2019-10-17

A Cyber-Security Review of Emerging Technology in the Maritime Industry

K Tam *School of Engineering, Computing and Mathematics*

K Jones

A Cyber-Security Review of Emerging Technology in the Maritime Industry

Kimberly Tam & Kevin Jones
Institution: University of Plymouth
E-mail: kimberly.tam@plymouth.ac.uk & kevin.jones@plymouth.ac.uk
Contact phone: +44 1752586305
Address: University of Plymouth, Drake Circus, Plymouth UK

Summary

The maritime industry is a complex cornerstone of global transportation infrastructure. To ensure smooth, safe and timely operations, technologies have been created or adapted over time to aid the maritime sector. Agile adaptations are an important part of maintaining safe operational standards despite economic, environmental, and technological changes. As ship-based systems and port infrastructure become more technologically advanced and complex, it is important to understand how emerging technology can both improve, and hinder, maritime operations. One of the main drawbacks of evolving technology is the increase of cyber-security vulnerabilities, as these systems become more complex and inter-connected. Maritime technology has the added complexity of hosting both information technology and operational technology (IT and OT) nearly equally. This paper gives an overview of emerging or growing technologies within maritime, specifically how they work, the benefits they bring, as well as cyber-security concerns to consider when accepting them into regular practice.

Key words: cyber-security, safety, technology, and maritime industry

1. INTRODUCTION

In today's world new, or variants, of existing technology are being integrated into shipping operations to assist in several areas including, but not limited to, logistic services, accurate navigation, frequent communications, and efficient cargo transportation. However as maritime technology becomes more complex and connected, the industry is seeing a rise in cyber-related incidences. Occurrences of cyber incidences, i.e. accidents and intentional attacks, are both fast-rising and significant threats to the industry. In an Allianz risk barometer paper maritime cyber-crime ranked as the second highest-ranked risk in 2018 [1]. This is a significant jump from 2013, when it was not even ranked in top ten risks. It is apparent that, just within the last five years, the vulnerabilities of modern maritime systems and the demands on the industry have increased cyber-risks. The rate of added-complexity, and therefore cyber-risks, is likely to only increase as more technology "emerge" in the maritime industry. This may be the result of new technology or the adaptation of existing technology in a new context.

More specifically, this paper shall look at the cyber-security aspects of autonomy, remote access or control, the Internet-of-Things (IoT), as well as newer renewable energies and cryptography-based security like block-chains. As the global maritime transportation industry moves 90% of all goods [2], any adopted technology will likely be far reaching and experience a wide range of cyber-threats. Cyber-risks arise the larger and more complex code becomes [3], and, due to the size of the industry, maritime organisations face are likely to need complex technical solutions to at both strategic planning and operational levels. The remainder of the paper will be as follows. First, Section 2 introduces cyber-security in maritime, providing some background information. This leads into to Section 3 where a more in-depth discussion of specific technologies that are now being adopted by significant players in the maritime industry and concludes with Section 4.

2. CYBER SECURITY

Maritime transportation, unlike maritime cyber security, has had a long history. Because of this, the industry has faced many threats before, particularly physical attacks like theft. This history means that the industry has built defences and resiliency against these kinds of threats. However, the introduction of electronic systems in a maritime vessel in the early 1900's [4] has changed the potential threats to the industry. Since then, relatively quick integrations of digital systems, both on-shore and on-ship, has helped increase operational efficiency, safety, and reduced physical labour for the crew. Unfortunately, traditional threats like pirates and common criminals have also become more technologically adept, increasing the cyber-threat.

