ARCHIVES OF TRANSPORT *ISSN (print):* *0866-9546*
Volume 77, Issue 1, 2026 ***e-ISSN (online):*** *2300-8830*
DOI: *10.61089/aot2026.1jaejy17*

CYBERSECURITY CHALLENGES AND VULNERABILITIES OF THE AUTOMATIC IDENTIFICATION SYSTEM IN MARITIME TRANSPORT

Rafał CICHOCKI[1], Tomasz NEUMANN[2]

[1, 2] *Gdynia Maritime University, Gdynia, Poland*

***Abstract**:*

The Automatic Identification System (AIS) has become a fundamental component of modern maritime navigation, supporting real-time vessel tracking, collision avoidance, and traffic management. However, its protocol was developed without cybersecurity considerations, resulting in structural vulnerabilities that increasingly threaten operational safety and reliability. AIS broadcasts are neither encrypted nor authenticated, allowing adversaries to intercept, manipulate, or fabricate messages with minimal technical effort. This exposes maritime operators to a spectrum of cyber threats, including identity spoofing, false-data injection, replay attacks, and targeted radio-frequency jamming. As AIS data is routinely integrated into Electronic Chart Display and Information Systems (ECDIS), Vessel Traffic Services (VTS), and autonomous navigation modules, these weaknesses propagate across interconnected maritime infrastructures, amplifying the potential consequences of compromised data integrity. This article provides a systematic assessment of the core vulnerabilities inherent in AIS communication, emphasizing the absence of cryptographic protections, the ease of broadcasting falsified vessel information, and the susceptibility of the VHF communication channel to intentional interference. The operational impacts of these threats are analyzed with regard to navigational decision-making, port coordination, surveillance accuracy, and maritime domain awareness. Particular attention is given to the risks resulting from excessive dependency on AIS as a primary sensor input, especially in automated or minimally manned operational environments. In response to these challenges, the study outlines a set of technical and organizational countermeasures. Proposed solutions include the integration of authentication layers and lightweight encryption into future AIS/VDES protocols, the deployment of anomaly-detection algorithms for real-time identification of spoofed or inconsistent data, the cross-verification of AIS information with independent sensors, and the systematic maintenance of AIS-capable equipment. Additionally, the article highlights the need for harmonized regulatory reforms and enhanced cybersecurity training for crews and port operators. Collectively, these measures aim to strengthen the resilience of maritime communication systems and ensure that AIS continues to serve as a reliable component of navigational safety in an increasingly digitalized and threat-exposed maritime domain.

Keywords: *automatic identification system, maritime cybersecurity, spoofing and jamming attacks, data integrity and authentication, defense-in-depth strategies*

To cite this article:

Cichocki, R., Neumann, T. (2026). Cybersecurity challenges and vulnerabilities of the automatic identification system in maritime transport. Archives of Transport, 77(1), 27-43. https://doi.org/10.61089/aot2026.1jaejy17

Contact:
1) r.cichocki@wn.umg.edu.pl [https://orcid.org/0000-0002-5004-5587] – corresponding author; 2) t.neumann@wn.umg.edu.pl [https://orcid.org/0000-0002-4149-8293]

1. Overview of the AIS Technology

The Automatic Identification System (AIS) is a maritime communication technology designed to enhance navigational safety and improve vessel traffic monitoring. Mandated by the International Maritime Organization (IMO) under the SOLAS Convention, AIS is required on all SOLAS-class vessels over 300 gross tonnage and on all passenger ships, as well as many smaller commercial vessels depending on national regulations. The system operates by automatically transmitting a vessel's identity, position, speed, course, navigational status, and other voyage-related data at regular intervals via VHF radio frequencies (161.975 MHz and 162.025 MHz). This information is broadcast in real time and can be received by nearby ships, coastal stations, and satellites, allowing for enhanced situational awareness, collision avoidance, and traffic coordination (Stupak, 2014).

AIS equipment is typically categorized into two classes: Class A transceivers, which are used on large commercial vessels and transmit at higher power and more frequent intervals, and Class B transceivers, which are designed for smaller vessels and transmit less frequently with lower power. The AIS protocol, standardized under ITU-R M.1371, supports a wide range of message types—ranging from static ship information (e.g., MMSI, name, type) to dynamic data (e.g., position, course, speed) and voyage-specific data (e.g., destination, ETA, draft). Over time, AIS has also been integrated into port management systems, Vessel Traffic Services (VTS), and Electronic Chart Display and Information Systems (ECDIS), becoming a core component of modern maritime navigation infrastructure (Emmens et al., 2021; Svanberg et al., 2019).

Despite its benefits, AIS was developed in a pre-cybersecurity era, with limited consideration for digital threats. Its open, unauthenticated, and unencrypted design—while facilitating interoperability and transparency—also introduces significant vulnerabilities, which are increasingly being exploited in the current threat landscape. As such, understanding the technical foundations of AIS is essential for assessing its cybersecurity risks and identifying opportunities for secure enhancements (Goudosis & Katsikas, 2020).

1.1. Objectives, Research Questions, and Scope

The objective of this study is to provide a structured assessment of cybersecurity vulnerabilities of the Automatic Identification System (AIS) and to identify feasible mitigation strategies across shipboard, shore-based, and regulatory contexts.

The study addresses the following research questions:

RQ1: Which protocol-level and operational vulnerabilities of AIS most critically affect navigational safety and maritime situational awareness?

RQ2: Which categories of cyber threats (integrity, availability, deception/manipulation) pose the highest operational risk to AIS-dependent systems?

RQ3: Which mitigation measures are most feasible in the short, mid, and long term for maritime stakeholders?

The scope of the assessment is limited to AIS deployments on SOLAS-class vessels and VTS environments, focusing on cybersecurity threats reported in the period 2019–2025, including spoofing, data injection, replay attacks, and RF jamming. The assessment is based on a structured synthesis of peer-reviewed literature and regulatory documents rather than on original empirical experiments.

1.2. Methodology of the Systematic Assessment

The study adopts a structured literature-based assessment of AIS cybersecurity vulnerabilities and countermeasures. Literature was identified using Scopus, Web of Science, IEEE Xplore, and Google Scholar (2019–2026) with keyword combinations including “AIS cybersecurity”, “AIS spoofing”, “AIS jamming”, “VDES security”, and “maritime anomaly detection”.

Included sources comprise peer-reviewed journal articles, conference papers, and authoritative regulatory documents (IMO, IALA, IACS, USCG). Studies without explicit relevance to AIS cybersecurity were excluded. Identified threats and countermeasures were categorized using a risk-based framework (integrity, availability, deception/manipulation). The Risk Matrix is a qualitative synthesis of reported incidents and expert assessments in the literature and is intended as a conceptual prioritization tool rather than a statistically derived model.

