Research Article
Turkish Journal of Maritime and Marine Sciences
DOI: 10.52998/trjmms.1519901
Volume: 10 Special Issue: 1 (2024) 1-18

Understanding of the Maritime Future Mentality; Safe E-navigation and Safe Maritime Surface Communication

Denizciliğin Geleceği Mantığının Anlayışı; Emniyetli E-Seyir ve Emniyetli Suüstü İletişimi

Türk Denizcilik ve Deniz Bilimleri Dergisi
Cilt: 10 Özel Sayı: 1 (2024) 1-18

Hasan Bora USLUER[1,*]
[1] *Galatasaray University, Maritime Vocational School, Istanbul*

ABSTRACT

Developing and changing technology affects all sectors globally. Although it primarily affects information systems digitally, it affects all sectors indirectly. Maritime transport, the most important transportation mode in the world, is affected by technological progress as seafarers, ships, and ports. When used for its intended purpose, the technology employs intelligent and rational solutions based on the logic of identifying previous errors and developing predictions accordingly. Maritime transportation is the movement of ships between ports safely and without harming the environment. The sea is a dynamic surface not previously exposed to fixed effects and is affected by meteorological and environmental conditions. As the international maritime authorities keep pace with technological advancements, they have embraced the e-navigation concept, a digital revolution that is set to transform the industry. This shift to Electronic Navigation requires all operations to be digital, making transmission easier and more efficient. It also mandates uninterrupted and high-quality digital communication with ships' land facilities during the entire voyage. ECDIS, one of the advanced automation technology products used for e-navigation, and the vector map ENC it uses are of great importance. ENC maps are produced with specific standards. S-100, which is described as the latest and most advanced standard, provides sailors with good opportunities for safe navigation and communication. The study has been prepared to explain e-navigation types of equipment, their standards, and how they communicate according to cyber security.

Keywords: e-Navigation, Maritime Communication, S-100, ECDIS, ENC, Maritime Management.

Article Info
Received: 21 July 2024
Revised: 30 July 2024
Accepted: 05 August 2024

[*] (corresponding author)
E-mail: hbusluer@gsu.edu.tr

To cite this article: Usluer, H.B. (2024). Understanding of the Maritime Future Mentality; Safe E-navigation and Safe Maritime Surface Communication, *Turkish Journal of Maritime and Marine Sciences*, 10 (Special Issue: 1): 1-18. doi: 10.52998/trjmms.1519901.

ÖZET

Gelişen ve değişen teknoloji küresel anlamda tüm sektörleri etkilemektedir. Öncelikle bilgi sistemlerini dijital olarak etkilese de dolaylı olarak tüm sektörleri etkilemektedir. Dünyanın en önemli ulaşım şekli olan deniz taşımacılığı, denizciler, gemiler ve limanlar gibi teknolojik gelişmelerden de etkilenmektedir. Teknoloji, amacına uygun kullanıldığında, geçmişteki hataları tespit edip buna göre tahminler geliştirme mantığına dayalı, akıllı ve akılcı çözümler kullanır. Deniz taşımacılığı, gemilerin limanlar arasında güvenli ve çevreye zarar vermeden taşınmasıdır. Deniz, daha önce sabit etkilere maruz kalmayan, meteorolojik ve çevresel koşullardan etkilenen dinamik bir yüzeydir. Uluslararası denizcilik otoriteleri teknolojik gelişmelere ayak uydururken, sektörü dönüştürecek dijital bir devrim olan e-navigasyon konseptini benimsemektedir. Elektronik Seyir'e geçiş, tüm işlemlerin dijital olmasını gerektirirken,iletimi daha kolay ve daha verimli hale getiriyor. Ayrıca tüm seyir boyunca gemilerin kara tesisleriyle kesintisiz ve yüksek kalitede dijital iletişim kurulmasını da zorunlu kılıyor. E-Seyir için kullanılan ileri otomasyon teknolojisi ürünlerinden biri olan ECDIS ve kullandığı vektör haritası ENC büyük önem taşımaktadır. ENC haritaları belirli standartlarda üretilmektedir. En yeni ve en gelişmiş standart olarak nitelendirilen S-100, denizcilere güvenli seyir ve iletişim konusunda önemli ve etkili faydalarda bulunmaktadır. Çalışma, e-navigasyon ekipmanlarının türlerini, standartlarını ve siber güvenliğe göre nasıl iletişim kurduklarını açıklamak amacıyla hazırlanmıştır.

Anahtar Sözcükler: e-Seyir, Deniz Haberleşme, S-100, ECDIS, ESH, Denizcilik Yönetimi.

1. INTRODUCTION

The primary purpose of e-navigation is to explain the real world in full detail, which is important in its logic, and to ensure safe navigation and management on the bridge. The Main issue is to define the nowcasting, which is potentially better than forecasting. But the first question is how to reach the nowcasting about e-nav and maritime communication. Years of work on navigation and maritime communication have led to a wealth of data in the field of marine and marine sciences. (Usluer, 2022)

This data, which includes sea, oceanography, bathymetry, meteorology, land details, communication routes and instruments, effective ranges, and working mechanisms, presents an opportunity for further exploration and potential collaboration (Figure 1; Figure 2; Table 1). As the marine industry continues to decipher and apply this data in the real world, we invite you to join us on this journey of discovery. S-100 international standards, prepared by IHO and understood to be of great use to maritime companies in the future, draw attention to compatibility and interoperability. When creating and implementing e-navigation strategies, it's crucial to remember their pivotal role in preventing ship-borne pollution.

Figure 1. IHO S-100 Digital Communication. (IHO, 2021)

With safety at sea and navigation as our primary goals, it must address the issue of ship-borne pollution. Numerous techniques have been explored and developed to tackle this pressing issue. With electronic navigation being a key aspect of maritime operations, it's clear that marine sciences, such as hydrographic and oceanographic information, are indispensable. (Joseph *et al.*, 2021) The need for their standardization, particularly through the Common Maritime Data Structure (CMDS) working structure and the S-100, has become increasingly apparent in recent years (Lee *et al*., 2024). Interoperability involves creating

consistent services for users when individual components are technically different and managed by various organizations. The essential element of ensuring compatibility and interoperability of the dataset is standardization through consistent semantic data modeling.

