Maritime Technology and Research

https://so04.tci-thaijo.org/index.php/MTR

Research Article

The influence of information technology on the implementation of the International Safety Management (ISM) Code: A shift from paper-based to paperless ships

Samrat Ghosh* **and Apsara Abeysiriwardhane**

National Centre of Ports and Shipping, Australian Maritime College, University of Tasmania, Australia

Article information

Received: February 9, 2021
Revised: April 24, 2021
Accepted: April 27, 2021

Keywords

Maritime,
Safety,
Quality assurance,
International Safety Management Code,
Security,
Information technology

Abstract

To provide an international standard for the safe management and operation of ships and for pollution prevention, the International Maritime Organization (IMO) introduced the International Safety Management (ISM) Code (adopted in 1993 and entered in force on 1st July 1998). The Code, through its guidelines and recommendations, provides seafarers (ship's crew) the course of action for the safety and quality assurance process on ships. Traditionally a paper-based system, the ISM Code is now being digitalized in every aspect to streamline the processes to improve ship operations. This paper presents findings of a review of existing literature available on the world wide web to highlight areas of the Code that have been impacted by technology and the benefits that are being reaped. However, recent cyber attacks on ships and the maritime industry require a discussion on various implications associated with ships becoming increasingly reliant on technology and the advancing digital world. This paper highlights and explains the related implications and suggests strategies to address them.

1. Introduction

The International Safety Management Code (ISM code), a vital component of the SOLAS (Safety of Life at Sea) convention entered into force in July 1998. This code was introduced by the International Maritime Organization (IMO) after the ship 'MS Herald of Free Enterprise' sank off the port of Zeebrugge in 1987, killing 193 out of its 539 passengers and crew (Vandenborn, 2018). Its purpose is to provide an international standard for the safe management and operation of ships and for pollution prevention. The Code's overall objectives include the safety of human life at sea, the prevention of human injury and loss of life, and the avoidance of damage to the marine environment and maritime property (IMO, 2019a). The structure of the ISM Code is split into two parts. First, 12 elements (resources and personnel, maintenance of the ship and equipment, documentation, etc.) out of 16 elements come under Part A (Implementation), and the remaining 4 elements represent Part B (Certification and Verification). The guidelines and recommendations laid out in the Code facilitate the procedures for safety and quality assurance on ships and similar vessels. Many shipping companies have adopted the ISM Code as a means to achieve quality

**Corresponding author: Australian Maritime College, University of Tasmania, Australia*
E-mail address: sghosh@utas.edu.au

assurance, since the Code provides an internationally recognized standard for the safe operation of ships, through introducing systems of safety, documentation, and management based on the ISO 9002 standards of quality management systems. The Code promotes quality assurance on ships through safe operations and pollution prevention by laying down rules to ensure that existing regulations and conventions (MARPOL, SOLAS, STCW, etc.) are complied with (Theotokas & Alexopoulos, 1998). The principles set down by the code are interpreted as safety policies from the shipping company to the ship's crew through a documentary system subject to periodical audits and assessment by the company and by external agencies. Failure to comply with the requirements of the Code and the resulting quality management systems may prevent a vessel from commercial trading. When it comes to implementing the ISM code on ships, all of the 3 parties (shipping companies, maritime regulators (for example, the Australian Maritime Safety Authority, or AMSA) or governing authorities (flag state and/or port state control), and the ship's crew (seafarers)) together play important roles. However, the research (Johns, 2018; Cosgrave, 2018) presented in this paper will explain how these important roles are incrementally being impacted by the modern digitalization of ships.

With the advancement of technology, the digitalization of industries is on the rise. In the maritime industry, digitalization has created huge impact. Ships have become information centers where data is being generated and transmitted throughout the world. Meanwhile, advancement in satellite communication has improved connectivity, allowing the exchange of huge volumes of data at very low cost. This advancement in technology is driving the industry in the automation of processes and functions, where it has created positive impact on safety, the environment, and commercial performance. Although, it is not a new concept, digitalization has entered the shipping industry in the recent past and is still evolving. The technologies used can be considered complex and, as digital solutions replace traditional paper-based systems, this paper presents a study of the relationships between the old and new systems.

Digitalization, as defined by Clerck (2017) and Hagberg et al. (2016), is the process of using digital technologies to transform processes to facilitate new forms of value creation. According to Hagberg et al. (2016), one of the ways to do so is a transformation from 'analogue' to 'digital'. Although digitalization includes both operational technology (managing the operation of physical process, systems and machineries) (Devereux & Vella, 2018; Crittenden et al., 2019) and information technology (the flow of digital information and data) (Gobble, 2018; Morley et al., 2018), the focus of this paper is solely on how information technology and its evolution is transforming the implementation of the ISM Code and the resulting safety and quality assurance processes on ships and similar vessels. Hence, a key research question investigated and answered in this paper is as follows: How is the evolution of information technology changing the implementation of the ISM Code on ships? In doing so, this paper presents ways in which information technology has impacted the documentation, maintenance systems, certification, recording systems, reporting systems, and audits and inspections which form part of the quality assurance systems on ships through the ISM Code.

