INTERTANKO

Jamming and Spoofing of Global Navigation Satellite Systems (GNSS) (2nd Edition)

TWENTY 25

Jamming and Spoofing of Global Navigation Satellite Systems (GNSS) 2nd Edition

Contents

Foreword

Global Navigational Satellite Systems (GNSS) are supreme navigational aids which, if used wisely, will greatly contribute not just to navigational safety, but can also help to minimise bridge workload. While GNSS position data feed to ECDIS has transformed the face of navigation and bridge team habits, it has introduced risks which must not be disregarded. The dependence on stability and accuracy of a GNSS signal has led to complacency and overreliance on satellite positioning, eroding watch officers' attitude, experience, and competence of navigating in a GNSS-compromised environment.

All of this can leave the bridge working environment exposed and vulnerable, just as the adverse man-made GNSS interference – jamming and spoofing attacks – have become a daily occurrence. Rather suddenly, in many navigationally busy areas of the world, the GNSS systems we have overrelied on for so long cannot necessarily be relied upon anymore, which is exactly the challenge these guidelines aim to address.

Captain Pantelis Patsoulis
Anglo-Eastern Shipmanagement (Hellas)

INTERTANKO extends special thanks and gratitude to Tobias Ehlers from Federal Maritime and Hydrographic Agency of Germany (BSH) and Saab TransponderTech AB team for their invaluable input into the updating of this document.

Introduction

A Global Navigation Satellite System (GNSS) refers to a constellation of satellites providing signals from space that transmit ranging and timing data, which GNSS receivers use to determine their locations. While GNSS provides global coverage, the extent and effectiveness of this coverage can vary based on the number of satellites in view, their positions, and environmental factors. Augmentation (differential) systems offer improved accuracy for single frequency receivers, but they rely on a network of reference base stations which are not available everywhere, or in closer proximity of the receiver's location. It is expected that dual-frequency – or multi-frequency – GNSS receivers will be more broadly available to merchant shipping soon, which can offer improved position signal stability through better resistance to adverse GNSS interference, including jamming and spoofing.

High standards of navigation are fundamental to the safety of vessels, crew, cargoes and protection of the environment. Such high standards demand high position availability, accuracy and stability, as well as resilience to disturbances. However, while we became more reliant on GNSS for safe navigation, growing threats to reliability have been identified which can affect how we use them for navigation, and how we can mitigate the risk of disruption of its services.

Many reports on GNSS disturbances show high vulnerability of transport modes that rely solely on satellite navigation. To increase the resilience of maritime transport and reduce the risk of using misleading information to the grave risk of navigational safety, maritime administrations and manufacturers must look more actively for solutions to identify and mitigate GNSS disruptions or deceptions. At the same time, shipping companies, bridge teams and navigational officers must remain vigilant and be prepared to operate their vessels in a GNSS-compromised environment, a process which this guide intends to support.

Scope

This document is aimed at shipowners, operators and Masters. It provides guidance on multiple GNSS systems, explains the risk associated with their suboptimal operation and recommends ways to manage this risk. It is not intended to cover all technical aspects related to satellite navigational systems, but it will aim to identify practical and pragmatic ways to mitigate possible disruptions hindering safe navigation.

Intentional man-made signal interference: Jamming and Spoofing

Since GNSS signals arrive at low power on the earth's surface, even a weak interference source can cause the receiver to fail or to produce hazardously misleading information. Until now, the most prominent threat was GNSS jamming, occurring frequently in many regions of the world. Jamming can be regarded as a broadcast of special signals masking the GNSS satellite signal with highly disturbing RF-N (Radio Frequency Noise), or signals designed to interfere directly with the GNSS frequencies. While a complete loss of GNSS is relatively easy to detect, subtle movements as an effect of jamming are not. They may look like spoofing, which is harder to detect.

Spoofing is more insidious, as false signals from a ground station or flying drone simply confuse a satellite receiver. To simplify, jamming causes the receiver to die, and spoofing causes the receiver to lie. While this statement – explained below in full – is not *technically* correct, it does provide a broader overview of the main differences between jamming and spoofing.

What is jamming?

When signal interference is intentional, narrow-band or broad-band signals are radiated deliberately to interfere with GNSS frequencies to prevent the reception of navigation signals. This type of GNSS interference is called **jamming**, which can be caused by various sources, including:

1. **Intentional jamming devices**: Designed to disrupt GNSS signals.
2. **Unintentional interference**: From other electronic devices or systems.
3. **Natural interference**: From solar activity or other environmental factors.