Table 1..Literature General Overview

Author/Authors	Publish Date	Article Information
Xiao *et al.*	2015	AIS
DiRenzo *et al.*	2015	Cyber Security
Ming-Cheng	2016	ECDIS
Hareide *et al.*,	2018	Cyber Security
Liangbin *et al*	2018	AIS
Shapiro *et al.*	2018	Maritime Transportation Risks
Rutkowski	2018	ECDIS
Kaleem Awan and Al Ghamdi	2019	e-Navigation
Svilicic *et al.*	2019	ECDIS
Tam and Jones,	2019	Cyber Security
Androjna *et al.*	2020	Cyber Security
Joseph *et al.*	2021	Maritime Safety
Bolat *et al.*	2022	Cyber Security
Usluer	2022	Marine Science
Arıcan *et al.*	2023	ENC-CATZOC
Algani *et al.*	2024	Maritime Communication
Jios *et al.*	2024	ENC
Kayışoğlu *et al.*	2024	Cyber Security
Lee *et al*	2024	S-100
Uflaz *et.al.*	2024	Cyber Security

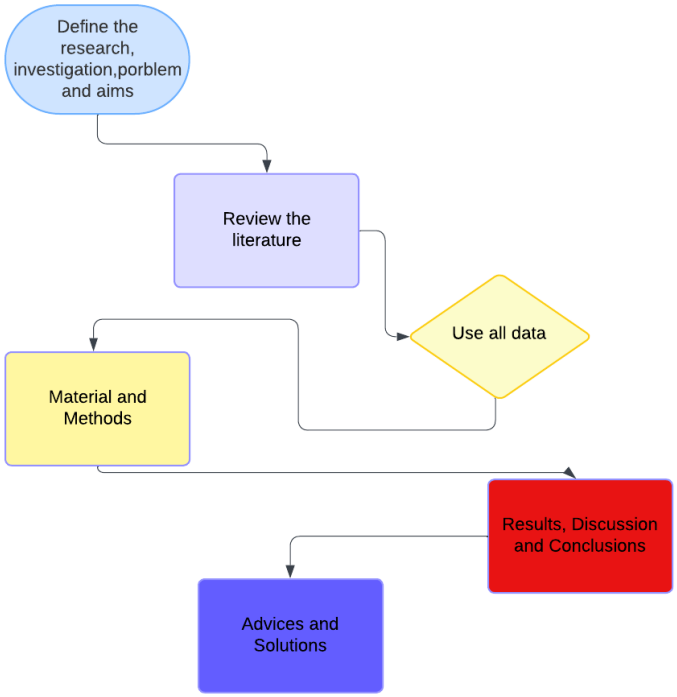

Figure 2. Flowchart of the study

1.1. E-Navigation Overview

The geomatics studies and satellite observations have proven that more than 70% of the world, which does not have a regular shape, is covered with water geography. It is known that more than 80% of the world's population lives near the coastline. It is known that 90% of the transportation activities carried out to meet endless human needs are carried out by maritime transportation. Also, well known that the seas and oceans connect the globe. E-navigation is the safe use of all marine cartographic data sets obtained using the technology resulting from the conversion from analog to digital. It is converting from analog to digital. The first step towards e-navigation was using digital maps for navigational purposes in the early 1990s. At this stage, IHO member countries worked jointly to ensure navigational safety and standards, which are currently ongoing (Figure 3). Due to developing technology, digital maps, and all related systems began to be used on ships with an integrated and compatible automation working method following IMO's founding rules in the early 2000s.

Figure 3. e-nav concept (safety4sea, 2024)

The integrated systems in question are devices such as RADAR, SONAR ECDIS, ENC, AIS; NAVTEX, GYRO, VHF, BNWAS, ECHOSOUNDER, VDR, AUTOPILOT, DPS, and AIS can easily be seen by Figure 4. While e-Navigation was first defined as the technology of tomorrow, it has now become available due to development. Seafarers globally are actively using developing technology devices for safe navigation, which have many strengths.

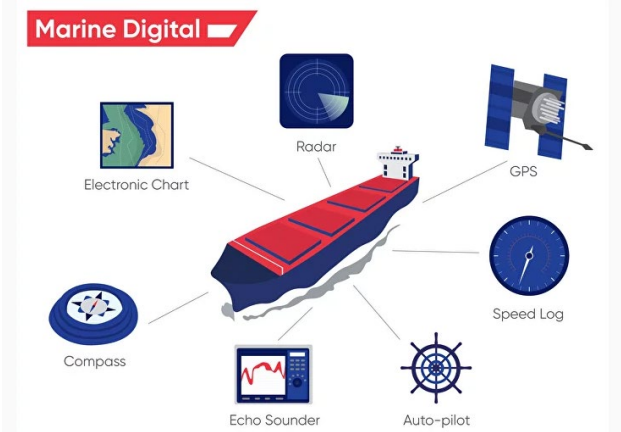

Figure 4. E-Nav systems overview. (Marine-Digital, 2024)

The support of institutions and organizations working for navigational safety, such as IHO and IMO, simplifies the duties of watchkeeping officers during navigation by easily using standardized data, which refers to data that is uniformly formatted and can be easily interpreted by different systems, reducing workloads, increasing safety and environmental performance, and offering real economic advantages to the maritime industry. After a stage, e-navigation has created a fundamental basis for autonomous ships. In this way, connected, digitalized ship systems that operate with high efficiency and safety will be able to operate with constant and standard discipline.

1.2. E-Navigations Equipment's

1.2.1. ECDIS

The universality of device electronic chart display and information system (ECDIS) installations, considered the most important of the e-navigation components, will provide revolutionary solution plans for the era of e-navigation informatics, and intellectualization. (Ming-Cheng, 2016) According to Rutkowski (2018), ECDIS is a useful component that is also a complex, safety system with multiple options for display and integration for working safety navigation (Figure 5). According to the Safety of Life at Sea (SOLAS) convention's regulation V/19, international vessels must carry ECDIS, with some criteria beginning in 2011 (Kayışoğlu *et al.*, 2024).

Figure 5. ECDIS system on board. (Safety4sea, 2024)

1.2.2. ENC

Electronic navigation charts, which stand for ENC, are geographic databases compiled in strict accordance with the IHO specifications. ENCs are GIS products that work with ECDIS for safety navigation. (Arıcan *et al*., 2023; Jios *et al.*, 2024)

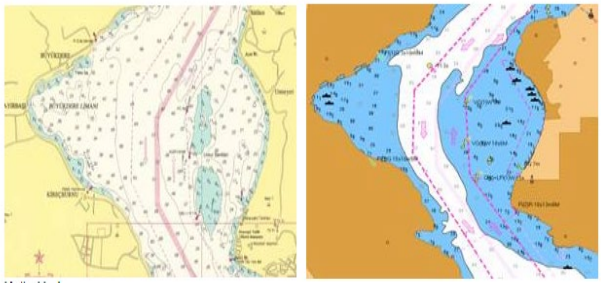

Figure 6. Paper and ENC Charts together. (SHODB, 2024)

Hydrographic organizations produce products that all sailors can understand. This is called standardization. One of the main tasks of IHO is to determine how standard products will be created and to ensure their dissemination. In this context, vector maps were decided to be produced according to certain standards at ENC. According to the vector chart standards S-57, this transition from paper to digital chart marks significant progress and modernization in hydrography (Figure 6). However, it needs to be protected in this state, so the standard called S-63 works to encrypt it. The vector chart produced according to S-57 conditions is encrypted and presented to the user securely (IHO, 2024).