However, recent studies have revealed that the evolution of information technology has brought about a spate of cyber attacks on ships and shipping companies. For example, due to an increasing number of sophisticated cyber attacks, Fairplay and BIMCO jointly conducted a maritime cyber security survey and found that, out of 350 respondents more than a fifth reported that they had been the victim of an attack (IHS Markit, 2018). In addition to the previous finding, 72 % reported that their own company had been a victim of a cyber-related incident in the previous 12 months; 49 % reported service disruption as the result of the attack, with the incident causing financial loss for 25 % of respondents; and only 16 % reported that the breach had been covered by insurance, meaning 84 % had not been covered (IHS Markit, 2018). With a vast number of ships at sea or in port at any one time, the maritime transport industry is highly exposed to cyber attacks. The link between onboard and shore side systems also adds to the complexity, and the cyber security of a ship is also dependent on the cyber security of the land-based infrastructure that makes it possible. The disruption caused by a cyber attack could be significant, costly, and dangerous. A compromised ship system could initiate physical harm to the information technology (IT) and operational technology (OT) systems on the ship, or to its personnel and/or cargo, potentially endangering lives or causing the loss of the ship (Splash, 2020). Thus, it is evident that the evolution of digital technologies can cause a threat to not only maritime security (terrorist acts against shipping and other maritime interests, unlawful acts, resource security, etc.) (Nas, 2015), but lead to complications in ensuring maritime safety (Nas, 2015) (e.g., a vessel's navigation system may be hacked and lead to intentional grounding or collision).

In this regard, this paper also presents the implications of using information technology in the maritime and shipping industry. The findings presented in this paper are based on a review of the existing literature available on the world wide web and are intended to educate seafarers, shipping companies, and other stakeholders. It is the authors' understanding that a literature review adopted as a research methodology will advance knowledge in this field in the future.

2. The benefits of information technology of the implementation of the ISM Code on ships

2.1 Documentation

The ISM Code requires every vessel to develop, implement, and maintain a safety management system (SMS). According to the Code, SMS *"means a structured and documented system enabling Company personnel to effectively implement the Company safety and environmental protection policy"* (IMO, 2002, p. 6). An SMS is designed to have procedures in place to protect the crew, ship, and the environment. Before the introduction of information technology on ships, an SMS was paper-based, with a limited number of copies available to read. Updates to an SMS were sent as paper documents that were attached to the SMS externally. Having an SMS in a digital format allows for it to be a controlled document, so that any of the changes to procedure that are approved can be accessed from one spot, i.e., the company server (Hutchins, 2017). This ensures that the ship's crew are working to the current procedures, rather than previous procedures that may have not been updated in a physical copy. When a company has several vessels, these improvements in procedures can be updated across the whole fleet. This not only increases the safety of the procedure being used, but limits confusing conflicts when crew are transferred to other vessels within the fleet.

When a company SMS is accessed via a ship's computers, accessing the SMS for the ship's crew can be quick and easy. With hard copies, changes and updates to the SMS need to be posted to every individual ship, which causes delays between updates and implementation. However, by converting the ship's SMS to a digital format, real-time changes made to the SMS by the company are reflected instantly without delay (Hutchins, 2017). Furthermore, company officials (ship superintendents, fleet superintendents, etc.) can refer to the SMS from anywhere in the world. Seafarers can be trained and briefed ashore regarding the upcoming changes to the SMS and can be given access to the SMS even when they are on leave. They can also update their knowledge regarding new regulations, codes and guidelines coming into effect, and changes in the company policies and work procedures during their vacation period ashore.

Converting an SMS to a digital format allows a ship's staff to access the SMS more efficiently, as many people can access the copy at the same time using a computer. Required reference documents, such as IMO resolutions and circulars, can be attached as links on the same page where it is relevant. This has made it much easier to find reference documents (Hutchins, 2017) and to search for information on a ship's SMS through the use of keywords on the computer. For example, in order to convert their company's SMS to a digital format, many ship operators have implemented the DocMap®, a web-based documentation tool for navigating through quality assurance documents (Wilhelmsen, 2020). Each crew member has their own logging details on the

DocMap® document navigation system; hence, provisions are given to review, give feedback, and provide suggestions to the company.

2.2 Maintenance systems

The necessity of standardized and secure functioning equipment is understood when it does not function correctly or has mechanical failure. Equipment breakdown will cause additional labor and costs. Failure in one component may cause damage to other components and machinery or result in accidents. In extreme situations, the ship itself could be at risk, or might even be lost. Failure prevention with planned maintenance is more pragmatic than the time and costs required for reparation of machinery after a breakdown. According to the ISM Code, "*The Company should establish procedures to ensure that the ship is maintained in conformity with the provisions of the relevant rules and regulations and with any additional requirements which may be established by the Company"* (IMO, 2002, p. 10).

