Modern shipping needs to be cybersecure: A South African perspective

Rossouw von Solms[†] *and Suné von Solms*[‡]

ABSTRACT

The traditional standalone operational technology systems that control multiple mechanical systems on board a ship get increasingly integrated with modern information and communications technology (ICT)-related systems. These ICT systems that continuously become interconnected with operational technologies and systems include the Internet-of-Things (IoT), autonomous technologies and the internet with adequate bandwidth etc. The IoT typically employs numerous sensors and captures vast amounts of data, which is processed, transmitted and turned into trusted intelligence to the advantage of all parties involved. Furthermore, modern navigational systems utilise global positioning systems (GPS), radar, sonar and computerised maps. These are used in conjunction with modern communication systems to communicate related data used for accurate navigation. In addition, autonomous technologies are highly dependent on accurate data communicated to them. Thus, it is clear that data is rightly termed 'the new gold' in the shipping industry. On the other hand, the maritime industry, like most other industries, is highly vulnerable to cybersecurity attack. As more data is captured, processed and communicated for the more critical shipping activities, the more vulnerable the industry will become to modern cybersecurity threats. Therefore, the interfaces between sensors, devices and different technologies, and the communication of captured data need to be properly secured. Furthermore, many of the shipping industry staff working with technologies where data are captured and communicated need to be educated on how to assist in securing this data. This paper will emphasise the continued use of ICT-related systems in the shipping industry, and how this digitalisation and smart use of ICT solutions will benefit the maritime industry. In light of this, the purpose of this paper is to highlight the continued vulnerabilities to modern cybersecurity threats, and to discuss some solutions to securing these technologies towards securing the industry as a whole. The paper will also address aspects of educating maritime staff in technology-related areas ranging from the ICT- and cybersecurity-related topics that need to be included in maritime curricula, on the more formal side, to making all staff members more cybersecurity aware, on the more informal side.

[†] Emeritus Professor, Centre for Research in Information and Cyber Security (CRICS), School of Information Technology, Nelson Mandela University; South African International Maritime Institute

[‡] Head of Department, School of Electrical and Electronic Engineering Science, University of Johannesburg; South African international Maritime Institute

https://doi.org/10.47348/SAJMET/2023/i1a2

I INTRODUCTION

Modern shipping may not use technologically advanced ICT systems such as used on passenger airplanes, but certainly the shipping industry is continuously introducing highly advanced ICT-related systems to modern vessels.[1] The traditional standalone operational technology systems that control multiple mechanical systems on board a ship have become increasingly integrated with modern ICT-related systems. These ICT systems that are continuously interconnected to operational technologies and systems include IoT, autonomous technologies and the internet with adequate bandwidth etc. The IoT typically employs numerous sensors to capture vast amounts of data, which is processed, transmitted and turned into trusted intelligence to the advantage of all parties involved.[2] As ICT-related systems become increasingly integrated and more data is captured, stored, analysed and transmitted, it is logical that these systems and data become increasingly vulnerable to cyberattacks. Furthermore, the staff working with these systems or on these vessels are increasingly exposed to cyberattacks.

The main objective of this paper is to investigate and research the current use of ICT in the maritime industry and related cybersecurity issues. The core deficiencies, application and protection of related ICT systems in the maritime industry, specifically from a cybersecurity point of view, will be reported on, along with the identified use and integration of ICT.

First, this paper will report on current advances in the maritime industry, followed by the integration of ICT into modern shipping systems. The generation of high volumes of data by these ICT systems and possible future advances will then be discussed, along with the typical vulnerabilities this data is exposed to. The situation regarding the education of maritime professionals is South Africa will briefly be reported on, specifically with regard to the ICT- and cybersecurity-related aspects of technology covered in these curricula. Lastly, possible interventions, which include awareness, will be proposed to ensure that ICT-related systems in the maritime industry are better protected from a cybersecure point of view.

II ADVANCES IN THE MARITIME INDUSTRY

Shipping has evolved by leaps and bounds over the last number of decades. Modern ships have advanced in terms of design, materials, propulsion and navigation, among other areas. Gone are the days of wooden, wind-propelled ships that were navigated by star maps and astrolabes.[3] Communication with the shore was extremely limited once at sea.