1.2.3. AIS

With navigational safety being the top priority for ships during navigation, the authorities are committed to leveraging devices for this purpose. The Automatic Identification System emerges as a key player in this arena (Figure 7). It provides crucial input parameters in ship traffic simulation models, significantly enhancing risk analysis, especially in the ship's operational area, and thereby preventing potential ship collisions/accidents (Xiao *et al*., 2015; Liangbin *et al*, 2018).

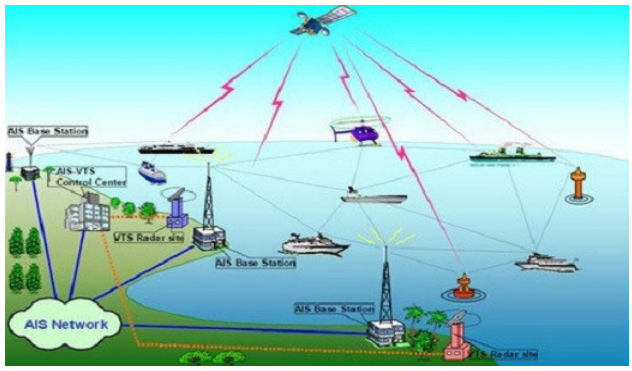

Figure 7.AIS Working cycle. (NATO, 2024)

1.2.4. NAVTEX

At the heart of maritime safety, Navigational Telex is an international communication system that automatically transmits possible danger, safety, and weather reports and warnings to ships on medium frequency. As a crucial part of the International Maritime Organization and the Global Maritime Hazard and Safety System, it works for navigation and seafarer safety, broadcasting free of charge and for the public benefit can easily be seen by Figure 8.

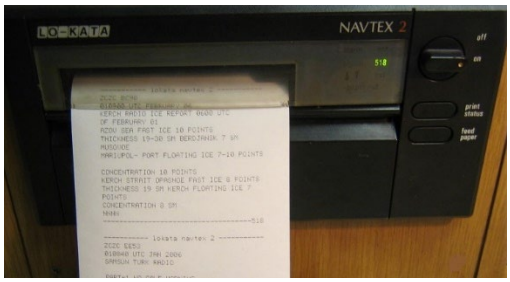

Figure 8.NAVTEX is working onboard (Wikipedia, 2024)

1.2.5. RADAR

Another device used for navigational safety is the Radio Detection and Ranging system. The system, known by the abbreviation RADAR, sends radio signals to perform target detection and distance measurement. It is a versatile vessel device that operates with the help of radio signals. It displays the images of the objects within the signal range by reflecting the radio waves broadcast from its antenna off complex objects and returning them to the antenna, leaving a trace on the screen. This versatile device is one of the essential navigational aids on ships, providing the opportunity to detect objects in difficult navigation conditions, such as darkness at night, fog, or rain, show by Figure 9.

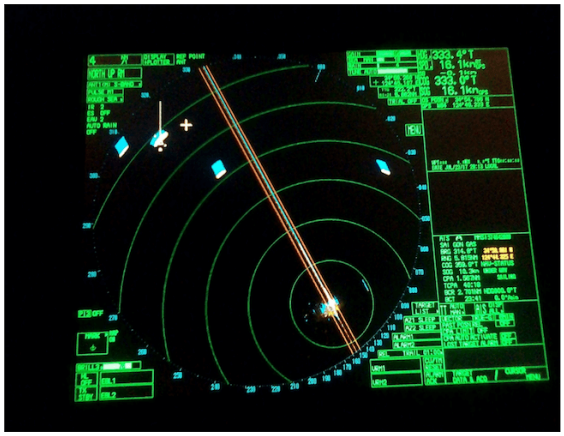

Figure 9. RADAR Screen. (Marineinsight, 2024)

1.2.6. INMARSAT

The International Maritime Satellite Organization and its system provide telephone and data services worldwide, primarily to seafarers and all users who can benefit from this service through terminals established for this purpose (Figure 10). The terminal generally communicates with the satellite and the ground station via the satellite. It provides effective communication services to users who need to communicate over long distances, especially in places without reliable terrestrial networks. Inmarsat also provides free GMDSS services to ships as a public service, demonstrating our commitment to the safety and well-being of the maritime community.

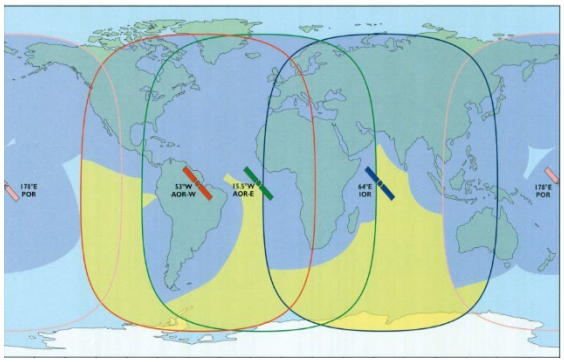

Figure 10. INMARSAT Coverage on Earth (e gmdss, 2024)

1.2.7. VSAT

Marine VSAT (Very Small Aperture Terminal) systems, purposefully designed for maritime use, enhance navigational safety through their adaptable data and voice technology (Figure 11). They facilitate ship tracking over frequencies that determine connection quality and coverage area.

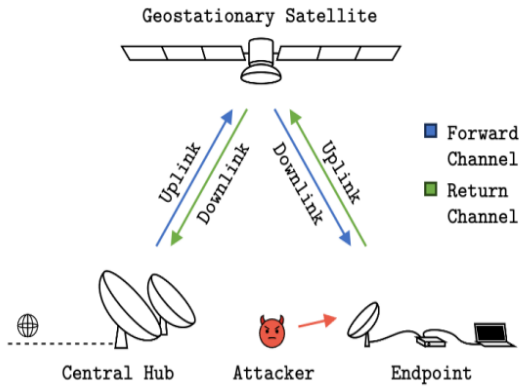

Figure 11. VSAT Communication System working flow (Bisping *et al*., 2024)

Their principle of operation, utilizing C-band, a lower frequency range that requires larger antennas, ensures high-quality satellite Internet communications even in adverse weather conditions, providing reassurance and preparedness for any situation.

1.2.8. GNSS

Global positioning service providers provide latitude-longitude satellite location information

that is globally available. To express these correctly, the known and developed positioning systems known as GNSS-Global Navigation Satellite Systems are as follows, GPS-Global Positioning System to the United States, GLONASS – To the Russian Federation, BEIDOU – To China, QZSS – To Japan GALILEO – To the European Union, IRNSS/GAGAN – It is an Indian global positioning system by shown Figure 12.