As previously mentioned, a complex computing environment often results in more vulnerabilities in technological systems. More importantly, although individual systems on ships or in ports may not be considered complex by conventional standards, the connected systems (i.e., "system of systems" or SoS [5, 6]) are considerably complex. This is due to the convergence of information technology (IT) and operational technology (OT) that is unique to the modern maritime context. As a transporter of 90% of the world's good in volume and in

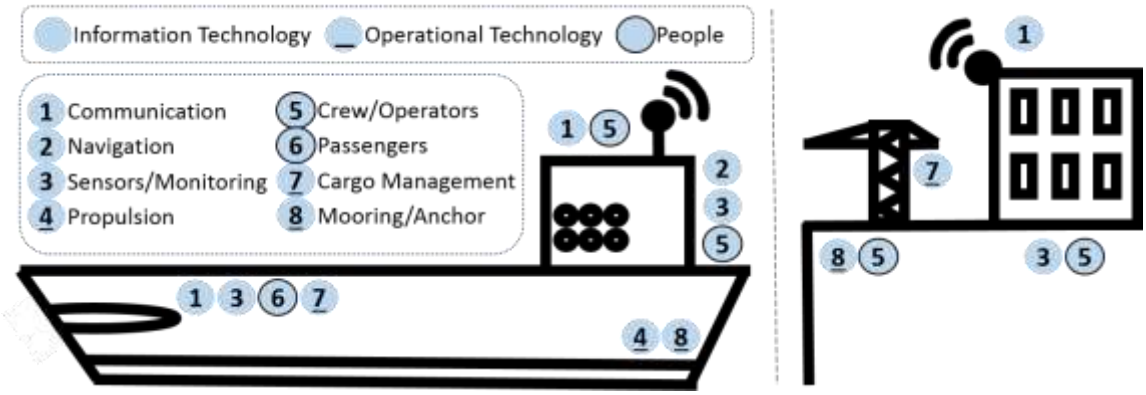

Figure 1 IT, OT, and human elements on-ship and at port

value [2], many physical operations rely heavily on technology. However, although automation in ports are being developed [7] and there are efforts toward autonomous ships (see more in Section 3.4), humans are still integral to the industry. While OT often receives less cyber-security attention than IT, this is partially because it is less used in other industries, in maritime it is used extensively and should considered a key part of maritime cyber-security. As seen in Figure 1, there are several areas where OT is both required for basic operations, but also integrated with IT systems and human interaction. It is also important to note that, while human error can contribute to physical and cyber incidences [8], a well-trained crew can be an asset in preventing incidences.

There are several reasons why the complexity of systems-of-systems can contribute to cyber-vulnerabilities. Generally when information is in transit, whether wirelessly or through physical wires, there is opportunity to alter or deny data if proper protections and authentications are not in place. In a system-of-system, this problem is compounded as individual systems change, or get replaced, and as they often come from a wide range of manufactures. This is further complicated when considering maritime specifically, given how ships traverse international waters but are still expected to function despite interacting with different regions, technologies, crews, laws and policies. Expecting IT and OT systems to accommodate such a wide set of possibilities can lead to extremely complex systems and create exploitable vulnerabilities.

3. EMERGING TECHNOLOGY

This section explores a few technologies that are gaining popularity in the maritime industry with an in-depth cybersecurity perspective. First, Section 3.1-3.4 discusses some maritime relevant cryptography, smart renewable energy, and remote access and remote control technologies. While such topics are less popular compared to the internet of things (IoT) and autonomy, these concepts are central to IoT networks and are found at different levels of autonomy. Lastly, Section 3.5 discusses changes in energy, specifically smart grids and the transition to newer, environmentally friendly, and renewable energies.

3.1. Supply chains: blockchain and “digital twin”

The introduction of blockchains to the computing world has resulted in many innovations and solutions to enhance security. This concept, in essence, decentralizes the storage and access to data. Cryptography is used to create “blocks” of data, and that data’s past transactions, and uses secure “chains” to connect those blocks in a fixed order. The cryptographic properties of these blocks and chains allow viewers to see the most current data version as well as the entire transaction history of that piece of data. There has been a lot of excitement surrounding block-chains, however, it is important that the technology is applied correctly in order to solve any existing problems. As highlighted by in-depth studies in [9], blockchains are currently regarded as a new and novel “solutions” to many technical problems; occasionally a technical solution is sometimes picked first, and then applied to a problem without fully understanding whether blockchains are the best solution to that problem. Moreover, in maritime specifically, the benefits are not wholly comprehensive. While the current number of projects involving blockchains in shipping are high, there almost no finished, in-depth projects with meaningful results to assess how well this technology is applicable to the maritime sector [9].