Jamming may be caused by individuals or groups, including military, but also unintentional means including 'space weather' or faulty equipment that can radiate signals on the GNSS working frequencies and jam signal reception. Intentional jamming is designed to overpower the very weak GNSS signals receiver.

Some GNSS bands are shared with certain radars, other satellite equipment as well as amateur radio. Other sources include distance measuring equipment used for airplane navigation, TV harmonics, and malfunctioning electronic equipment. As an example, a 25W Inmarsat transmission near a poorly designed GNSS receiver will at minimum "blank" all GNSS reception, and at worst "fry" the receiver front end.

The most recent global GNSS jamming data indicates that vast geographical areas are frequently jammed which exclude small private interference occurrences and suggests key state players are strongly involved.

Figure 1: Jamming

What is spoofing?

Another type of intentional man-made GNSS signal interference, but more complex to implement, is the transmission of falsified signals. This type of activity is called **spoofing**. The intention is to lock the receiver into a simulated or re-transmitted GNSS signals. This way, the receiver can be deceived to provide a false positioning, navigation, and timing (PNT) solution or no PNT information at all. Manipulated signals can feed fake position and speed data into primary and secondary ECDIS, leading to integrity risk due to unrecognised wrongful operation of the navigation receiver. A resulting ECDIS position offset, if not detected by a bridge team, may lead to serious navigational incident.

GNSS spoofing is the provision of GNSS-like signals, transmitted locally and coded to fool the receiver to think it is somewhere it is not. Although spoofing requires much more effort than jamming, spoofing events have

been increasingly observed and reported in recent years. The consequences of spoofing can be far more serious than those from jamming. If the false signals are indistinguishable from the real ones and give a position close enough to be believable, the user may not be aware of the deception which may lead to casualty.

A GNSS spoofing attack attempts to deceive a GNSS receiver by broadcasting incorrect GNSS signals, structured to resemble a set of normal GNSS signals, or by rebroadcasting genuine signals captured elsewhere or at a different time. These spoofed signals may be modified in such a way as to cause the receiver to estimate its position to be somewhere else than where it actually is, or to be located where it is but at a different time, as determined and desired by the attacker.

An interesting form of a GNSS spoofing attack, commonly termed as "**carry-off attack**", begins by broadcasting signals synchronised with the genuine signals observed by the target receiver. The power of the counterfeit signals is then gradually increased so that the vessel's GNSS receiver tracks the false signals, which can then be manipulated to report a different location to the genuine signals. Spoofing GNSS signals with the aim of not being detected is also possible, but this is military grade technology.

GNSS Time Spoofing

GNSS time spoofing is a cyberattack where fake GNSS signals are transmitted to deceive a receiver into using an incorrect time. This can disrupt critical systems relying on accurate time synchronisation, such as power grids and communication networks. Sophisticated spoofing can be difficult to detect, as the fake signals can mimic legitimate ones, causing the receiver to miscalculate its position and time. Companies should cross-reference GNSS time spoofing vulnerabilities within their SMS with reference to the Cyber Risk Management Plan as per MSC.428(98)

Figure 2: Spoofing

Meaconing

'Meaconing' is a type of spoofing where GNSS signals are re-transmitted. This requires simpler equipment than that required for a spoofing attack.

The source of a meaconing attack could also be GPS/GNSS repeaters such as those installed in airport hangars, allowing indoor reception of GPS signals for testing purposes. Should the power of such a repeater be increased intentionally or not, it would lead to a fake position being sent out.

AIS Spoofing

Reports exist of AIS spoofing where an acquired target visible on the ECDIS and ARPA screens was confirmed by visual and radar observations as non-existing on the sea surface. A "fake" AIS echo – or echoes – have the potential to create considerable confusion on the bridge and may induce watch officer into actions desirable by the attacker(s), leading to unacceptable safety and security risks. For instance, course or speed changes necessary to avoid collision could take the vessel into territorial waters of Iran, opening possibility of a vessel seizure.

Navigators are encouraged to conduct sharp visual and radar lookout duty to identify and confirm whether the screened AIS echo(es) are the actual ships operating in the vicinity of the vessel's courseline. It must be said that the AIS should not be used for collision avoidance, and the use of VHF is discouraged to plan or agree such action. Approaching AIS manufacturers could help determine whether other options exist to verify the authenticity of the AIS echo (target position quality) when operating the AIS receiver. If yes, a procedure could be posted on the bridge to aid such identification.