Today the propulsion, navigation, supplies and maintenance etc of modern ships employ advanced equipment and machinery. Fuel and oil flow rates, revolutions per minute, temperature changes and other parameters need to be monitored, recorded and analysed continuously. Computers and ICT systems are used nowadays and integrated into the workings of a ship to capture vast amounts of data to assist and improve the performance of a modern ship.[4]

III ICT IN MODERN SHIPPING

Data that is captured from numerous IoT systems and sensor equipment all over the ship goes along way but this is not enough. This data needs to be analysed, stored and/or transmitted to prove useful and beneficial to a ship and the related industry.[5] In some cases, the processed

---

1 JP Apud 'Information Technology Applications in the Maritime Industry' *The Maritime Review* 1 November 2016 (available from: <https://maritimereview.ph/information-technology-applications-in-the-maritime-industry/>).

2 M Lind-Olsen 'ICT Solutions Bring Ship and Shore Closer' *Dualog* 30 July 2019 (available from: <https://www.dualog.com/blog/ict-solutions-bring-ship-and-shore-closer>); R Larsen 'What's the Value of Maritime-specific Software?' *Dualog* 23 October 2019 (available from: <https://www.dualog.com/blog/whats-the-value-of-maritime-specific-software>); J Cusimano, M Ayala & G Villano 'Navigating Cybersecurity Challenges in Maritime Operational Technology' *The Maritime Executive* 10 November 2020 (available from: <https://maritime-executive.com/editorials/navigating-cybersecurity-challenges-in-maritime-operational-technology>).

3 Apud op cit note 1.

4 Lind-Olsen op cit note 2.

5 Ibid.

https://doi.org/10.47348/SAJMET/2023/i1a2

data is used on board for aspects of operation such as preventative maintenance, opening and closing of valves and steering etc. On the other hand, in most cases, this data needs to be transmitted in a trustworthy manner to the shore, where it will be further analysed, processed and used for the well-being of the ship or the related industry.[6] Transmitting the data safely from ship to shore and from shore to ship has become critically important.[7] Thus, the smart use of ICT, on and off a ship, provides for effective business flow by connecting ships at sea to shore-based operations, maintenance service providers and customer support centres etc.[8] The advances in ICT systems create vast amounts of data for analysis and integration into decision-making at various levels.[9]

The advantages that ICT offers assist shipping owners and operators to meet the demands of their customers and to deliver on global and sustainability expectations.[10] Digitalisation and the smart use of ICT systems not only contribute to the shipping industry on an operational basis, but also strategically. Added value contributes to making operations at sea smarter, safer and more sustainable.[11] Shipping companies that aim to harness the power of 'big data' and advanced analytics, will move and stay ahead of competitors in future.[12] The digital future will increase business opportunities and create a competitive advantage to sustain the business in a global market.

IV ICT AND RELATED DATA USAGE

It is clear from above that data is continuously captured, transmitted and analysed by means of various ICT systems. Following are some of the more popular areas where this data is used:

- Improve vessel performance: Modern ships are dependent on the continuous monitoring of and reporting on systems such as the engine, electrical power and climate control. Data on aspects of performance, such as revolutions per minute, fuel and oil flow rates and temperature changes, need to be recorded and analysed and used to improve the performance of the ship.[13]
- Supply chain management: Cargo systems today make extensive use of sensors. As part of the IoT-based solutions, these sensors are integrated into monitoring systems to allow customers, captains and crew members to monitor temperatures or position etc in real time.[14]
- Navigational purposes: Modern navigation makes use of GPS, radar, sonar and computerised maps. Navigational information is used in conjunction with radio- and satellite-based communication systems. These systems assist navigation officers in dark, inclement weather, or low visibility.[15]
- Environmental compliance: By utilising cargo, port and environmental data captured continuously, ships can plan voyages, take shorter routes and adapt the speed to port availability, and, accordingly, save fuel.[16] Various technologies that rely heavily on ICT are used to measure, manage and report on the environment-related aspects of each ship. This is important because ships need to be compliant with ever-increasing environmental regulations. These regulations support the United Nations Sustainable Development Goals (SDGs).[17]

---

6 Ibid.
7 Ibid.
8 Ibid.
9 S Moan 'The Value of ICT in the Maritime Industry' *Dualog* 26 June 2022 (available from: <https://www.dualog.com/blog/the-value-of-ict-in-the-maritime-industry#:~:text=ICT%20systems%20add%20value%20to%20the%20maritime%20industry,shore-sea%20collaboration%20and%20the%20best%20possible%20business%20flow>).
10 Ibid.
11 R Larsen 'How ICT Solutions Can be Used Strategically in Shipping' *Dualog* 17 January 2020 (available from: <https://www.dualog.com/blog/how-ict-solutions-can-be-used-strategically-in-shipping>).
12 Ibid.
13 Apud op cit note 1.
14 Larsen op cit note 11.
15 Apud op cit note 1.
16 Moan op cit note 9.
17 Larsen op cit note 11.