Of the potential applications of blockchain to maritime, the most promising is a secure, distributed, ledger. In this application of blockchain technology, it would become easier to see, and trust the records of, the transactions of goods. Instead of a centralized ledger, a company and the ports it utilizes can distribute a ledger that uses cryptography to ensure that all logs of past transactions are trustworthy, as well as ensure that the information can be public or cryptographically private and secure. The volume of goods in shipping make this a compelling solution in terms of supply chain management [10], general logistics. Cryptographically ensuring trust in ledger entries would add reliability to the system. Moreover, autonomous ports with a de-centralized network would make ledger data more resilient to incidents where one or more locations becomes been compromised.

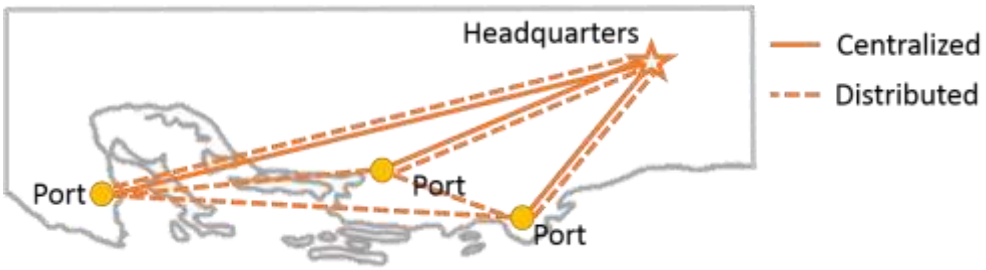

Figure 2 Example of centralized data versus distributed ledges using blockchain technology

Notable efforts by IBM and Maersk are attempting to use global supply blockchains on 10 milling shipping containers [11]. An example of centralized and distributed networks can be seen in Figure 2. As can been seen, the main difference in this simplified example is that the ports are more involved in the data distribution of cargo transactions, storing the ledger, and communications with all parties. While more complex, the actual transactions are also more secure and there is less reliance on a central location to protect a ledger on its own. While blockchain-enabled secure ledgers for the supply chain is an emerging technology to aid the transport of goods, "digital twin" technology is emerging to aid ship design, construction, and track ship performance across its life cycle. Similar to the IBM and Maersk project driving blockchain in shipping logistics, DNV GL, Rolls-Royce and several other groups are driving digital twin projects for ships.

The core of the "digital twin" concept is driven by sophisticated simulations of a physical assets, like a ship, by creating a suite of simulations models that can be placed in a common platform. This platform would allow a number of simulation models to be loaded at one time and to interact with each other, allowing for a highly customizable platform for a multitude of analysis. In terms of cyber-security, the digital twin cannot easily enhance cyber-security analysis capabilities. This is because the components are simulated and would not have the same vulnerabilities as the actual ship. Moreover, while less likely and less effective, since digital twins consist only of virtual parts and reside purely in cyber-space, there is a possibility that the digital files can be targeted in a cyber-attack to affect operations. In summary, while the digital twin might heavily effect the building and monitoring of ships, it is unlikely to have any significant negatives or positives regarding cyber security. Alternatively, there may be several benefits, and not many added vulnerabilities, if the maritime sector accepted secure ledgers. The main concern with applying blockchains to maritime problems is, instead, whether they are best solution. In a white paper by the World Economic Forum [13], a decision tree is available to determine whether a distributed ledger (DLT) is the correct approach for a business. It is advisory for individual businesses to fully consider their problem first before applying DLT. For example, if an asset, or in this case goods, has a physical representation that can change form, it is difficult to effectively manage on a blockchains. In some cases, this could prevent the successful application of a blockchain solution.