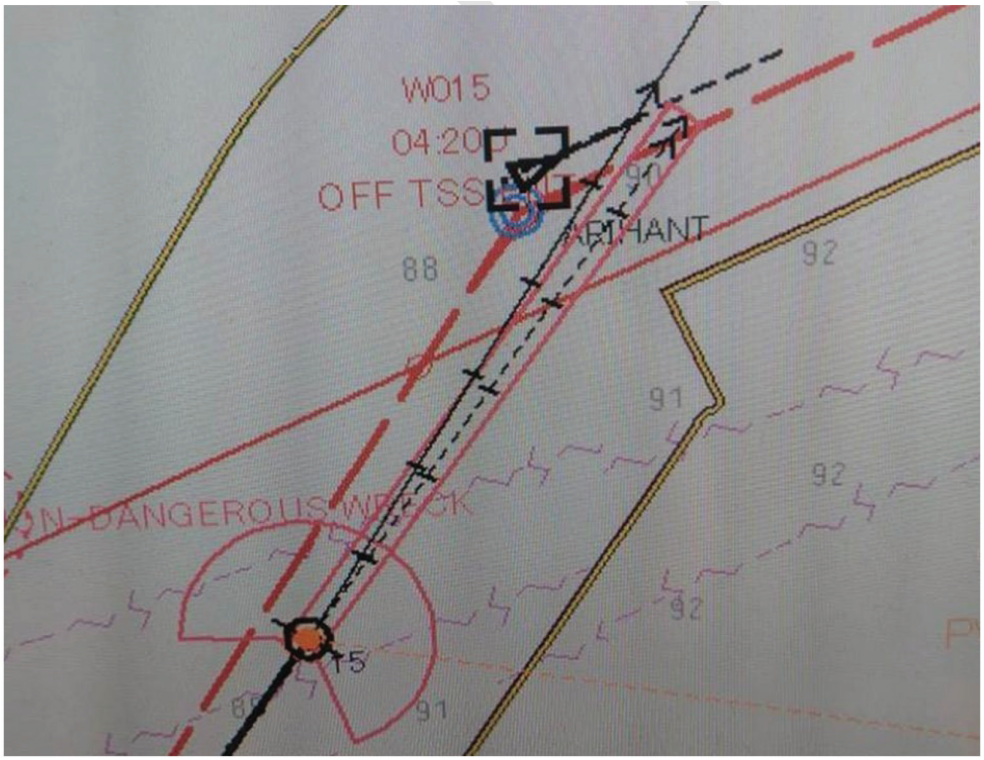


Figure 3: AIS Spoofing in the Strait of Hormuz. The acquired AIS echo only exists on the screen

Summary

A spoofing attack is considerably more complex – and dangerous - than a jamming attack, especially if the attack is supposed to remain undetected. Unrecognised, wrongful operation of GNSS receivers can be a bigger danger than loss of signal itself.

Unintentional and natural signal interference

Man-made interference can be either unintentional or deliberately generated. Despite regulations and licensing, unintentional interference between radio transmissions cannot be totally avoided. Navigation signals may be accidentally or intentionally blocked by other high-powered signals or locked into strong and deliberately transmitted falsified signals.

Radio signals can be affected or disrupted by natural events, such as space weather, natural or artificial obstacles or by man-made interference. Effects of natural events may be observed in large areas and during any phase of navigation. However, the risk of man-made interference, as well as natural interference of natural or artificial obstacles, is much higher in coastal waters and ports. Due to proximity of the coastline, traffic and shallow waters, it is also the most dangerous. Most of the interference, however, affects only limited line-of-sight areas.

Unintentional sources of man-made GNSS interference include television or radio broadcasting stations, microwave communication links or Vessel Traffic Service (VTS) surveillance radars. Although less frequently observed, onboard equipment such as satellite uplinks and radars may also cause interference to a vessel's own GNSS receiver or other GNSS receivers in the vicinity. Although rare, interference is possible from poorly designed active TV shipboard antennas, temporarily preventing the receiver from tracking satellite signals.

Multipath

A common type of interference affecting GNSS receivers is known as **multipath**. This phenomenon occurs when a satellite signal is received at the user GNSS receiver's antenna by different paths due to the presence of obstacles on which the signal is reflected. The effects produced by the multipath are mainly a distortion in the modulation of the signal and the phase of the carrier producing a degradation of the accuracy, which implies increased positioning errors. In addition to this phenomenon, there is similar interference that also affects GNSS signal reception by receivers. This undesired phenomenon is associated to the direct blockage of GNSS signals due to obstacles (e.g. mountains or buildings). The reception of only non-line-of-sight (NLOS) signals via reflection (referred as NLOS multipath) introduces errors in measurements due to the increase in the length of the path of the reflected signal compared to the direct path between the satellite and the receiver. Sometimes, the multipath and NLOS multipath phenomena may occur together, especially near ports.

