Cyber security risk assessment of navigation sensors in maritime autonomous surface ships

University of Turku
Department of Computing
Master of Science (Tech) Thesis
Cyber Security Engineering
January 2026
Topi Haatainen

Supervisors:
Seppo Virtanen
Jouni Isoaho

UNIVERSITY OF TURKU
Department of Computing

Topi Haatainen: Cyber security risk assessment of navigation sensors in maritime autonomous surface ships

Master of Science (Tech) Thesis, 50 p.
Cyber Security Engineering
January 2026

This thesis conducts a risk assessment for key maritime autonomous surface ships (MASS) navigation technologies using the Formal Safety Assessment (FSA) framework. MASS is in the early stages, and understanding risks is crucial to ensuring safe and reliable autonomous operations. Risks are assessed in the context of global autonomous operations with MASS levels 3 and 4, which represent a high level of autonomy. Risks are identified from the literature and an expert interview with an academic researcher is used to validate the findings. Mitigation solutions are also covered for identified risks. The assessment focuses on six core navigation technologies: Global Navigation Satellite System (GNSS), Automatic Identification System (AIS), radar, LiDAR, and Electronic Chart Display and Information System (ECDIS) and Inertial Measurement Unit (IMU). Common vulnerabilities in these technologies include spoofing and jamming. The assessment suggests that attacks on a single key technology are relatively easy and inexpensive to implement, but effectively disabling the navigation system requires simultaneous attacks on multiple key technologies. The thesis integrates the current findings on risks and mitigation strategies for MASS, offering a structured basis for future research.

Keywords: MASS, risk assessment, navigation, GNSS, AIS, LiDAR, radar, ECDIS, IMU

Contents

1 Introduction **1**

2 Background **4**

2.1 Maritime autonomous surface ships 4

2.2 Global navigation satellite system 6

2.2.1 GPS 7

2.2.2 Galileo 9

2.2.3 GLONASS 9

2.2.4 BeiDou 10

2.3 Radar 11

2.4 Automatic identification system 11

2.5 LiDAR 12

2.6 Electronic Chart Display and Information System 13

2.7 Inertial Measurement Unit 14

2.8 Classification Societies 14

2.9 Route Planning 17

2.10 Berthing and Open sail 18

3 Risk assessment methodologies **19**

3.1 literature review 19

3.2 Risk assessment approach 20

3.3 Interview 21

4 Risks **23**

4.1 Related work 23

4.2 Identifying risks and threats 24

4.2.1 GNSS 24

4.2.2 Radar 26

4.2.3 AIS 28

4.2.4 LiDAR 29

4.2.5 ECDIS 30

4.2.6 IMU 30

4.3 Risk assessment 31

5 Mitigation **36**

5.1 Control options 36

5.1.1 GNSS 37

5.1.2 Radar 40

5.1.3 AIS 42

5.1.4 LiDAR 43

5.1.5 ECDIS 45

5.1.6 IMU 45

5.2 Cost benefit assessment 46

5.3 Recommendations 46

6 Conclusion **49**

References **51**

1 Introduction

We are currently living in an era where we are trying to automate and use artificial intelligence (AI) in all possible ways. The maritime field is no exception, and it also tries to implement as much automation as possible. It is a great opportunity to have better efficiency when ships have automation involved in them, but it also opens up new attack vectors for the possible adversaries to use when they try to exploit the systems. Maritime transportation of commercial goods is the most energy efficient way and the personnel take a large portion of the overall transportation costs. Using automation can reduce the amount of personnel required to operate ships, which could lead to large cost reductions in the whole process.

The International Maritime Organization (IMO) Safety Committee has already discussed the idea of automated ships in 1964 [1]. Rapid advancement in technology has made these autonomous ships more feasible. Japan had a project in 1982-1988 for automated operational systems for maritime operations. In the 2010s, research related to autonomous surface ships began to gather participants. Korea started investigating autonomous surface vessels for survey and surveillance in 2011, and many others followed, such as The European MUNIN project in 2012 and Lloyd's register Guidance in 2016. [2]

It is crucial to identify potential cybersecurity risks as early as possible in the maritime field, as changes in this industry take a long time. It could even take years for the changes to take place. These risks could lead to a catastrophic event

if autonomous vessels are compromised. These ships could be redirected to collide with one another or in a harbor, leading to major financial losses or threatening humans.

When it comes to maritime ships, there are many different components that are potential targets for cyberattacks. Possible target areas include navigation, decision-making software, communications, different sensors, shore-based infrastructure, and supply chain. Autonomous navigation is highly dependent on situational awareness sensors to avoid collisions. This thesis will focus on navigation sensors and provides a risk assessment on them.

More than 80% of the goods traded in the world are transported by maritime transport [3]. To ensure that all these goods reach their destination, maritime vessels must be safe and secure. In 2024 43.1% of maritime incidents were navigational incidents [4]. Navigation safety is a critical part of maritime transports.

This thesis aims to assess and mitigate risks and threats related to the navigation of maritime autonomous surface ships. This is achieved with the help of the following research questions:

Research Question 1: What are the key risks and threats to the navigation systems of maritime autonomous surface ships?

Research Question 2: What emerging cyber security threats are likely to impact the navigational systems of maritime autonomous surface ships in the coming years?

Research Question 3: How can we mitigate these risks and threats?

The risk assessment is based on the formal safety assessment (FSA) recommended by the IMO. Risks are identified through literature and expert interviews.

The core navigation and perception systems are within the scope of this thesis. Specifically, Global Navigation Satellite System (GNSS), Radar, Automatic Identification System (AIS), LiDAR, Inertial Measurement Unit, and Electronic Chart

Display and Information System (ECDIS). This thesis excludes propulsion and steering systems and non-navigation related subsystems. This thesis contributes to the growing body of work on maritime cyber risks. The results aim to help the maritime industry achieve practices in the development of maritime autonomous surface ships.

The structure of the thesis is as follows. Chapter 2 sets the foundation with background information about related technologies. Chapter 3 covers the methodology. Chapter 4 focuses on finding the risks and making the risk assessment. Chapter 5 looks at the mitigation strategies for these identified risks. And finally, chapter 6 concludes all the findings in this thesis.

2 Background

To better understand the cybersecurity threats and risks that are present for MASS navigation, we must first understand how the different systems that contribute to navigation work. There are multiple different systems that contribute to navigation in different ways, such as providing data, making decisions, and performing maneuvers. The focus of this thesis is on the systems that provide navigational data, and the main purpose of the following systems is to provide navigational data to the ship.

2.1 Maritime autonomous surface ships

The International Maritime Organization (IMO) describes commercial vessels that use little to no human intervention to perform the tasks and functions of the vessels, such as navigation and collision avoidance, as maritime autonomous surface ships (MASS). MASS can be currently categorized to four degrees. Degree one means that the vessel has automated processes and decision support, but there are still seafarers on board who control the vessel and can take control of these automated processes. Degree two means that the vessel is controlled remotely but there are still seafarers on board. Degree three means that the vessel is remotely controlled and there are no seafarers on board. Degree four means that the vessel is fully autonomous and capable of making decisions and determining actions on its own. [5] This thesis will focus mainly on degrees four and three.

Electronic systems play a key role in enabling MASS autonomy. There are four main categories for these systems: communication, sensing, decision-making, and actuation. Communication systems are systems that allow the vessel to transmit and receive information from other entities. These systems include radios, satellites, Wi-Fi, cellular networks, and optical links. sensing systems are systems that allow the vessel to collect data from the environment and the vessel itself. These sensors are e.g. radars, GPS, and cameras. Decision-making systems are the systems that allow the vessel to process the data that communication and sensing systems have gathered, and to use the data to plan the route, execute the mission, react to unexpected events, and learn from the past. These systems include computers, algorithms, artificial intelligence (AI), and machine learning (ML). Actuation systems are the systems that execute the decisions made by the decision-making systems. These systems include e.g. the motor, propellers, and thrusters. [5] From figure 2.1 we can see where the navigational systems further inspected in this thesis fit in the categorization.

The core onboard system for autonomous navigation is the guidance, navigation, and control system (GNC). The guidance systems estimate the linear and angular velocities and positions of the vehicles. Navigation systems identify the current and future position of the ship and the environment. The control systems provide the actuator signals. Radio detection and ranging (RADAR) presents a map-like structure of local environments to the GNC system, and the global position system (GPS) provides the position coordinates and the movement speed. [6]

There are five different categories into which the autonomous navigation problem of MASS can be divided. Global routing optimization, navigation decision-making, collision avoidance, path planning, and control. [7]

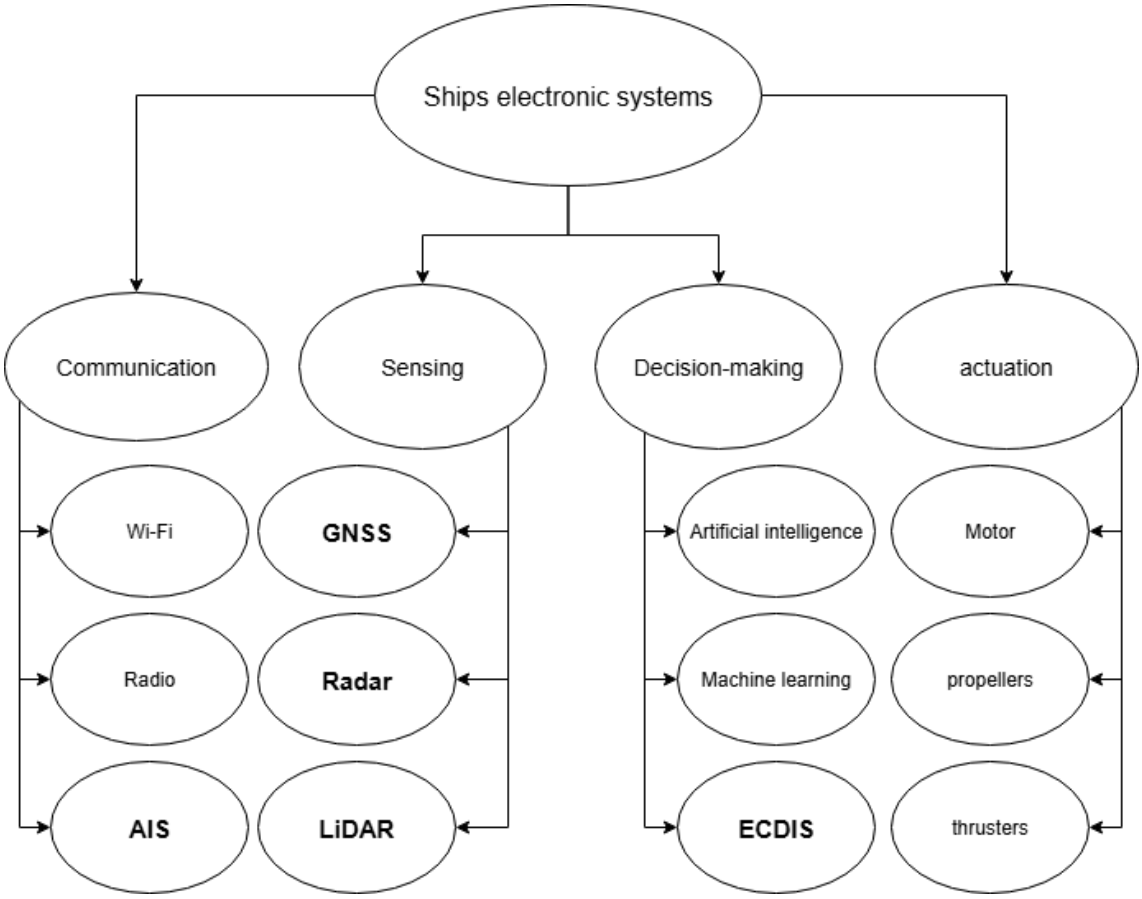

Figure 2.1: Electronic systems used in ships

2.2 Global navigation satellite system

The Global Navigation Satellite System (GNSS) is the most popular technology used to provide position and timing information. GNSS covers the whole world and provides positional information with great accuracy. The first GNSS system developed was the Global Positioning System (GPS). Russian global navigation satellite system (GLONASS) was also introduced around the same time. Major GNSS systems that have later come include Galileo and BeiDou. These are the four major GNSS systems that this thesis is going to examine further. There are also regional systems called Navigation with Indian Constellation (NavIC) developed by India and the Quasi-Zenith Satellite System (QZSS) developed by Japan. [8]

There are various signal components that are used in different GNSS constellations, including L1C, B1C, E5a, and so on [9]. These will be covered in more detail in their corresponding constellations. It is possible to use multiple of these constellations simultaneously to gain a more resilient signal. [10]

GNSS does not consist only of satellites in space; there are also ground stations that operate the satellites. These stations make sure that the satellites are synchronized to the coordinated universal time (UTC). They upload the data to the satellites and monitor the performance and status of the satellites. The third part of GNSS is the user device. The user device can also be called the GNSS receiver. It receives the signal and processes the signal. [11] An overview of the GNSS structure can be seen in Figure 2.2. The following subsections cover the four constellations in more detail.

