi:10.4236/jtts.2022.121001.

United Nations, 1982. United Nations Convention on the Law of the Sea. United Nations. doi:10.1093/acprof:oso/9780199299614.003.0002. http://dx.doi.org/10.1163/9789004249639_rwunclos_laos_9789024731459_206_403.

Vagale, A., Osen, O.L., Brandsæter, A., Tannum, M., Hovden, C., Bye, R.T., 2022. On the use of maritime training simulators with humans in the loop for understanding and evaluating algorithms for autonomous vessels, in: The International Maritime and Port Technology and Development Conference (MTEC) & The 4th International Conference on Maritime Autonomous Surface Ships (ICMASS) 05/04/2022 - 07/04/2022 Singapore, Singapore, IOP Publishing Ltd. URL: https://dx.doi.org/10.1088/1742-6596/2311, doi:10.1088/1742-6596/2311.

Veitch, E., Andreas Alsos, O., 2022. A systematic review of human-AI interaction in autonomous ship systems. Safety Science 152, 105778. URL: https://www.sciencedirect.com/science/article/pii/S0925753522001175, doi:https://doi.org/10.1016/j.ssci.2022.105778.

Veitch, E., Hynnekleiv, A., Lützhöft, M., 2020. The Operator's Stake in Shore Control Center Design: A Stakeholder Analysis for Autonomous Ships. International Conference on Human Factors 2020 doi:10.3940/hf.20.5.

Vojković, G., Milenković, M., 2020. Autonomous ships and legal authorities of the ship master. Case Studies on Transport Policy 8, 333–340. doi:https://doi.org/10.1016/j.cstp.2019.12.001.

Wróbel, K., Gil, M., Montewka, J., 2020. Identifying research directions of a remotely-controlled merchant ship by revisiting her system-theoretic safety control structure. Safety Science 129, 104797. URL: https://doi.org/10.1016%2Fj.ssci.2020.104797, doi:10.1016/j.ssci.2020.104797.

Xu, W., Gao, Z., 2024. Applying hcai in developing effective Human-AI teaming: A perspective from human-ai joint cognitive systems. Interactions 31, 32–37. doi:10.1145/3635116.

Zagan, R., Raicu, G., Sabau, A., 2022. Studies and research regarding vulnerabilities of Marine Autonomous Surface Systems (MASS) and Remotely Operated Vessels (ROVS) from point of view of cybersecurity. International Journal of Modern Manufacturing Technologies 14, 310–318. URL: https://doi.org/10.54684%2Fijmmt.2022.14.3.310, doi:10.54684/ijmmt.2022.14.3.310.

Zhang, W., Zhang, Y., 2023. Research on coupling mechanism of intelligent ship navigation risk factors based on N-K model. Journal of Marine Science and Technology 28, 195–207. URL: https://doi.org/10.1007%2Fs00773-022-00919-0, doi:10.1007/s00773-022-00919-0.

Ziajka-Poznańska, E., Montewka, J., 2021. Costs and Benefits of Autonomous Shipping—A Literature Review. Applied Sciences 11, 4553. URL: https://dx.doi.org/10.3390/app11104553, doi:10.3390/app11104553.

Zongo, P., 2017. The automation conundrum. ISACA Journal 1. URL: https://www.isaca.org/en/resources/isaca-journal/issues/2017/volume-1/the-automation-conundrum.