Shadowing

GNSS signals can also be totally blocked. While this is not signal interference, it should be considered when estimating possible disturbances on GNSS signal reception by the user. The line of sight between GNSS satellites and GNSS receivers can be blocked by natural or artificial obstacles, negatively impacting on the reception of GNSS signals. A situation where the GNSS signal does not reach the receiver at all is referred to as **shadowing** or **obstruction**, which will result in increased positioning errors because of two unwanted effects: fewer satellites in view and poorer satellite geometry. Both effects, indirectly or directly, increase the Dilution of Precision (DOP) value observed on the GNSS receiver which is related to the inaccuracy of the position measurement. The smaller the DOP value, the more precise position is calculated. Please refer to the pocket guide on GNSS signal quality in Appendix C.

Detection and mitigation against jamming and spoofing

In 2017, the IMO published MSC.1/Circ.1575, *Guidelines for shipborne Position, Navigation and Timing (PNT) data processing to the Performance standards for multi-system shipborne radio navigation receivers* (MSC.401(95) & MSC.438(98) MSR amendment). The International Electrotechnical Commission (IEC) and Radio Technical Commission for Maritime Services (RTCM) will soon develop test specifications for multi-system receivers, which will include at least the combination of two GNSS systems and augmentation services (for instance, SBAS – Satellite Based Augmentation System or International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) -beacon differential GNSS). **Multi-frequency GNSS units** are **expected to be used with a terrestrial component**, such as e-Loran or the R-Mode ("Ranging" through VDES and MF shore-to-ship distance measurements). These works are based on the IMO "Minimum performance standard for multi-system radionavigation receiver" (MSC.401(95)) and associated "Guidelines for shipborne PNT data processing" (MSC.1/Circ.1575).

If the equipment onboard meets the MSC.401(95) and MSC.1/Circ.1575 specification and there are multiple types of GNSS systems available, as well as other inputs, the system should raise an alarm in case of a detected error to inform the navigator that the position has been lost. Modern equipment exists that meets basic requirements MSC.401(95) and, partially, MSC.1/Circ.1575 guidelines but, due to lack of maritime test standards, the requisite type approvals for fitting such equipment on board are not yet available. INTERTANKO recommends that navigation systems, equipment and software onboard are designed and installed, as far as practicable, in line with these guidelines.

In December 2023, IALA issued *Guidelines for Resilient Position, Navigation and Timing (PNT)*. This publication is free to be downloaded or accessed online. Due to increased reliance of bridge teams on PNT data, which is supplied by GNSS, we recommend this publication was included in the shipboard library and officers of the watch made familiar with it. Please note that effective August 22, 2024, IALA officially changed its status from a Non-governmental Organization (NGO) to an Intergovernmental Organization (IGO) and the new organization is named the International Organization for Marine Aids to Navigation.

Multi-constellation GNSS receivers

Adding GNSS signals to GNSS receivers from more than one global positioning system and on multiple frequencies will ensure more satellites are available for navigation, resulting in higher position accuracy, stability and self-error corrections of the atmospheric delays. A higher availability of satellites will enhance safe navigation in areas with steep mountains such as the Norwegian coast or in built-up areas of harbours or inland waterways, where the satellite view can be obscured. It is also more suitable for use in higher latitudes (north or south). In this sense, utilising up to four truly global GNSS receivers can enhance their current coverage, providing more seamless and accurate experience for multi-constellation users around the world.

Most new GNSS receivers, chipset and modules available at present support GPS (USA), GLONASS (Russia), Galileo (EU), and BeiDou (China). Additionally, they can incorporate regional positioning systems for even better accuracy and stability. More on the full GNSS frequency spectrum available at present overleaf (Figure 4).

Multi-frequency GNSS Receivers

Type-approved multi-frequency GNSS equipment is becoming available which offers reception on more than one frequency to mitigate atmospheric delays for higher accuracy and stronger resilience to interference and disturbances.

All global GNSS constellations transmit on multiple frequency bands (refer to the GNSS spectrum on Figure 3). However, most legacy GNSS receivers lock onto L1 only, with that being sufficient to meet the IMO carriage requirements for an Electronic Position Fixing Device.

The primary frequency bands are L1 (GPS), E1 (Galileo), G1 (GLONASS), and B1-I (BeiDou), which are the basic civilian signals. The additionally available advanced bands are: L2+ L5 (GPS), E5a + E5b (Galileo), B2a + B2b (BeiDou), G2 (GLONASS). Utilisation of all available GNSS signals on all frequency bands can help in unlocking increased signal availability, and therefore position accuracy and navigational resilience.