2.2.1 GPS

GPS was developed by the US government and was operational in 1995. [8] Initially GPS consisted of 21 satellites with 3 spare satellites that orbit the Earth. Later, the number of satellites used has increased and the current number is 31 satellites. Satellites cover the world and provide position, navigation and timing (PNT) services for military and civilian use. The principle behind GPS positioning is to determine the distance between the satellite and the user's receiver. This is done with multiple satellites and then the data is integrated to get the receiver's position. At least 4 satellites are needed to get the three-dimensional position of the receiver. [12]

The current phase of GPS satellites is that of GPS III satellites. There are currently 7 GPS III satellites in the orbit. The first GPS III satellite was launched in 2018, and the 7th satellite was launched in December 2024. These GPS III satellites offer a civil signal L1C that is compatible with other GNSS systems. There are also GPS IIIF satellites, which are limited to military use. [13] This means that those

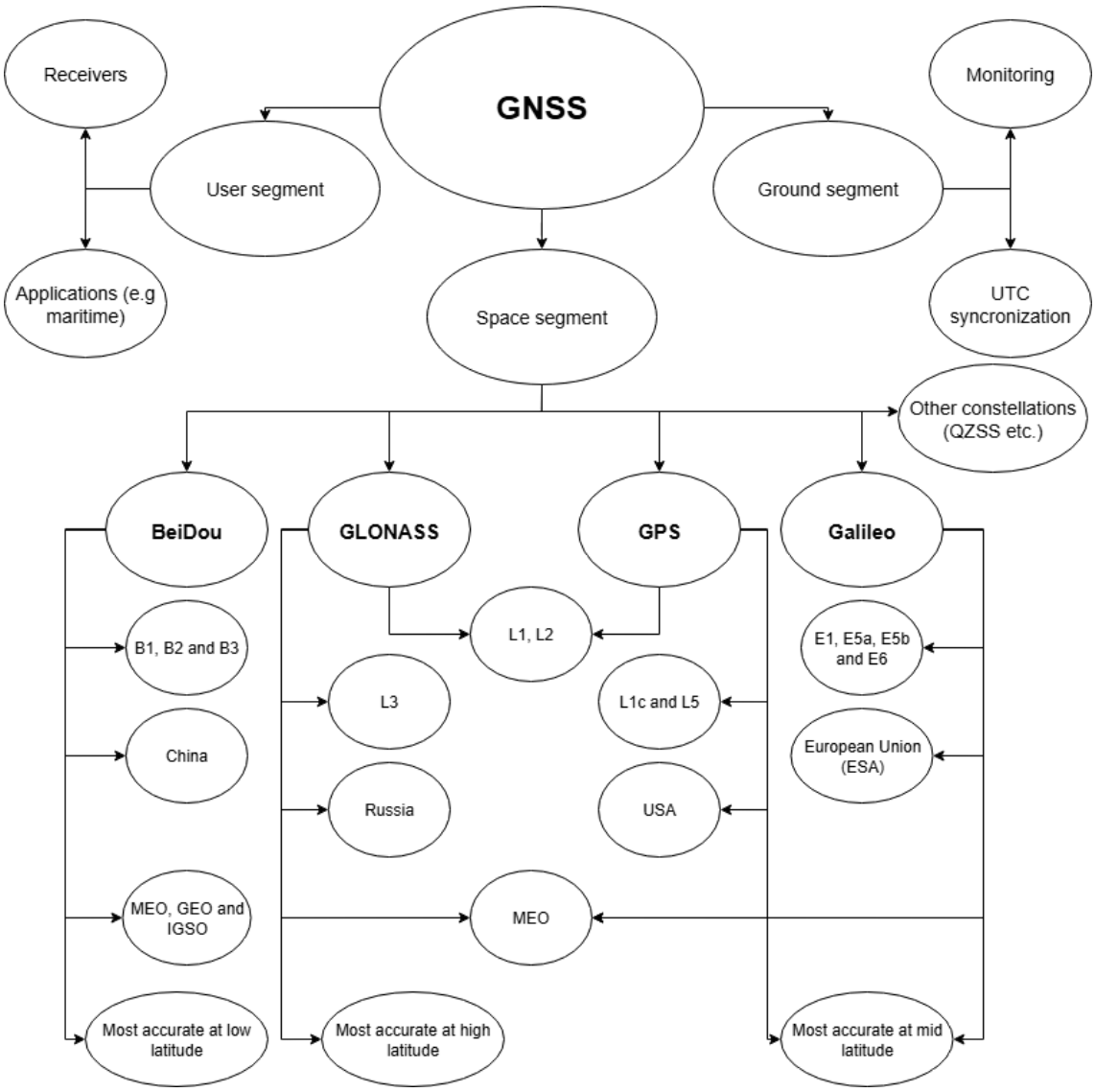

Figure 2.2: GNSS constellations differences

are out of scope for this thesis.

This critical part of navigation is threatened by multipath, jamming, and spoofing attacks. Spoofing attacks try to intentionally mislead navigation solutions by fabricating GPS signals. One way to do these attacks is to record the GPS signal and replay it after a set delay. This usually leads to the receiver producing the wrong position, time, and velocity solutions. The advanced spoofing attack, with enormous threat, called nulling, utilizes two signals, one spoofed signal to mislead the receiver, and another signal, which is the negative of the actual signal. This negative signal cancels out the actual signal leaving only the spoofed signal to the receiver. However, this method is extremely difficult to pull off as the carrier phase and amplitude need to be matched exactly right. [14]

2.2.2 Galileo

Galileo is the newest GNSS system that was launched in 2016 and was funded by the European Union. Galileo constellation has 24 satellites in orbit. Galileo satellites provide navigation signals in three different frequency bands. These frequencies provide access to positioning, ranging, and timing services to users. Galileo provides UTC time determination and single-frequency (SF) and dual-frequency (DF) positioning and ranging. Galileo uses four different carrier frequencies, which are E1 centered at 1575.42MHz, E5a centered at 1176.45MHz, E5b centered at 1207.14MHz and E6 centered at 1278.75MHz. The frequency usage modes for SF are E1, E5a, and E5b and DF uses E1, and either E5a or E5b. [15]

2.2.3 GLONASS

GLONASS has a higher inclination angle than the rest of the four major GNSS systems. GPS and BeiDou are at an angle of 55°, Galioleo is at 56°, while GLONASS is at 64.8°. This higher angle of inclination provides higher availability at a higher

latitude. The geographical location of Soviet Union/Russia is the key reason why GLONASS has chosen the higher inclination angle. GLONASS has better accuracy in positional data than GPS when operating in high-latitude locations. Then again, when the position is closer to the equator, the GPS performs better. In the low-latitude region GLONASS has the worst accuracy compared to high- and middle-latitude. [16]

When combining GPS and GLONASS, the accuracy in high latitude is even better than with only GLONASS or GPS. In middle-latitude, adding GLONASS to GPS does not provide any increase in accuracy. Although GLONASS performed the worst in the low latitude, adding it to the GPS improves the accuracy in the low latitude. GLONASS can work as a standalone solution when the operating environment is in high latitude, and GLONASS is a great addition to multi-GNSS solutions when operating in high- or low-latitude areas. [16]

2.2.4 BeiDou

Beidou satellite navigation system (BDS) provides global services, including PNT. BDS-3 constellation consists of 3 geostationary earth orbit (GEO) satellites, 3 inclined geosynchronous orbit (IGSO) satellites, and 24 medium earth orbit (MEO) satellites. The accuracy of single-point positioning is only at a meter level and cannot be used in devices that require high precision. [17]

BDS is operated by China and is determined to be compatible with other GNSS systems. BDS has more satellites on high orbits to provide better anti-shielding capabilities. This helps to increase performance in low-latitude areas. BDS also uses multifrequency signals to provide navigation signals. [18]

2.3 Radar

Radio detecting and ranging (RADAR) systems use electromagnetic waves to detect objects. The core principle behind radar is sending a signal towards the target and then receiving the signals reflected echo back. It is possible to analyze these reflected signals and determine several parameters of the target, including range, velocity, and orientation relative to the target, with various radar signal processing (RSP) techniques. [19]

The radar can be two-dimensional (2D) or three-dimensional (3D). 2D radar uses range, velocity, and azimuth to determine the position of the object, while the 3D radar also uses the height of the object. The capability of the radar to detect the object depends on the signal strength and noise. Noise is inevitable because of the thermal movement of the conduction electrons in the receiver. For the receiver to pick up the signal, the strength of the signal must be greater than the noise floor. [19]

There are seven components that are used in 2D radars. The transmitter is the component that generates high-power radio frequency (RF) pulses. The antenna is used to transfer the transmitter energy to signals in space. The receiver is used to receive the RF signals. The duplexer allows the antenna to switch between receiver and transmitter, enabling the use of a single antenna for both. The radar signal processor uses RSP techniques to process the signals. The display gives a graphic representation of the location of the object on the radar. The synchronizer is used to, for example, timing pulses that are necessary for the radar to operate. [19]

2.4 Automatic identification system

Automatic identification system (AIS) sends the ships static and kinematic data to other ships and shore-based facilities. This ship data includes the real-time location,

ship type, Maritime mobile service identity (MMSI), speed, etc. The data transmission frequency can vary from 2 seconds to 10 minutes. This frequency is based on the movement speed of the ship. AIS works best when there is no sudden acceleration/deceleration. [20] The range from which the AIS collects data from other ships is 20 nautical miles [21]. Terrestrial means and satellite base stations can also be used to transfer these AIS data across long distances. Both real-time and historical AIS data can be used in the early identification of collision risks and anomalous activities. [21] 31st of December 2004 was the day when all ships weighing 300 gross tons or more, used in international voyages, and ships weighing 500 gross tonnage or more, which do not engage in international voyages, were required to fit AIS abroad by IMO regulations. AIS must always be used, unless international agreements on navigational data protection allow it to be turned off. [22]

Compared to traditional maritime approaches, for example, radar and sonar, AIS has some strong points, including resilience against weather and sea conditions, it gives a great amount of information about the ship in almost real-time, and AIS has very long range. [21]

2.5 LiDAR

Light Detection And Ranging (LiDAR) scans its surrounding areas in 3D regardless of the lighting conditions. LiDAR sends laser pulses towards the area it is scanning, and if these lasers hit an object, some of the lasers are reflected back to the LiDAR sensors. Then, the time for the pulse to travel back to the sensor is measured, utilizing the constant speed of light. This time can then be used to determine how far the object is. These points of objects are then used in a 3D space to map the object and the surrounding world. [23]

There are three categories that LiDAR can be classified into: Mechanical LiDAR, scanning solid-state LiDAR, and flash LiDAR with non-scanning architecture. Me-

chanical LiDAR uses a rotating assembly to direct a laser beam across different angles. Mechanical LiDAR provides good quality measurements. Mechanical parts require maintenance, are vulnerable to shocks and vibrations, and the data collection speed is relatively slow. Scanning solid-state LiDAR uses different ways to remove the need for mechanical rotation. One way is to use electromechanical mirrors and lasers pointed at these mirrors. Then the mirror's tilt angle is adjusted with the difference between the input voltages. This is used to replace the rotational component. Another way is to use an optical phased array (OPA) that uses phase modulators to modulate the wave shapes similarly to a phased array radar. [23]

