engineering proceedings

MDPI

*Proceeding Paper*

# Satellite Navigation in Safety-Critical Decision Making †

**Wili Helenius, Hanna Kajander ‡ and Janne Lahtinen ***

Faculty of Logistics and Maritime Technology, Satakunta University of Applied Sciences, 28100 Pori, Finland; wili.helenius@samk.fi (W.H.); hanna.kajander@fintraffic.fi (H.K.)

* Correspondence: janne.lahtinen@samk.fi; Tel.: +358-447103805

† Presented at the European Navigation Conference 2025 (ENC 2025), Wrocław, Poland, 21–23 May 2025.

‡ Current address: Fintraffic, PL 71, 00241 Helsinki, Finland.

**Abstract**

GPS GNSS position signal manipulation in shipping can lead to significant navigational challenges. Such disruptions may result from various factors, including atmospheric conditions, satellite malfunctions, or intentional positioning satellite signal disturbance. Impacts on shipping operations include delays, increased operational costs, and safety risks for crews and vessels. Understanding these disturbances and their implications is crucial for enhancing maritime safety and efficiency. Common causes of GNSS disturbances in shipping include atmospheric effects such as ionospheric and tropospheric delays, satellite signal obstructions due to terrain or buildings, satellite malfunctions or failures, and intentional interference like jamming. These factors can lead to inaccuracies in positioning, affecting navigation and safety. GPS signals are vulnerable to various cyber threats, including spoofing, jamming, and signal interference. Spoofing involves sending counterfeit GPS signals to mislead receivers, while jamming disrupts the legitimate signals. Ensuring the integrity and security of GPSs is crucial for applications like navigation, timing, and critical infrastructure. Advanced encryption and authentication methods can help safeguard the security of GPS signals. These vulnerabilities can have profound implications for navigation systems and critical infrastructure. Enhancing GPS security requires a combination of advanced technologies and policies to improve signal integrity and authentication processes. The Global Positioning System (GPS) is the most widely used GNSS positioning method in commercial shipping. Moreover, deliberate disturbance technical birth mechanisms are similar across the field of GNSS systems. Therefore, this study focuses on the deliberate disturbance of the GPS, recognising the ability to upscale the research results to other commonly used GNSSs such as Beidou, Galileo, and Glonass. This paper introduces a behavioural approach to enhancing cybersecurity and preparedness to external threats in commercial shipping through European collaboration in the CyberSEA project.

**Keywords:** navigation; positioning; global positioning system; global navigation satellite system; disturbance; security

Check for updates

Academic Editor: Tomasz Hadaś

Published: 13 April 2026

**Copyright:** © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

## 1. Introduction

It is generally known that the shipping industry regularly experiences negligent disturbance of global satellite navigation systems, mainly focusing on the GPS signal [1]. Preparation for threats to ships' positioning system disturbance is increasingly important as integrated bridges have multiple systems relying on accurate and dependable GPS positioning signal input. Vessels navigating in congested waters and inland waterways may experience manipulation of longitudinal and transverse vessel position. Manipulating the GPS signal has a

high potential to lead to severe accidents that jeopardise the vessel, crew, cargo, and marine environment, thus having operational, environmental, and economic impacts.

SOLAS (Safety Of Life At Sea) is an IMO (International Maritime Organization) convention that merges the ISM (International Safety Management) and ISPS (International Ships and Port Security) codes, thus integrating both internal and external aspects into safety and security onboard [2].

Third, the safety management system is a mandatory requirement that, as dictated by the ISM code [3], must be facilitated by the shipping company. The shipping company's safety management system is the sole documentation that states how internal or external threats must be responded to. The safety management system is for the vessel crew to implement, and the shipping company's responsibility is to supervise how the safety management system is practically followed.

Based on the above, the safety management system is a crucially important tool that acts as the pathway onboard to enhance security and safety. Preparing for GPS spoofing and jamming presents navigators with novel knowledge-based challenges that require new, fast-adapting, and agile learning tools to respond to the needs dictated by the migrating security landscape.

This paper focuses on the tools enhancing preparedness for the manipulation of GPS positioning.