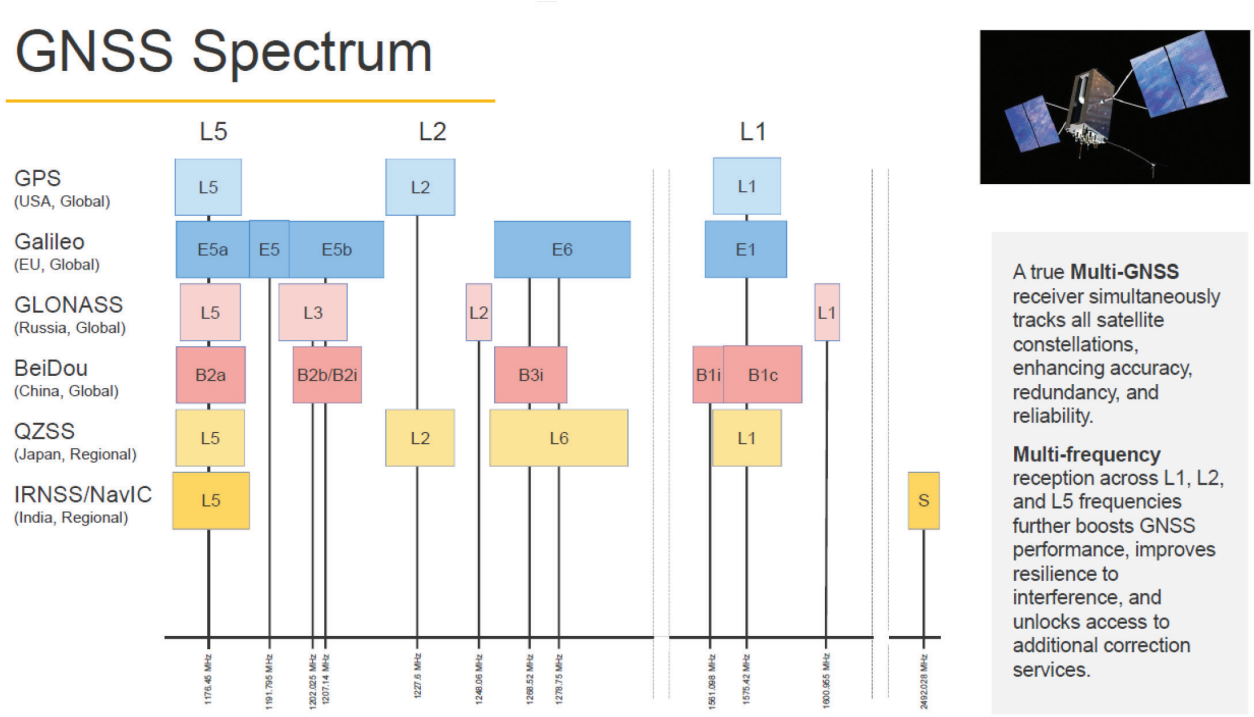


Figure 4: GNSS frequency spectrum (Saab TransponderTech)

- **Superior Availability**: By tracking all satellites from all constellations simultaneously, a modern receiver maintains a continuous position fix even in challenging areas like ports with high buildings or deep fjords, where a legacy unit would lose signal.
- **Increased Accuracy**: Using multiple frequency bands allows the receiver to correct for atmospheric signal delays, improving accuracy. Especially when combined with a correction service such as local RTK or the global Galileo HAS service.
- **Enhanced Resilience to Jamming**: Intentional jamming often targets the common primary frequency band (L1/E1/G1). A legacy receiver operating only on this band would be completely disabled during such an event. Multi frequency receivers may be able to continue to calculate a precise and reliable position using only the signals in other bands (such as L5/E5a).
- **Enhanced Resilience to Spoofing**: Spoofing attacks often start with a jamming phase, forcing receivers into reacquisition mode, then inject synthetic or rebroadcast (meaconed) signals. Resilience to jamming is therefore a first step to protect from spoofing. The receiver may also cross check the data received from the various GNSS systems to detect anomalies and uncertainties in the produced navigation solution.

In summary: by blending four global constellations, and multiple frequencies, today's ships may gain availability, accuracy, anti-jamming and anti-spoofing safeguards.

Inertial Measurement Units (IMU)

Inertial Measurement Units (IMU) rely on accelerometers and gyroscopes to track movement and orientation. Accelerometers measure linear acceleration along different axes, while gyroscopes detect rotational motion. By integrating data from these sensors over time, inertial navigation systems (INS) can calculate changes in velocity and position relative to a known starting point. This **improved dead reckoning** approach can allow ships to navigate in the short term without external references, making it useful for applications where GNSS might be compromised or unavailable.