3.2. Remote operations and realities

As discussed further in Section 3.4, there are many levels of autonomous and semi-autonomous ships. There are many technologies to aid with middle levels of autonomy, several of which can be considered on their own as significant, emerging, tools for the maritime sector. More specifically this section considers remote communications, remote control, virtual reality, and augmented reality. While there are several communication and networking systems involved in maritime operations (e.g., satellite, radio, internet), the types of cyber-attacks and vulnerabilities are similar due to the wireless transmission. Because of this, no matter how remote access or remote control signals are sent, those transmissions are vulnerable to jamming and potentially spoofing attacks [14]. Based on this analysis of communication technology vulnerabilities in maritime, remote operations where humans receive and send data from on-shore facilities to ships can be vulnerable to cyber-attacks. Because of this, using virtual reality as a remote control aid has similar vulnerabilities. Hence, it is important to make sure all communications are trustworthy and to set up contingencies if communications are untrustworthy or unreliable.

Augmented reality, unlike virtual reality and remote operations, is more helpful to a crew on a manned ship, instead of a remote crew. This means that it does not share the same communication-based cyber-vulnerabilities. However, similar to virtual reality, the dangers lie in misinformation causing people to make the wrong decisions. This is because virtual objects are less easily verifiable, meaning if a cyber-attack is able to alter data, the likelihood that the false information is discovered before an incident goes down. This kind of vulnerability has been speculated about before with eAtons [14] as they are virtual markers and could potentially be spoofed or altered. Considering newer, emerging technology, augmented systems for ship bridges could result in a wider range of incidences, as there are more ways to trick people. The benefits of augmented bridges, disregarding security, is how data can be displayed in a more human-friendly manner [15, 16]. In particular, using augmented systems in areas difficult to navigate, and difficult to place physical markers, can make navigation much easier. Artic waters in particular has highlighted the benefits to eAtons as well as augmented realities on bridges [16]. An example of how malicious changes to the underlying data of an augmented reality program is changing the correct shipping lane on the screen enough to increase the changes of a collision with ice.

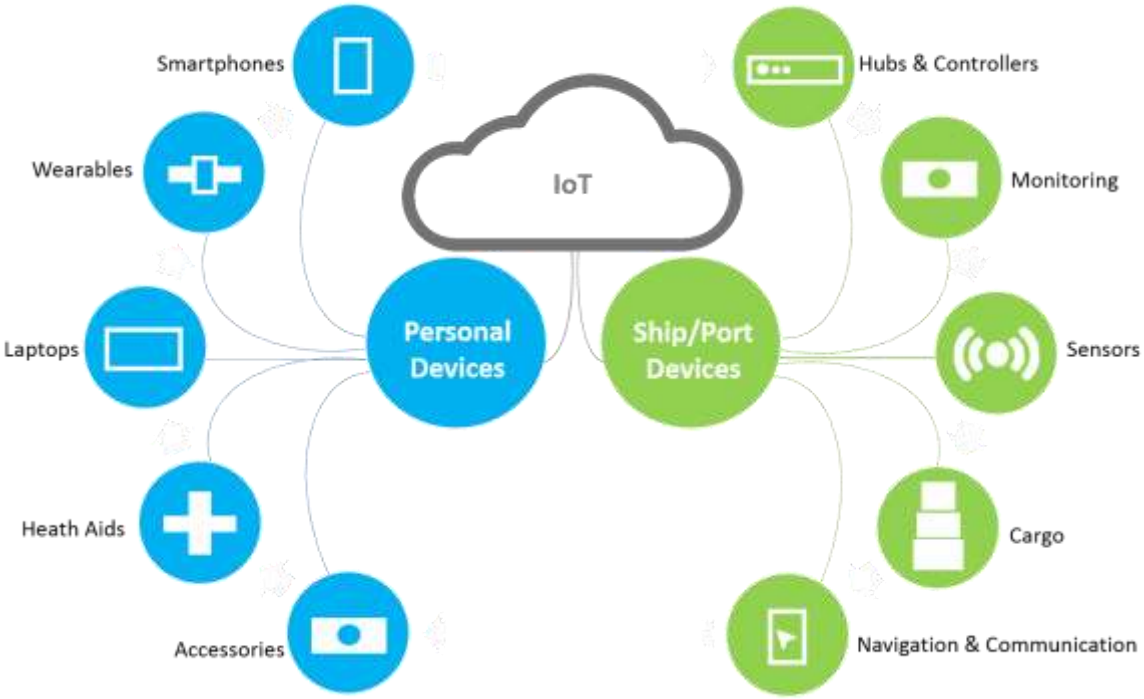

Figure 3 Categories of devices, personal, ship, and port, within a maritime Internet-of-Things