Planned Maintenance Systems (PMS) are installed onboard to comply with the aforementioned requirement of the ISM code. These systems assist a ship's crew with planning the maintenance of onboard equipment and ships, as per the requirements of the important conventions (SOLAS, MARPOL, etc.), flag state, and manufacturers. A PMS allows shipowners and operators to plan, perform, and document a vessel's maintenance at intervals, complying with the classification society (Lloyd's Register, DNV GL, Indian Register, etc.) and manufacturer requirements. The objective is to ensure safe and reliable vessel operations, including equipment, in addition to ensure compliance with all applicable regulations. There are different ways of achieving this, depending on the size and complexity of the shipping company and the types of vessels in operation. In all cases, a systematic approach to maintenance is based on risk assessment and begins with the establishment of a complete database of machinery, equipment, and fittings.

A PMS was originally a paper- or a chart-based system in which all maintenance required to be done on ship's equipment is recorded. When the running hours of the machinery are updated, or when the time is due for the routine maintenance of equipment, it will be reflected in the system. Records of the inspection findings, maintenance, damages, and non-conformities can also be recorded in the system. Photos can be attached to the work orders, and work order findings can be flagged to be checked during the next inspection or maintenance. A PMS does not always necessitate the use of a computer program. A simple record of equipment-associated maintenance tasks and running hours, along with the dates of the last maintenance and a calculation of the next maintenance schedule, is adequate. But with reference to expanding fleet size and complexity of equipment, the number of maintenance tasks grows. A PMS based on paper documents will require excessive administration work, adding to the seafarers' workload. This is where digitalization plays a vital role on modern ships.

A digitalized PMS is a software integrated into shipboard computers in which all maintenance required on a ship's equipment is recorded. Most companies are using computer programs for PMSs which are capable of being updated online; the companies can monitor the maintenance of the ships and their equipment (DNV GL, 2020a). With advancements in technology, the PMS has advanced, and data-driven prognostics and health management (PHM) for predictive maintenance, especially on fully autonomous and semi-autonomous ships (autoships) (Niculita et al., 2017), have been developed. PHM utilizes algorithms built on historical sensor measurements to provide automatic data pre-processing, detection of faults, isolation of faulty components, prediction of fault probabilities, and estimation of the progression of already-detected and classified fault-types. Thus, PHM can provide intelligent maintenance recommendations or directions when maintenance operations are needed (Ellefsen et al., 2019) and provide decision support to create a perfect maintenance schedule that reduces failures. Subsequently, this schedule can be used to optimize maintenance operations for autoships in the next appropriate ports of call.

One of the vital parts of the ISM code is the preventative maintenance system which forms part of the SMS. With the use of information technology, the document can now be a live document which can be viewed in real time on the ship and ashore, and updated accordingly. The benefits of this are the confirmation that work is being completed as required, and that shore side work requests can be actioned in a timely manner (Shipnet, 2020). These procedures should be updated when potential risks within a procedure are discovered. With the integration of information technology in these systems, advance notices are issued by the system with respect to critical inspections and maintenance, while warnings are issued to work orders on the due date (UpKeep, 2020). Such systems will prevent the ship's crew from missing any required inspection or maintenance to be carried out on time. In the event where the ship's staff need to find records of the previous inspections and maintenance, they can be easily found in the system under the equipment maintenance history, instead of wasting time and manpower to find old records. A properly followed PMS will provide a well-maintained ship and shipboard equipment. Properly maintained and fully functioning ships and equipment have a major positive impact on the safe operation of ships and the objective of the ISM Code. Newly developed Advanced PMSs, such as "*NS Enterprise*" developed by "*ABS Group*", provide a wide range of digitalization with respect to the ISM Code. Such systems are not only limited to maintenance of the ship and shipboard equipment (ABS Group, 2020). Such software contains systems to report non-conformities, accidents, and near-misses onboard.

2.3 Certification

The use of information technology in safety and quality assurance systems allows official forms, checklists, and work permits to be downloaded on to a ship's computer systems. It also allows the ship's staff to monitor the status of the mandatory certificates in real time (DNV GL, 2020b). The ship is required to carry the original and updated certificates onboard, and systems can be set to send alerts ahead of time to prevent oversights for the revalidation or re-issuance of these certificates. For a long time, classification societies (also known as class) provided paper certificates on completion of their inspections and audits but, with the increasing use of information technology, electronic certificates are becoming popular. The certificates are published on the customer portal immediately upon completion of a survey or issuance from the class. Certificates can also be received by utilizing an e-mail subscription facility or delivered in an electronic format onboard the vessel. For example, in 2015, DNV GL formulated the digital development strategy and started the transformation journey of modernization and the digital classification society (DNV GL, 2015). The electronic classification certificate, which was first launched in 2017, has been recognized by almost all flag states, and has basically replaced the previous paper certificate, which greatly facilitates ship owners and ship management. DNV GL was also the first classification society in the industry to issue digital certificates, accelerating industry change and digital transformation (DNV GL, 2020b). The traditional certificate process takes about 3 weeks from issuance to delivery to the appropriate recipient, and DNV GL (2020b) issues an electronic certificate in just 4 minutes.