## 2. Project CyberSEA

Project CyberSEA is a multinational, Erasmus+ co-funded project fostering a group of maritime and cybersecurity professionals. The project team consists of European research institutions. Research group members include Satakunta University of Applied Sciences (Rauma, Finland), Polytechnic University of Catalonia (Spain), Berlin School of Business and Innovation (Germany), Centre for Factories of the Future (Sweden), Maritime University of Szczecin (Poland), Hellenic Mediterranean University (Greece), Spinaker (Slovenia), IDEC SA (Greece), and Mircea cel Bătrân Naval Academy (Romania). Project CyberSEA aims to enhance cybersecurity in the maritime industry through an online training tool for students, actively serving seafarers, and relevant onshore personnel. Educational material facilitated by the project team consists of the latest knowledge, presenting the focal points of cybersecurity aspects in terms of safety-critical shipping operations. A current research directions is the deliberate disturbance of a satellite's positioning and its effect on navigation. The project's online laboratory unites students, both onboard and from various countries, to jointly seek ideal responses to the emerging threat of deliberate GPS signal disturbance.

## 3. Literature Review

The literature review discusses relevant authors in maritime cybersecurity in GNSS manipulation regarding maritime safety and security concepts.

### *3.1. Safety and Security*

The ISM code and its tools to avoid unwanted outcomes focus on two concepts [3]. First, safety refers to threats that emerge from safety culture, which refers to the rationale of our behaviour in safety-critical operations [4]. It is essential to understand that the ISM code and the concept of safety focus on behavioural aspects through the intended vessel's crew implementation [5]. Security as part of the ISPS code refers to threats that emerge from the actions of external parties [6]. External threats have root causes beyond the effects of the vessel crew or shipping companies. An entity with malicious intent towards the vessel or the shipping company cannot be stopped or hindered by the shipping company's actions. Therefore, the only way to enhance security is through preparation

for a cybersecurity attack. Generally, there are two ways of achieving this goal. First, the increased situational awareness of the cybersecurity climate provides time to counteract, for example, when navigating in congested waters. Second, correct crew actions are required when, for example, the GPS positioning of the vessel is manipulated.

### 3.2. Risk Management

Risk management steps start with recognizing hazards and defining risks and the associated criticality, followed by mitigating actions to control the risks identified. After the controls are in place, the residual risk indicates the efficiency of the risk management process. It is generally understood that associated risks cannot be managed if the hazard is not recognised. The above emphasises the timely recognition of hazards related to the positioning of the vessel [7].

### 3.3. Role of GPS Position Information

First, in their bachelor's thesis study on GPS signal jamming, Lindroth and Falk indicated that high reliance on position information is a risk. Interestingly, rather than suspecting positioning data manipulation, the vessel crew more likely suspect that the navigation marks have drifted. This means that the navigator thinks that a drifting navigation mark explains the difference between the radar image and the electronic chart. Notably, a lack of landmarks or other known fixed targets in open waters hinders the possibility of using radar as a reference against the electronic chart information [8].

Second, peer-reviewed research from 2021, conducted by Wu et al., supports Lindroth and Falk's findings. Over-reliance on technology poses a relevant risk in navigation [9].

Third, research on the construction of onboard situational awareness by [7].reveals the level of GPS usage in navigation. Navigators' situational awareness combines data collected from radar, the ECDIS (Electronic Navigation Display and Information System), the AIS, and visual observations [7]. However, the weighing of these information sources depends on individual preferences and work culture. With this in mind, the navigator practices what they learned, and the learned onboard working culture paves the way toward balanced use of information without overreliance on any single source of information [10].

Finally, Orban concludes that although GNSSs have inbuilt mechanisms to reveal degraded signal accuracy, these systems are not able to differentiate between deliberate and natural error causes. Therefore, the technical aspect dictates the sole importance of the GPS signal [11,12]. AIS requires a GPS signal for positioning and a gyro compass for automatic latitude correction. The alteration of behavioural aspects will not impact the imminent technical overreliance on the GPS signal.

## 4. Research Methods

Research consisted of multiple phases, each with an individual applied research method. First, a thorough mapping of prevailing cybersecurity vulnerabilities and threats in the maritime sector was conducted. This was performed by collecting a list of relevant maritime cybersecurity vulnerabilities from each CyberSEA project partner.

Second, a review of the best maritime industry practices was conducted. In this part, all project partners mentioned practical approaches as best industry practices in tackling cybersecurity challenges in shipping. Various companies and individuals onboard and ashore were contacted globally to list approaches to safeguarding onboard operations. All partners gathered a national focus group to validate the work conducted so far. These first two parts of the research provided a foundation for developing training materials and protocols for onboard cybersecurity.

https://doi.org/10.3390/engproc2026126048

Third, the project partners established a training curriculum. Again, a focus group validated the curricula. Next, the project partners established an e-learning platform allowing student attendance regardless of their physical location. The e-learning platform is based on the learning material focal points, such as GPS position in navigation and GPS signal manipulation. Every partner established a national e-learning section as part of a larger training context. All created e-learning material was uploaded to an online hub computer in Greece. This computer summarises all the e-learning material and allows students to log in to join the cybersecurity training course.