2.6 Electronic Chart Display and Information System

IMO defines the electronic chart display and information system (ECDIS) as a complex safety-relevant software-based system with multiple options for display and integration [24]. ECDIS is used in route planning and route monitoring [25]. IMO made changes to regulation V/19 in 2009, making ECDIS a mandatory part of new ships. This change came into effect on January 1, 2011. [24]

The Electronic Navigational Chart (ENC) is the database and contains all the necessary data for safe navigation. System Electronic Navigational Chart (SENC) is the manufacturer's internal ECDIS format of the database. This is the database that ECDIS accesses when it generates the display and other navigational functions. This is the same as an up-to-date paper chart. [25]

2.7 Inertial Measurement Unit

The objective of the Inertial Measurement Unit (IMU) is to measure the orientation of the object. This is done by measuring acceleration, rotation, and velocity. Other names for IMU are Inertial reference unit (IRU) and motion reference unit (MRU). The IMU uses an array of sensors to measure the acceleration and angular rate in the X, Y, and Z axes. The IMU utilizes the object's resistance for changing direction to determine the motion of the object. [26]

The IMU contains accelerometers and gyroscopes and sometimes magnetometers as the sensors. Accelerometers measure linear acceleration, and gyroscopes measure rotation. Magnetometers measure the strength and direction of the Earth's magnetic field to determine the direction. [26]

There are multiple different performance grades for IMU. These range from commercial use to strategic use. The bias instability is the main factor to determine the grade to which the IMU belongs. The bias instability tells how much the sensor output drifts during operation. The navigation grade IMU is the second highest grade after the strategic grade. The drift for navigation grade IMU ranges from 0.01° to 0.1° in an hour. [26]

The scale factor measures the error between the sensor output and the change in the measured input. If the vessel accelerates 19.61 m/s^2 and the scale factor is 0.1%, the sensor output might be 19.63 m/s^2. A smaller scale factor means less error. [26]

2.8 Classification Societies

Classification societies play a key role in the maritime field. Their role is to create standards for ships, classification of ships and offshore units, certify materials, components, and systems, and to create guidelines for ships. There are multiple classification societies working on creating the proper guidelines for the MASS. These

societies include Det Norske Veritas (DNV), Lloyd's Register (LR), American Bureau of Shipping (ABS), Nippon Kaiji Kyokai (ClassNK), Korean Register (KR), China Classification Society (CCS), Russian Maritime Register of Shipping (RS), and Bureau Veritas. These classification societies have the same objective and similar approaches to achieving them. This thesis examines three of these to see the current state of the classification societies regarding MASS. These three are DNV, LR and ABS.

IMO has not yet fully regulated autonomous shipping. The MASS code is expected to enter into force on January 1, 2032 [27]. Currently, it is up to the flag states to decide how they want to regulate autonomous shipping in their regions. DNV has published their first autonomous shipping guidelines in 2018 [28]. DNV has promised that their Autonomous and Remotely Operated Ships (AROS) class notations provide the same or better safety than conventional ships. Four key functions on which AROS is focused are navigation, engineering, operations, and safety. These functions have separate categories for the different MASS levels. [29]

LR noted that there are three challenges to the introduction of MASS. These are regulations, collaboration with industries and partnerships, and government funding. They also noted that technology is advancing faster than regulations. This rapid advancement makes it difficult for regulators to establish clear guidelines for safety and performance standards. LR states that the most important part is having flexibility and adaptability to keep up with evolving autonomous systems. The International Regulations for Preventing Collisions at Sea (COLREGs) are a vital part of safe navigation, but currently they assume that all ships are manned. LR also noted that the terminology and language used in COLREG is problematic in the MASS context. LR states that the use of regulatory sandboxes can help formalize the new regulations. By allowing the usage of MASS in the controlled area, the regulators can better understand the safety, infrastructure, and other relevant

factors. This can be then utilized to fix gaps and challenges in existing frameworks. [30]

LR states that unspecified performance could lead to major issues. They give an example where weather could affect object detection and lead to collision if the detection and classification of objects bigger than 5m within 2m, done in x seconds, is not proper. They also state that Conventional engineering design review, system testing and surveys are not good enough when autonomous systems are assessed. MASS has brought new challenges to regulation. Previously, it was quite straightforward to determine the precise requirements, for example, for the engine, the fatigue resistance, and the surface finish. Now, MASS software has introduced new variables. Decision-making algorithms can create unbounded behavior if they are not properly constrained. [31]

ABS has made its own framework, where there are set goals, functional requirements, verification of conformity, and foundational requirements. The goals are the objectives to be met. They can be divided into the goal and sub goals that are part of the goal that help to achieve the primary goal. This approach makes the framework more scalable. For autonomous ships, the goal is to design the functionality that will be constructed, operated, and maintained for its planned mission safely, reliably, and predictably. The functional requirements are the requirements that must be met to achieve the goal. for autonomous systems, these functions can be categorized to smart, semi-autonomous, and autonomous. Verification of conformity verifies that the set details of the function comply with the set goals and function requirements. Foundational requirements for multiple parts, such as quality, robustness, functionality, security, and integrity, to ensure the implementation of the required technologies for autonomous vessels. [32]

We can see that classification societies have similar ideas about how the regulations should be made with some minor differences. The main idea for all classification

societies is to have robust, secure, and safe frameworks for MASS.

2.9 Route Planning

Route planning is the step where all the data collected from the GNSS, AIS, LiDAR, radar, and ECDIS is taken into account. The planned route is then passed on to motion controls which cause the ship to move.

Route planning can be divided into global and local route planning. In Global route planning, the system uses prior information to avoid known obstacles such as islands. Local route planning is used for dynamic obstacles. The system plans the route in response based on the information gathered from the sensors. When global and local route planning are used in combination, it is called hybrid route planning. [33]

There are multiple different methods that can be implemented to perform route planning. One of the methods is the velocity obstacle (VO) method first proposed by Fiorini and Shiller in 1998 [34].

Historical data from AIS can be used in route planning because the general idea of route planning is to reduce the distance and increase the safety of the vessel. For the same reason, most ships have similar trajectories. [35]

There are three methods that can be used to extract maritime routes. Density analysis, cluster analysis, and Traffic-aware Realistic Automatic Design (TREAD). TREAD with AIS data can be used to classify and predict maritime traffic patterns. This can be used to detect anomalies in vessel operation patterns. By extracting patterns from maritime traffic networks, it is possible to create a method that creates lane boundaries, lane centerline, and junctions for the vessels. Then by using Kernel density estimation analysis (KDE) density analysis the route can be created. [36]

2.10 Berthing and Open sail

It is necessary to obtain accurate information on the position, speed, approach angle, and yaw rate of the ship when berthing. Most vessels rely on GNSS to determine their own position. Berthing requires centimeter precision on positioning, but GNSS is not capable of providing such an accurate location. There are two different ways that can be used to estimate the berthing state of the ship.

The first way is to use a shore-based system that measures the distance between the ship and the shore. This measures the berthing speed. One- and two-dimensional laser systems have difficulties in locating the ship, but three-dimensional laser systems can accurately capture the target ship and build the 3D surface geometry of the ship [37].

The other way is to use a ship-based system. LiDAR and ultrasonic sensors can be used to measure the distance between the ship and the shore. This method helps to correct for inaccuracies in maps and unmapped objects, such as moored vessels [38].

Even with these techniques, berthing is such a precise operation, with many challenges that remain unsolved. Currently, level 3 and level 4 MASS would require a crew to help with docking [33].

Marine traffic in the oceans near coastlines has predefined routes that the ships use to navigate, but in the open seas there are no defined routes. The density analysis is expected to be applicable to MASS, and it can be used to create maritime traffic routes on the ocean. [36]

3 Risk assessment methodologies

The research methods chosen for this thesis are a literature review and an expert interview. The risks are first identified from the literature. The identified risks are then assessed. Finally, the assessment is validated with an expert interview.

3.1 literature review

A literature review of technologies used in maritime navigation was conducted to identify the roles they play in navigation and to understand the risks and threats associated with these technologies. The identified risks and threats are then categorized to create the risk assessment.

Data for this thesis' literature review have been collected from the IMO's official website and the Web of Science. Artificial intelligence Keenious has been used to collect research articles to support this thesis.

Keenious uses a large language model to identify published articles that correspond to the user's query. It can retrieve related articles, even when they use different terminology to describe the same concept. This makes it an effective tool alongside keyword search. [39]

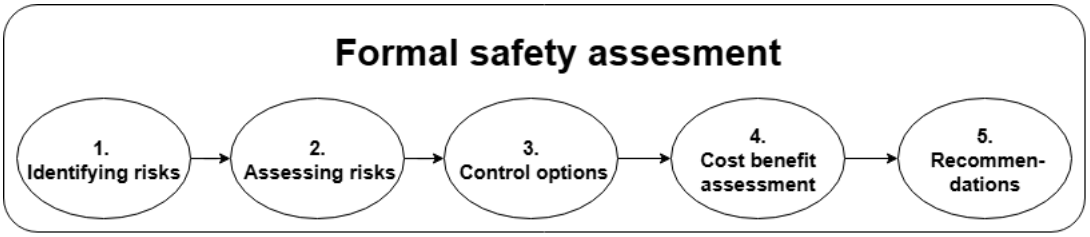

Figure 3.1: FSA steps

3.2 Risk assessment approach

There are multiple different methodologies that could be used to condone risk assessment. These methodologies vary from global standards to manage risks to field-specific, such as Hazard and Operability Study (HAZOP) which is used when dealing with e.g. chemicals. Some potential candidates to use include ISO 31000, which is an international standard that provides principles and guidelines for risk management [40], and NIST SP800-30, which focuses on providing guidance on risk assessment of IT systems [41]. Choosing the right methodology is crucial to the success of the assessment.

IMO recommends the use of formal safety assessment (FSA) to ensure that actions are taken before disasters occur [42]. This thesis will use FSA to conduct the risk assessment, and the main focus will be on the main risks that could cause total system failure.

FSA has five steps. The first step is to identify the risks and threats, with potential causes and outcomes. The second step is to assess these risks and threats. The third step is to create control options for these risks and threats so that they can be mitigated. The fourth step is to create a cost benefit assessment, where the controls cost effectiveness related to the realization of the risk is determined. The fifth and final step is to create recommendations for decision-making, for example what should be done.[42] These steps can also be seen in figure 3.1.

The risks will be categorized by their likelihood of happening and the impact if

it does happen. These metrics are then used together to form the final risk level metric. The scale will be in three steps with high, medium, and low. FSA uses three steps to risk acceptance: intolerable, As Low As Reasonably Practicable (ALARP), and negligible [43]. Intolerable risks are risks that must be fixed no matter the cost. Negligible risks do not need to be reduced. The ALARP category falls between these two, where something should be done to the risk, but simultaneously think how long the benefits are cost effective.

3.3 Interview

The validation of this risk assessment was carried out with expert interview. MASS is still in the early stages of development and there are no consistent regulations or certification frameworks for each MASS level. This limits the thesis, as there is no hard evidence to support the claims, except for opinions of experts. Maritime regulatory inertia slows the process, even if the technology is developed quickly.

Expert opinions were collected through an interview. This interview was done semi structured, where there were few set questions, and then the discussion about the risk assessment was free to go naturally. The expert is an academic researcher specializing in maritime autonomous surface ships and has a deep understanding of the cybersecurity risks and threats in this field. The expert has multiple publications in this field. The expert was chosen based on their knowledge of the topic.

The interview was a live video call. The entire interview was recorded, and the recording was used to ensure that the statements made by the expert were not changed in this thesis. The interview was around 30 minutes long. The communication before the interview was done by emails.

The aim was to have multiple experts to interview, but during the making of this thesis there were issues that caused the final number of successful interviews to be one. This is a clear limitation to the validation of the thesis. But should not

undermine the opinion of the one expert. The interview provided a new perspective on the thesis, providing insight that helped validate some of the claims. In addition, it highlighted some areas that could be more considered and confirmed that the selected technologies and risks are relevant.