However, INS suffer from a significant drawback: shift. Small errors in acceleration and rotation measurements, which are inherent in mechanical sensors, accumulate over time. This accumulation leads to increasingly significant positioning errors as a journey progresses. For example, when operating unaided (without external correcting input) the IMU could expect to "drift" by up to **one nautical mile per hour**, which can be very problematic for longer routes. As a result, traditional IMU often require periodic recalibration using external references such as GNSS to maintain accuracy. For example, a submarine relying on acoustic position systems and INS that accumulate errors over time may require periodic surfacing to recalibrate their position using GNSS. Such recalibration will not be possible for a ship if a reliable GNSS signal is not available.

In the future, it is expected that accurate positioning without GNSS may be possible with the use of new technologies, such as atom interferometers and quantum inertial navigation systems (Q-INS), enabling ultra-precise measurements of acceleration and rotation without relying on an external signal. However, such systems are extremely complex and prohibitively expensive at present.

There are IMU-equipped GNSS receivers available which incorporate enhanced motion monitoring to provide higher accuracy position through improved measurement of speed, heading, course, rate of turn, roll, pitch and heave. However, navigation in a GNSS-compromised environment based on GNSS' IMU must always be conducted with extreme caution and under direct Master supervision.

Navigation Message Authentication (NMA)

Currently all open civil GNSS signals are transmitted without any security measures, conforming to interface specifications that are fully available in public domain. Such a signal is vulnerable to adverse interference, especially spoofing. Message authentication is based on a concept that the receiver of a message gets enabled to ensure that the message it received is:

- Identical to the message that was transmitted;
- From a trusted source.

Navigation Message Authentication (NMA) is one of the many tools which can be used against spoofing. While it does not solve all the spoofing problems by itself, it is certainly a step towards the better PNT resilience in navigation.

Implementing NMA would in most cases require a new GNSS receiver. Several of the existing GNSS do not support work on NMA applications yet. As an example, the USA is working on an Asymmetric NMA for GPS and European Satellite Services Provider (ESSP) already released a Hybrid Symmetric/Asymmetric NMA solution in 2024.

It is up to the international maritime community to foster the corresponding work in maritime standardisation and thus enable individual equipment manufacturers to implement these technologies in their products, to enable the mariners to take full advantage of these services as they are made available for reliable and resilient navigation.

Guide for the Navigator

ECDIS manufacturers can provide instruction on the use of their ECDIS in case of GNSS signal loss or distortion, including adverse and deliberate interference in the form of spoofing and jamming. Watch officer should be familiar with such instruction, and as far as practicable, follow it when navigating in a GNSS-compromised environment.

Actions to detect GNSS interference or poor signal

- The use of radar overlay on ECDIS is considered one of the best methods to identify jamming and spoofing and related signal loss, or position signal quality degeneration provided the coastline and special identifiable landmarks, as well as other aids to navigation, are visible on the radar.
- Position verification at appropriate intervals as laid out in the *Guide to Safe Navigation, including ECDIS* (INTERTANKO 2017 (revised Nov 2021)).
- GNSS position jumps, shifts, and gaps in the ship track line on the ECDIS can be one of the first indicators of jamming and spoofing.

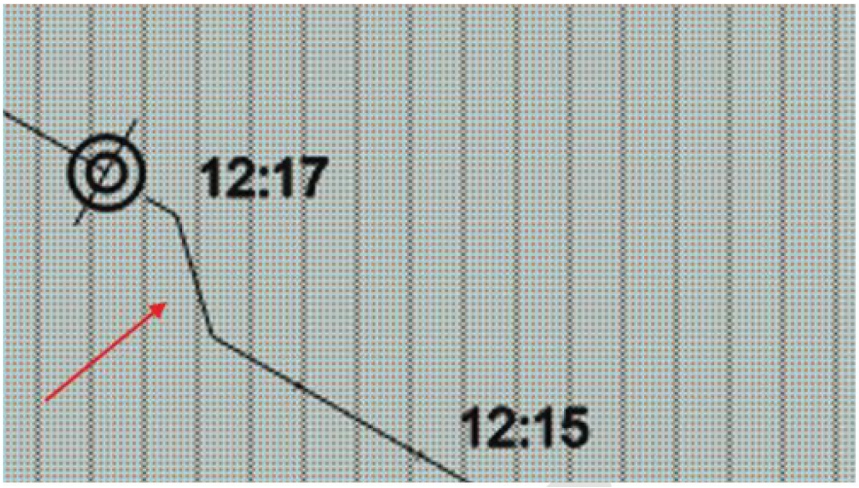


Figure 5: GNSS "position jump" (ChartWorld)