*Navigation Simulation*

A navigation training simulator is located at Satakunta University of Applied Sciences in Rauma, Finland. Navigation simulation serves as the basis for the Finnish E-learning platform. A fairway navigation scenario was established to simulate the effects of GPS signal manipulation on navigation safety.

## 5. Research

In the testing scenarios conducted in the simulation environment at Satakunta University of Applied Sciences, the vessel position was moved in four different directions, simulating negligent manipulation of the GPS signal. Training scenarios 1–4 detail the arrangement and visualise the results.

### *5.1. Training Scenario 1*

In training scenario 1, the vessel's position was manipulated with an offset of 100 m in the 021° direction (to port) from her real position. The manipulated ship's position is illustrated in Figure 1, left. The ship's outline is illustrated with a black line. The simulator instructor's ECDIS view (middle—not visible to the navigator) and the associated radar image (right—not visible to the navigator) show the real vessel's position.

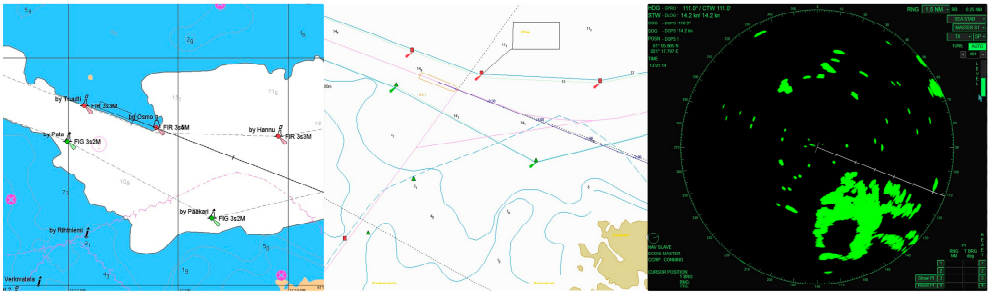


**Figure 1.** Training scenario 1 (Janne Lahtinen 2025).

### *5.2. Training Scenario 2*

In training scenario 2, the vessel's position was manipulated with an offset of 100 m in the 111° direction (ahead) from her real position. The manipulated ship's position is illustrated in Figure 2, left. The ship's outline is illustrated with a black line. The simulator instructor's ECDIS view (middle—not visible to the navigator) and the associated radar image (right—not visible to the navigator) show the real vessel position.

https://doi.org/10.3390/engproc2026126048

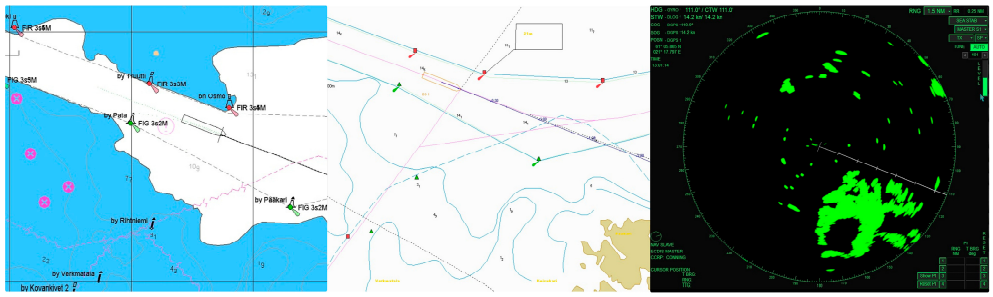


**Figure 2.** Training scenario 2. Janne Lahtinen 2025.

### *5.3. Training Scenario 3*

In training scenario 3, the vessel's position was manipulated with an offset of 100 m in the 201° direction (to starboard) from her real position. The manipulated ship's position is illustrated in Figure 3, left. The ship's outline is illustrated with a black line. The simulator instructor's ECDIS view (middle—not visible to the navigator) and the associated radar image (right—not visible to the navigator) show the real vessel position.