There were a total of five different predetermined questions to ensure that the interview contains all the necessary information. These questions are as follows:

To your knowledge, what are the biggest risks/threats to GNSS/AIS/radar/LiDAR/ECDIS?

Does my assessment of the risks align with your expectations?

Is there some other technology that would be more important to consider than the ones chosen?

What do you believe is the next emerging threat to these technologies?

Is there in your opinion something critical that i omitted?

4 Risks

Risks are things that can cause a security event to have an unwanted impact on the object, and threats are actions, actors, or events that could cause something harmful. Essentially, risks are potential for loss and threats are a source of potential harm. To minimize these risks, they must first be identified.

After identifying the risks, it is important to perform the risk assessment to better understand how these risks compare with each other and which of them are the most crucial to mitigate.

4.1 Related work

The existing literature on MASS navigation often focuses on higher level and the sensors are just covered as part of situational awareness [44], [45].

There is a substantial body of research on the vulnerabilities of individual navigation sensors. GNSS availability has been extensively studied, including threats such as jamming and spoofing [46], [47], [48]. Limitations to radar performance in cluttered or adverse weather conditions are also highlighted [49]. AIS has been shown to be vulnerable to signal manipulation and reporting errors [50], [51]. LiDAR exhibits vulnerabilities both at the sensor level, such as saturation and replay attacks, and at the interface level, including tampering with point cloud data [52], [53]. ECDIS has also been identified to be vulnerable to attacks, such as the introduction of malware through the Internet [54]. Maritime grade IMU are well studied with respect

to sensor drift and bias instability [26]. These studies provide the foundation for sensor risks in this risk assessment.

A clear research gap emerges from this body of literature. There are only a few articles where the topic is the risks towards these sensors in the context of MASS. Reference [55] is one of few examples in which ECDIS, AIS and radar are taken into further inspection in the context of MASS safety.

4.2 Identifying risks and threats

The first step in the FSA is to identify risks and threats. In this step, potential causes and outcomes are also identified. The risks and threats are identified with the literature on the topics.

4.2.1 GNSS

GNSS will be one of the primary sources for navigational data for MASS. The risks and threats to GNSS are rising as there are more high-power transmitters, ultra-wideband radars, televisions, and personal electronic devices that can interfere with the GNSS signals. The more users there are in the same waveband, the more likely the appearance of interference is. Forecast and some surveillance services use the same waveband as GNSS and might unintentionally interfere with the navigation service. [46]

Malicious actors with deliberate jammer to GNSS signals are becoming more common. Personal privacy devices (PPD) are inexpensive and can work as jamming machines [48]. Denial of GNSS signals cripples the system as without proper data the system cannot perform in the intended way. Jamming the GNSS causes alarms and failures to other systems, for example, ECDIS [48].

Another threat to GNSS is the intentional false signals that try to trick the

system. These were previously thought to be unlikely, but there is evidence pointing towards this being a proper threat to GNSS. [46] This is called GNSS spoofing. The older signals used, such as L1, do not use any type of protection against jamming or spoofing. This makes the spoofing and jamming attack easy towards the older signals. The hardware needed to perform successful spoofing attacks is also minimal. [47] Commercial software-defined radios (SDR) can be used to spoof GNSS signals at a low cost. HackRF one and BladeRF are commonly used SDR's and they can be used to successfully spoof GPS [56] [57]. There is a suggestion that the quality of the spoofed signals in terms of strength and system geometry translates directly into the effectiveness of the spoof. The signal does not need to overpower the real signal to be effective. Even if the spoofed signal is 8.04 dB weaker than the real signal, the position estimation begins to have errors when the used system is GPS. a 4.52 dB weaker spoofed signal has managed to control the position over the real GPS signal. [47] With unencrypted GNSS signals, the attacker can gradually build the measurement errors in the receiver to avoid detection. After a while, the spoofing error is comparable to the expected drift errors. [58] When the errors are comparable, the attacker has successfully spoofed the system.

GNSS signals can be secured with security codes, but there is also a way to attack these signals. The attack is called the security code estimation and replay (SCER) attack. The idea behind this attack is to estimate the security code as close to the real one as possible in real-time for every targeted GNSS signal. Immediately after obtaining the estimate of the security chip, the estimate is injected into the signal replica generator, which contains spreading codes and carrier replicas. [59]

There are two types of SCER attacks, zero-latency SCER attacks and non-zero-latency SCER attacks. In zero-latency SCER attack, the attacker rebroadcasts the counterfeit signal which is initially exactly aligned with the authentic signal in the target's receiver. In non-zero-latency SCER attack, the counterfeit signal is

rebroadcast and arrives in a delay to the target receiver compared to the authentic signal. The delayed signal would be easy to detect as a spoofing attempt if the target had tracked the authentic signal before the attack. The strategy is to jam or block the authentic signal for a period of time to make the target uncertain of the timing. The jamming duration depends on the desired delay and, for low-cost temperature-compensated crystal oscillators, which are typical in commercial GNSS, the jamming or blocking should be 20 seconds to achieve successful attack. [59]

These attacks are more relevant to commercial GNSS [47]. There are methods to counteract jamming. GNSS used in military setting is more encrypted and has a higher tolerance for jamming and spoofing. These methods will be discussed in the mitigation chapter.

4.2.2 Radar

All Purpose Structured Eurocontrol Surveillance Information Exchange (ASTERIX) is a collection of standard protocols for exchanging radar information between systems. The Asterix CAT-240 is widely used as the network video standard by many radar manufacturers since 2009. CAT-240 contains a header and a video block. The Asterix protocol does not include encryption or authentication methods. [60] The key vulnerability in radar systems is that Asterix assumes that the navigation network and all subsystems are trusted [60]. This creates a large attack surface for the adversary.

It is possible to simply inject Asterix packets with a false echo into the target and manipulate the displayed image. This attack is easy to execute, and it is possible to gain significant results by disturbing radar systems. With more effort, it is possible to simply monitor the status of the ship and alter the data only when necessary to create the desired outcome, for example, harming the ship. If done correctly, the false packets do not seem anomalous during the attack. [60]

Like every sensor that receives any kind of signal, radars are vulnerable to jamming. Radar jamming uses equipment or materials to radiate, scatter, or absorb electromagnetic waves. These will disrupt or weaken the capability of the radar to detect and track targets. The key attributes that contribute to successful jamming are timing, jamming style, resource usage, and jamming waveforms. [61] People are constantly trying to improve the defensive capabilities of radars, and this also leads to attackers developing improved ways to jam the radar. To counteract jamming mitigation, they are researching ways to improve the jamming waveform [61].

Radar jamming can be categorized into two types based on its effect, barrage jamming, and deceptive jamming. Barrage jamming utilizes noise to overwhelm the target, and deceptive jamming confuses the real target echo by using jamming signals, this causes the radar to obtain false information. [61]

barrage jamming can be further divided into broadband jamming and directed jamming. In broadband jamming, the idea is to jam a wide range of frequencies simultaneously. Directed jamming, on the other hand, focuses on a narrow and targeted range of frequencies to jam and thus requires less total energy from the jammer to be effective. These jamming methods are simple to do. Frequency agility technologies make it more difficult to intervene with the radar signal using directed jamming, and broadband jamming requires more energy. This means that if the attacker has limited available energy for jamming, the effectiveness is limited. [61]

To counteract this frequency agility, comb spectrum jamming can be utilized. Comb spectrum jamming can target the frequency points used in the radar and frequency shift the jamming signal to work in them simultaneously. The limitation in practical applications for this is the reconnaissance for the baseband signal. If the baseband signal is chosen poorly, the effectiveness of this jamming could suffer greatly. [61]

4.2.3 AIS

Currently, AIS protocols do not use any authentication or encryption, making attacks possible. Attackers can use software defined radios (SDR) to produce fake AIS signals. The SDR does not need to be a high-end model, and attacks are possible with an SDR that costs less than $500. [50] Ray et al. did a risk assessment of AIS in 2016 and found around 350 different threat scenarios for AIS [51].

AIS is vulnerable to multiple different attacks. There are studies showing that it is possible to produce fake or spoofed ships visible to all AIS receivers, including commercial ones. The man overboard (MOB) is an alert system that transmits a distress AIS signal to a nearby vessel to inform that a human is in the water and needs rescue. It is possible to produce fake MOB alerts. This could lead to costly rescue operations of fake humans. [50] These operations cost time and money.

Creating fake ships allows the attacker to trigger the collision alerts, and this could lead to the target ship changing directions. This can be utilized to manipulate the target ship path. These collision alerts are triggered when closes point of approach (CPA) and time to closes point of approach (TCPA) values fall behind threshold. If the attacker creates thousands of fake collision alerts, it disrupts the service and creates the possibility that real alerts are missed. ShipPlotter software v12.5.4.6 can crash when it is exposed simultaneously to a large number of alerts. [50]

AIS can be jammed by sending enough AIS frames to the receivers on both channels. This has been tested in a lab environment and with two SDR they managed to use 96% capacity of one channel and 100% capacity of the other channel. They noted that this type of attack would be limited in vast seas. This can be used to perform Denial-of-Service (DoS) attacks. [50]

AIS transponders mainly rely on the MMSI number as a reference to the AIS message. It is possible to use tools to create multiple emitters with different messages

but the same MMSI number. This can create confusion in the receiving party as the ship type, location, or other AIS field changes. This type of attack is called a coordinated attack. Another vulnerability of AIS messages is that the message decoder does not check if the message is logical or technically correct. This means that the ship can move between messages even if the speed is zero. If the speed is zero on the messages, it will not trigger TCPA. [50]

4.2.4 LiDAR

The attacks towards LiDAR can be divided into two main categories, attacks to sensor level and attacks to interface level. The sensor level attacks include saturation attack, where the attacker floods the target with bright light, and the replay attacks, where the attacker captures and re-sends the LiDAR pulses. Sensor level attacks require deep knowledge of the target system, and attacks are nullified with preprocessing steps. To perform these attacks, the attacker must know the pulse sequence, the receiving angle, and the listening time intervals. The preprocessing steps could be, for example, correlation or random probing. [52] The attacker can also use reflective material to create false objects or light-absorbing materials to make the object invisible to the LiDAR. LiDAR sensors can be spoofed by using lasers. These lasers can be used to either make an object appear or disappear from the sensor. These lasers are emitted on pulses to mimic different positions. [53]

Interface-level attacks are also transmission-channel attacks. If the attacker can manage to get access to the network interfaces, he can tamper with the point-cloud data and either remove target objects or create false objects. [52] These attacks could lead to a collision if the object is removed. Creating a false object can be used to guide the ship to a path more suitable for the attacker or to stop the ship.

4.2.5 ECDIS

ECDIS has multiple different threats. These threats include Malware injection through the internet or the intranet, introduction of malware through removable media, intrusion through remote access, Vulnerabilities of standard components of IT systems and other control systems connected to the internet, and human error or sabotage. A study has shown that the importance of these threats is in the same order as listed previously. The most important threat is malware injections via the internet, and the least important being human error or sabotage. This is based on the opinions of five experts in the field. [54]

There are cases where the ECDIS uses older operating systems that are more vulnerable to attacks. In 2019 some ECDIS operated on windows 7 [62], which was the last year it was supported. meaning that it needs to be updated soon. The same system ran an older Apache web server that had been obsolete since 2017 [62]. This implies that keeping the systems up-to-date might be lacking in this particular ECDIS and it might have become outdated.

These threats can cause the system to become unavailable or corrupted, the files in ECDIS being deleted, other devices connected to ECDIS such as GPS or AIS being hijacked, or infrastructure damage. [54]

4.2.6 IMU

One possible attack towards IMU is Intentional Electromagnetic Interference (IEMI). By generating a strong electromagnetic pulse, it is possible to disrupt the IMU. [63] However, The probability that this will impact large maritime vessels is low. The thesis assumes that the vessels follow the proper regulations and guidelines [64], which would mean that the vessel should be shielded against this kind of attack.