- Observing significant and unexpected differences between COG (Course Over Ground) and Gyrocourse (and Magnetic Course if deviation is well known and confirmed).
- Observing significant and unexpected differences between SOG (Speed Over Ground) and Log Speed.
- Monitoring GNSS receiver working parameters in line with manufacturer's manual: Signal-to-Noise Ratio (SNR), HDOP (Horizontal Dilution of Precision), RAIM (Receiver Autonomous Integrity Monitoring), SBSA (Satellite-Based Augmentation Systems) and DGPS status. Refer to *APPENDIX C: GNSS receiver. Pocket guide on signal quality*. Some of the newest GNSS receivers can estimate their **Jamming Status**.
- In case of GNSS signal loss, mandatory ECDIS alert (positioning system failure) should sound. It is imperative that the alert is not merely acknowledged, but actions must be taken to enhance safe navigation. Care must be applied to ensure alarm fatigue will not cause navigators to mute the alarm so they can continue their watch as normal, undisturbed.
- Observing significant difference between DR (Dead-Reckoning) position (position determined with the Gyro Course steered and distance measured by speed log) and the GNSS position fix.
- Verification of actual echo sounder depths compared to charted depths.
- In deep sea and good weather conditions, astronavigation plots through celestial observations could be made, if the vessel is equipped with a sextant.
- If in the slightest of doubt, the Master to be contacted for a second independent opinion and additional judgment. **The really good officer is the one Masters can rely on to call them.**

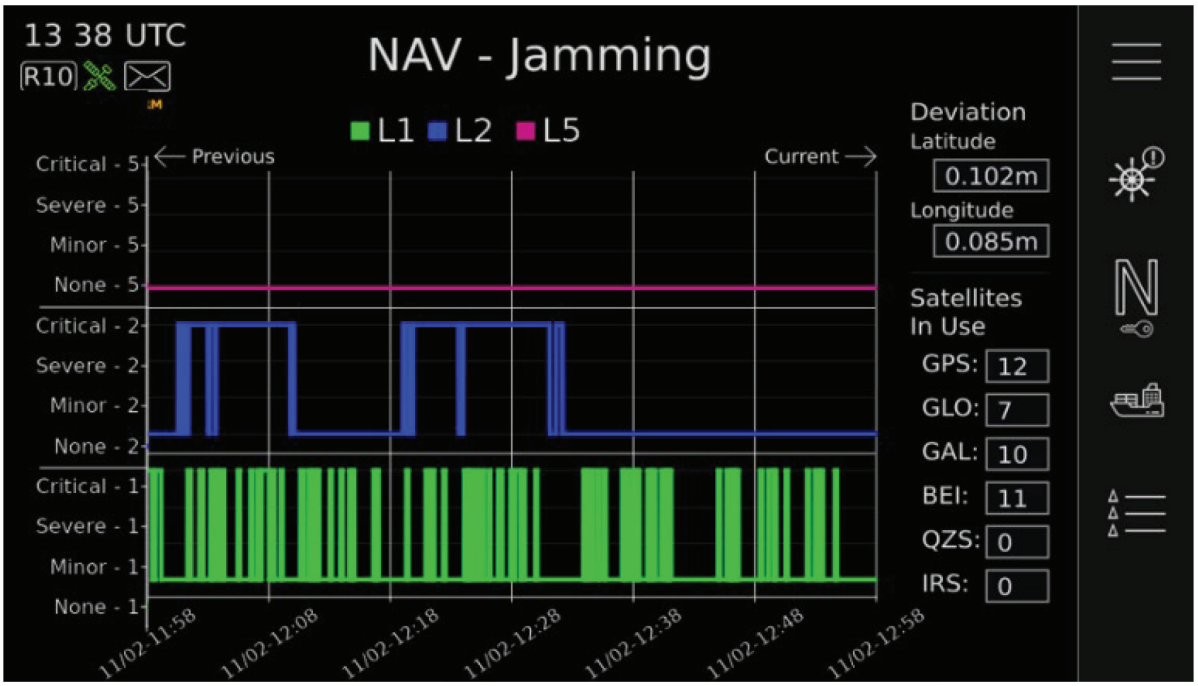


Figure 6: Saab TransponderTech R6 NAV PRO, Jamming Status

Actions if jamming or spoofing is detected

Immediate actions:

