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

J Palbar Misas, BSc[a*], R Hopcraft, MSc, SIMarEST[a], Dr K Tam, PhD[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 grows, and will continue to grow significantly, as the industry strives for fully autonomous vessels. Current maritime operations on board rely on a mixture of automated processes, human decision making, and human interventions. In the future autonomy may lead to the removal of the mariner physically on board, increasing remotely operated vessels. The remote nature of these operations will subject mariners to new operational risks, such as a potential reduction in Situational Awareness (SA) and/or cyber threats. This article will discuss the importance of SA in maritime operations, and the potential challenges facing this when engaging in remote operations. Secondly, this article will discuss the training that mariners may need to navigate within such a remote operational landscape. Lastly, it is fundamental to understand how mariners currently manage higher risk operations (e.g. heavy traffic and port arrival/departure), and how this will change with the introduction of remote operations.

Keywords: Autonomy; Trust; Cybersecurity; Maritime; 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 (Chae et al., 2020; IMO, 1964). It took over half a century before the IMO approved a regulatory framework for exploring the impacts of including Maritime Autonomous Surface Ships (MASS) in the World's fleet. Finalized in May 2021 through a regulatory scoping exercise (RSE), the IMO prioritised identifying the vital issues and importance of the human element, specifically for remote controlled and fully autonomous ships (IMO, 2021b).

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 new technologies and digital capabilities. However, implementing these without due care could introduce new risks. For example, many organisations do not align their innovation strategies to their machine operator work processes when developing new technologies (Chae et al., 2020; Digitalisation World, 2020; Zongo, 2017). Instead, advancements are typically driven by profits, or impact on the environment (Digitalisation World, 2020).

Consequently, this can lead to gaps in situational awareness (SA), or cybersecurity knowledge affecting critical safety failures 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 of 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. However, in remote operations the perception of the environment is gained from data and screens. Moreover, SA for fully autonomous vessels is based according to the provided data and tools to make the appropriate decision (Hammernes, 2022; International Maritime Organization, 2018).Thus, this study analyses the challenges of maintaining mission critical SA in remote maritime operations, and the importance of cybersecurity awareness in increasingly digitalised operational environments. Secondly, it identifies the skills remote operators 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 navigation cadets. The cadets' responses to various simulations and tabletop exercises were recorded, and inform the discussions hereafter. The paper concludes by discussing how autonomy affects SA and cybersecurity, and how this should inform the development of future training, autonomous ships, and remote control centre designs.

Authors' Biographies

Juan Palbar Misas is a Research Assistant in Navigation and Maritime Cyber at the University of Plymouth. He works on the EU Horizons Cyber-MAR project. Prior to this attained be BSc in Navigation and Maritime Science with an interest in maritime autonomy.

Rory Hopcraft is a industrial researcher at the University of Plymouth, working on the EU Horizons Cyber-MAR project. Mr 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 a lecturer at the University of Plymouth having gained a B.S in Computer and System Engineering at Rensselaer Polytechnic Institute in the USA and a PhD in Information Security from Royal Holloway University of London in the UK. Dr Tam is currently a co-investigator for the EU H2020 Cyber-MAR project, the academic lead for the Cyber-SHIP project, and co-I in a number of other maritime cybersecurity projects across a number of topics including security of vessels, ports, and offshore platforms.

 https://doi.org/10.24868/10703

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. Based on Tam et al. (2021)

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, 2021c). 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: 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 downsides.

2.1 Trust in autonomous systems

Whilst it is beyond this paper to fully explore trust in autonomous systems, it is important to note that there are still questions regarding the sector's level of trust in such systems (Lee and See, 2004). Broadly speaking, the transit of goods through the global supply chain requires a degree of trust between stakeholders (ship operator, crew, freight forwarders etc) and their trust in the digital systems used to ensure the safe passage of goods. Any acceptance of autonomous systems as the norm within this sector requires developing trust in the accuracy, reliability, safety and security of these systems (Mallam et al., 2020). This is still a challenge within commercial MASS projects, which implies that the human element cannot be fully removed in the near future; meaning remote control and remote monitoring will be significant in the interim (Sharma et al., 2021).