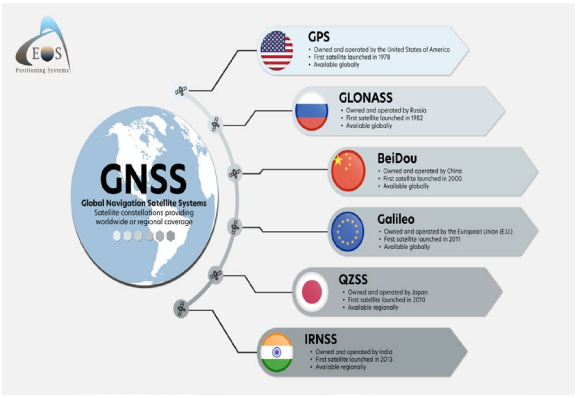

Figure 12. GNSS systems of the world (eos-gnss, 2024)

1.3. S-100 and General Aspects

Institutions and organizations such as the International Maritime Organization work to ensure safe navigation in the world's seas and ensure that all systems and rules are in a clear and understandable structure so that seafarers speaking different languages can understand each other. This understanding is called standardization. S-100, a globally applicable advanced technology product, is a prime example of this understanding. It is a universally understandable data set, designed to provide data from many different data groups in a specific format that all sailors worldwide can understand. Some standards can easily be seen in Table 2 and Figure 13.

This comprehensive framework utilizes data from a wide range of disciplines, including water level information for surface navigation, weather overlay, radio services, aid to navigation information, current information, AIS information, GNSS information, marine traffic management information, underwater keel clearance information, and navigational warnings. It brings together marine protection area information, ensuring that all necessary data is readily available and usable (IHO, 2021).

Figure 13. S-100 Data Set and Standards. (IHO,2021)

Thanks to S-100, a relationship, almost a bridge, has been created between bathymetry and oceanography data. It should be understood as a completely digital version of marine ecosystem data that all e-navigation systems can understand the real world with digits. So, all these products are used in e-navigation just because the e-nav systems are becoming more intelligent.

- S-101, Electronic Navigational Charts,
- S-102, Bathymetry Surface,
- S-104 Water Level Information for Surface Navigation,
- S-111 Surface Navigation,
- S-41X Weather Overlays are very important standards for e-navigation and S-100 production can seen in Figure 14.

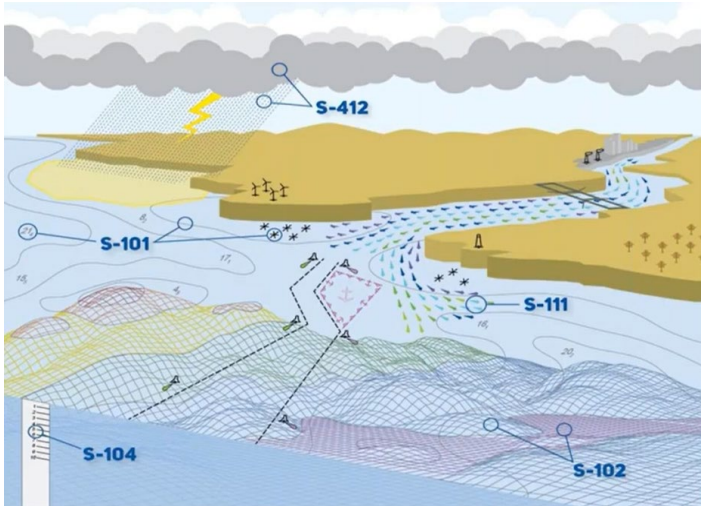

Figure 14. Very important standards for S-100 productions (IHO, 2021)

Table 2. Hydrographic Productions Standards

Standards and numbers	Descriptions
S-4	Regulations for International (INT) Charts and Chart Specifications of the IHO
S-5A	Standards of C.ompetence for Category "A" Hydrographic Surveyors
S-5B	Standards of Competence for Category "B" Hydrographic Surveyors
S-8A	Standards of Competence for Category "A" Nautical Cartographers
S-8B	Standards of Competence for Category "B" Nautical Cartographers
S-11	Guidance for the Prep. and Maint. of Int.(INT) Chart and ENC Sch. and Cat. of INT Charts
S-12	Standardization of List of Lights and Fog Signals (June 2004 - Corrections to June 2006)
S-23	Limits of Oceans and Seas (1953). Sheet maps 1, 2 and 3
S-32	Hydrographic Dictionary
S-44	IHO Standards for Hydrographic Surveys
S-49	Standardization of Mariners' Routeing Guides
S-52	Specifications for Chart Content and Display Aspects of ECDIS
S-53	Joint IMO/IHO/WMO Manual on Maritime Safety Information
S-57	IHO Transfer Standard for Digital Hydrographic Data
S-58	ENC Validation Checks
S-60	User´s Handbook on Datum Transformations involving WGS 84
S-61	Product Specification for Raster Navigational Charts (RNC)
S-62	List of IHO Data Producer Codes
S-63	IHO Data Protection Scheme
S-64	IHO Test Data Sets for ECDIS
S-65	ENCs: Production, Maintenance and Distribution Guidance
S-66	Facts about Electronic Charts and Carriage Requirements
S-67	Mariners' Guide to Accuracy of Depth Information in Electronic Navigational Charts (ENC)

Table 2. Hydrographic Productions Standards (continued)

S-97	IHO Guidelines for Creating S-100 Product Specifications
S-99	Operational Procedures for the Org. and Managem of the S-100 Geospatial Inf. Registry
S-100	I HO Universal Hydrographic Data Model - S-100 based Product Specifications
S-101	ENC Product Specification
S-102	Bathymetric Surface Product Specification
S-111	Surface Currents Product Specification
S-121	Maritime Limits and Boundaries Product Specification
S-122	Marine Protected Areas
S-123	Marine Radio Services
S-127	Marine Traffic Management
S-129	Under Keel Clearance Management
S-41X	Weather Overlay

With up-to-date real-world data, all the officers on the vessels can calculate the fastest, safest, and most efficient voyage globally. Also, the maritime industry is affecting many industries (Figure 15). These technological advantages lay the foundations for the future safe navigation of Maritime Autonomous Surface Ships (MASS).

Figure 15. The Maritime Industry works for many reasons. (IHO, 2021)

1.4. MASS Technology

In addition to the benefits that developing technology products provides to humanity, the most important issue to be faced in the future will be the systems and devices that operate unmanned and will be controlled by humans. In maritime trade and transportation, which as a sector has to use more advanced technology compared to other sectors, the issue currently being worked on and causing many discussions about the future is the Maritime Autonomous Surface Ship.