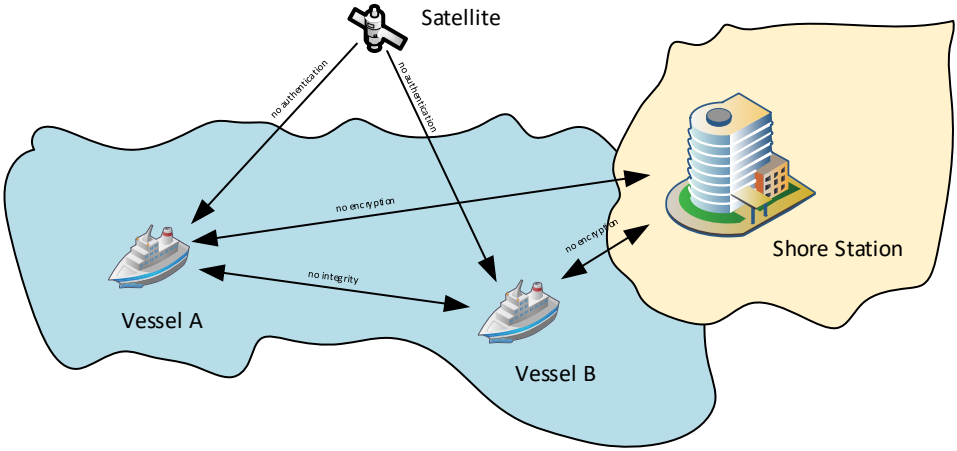

Fig. 1. AIS Architecture and Vulnerabilities

2. Risk-Based Structuring of AIS Cyber Threats

The analysis of AIS vulnerabilities presented in this section aligns with broader concerns documented in the maritime cybersecurity literature. In particular, recent work by (Cichocki & Wójcik, 2025) highlights the systemic exposure of interconnected maritime systems and underscores the need to identify protocol-level and operational weaknesses as a basis for mitigation strategies. By situating AIS vulnerabilities within this broader landscape of maritime cyber threats, our analysis contributes a focused and operational perspective that complements the higher-level frameworks previously proposed. In addition to conceptualizing AIS vulnerabilities, analytical approaches such as optimization and search algorithms have been applied to maritime security problems. For instance, (Chang et al., 2025) employ a genetic algorithm to model and mitigate ship robbery risk, demonstrating how computational intelligence can support the identification of high-risk scenarios in maritime transport. Although focused on a different domain, this methodology illustrates the potential for similar algorithmic tools to assist in AIS vulnerability analysis and anomaly detection. In addition to domain-specific analyses of AIS vulnerabilities, broader studies have examined cybersecurity challenges across the wider maritime industry. (Neumann, 2024) provides a systemic perspective on industry-wide cyber risks, including governance, organizational readiness, and holistic defense strategies. Integrating these insights highlights that AIS security concerns should be contextualized not only at the protocol and system level but also within the larger framework of maritime industry cybersecurity practices. Recent studies exploring cybersecurity trends in maritime systems offer useful context for our vulnerability analysis. (Junaidi et al., 2024) identifies key trends in maritime cyber threats and defenses, emphasizing the rapid evolution of both attack vectors and protective measures in digitalized shipping environments. By situating AIS-specific vulnerabilities within these broader maritime cybersecurity trends, this paper highlights how sector-wide dynamics influence the threat landscape and inform targeted risk mitigation strategies.

2.1. Integrity Attacks

No Authentication of Data Sources

Another major vulnerability of the AIS is the lack of authentication mechanisms for data sources. AIS does not verify whether the transmitted information actually originates from a legitimate vessel or maritime authority. Every AIS transponder can freely transmit messages, and the system does not incorporate any cryptographic techniques, such as digital signatures or certificates, that would allow receivers to validate the identity of the sender. This design flaw enables a wide range of spoofing at-

tacks, in which malicious actors transmit falsified AIS messages, impersonating real vessels or creating entirely fictional ones (Tsiopoulos & Vaarandi, 2025). Such attacks can lead to serious operational and security consequences. For example, a fake vessel can be injected into maritime traffic systems, potentially causing confusion in port coordination or even triggering collision avoidance manoeuvres by nearby ships. Spoofed AIS data can also be used to obscure the actual location of a vessel, support illegal activities such as smuggling or fishing in restricted zones, or manipulate public awareness during geopolitical tensions. The absence of sender authentication fundamentally undermines trust in the AIS network, especially when it is integrated with other navigational and decision-support systems such as radar overlays, ECDIS, and Vessel Traffic Services (VTS) (Wimpenny et al., 2022).

In modern cybersecurity terms, the inability to verify the identity of a data source violates a basic principle of secure communication. As AIS continues to serve as a cornerstone of maritime situational awareness, this weakness must be addressed, whether through protocol redesign, supplementary authentication layers, or regulatory mandates to integrate AIS with more secure maritime communication systems.

No Data Integrity Verification

One of the fundamental limitations of the AIS protocol is the absence of any built-in mechanism for verifying the integrity of transmitted messages. Unlike modern communication systems that employ checksums, hash functions, or digital signatures to ensure that data has not been altered in transit, AIS messages are transmitted in clear text without any such validation. This means that receivers have no way of determining whether a message has been tampered with, corrupted, or maliciously modified during transmission. This creates a significant security gap, especially in scenarios where AIS data is relied upon for real-time decision-making (Banyś et al., 2024).

Due to the lack of integrity verification, AIS messages can be intercepted and subtly modified without triggering alarms or alerts in most maritime systems. This vulnerability allows attackers to perform stealthy data manipulation, such as altering a vessel's position by a few nautical miles, changing its name or status, or modifying its destination port. Such changes may appear minor, but they can have serious consequences in congested maritime zones, during emergency response operations, or when automated systems (such as collision avoidance algorithms or port traffic managers) are in use. Modern maritime operations increasingly rely on automated and integrated systems for navigation, surveillance, and traffic control. These systems often fuse AIS data with radar, satellite, and chart information to build a situational picture. Without guaranteed data integrity, however, such systems are vulnerable to corrupted or falsified input, potentially leading to incorrect assessments and unsafe actions. For example, an altered AIS message could mislead a collision-avoidance system into ignoring an approaching vessel or cause a port to reroute traffic unnecessarily, resulting in delays and increased operational costs.

The lack of verifiable integrity in AIS messages also complicates post-incident investigations and legal accountability. If an incident occurs—such as a collision, smuggling attempt, or maritime cyberattack, it may be impossible to prove whether AIS data was accurate or manipulated. Without cryptographic assurance, AIS logs can be questioned or challenged in court, weakening their role as digital evidence. This presents a challenge not only for maritime safety regulators but also for insurance companies, law enforcement agencies, and naval operations that depend on the trustworthiness of AIS records.

To address the lack of data integrity verification, there is an urgent need to modernize the AIS protocol or supplement it with external verification layers. Potential solutions include the use of cryptographic message signing, blockchain-based logging systems, or the development of a secure AIS overlay protocol that ensures end-to-end integrity. Until such measures are adopted at scale, AIS will remain a vulnerable component in the broader maritime cybersecurity landscape. In the meantime, stakeholders should implement cross-validation methods, such as comparing AIS data with radar or satellite imagery, and adopt anomaly detection algorithms to flag suspicious message patterns in real time.

Vulnerability to Data Injection

The AIS protocol is highly vulnerable to data injection attacks due to its open and unauthenticated communication model, which allows attackers to easily transmit falsified messages using inexpen-

sive equipment and freely available software. Without any safeguards to prevent the injection of arbitrary or maliciously crafted data, adversaries can broadcast fake vessel positions, false distress calls, incorrect navigational statuses, or even artificial hazards such as phantom storms or congestion zones. These fabricated messages can mislead ship crews, port authorities, and autonomous navigation systems, resulting in poor decision-making, unnecessary evasive manoeuvres, or traffic disruptions. Unlike passive eavesdropping or simple spoofing, data injection represents an active and potentially large-scale threat that exploits both the technical limitations of AIS and the trust placed in its data by maritime systems. Attackers can not only fabricate non-existent vessels but also influence the behaviour of legitimate ones by manipulating surrounding traffic information. Coordinated injection attacks may disrupt port operations, interfere with search and rescue missions, or serve as tools in hybrid warfare and maritime disinformation campaigns. Mitigating this vulnerability requires a combination of technological and procedural countermeasures, including the implementation of anomaly detection algorithms, authentication layers, and the development of updated international standards to ensure secure and resilient maritime communications (Benterki et al., 2025).