4.3 Risk assessment

We have identified multiple risks and threats to the technologies used in navigation. Most of the risks and threats assessed assume that there is an attacker who deliberately targets the ship and tries to achieve a goal with the attack, such as altering the path of the ship or stopping the ship. Piracy has been on the rise and in the first half of 2025 there have been 50% more reported attacks than in the first half of 2024 [65]. In this period, there have been a total of 90 attacks and armed robberies on ships and it is the highest number since 2020 [65]. This means that there are still people around who are willing to exploit any vulnerabilities in ships and use all available options in attacks. The geopolitical environment can also impact maritime safety, as nation-level actors may exploit vulnerabilities in ships during times of conflict.

These risks already exist on current operational ships, but the risk tolerance is higher as there are still humans onboard the ship that can intervene if they notice that the systems are having issues. It is possible for a human to check with their own eyes if there is something in front of the ship that requires the ship to suddenly change course. When the topic is MASS levels 3 and 4 there are no humans onboard the ship and the decision-making is done with the data provided to the system. If these data are compromised, then it is game over.

Table 4.1: Risk assessment table

System	Threat	Vulnerability	Impact	Likelihood	Risk Level
GNSS	Interference from forecast and other surveillance services	GNSS signals are weak near the Earth's surface	3	1	3

GNSS	Jamming	GNSS signals are weak near the Earth's surface and can be overwhelmed with noise	3	4	12
GNSS	Spoofing	Unencrypted communication on civilian channels	3	4	12
IMU	IEMI	IMU contains sensitive sensors that can be influenced with strong electromagnetic pulse	1	4	4
Radar	Packet injection	ASTERIX assumes all networks are trusted.	3	4	12
Radar	Jamming	Predictable waveform, frequency or timing allows the attacker to transmit noise or fake echoes.	3	4	12
AIS	Spoofing	No authentication or encryption	3	4	12
AIS	Jamming	Limited capacity of two channels	3	4	12
AIS	Coordinated attack	Relying mainly to MMSI as reference	4	4	16

LiDAR	Spoofing	Simple pulse sequences allow manipulation	3	4	12
ECDIS	Malware injection	Unsecured network interfaces, outdated or unpatched software	3	3	9
ECDIS	Malware through removable media	Lack of media control and malware scanning	3	3	9
ECDIS	Intrusion via remote access	weak authentication, outdated components or poor segmentation	3	4	12
ECDIS	Internet connected systems vulnerabilities	Use of obsolete OS or software without security patches	3	4	12
ECDIS	Sabotage	insider threat or poor access control	4	4	16
All	Combination attack	Multiple weak systems can be targeted simultaneously	5	5	25

In table 4.1 these risks and threats identified in Section 4.1 are assessed based on the likelihood and possible impact of the risk if it is realized. Impact and likelihood are rated from 1-5, where 5 is the highest, and the risk level is calculated by multiplying impact by likelihood, ranging between 1 and 25. This risk level range from 1 to 25 can then be divided into three parts to give numerical values to the FSA's risk acceptance steps. 1 to 8 is negligible, 9 to 16 is ALARP, and 17 to 25 is intolerable.

The value 1 can be interpreted as a minor inconvenience and is unlikely to occur. The value 5 can be interpreted as extremely catastrophic and is most likely to occur.

From the literature, we have identified that AIS, GNSS, Radar, and LiDAR are all vulnerable to spoofing and jamming. If only one of these is under attack and the rest of them are left alone, the attack would most likely fail. The real risk comes when a possible attacker targets all systems simultaneously. The literature has shown that jamming and spoofing of these systems is relatively easy and inexpensive enough, meaning that it would not be a big step to simultaneously target all of the systems compared to just targeting one of the systems. It does not matter how the decision-making of the ship is implemented if all the navigational data can be spoofed. If all navigational data are compromised, then it is impossible to make the "right" decision, since the premise is that you only have false information. On their own, these spoofing and jamming risks of the systems could be categorized into the ALARP category, but if multiple of these possibilities exist simultaneously, then the risk category for them becomes intolerable.

These technologies have advanced greatly from the early stages, and although the risks of accidental interference from forecast and other devices still exist, the likelihood of it affecting the systems is extremely low. It is safe to categorize these accidental interferences into the negligible category, as there is no further need to reduce them. Recognizing that there are minimal chances of these interferences is enough.

The lack of clear global guidelines to follow enhances all existing risks, as everyone needs to think about all the possible scenarios themselves, and they cannot yet rely on the governing bodies. IMO and classification societies are working to resolve this issue as discussed in chapter 2.8 but before the complete mass code, even classification societies are left without the complete recommendations on how to implement everything in their own area.

Berthing only leads to the need for even more precise sensors. The risk of collision is higher in crowded areas and when moving right next to other infrastructure. This leads to a situation where even one wrong decision could lead to a major incident. If the system is compromised for even a short period of time, the result could be catastrophic. In busy harbors, there are also more nearby transmitters from the harbor and possible other ships. This increases the risk of jamming the systems. In the open sea, there is less traffic in close proximity to the ship, which means that there is less accidental interference and more room for errors.

This assessment has been discussed with maritime expert with experience in academic research of the topic. The expert was mostly in agreement with the assessment. The most notable disagreement is about the importance of GNSS for autonomous ships. Other sensors, such as IMU can compensate for GNSS strongly and lower the importance of GNSS.

This thesis omits cameras from the assessment. The interview revealed that cameras are also important for situational awareness and including them would increase the realism of the attack scenario.

Based on the interview, quantum computing and AI are the two major changes in the field that will cause new emerging threats. They can also be utilized to mitigation these risks and threats in the future.

5 Mitigation

Mitigating set risks is not as straightforward as just identifying all risks and then creating control options to remove these risks. There could be multiple control options for the same risk and some of the control options could completely remove the risk, while others make it less probable.

The cost of mitigation methods differs, and the possible outcomes of risks also vary. From a business perspective, the most cost-effective solution is the best. Sometimes, it might be better to let the incident occur rather than mitigate it if the mitigation cost is significantly higher than the cost of damage that the incident might cause. This is where the cost benefit assessment comes into play, to identify when the risks are worth mitigating. After exploring all options, the last part is finally to give recommendations on the best actions to take to ensure the safety of the ships and minimize the risk.

5.1 Control options

Control options are the key to mitigating the risks. The authorities that decide how to mitigate the risks cannot decide what to do if there are no options given for them. Different technologies require different solutions.

5.1.1 GNSS

Many of the GNSS threat countermeasures can be divided into four categories [66]. These categories are encryption mechanisms, Codeless-cross-correlation measures, signal statistic analyzing methods, and antenna based.

Encryption mechanisms are based on algorithms to restrict access to the signal. These solutions are often expensive and are used only in military communications. Galileo has made Open Service Navigation Message Authentication (OSNMA) operational on 24th of July 2025. This allows authorized user devices to interpret encrypted signals [11]. ONSMA can be used free of charge for all Galileo users [67]. This will increase position accuracy and signal robustness [11].

In codeless-cross-correlation the idea is to use two receivers to receive the GNSS signal, if the two received signals are noticeably different, it is highly likely that the signal has been spoofed. This idea has been extended to a version where the cross-check receivers are not next to each other and they send snippets of the received signal to each other, then the other receiver can decide if the signal is like the one it received or not. To mitigate malicious cross-check receivers, they have also introduced delay in operation. Third-party servers can also be utilized in this process. [11]

Performing statistical tests on signals features, including automatic gain control (AGC), clock error, signal quality, signal power, propagation delay, and angle of arrival, is called signal statistic analysis. Spoofing can be detected by using structural power analysis. After the signal has passed through the structural power analysis unit, spoofing can be detected by evaluating correlation peaks using the cross-ambiguity function or if the number of correlation peaks is abnormal. The Neyman Pearson (NP) detection theory can be used in signal quality monitoring (SQM). Spoofed GNSS signals can be detected with this method by comparing one or more metrics against the threshold. The delta test metric and the ratio test met-

ric are two metrics that are widely used in the literature. Using multiple metrics improves the detection of spoofing compared to just using one. [11]

Antenna based methods utilize multiple GNSS antennas to operate. Multiple antennas improve the estimation of the direction of arrival (DoA) of possible spoofing signals. The spatial features of these multiple antennas can be manipulated to mitigate spoofing from the perspective of an electromagnetic signal. When the DoA of the spoofing signal is determined, it can be mitigated with null signals. [11] These synthetic null signals create a blind spot for the receiver from the direction of the spoof signal; thus, the spoofed signals are suppressed and mitigated. These methods have shown promising results, but assume that the spoofing signals come only from the same direction [11].

The Air Force Research Lab (AFRL) has developed chip-message robust authentication (Chimera) signal enhancement for GPS L1C signals. This enhancement is designed to counter possible spoofing attacks. The chimera is based on the authentication method [68] first proposed by Logan Scott in 2003. The testing of chimera GPS authentication service for civilian use began in 2023. The idea is to give encrypted markers to the L1C spreading code in the pilot channel. It is not possible to predict the markers and can be verified using either a digital signature or marker keys that can be provided with short latency. Receivers with access only to L1C can receive these keys every 3 minutes, and users with out-of-band access, such as a secure internet connection, can receive them once every 1.5 or 6 seconds. This duration between the authentications is called a chimera epoch. [58]

However, when the GPS receiver is on a moving target, such as a ship, the authentication speed is not enough. Authentication greatly increases position error. [58] Without authentication the GPS uses the 20 Hz update rate, with position errors of approximately 1.5 m, while the GPS/inertia measurement unit filter that uses chimera authentication increases this position error to 10 m in navigation grade

receivers and 300 m in tactical grade receivers [69]. When designing a filter that uses chimera enhancement, the two key objectives that collide are security and real-time navigation performance. [58]

One proposed filter claims that it found the balance between security and real-time navigation performance. They validated it using a ground vehicle model. In their test, they assumed that the attacker has full knowledge of the state of the vehicle. This GPS spoofing-resilient filter framework should provide secure state estimate between chimera authentication times. it uses self-contained sensors to determine how much trust it should place to the unauthenticated signals in real-time using M-estimation based weighting scheme. It achieved a lower overall position error than filters that switched away from GPS when they detected spoofing. [58]

To detect spoofing in the cryptographic GNSS signal, a simple way is to look at the correlation power. When the signal is spoofed, there is a drop in correlation power. The goal of anti-spoofing with cryptography should not be protection at all costs but to make it difficult. [59]

If the attacker uses the common over-the-air, unobstructed, low-power, non-nulling attack method, the defender has an advantage when detecting spoofing attempts using SCER [59]. By making sure that the attacker does not gain physical access to the receiver mitigates most of the ways to make the spoofing attack successful. The attacker could try to block the targets antenna with material that blocks RF signals, or the attacker could try to inject the counterfeit signal directly into the targets RF input and completely bypass the antenna [59]. Without physical access, these methods are not viable. The attacker can still use a high power transmitter to eliminate the authentic signal or transmit a signal that nullifies the authentic signal [59].

High-rate security codes have shorter intervals for detection tests and they strictly limit the attackers ability to use delayed security code estimation, as the estimates

cannot exceed the interval. However, low-rate security codes are great against SCER attacks. Low-rate security codes perform extremely well against zero-delay SCER attacks, and they are also strong against non-zero-delay SCER attacks. [59]

Jamming was identified as one of the biggest threats to GNSS in chapter 4. There are three solution groups that can be used to mitigate GNSS jamming. The first being the possibility to handle jamming inside the GNSS receiver, for example, with filtering. The second is to use alternative terrestrial radio navigation systems as a backup. However, currently there are no backups available in the US or Europe as LORAN-C was decommissioned. The R-mode is currently being developed for backup. The third option is to combine the GNSS receiver with a multi-sensor fusion scheme. [48]

Using receivers that support multi-constellation and multi-signal GNSS are less prone to jamming than those that support only one constellation. Different constellations operate at different frequencies so that to jam the multi-constellation receiver, the attacker needs to jam a wider range of frequencies [48]. The broader the frequency spectrum, the more resources the adversary needs to successfully jam the system.