The maritime industry has always been a sector where innovation and advanced technology have found applications. The need for increased efficiency and operational safety has led to the development of various levels of automation both on ships and on land. Recent surveys and expeditions have included situational awareness sensors, such as radar and sonar systems, autonomous navigation systems, off-board communications technologies like satellite communication, and robotics, among others.

Automation, with its potential to reduce the human element and significantly reduce the likelihood of human error, offers a reassuring prospect for the safety of maritime operations. However, it's important to remember that some risks will always be present. Automated systems, while powerful, are not immune to vulnerabilities, from the most straightforward faults like power outages to more threatening faults like cyber/radio frequency/satellite attacks. Risks vary depending on levels of automation and degrees of autonomy; as fully autonomous ships emerge; a set of unique and completely new challenges will need to be addressed. According to IMO studies, a maritime autonomous surface ship can operate independently of human interaction at four degrees. (IMO, 2019)

Degree one: Ship with automated processes and decision support: Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated and, at times, unsupervised, but with seafarers on board, they are ready to take control.

Degree two: Remotely controlled ship with seafarers on board: The ship is controlled and operated from another location. Seafarers are available on board to take control and manage the shipboard systems and functions.

Degree three: Remotely controlled ship without seafarers on board: The ship is controlled and operated from another location. There are no seafarers on board.

Degree four: Fully autonomous ship: The ship's operating system can make decisions and determine actions independently, opening up a world of exciting possibilities.

1.5. Cyber Security

As in almost every sector, the maritime industry also works by keeping up with changing and developing technology. This technological evolution is not just about digitalization, but also about enhancing safety. The global maritime industry is increasingly trying to digitalize, work with operational integration and automation, and reduce human errors. Major mariner nations and maritime trade organizations use the latest technologies and systems that surpass the familiar classical and traditional designs to produce ships and port equipment with advanced remote-controlled communication and connectivity capabilities (DiRenzo *et al*., 2015; Uflaz *et al*., 2024). Despite the significant benefits that high-level technology and digital systems bring to their users, they also operate in a vulnerable manner to potential technological threats. Cyber-attacks, in particular, pose a critical and immediate threat to the safety and digital security of ships at sea.

Cyber-attacks can be targeted, aiming at a specific company and its ship, or they can be indiscriminate, striking ships with potential cyber vulnerabilities.

One of the e-navigation elements that may be affected by the attack is the Bridge, where ship navigation and management are carried out. Many elements such as ECDIS, AIS, GNSS, and EPIRB located in Bridge, the ship's brain, can be directly affected. The risk of encountering such attacks increases, mainly thanks to the internet service, which has become an essential human need in today's technology and is primarily requested by the crew (Bolat *et al*., 2022).

The potential consequences of cyber-attacks are severe, with the possibility of permanent damage to the hull and electronic systems of all ship systems, both commercial and military. In addition to preventing the ship from seeking help, all technical and documentary information and documents belonging to the ship and companies can be seized, leading to significant operational disruptions.

This situation poses a significant threat to the navigational safety of ships, personnel safety, and the reputation of companies. Therefore, it is of utmost importance for ships to proactively prepare against potential cyber-attacks and establish the necessary protective and preventive infrastructures.

1.6. Maritime Communication Information

When humankind first ventured into seafaring, it was a means to secure food and submarine resources for survival. This journey of exploration and discovery continued, evolving with industrialization and the ambition of powerful civilizations to find and utilize resources. Despite the changing priorities of seafarers, the need for maritime communication has always remained constant, marking a fascinating evolution in the history of seafaring (Figure 16).

Particularly in the marine sector, developments and measures have been prepared due to major disasters. The maritime industry has learned a great lesson and standardized the implementation of measures globally.

The Titanic disaster, a tragic event with global repercussions, demonstrated the benefits of remote and wireless communications. Systems that respond especially to emergency calls and Search and Rescue calls have served maritime for more than 100 years, connecting seafarers across the world (IMO-Radio Communications, 2024).

Figure 16. Navigation and communication, search and rescue. (Safety4sea, 2024)

The International Maritime Organization, a key player in maritime safety, considers issues such as navigational safety, survival at sea, and ship-related marine pollution. It has been particularly effective in coordinating and arranging radio communications for search and rescue in case of emergency at sea, providing a reassuring safety net for maritime professionals and policymakers. The first regulation on the subject, a significant milestone in the history of maritime safety, was implemented by the International Telecommunication Union (ITU) in 1906. This was when the SOS signal was first adopted and put into use, a momentous occasion during the International Radio Telegraph Convention accepted in Berlin (Algani *et al*., 2024).

The International Convention for Search and Rescue at Sea (SAR) and the International Convention for the Safety of Life at Sea (SOLAS) have gained importance as amended in 1974. These regulations are not just historical artifacts, but are still being developed and used today, demonstrating the adaptability and ongoing effectiveness of maritime safety regulations.

2. MATERIALS AND METHODS

According to Researchers at NHL Stenden University of Applied Sciences in the Netherlands, from 2001 to 2024, the Maritime Cyber Attack Database was created. Researchers have collected information on over 170 cyber incidents involving the maritime sector, including incidents impacting vessels, ports, and other maritime facilities worldwide.

Due to the development of technology, maritime cyber security affects both ships and relevant units on land. However, it has been understood that one of the most affected electronic navigation aids used for safe navigation is ECDIS. It has been revealed that ships using ECDIS contain many cyber vulnerabilities, such as collisions, grounding, and accidents that may disrupt safe navigation. (Svilicic *et al*., 2019b; 2019c; Tam and Jones, 2019; Androjna *et al*., 2020, Kayışoğlu, *et al.*, 2024). When all ship assessment types are applied as per the IMO recommendation, a standard of excellence is upheld. It is understood that the most specific element of cyber security assessment is the execution of cyber security testing based on computational vulnerability scanning and Penetration testing techniques. Penetration testing, on the other hand, is a systematic and comprehensive use of legal and authorized attempts to exploit the target system/asset. Its primary role is to prove the existence of potential cyber risks, making it an essential part of the cyber security assessment process. Electronic Chart Display and Information System has revolutionized the safe navigation of ships. By combining paper maps and other nautical publications, ECDIS has digitized navigation, providing real-time updates, accurate positioning, and enhanced situational awareness. This has significantly improved navigational safety (Brčić *et al*., 2019).