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 situational awareness. 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 need to take manual control of an otherwise autonomous vessel. Without maintaining good SA, these situations could lead to safety issues. This was demonstrated in a 2009 Airbus A330-203 incident, where pilots in an automated cockpit systems lost SA. In this case, when the pilots had to take manual control, they failed to maintain sufficient SA and recognise the dangerous position of their aircraft, leading to the crash (BEA, 2012; Endsley, 2017). Although they 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), and proper SA helps inform that problem-solving.

The IMO RSE further agreed that no passenger transport will occur without seafarers on board (IMO, 2021a). Thus, even if all cargo ships become fully autonomous, passenger ships will still require trained personnel onboard. This further illustrates that seafarers will continue to have critical roles in controlling, maintaining and supervising 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 is trustworthy, including being cyber-secure, maritime transportation will require human intervention (Ahvenjärvi, 2016). Therefore, it is critical that mariners are provided 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 challenges. The development of digital navigation aids, such as Electronic Chart Display and Information Systems

 https://doi.org/10.24868/10703

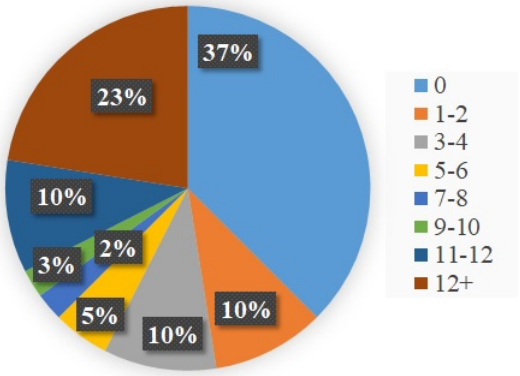

Figure 1: Month(s) of sea time experience of participants

(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-paces this process, creating issues (Hopcraft, 2021).

Under Article 94 of the United Nations Convention on the Law of the Sea, each vessel must have a master who possess appropriate qualifications (United Nations, 1982). This mariner must comply to regulatory obligations, including those under collision avoidance (COLREGS) and the safety of life at sea (SOLAS) (International Maritime Organization, 2020, 2003). When considering remote operations, when the master is physically removed from the vessel, it brings their specific roles and responsibilities into question (Ghaderi, 2019; Vojković and Milenković, 2020). For example, what elements of maritime training need to be introduced, or changed, to ensure remote masters possess the required navigational or communication skills to maintain SA and operate safely? Moreover, how can cyber-attacks or accidents take away or reduce SA when it relies entirely on digital information. In some situations (e.g. GPS 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 situational awareness in a remote operations must include the ability to identify and mitigate cyber incidents in order to maintain the safety of operations (Endsley, 2017).

3 Methodology

To better understand the impacts of autonomy and cyber-security on a seafarer's SA, the authors engaged with a group of 60 navigational students enrolled at a British university for a one-day workshop. Within this group, over 60% had some professional sea based training experience (see Figure 1). These students 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. 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, students were provided with a questionnaire, to determine the group's baseline understanding and knowledge of autonomy and cyber-security. The questionnaire was divided in two parts. The first included ten maritime cyber awareness questions, in which the majority of answers were quantitative (i.e. 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 ship they served on (see more questionnaire results in Section 4).

3.2 Tabletop

During the second half of the workshop, participants were split into groups of five or six. Each group completed a 50-minute tabletop discussion on what they perceived to be the impact of autonomous operations on their situational awareness, and how this could affect their safety and security. To seed discussions, participants were given a the questions below, and were encouraged to draw on their own experiences, knowledge and ideas:

 https://doi.org/10.24868/10703

1. Will the roles and responsibilities as a navigation officer change with remote control?
2. What challenges 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 (see Figure 2).