3.3. IoT

The internet of things (IoT) is the concept that many types of devices are interconnected, and share vast amounts of data, via the Internet. As this definition is relatively broad, IoT networks are inherently massive considering the number and types of internet-connected devices in the modern world. More specifically, in a recent survey, maritime trends show that 42% of maritime organisations believe they can benefit from additional IoT skills and 2.5 million dollars will be spent on IoT solutions over the next three years, more than cloud computing or big data analytics [17]. Part of the driving factor toward IoT solutions is that predicted cost savings are up to 14% over the next five years. Regarding the maritime sector, IoT devices can be categorized broadly into personal devices, ship devices, and port devices. As seen in Figure 3, personal devices and ship/port devices are separated as personal device cyber-security takes generic technology and puts them in a maritime setting, while ship and port devices are more bespoke to the maritime sector even though the underlying technology may be more commonplace. For example, while ships and airplanes may use similar navigation technology, the specific application and security risks will differ because of the context in which they were used. Both personal devices and ship devices are often physically mobile and, based on local and international Internet infrastructures, devices will be mobile across several networks and international lines. These device communications across the Internet are a vulnerable aspect of IoT that must be considered. Moreover, a network is often as secure as its most vulnerable device, meaning device access and permissions must be set accordingly. Sensing devices (e.g., temperature, vibration, sound) in the maritime context are also used differently when compared to other. While many sensors are installed in the control areas, many are also placed in engineering. These support a number of systems and human decisions across a ship, as seen in in Figure 1. This diversity is what separates ship and port devices most from more traditional IoT devices, and defines the unique aspects of a maritime IoT.

Many benefits of an IoT comes from large data analytics and the rich flow of information from multiple sources. In particular, cargo management using IoT enabled tags may revolutionise the shipping industry [18]. Not only would this have significant effects on the maritime industry, if fully implemented and considering the volume of cargo shipped around the globe, maritime devices could become the biggest device contribution to the global IoT. It has been reported that a single modern shipping ship can host 5,000 data tags, and 3,000 sensors across the main control system and engine room [17]. These types of IoT devices can be seen on the ship-device part of the IoT diagram in Figure 3. The diversity and number of devices as well as the maritime cyber-security skill levels of crews today have contributed to 87% of mariners to think their IoT security could be improved [17]. This would mean that a significant portion of a global IoT would be dedicated to maritime operations, therefore also having significant effects on the cyber-security of other industries. Another factor that could lead to maritime devices dominating the IoT space would be if more ships decided to follow the remote control, remote access, or autonomous routes, as they are likely to need more sensors (and monitoring) devices, and more communication devices, to compensate for a reduced crew, or no crew at all [21].

3.4. Autonomy

Because of growing demands on maritime-based trade, many organisations in this sector have begun to consider different levels and types of autonomy as a solution. Autonomous ports, where cargo is handled by advanced OT systems [7, 20], have already been implemented in the real world. Because of the complexity in autonomous navigation, autonomous ships are a little further behind in being fully realised [21]. However, despite the complexity in designing a fully-autonomous ship, the potential reductions of annual operation costs (estimated up to 90%) are a key driver for this emerging technology [22]. Besides the technical challenges, international laws and the risk of the unknown have complicated the progress toward fully autonomous. Because of this, some organisations have opted for lesser degrees of autonomy. While there are definitions for autonomous cars, provided by SAE, there are no formal definitions for different levels of ship autonomy. However, an adaption of SAE autonomous car definitions for autonomous ships has been provided in [21] and simplified into Table 1.

Table 1 Modified SAE autonomy definitions for ships and relevant emerging technology.