Over the last forty years, studies have created the necessity for the formation and use of ECDIS. Of course, along with the benefits of technology, it also caused various problems that posed a threat to navigational safety, such as safe navigation, which faced cyber threats. (Svilicic *et al*., 2019a, b, c; Kaleem Awan and Al Ghamdi, 2019; Lee *et al.*, 2019, Tam and Jones, 2019; Hareide *et al.*, 2018; Shapiro *et al.*, 2018). The International Maritime Organization (IMO), a specialized agency of the United Nations responsible for regulating shipping, has taken necessary steps to manage cyber risk and prepared guidelines and rules for all the world's seas (IMO, 2017b). It has also regulated performance standards (IMO, 2017a) for better and more efficient operation of ECDIS. In cooperation with the International Electrotechnical Commission (IEC), a new maritime standard for maritime navigation and radiocommunication equipment and systems,

IEC 63154, "Cyber Security - General requirements, test methods, and required test results," has started to be studied (IEC, 2019).
Researchers who follow and study digital attacks at sea draw attention to the move to take over the command and control systems of the ships. ECDIS, along with other systems, is significantly impacted by this. When studies on ECDIS between 2010 and 2020 are examined, it is understood that not only one device but also other devices it interacts with are affected. Reports of attacks on more than 20 known e-navigation systems were examined shown by Figure 17.
When cyber-attacks are discussed, it is understood that they attack ship systems using communication systems and communication channels at sea. The investigation revealed that cyber security is aimed at the bridge from which the ship is controlled, especially to take over the cruise control of the ship remotely by affecting the ECDIS device and AIS device. This underscores the urgent need for immediate action to address this critical issue.

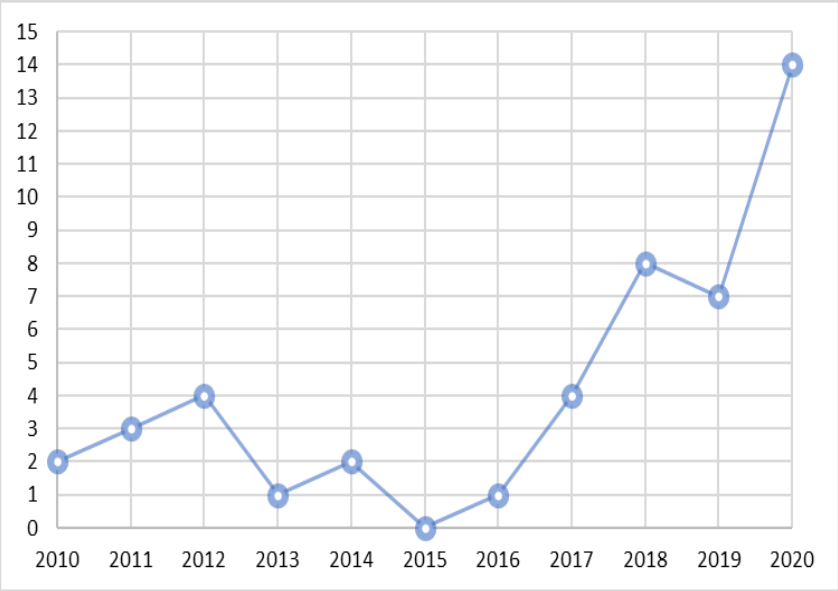

Figure 17. Cyber Incident numbers per year 2010-2020 (Meland *et al*., 2021)

3. RESULTS

The main question is, how can we safely e-navigate the ships?
To ensure safe e-navigation on the ships, the following steps should be taken:

1. **It is crucial to train crew members in effectively utilizing e-navigation systems and how to protect the cyber-attacks. This is a key factor in ensuring their proper use onboard, thereby contributing to the safety and efficiency of the voyage.**
2. Prioritize the use of the most up-to-date electronic navigational charts (ENCs) for route planning. This ensures the ship's route is well-informed and avoids potential hazards and obstacles, thereby enhancing the safety of the voyage.
3. Utilize accurate and reliable data sources: Access accurate and reliable data sources for e-navigation, including meteorological information, water depth, wind speed, and other relevant factors to plan the vessel's course.
4. Identify safety zones and hazard areas: Before commencing navigation, it's crucial to identify potential hazard areas. This vigilance will help you keep clear of these regions during the voyage, ensuring the safety of your vessel and crew.
5. Properly configure automatic pilot systems: It's your responsibility to ensure that automatic pilot systems are accurately configured. This diligence will help maintain the vessel on its intended

course, contributing to the overall safety of the voyage.

6. Verify that radar and other sensors are functioning correctly: Confirm that radar, AIS (Automatic Identification System), and other sensors onboard are in proper working order.
7. Prepare emergency response plans: Develop plans for responding to emergencies such as accidents or fires, train crew members on these procedures, and conduct regular drills to prepare them for any eventuality while using e-navigation systems.
8. **All devices on ships and land must be equipped following cyber security conditions.**

After the eight items explained above, the types of threats that were tried to be explained and the conditions for resisting the threat are mentioned in Table 3. Since all e-navigation systems are integrated and work simultaneously, one cyber-attack element can easily and quickly affect another.

Table 3. Possible Cyber-Attack countermeasure projection.

Affected System	**Affected Devices**	**Possible Precaution against Intimidation and Threats**	**Vulnerabilities effects**
E-Nav Systems (Bridge Navigation System Radiocommunication systems)	Radar ECDIS Conning AIS GPS VDR GMDSS NAVTEX ENC BNWAS Satellite	Ensure the using safe internet and network Internet working security, Ensure using eligible Software, Ensure prepare the Cyber Security applicable procedures, Ensure having available Access controls, Ensure backup of the use of external devices	Make sure that external and internal connections (internet LAN, etc.) are established, Make sure that the software and systems used on all devices are up to date, Ensuring situational awareness, detection, analysis, and intervention during any threat, Ensure all ports to which External Memory can be connected are reliable.
Power systems (generation and distribution)	All the systems (Control, Monitoring, Alarm)	Ensure the possibility to access controls (Physical and logical) Ensure authorized persons' identification checks Ensure Control and audit any time, Ensure it is easy to access by authorized crew member	All-access should be provided to authorized personnel only. All control mechanisms regarding the system must be applicable. All movements must be recorded in the system. The obligation to log out is applied when logging out of the system.

Table 3. Possible Cyber-Attack countermeasure projection (continued).

Affected System	Affected Devices	Possible Precaution against Intimidation and Threats	Vulnerabilities effects
Loading management systems (Dispatch and Administration)	All the systems (Control, Monitoring, Alarm)	Authentication checks must be carried out. (Remote and close) Physical access should only be granted to authorized personnel. National and International Policies and procedures need to be checked periodically. Before using all systems and programs, relevant personnel must be trained.	Authentication using high-level cryptography (Remote) All passwords used should be changed periodically. Situation detection, analysis, and intervention should be carried out when necessary. Every accessible system must be physically and environmentally protected.
Control systems (Access)	All the systems (Control, Monitoring, Alarm)	Ensure that authentication checks are in place. Access permissions should only be provided to authorized personnel. (Physical) All National and International Policies and procedures should be reviewed periodically. Training must be received before using the systems.	Authentication using high-level cryptography (Remote) All passwords used should be changed periodically. Situation detection, analysis, and intervention should be carried out when necessary. Every accessible system must be physically and environmentally protected.
Service and management systems (Crew and Passenger)	All the systems (Control, Monitoring, Alarm)	Ensure the possibility to access controls (Physical and logical) Loading Procedures Ensure authorized persons' identification checks policy Necessary training must be provided to security personnel. Training on security safeguards.	Users must be documented (according to their authority and privileges). Backup systems need to be determined. Sharing of passwords and shared use of accounts is prohibited for all users. The need to recognize and process emergency situations due to situational awareness

Table 3. Possible Cyber-Attack countermeasure projection (continued).