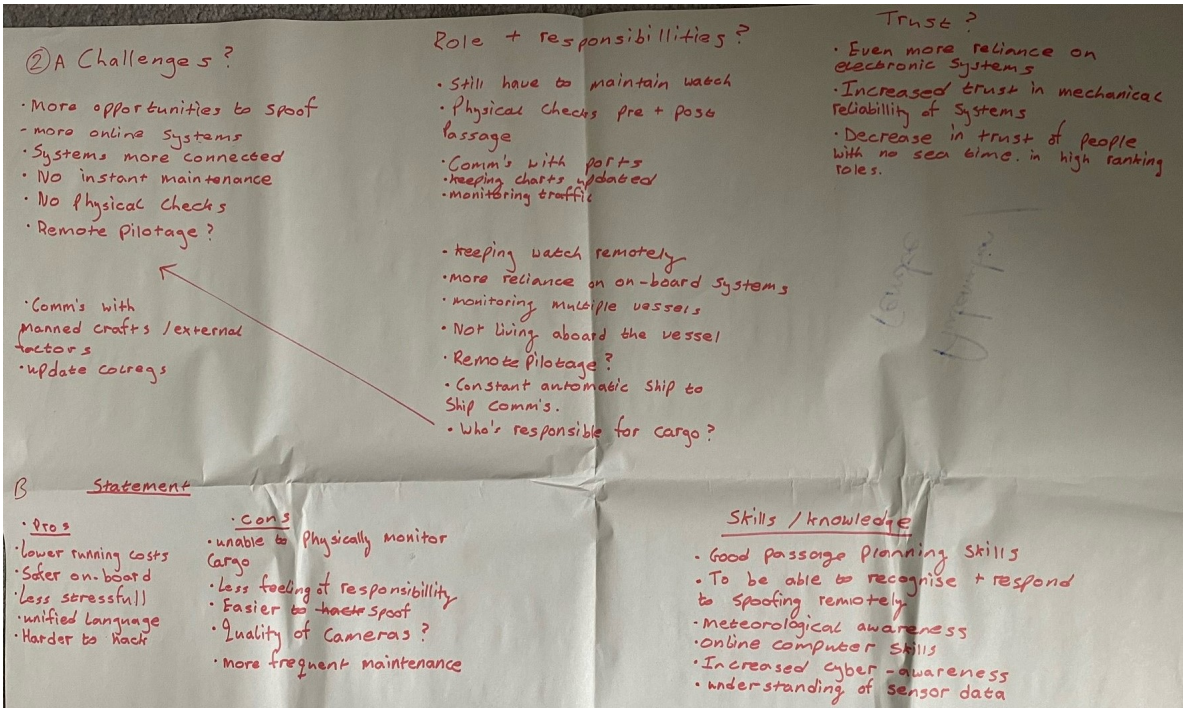

Figure 2: Example of a groups tabletop exercise ideas

3.3 Simulations

Each group was taken through two different simulation exercises. Each exercise consisted of a 5-minute briefing, a 10-minutes Watchkeeping section, during which a simulated cyber-incident occurs, and a 10-minute group discussion. Whilst both simulations used a ship model the students had operated before, a 5-minute familiarization and setup period was given. Both of the scenarios tested participant's SA in different ways as a response to incidents when ships navigational systems had been compromised. Using the full-bridge simulator (Figure 3)brought a level of realism through the use of an appropriately represented scenario allowing the participants to suspend belief ensuring the highest possible levels of SA in a simulated setting (Lateef, 2010; Salas et al., 1998). Therefore, any issues with participant SA was more likely to be attributed to the cyber-attack within the scenario, instead of simulation quality.

The first scenario introduced a GPS drift of 300 metres every two minutes, simulating a spoofing attack as the ship transits the UK Land's End Traffic Separation Scheme (TSS). On average it took students 8 minutes after the first manipulation to spot the error, leading to a significant course offset of 1.2km. Even when response time was less (<3 minutes) they struggled to comprehend the direction the spoofing had occurred. The position error was apparent due to the 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 they did not know how to validate information.

The second scenario involved a more dramatic and sudden incident than the first. Occurring during an inbound passage to port, participants were timed to see how quickly they would detect the loss of rudder and engine control. Even with fast detection (within seconds) the scenario was designed so that due to the ships momentum (high rate of turn and speed) and limited time a collision was assured Tam et al. (2022).

 https://doi.org/10.24868/10703

Figure 3: One group of participants in the full bridge simulator

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 day, participants expressed concerns (Table 2) about future autonomous systems and the quality of information they would need to carry out their daily tasks remotely. They perceived difficulties in completing tasks if cut off from physical senses (e.g. sound, smell, feel) and the physical ability to check systems, environment, engine, bow thrusters and cargo. Participants felt they would not be able to maintain good SA without this sensorial data. As Munir et al. (2022) states, sensory data forms a vital part of enhancing situational awareness. 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, students were able to maintain SA to the end.However, as confirmed by discussions with master mariners present during the workshop, the incident is unavoidable regardless of reaction time.This raised interesting questions when considering the same scenario for a remote crew as the simulator represents remote operations. Could response time be positively or negatively affected (i.e. shortened/lengthened) if the crew were remote and relying on only digital data for SA? 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?