Digitally signed electronic documents are both secure and more shareable with charterers, ports, flag administrations, insurers, and other stakeholders. The documents are secured against tampering and carry a digital signature and a unique tracking number (UTN) for the purpose of checking their validity and authenticity (Cosgrave, 2018). The validity and authenticity of a document can be verified via an online authentication service. Electronic certificates eliminate the costs associated with paper handling (e.g., printing and archiving) and, hence, save time and money because of reduced administrative workload. Digital documents can be saved on computer and pose no risk of misplacement. They can also be shared with stakeholders using specialized codes that allow exclusive access. Digital statutory certificates of ships can be subjected to continuous observation and verification, ensuring that they are available with the latest updates (DNV GL, 2020a).

Reducing the number of documents being completed on paper minimizes the chance of the documents being lost or destroyed. When an ISM auditor comes onboard, it is a lot easier to access the online database to find all relevant completed documents and checklists. Digitally signed electronic documents are becoming easier to create, more secure, and more widespread in all industries, shipping included. DNV GL is one of the first classification societies that have achieved full-scale production capability of electronic certificates (DNV GL, 2020b) which supports the issuance of electronic certificates to the entire fleet of vessels at the first periodical survey after roll out, subject to respective flag state acceptance. Ship owners and managers, as well as flag states and port state authorities, vetting agencies, and other companies benefit from a paperless class and statutory regime. Managing, sharing, storing, and verifying the authenticity of certificates is easy and secure with the support of the relevant class.

2.4 Reporting systems

Section 9 (Reports and Analysis of Non-Conformities, Accidents and Hazardous Occurrences) of the ISM Code specifies that SMSs should include procedures ensuring that non-conformities, accidents, and hazardous situations are reported to a ship owner’s company, investigated, and analyzed, with the objective of improving safety and pollution prevention (IMO, 2002). It also specifies that the company should establish procedures for the implementation of corrective action, including measures intended to prevent recurrence. This is where information technology has really added another layer of safety to the ISM code, by allowing real time reporting of an accident on board the ship (DNV GL, 2020c). This real time reporting can quickly alert the Designated Person Ashore (DPA), who can then make a quick analysis of the report. The DPA provides a link between the ship’s crew and the company (IMO, 2002). The DPA, in consultation with the ship’s master and safety officer, provides a quick and safe solution to rectify the safety issue onboard and to prevent another accident potentially happening. Before the introduction of reporting in a digital format, this corrective action would take a lot longer to implement and, thus, possibly cause another accident onboard before any control measures were put in place. The digital data also enhances the reporting requirements in real time for the relevant shore-based authorities. In Australia, the AMSA has to be notified of any shipboard accident when a crew member is injured. The electronic format of the reporting forms has enabled the ship’s master to submit an Incident Alert Form (Form 18) to the AMSA within the required time of 4 hours.

2.5 Recording systems

According to Section 2.3.2 of the revised guidelines on the implementation of the ISM Code by administrations, as introduced by the Australian Government, “*All records having the potential to facilitate verification of compliance with the ISM code should be open to scrutiny during the examination*” (Australian Government, 2006). With the introduction of information technology in the shipping industry, hard copy records are being increasingly replaced with electronic record books. For example, from 1 October 2020, IMO amendments to MARPOL (International Convention for the Prevention of Pollution from Ships) Annexes I, II, IV, and V (and the NOx Technical Code, 2008) will allow the use of electronic record books (in lieu of hard copy records) (Lloyd’s Register, 2020).

The IMO amendments and guidelines apply to the following record books:
Oil Record Book, parts I and II (MARPOL Annex I)
Cargo Record Book (MARPOL Annex II)
Garbage Record Book, parts I and II (MARPOL Annex V)
Ozone-depleting Substances Record Book (MARPOL Annex VI)
Recording of the tier and on/off status of marine diesel engines (MARPOL Annex VI)

Record of Fuel Oil Changeover (MARPOL Annex VI)

Record Book of Engine Parameters (NOx Technical Code, 2008) (Lloyd's Register, 2020).

To comply with these record keeping provisions, new and prevailing installations of electronic record books shall be verified by the flag states, or where authorized by the flag state, to the IMO's Guidelines for the Use of Electronic Record Books under MARPOL (Resolution MEPC.312 (74)). Where the class is performing the approval, it will consist of type approval of the software and a subsequent installation survey on board. It is essential for any ship choosing to use MARPOL electronic record books to carry a ship-specific declaration which attests the installation and meets the prerequisites of the IMO guidelines. The declaration may be issued by the flag state or, where authorized by the flag state, may be issued by the class following an installation survey on board. During MARPOL surveys or port state control inspections, the lack of such a declaration means an electronic record book (and the records it contains) may not be considered as fulfilling the record-keeping provisions of MARPOL and the NOx Technical Code, 2008.