Affected System	Affected Devices	Possible Precaution against Intimidation and Threats	Vulnerabilities effects
Communication systems must use reliable internet.	Connection control equipment must work in harmony with cyber security software.	Protecting confidentiality should be the basic principle. (Especially Network privacy) Updates should be followed. It must be equipped with protection mechanisms against all possible attacks. Latest version protection programs should be used (covering all viruses).	Advanced security measures (such as Routers and firewall) should be used by adopting rules and policies. Continuous notification should be made to the institution and organization where the employee works. Malware infections can be identified.

4. DISCUSSIONS

Maritime transportation carries more than 90% of world trade. Therefore, the maritime industry has a say in all countries with coasts and ports. The sector moves with technology and keeps up with developments quickly. First of all, ships and ports are equipped with advanced technology. The most crucial element, trained human resources, is trained following technological possibilities. However, the development of technology allows malicious use as well as good intentions. Therefore, systemic gaps become cyber threats. Although international institutions and organizations work to ensure safe navigation and prevent marine pollution, cyber security is affected by the rapid development of technology. Ships can be stranded in many threats, from changing their routes to changing their destination port, from opening ship rescue systems to the danger of sinking.

5. CONCLUSIONS

With the rapid evolution of technology, the frequency of cyber-attacks on the maritime sector is on the rise. Shipping Networks and Ships are particularly vulnerable. Notably, even large and crucial companies have fallen victim to these attacks, underscoring the severity of the situation. Despite the professional management of IT staff tasked with defending against these attacks, cyber hackers persist in their activities, employing new methods and effects daily.

Targeted attacks are honing in on the command and control systems of ships, aiming to disrupt both IT and OT technologies. In this context, ECDIS, a key piece of electronic equipment on the bridge, is frequently targeted. While research and tests for precautions are improving daily, the number and severity of threats are also on the rise. It's been found that advanced systems used on ships have previously unrecognized vulnerabilities. Both IMO and electronic device manufacturers advocate and implement preventive measures during production, but the effects of cyber-attacks evolve with technology. Therefore, conducting high-level checks of vulnerabilities and outdated aspects of systems during the production phase can significantly delay and reduce threats.

AUTHORSHIP CONTRIBUTION STATEMENT

Hasan Bora USLUER: Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing - Original Draft, Writing-Review and Editing, Data Curation, Software, Visualization, Supervision.

CONFLICT OF INTERESTS

The author declares that for this article they have no actual, potential or perceived conflict of interests.

ETHICS COMMITTEE PERMISSION

No ethics committee permissions is required for this study.

FUNDING

No funding was received from institutions or agencies for the execution of this research.

ORCID IDs

Hasan Bora USLUER:
https://orcid.org/0000-0001-8988-9288

6. REFERENCES

Algarni, A., Acarer, T., Ahmad, Z. (2024). An Edge Computing-Based Preventive Framework With Machine Learning- Integration for Anomaly Detection and Risk Management in Maritime Wireless Communications, *IEEE Access*, 12: 53646-5366. doi: 10.1109/ACCESS.2024.3387529

Androjna, A., Brcko, T., Pavic, I., Gredanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering*, 8 (10): 776. doi: 10.3390/jmse8100776.

Arıcan, O.H., Arslan, O., Unal, A.U. (2023). The Importance of CATZOC in Passage Planning and Prioritization of Strategies for Safe Navigation. *Marine Science and Technology Bulletin*, 12(4): 445-458. https://doi.org/10.33714/masteb.1333432

Bisping, R., Willbond, J., Strohmeier M., Vincent, L. Wireless Signal Injection Attacks on VSAT Satellite Modems, (2024). Accessed Date: 19.07.2024. https://www.usenix.org/system/files/sec24fall-prepub-538-bisping.pdf is retrieved.

Bolat, P., Kayişoğlu, G. (2022). Security Studies: Classic to Post-Modern Approaches, Section 7, Cyber Security,General Perspective on Cyber Security. (Editor: Arda Özkan and Göktürk Tüzsüzoğlu) Lexigton Book, 175-190

Brčić, D., Žuškin, S., Valčić, V., Rudan, I. (2019). ECDIS transitional period completion: analyses, observations and findings. *WMU Journal of Maritime Affairs*, 18: 359–377. doi: 10.1007/s13437-019-00173-z.

DiRenzo, J., Goward, D.A., Roberts, F.S. (2015). The little-known challenge of maritime cybersecurity. In Proceedings of the 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA), 1–5, Corfu, Greece

eos-gnss, GNSS systems of the world, (2024). Accessed Date: 20.07.2024 https://eos-gnss.com/knowledge-base/gps-overview-1-what-is-gps-and-gnss-positioning is retrieved.

Hareide, O.S., Jøsok, Ø., Lund, M.S., Ostnes, R., Helkala, K. (2018). Enhancing navigator competence by demonstrating maritime cyber security. *The Journal of Navigation*, 71: 1025–1039. doi: 10.1017/S0373463318000164.

Jiao, C., Wan, X., Li, H., Bian, S. (2024). Dynamic Projection Method of Electronic Navigational Charts for Polar Navigation. *Journal of Marine Science and Engineering*, 12: 577. doi: 10.3390/jmse12040577.

Joseph, A., Dalaklis, D. (2021). The international convention for the safety of life at sea: highlighting interrelations of measures towards effective risk mitigation, *Journal of International Maritime Safety, Environmental Affairs, and Shipping*, 5(1): 1-11. doi: 10.1080/25725084.2021.1880766

IHO, An all embracing data model S-100, (2021). Accessed Date: 19.07.2024. https://www.youtube.com/watch?v=IfKqA7ZkN1w is retrieved.

IHO, Definitions (2024). Accessed Date: 20.07.2024. https://iho.int/en/enc-production is retrieved.

IMO, MSC MASS Degrees, (2019). Accessed Date: 20.07.2024. https://maiif.org/wp-content/uploads/2019/06/MSC-100_20-Annex-20-1.pdf is retrieved.

IMO-Radio Communications, (2024). Accessed Date: 20.07.2024. https://www.imo.org/en/OurWork/Safety/Pages/RadiaCommunicationsSearchRescue-Default.aspx is retrieved.