https://doi.org/10.47348/SAJMET/2023/i1a2

Thus, the effective use of ICT-based systems contributes to, among other things, the delivery of supply chain transparency, assists with effective navigation, reduces the ecological footprint and minimises the operational costs associated with ship inspections and maintenance. The aspects of data use highlighted above are just a few of the many reasons for the proliferation of data-capturing sensors and related ICT systems that are integrated into modern shipping vessels and associated cargo.

As 'data is the new gold of the shipping industry', more effective ways and means will be found to ensure data are captured, processed, analysed and turned into trusted intelligence.[18] Data that is captured in isolation or at random, has little value today.[19]

V THE POWER AND VULNERABILITIES OF DATA

Data become valuable when used to obtain understanding, and to strategically integrate operations and decision-making from the information.[20] It is clear that data needs to be accurately captured, processed and analysed to be turned into trusted intelligence. Furthermore, for data to deliver operational value, information needs to be standardised, properly and securely distributed, and transmitted from ship to shore, and vice versa. Reliable, seamless internet connectivity that guarantees the safe and secure flow of business traffic intelligence becomes a must-have.[21]

With the proliferation of data-capturing devices, mostly by way of the further introduction of IoT, the following ICT-related utility aspects will add value and become very important.

Predicative maintenance

Currently, the following types of maintenance are predominantly prevalent in the shipping industry: periodic or scheduled maintenance, which is mostly time-based; preventative maintenance that depends on regular inspections and services etc; emergency maintenance, which normally takes place following a breakdown or failure; and condition-based maintenance that depends on accurate data that gets captured and used pre-emptively to determine whether any maintenance is required. Thus, predictive maintenance is dependent on IoT data for proactive analysis of the condition of the related machinery or equipment.[22]

Sensors, robots and smart condition monitoring technologies capture large volumes of real-time data from equipment, systems and machinery etc about the 'health' and status of the ship.[23] This captured big data is then collated by the on board ICT systems[24] and sent ashore, where it is assessed and analysed.[25] Depending on results and parameters set, early warnings can be given that might eliminate costly inspections and possible downtime.[26] Predictive maintenance can be classified of one of the major benefits of IoT integration on board ships.

Artificial intelligence (AI) and machine learning (ML)

From the above, it is clear that quality data that are processed and analysed are used in high-level decision-making for the well-being of the organisation. It is here that AI and ML come to the fore. AI is the science and engineering of making computers behave in ways that resemble human intelligence. AI has the potential to improve standard vessel operations,

---

18 Larsen op cit note 2.
19 Ibid.
20 Ibid.
21 Ibid.
22 Marine Digital 'Predictive Maintenance for Marine Vessels' *Marine Digital* (available from: < https://marine-digital.com/article_predictive_maintenance_for_marine_vessels#:~:text=Maintenance%20prediction%20is%20a%20proactive%20approach%20to%20dealing,that%20is%20strictly%20adhered%20to%20on%20board%20ships>).
23 Larsen op cit note 11.
24 Moan op cit note 9.
25 Larsen op cit note 11.
26 Ibid.

https://doi.org/10.47348/SAJMET/2023/i1a2

reduce organisational expenses and optimise business processes and decisions.[27] The high level of 'intelligence' stemming from ML algorithms and industry experience can create significant advantages for shipping companies. The higher the level of investment in AI and ML, the greater the benefit of big data analysis capabilities.[28] Typically, ML is used in voyage planning, cargo optimisation, marine network planning and estimating fuel consumption etc. At this stage, the use of ML in the maritime industry remains limited.[29]

Stena Lines, one of the world's largest ferry companies, uses AI and ML for reducing plastic on board, managing crew members, passenger accidents and fuel usage.[30] The port of Rotterdam uses ML-based systems to accurately determine vessels' time of arrival.[31] While ML is used extensively elsewhere in the digital world, its adaption to the maritime industry remains limited to date.[32]