2.6 Audits and inspections

According to the ISM Code, it is the responsibility of the company (owner or charterer) to operate ships and take over all responsibilities and duties under the ISM Code. They should develop, implement, and maintain an SMS which consists of procedures for internal audits and management reviews. More than 30 years ago, all ships had to be put into dock for inspection. Later, professional third-party agencies could judge the underwater bottom condition through underwater cameras and other equipment, which was the beginning of the gradual development of the use of digital technology for audits and inspections. In special circumstances (e.g., the trade routes of vessel or border restrictions due to pandemics like COVID-19), an inspector or auditor may be unable to attend to the vessel physically to carry out audits. In such circumstances where physical audits and inspections are challenging, many companies have come up with remote audit procedures where they carry out the ship's audit without physically reaching the ship, conducting part of their job efficiently and meeting the requirements for ISM code and SOLAS. In doing so, companies have amended their SMSs and introduced this practice. For example, Stag Marine Management (a marine consultant and ship management company) conducts remote audits using the data obtained from the voyage data recorder (VDR) and ensuring that such audits meet the requirements of the ISM Code (Stag Marine Management, 2018).

By carrying out remote audits, companies can save significant amounts of money from their vessel's budget and manage the workload of their staff. In remote audits, auditors will provide lists of documents with respect to the audit and then carry out checks and recommend what areas need attention to avoid any incidents/accidents. With the help of VDR audits, real-time assessment can be carried out (Stag Marine Management, 2018). This audit is generally carried out during the arrival/departure of vessel at certain ports. This way, outcomes can be discussed with the vessel as well as the office staff, so the hard work of ship's crew can be appreciated, as well as recommend to them corrective actions which should be done prior to external audits, vetting inspections, and upcoming PSC inspections. In the initial stage, the whole remote inspection is only applicable to a few projects of relatively less importance. For example, if it is a special ship inspection carried out every 5 years, DNV GL still uses field surveyors to conduct the inspection, to ensure comprehensive quality.

The records of internal/external audits are included in advanced PMSs. Any findings, observations, or non-conformities that require corrective actions will be shown as work orders linked to the audit report. Therefore, the ship's staff can easily take the required corrective actions and record those actions in the same system. An advanced PMS will also provide the ship's staff with the details of the ship's certificates, annual / intermediate and 5 yearly surveys details, and records of equipment calibrations. The last carried out date and next due dates of maintenance works are also clearly indicated. Advance notices show up in the system and give warnings of the due date. Such a system will prevent the ship's staff from missing the expiry of certificates, surveys, and the calibration of equipment. Records of drills, exercises, and training sessions carried out are also included in an advanced PMS. It will also show the scheduled drills, exercise, and training, in accordance with the rules and regulations laid down by the IMO codes, flag states, etc.

3. Implications of evolving digital technology for the maritime and shipping industry

3.1 Cyber threats

The cyber threat to the maritime and shipping industry is analyzed and explained based on the Confidential, Integrity, Availability (CIA) Model of traditional security and cyber security. Confidentiality deals with the loss of privacy and authorization, integrity with the loss of trust and accuracy, and availability with the loss of resources (Ruha, 2018). With the introduction of information technology on ships, and an ever-increasing number of systems on board being reliant on networks across vessels, it is imperative to safeguard shipping from cyber threats and vulnerabilities. A vessel's operational systems are now more frequently connected to the internet. This can possibly give unauthorized access to ships and cause malicious attacks on the ship's equipment. Systems can also be compromised when not connected to the internet with removable media such as USB drives, which can introduce viruses and malware. Cyber security threats continue to be one of the top threats facing governments, businesses, and private individuals around the world, and attacks have increased exponentially on vessels and the maritime industry. A recent example was the ransomware attack on the Maersk shipping company. In that attack, the company's container shipping, oil tanker, and tugboat operations were crippled by computer outages that allegedly slashed the company's profits by up to US$300 million (Lord, 2020).

With ever-increasing technology, the risk of cyber attacks has required cyber risk management to be incorporated into the ISM Code. In 2017, the IMO amended the ISM Code to explicitly include cyber security by adopting "Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems" (IMO, 2019). The resolution encouraged administrations (ship owners, flag states, classification societies, etc.) to ensure that existing SMSs addressed cyber risks no later than the first annual verification of a company's Document of Compliance (DoC) after 1 January 2021 (IMO, 2019b).