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, logbooks, and route planning, including weather conditions, would look like in a remotely controlled world.

Participants also stressed that good communication will be key factor to maintain sufficient SA at high levels of autonomy. Finally, there was concern that the sense of "realism" may be lowered, if remote control felt too game-like. All of which could impact on a remote crews ability to achieve, and maintain appropriate SA.

4.2 Cybersecurity affecting SA

Another theme identified by the participants was the relationship between situational awareness and cybersecurity. As part of the questionnaire, students were asked to indicate whether they were aware of IMO Resolution MSC428(98) (Maritime Cyber Risk Management in Safety Management Systems). Only 30% of participants responded "Yes", indicating a lack of awareness of the significant regulations affecting their operations. Interestingly,

 https://doi.org/10.24868/10703

real world experience seems to have had a slight positive effect on this. With this set of participants, those who have had real world experience had 3% more awareness of this resolution. The type of vessel people have served on did not seem to have a noticeable effect on this. On a more positive note, during the simulation exercises, students were acutely 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, participants did not consider insider cyber threats to be a large threat, with only 2.5% of responses indicating as such. However, as Khan et al. (2021) illustrate the insider represents a credible threat to the sector. The more obvious options of criminal, terrorists and state sponsored actors were all identified with a high rate (>82.5%). Interestingly, participants somewhat contradicted themselves by considering the human element as an area of risk, with 57.5% of responses 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.

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 respondents indicated that they strongly trusted the systems they use to navigate, and 82.5% noted they only slightly trust their systems. However, during the first simulation exercise, it took on average 8 minutes for participants to stop trusting a compromised system. This suggests that, while participants may be aware of untrustworthy (i.e. unsecure) systems, many are still subconsciously inclined to trust them during familiar operations. During the tabletop exercise, several groups spoke about the need to validate the information ship systems provide. Yet again, during the simulation exercises, several groups due to inexperience failed to identify other sources (e.g. gyro compass, radar) of information that could be used to help understand their position. Experience mariners in this scenario would be more inclined to have an earlier reaction to use other systems to validate information.

While outside the scope of this research, it is interesting that those in the younger age range, and those who have had less sea time, indicated more trust in digital systems. This suggests that modern technology and/or cadet training rely more heavily on digital aids, promoting a high level of trust in them. This is not inherently bad, 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.

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 level, and sometimes a 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 adapted from IMO (2021a)

 https://doi.org/10.24868/10703

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 this on one small remote team. While MASS prototypes, and the control of them, 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 control-centre designs.

When asked if a cyber-attack could cause a catastrophic event (e.g. collision, pollution, loss of life), 92.5% of respondents agreed it was possible to some degree, especially as vessels operating and remote degrees 2-4 would be heavily reliant on technology and connectivity. Thus, participants discussed changes in their responsibilities that could reduce the possibility of a catastrophic event through information verification, and better cyber-security.

Many of the participants also wanted to maintain the seafarer lifestyle as it provides them 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 remote-control centres will provide more attractive aspects that will help remote operators wellbeing and the efficiency and safety of commercial shipping.

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. (2021), argue training is only effective if it changes behaviours of crew, which is achieved most effectively through the development of a safety culture.

When asked, 75% of participants indicated that training would be needed to detect, report, and stop a cyber-attack on board a vessel. Of concern is that 20% were neutral and 7% disagreed that training would help. As these responses were collected prior to the simulation exercises several participants commented how their initial impression was wrong.

Many participants during the tabletop exercise identified multi-ship operations as a new skill set required for remote control operations. Moreover, emergency response training for remote operations was rated highly, following the simulator exercises. It was also highlighted that there was a need to develop skills to validate information and how to deal or cope with the cyber threat distractions. Additionally, the authors also noticed some disconnects between the written survey answers and the behaviours. Particularly around the perception of insider vulnerabilities, 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.

Consequently, to improve the alignment between humans and autonomy technology, a 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, like the process of including cyber risk management within the ISM Code. One such amendment could be the creation of new competencies for remote operations within the Standards of Training, Certification and Watchkeeping for Seafarers (STCW) Convention.