5.1.2 Radar

There are many different ideas on different ways to mitigate the threats to false alarms caused by sea cluttering. The increased signal-to-noise ratio is the key metric of successful suppression of sea clutter [49]. The suppression can happen in the time domain, where the radar signal is trusted in some instance of time and not trusted in another instance of time. It can also happen in the frequency domain, where the signals are filtered usually with finite impulse response (FIR) or infinite impulse response (IIR) filters. The third option is the space domain, where the adjacent distance units are used to estimate the sea clutter. It can also be done in the

polarization domain, where the polarization difference characteristics between the targets and the sea clutter is used for mitigation. The final option is the joint domain, where multiple of these are used to reduce the limitations of the methods [49].

Another method of increasing the SNR and the detection capabilities of the radar is to enhance the target echo. These improvements can be made in the same domains as sea clutter mitigation. These methods are usually limited to theory, but combining them with sea clutter suppression can efficiently improve SNR in radars. [49]

When mitigating the possible jamming attempts towards radar systems, the interaction between the system and the jammer can be seen as two player zero sum game. In this game, the objective is to maximize your own gain while minimizing the gains of the other party. The scale of the environments is usually large and continuous learning steps are required to complement the gaming theory. [70]

Reinforced learning algorithms can be used to dynamically optimize anti-jamming strategies and help with the difficulties brought by diverse jamming signals. Reinforced learning algorithms typically provide effective solutions to low-dimensional decision-making problems using Q-learning, but when the scale grows, the Q-value tables grow exponentially, leading to slow computational speed and greatly increased costs. [70]

The deep Q-network (DQN) that uses neural networks outperforms Q-learning with a noticeable difference in complex jamming environments. As evaluation and selection are performed on the same network, the action values are often overestimated by the DQN. This causes local optima and convergence difficulties. To mitigate overestimation, the double deep Q-network (DDQN) can be used. DDQN uses separate evaluation and target networks. DDQN also has performance challenges in highly complex jamming environments. The more optimized version of

DDQN is dueling double deep Q-network, which expresses the Q-value as the sum of a state-value function and an action advantage term, allowing for more precise and frequent updates to the state-value. [70]

There are three main focus areas in radar anti-jamming decision-making methods: anti-jamming strategy optimization, anti-jamming waveform strategy optimization, and frequency selection strategy optimization. Dueling double deep Q-networks show promise in both anti-jamming strategies [71] and anti-jamming waveform strategies [72].

5.1.3 AIS

AIS is vulnerable to multiple different attacks and mitigating all of them is no simple task. One proposed method is to check for the integrity of the AIS signals. False AIS messages can be checked both at the physical and logical levels. The physical level focuses on the signals transmitted, and the logical level focuses on the information in the messages. [51]

The falsification of the signal can be identified in the physical level by performing signal analysis. The signals destination, masking or disappearance can be used to determine if the signal is false. The signal can be characterized, which helps to identify the ships. Still, this characterization cannot fully guaranty the identity of the ship, but it helps to notice inconsistent values. On the logical level, the identification of abnormal messages can be done with data mining. It is possible to identify MMSI numbers that do not exist. The integrity of the message can be verified by comparing the fields of the message with other fields of the same message, analyzing the fields individually, or comparing it to different messages. [51]

There are proposals to implement AIS authentication to improve security. An idea is to use asymmetric cryptography to implement digital signatures. The owner of public keys cannot be verified solely by digital signatures; a third-party certifi-

cation authority (CA) should be used. This way a digital certificate can be implemented to AIS and when it is combined with mix-zone theory the vessels privacy is also protected. The mix-zone theory uses pseudonyms that vessels can use in set areas to hide the location of the signal sender. [73]

Another proposed authentication framework is called auth-AIS. Auth-AIS claims to be a secure, flexible, standard-compliant, and backward-compatible authentication framework. Auth-AIS is a software update to existing AIS systems and does not require hardware updates to work on current AIS systems. It uses message type 8, which can be used in any application running on top of AIS. The authentication information is sent in the payload of the message, and the messages can be broadcast with a specific Function ID. Auth-AIS uses trusted third-party authority to share keys. Timed Efficient Stream Loss-tolerant Authentication (TESLA) would be integrated into AIS communication. It also utilizes bloom filters to perform membership queries on data sets. The key is that the trusted third party shares the transmission, and the precise timing is hidden. In this way, the attacker is unlikely to find the exact timing of the transmissions and the other ships will not authenticate the false transmissions. [74]

5.1.4 LiDAR

LiDAR can be configured to mitigate the risks of being affected by sensor attacks. These configurations include the usage of different wavelengths for lasers and different time intervals for transmitting. These configurations are cost-effective and easy to implement. If these methods are applied, the attacker needs to scan multiple wavelengths, which reduce the success rate of the attack, or use multiple transceivers, which increases the cost of the attacks significantly. The mitigation method for changing the intervals is random probing. In random probing, the proper measure is to pseudo-randomly skip pulses. [53]

Physical properties can be used to detect forged objects. There is a method called oCclusion-Aware hieRarchy anomaLy detectiOn (CARLO). It can be used to defend spoofing attacks by ignoring occlusion patterns as invariant physical features. CARLO uses the free space in the detected bounding boxes to determine if the object is real or fake. CARLO performs poorly on small objects, but this should not be an issue in large cargo ships. Fake shadow detection and azimuth-based detection can be used to prevent physical removal attacks. Fake shadow detecting takes a long time to compute. This makes it unsuitable for real-time tasks. Azimuth-based detection identifies the removed objects by finding disparities in point cloud. [53]

Another way to mitigate spoofing attacks is to check for the consistency of the frames. If there are inconsistencies in the point cloud between frames, the anomalies can be detected. Inconsistencies occur between expected and observed frames. [53] There are multiple ways this can be done. One proposed method is to use the 3D Temporal Consistency check (3D-TC2) which verifies object detection with spatiotemporal inconsistency [75]. Another suggested method for this is Anomaly Detection based on Point-level Temporal consistency (ADoPT), which detects anomalies in consecutive frames [76].

There are also suggestions to use multiple sensors to combat these attacks. These sensors could be multiple LiDARs or other sensors, for example GNSS. The problem with many of these solutions is that they assume that only one of the sensors is attacked at the time and they do not consider the possibility of coordinated attack towards multiple sensors simultaneously. [53] There are some proposals to mitigate these attacks towards multiple sensors. One example was to use multi-sensor fusion in this case against camera and LiDAR attack. The method utilizes input transformation and data augmentation [77].

AS all the communication data are unencrypted the integrity of the data can be compromised. One idea is to use watermarks, as weak encryption methods might

not be sufficient on their own. The recommended way is to use watermarks and encryption in combination [53].

5.1.5 ECDIS

To counteract malware injection through the Internet, ECDIS should have up-to-date virus protection and scanning software. To mitigate the risk of malware through removable media, the most effective method is to secure the USB-ports. The best option to prevent intrusion through remote access is to use whitelisting of systems previously authorized for remote connection and to use a proper VPN with encryption methods. To mitigate vulnerabilities of standard components of IT systems and other control systems connected to the internet is to manage updates.The best method to mitigate human error is training. [54]

The biggest consequence from attacks towards ECDIS is that the system becomes unavailable. To mitigate the risk that this happens, there are several possible methods. The most effective way to mitigate this is to use network segregation. The next best options are collecting network traffic information and machine-readable reporting of current security settings. [54]

5.1.6 IMU

Calibration is a crucial part of error avoidance. With proper calibration, the IMU avoids sensor bias, scale factor stability, cross-axis sensitivity, and misalignment of sensor axis. This calibration should happen before the IMU leaves the factory. They also check compliance with relevant industry standards. [26]

The mitigation to GNSS threats can be implied to IMU also as they are closely related and IEMI attacks are already mitigated in the assumed regulation following system.

5.2 Cost benefit assessment

The first thing to consider when assessing cost and benefits is to give a value to the possible effects. It is important to decide how the value is measured. The simple answer is to value them in money. Loss of revenue, repair cost of damaged ships and missing shipments are easy to calculate, but the tricky part comes when human lives are involved. How valuable human life is is a deeply philosophical question. One way to measure this is to check how much insurance companies are willing to compensate for life insurance. In Finland, the usual highest compensation is 500 000€ [78][79]. But then there come reputation risks for the company accepting a risk where human lives might be lost to save a little bit of money.

The main objective of mitigation is to make possible risks and threats unlikely to occur. The complete removal of risks is usually not cost effective, and most of the time the benefit is little compared to reasonable mitigation. The potential cost of damage that could be caused by identified risks is high. This means that costly mitigation's could still offer benefits compared to just allowing the risks to happen. In the end, it is up to the parties responsible for the risks to decide which mitigation methods they use, but it is highly recommended that proper mitigation be used, even if they are expensive.

5.3 Recommendations

The author of this thesis recommends that we research methods to make sensors have at least some security measures such as encrypted communication to mitigate the easiest to implement attack before even trying to make fully autonomous ships with valuable cargo. The increase in pirates, discussed in chapter 4, means that people will exploit the systems if there are possibilities. This does not mean that we should aim to solve spoofing or jamming completely, but rather to reach the

ALARP category preferably on every identified risk before the MASS ships set sail.

Implementing robust navigation systems that consider all the data from different systems makes it more difficult to make a successful attack. By merging information from different sensors and positioning systems , the system can identify inconsistencies and reduce the reliance on any single data stream that could be compromised. This would increase the complexity of executing a successful attack as the attacker would need to manipulate multiple systems simultaneously. This would also make it more expensive for the attacker to achieve the desired result and will most likely eliminate some attackers.

The decision making system must be designed so that it can work even under attack and must know how to handle spoofed navigational data and reliably operate. This would require built-in resilience measures, such as data validation, sensor redundancy, and fault-tolerant algorithms. These would allow the system to assess the reliability of the incoming information. Decision making was not the focus of this thesis, but it is one method to reduce the risks identified in this thesis if it is done properly.

Higher autonomy levels of the MASS ship mean that the decision making systems have less human interaction. In MASS level 4 there are no human interactions and the ship is fully autonomous. The importance of robust sensors is the highest in this level, as the system relies heavily on the available sensor data. At this level, failure or manipulation of sensor inputs can have a significant impact on system performance and safety. This makes sensor resilience a critical requirement for fully autonomous operation.

The author recommends having wide sensor diversity in the MASS ships to ensure that if some of the sensors are compromised, the system can still operate with the functioning sensors. These sensors could be independent. Sensor diversity reduces dependence on any single sensing modality and enables cross-checking of data to

detect faults or malicious interference. This leads to a situation where the vessel can maintain situational awareness and safe operation using the remaining reliable sensors. This increases robustness in both adverse and hostile conditions.

Implementing real-time integrity monitoring could help detect spoofing, jamming, and abnormal behavior of sensors. If this integrity cannot be ensured, there should be some automatically triggered mode that prevents autonomous decision making. The navigation authority should then be transferred to the remote operator or to the crew if there is onboard crew.

Another recommendation is to include a radio frequency interference detection mechanism, which could identify deliberate manipulation of the input of navigation sensors. Characteristics associated with jamming or spoofing, such as unexpected signal strength, timing inconsistencies, or abnormal frequency patterns, can be identified. Early detection would allow the system to trigger alerts and switch to an alternative navigation system.

Lastly, regular testing and training scenarios where the sensors are compromised are recommended. These scenarios should validate system performance and train the remote operator to be ready to prevent incidents in unexpected scenarios.

Implementing sensor diversity, integrity monitoring, and human intervention mechanisms can reduce the risks of navigation sensors to the ALARP level. This would be the best case scenario as complete prevention of these risks is not feasible.

6 Conclusion

This thesis assessed the risks and threats in key technologies used in MASS. These technologies were as follows: GNSS, AIS, radar, LiDAR, ECDIS and IMU.

The research methods chosen for this thesis were a literature review and an expert interview. The literature review was performed by searching the Web of Science and utilizing the AI keenious. From the literature review, a synthesis of key risk identification and mitigation solutions was performed for these risk. This was then validated through an expert interview, which provided both confirmation that most claims were accurate and noting that certain elements were ranked incorrectly, most notably the role of GNSS, which is not as important as stated in the thesis. The interview was conducted as a 30 minute online video call.