3.2 Training needs and associated costs

Although the IMO has recognized the need to incorporate cyber security measures firmly into SMSs, recent incidents have shown how the weak link in these measures stem from the human element on board ships. For example, the Maersk line was subject to a cyber attack after an employee ashore responded to an email carrying malware virus that impacted a number of its container terminals and online cargo booking systems (Safety4sea, 2020). Although vessels remained unaffected in this attack, the maritime industry should draw lessons from such attacks, and engage in the proper training of their seafarers working on board ships. The seafarer needs to be trained in authentic scenarios simulating real-world situations (Ghosh, 2017) to understand what it means to work on a cyber-enabled ship and to be at the front line of cyber security (Cyber Citadel, 2020). Hence, there is a need for shipping companies to invest in training their staff regarding cyber security awareness and test their crew through cyber drills that simulate 'hacking' of systems onboard.

Electronic transactions and the digital exchange of data has become the new normal and a means of survival for companies in the maritime industry. As the industry progresses towards the further digitalisation of operations and systems on board ships, the advancing technology requires more automation, more complicated software, and more connectivity. This increased connectivity makes protecting all these systems a complex, challenging, confusing, and costly process (Kapalidis, 2019). The key issues that make cyber security difficult for the maritime industry include the many different classes of vessels that operate in different environments. These vessels tend to have different computer systems built into them. Many of those systems are designed to last no more than 3 decades, and many ships operate outdated and unsupported operating systems, which are the ones most prone to cyber attacks (Kapalidis, 2019).

The users of these maritime computer systems also change frequently. For example, ship crews are highly dynamic, often changing at short notice or more regularly over periods of 3 to 6 weeks. As a result, crews often use systems that they are unfamiliar with, increasing the potential for cyber security incidents relating to human error. The maintenance of shipboard systems, including navigational systems, is often contracted out to a variety of third parties. A similar situation exists in land-based small enterprises. It is perfectly possible that a ship's crew may have little understanding of how different onboard systems interact with each other. Hence, shipping companies will face significant costs in keeping their systems and the operators of these systems updated.

3.3 Legal status of digital certificates and documents

The legal status of digital certificates is a concern for both flag states and port states. Two issues that mainly cause concern in ensuring trust and security in the use of electronic documents is the validity of digital signatures and issuer validity (Cosgrave, 2018). The legal basis to address these concerns is provided through the IMO and the national laws of the state. For example, many European nations have been at the forefront of initiating the use of unique identification numbers and software (e.g., E-IDAS) to ensure signatures and certificates are authentic and validated. Countries like Denmark have created e-certificates that are tamperproof due to encryption and digital file signature. However, there is an absence of a clear legal framework that will allow the widespread replacement of paper certificates with digital documents (Cosgrave, 2018). As a result, at the current stage, many flag states do not accept electronic statutory certificates. For example, the digital certificates issued by DNV GL is not accepted by countries like Egypt, France, and Greece (DNV GL, 2020).

3.4 Risk of loss of employment for seafarers

A ship is only allowed to sail if the minimum safe manning is fulfilled. Minimum safe manning is discussed under the ISM code in terms of resources and personnel (IMO, 2002). The company should ensure that each ship is appropriately manned in order to encompass all aspects of maintaining safe operations on board. The introduction of digital technology on ships has reduced the workload of seafarers so that the shipping companies have the opportunity to reduce the crew by a huge percentage (HSBA, 2018; Hogg & Ghosh, 2016; Kinthaert, 2017). Hence, over the past years, the minimum safe manning has reduced dramatically on ships. Some of the ranks no longer exist on ships because of automation that has resulted due to the evolution of digital technologies. For example, there were "radio officers" earlier, to operate the radios which were used as tools of communication between the coast guard and the ship. However, with the increasing use of advanced technological systems, communication has become more user-friendly and convenient, and the position of radio officer is almost obsolete on modern ships. As another example, the introduction of the electronic chart display and information system (ECDIS) has highly eased the deck officer's workload with its automatic capabilities, such as the route planning and route monitoring of ships; and automated types of machinery have reduced a considerably large amount of workload for a ship's engineers, which allows reducing the safe minimum crew. Hence, the use of digital technologies in the implementation of the ISM Code on ships may replace the traditional roles and duties of seafarers, and lead to their loss of employment as well.

4. Conclusions

Over the last decade, the digitalization of the world has increased exponentially. Leading industries have adopted many of these technological advancements as profitable and sustainable business strategies. These technological advancements have been integrated into the global shipping and maritime trade as well. Due to the large volume of goods carried by sea, ship owners and operators have integrated technological advancements into the operation and management of their ships. By doing so, the shipping companies intend to improve safety, efficiency, and reliability. One of the ways to reduce accidents on ships is to improve the safety and quality assurance processes, achieved through following the procedures laid out in the ISM Code. In this paper, the impact of information technology (as part of the digitalization of the shipping industry) on the implementation of the ISM Code is studied to understand how the safety management process has become more streamlined and transparent due to the allowing of many more parties to be involved in the process and, hence, giving access to differing ideas and contingencies, instead of relying on a ship's crew to solve all issues.