Susceptibility to Replay Attacks

The AIS is notably susceptible to replay attacks, a form of cyber threat in which legitimate AIS messages are recorded and later rebroadcast to deceive receivers. This vulnerability arises from the fact that AIS messages do not contain timestamps, unique session identifiers, or cryptographic protections that would allow systems to detect whether a message is original or repeated. As a result, an attacker can capture genuine transmissions from a vessel, such as its position, speed, and identity, and rebroadcast them hours or even days later, either in the same location or in a completely different maritime area (Lázaro et al., 2023).

Replay attacks can have serious operational and strategic consequences. For example, they may create the illusion of a vessel's presence in a location where it is no longer operating, or obscure the true movements of a ship by replaying outdated position data. Such tactics can be used to mislead port authorities, disrupt shipping logistics, or support illicit activities like smuggling and sanctions evasion. In military or geopolitical contexts, replay attacks could serve as part of deception operations, giving adversaries a false sense of maritime traffic patterns or force deployment (Soner et al., 2024).

Because AIS was not designed with cybersecurity in mind, it lacks mechanisms to validate the freshness and authenticity of received messages. As AIS data becomes increasingly integrated into automated systems and situational awareness platforms, the threat posed by replay attacks grows accordingly. Mitigation strategies may include time-based anomaly detection, cross-verification with radar or satellite data, and the development of enhanced AIS standards that incorporate cryptographic timestamping or message chaining.

The lack of authentication and integrity verification mechanisms in AIS directly enables integrity attacks such as data injection and replay, allowing adversaries to manipulate navigational information without detection.

2.2. Availability Attacks

Susceptibility to Jamming

The AIS is also inherently susceptible to radio frequency jamming, a form of denial-of-service (DoS) attack in which malicious actors intentionally interfere with the radio spectrum used for AIS transmissions. Since AIS operates on fixed, narrowband VHF frequencies (161.975 MHz and 162.025 MHz), it is relatively easy to disrupt communications using low-cost equipment that emits continuous or pulsed signals on the same frequencies. This can effectively prevent AIS messages from being received by other vessels, shore stations, or satellites, thereby reducing maritime situational awareness and compromising navigational safety (Steiner et al., 2023).

Unlike spoofing or data injection—which rely on manipulating or falsifying information—jamming attacks are purely disruptive, aiming to silence the system entirely. In congested sea lanes or near critical infrastructure such as ports, offshore platforms, or naval installations, even brief interruptions in AIS functionality can lead to traffic delays, loss of vessel tracking, and increased collision risk. Additionally, jamming can be used in combination with other cyberattacks, such as spoofing or replay attacks, to mask malicious activities or delay detection of anomalies.

The vulnerability of AIS to jamming stems from its lack of built-in resilience or anti-interference mechanisms, such as frequency hopping or signal redundancy. As reliance on AIS continues to grow, this susceptibility highlights the urgent need for redundant tracking systems, improved signal verification techniques, and policy frameworks that classify AIS interference as a serious maritime threat.

Availability attacks, particularly RF jamming, can significantly degrade AIS reception, leading to a loss of situational awareness in congested waters and port approaches.

2.3. Deception and Manipulation Attacks

Lack of Encryption

One of the most fundamental and dangerous weaknesses of the AIS is the complete lack of encryption in its data transmissions. The AIS protocol was developed in the 1990s with a focus on simplicity and interoperability, not anticipating the cybersecurity threats of the modern digital age. AIS messages are transmitted in plain text over publicly accessible VHF radio frequencies (161.975 MHz and 162.025 MHz), meaning that anyone with a basic radio receiver or software-defined radio (SDR) can easily intercept, decode, and analyse the data. The absence of any form of encryption allows sensitive information about vessels, such as name, MMSI number, real-time position, course, speed, and navigational status, to be accessed without authorization (Sun et al., 2025).

While this openness was originally intended to enhance navigational safety and facilitate maritime coordination, it now poses a serious cybersecurity risk. AIS data can be intercepted by third parties and used for unlawful or malicious purposes, such as industrial espionage, piracy planning, military vessel tracking, or targeted disinformation campaigns. Furthermore, the lack of encryption prevents verification of the authenticity and integrity of transmitted messages, making the system highly vulnerable to spoofing and replay attacks, in which falsified or previously recorded messages are broadcast to mislead receivers. In an era of increasing digitalization and automation of maritime transport, where AIS is integrated into systems like ECDIS, radar, and port infrastructure, the lack of secure communication channels is a critical weakness in maritime traffic management. Unencrypted data within such essential systems should be regarded as a significant security gap requiring urgent attention. This includes the implementation of additional protective measures and a reassessment of international technical regulations to ensure that AIS communications are resilient in the face of contemporary cybersecurity threats (Androjna et al., 2021).

Overreliance on AIS Data

As maritime operations become increasingly digitalized and interconnected, the AIS is often treated as a primary source of navigational and situational awareness data. Modern bridge systems, ECDIS, and port traffic management platforms frequently rely on AIS inputs to monitor vessel positions, detect potential collisions, and coordinate traffic flows. While AIS was originally intended as a supplementary safety tool, it is now routinely used as a trusted data feed, sometimes without adequate cross-validation from radar, visual observation, or satellite tracking. This growing dependency heightens the risks associated with spoofed, manipulated, or incomplete AIS messages.

Overreliance on AIS data poses serious challenges, especially in environments that involve automated systems or minimal human oversight. If AIS data is falsified, intentionally or unintentionally, autonomous navigation algorithms or collision-avoidance systems may respond inappropriately, increasing the risk of grounding, traffic conflicts, or unsafe manoeuvres. Similarly, in busy ports or strategic chokepoints, a single falsified transmission could trigger broader operational disruptions. Trusting AIS data without verification can also lead to failures in threat detection, such as missing vessels operating without transponders ("dark ships") or incorrectly assuming that a spoofed vessel is legitimate.

To mitigate the dangers of overreliance on AIS, maritime systems must incorporate redundancy and robust data validation mechanisms. This includes cross-checking AIS data with independent sensors (e.g., radar, sonar, optical cameras), deploying anomaly detection algorithms, and training maritime personnel to interpret discrepancies critically. Additionally, shore-based systems like Vessel Traffic Services (VTS) should adopt layered approaches that combine AIS with other surveillance technologies to build a more reliable picture of maritime activity. Recognizing AIS as a useful, but

fallible, source of information is essential for ensuring safety and resilience in both manned and autonomous maritime operations.

The absence of encryption and the operational overreliance on AIS significantly amplify deception and manipulation attacks, enabling adversaries to construct misleading traffic pictures and influence navigational decision-making.

2.4. Cross-cutting Enablers

Insufficient Regulatory Requirements

The AIS protocol was developed in the late 1990s under the auspices of the International Maritime Organization (IMO) and the International Telecommunication Union (ITU), at a time when cybersecurity was not a major consideration in maritime communication systems. As a result, the design of AIS prioritizes openness and interoperability over data protection and authenticity. Although AIS has since become a critical component of maritime safety and traffic coordination, the original specifications have not been significantly updated to reflect modern cybersecurity threats. This leaves a dangerous gap between the increasing reliance on AIS and the lack of technical safeguards embedded in its standard.