Securing the data and related cyber systems

Operational technology (OT) systems are becoming increasingly integrated with modern ICT systems, which causes numerous vulnerabilities. The proliferation of the adoption of cloud computing, the IoT and the autonomous technologies used to interconnect OT and ICT will lead to more cybersecurity risks coming to the fore. Therefore, the maritime industry is increasingly being exposed to cyber-related risks and cybersecurity has become an issue of increased vulnerability.[33]

With the continued integration of IoT and related ICT systems into the maritime industry, cybersecurity has become a new focus in the industry.[34] IoT devices are not necessarily secure by nature and need to be secured. Cybersecurity is concerned with securing ICT systems, onboard hardware and sensors, and data leaks from unauthorised access, manipulation and disruption.[35] Cyberattacks on navigational systems by means of interference with automatic identification systems and electronic maps, the jamming of GPS and manipulating cargo and ship management systems are well-known. Many of these take place by introducing malware, ransomware software and viruses.[36] Cybersecurity should be implemented at all levels of the organisation, from top management onshore to onboard crew members. All of these contribute to the safety culture for the safe and efficient operation of a ship.[37]

Governing data usage in the maritime industry

As a result of the proliferation of ICT-related components and systems in the maritime industry, and the related cybersecurity risks, regulatory agencies, industry associations and standards bodies all deem it critically important to address maritime cybersecurity.[38] The International Maritime Organisation (IMO) regulations and the International Standards Organisation (ISO) standards for IoT and sensors have certainly changed the focus and calls for proper governing thereof.[39] Shipping companies have a deadline to introduce specific cybersecurity in their vessels' safety management systems.[40] It is clear that the integration and protection

---

27 Marine Digital 'Artificial Intelligence (AI) and Machine Learning (ML) in Maritime Logistics' *Marine Digital* (available from: <https://marine-digital.com/article_ai_and_ml>).
28 Ibid.
29 Ibid.
30 Ibid.
31 Ibid.
32 Ibid.
33 Cusimano et al. op cit note 2.
34 Ibid.
35 Marine Digital 'The Importance of Cybersecurity in the Maritime Industry' *Marine Digital* (available from: <https://marine-digital.com/article_importance_of_cybersecurity>).
36 Prinston, P 'Top 4 Trending Technologies in the Maritime Industry' *Searates Blog by DP World* (available from: <https://www.searates.com/blog/post/it-technologies-in-the-marine-industry>).
37 Marine Digital op cit note 35.
38 Cusimano et al. op cit note 2.
39 Lind-Olsen op cit note 2.
40 Cusimano et al. op cit note 2.

https://doi.org/10.47348/SAJMET/2023/i1a2

of OT and ICT systems, and the relatively new regulatory compliance, calls for maritime organisations to develop a comprehensive cybersecurity strategy to govern the environment properly.[41]

Skilling of employees

As more data is captured from onboard sensors and used, increasingly more operational decisions by crew members will be based on captured data streams. As a result, data science skills have become essential for modern crew members.[42] Adopting new ICT solutions will assist in attracting young professionals to enter the maritime industry as an attractive workplace.[43]

From a cybersecurity point of view, understanding what is required to create, implement and maintain a cybersecurity programme is just the start. Specialised skills and expertise are needed to successfully perform all these cybersecurity-related tasks.[44] Adding to this, cybersecurity is a relatively young focus area in the maritime industry. Maritime organisations mostly lack the experience and expertise to identify, assess, manage and respond to cyberthreats.[45]

From the above, it is clear that the maritime industry must, indeed, embrace ICT solutions to become more effective. The above-mentioned five ICT-related aspects have been identified and motivated as important areas that will receive attention in future. Cybersecurity probably stands out as an overarching issue that needs to be addressed because all the other ICT-related issues somehow depend on secure data.

VI MARITIME TRAINING AND EDUCATION IN SOUTH AFRICA

Education and training in ICT-related topics, especially cybersecurity, should be a core competence of the future maritime employee. For this reason, a brief study was conducted into some of the more prominent South African education and training institutes and centres offering maritime educational programmes.