	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**	**Tier 5**
SAE-based Ship Autonomy	No/minimal autonomy. Small crew required for most, if not all, ship operations.	Partial automation with local crew for simple tasks, e.g. advanced auto pilot.	Conditional autonomy, potential interventions by crew	High autonomy, ship is mostly self-running. Local or onshore crew is rarely required.	Complete autonomous operations in all potential settings.
Remote operations	Not required	Not required	Not required, but likely	Required for operations	Not required, but likely
Sensors / IoT	Needed to aid crew decision	Needed to aid crew decision	Needed to aid crew and autonomy decision	Needed to aid remote crew and autonomy decision	Needed for complete autonomous decisions

Remote access and control, as discussed in Section 3.2, plays into the higher levels of autonomy. With roughly 2GB of data stored per day on a modern ship [17], autonomous ships at tiers 3 and 4 are likely to accrue even more data, in order to feed certain control algorithms, and need to send that data frequently to remote crew. While tier 3 autonomous ships have on-ship crew that can analyse data and react, with a reduced crew it is highly likely that a more specialised off-ship crew will be set up to access data remotely. This can result in communication vulnerabilities, where data can be denied or altered. However, as previously discussed with virtual reality and augmented reality, data can also be altered while stored on the ship or at a remote location. In tier 4 autonomous ships, it is highly likely that both remote access and remote control will be implemented since higher levels of autonomy makes it likely that crew will be off-ship. Lastly, tier 5 autonomy means that, potentially, the ship is fully autonomous and self-directing and does not need contact or assistance from remote crew. However, it is highly unlikely that the owner of the ship will not have contingency plans. Therefore, it is highly likely that remote operations are possible, but unlikely to be used for a fully autonomous ship.

As discussed in Section 3.3, the number of devices that maritime could contribute to an IoT network are extensive. The previous statistics on roughly 3,000 sensors in a modern ship [17] is impressive, however, it has been reasoned that an autonomous ship must host significantly more sensors in order to continue normal operations. This is necessary, as there will be little to no crew to monitor surroundings and ship health and all this data must be gathered digitally [21]. Therefore, it is likely that the number of additional IoT sensors needed to gather critical data for decision-making would increase significantly from tier 1 to tier 5 autonomy. By eventually making sensors the only source of information, the security of the individual sensors themselves should be enhanced as well. Moreover, in these cases data integrity becomes imperative, which makes the secure storage and transfer of this data an important cyber-security decision as this technology develops.

3.5. Energy

Besides cost savings and safer operations, another driver for emerging technology in maritime is protecting the environment. Regulations have changed operations, such as max speeds, however it is important to note that the change of energy collection, storage, and use, will likely have effects on cyber-security as well. By potentially drawing from multiple energy sources, such as wind during a voyage, the energy storage and distribution systems must be able to cope with several inputs as well as outputs and be able to control the flows of energy with high precision. Especially on a ship, which can be highly isolated and stricter with energy consumption, a smart grid may be necessary to direct all these flows [23]. With power systems, for IT and OT, becoming interconnected and integrated with multiple sensors and external systems, this opens a completely new range of cyber threats. Similar to data storage and transfer, energy must be stored safely to prevent hazardous outcomes, and the flow of energy must be correct to both ensure optimal operations as well as prevent certain systems from overloading or systems malfunctioning because they are not receiving enough power. As these renewable energies and smart grids continue to emerge into ships, it is important to note the potential cyber risks.

4. CONCLUSION

In conclusion, the maritime sector is accelerating its use of advanced technology in a wide range of maritime operations. These emerging technologies, whether they be brand new or technology adapted to the maritime sector, have many uses for improving efficiency and physical safety, however, they may also increase the number of cyber-vulnerabilities in ports and ships. This article discussed several of these technologies, including blockchains, the “digital twin”, remote operations, virtual/augmented reality, IoT, autonomy, and smart renewable energy. As systems become more interconnected and shift more decision making and operations to computers, both in cyber-space and in the physical world, it is important to note the potential cyber-risks as these technologies become more prevalent in the maritime sector in order build in cyber-protections early on. This will help ensure physical and cyber security as ships evolve, as well as protect shipping operations.