Current international regulations, including SOLAS (Safety of Life at Sea) and ITU-R M.1371, define AIS functionality and carriage requirements but do not mandate any specific cybersecurity features such as encryption, authentication, or message integrity checks. Furthermore, there is a lack of binding global enforcement regarding how AIS devices, especially low-cost Class B transponders, are implemented or maintained. This regulatory vacuum enables the proliferation of unsecured and potentially exploitable AIS equipment, particularly on small commercial vessels, fishing boats, and leisure craft. Without a harmonized global framework, national authorities are left to adopt inconsistent or minimal protection standards.

While cybersecurity has recently gained attention through IMO guidelines such as MSC-FAL.1/Circ.3 on maritime cyber risk management, these documents provide only high-level, non-binding recommendations. AIS is rarely addressed directly or in sufficient detail, and most guidance is focused on general IT/OT systems aboard ships, rather than communication protocols specifically. This lack of specificity contributes to a low level of awareness and preparedness among maritime operators and vessel owners, who may not fully understand the risks associated with AIS misuse or compromise. The absence of enforcement mechanisms further undermines the practical implementation of even the existing guidelines.

Addressing the cybersecurity weaknesses of AIS requires coordinated international policy reform that treats secure communication as a mandatory component of maritime safety. This could involve the revision of ITU and IMO technical standards to incorporate cryptographic protections, authentication protocols, and regular firmware updates for AIS equipment. Additionally, flag states and classification societies could play a greater role in enforcing compliance through certification schemes and audits. Without such measures, the maritime domain will continue to rely on a foundational system that is technically obsolete and inadequately protected against 21st-century cyber threats.

Insufficient regulatory requirements act as a cross-cutting enabler of AIS cyber risks, slowing down the adoption of security-by-design mechanisms and prolonging the exposure of legacy systems.

The qualitative risk mapping of AIS vulnerabilities and their operational impacts is summarized in Table 1, which provides a comparative overview of attack types, likelihood, and severity. The Risk Matrix (Fig. 2) represents a qualitative synthesis of published incident reports and expert assessments in the literature and is intended as a conceptual prioritization tool rather than a statistically derived model.

Likelihood and severity are assessed qualitatively (Low/Medium/High) based on technical feasibility, required attacker capabilities, and potential operational consequences.

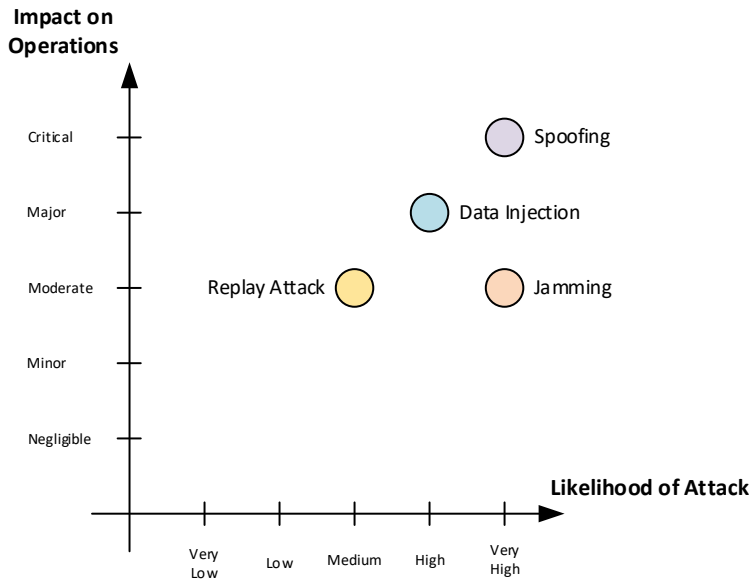

Fig. 2. Risk Matrix of Cyberattacks on AIS

Table 1. Risk Mapping of AIS Vulnerabilities

Vulnerability	Attack type	Impact (operational)	Likelihood	Severity
No authentication of data sources	Integrity / Deception	Vessel impersonation, ghost targets, false CPA/TCPA	High	High
No data integrity verification	Integrity	Undetected data manipulation, misleading tracks	Medium–High	High
Vulnerability to data injection	Integrity / Deception	Traffic disruption, false distress/AtoN, unsafe manoeuvres	Medium	High
Susceptibility to replay attacks	Integrity / Deception	False vessel presence, masking true movements	Medium	High
Lack of encryption	Deception	Tracking of vessels, preparation of targeted attacks	High	Medium
Susceptibility to jamming	Availability	Loss of situational awareness in VTS/bridge	Medium	High
Overreliance on AIS data	Risk amplifier	Automation errors, unsafe decisions	High	High
Insufficient regulatory requirements	Cross-cutting enabler	Slow adoption of protections, legacy exposure	Medium	High

3. Best Practices and Recommendations

3.1. Cross-verification of AIS data with independent sources

Cross-checking with other sensors (i.e., data fusion) is one of the most practical ways to harden AIS. Because today's AIS lacks built-in authentication and integrity, spoofing, hijacking, and selective jamming are all possible. By comparing AIS with independent sources, you can (a) catch inconsistencies early, (b) keep navigating safely when one feed is dubious, and (c) limit the operational impact of attacks.

1. Fuse radar and AIS on the bridge and at VTS: overlay ARPA/radar plots with AIS targets, and alert on mismatches—track with no return ("ghost ship") or return with no track ("silent vessel"). This flags classic AIS spoofing and "ghost fleets" and follows research recommending radar–AIS correlation to boost reliability.

2. **Cross-check dynamic kinematics against shipboard sensors.** AIS positions/COG/SOG come from GNSS; sanity-check them against inertial sensors, log, gyro and heading change rates. GNSS anomaly-detection methods (e.g., Inertial Navigation System+GNSS integration, C/No monitoring, NMEA-based anomaly detection) help you decide whether to trust the AIS feed, since falsified PNT will propagate into AIS.
3. **Fleet-level consistency checks.** Look for impossible behaviors across vessels (e.g., two ships sharing an MMSI, "ring" patterns, mass coordinate loss). Formal AIS risk analyses recommend checking content plausibility (type vs cargo, draught vs class) and consistency with other ships; industry studies also show you can detect regional GNSS jamming by correlating "position lost" states across many AIS feeds.
4. **Validate statics against registries.** Verify MMSI/IMO/call sign and declared vessel type against authoritative registries, flag changes and mismatches.
5. **AtoN reality checks.** Treat virtual AtoNs with caution: confirm them against radar returns or physical AtoNs/visual bearings. Research notes V-AtoNs are easier to spoof, and combining physical and virtual AtoNs reduces the risk of being misled (Androjna et al., 2021).
6. **Shore-side fusion & anomaly triage.** In VTS, fuse AIS with coastal radar and multi-receiver AIS networks; use voting/multilateration and outlier detection to suppress single-receiver artifacts and tampering before data reaches mariners or public portals. Studies show Internet-facing AIS services have accepted spoofed and modified messages; independent feeds and majority voting prevent a single poisoned source from shaping the picture (Balduzzi et al., 2014).

Cross-verification provides diversity in *physics* (RF ranging vs. radar reflection), *links* (VHF vs. satellite), and *governance* (open broadcast vs. controlled systems like LRIT). That diversity breaks an attacker's assumption that one forged broadcast will be believed everywhere, shortens the time-to-detection of spoofing/jamming, and preserves situational awareness when AIS is degraded (e.g., slot-starvation or frequency-hopping attacks).

3.2. Use of anomaly detection algorithms

Because legacy AIS lacks authentication and integrity checks, adversaries can inject false identities, positions, and voyage data or degrade availability. Anomaly-detection (AD) adds a *behavioral* defense layer that spots and quarantines suspicious data before it misleads bridge teams or VTS.