5 Limitations and Future Research

While it was important to have real mariners inform this research, there were limitations with the group selected to complete the exercises. Due to the need for physical access to the simulator the group comprised of students enrolled at the University. To ensure the participants could engage effectively with the given scenarios final year students 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 more experienced group with an average age closer to the

 https://doi.org/10.24868/10703

industry average of 34 (Bergeron, 2018). Similarly, a group with a greater diversity in educational, national and cultural backgrounds would be a better representation (Janićijević, 2019).

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 may 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 automation projects in other transport sectors (aviation, road vehicles).

As discussed above the transition to a fully autonomous world fleet will take time to develop, even then the human element will never be completely removed (e.g. remote control, maintenance). Therefore, as the sector adds more autonomy to systems, it must consider whether this has been done in such a way 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 the information and systems used by crew in specific systems and how this could be transferred ashore, ensuring there is a balance between safety 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 many ships could a remote operator or operating team safely handle? How would multiple ships affect their SA? What information and how much time would remote operators need for watch handovers? Would this be dependent on ship type? How could they determine the receiving data is trustworthy?

2. Would the roles or responsibilities for remote operations still be as per current hierarchy (e.g. 3rd Officer of the Watch (OOW) when taking command in open waters and master in restricted waters)?

3. How much training for remote operations would be based on simulation? How much training in remote simulator operations would be needed to obtain SA of the vessel? Could future simulation be implemented similar to aviation remote control simulation (Flight Safety, 2022)? Would sea time still be required (Karlis, 2018)? Would virtual reality need to be implemented for future remote operations and/or training?

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. Cyber awareness in the sector is low, which could have a long term impact on the situational aware. For example, the potential over trusting of digital aids, coupled with a lack of skills to validate information.

2. What regulations and guidelines need to change, especially with the incorporation of autonomous technology the cyber-threat landscape changes, and how?

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

4. How can the over reliance in digital aids be reduced?

5. How could being removed from the physical ship hinder an operators ability to sense and check safety.

In conclusion, this study has considered some of the challenges the maritime sector faces as it moves towards fully autonomous operations. The ability for remote operators to operate safely is contingent upon good situational awareness, which itself faces challenges. 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. Thus, future mariner training needs to focus on providing theses skills to operators whilst considering the new skills required (e.g communication skill, mutli-ship management etc).

Acknowledgement

This paper is a partly funded by the research efforts under Cyber-MAR. 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 Kevin Jones and Tom Crichton, and all the students who participated.

References

Ahvenjärvi, S., 2016. The human element and autonomous ships. TransNav 10, 517–521. doi:10.12716/1001.10.03.18.

BEA, 2012. Final Report On the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro - Paris. Technical Report. URL: https://www.bea.aero/docspa/2009/f-cp090601.en/pdf/f-cp090601.en.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.

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.

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.

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.

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.

Flight Safety, 2022. Preparing for the future in simulation. URL: https://www.flightsafetyaustralia.com/2022/02/preparing-for-the-future-in-simulation/.

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. URL: https://www.kongsberg.com/maritime/products/situational-awareness/.

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.

Hopcraft, R., 2021. Developing maritime digital competencies. IEEE Communications Standards Magazine 5, 12–18. doi:10.1109/MCOMSTD.101.2000073.

Hopcraft, R., Tam, K., Moara-Nkwe, K., Jones, K., 2021. The development of a cyber safety culture, in: ErgoSHIP 2021.

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

IMO, 2018. International Maritime Organization MSC100/20/add.1 - Report of the Maritime Safety Committee on its One Hundredth Session.

IMO, 2021a. International Maritime Organization MSC103/21/add.1 - Report of the Maritime Safety Committee.

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

IMO, 2021c. International Maritime Organization Takes First Steps to Address Autonomous Ships. URL: https://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx#:~:text=For%20the%20purpose%20of%20the,operate%20independently%20of%20human%20interaction.

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

International Maritime Organization, 2018. Msc100/20 add.1 - report of the maritime safety committee on its one

hundredth session.

International Maritime Organization, 2020. Safety of Life at Sea Convention. IMO, IMO.

Janićijević, N., 2019. The impact of national culture on leadership. Economic Themes 57, 127–144. URL: https://dx.doi.org/10.2478/ethemes-2019-0008, doi:10.2478/ethemes-2019-0008.

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.

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.

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.

Munir, A., Aved, A., Blasch, E., 2022. Situational awareness: Techniques, challenges, and prospects. AI 3, 55–77. doi:10.3390/ai3010005.

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.

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.

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.

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.

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.