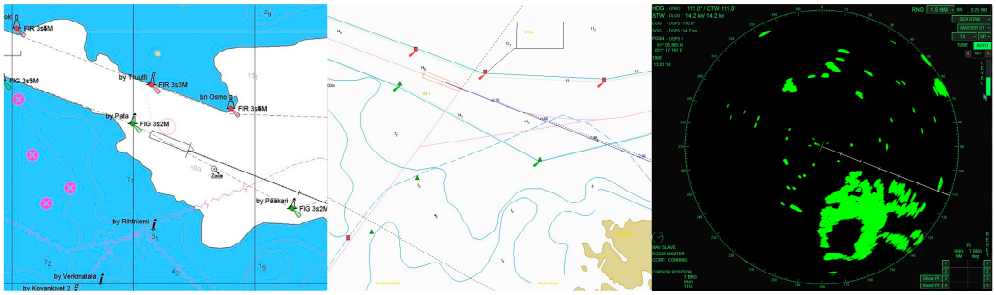


**Figure 3.** Training scenario 3. Janne Lahtinen 2025.

### *5.4. Training Scenario 4*

In training scenario 4, the vessel's position was manipulated with an offset of 100 m in the 291° direction (aft) from her real position. The manipulated ship's position is illustrated in Figure 4, left. The ship's outline is illustrated with a black line. The simulator instructor's ECDIS view (middle—not visible to the navigator) and the associated radar image (right—not visible to the navigator) show the real vessel position.

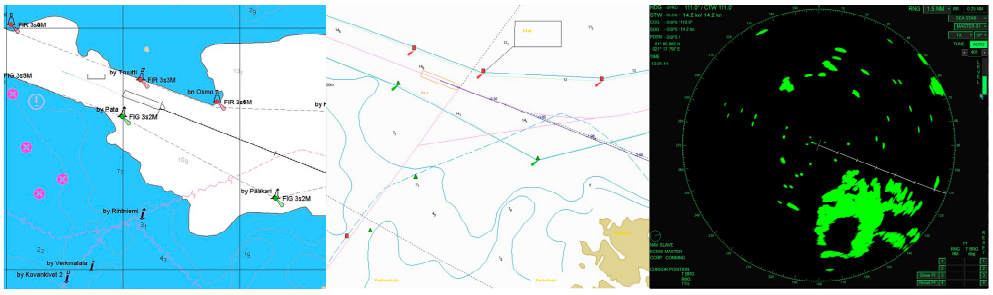


**Figure 4.** Training scenario 4. Janne Lahtinen 2025.

Figure 5 below illustrates the navigator's visual view through the vessel's forward bridge windows in the above-mentioned scenarios.



**Figure 5.** Navigator view from the bridge. Janne Lahtinen 2025.

## 6. Results

In training scenarios 2 and 4, above-mentioned, the vessel's manipulated position remained in the fairway area. Consequently, the vessel's manipulated position in training scenarios 1 and 3 was partially or entirely outside the fairway area. It is generally understood from Figures 1–4 that when the vessel's manipulated position is outside the fairway area, the navigator may realise the offset position with a glance at the ECDIS. In turn, it is challenging for the navigator to realise the position offset when the vessel position is manipulated along the fairway to the aft or ahead. Failure to take timely actions on the WOP (wheel over point) may lead to the vessel migrating outside the fairway area and potentially grounding.

## 7. Discussion

The research and associated simulation training scenarios reveal the importance of situational awareness in navigation in congested waters. According to ref [8], the lack of using visual navigation aids hinders the safety of shipping in congested waters, while according to ref [9], this is due to an overreliance on navigation technological aids.

Ref [4] explain safety as a status of the operation emerging from human actions. In turn, as per the ISPS code (2021) [6], security or lack of security emerges from the actions of external actors. In the case of a malicious act towards vessel navigation safety, such as the manipulation of the GPS signal, the magnitude or frequency of the manipulation cannot be controlled.

In light of all of the above, there are three factors to consider when a safer way of navigation is sought in a geopolitically unforeseeable environment, where GPS signal manipulation is frequent and to be expected.

First, the concept of cyber safety must become commonplace in shipping. Traditionally, in shipping, security encompasses preparing for the unexpected and using tools when an external threat has readily escalated. Similarly to how unsafe pen drives should not be used in bridge computers, GPS signal manipulation must be accepted as an ever-present threat.

Second, navigation should emphasize the constanct questioning of the reliability of the GPS signal. Currently, GPS signal reliance is overwhelming. It is generally understood that the GPS signal is required by a number of bridge systems along with the vessel's positioning systems. For example, practically all gyro compasses today have an automated latitude error correction. The gyro compass requires the latitude input from the GPS to enable the latitude correction calculation. Therefore, the manipulation of the GPS signal may lead to the failure of the gyro compass and thus a loss of vessel heading information. If the Global Maritime Distress and Safety System does not have the correct position of the vessel, then false positions are used in, for example, distress calls. Moreover, distress calls will have no effect if the position is lost altogether. The AIS (Automatic Identification System) sends the vessel's manipulated position to the surrounding environment. Other vessels and VTS stations could then see a false vessel position. This technical overreliance is rooted in the design of the navigation systems. This calls for increased need for supervision of GPS signal quality, particularly in areas like the northern Baltic Sea.