1. **Catch data/content manipulations early.** Risk assessments of AIS recommend checking plausibility and consistency (e.g., type–cargo mismatches, impossible kinematics, duplicated MMSIs). AD algorithms and filters operationalize this by flagging "impossible with respect to other information" or "unexpectedly changing data," improving the reliability of the recognized maritime picture.
2. **Detect GNSS spoofing/jamming that propagates into AIS.** Modern AD methods monitor GNSS features and message streams used by AIS:
   a) **Signal/receiver features:** carrier-to-noise (C/No) changes and RAIM-style integrity checks help recognize spoofing.
   b) **Protocol-level monitoring:** the low-cost **MANA** framework detects spoofing via NMEA sentence anomaly checks (pairwise distance, clock drift), enabling real-time alerts without new hardware (Spravil et al., 2023).
   c) **Learning-based detectors:** CNN models on vessel GNSS data improve automatic detection of spoofed signals (Raiyn, 2024).
3. **Population-level inference:** Bayesian analysis of AIS messages across many ships reveals *regional* GNSS jamming via correlated "coordinate loss," giving shore-side early warning (Glomsvoll & Bonenberg, 2017).

Provide concrete protection in real incidents. In the Elba (Dec-2019) spoofing case, thousands of message-type-1 reports with *sequential MMSIs* saturated the area. Even simple burst/sequence-pattern AD would have rapidly isolated these streams, preventing CPA alarms and cognitive overload on the bridge/VTS (Androjna et al., 2021).

AD shortens time-to-detection for spoofing/jamming, contains false tracks before they reach decision-support tools, and supports graceful degradation (e.g., fall back to radar/visual/INS when AIS or GNSS looks anomalous). While AD

cannot stop RF-level denial or on-air injection by itself, literature treats it as a *complementary* measure alongside cryptographic hardening (e.g., SecAIS) and interface security.
Performance characteristics are synthesized from reported results in the cited studies and indicate typical trends rather than uniform benchmark values (see Table 2).

Case Illustration: Elba 2019 AIS Spoofing Incident

The AIS spoofing incident reported near the island of Elba in December 2019 provides a concrete illustration of how a defense-in-depth approach can mitigate operational risks even in the absence of protocol-level security. During the incident, thousands of fabricated AIS messages with sequential MMSI numbers created a dense "cloud" of ghost vessels in a confined maritime area, temporarily degrading situational awareness for mariners and shore-based monitoring services. The event demonstrated how unauthenticated AIS broadcasts can be exploited at scale to distort the recognized maritime picture and to overload bridge and VTS displays with false targets.
Applied to this scenario, anomaly detection (AD) mechanisms would have enabled early identification of the spoofing campaign by flagging burst transmissions, sequential MMSI patterns, and implausible traffic densities inconsistent with normal vessel behavior in the Elba region. In parallel, radar–AIS fusion on the bridge and in VTS centers would have revealed systematic mismatches between AIS targets and radar returns (AIS targets without corresponding radar echoes), allowing operators to discount false tracks and maintain safe navigation based on independent sensors. At the shore side, multi-receiver AIS filtering and voting could have reduced the impact of a single compromised or spoofed feed by correlating messages across geographically distributed receivers and suppressing outliers before publishing traffic information to operational systems and public portals.
Finally, the incident highlights the importance of training watchstanders and VTS operators to recognize characteristic signatures of AIS spoofing and to execute documented fallback procedures. Scenario-based training that rehearses responses to sudden bursts of ghost targets—such as reverting to radar-centric navigation, increasing visual lookout, and reporting suspected interference—can preserve safety and continuity of operations even when AIS integrity is compromised. Together, these layered measures demonstrate the practical value of the proposed defense-in-depth framework: while none of the controls alone can prevent RF-level injection, their combined application would have significantly reduced the operational impact of the Elba spoofing event and shortened time-to-detection, thereby preserving maritime situational awareness during the attack.
This illustrative mapping demonstrates the practical applicability of the proposed defense-in-depth framework to real-world AIS spoofing scenarios, even in the absence of empirical simulations in the present study.

3.3. Incorporating authentication and encryption in future AIS protocol

AIS today has no message authentication or confidentiality, enabling identity/position spoofing, AtoN and distress beacons spoofing, slot-level manipulation, and even Internet-side injection; these stem directly from unauthenticated, in-the-clear broadcasts. Cryptographic source authentication would let receivers reject forged frames; encryption would prevent eavesdroppers (and malware C2 channels) from exploiting AIS content.

Table 2. Comparative overview of AIS/GNSS anomaly detection approaches

Method	Detection strength (typical)	False-positive risk	Computational cost	Real-time suitability
Rule-based / heuristics	Low–Medium	Medium	Low	High (shipboard)
Bayesian networks	Medium	Medium	Medium	Medium (shipboard/shore)
CNN (AIS/GNSS features)	High	Medium	High	Low–Medium (mostly shore-side)
Fleet-level statistical AD	High (regional patterns)	Low	Medium–High	Shore-based

Goudosis and Katsikas (2022) propose SecAIS which demonstrates a backwards-compatible way to sign AIS messages using an identity-based maritime PKI (mIBC) built on ECCSI/SAKKE (RFC 6507/6508): receivers verify a sender's signature using only the MMSI (no heavy X.509 exchange), giving broadcast authentication and tamper evidence. Performance tests show feasibility with affordable overhead. SecAIS includes two encrypted modes: (i) SK-IBE-SecAIS to deliver per-recipient secrets over broadcast, and (ii) AES-SecAIS for group encryption once a symmetric key is shared—useful for trusted convoys or high-risk areas (Goudosis & Katsikas, 2020). This addresses use cases where open AIS leaks sensitive data but preserves compatibility with legacy receivers when encryption is not desired. The literature warns that large, distributed transport systems require asymmetric methods and a robust infrastructure; identity-based schemes avoid certificate bloat on a narrowband VHF link. Using open, vetted standards (ECCSI/SAKKE, AES) aligns with best practice and avoids the well-documented failures of proprietary ciphers in radio systems. Independent lines of work (e.g., Auth-AIS using TESLA/Bloom filters (Sciancalepore et al., 2022); pAIS for signed messages (Kessler, 2020)) show message authentication can be added with moderate overhead and software updates, reinforcing that cryptographic hardening is practical.

Even with crypto, jamming/slot-starvation remain RF-layer risks; however, authentication and encryption drastically reduce successful injection and data poisoning—the core weaknesses highlighted by empirical AIS threat studies and incident analyses. They should sit alongside anomaly detection and cross-sensor fusion.

3.4. Regular software and firmware updates for AIS devices

The requirement for routine software and firmware maintenance in Automatic Identification System (AIS) equipment follows directly from broadly adopted cybersecurity regulations, standards, and good practice. AIS stacks—spanning embedded transponders, bridge workstations, and shore-side services—inevitably accumulate implementation defects. Timely updates are therefore the primary control for removing exploitable bugs before they are used to compromise safety-critical navigation functions.

A first principle is host hardening through operating-system patching on bridge systems that process AIS data, including ECDIS, multifunction displays, and radar integrations. Keeping these platforms current closes OS-level exposure created by obsolete services and weak default protections that are routinely targeted by ransomware and remote-code exploits. The same logic extends to Internet-connected components. Software and middleware that transport, parse, or broker AIS messages—particularly on shore—require regular updates to maintain secure defaults and to correct vulnerabilities in parsers or data paths that might otherwise permit crafted or manipulated messages to be accepted. Modern AIS security also depends on features that do not exist without updated code. Source authentication and confidentiality mechanisms, such as schemes exemplified by SecAIS, rely on cryptographic libraries and protocol support delivered through software releases. Maintaining an update cadence is thus the only viable route to deploy, iterate, and sustain these protections so that integrity and confidentiality improve over the equipment's lifetime.