The use of information technology in the implementation of the ISM code when used with a ship's SMS (converted to a digital format) increases the efficiency for which the code was intended. In the past, ships would have to either wait until port to exchange documents with the company or use limited satellite communications. Now, with a continuous connection to shore, parts of the SMS can be monitored for compliance and ensure that there is a reduction in oversights in following safety procedures which can result in a ship potentially being detained. The flow of digital information has a positive impact on safety, profitmaking, time saving, and marine environment. Gathering all the data from multiple sources allows shipping to make better future decisions within specific time frames by creating more efficient and responsive organizations. Using the electronic format of the PMS together with the digital format of the SMS allows companies to monitor real-time events onboard vessels, such as engine performance, bridge watching, and cargo work monitoring, which can lead to rectification of the issues or improvement in safety onboard vessels, which eventually leads to higher performance standards.

However, recent reports of maritime cyber security threats and incidents have increased greatly as technology becomes more sophisticated. The maritime industry has been relatively slow to realise that ships are now intricately linked to cyberspace. The maritime industry is heavily reliant on electronic commerce in many of its daily business transactions, including recordkeeping, human resources data, the loading and discharging of cargo, and the location of containers on the docks, on land transportation and on ships. The industry is, therefore, exposed to cyber attack threats that can have severe repercussions. While the IMO and governments have enacted legislation to counter such attacks, the implementation of the same does not, at present, appear to be entirely effective, and is not keeping pace with the advances of technology and digitalization. To ensure worldwide implementation, governments and regulatory bodies need to join forces to amend national laws and legislation, which will promote the safe use of digital systems and documents on board ships.

Although shipping companies need to hire specialist IT professionals to resolve failings in the system, the ship's crew need to play their part to prevent breaches of cyber security on ships and have contingencies to manage the results of such breaches. This requires shipping companies to not only invest in the training of seafarers to manage cyber risks on board, but also to shortlist highly skilled employees and find ways for them to contribute ashore if technology replaces their roles on board ships. With the ever-increasing reliance on direct internet server connections between ships and shore, the safety management system must continue to have its information protected. Stakeholders in the maritime industry must look into ways to set aside an amount of their budget to protect the integrity of safety and quality assurance systems as future technologies develop. The digital evolution is forming the maritime future in every aspect, and impacts all of its segments, taking advantage of modern ship design and new technologies. Therefore, in this transformation phase, the impact of using information technology in shipping must be considered as an important factor, in order to establish an international standard for the safe management and operation of ships, as well as for pollution prevention.

References

ABS Group. (2020). *Marine vessel management software*. Retrieved from https://www.abs-group.com/What-We-Do/Software-Solutions/Nautical-Systems-Software

Australian Government. (2006). *Marine orders: Part 58. International Safety Management Code. Issue 2. Consolidation No. 1*. Australian Maritime Safety Authority (AMSA). Retrieved from https://www.legislation.gov.au/Details/F2006C00466

BIMCO. (2018). *The guidelines on cyber security onboard ships. Version 3.* https://www.bimco.org/news/priority-news/20180924-cyber-security-survey

Clerck, J. (2017). *Digitalizaton, digital transformation: the differences*. I-Scoop. Retrieved from https://www.i-scoop.eu/digital-transformation/digitization-digitalization-digital-transformation-disruption

Cosgrave, B. (2018*). Electronic certificates for ships: A LOFTY (legal, operations, fraud, trust) analysis* (Master's thesis). World Maritime University.

Crittenden, W., Biel, I., & Lovely III, W. (2019). Embracing digitalization: Student learning and new technologies. *Journal of Marketing Education, 41*(1), 5-14. doi:10.1177/0273475318820895

Cyber Citadel. (2020). *Logistics cybersecurity far from 'ship shape'*. Retrieved from https://www.cybercitadel.com/logistics-far-from-ship-shape

Devereux, M., & Vella, J. (2018). Debate: Implications of digitalization for international corporate tax reform. *Intertax, 46*(6), 550-559.

DNV GL. (2015). *Our ships in the digital world: DNV GL Innovation Day examines shipping in the age of digitalization*. Retrieved from https://www.dnvgl.com/news/our-ships-in-the-digital-world-dnv-gl-innovation-day-examines-shipping-in-the-age-of-digitalization-45530

DNV GL. (2020a). *Planned maintenance system for technical ship management: Ship manager technical*. Retrieved from https://www.dnvgl.com.au/services/planned-maintenance-system-for-technical-ship-management-shipmanager-technical-1509

DNV GL. (2020b). *Electronic class and statutory certificates*. Retrieved from https://www.dnvgl.com/maritime/electronic-certificates/index.html

DNV GL. (2020c). *Digital MRV and DCS reporting streamlines the verification process*. Retrieved from https://www.dnvgl.com/expert-story/maritime-impact/Digital-MRV-and-DCS-reporting-streamlines-the-verification-process.html

Ellefsen, A. L., Æsøy, V., Ushakov, S., & Zhang, H. (2019). A comprehensive survey of prognostics and health management based on deep learning for autonomous ships. *IEEE Transactions on Reliability, 68*(2): 720-740. doi:10.1109/TR.2019.2907402