International Maritime Organization (IMO), (2017a). *ECDIS—Guidance for Good Practice, Resolution* MSC.1/Circ.1503/Rev.1

International Maritime Organization (IMO), (2017b). *Guidelines on Maritime Cyber Risk Management*, MSCFAL.1/Circ.3

International Maritime Organization (IMO), (2017c). *Maritime Cyber Risk Management in Safety Management Systems,* MSC 98/23/Add.1

International Electrotechnical Commission, (2019). *Maritime navigation and radiocommunication equipment and systems-cybersecurity-general requirements, methods of testing and required test results*. IEC 63154 ED1

INMARSAT Coverage on Earth, (2024). Accessed Date: 20.07.2024. https://www.egmdss.com/gmdss-courses/mod/page/view.php?id=2370 is retrieved.

KaleemAwan, M.S., AlGhamdi, M.A. (2019). Understanding the vulnerabilities in digital components of an integrated bridge system (IBS). *Journal of Marine Science and Engineering*, 7: 350–370. doi: 10.3390/jmse7100350.

Kayişoğlu, G., Güneş, B.İ., Bolat, P. (2024). ECDIS Cyber Security Dynamics Analysis based on the Fuzzy-FUCOM Method. *Transactions on Maritime Science,* 13 (1). doi: 10.7225/toms.v13.n01.w09.

Lee, E, Mokashi, A.J., Moon, S.Y., Kim, G. (2019). The maturity of Automatic Identification Systems (AIS) and its implications for innovation. *Journal of Marine Science and Engineering*, 7: 287–304. doi: 10.3390/jmse7090287.

Lee, S., Kim, H. (2024). IHO S-100 Data Model and Relevant Product Specification. *the International Journal on Marine Navigation and Safety of Sea Transportation.* 18(2). doi: 10.12716/1001.18.02.04.

Leite Junior, W.C., de Moraes, C.C., de Albuquerque, C.E.P., Machado, R.C.S., de Sá, A.O.A. (2021). Triggering Mechanism for Cyber-Attacks in Naval Sensors and Systems. *Sensors*, 21: 3195. doi: 10.3390/s21093195.

Liangbin, Z., Guoyou, S.İ., Jiaxuan, Y. (2018). Ship Trajectories Pre-processing Based on AIS Data**.** *The Journal of Navigation*, 71(5): 1210-1230. doi: 10.1017/S0373463318000188.

Marine-digital, 21 different types of marine digital equipment's, (2024). Accessed Date: 20.07.2024. https://marine-digital.com/article_21types_of_navigation_equipment is retrieved.

Meland, P.H., Bernsmed, K., Wille, E., Rodseth, O.J., Nesheim, D.A. (2021). A Retrospective Analysis of Maritime Cyber Security Incidents, *International Journal on Maritime and Safety of Sea Tranportation* 15(3): 519-530. doi: 10.12716/1001.15.03.04.

Ming-Cheng, T. (2016), Multi-target collision avoidance route planning under an ECDIS framework, *Ocean Engineering*, 121: 268-278. doi: 10.1016/j.oceaneng.2016.05.040.

NATO Shipping Centre, (2024). Accessed Date: 20.07.2024. https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview is retrieved.

RADAR Screen, (2024). Accessed Date: 20.07.2024. https://www.marineinsight.com/marine-navigation/using-radar-on-ships-15-important-points/ is retrieved.

Rutkowski, G. (2018). ECDIS Limitations, Data Reliability, Alarm Management and Safety Settings Recommended for Passage Planning and Route Monitoring on VLCC *Tankers the International Journal on Marine Navigation and Safety of Sea Transportation*, 12(3). doi: 10.12716/1001.12.03.06.

Shapiro, L.R, Maras, M.H., Velotti, L, Pickman, S., Wei H.L., Till, R. (2018) Trojan horse risks in the maritime transportation systems sector. *Journal of Transportation Security*, 8: 1–19. doi: 10.1007/s12198-018-0191-3.

Safety4sea, e-nav concept, (2024). Accessed Date: 19.07.2024**.** https://safety4sea.com/cm-the-future-of-seafaring-in-an-age-of-safer-smarter-greener-shipping is retrieved.

Safety4sea ECDIS, (2024). Accessed Date: 19.07.2024**.** https://safety4sea.com/cm-ecdis-prons-and-cons-of-paperless-navigation/ is retrieved.

Safety4sea (2024). Navigation and Communication on sea, Accessed Date: 19.07.2024**.** https://safety4sea.com/imo-navigation-communications-and-search-and-rescue-sub-committee-whats-on-the-agenda/ is retrieved.

SHODB, (2024). Paper and ENC Charts together, Accessed Date: 19.07.2024**.** https://www.shodb.gov.tr/shodb_esas/index.php/tr/urunler/haritalar/elektronik-seyir-haritalari is retrieved.

Svilicic, B., Kamahara, J., Rooks, M., Yano, Y. (2019a). Maritime cyber risk management: an experimental ship assessment. *The Journal of Navigation*, 72: 1108–1120. doi: 10.1017/S0373463318001157.

Svilicic, B., Kamahara, J., Celic, J., Bolmsten, J. (2019b). Assessing ship cyber risks: a framework and case study of ECDIS security. *WMU Journal of Maritime Affairs*, 18: 509–520. doi: 10.1007/s13437-019-00183-x.

Svilicic, B., Rudan, I., Frančić, V., Doričić, M. (2019c). Shipboard ECDIS cyber security: third-party component threats. *Pomorstvo-Scientific Journal of Maritime Research*, 33 (2): 176–180. doi: 10.31217/p.33.2.7.

Tam, K., Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18: 129–163. doi: 10.1007/s13437-019-00162-2.

Uflaz, E., Sezer, I.E., Tunçel, A.L., Aydin, M., Akyuz, E., Arslan, O. (2024), Quantifying potential cyber-attack risks in maritime transportation under Dempster–Shafer theory FMECA and rule-based Bayesian network modelling, *Reliability Engineering and System Safety*, 243(1). doi: 10.1016/j.ress.2023.109825.

Usluer, H.B. (2022). The effect of the developing and changing Electronic Bridge Equipment and Electronic Navigation Charts on Intelligent Maritime Transportation Systems. *Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi,* 5(1): 116-125. doi: 10.51513/jitsa.1097807.

Xiao, F., Ligteringen, H., Coen van Gulijk, A., Ale, B. (2015). Comparison study on AIS data of ship traffic behavior, *Ocean Engineering*, 95: 84-93. doi: 10.1016/j.oceaneng.2014.11.020.

Wikipedia, NAVTEX, (2024). Accessed Date: 19.07.2024**.** https://tr.wikipedia.org/wiki/NAVTEX#/media/Dosya:Navtex.jpg is retrieved.