Another concern is the misuse of AIS as a covert channel for command-and-control or as a trigger for malware. Updates that strengthen input validation, tighten protocol conformance, and introduce filtering at trust boundaries materially reduce this risk by hardening interfaces where untrusted messages enter operational technology networks. Given the long service life of maritime systems, the update process itself must be secured. Signed packages, verified installation, and controlled versioning prevent downgrade attacks that would re-introduce known flaws and ensure that security improvements propagate consistently across heterogeneous fleets. Maintaining auditable version histories further supports risk management by allowing operators to verify that minimum supported versions are in force.

Finally, a disciplined update program is an integral element of compliance with maritime cybersecurity guidance from authorities, class societies, and auditing organizations. Embedding patch management in normal operations across bridge, embedded, and shore-side assets demonstrates conformity with industry expectations for cyber-resilience and

provides defensible evidence during assurance activities. In sum, regular, authenticated updates close known vulnerabilities, enable modern cryptographic safeguards, suppress covert-channel abuse, and protect against version downgrades, thereby preserving the integrity and availability of AIS over its extended lifecycle.

3.5. Development of cybersecurity training for crew and port operators

Maritime navigation and port operations have become deeply dependent on interconnected IT/OT systems—especially the Integrated Navigation System (INS), which fuses AIS, GNSS, radar, and ECDIS—and the threat landscape has expanded accordingly. Publicly documented maritime cyber incidents have risen sharply since 2019, spanning GNSS interference, AIS spoofing, ransomware, and compromises of remote access and web services; this pattern, confirmed by sector incident databases, underscores a systemic exposure that cannot be addressed by technology alone and demands sustained, role-specific human training for crews and port operators (Oruc et al., 2025). Training is indispensable because several core maritime radio/communication technologies were not designed with robust security primitives; in many special-purpose wireless systems—including those used in civil transportation domains—common failure modes include missing authentication, missing or broken encryption, protocol design flaws, and implementation weaknesses. In radio systems anyone within range "touches the medium," so procedural detection and response skills are a necessary control layer while technical mitigations mature (Dansarie, 2024).

Within bridge operations, AIS deserves particular attention in training curricula because it is both pervasive in situational awareness and historically unauthenticated. Practical studies and field evidence show that AIS can be spoofed to create "ghost" vessels and false Aids-to-Navigation, hijacked to alter legitimate traffic, or disrupted through timing and slot-reservation abuse—each of which can distort the traffic picture presented to the Officer of the Watch or VTS. These attack classes are well documented and feasible with commodity SDR tooling, making human recognition and procedure-driven cross-checks (e.g., radar/AIS correlation, sanity checks on kinematics, and controlled fallbacks) an operational necessity (Balduzzi et al., 2014). The consequences are not theoretical: a 2019 incident near Elba produced a dense "spoofing cloud" of artificial targets that affected navigation visibility; training that rehearses detection, reporting, and safe-navigation workarounds against such deception measurably improves resilience. Crews should also understand that attackers can misuse AIS as a covert command-and-control channel to steer onboard malware operations in environments without Internet connectivity; recognizing telltale message patterns and knowing escalation paths and containment steps is therefore a crew competence, not only a SOC function.

Training must translate abstract frameworks into watchstanding and port-process behaviors. IMO Resolution MSC.428(98) requires cyber risk management to be embedded in Safety Management Systems; in practice this implies recurring awareness, drills, and competencies tailored to the bridge, engineering, and port/VTS roles rather than generic IT briefings. For bridge teams, scenario-based exercises that couple ECDIS and radar with manipulated AIS/GNSS data teach cross-verification under pressure and reinforce conservative navigation when data sources disagree. For port operators, modules should rehearse responses to manipulated gate/terminal data and OT network anomalies, emphasizing segmentation, least-privilege workflows, and disciplined change management. Evidence from industry interviews and a systematic literature review on INS cybersecurity shows that practitioners face compatibility and cost constraints that delay deployment of advanced technical safeguards; training closes part of this gap by operationalizing best practice, improving anomaly recognition, and tightening incident reporting loops even where tooling is heterogeneous or legacy.

Because special-purpose radio systems were built with availability and interoperability foremost, and because many OT components still run outdated operating systems, human factors are often the last reliable barrier. Crew and port training should therefore internalize the characteristic signatures of spoofing and jamming across AIS/GNSS, the limitations of middleware and OS baselines on ECDIS/RADAR/MFDs, and the procedures for safe fallback, logging, and notification. The wider security literature synthesizes these weaknesses into recurring themes—absent authentication, absent

encryption, protocol/implementation flaws—making structured education a first-line mitigation until secure-by-design replacements are broadly fielded. In parallel, trainees should be introduced to emerging authenticated/encrypted AIS concepts (e.g., identity-based cryptography overlays that add source authentication and confidentiality without replacing the legacy broadcast), so that organizations can plan for transition and so operators understand what benefits to expect when such capabilities are piloted. In sum, cybersecurity training tailored to crews and port operators is not ancillary to technical hardening; it is the mechanism that turns standards and controls into navigational discipline and port-process reliability. Rising incident counts and concrete case studies validate that well-rehearsed human responses—cross-checking sensors, recognizing spoofing cues, invoking documented fallbacks, and escalating coherently—are essential to maintaining safety and continuity in a domain where adversaries can inject falsehoods over the air and exploit legacy constraints on the bridge and at the quayside.

3.6. Defense-in-depth strategies for maritime communication systems

Maritime communication systems—VHF/MF/HF radio and DSC, GMDSS satellite services, AIS/VDES, NAVTEX, LRIT, and VTS data links—are foundational to safety and business continuity. They are also governed by safety and security obligations, notably SOLAS Chapter IV for radiocommunications and the Global Maritime Distress and Safety System (GMDSS), which was modernized with amendments entering into force on 1 January 2024. Those amendments acknowledged evolving technologies while preserving core reliability requirements for distress, safety, and general communications (IMO, 2025.2), (ClassNK, 2025), (Eagle.org, 2025). A defense-in-depth approach is therefore essential: multiple, mutually reinforcing layers must prevent, detect, and contain cyber-physical failures without compromising the availability of distress and safety services.

Cyber risk management is now an explicit part of the Safety Management System: IMO's **Guidelines on maritime cyber risk management** (MSC-FAL.1/Circ.3/Rev.3, 4 April 2025) call for organization-wide cyber governance, risk assessment, controls, training, and continuous improvement, and are intended to be integrated with existing safety processes rather than run in parallel (IMO, 2025.1). For newbuilds and onboard systems, the International Association of Classification Societies mandates cyber resilience through **UR E26** (ship-level) and **UR E27** (equipment-level), applicable to ships contracted from 2024/2025 and refined through 2024–2025 updates; these requirements harden architectures, interfaces, and maintenance practices with verification by class.

In ports and at the ship–shore interface, European operators fall under the **NIS2 Directive**, which imposes risk-management measures and incident reporting for essential and important entities, with sector guidance from ENISA (2025) and port-specific handbooks from IAPH. In the United States, the Coast Guard's **final rule on Cybersecurity in the Marine Transportation System** (July 2025) establishes minimum mandatory cybersecurity measures for MTSA-regulated facilities and vessels, building on NVIC 01-20 (United States Coast Guard, 2025)(*Final Rule*, n.d.). Across sectors, organizations can align defenses with **NIST CSF 2.0**—now structured around the functions *Govern, Identify, Protect, Detect, Respond, Recover*—and with the **Cross-Sector Cybersecurity Performance Goals (CPGs)** that prioritize a baseline of high-impact actions for critical infrastructure ('NIST Releases Version 2.0 of Landmark Cybersecurity Framework', 2024).