Ghosh, S. (2017). Can authentic assessment find its place in seafarer education and training? *Australian Journal of Maritime & Ocean Affairs, 9*(4), 213-226. doi:10.1080/18366503.2017.1320828

Gobble, M. (2018). Digitalization, digitization, and innovation. *Research-Technology Management, 61*(4), 56-59. doi:10.1080/08956308.2018.1471280

Hagberg, J., Sundstrom, M., & Egels-Zandén, N. (2016). The digitalization of retailing: An exploratory framework. *International Journal Retail & Distribution Management, 44*(7), 694-712. doi:10.1108/IJRDM-09-2015-0140

Hogg, T., & Ghosh, S. (2016). Autonomous merchant vessels: Examination of factors that impact the effective implementation of unmanned ships. *Australian Journal of Maritime & Ocean Affairs, 8*(3), 206-222. doi:10.1080/18366503.2016.1229244

Hutchings, S. (2017). *Safety management systems*. Safety4sea. Retrieved from https://safety4sea.com/safety-management-systems

IHS Markit. (2018). *Maritime cyber survey 2018: The results*. BIMCO. Retrieved from https://www.bimco.org/news/priority-news/20180924-cyber-security-survey

IMO (International Maritime Organization). (2002). *International Safety Management Code: And revised guidelines on implementation of the ISM Code*. International Maritime Organization, London.

IMO (International Maritime Organization). (2019a). *The International Safety Management (ISM) Code*. Retrieved from https://www.imo.org/en/OurWork/HumanElement/Pages/ ISMCode.aspx

IMO (International Maritime Organization). (2019b). Maritime cyber risk. Retrieved from https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

Johns, M. (2018). *Seafarers and digital disruption: The effect of autonomous ships on the work at sea, the role of seafarers and the shipping industry*. HSBA (Hamburg School of Business Administration). Hamburg / London.

Kapalidis, K. (2019). *Cyber security challenges for the maritime industry*. Safety4sea. Retrieved from https://safety4sea.com/cm-cyber-security-challenges-for-the-maritime-industry

Kinthaert, L. (2017). *Digital transformation: How will it change the seafarer's role?* Informaconnect. Retrieved from https://informaconnect.com/digital-transformation-how-will-it-change-the-seafarers-role

Lloyd's Register. (2020). *Statutory alert: Use of MARPOL electronic record books*. Retrieved from https://info.lr.org/l/12702/2020-09-29/9kc976

Lord, N. (2020). *The cost of a malware infection? For Maersk, $300 million*. Digital Guardian. Retrieved from https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million

Morley, J., Widdicks, K., & Hazas, M. (2018). Digitalisation, energy and data demand: The impact of internet traffic on overall and peak electricity consumption. *Energy Resource & Social Sciences, 38*(1), 128-137. doi:10.1016/j.erss.2018.01.018

Nas, S. (2015). The definitions of safety and security. *Journal of ETA Maritime Science, 3*(2), 53-54. doi:10.5505/jems.2015.42713

Nikulita, O., Nwora, O. & Skaf, Z. (2017). *Towards design of prognostics and health management solutions for maritime assets* (pp. 122-132). In Proceedings of the International Conference on Through-life Engineering Services 2017.

Ruha, T. (2018). *Cybersecurity of computer networks* (Thesis, Bachelor's Degree). Helsinki Metropolia University of Applied Sciences, Helsinki.

Safety4sea. (2020). *Maersk line: Surviving from a cyber-attack*. Retrieved from https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack

Shipnet. (2020). *Planned maintenance system for ships*. Retrieved from https://www.shipnet.no/planned-maintenance-system-for-ships/#1576765249087-%200b620a32-4242

Splash. (2020). *The cyber imperative: A vessel as one digital ecosystem*. Retrieved from https://splash247.com/the-cyber-imperative-a-vessel-as-one-digital-ecosystem

Stag Marine Management. (2018). *VDR navigation audit.* Retrieved from https://www.stagmarine.com/VDR-navigation-audit.php

Theotokas, I., & Alexopoulos, A. (1998). Safety & quality in the shipping industry: A legal analysis of the ISM Code's principles & applications. *European Research Studies Journal, 1*(3), 81-98.

UpKeep. (2020). *Planned maintenance systems (PMS)+ 6 features*. Retrieved from https://www.onupkeep.com/answers/preventive-maintenance/planned-maintenance-systems

Vandenborn, Y. (2018). *Twenty years of the ISM code*. Safety4sea. Retrieved from https://safety4sea.com/twenty-years-of-the-ism-code/#:~:text=The%20ISM%20code%20was%20born,its%20539%20passengers%20and%20crew

Wilhelmsen. (2020). *DocMap*. Retrieved from https://www.wilhelmsen.com/other-services/imtc/courses/information-technology-courses/docmap-course