As far as could be established from literature available and interviews with a number of role-players in tertiary education in South Africa, only three South African universities currently offer maritime-related higher education qualifications.

a. Durban University of Technology offers a one-year Advanced Diploma in Maritime Engineering. This qualification is accredited by the Engineering Council of South Africa (ECSA). Little detail on the curriculum could be found, but it seems that little, if any, ICT-related content is offered.
b. Cape Peninsula University of Technology offers a three-year ECSA-accredited Bachelor of Marine Engineering. A module called 'Computer Science for Marine Engineers' is offered, but the exact content could not be established.
c. The Nelson Mandela University offers a three-year ECSA-accredited Bachelor of Engineering Technology in Marine Engineering. This offering does include some data acquisition by means of digital devices and some low-level controls. Thus, it can be argued that limited content on data capturing it taught, but very little ICT and no cybersecurity.

Various institutes, academies and training centres offer maritime-related training. Examples include the South Africa Maritime Training Academy (SAMTA), the Maritime School, the Sea Safety Training Group (SSTG), the SA Maritime School, the Maritime School of Excellence (MSOE) and the Marine Oil & Gas Academy (MOGA). It would seem that the focus of all of these institutions is on general sea safety and seafarer skills. No ICT content or related skills training could be identified.

41 Ibid.
42 Larsen op cit note 11.
43 Ibid.
44 Cusimano et al. op cit note 2.
45 Ibid.

https://doi.org/10.47348/SAJMET/2023/i1a2

From the above it is clear that little, dedicated and focussed ICT education and training is offered to students studying maritime studies in South Africa. Furthermore, as far as could be established, no cybersecurity content is taught at all. This is in direct contrast to the findings earlier in this paper that the modern maritime employee corps should be properly schooled in specific ICT and, in particular, cybersecurity content.

From a short course or short learning programme point of view, definitely no maritime-focussed offering that includes any specific ICT-oriented content could be identified.

Thus, taking into account the importance of related ICT and cybersecurity knowledge and skills highlighted in this paper, it definitely seems as though related higher education curricula should include such content. In addition, there is probably a place for short learning programmes focussing on ICT and cybersecurity in the maritime industry.

VII TRIANGULATING THE FINDINGS ABOVE

During November 2022, a meeting was held with BW Offshore, a large shipping company that is based in Norway.[46] The meeting took place via MS Teams and was attended by four senior ICT staff members from BW Offshore who work in the IT, OT systems and cybersecurity domains. Three ICT staff members from Noroff University College in Kristiansand, Norway and one staff member from Nelson Mandela University in South Africa attended the meeting.

The objective of the meeting was to discuss the ICT- and cybersecurity-related developments in the maritime industry and to validate some of the theoretical findings made from literature, as discussed above. The following are a few extracts of some of the major IT and security aspects discussed and statements made by these professionals from the maritime industry.

- Integrating 'OT and IT environments'
- 'OT and legacy systems integrating with modern IT systems'
- Transmitting data 'from offshore to onshore'
- 'Cybersecurity awareness and training is a big focus area but is also very challenging'
- 'Cybersecurity training has not been part of their (offshore crew members) education agenda'
- 'Hire competence in cybersecurity'
- 'Most incidents triggered by user faults and lack of (cybersecurity) awareness'
- 'IT governance documentation project', specifically 'procedures and documentation'
- 'Mandatory for cybersecurity awareness and training'
- IT governance issues as 'IMO 2022 regulations will soon get audited'
- 'AI-penetration testing'.

These quotations were abstracted from the meeting and summarise some of the major issues that stemmed from the discussion. Certainly, this discussion confirmed almost all aspects and issues identified earlier in literature.

From this discussion it is clear that, IoT proliferates in the modern shipping industry, and more OT and IT systems integrate and transmit more and more information between on- and offshore. The fact that cybersecurity dominated the discussion highlights that this area is a huge problem and concern, from technical system infiltration and vulnerabilities ('AI-penetration testing') to incompetent on- and offshore staff members (see quotations above). Furthermore, as more and more regulations and standards are introduced, it becomes imperative to properly govern ICT in the maritime industry ('IT governance documentation project', specifically 'procedures and documentation' and 'IMO 2022 regulations will soon get audited').