Defense-in-depth for maritime communications starts with architectural separation. The **IEC/ISA 62443** family formalizes **zones and conduits** to isolate assets with similar security requirements and to strictly control flows between them—an approach that fits radio, satcom, and navigation networks as much as terminal OT. Applying 62443 at system design and retrofit phases yields enforceable boundaries between bridge networks, radio racks, ECDIS/INS, engine/automation, cargo systems, and shoreside interfaces. Practical guidance converges on three steps. First, perform a system-under-consideration assessment (IEC 62443-3-2), partition into zones, and assign **target security levels**; second, implement technical requirements at the system level (IEC 62443-3-3) and component level (IEC 62443-4-2) including authenticated services, hardened protocols, and secure boot; third, map access pathways into **conduits** with filtering, inspection, and logging. ANSI Web-

storeIndustrial Cyber CISA's CPGs operationalize this for mixed IT/OT estates: enforce **segmentation between IT and OT**, default-deny on OT conduits, and mediated remote access.

3.7. Policy and regulatory enhancements

Policy and regulatory enhancements raise the security floor for AIS by turning good practice into enforceable requirements across ship, shore, and supply chains. Integrating cyber risk management into the Safety Management System through IMO's updated Guidelines (MSC-FAL.1/Circ.3/Rev.3, 4 April 2025) and Resolution MSC.428(98) compels operators to assess AIS-related risks, define procedures for anomalies, and embed training and maintenance into audited processes. Equipment-level rules such as IACS UR E27 require cyber-resilient onboard systems—secure development, hardening features, and update mechanisms—that can be applied directly to AIS transponders and gateways. Standards bodies can further strengthen resilience by updating radio recommendations: ITU-R M.1371 defines AIS today, while the VDES framework in ITU-R M.2092 provides the vehicle to incorporate authenticated or protected modes; policy direction and procurement mandates can accelerate adoption of such security extensions proposed in recent research (*Maritime Cyber Risk*, n.d.), ('UR E27 Rev1', n.d.), (*M.1371 : Technical Characteristics for an Automatic Identification System Using Time Division Multiple Access in the VHF Maritime Mobile Frequency Band*, n.d.), (*M.2092 : Technical Characteristics for a VHF Data Exchange System in the VHF Maritime Mobile Band*, n.d.).

National and regional regulations close remaining gaps by imposing minimum controls, governance, and reporting. The U.S. Coast Guard's 2025 final rule for the Marine Transportation System establishes mandatory cybersecurity plans, designated officers, and incident response expectations that cover communications and navigation equipment; in the EU, NIS2 and sector guidance from ENISA push essential entities, including maritime operators and ports, to implement risk management, incident reporting, and supplier assurance that encompass AIS data paths and services. IALA guidance reinforces that networked AIS systems must adopt common Internet cybersecurity measures, aligning VTS and coastal infrastructure with these requirements. Together, these measures harmonize expectations, drive secure-by-design features into AIS products, ensure timely patching and configuration control, and create accountability for the integrity and availability of AIS information across the whole distribution chain.

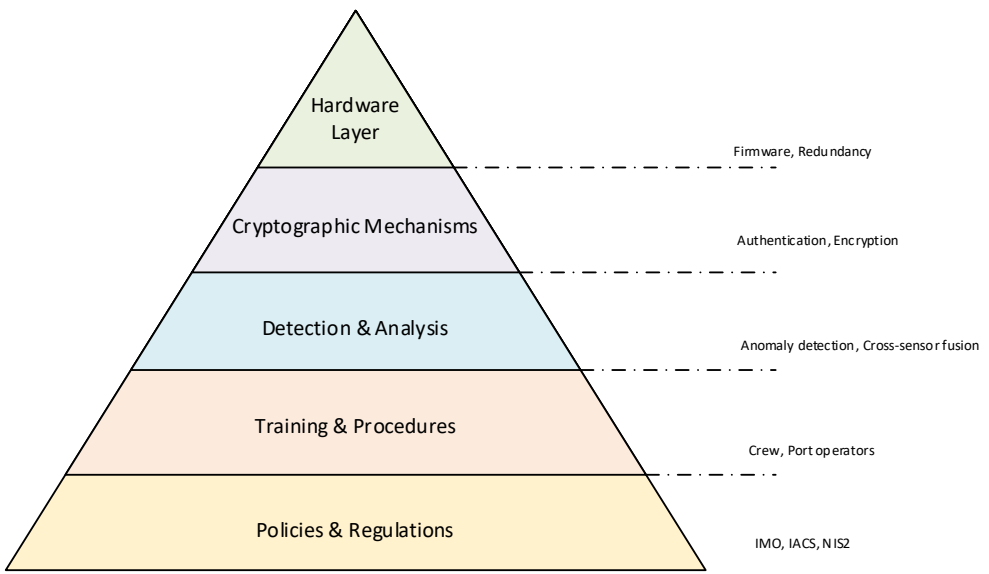

Fig. 3. Defense-in-Depth Layers for AIS Security

3.8. Encouraging research on secure alternatives to legacy AIS

Encouraging research on secure successors and overlays to legacy AIS strengthens cyber resilience by addressing the protocol's root weaknesses—open, unauthenticated broadcasts with no integrity protection—which have been shown to enable practical spoofing and data tampering. A rigorous research pipeline provides the evidence needed to update requirements, quantify trade-offs between security and availability, and guide standards bodies and regulators toward options that preserve safety-of-life functions while preventing false data from being accepted by default. This aligns with the IMO's mandate to manage cyber risk within the Safety Management System and helps translate "good practice" into implementable, auditable measures for ship and shore.

Focused investigation also accelerates viable migration paths. Prototypes such as **Auth-AIS** demonstrate backward-compatible broadcast authentication using lightweight cryptography, offering a software path to verifiable origin and tamper evidence, while the **VDES** framework (ITU-R M.2092) defines a higher-capacity VHF data system within which authenticated or protected application traffic could be carried alongside legacy services. Complementary work—e.g., integrity-assured distribution and auditing of AIS data—broadens the toolbox for coastal networks and data providers. A healthy research ecosystem around these alternatives gives industry and authorities practical designs to trial, performance data to compare, and interoperability guidance to incorporate into future revisions of ITU-R/IALA recommendations and procurement baselines.

4. Conclusions

AIS remains foundational to maritime safety and traffic services, but its legacy design leaves it critically exposed: broadcasts are unencrypted and unauthenticated, messages have no integrity or freshness checks, and the system is vulnerable to spoofing, false-data injection, replay, and straightforward RF jamming. As AIS is fused into ECDIS, VTS, and automation, these weaknesses scale into operational risk, amplified by regulatory gaps and a common tendency to over-trust AIS without cross-validation. Treating AIS as authoritative data invites navigational errors, service disruption, and adversary exploitation.

Further work must move decisively beyond incremental mitigations. Priorities include backward-compatible source authentication and confidentiality for AIS/VDES; robust anomaly detection and fleet-level analytics; systematic cross-sensor fusion and multilateration; secure development and update pipelines for shipboard and shore equipment; and role-specific cybersecurity training for bridge and port personnel. These technical advances should be anchored in enforceable standards and regulation (IMO/ITU/IACS and national authorities) and validated through pilots, performance measurement, and safety cases. Only by combining protocol hardening with defense-in-depth and governance reforms can the community reduce AIS's attack surface while preserving its safety-of-life mission.