Three research questions were used to investigate these risks. Research Question 1: What are the key risks and threats to the navigation systems of maritime autonomous surface ships? This question was answered in Chapter 4 where risks were first identified from the literature and after the assessment the findings were validated with the expert interview. The key risks and threats found in the assessment were jamming and spoofing of unencrypted navigation data through different technologies.

Research Question 2: What emerging cyber security threats are likely to impact the navigational systems of maritime autonomous surface ships in the coming years? This question was also answered in Chapter 4. Quantum computing and Artificial

Intelligence are the two factors that most likely impact the creation of new emerging threats in the coming years. The interview validated this.

Research Question 3: How can we mitigate these risks and threats? The final question was answered in chapter 5, which discussed mitigation solutions of the identified risks. These solutions were identified from the literature. Mitigation strategies included encryption and filtering to counter these risks.

In conclusion, there are exploitable vulnerabilities that can be used to completely disable navigation operations. The global guidelines are not yet fully ready, which enhances existing risks.

Several limitations affect the study. First, there is no hard evidence to support the claims except for the opinions of an expert. There was only one interview with a single expert. Multiple interviews would have made the claims stronger. The literature focuses almost exclusively on civilian technology and often just mentions that military technology is more secure. Finally, the scope focuses only on the six technologies and omits the risks that could be caused by other factors.

This thesis contributes to the cyber security body of maritime autonomous surface ships, which is in a relatively early stage. The systematic identification, contextualization, and mitigation proposition provides a structured overview of the threat.

Future research could focus either on how quantum computing could change everything or on how AI creates new emerging threats and possibilities for the attacker and how AI could enhance mitigation. The experts interviewed support the claim that quantum computing and AI are emerging threats that are important research topics.

References

[1] European Maritime Safety Agency (EMSA), *Maritime autonomous surface ships (MASS)*, Online, Accessed: Aug. 29, 2025., 2025. [Online]. Available: https://www.emsa.europa.eu/mass.html.

[2] K. Matikka, *Evolution of autonomous maritime operations driven by automation technology and digitalisation*, Online, Accessed: Sep. 28, 2025., 2021. [Online]. Available: https://www.elomatic.com/evolution-of-autonomous-maritime-operations-driven-by-automation-technology-and-digitalisation/.

[3] United Nations Conference on Trade and Development (UNCTAD), *Shipping data: UNCTAD releases new seaborne trade statistics*, Online, Accessed: Jul. 17, 2025., Apr. 2025. [Online]. Available: https://unctad.org/news/shipping-data-unctad-releases-new-seaborne-trade-statistics.

[4] European Maritime Safety Agency, *EMSA facts and figures 2024*, Online, Accessed: Jul. 17, 2025, 2025. [Online]. Available: https://www.emsa.europa.eu/publications/item/5484-emsa-facts-figures-2024.html.

[5] International Maritime Rescue Federation. "Maritime Autonomous Surface Ships (MASS) and SAR". Accessed: Feb. 4, 2025. (2024), [Online]. Available: https://www.international-maritime-rescue.org/news/maritime-autonomous-surface-ships-mass-and-sar.

[6] Z. Dong, J. Liu, C. Li, and S. Li, "Classification, design, and challenges of unmanned ships in marine transportation", in *2021 6th International Conference on Transportation Information and Safety (ICTIS)*, Wuhan, China, 2021, pp. 985–992. DOI: 10.1109/ICTIS54573.2021.9798471.

[7] C. Wang, X. Zhang, and L. Wang, "Navigation situation adaptive learning-based path planning of maritime autonomous surface ships", in *2021 6th International Conference on Transportation Information and Safety (ICTIS)*, Wuhan, China, 2021, pp. 342–347. DOI: 10.1109/ICTIS54573.2021.9798502.

[8] D. Egea-Roca, M. Arizabaleta-Diez, T. Pany, *et al.*, "GNSS user technology: State-of-the-art and future trends", *IEEE Access*, vol. 10, pp. 39 939–39 968, 2022. DOI: 10.1109/ACCESS.2022.3165594.

[9] O. Montenbruck, P. Steigenberger, and J. Sleewaegen, "Data + pilot biases in modern GNSS signals", *GPS Solutions*, vol. 27, no. 1, p. 112, 2023. DOI: 10.1007/s10291-023-01448-y.

[10] A. Elmezayen, M. Karaim, H. Elghamrawy, and A. Noureldin, "Enhanced GNSS reliability on high-dynamic platforms: A comparative study of multi-frequency, multi-constellation signals in jamming environments", *Sensors*, vol. 23, no. 23, 2023, ISSN: 1424-8220. DOI: 10.3390/s23239552.

[11] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins, "GNSS vulnerabilities and existing solutions: A review of the literature", *IEEE Access*, vol. 9, pp. 153 960–153 976, 2021. DOI: 10.1109/ACCESS.2020.2973759.

[12] Y. Wang and Y. Li, "The positioning principle of global positioning system and its application prospects", *IOP Conference Series: Earth and Environmental Science*, vol. 781, 2021. DOI: 10.1088/1755-1315/781/2/022085.

[13] L. Martin, *GPS*, Accessed: 9-Mar-2023, 2023. [Online]. Available: https://www.lockheedmartin.com/en-us/products/gps.html.

[14] Q. Meng, L.-T. Hsu, B. Xu, X. Luo, and A. El-Mowafy, "A GPS spoofing generator using an open sourced vector tracking-based receiver", *Sensors*, vol. 19, no. 18, 2019, ISSN: 1424-8220. DOI: 10.3390/s19183993.

[15] E. G. A. (GSA), *Galileo open service (OS) system definition document (SDD)*, Accessed: 9-Mar-2023, 2020. [Online]. Available: https://galileognss.eu/wp-content/uploads/2020/08/Galileo-OS-SDD_v1.1.pdf.

[16] Y. Liu, Y. Chen, Z. Zuo, Y. Zhao, and Y. Liu, "Analyses of GLONASS and GPS+GLONASS precise positioning performance in different latitude regions", *Remote Sensing*, vol. 14, no. 18, p. 4640, 2022. DOI: 10.3390/rs14184640.

[17] W. Gao, W. Zhou, C. Tang, X. Li, Y. Yuan, and X. Hu, "High-precision services of beidou navigation satellite system (BDS): Current state, achievements, and future directions", *Satellite Navigation*, vol. 5, no. 1, p. 20, 2024. DOI: 10.1186/s43020-024-00143-8.

[18] BeiDou Navigation Satellite System, *Beidou navigation satellite system overview*, Accessed: 9-Mar-2023, 2023. [Online]. Available: http://en.beidou.gov.cn/SYSTEMS/System/.

[19] S. Liaquat, N. M. Mahyuddin, and I. H. Naqvi, "An end-to-end modular framework for radar signal processing: A simulation-based tutorial", *IEEE Aerospace and Electronic Systems Magazine*, vol. 39, no. 9, pp. 98–118, 2024. DOI: 10.1109/MAES.2023.3334689.

[20] X. Chen, C. Wei, G. Zhou, H. Wu, Z. Wang, and S. A. Biancardo, "Automatic identification system (AIS) data supported ship trajectory prediction and anal-

ysis via a deep learning model", *Journal of Marine Science and Engineering*, vol. 10, no. 9, 2022, ISSN: 2077-1312. DOI: 10.3390/jmse10091314.

[21] E. Tu, G. Zhang, L. Rachmawati, E. Rajabally, and G.-B. Huang, "Exploiting AIS data for intelligent maritime navigation: A comprehensive survey from data to methodology", *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 5, pp. 1559–1582, 2018. DOI: 10.1109/TITS.2017.2724551.

[22] International Maritime Organization (IMO), *AIS transponders*, Online, Accessed: Jul. 10, 2025. [Online]. Available: https://www.imo.org/en/ourwork/safety/pages/ais.aspx.

[23] D. Lee, M. Jung, W. Yang, and A. Kim, "LiDAR odometry survey: Recent advancements and remaining challenges", *Intelligent Service Robotics*, vol. 17, pp. 95–118, 2024. DOI: 10.1007/s11370-024-00515-8.

[24] International Maritime Organization (IMO), *Electronic nautical charts (ENC) and electronic chart display and information systems (ECDIS)*, Online, Accessed: Jul. 10, 2025. [Online]. Available: https://www.imo.org/en/ourwork/safety/pages/electroniccharts.aspx.

[25] International Maritime Organization (IMO), "Resolution msc.232(82): Adoption of the revised performance standards for electronic chart display and information systems (ECDIS)", International Maritime Organization, London, UK, Resolution MSC.232(82), Dec. 2006, Adopted on 5 December 2006. Accessed: Jul. 10, 2025. [Online]. Available: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.232%2882%29.pdf.

[26] A. Navigation, *Inertial measurement unit (IMU) – an introduction*, Online, Accessed: Sep. 28, 2025, 2023. [Online]. Available: https://www.advancedna

vigation.com/tech-articles/inertial-measurement-unit-imu-an-introduction/.

[27] International Maritime Organization (IMO), *Autonomous shipping*, Online, Accessed: Jul. 10, 2025. [Online]. Available: https://www.imo.org/en/mediacentre/hottopics/pages/autonomous-shipping.aspx.

[28] Det Norske Veritas (DNV), *AROS class notations: Autonomous and remotely operated ships*, Online, Accessed: Jul. 10, 2025. [Online]. Available: https://www.dnv.com/maritime/autonomous-remotely-operated-ships/aros-class-notation/.

[29] Det Norske Veritas (DNV), *DNV launches class notations to provide framework for safe development of autonomous shipping technologies*, Online, Accessed: Aug. 5, 2025., Jan. 2025. [Online]. Available: https://www.dnv.com/news/2025/dnv-launches-class-notations-to-provide-framework-for-safe-development-of-autonomous-shipping-technologies/.

[30] Lloyd's Register (LR), "Maritime autonomous surface ships (MASS) — volume 2: The relevance of operational design domain (ODD) and operational envelope (OE) in design, implementation and assurance", Lloyd's Register, Research Report, May 2025, Accessed: Sep. 28, 2025. [Online]. Available: https://maritime.lr.org/MASS/report.

[31] Lloyd's Register (LR), "Maritime autonomous surface ships (MASS) — volume 2: The relevance of operational design domain (ODD) and operational envelope (OE) in design, implementation and assurance", Lloyd's Register, Research Report, May 2025, Accessed: Sep. 28, 2025. [Online]. Available: https://maritime.lr.org/MASS-report-vol2.

[32] American Bureau of Shipping (ABS), "Abs advisory on autonomous functionality", American Bureau of Shipping (ABS), Advisory, 2021, Accessed: Sep.

28, 2025. [Online]. Available: https://ww2.eagle.org/content/dam/eagle/advisories-and-debriefs/abs-advisory-on-autonomous-functionality.pdf.

[33] A. S. Alamoush and A. I. Ölçer, "Maritime autonomous surface ships: Architecture for autonomous navigation systems", *Journal of Marine Science and Engineering*, vol. 13, no. 1, p. 122, 2025, Accessed: Aug. 4, 2025. DOI: 10.3390/jmse13010122.

[34] P. Fiorini and Z. Shiller, "Motion planning in dynamic environments using velocity obstacles", *IEEE Transactions on Robotics and Automation*, vol. 14, no. 6, pp. 764–774, 1998, Accessed: Jul. 17, 2025. DOI: 10.1177/027836499801700706.

[35] Z. Yan, Y. Xiao, L. Cheng, *et al.*, "Analysis of global marine oil trade based on automatic identification system (AIS) data", *Journal of Transport Geography*, vol. 83, p. 102 637, Feb. 2020. DOI: 10.1016/j.jtrangeo.2020.102637.

[36] J.-S. Lee, H.-T. Lee, and I.-S. Cho, "Maritime traffic route detection framework based on statistical density analysis from AIS data using a clustering algorithm", *IEEE Access*, vol. 10, pp. 23 355–23 366, 2022. DOI: 10.1109/ACCESS.2022.3154363.