https://doi.org/10.3390/engproc2026126048

Third, ARPA (Automatic Radar Plotting Aid) radar must be used more actively in navigation. Radar is a tool that provides navigators with information solely based on their vessel equipment. Apart from gyro compass information for the heading, nothing originates from outside the radar equipment. Therefore, a chart overlay should be used on your radar screen to see the difference between radar and ECDIS views. Whenever the distances to external radar echoes differ from those of the ECDIS, you can rely on the incorrect ECDIS. Consequently, all onboard equipment and their associated DGPS inputs should be checked. Moreover, in navigation in congested waterways, such as archipelagic waters, parallel indexing tools in radar should facilitate safe passing distances to fixed targets such as islands and navigational marks.

Finally, in maritime training, the training curricula should consider the geographical variances in manipulating GPS signals. In the northern part of the Baltic Sea, GPS signal manipulation is frequent, while in many equatorial areas, sunspots and solar activity are the leading causes for GPS signal offsets. It is generally understood that the birth mechanism of the naturally caused offset and manipulation differs. With this in mind, the operational vigilance and the actions to take in the event of GPS disturbance must be carefully reconsidered, and the results must be integrated into maritime training curricula.

**Author Contributions:** Conceptualization, J.L.; Methodology, J.L.; validation, J.L.; investigation, J.L., H.K. and W.H.; Writing- original draft preparation, J.L.; writing, review and editing, J.L.; visualization, J.L.; supervision, J.L., H.K. and W.H.; project administration, J.L., H.K. and W.H. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The data presented in this study are available upon request from the corresponding author.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| ARPA | Automatic Radar Plotting Aid |
| DGPS | Differential Global Positioning System |
| ECDIS | Electronic Chart Display and Information System |
| GNSS | Global Navigation Satellite System |
| GPS | Global Positioning System |
| IMO | International Maritime Organization |
| ISM | International Safety Management |
| ISPS | International Ship and Port Facility Security |
| RADAR | Radio Aided Detection and Ranging |
| SOLAS | Safety Of Life At Sea |

## References

1. Charitou, N. Understanding and Mitigating GPS Spoofing Attacks in Shipping. Master's Thesis, University of Piraeus, Piraeus, Greece, 2025.
2. International Maritime Organization. *Safety of Life at Sea*, 7th ed.; International Maritime Organization: London, UK, 2020.
3. International Maritime Organization. *International Safety Management Code*, 3rd ed.; International Maritime Organization: London, UK, 2010.
4. Reiman, T.; Pietikäinen, E.; Oedewald, P. *Turvallisuuskulttuuri-Teoria ja Arviointi*; VTT Technical Research Centre: Espoo, Finland, 2008.

5. Rinaldy, D.Y. Reliability of International Safety Management (ISM) Code Implementation in Operational Risk Management of Shipping Industry. In Proceedings of the International Conference on Economics Business and Government Challenges, Surabaya, Indonesia, 21–22 July 2022.
6. International Maritime Organization. *Guide to Maritime Security and the ISPS Code*; International Maritime Organization: London, UK, 2021.
7. Lahtinen, J.; Valdez-Banda, O.; Kujala, P.; Hirdaris, S. Remote piloting in an intelligent fairway—A paradigm for future pilotage. *Saf. Sci.* **2020**, *130*, 104889. [CrossRef]
8. Lindroth, N.; Falk, A. GPS Spoofing at Sea. Bachelor's Thesis, Chalmers University of Technology, Gothenburg, Sweden, 2018.
9. Wu, J.; Thorne-Lange, J.; Zhang, P. Safety First: The Risk of Over-Reliance on Technology in Navigation. *J. Transp. Saf. Secur.* **2022**, *14*, 1220–1246. [CrossRef]
10. Lahtinen, J.; Valdez-Banda, O.; Kujala, P.; Hirdaris, S. The Risks of Remote Pilotage in an Intelligent Fairway—Preliminary considerations. In *Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC)*; Aalto University: Espoo, Finland, 2019; pp. 48–57.
11. Medina, D.; Lass, C.; Marcos, E.; Ziebold, R.; Closas, P.; Garcia, J. On GNSS Jamming Threat from the Maritime Navigation Perspective. In *Proceedings of the 22th International Conference on Information Fusion (FUSION)*; Curran Associates, Inc.: Red Hook, NY, USA, 2019.
12. Orban, J. Overview of GNSS Interference Risks in Transport Safety and Resilient Responses. In *Proceedings of the Sustainable Mobility and Transportation Symposium 2025, Győr, Hungary, 16–18 October 2025*; MDPI: Basel, Switzerland, 2025.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.