Acknowledgments

This study was funded by the Gdynia Maritime University, under the research project: WN/2026/PZ/07.

References

1. Androjna, A., Perkovič, M., Pavic, I., & Mišković, J. (2021). AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Applied Sciences*, *11*(11), Article 11. https://doi.org/10.3390/app11115015
2. Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A security evaluation of AIS automated identification system. *Proceedings of the 30th Annual Computer Security Applications Conference*, 436–445. https://doi.org/10.1145/2664243.2664257
3. Banyś, P., Gucma, M., & Fowdur, J. S. (2024). Assessment of Possible Misidentification of AIS Transponders within AIS Data due to Bit Inversions of MMSI. *Naše More*, (71(1)), 30–37. https://doi.org/10.17818/NM/2024/1.5
4. Benterki, A. S., Visky, G., Vain, J., & Tsiopoulos, L. (2025). Using Incremental Inductive Logic Programming for Learning Spoofing Attacks on Maritime Automatic Identification System Data. In S.

Bauk (Ed.), *Maritime Cybersecurity* (pp. 123–141). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-87290-7_7
5. Chang, T.-H., Kao, S. L., Chou, C.-C., & Chang, H. C. (2025). Genetic Algorithm for Ship Robbery Emergency Reporting System. *TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation*, *19*(2), 609–615. https://doi.org/10.12716/1001.19.02.33
6. Cichocki, R., & Wójcik, P. (2025). Cybersecurity in Maritime Transport Systems: Threats, Trends, and Countermeasures in the Last Decade. *TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation*, *19*(3), 715–722. https://doi.org/10.12716/1001.19.03.03
7. Dansarie, M. (2024). Security Issues in Special-Purpose Digital Radio Communication Systems: A Systematic Review. *IEEE Access*, *12*, 91101–91126. https://doi.org/10.1109/ACCESS.2024.3420091
8. Emmens, T., Amrit, C., Abdi, A., & Ghosh, M. (2021). The promises and perils of Automatic Identification System data. *Expert Systems with Applications*, *178*, 114975. https://doi.org/10.1016/j.eswa.2021.114975
9. *Final Rule: Cybersecurity in the Marine Transportation System – Implementation Timeline*. (n.d.). United States Coast Guard News. Retrieved 11 August 2025, from https://www.news.uscg.mil/maritime-commons/Article/4247529/final-rule-cybersecurity-in-the-marine-transportation-system-implementation-tim/
10. Glomsvoll, O., & Bonenberg, L. K. (2017). GNSS Jamming Resilience for Close to Shore Navigation in the Northern Sea. *The Journal of Navigation*, *70*(1), 33–48. https://doi.org/10.1017/S0373463316000473
11. Goudosis, A., & Katsikas, S. (2020). Secure AIS with Identity-Based Authentication and Encryption. *TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation*, *14*(2), 287–298. https://doi.org/10.12716/1001.14.02.03
12. Junaidi, A., Yudo, H., & Ab-Samat, H. A. (2024). Identify the Trends on Maritime Safety Management System Studies: A Review. *TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation*, *18*(4), 775–784. https://doi.org/10.12716/1001.18.04.03
13. Kessler, G. C. (2020). Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity. *TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation*, *14*(2), 279–286. https://doi.org/10.12716/1001.14.02.02
14. Lázaro, F., Raulefs, R., Bartz, H., & Jerkovits, T. (2023). VDES R-Mode: Vulnerability analysis and mitigation concepts. *International Journal of Satellite Communications and Networking*, *41*(2), 178–194. https://doi.org/10.1002/sat.1427
15. *M.1371: Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band*. (n.d.). Retrieved 25 February 2026, from https://www.itu.int/rec/R-REC-M.1371
16. *M.2092: Technical characteristics for a VHF data exchange system in the VHF maritime mobile band*. (n.d.). Retrieved 25 February 2026, from https://www.itu.int/rec/R-REC-M.2092
17. *Maritime cyber risk*. (n.d.). Retrieved 25 February 2026, from https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx
18. Neumann, T. (2024). Cybersecurity in Maritime Industry. *TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation*, *18*(4), 765–774. https://doi.org/10.12716/1001.18.04.02
19. NIST Releases Version 2.0 of Landmark Cybersecurity Framework. (2024). *NIST*. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework
20. Oruc, A., Kavallieratos, G., Gkioulos, V., & Katsikas, S. (2025). Perspectives on the Cybersecurity of the Integrated Navigation System. *Journal of Marine Science and Engineering*, *13*(6), 1087. https://doi.org/10.3390/jmse13061087
21. Raiyn, J. (2024). Maritime Cyber-Attacks Detection Based on a Convolutional Neural Network. In M. E. Cornejo, L. T. Kóczy, J. Medina, & E. Ramírez-Poussa (Eds), *Computational Intelligence and*

Mathematics for Tackling Complex Problems 5 (pp. 115–122). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-46979-4_16
22. Sciancalepore, S., Tedeschi, P., Aziz, A., & Di Pietro, R. (2022). Auth-AIS: Secure, Flexible, and Backward-Compatible Authentication of Vessels AIS Broadcasts. *IEEE Transactions on Dependable and Secure Computing*, *19*(4), 2709–2726. https://doi.org/10.1109/TDSC.2021.3069428
23. Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2024). Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. *Applied Ocean Research*, *142*, 103855. https://doi.org/10.1016/j.apor.2023.103855
24. Spravil, J., Hemminghaus, C., von Rechenberg, M., Padilla, E., & Bauer, J. (2023). Detecting Maritime GPS Spoofing Attacks Based on NMEA Sentence Integrity Monitoring. *Journal of Marine Science and Engineering*, *11*(5), 928. https://doi.org/10.3390/jmse11050928
25. Steiner, J., Havlíček, J., Duša, T., & Heinrichs, G. (2023). The Vulnerability of Inland Waterway AIS to GNSS Radio Frequency Interference. *Engineering Proceedings*, *54*(1), 26. https://doi.org/10.3390/ENC2023-15461
26. Stupak, T. (2014). Influence of Automatic Identification System on Safety of Navigation at Sea. *TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation*, *8*(3), 337–341. https://doi.org/10.12716/1001.08.03.02
27. Sun, J., Yi, Z., Zhuang, Z., & Jiang, S. (2025). Securing Automatic Identification System Communications Using Physical-Layer Key Generation Protocol. *Journal of Marine Science and Engineering*, *13*(2), 386. https://doi.org/10.3390/jmse13020386
28. Svanberg, M., Santén, V., Hörteborn, A., Holm, H., & Finnsgård, C. (2019). AIS in maritime research. *Marine Policy*, *106*, 103520. https://doi.org/10.1016/j.marpol.2019.103520
29. Tsiopoulos, L., & Vaarandi, R. (2025). A Scope Review of Secure Broadcasting Protocols for the Automatic Identification System. In S. Bauk (Ed.), *Maritime Cybersecurity* (pp. 103–121). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-87290-7_6
30. UR E27 Rev1. (n.d.). *Safer and Cleaner Shipping - IACS*. Retrieved 25 February 2026, from https://iacs.flumeserver.co.za/publications/ur-e27-rev1/
31. Wimpenny, G., Šafář, J., Grant, A., & Bransby, M. (2022). Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility. *The Journal of Navigation*, *75*(2), 333–345. https://doi.org/10.1017/S0373463321000837