[37] Q. Wang, Y. Tan, and Z. Mei, "Computational methods of acquisition and processing of 3d point cloud data for construction applications", *Archives of Computational Methods in Engineering*, vol. 27, no. 2, pp. 479–499, 2020, Accessed: Jul. 17, 2025. DOI: 10.1007/s11831-019-09320-4.

[38] A. B. Martinsen, G. Bitar, A. M. Lekkas, and S. Gros, "Optimization-based automatic docking and berthing of ASVs using exteroceptive sensors: Theory and experiments", *IEEE Access*, vol. 8, pp. 204 974–204 986, 2020. DOI: 10.1109/ACCESS.2020.3037171.

[39] U. of Missouri Libraries, *Keenious: Ai for the article search*, Online, Accessed: Dec. 8, 2025., 2025. [Online]. Available: https://libraryguides.missouri.edu/keenious/keenious-ai.

[40] *ISO 31000:2018 — risk management — guidelines*, Accessed: Aug. 5, 2025., International Organization for Standardization (ISO), 2018. [Online]. Available: https://www.iso.org/standard/65694.html.

[41] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments (nist sp 800-30 rev. 1)", National Institute of Standards and Technology (NIST), Special Publication 800-30, Revision 1, Sep. 2012, Accessed: Aug. 5, 2025. DOI: 10.6028/NIST.SP.800-30r1.

[42] International Maritime Organization (IMO), *Formal safety assessment*, Online, Accessed: Jul. 10, 2025. [Online]. Available: https://www.imo.org/en/ourwork/safety/pages/formalsafetyassessment.aspx.

[43] International Maritime Organization (IMO), "Msc-mepc.2/circ.12/rev.2: Revised guidelines for formal safety assessment (FSA) for use in the imo rule-making process", International Maritime Organization, London, UK, Circular MSC-MEPC.2/Circ.12/Rev.2, 2018, Approved: 9 April 2018. Accessed: Jul. 10, 2025. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/MSC-MEPC%202-Circ%2012-Rev%202.pdf.

[44] A. Laakso, M. Chaal, and O. A. V. Banda, "A risk assessment of an autonomous navigation system for a maritime autonomous surface ship", *Journal of Marine Engineering & Technology*, vol. 24, no. 4, pp. 253–269, 2025. DOI: 10.1080/20464177.2025.2460268.

[45] V. Bolbot, G. Theotokatos, L. Wennersberg, *et al.*, "A novel risk assessment process: Application to an autonomous inland waterways ship", *Proceedings of*

the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, vol. 237, no. 2, pp. 436–458, 2023. DOI: 10.1177/1748006X211051829.

[46] A. Felski and K. Zwolak, "The ocean-going autonomous ship — challenges and threats", *Journal of Marine Science and Engineering*, vol. 8, no. 1, p. 41, 2020, Accessed: Aug. 5, 2025. DOI: 10.3390/jmse8010041.

[47] J. Burbank, T. Greene, and N. Kaabouch, "Detecting and mitigating attacks on GPS devices", *Sensors*, vol. 24, no. 17, 2024, Accessed: Sep. 28, 2025. DOI: 10.3390/s24175529.

[48] R. Ziebold, D. Medina, M. Romanovas, C. Lass, and S. Gewies, "Performance characterization of GNSS/IMU/DVL integration under real maritime jamming conditions", *Sensors*, vol. 18, no. 9, p. 2954, 2018, Accessed: Aug. 4, 2025. DOI: 10.3390/s18092954.

[49] Y. Yang and B. Yang, "Overview of radar detection methods for low altitude targets in marine environments", *Journal of Systems Engineering and Electronics*, vol. 35, no. 1, pp. 1–13, 2024. DOI: 10.23919/JSEE.2024.000026.

[50] S. Khandker, H. Turtiainen, A. Costin, and T. Hämäläinen, "Cybersecurity attacks on software logic and error handling within AIS implementations: A systematic testing of resilience", *IEEE Access*, vol. 10, pp. 29 493–29 505, 2022. DOI: 10.1109/ACCESS.2022.3158943.

[51] C. Ray, C. Iphar, and A. Napoli, "Methodology for real-time detection of AIS falsification", in *Proc. Maritime Knowledge Discovery and Anomaly Detection Workshop*, Held on 5–6 July 2016, Naval Academy Research Institute (IRENav), Brest, France, Jul. 2016. [Online]. Available: https://minesparis-psl.hal.science/hal-01421910/document.

[52] R. Changalvala and H. Malik, "LiDAR data integrity verification for autonomous vehicle", *IEEE Access*, vol. 7, pp. 138 018–138 031, 2019. DOI: 10.1109/ACCESS.2019.2943207.

[53] M. A. Khan, H. Menouar, M. Abdallah, and A. Abu-Dayya, "LiDAR in connected and autonomous vehicles - perception, threat model, and defense", *IEEE Transactions on Intelligent Vehicles*, pp. 1–19, 2024. DOI: 10.1109/TIV.2024.3510787.

[54] G. Kayisoğlu, B. Güneş, and P. Bolat, "ECDIS cyber security dynamics analysis based on the fuzzy FUCOM method", *Transactions on Maritime Science*, vol. 13, no. 1, 2024, Accessed: Aug. 4, 2025. DOI: 10.7225/toms.v13.n01.w09.

[55] G. Kavallieratos and S. Katsikas, "Managing cyber security risks of the cyber-enabled ship", *Journal of Marine Science and Engineering*, vol. 8, Sep. 2020. DOI: 10.3390/jmse8100768.

[56] B. S. Margana, D. S. Achanta, K. K. Songala, and S. R. Ammana, "A simple SDR based method to spoof low-end GPS aided drones for securing locations", in *2021 IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON)*, 2021, pp. 32–36. DOI: 10.1109/RAAICON54709.2021.9929965.

[57] J. Aru Saputro, E. Egistian Hartadi, and M. Syahral, "Implementation of GPS attacks on DJI phantom 3 standard drone as a security vulnerability test", in *2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE)*, Yogyakarta, Indonesia, 2020, pp. 95–100. DOI: 10.1109/ICITAMEE50454.2020.9398386.

[58] T. Mina and coauthors, "GPS spoofing-resilient filtering using self-contained sensors and chimera signal enhancement", *NAVIGATION: Journal of the In-*

stitute of Navigation, vol. 71, no. 2, 2024, Accessed: Sep. 28, 2025. DOI: 10.33012/navi.636.

[59] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing", *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, 2013. DOI: 10.1109/TAES.2013.6494400.

[60] G. Longo, E. Russo, A. Armando, and A. Merlo, "Attacking (and defending) the maritime radar system", *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 3575–3589, 2023. DOI: 10.1109/TIFS.2023.3282132.

[61] Y. Pan, D. Xie, Y. Zhao, X. Wang, and Z. Huang, "Overview of radar jamming waveform design", *Remote Sensing*, vol. 17, no. 7, p. 1218, 2025, Accessed: Sep. 28, 2025. DOI: 10.3390/rs17071218.

[62] B. Svilicic, I. Rudan, V. Frančić, and M. Doričić, "Shipboard ECDIS cyber security: Third-party component threats", *Scientific Journal of Maritime Research*, vol. 33, no. 2, pp. 176–180, 2019, Received: 17 Sept. 2019; Accepted: 14 Oct. 2019; Accessed: 14 Aug. 2025. DOI: 10.31217/p.33.2.7.

[63] I. Boukabou, N. Kaabouch, and D. Rupanetti, "Cybersecurity challenges in UAV systems: Iemi attacks targeting inertial measurement units", *Drones*, vol. 8, no. 12, p. 738, 2024, Accessed: Sep. 28, 2025. DOI: 10.3390/drones8120738.

[64] *Electrical and electronic installations in ships – electromagnetic compatibility (EMC) – ships with a metallic hull*, International Electrotechnical Commission (IEC), 2015.

[65] S. Telegraph, *Piracy and armed robbery attacks up 50% in first half of 2025*, Accessed: Sep. 28, 2025, Jul. 2025. [Online]. Available: https://shippingtelegraph.com/piracy-news/piracy-and-armed-robbery-attacks-up-50-in-first-half-of-2025/.

[66] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the gnss spoofing threat and countermeasures", *ACM Computing Surveys*, vol. 48, no. 4, pp. 1–31, 2016, Accessed: Aug. 5, 2025. DOI: 10.1145/2897166.

[67] J. Khalil, *Galileo OSNMA authentication service now operational*, Online, Accessed: Aug. 5, 2025., Jul. 2025. [Online]. Available: https://www.gpsworld.com/galileo-osnma-authentification-service-now-operational/.

[68] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems", in *Proceedings of the 16th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS/GNSS 2003)*, Accessed: Sep. 28, 2025., Portland, OR, USA, 2003, pp. 1543–1552. [Online]. Available: https://www.ion.org/publications/abstract.cfm?articleID=5339.

[69] M. C. Esswein and M. L. Psiaki, "GPS spoofing resilience via nma/watermarks authentication and IMU prediction", in *Proceedings of the 34th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2021)*, St. Louis, Missouri, USA, Sep. 2021, pp. 3591–3620. DOI: 10.33012/2021.17997.

[70] H. Zhao, H. Song, R. Liu, J. Hou, and X. Yu, "Anti-jamming decision-making for phased-array radar based on improved deep reinforcement learning", *Electronics*, vol. 14, no. 11, p. 2305, 2025, Accessed: Sep. 28, 2025. DOI: 10.3390/electronics14112305.

[71] A. Lei, W. Fan, and F. Zhou, "A cognitive radar anti-jamming strategy generation algorithm based on dueling double DQN", in *2023 IEEE International Radar Conference (RADAR)*, Sydney, Australia, 2023, pp. 1–5. DOI: 10.1109/RADAR54928.2023.10371114.

[72] Z. Zheng, W. Li, and K. Zou, "Airborne radar anti-jamming waveform design based on deep reinforcement learning", *Sensors*, vol. 22, no. 22, p. 8689, 2022, Accessed: Sep. 28, 2025. DOI: 10.3390/s22228689.

[73] P. Su, N. Sun, L. Zhu, *et al.*, "A privacy-preserving and vessel authentication scheme using automatic identification system", in *Proc. 5th ACM Int. Workshop on Security in Cloud Computing*, Presented at the Fifth ACM International Workshop on Security in Cloud Computing, 2017. DOI: 10.1145/3055259.3055261.

[74] S. Sciancalepore, P. Tedeschi, A. Aziz, and R. Di Pietro, "Auth-AIS: Secure, flexible, and backward-compatible authentication of vessels AIS broadcasts", *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2709–2726, 2022. DOI: 10.1109/TDSC.2021.3069428.

[75] C. You, Z. Hau, and S. Demetriou, "Temporal consistency checks to detect LiDAR spoofing attacks on autonomous vehicle perception", in *Proceedings of the 1st Workshop on Security and Privacy for Mobile AI (MAISP'21)*, New York, NY, USA: Association for Computing Machinery, 2021, pp. 13–18. DOI: 10.1145/3469261.3469406.

[76] M. Cho, Y. Cao, Z. Zhou, and Z. M. Mao, "Adopt: LiDAR spoofing attack detection based on point-level temporal consistency", Manuscript, unpublished, 2023. [Online]. Available: https://openreview.net/pdf?id=Agsuz9JmVp.

[77] Y. Cao, N. Wang, C. Xiao, *et al.*, "Invisible for both camera and LiDAR: Security of multisensor fusion based perception in autonomous driving under physical-world attacks", in *Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP)*, United States: IEEE, May 2021, pp. 176–194. [Online]. Available: https://www.computer.org/csdl/proceedings-article/sp/2021/893400b302/1t0x9btzenu.

[78] LähiTapiola, *Henkivakuutus*, Accessed: Sep. 28, 2025, 2025. [Online]. Available: https://www.lahitapiola.fi/henkilo/vakuutukset/terveysvakuutukset/henkivakuutus/.

[79] N. B. Abp, *Henkivakuutus*, Accessed: Sep. 28, 2025, 2025. [Online]. Available: https://www.nordea.fi/henkiloasiakkaat/palvelumme/vakuutukset/henkilovakuutukset/henkivakuutus.html.