REFERENCES

[1] Allianz. (2018). Allianz risk barameter. Allianz Global Corporate and Speciality SE.

[2] International Maritime Organization (IMO), 2012, “IMO’s contribution to sustainable maritime development”. Available: http://www.imo.org/en/OurWork/TechnicalCooperation/Documents/Brochure/English.pdf.

[3] R. Subramanyam and M. S. Krishnan, "Empirical analysis of CK metrics for object-oriented design complexity: implications for software defects," in IEEE Transactions on Software Engineering, vol. 29, no. 4, pp. 297-310, April 2003.

[4] D 'amico, Angela & Pittenger, Richard. (2009). A Brief History of Active Sonar. Aquatic Mammals. 35. 426-434426. 10.1578/AM.35.4.2009.426.

[5] Ackoff, Russell, (1971). Towards a System of Systems Concepts. Management Science Vol 17, No. 11. https://doi.org/10.1287/mnsc.17.11.661

[6] Mansouri, Mo & Gorod, Alex & H. Wakeman, Thomas & Sauser, Brian. (2009). Maritime Transportation System of Systems management framework: a System of Systems Engineering approach. Int. J. Ocean Systems Management Int. J. Ocean Systems Management. 1. 200-226. 10.1504/IJOSM.2009.030185.

[7] Rebollo, M & Julián, Vicente & Carrascosa, Carlos & Botti, V. (2019). A multi-agent system for the automation of a port container terminal.

[8] A. Rothblum, “Human error and marine safety,” International Workshop on Human Factors in Offshore Operations (HFW2002), 2000.

[9] Verhoeven, Peter and Sinn, Florian and Herden, Tino T., “Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology,” Logistics vol 2, 2018.

[10] Boschi, Alexandre & Borin, Rogério & Cesar Raimundo, Julio & Batocchio, Antonio. (2018). An exploration of blockchain technology in supply chain management. 27-28.

[11] Allison, Ian. (2017). Maersk and IBM want 10 million shipping containers on the global supply blockchain by year-end. International Business Times. https://www.ibtimes.co.uk/maersk-ibm-aim-get-10-million-shipping-containers-onto-global-supply-blockchain-by-year-end-1609778

[12] Lo, Chris. (2017). Digital twins in shipping: the open-source approach. Ship Technology. https://www.ship-technology.com/features/digital-twins-shipping-open-source-approach/

[13] World Economic Forum (WEF). (April 2018). “Blockchain beyond the Hype: A Practical Framework for Business Leaders”. Available: http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf

[14] Tam K, Jones K. MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment, WMU Journal of Maritime Affairs, Jan 2019

[15] Baldauf, Michael & Procee, Stephan. (2014). Augmented Reality in Ships Bridge Operation.

[16] Frydenberg, Synne & Nordby, Kjetil & Eikenes, Jon Olav. (2018). Exploring designs of augmented reality systems for ship bridges in arctic waters.

[17] Drew Brandy, SVP Market Strategy, Inmarsat Maritime. “IoT in Maritime – Inmarsat Research Programme”. (2018). Digital Ship – CIOLondon Forum

[18] Jia, Xiaolin & Feng, Quanyuan & Fan, Taihua & Lei, Quanshui. (2012). RFID technology and its applications in Internet of Things (IoT). 2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings. 10.1109/CECNet.2012.6201508.

[19] Rolf H. Weber, “Internet of Things – New security and privacy challenges”, Computer Law & Security Review, Volume 26, Issue 1, Pages 23-30. 2010

[20] G. Wilshusen, “Maritime critical infrastructure protection: Dhs needs to enhance efforts to address port cybersecurity,” GAO-16-116T, 2015.

[21] K. Tam and K. Jones, “Cyber-risk assessment for autonomous ships,” IEEE TCS Cyber Security, 2018.

[22] D. MORRIS, “Worlds first autonomous ship to launch in 2018,” http://fortune.com/2017/07/22/first-autonomous-ship-yara-birkeland/, 2017.

[23] G. N. Ericsson, "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure," in IEEE Transactions on Power Delivery, vol. 25, no. 3, pp. 1501-1507, July 2010