[46] BW Offshore Meeting – Noroff and Visiting Professor – 202221108_144412 – Meeting Recording (available from: <https://www.dropbox.com/s/v8ej0iccdx0ohtw/Meeting%20BWOffshore%20-%20Noroff%20and%20Visiting%20Professor-20221108_144412-Meeting%20Recording.mp4?dl=0>).

https://doi.org/10.47348/SAJMET/2023/i1a2

VIII CONCLUSION

From a technology point of view, shipping has evolved by leaps and bounds in recent times.[47] Modern ships are dependent on equipment and machines that operate around the clock. Systems that control the engine, fuel delivery, electrical power and climate control etc need to be monitored continuously.[48] Integrated into these systems are IoT modules and sensor equipment that continuously capture and transmit data to be processed, analysed and stored elsewhere, most probably onshore. Thus, ICT is core to modern vessels and their operations. Furthermore, as vessels are dependent on the accurate capturing, processing, transmission and storing of this data, it is imperative that data needs to be secured. Therefore, the personnel developing and operating these highly technical systems need to be well-schooled and trained to ensure the security of the data, the systems using the data and the vessels that are totally dependent on the security of these systems. As almost all the transmission of the data takes place via the internet, sound cybersecurity should be an imperative.

The curricula of South African higher education institutes and of maritime training centres that educate and train mariners contain hardly any relevant ICT-related content taught to students, not to even mention highly critical cybersecurity content. With the need for modern-day mariners and related maritime personnel to be well-schooled in ICT and cybersecurity to ensure the secure operation of modern vessels, it is important that these people are, indeed, schooled in this subject, either at the initial education and training stage or skilled by means of further education and training. There exists considerable documentation, including the International Maritime Organization International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (IMO STCW) and the International Port Security Code (ISPS) Code Requirements for Seafarers, Ships and Ports that can be relevant in the development of cybersecurity educational and training material.

REFERENCES

Websites, Articles and Industry Reports

Apud, JP 'Information Technology Applications in the Maritime Industry' *The Maritime Review* 1 November 2016 (available from: <https://maritimereview.ph/information-technology-applications-in-the-maritime-industry/>).

BW Offshore Meeting – Noroff and Visiting Professor – 202221108_144412 – Meeting Recording (available from: <https://www.dropbox.com/s/v8ej0iccdx0ohtw/Meeting%20BWOffshore%20-%20Noroff%20and%20Visiting%20Professor-20221108_144412-Meeting%20Recording.mp4?dl=0>).

Cusimano, J, Ayala, M and Villano, G 'Navigating Cybersecurity Challenges in Maritime Operational Technology' *The Maritime Executive* 10 November 2020 (available from: <https://maritime-executive.com/editorials/navigating-cybersecurity-challenges-in-maritime-operational-technology>).

Larsen, R 'What's the Value of Maritime-specific Software?' *Dualog* 23 October 2019 (available from: <https://www.dualog.com/blog/whats-the-value-of-maritime-specific-software>).

Larsen, R 'How ICT Solutions can be Used Strategically in Shipping' *Dualog* 17 January 2020 (available from: <https://www.dualog.com/blog/how-ict-solutions-can-be-used-strategically-in-shipping>).

Lind-Olsen, M 'ICT Solutions Bring Ship and Shore Closer' *Dualog* 30 July 2019 (available from: <https://www.dualog.com/blog/ict-solutions-bring-ship-and-shore-closer>).

Marine Digital 'Artificial Intelligence (AI) and Machine Learning (ML) in Maritime Logistics' *Marine Digital* (available from: <https://marine-digital.com/article_ai_and_ml>).

Marine Digital 'Predictive Maintenance for Marine Vessels' *Marine Digital* (available from: <https://marine-digital.com/article_predictive_maintenance_for_marine_vessels#:~:text=Maintenance%20prediction%20is%20a%20proactive%20approach%20to%20dealing,that%20is%20strictly%20adhered%20to%20on%20board%20ships>).

[47] Apud op cit note 1.
[48] Ibid.

https://doi.org/10.47348/SAJMET/2023/i1a2

Marine Digital 'The Importance of Cybersecurity in the Maritime Industry' *Marine Digital* (available from: <https://marine-digital.com/article_importance_of_cybersecurity>).

Moan, S 'The Value of ICT in the Maritime Industry' *Dualog* 26 June 2022 (available from: <https://www.dualog.com/blog/the-value-of-ict-in-the-maritime-industry#:~:text=ICT%20systems%20add%20value%20to%20the%20maritime%20industry,shore-sea%20collaboration%20and%20-the%20best%20possible%20business%20flow>),

Prinston, P 'Top 4 Trending Technologies in the Maritime Industry' *Searates Blog by DP World* (available from: <https://www.searates.com/blog/post/it-technologies-in-the-marine-industry>).

Suné von Solms

Rossouw von Solms

https://doi.org/10.47348/SAJMET/2023/i1a2