- Manually select a secondary position sensor. NOTE: Not all GNSS receivers may be affected.
- For multiple-system GNSS receiver(s), verify whether position signal of all systems (GPS, Glonass, Beidou and Galileo) is lost or affected, and if not, manually switch to the system with valid positioning data (if automatic transfer did not activate or is not part of the original design).
- Check that the ECDIS position feed appears normal and verify the accuracy of this position by other means.
- If secondary sensor is unable to provide a vessel's position and no other means are available for position fixing, select the DR or EP (Estimated Position) mode. Some ECDIS units will default to either DR or EP in case of GNSS position signal failure. **NOTE:** Correct DR (EP) mode by LOP (Line of Position) as soon as possible (see: Figure 7 which demonstrates a position correction from EP to LOP)
- If the ECDIS is equipped with radar interface (overlay or underlay), and the vessel is close to the coast, ensure it is in operation and keep monitoring the vessel position in relation to the shoreline to the extent possible.
- Use distinctive land features and identifiable shore objects to plot position from by the radar bearing and distance(s) and keep inserting such positions on ECDIS. Use radar ERBL transferred to ECDIS, if provided.
- Continue to frequently manually plot ship's position if close to shore and seek greater sea room, if possible.

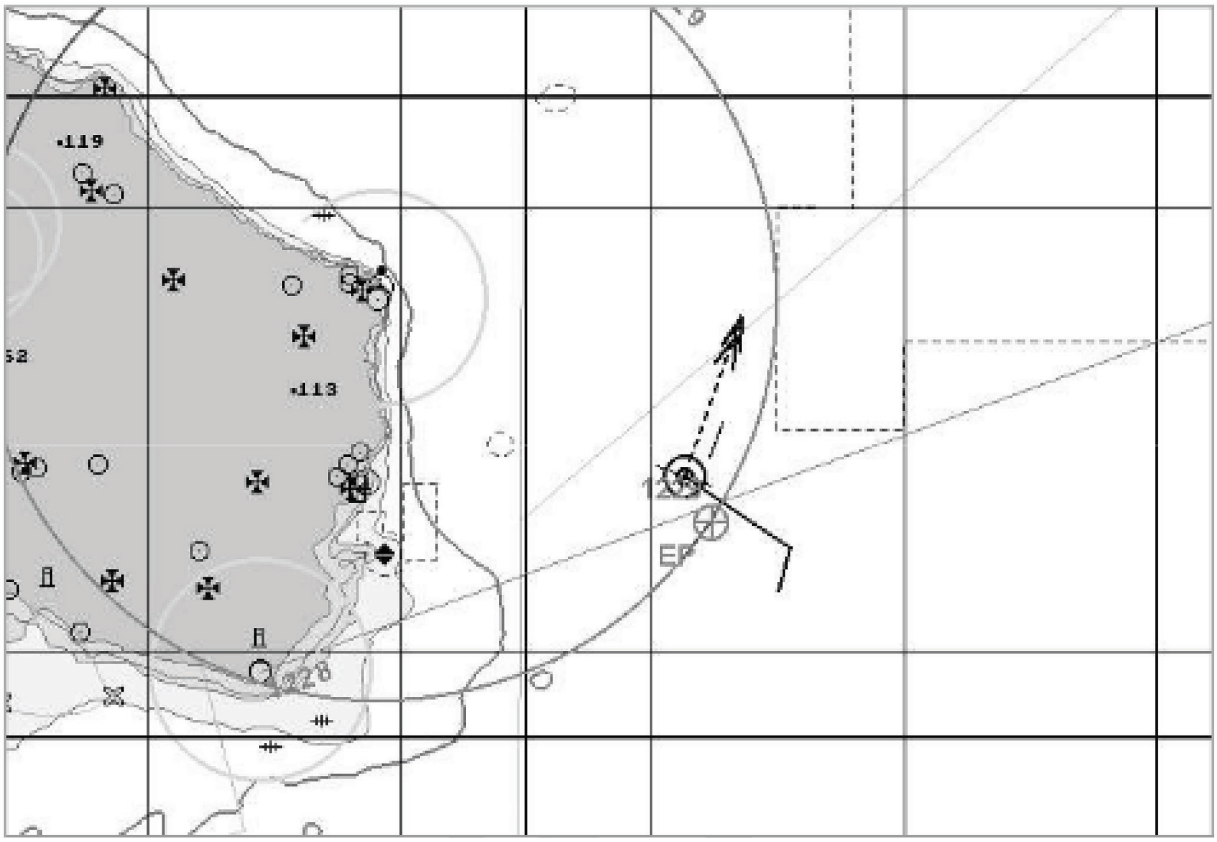


Figure 7: EP corrected by LOP from bearing and distance (Wärtsilä Navi-Sailor 4100 User Manual)

- Frequently record ship's log speed, gyro and magnetic course, wind speed and estimated current/tide. Bridge manning level should be increased to aid this process.
- The Automatic Identification System (AIS) can be affected by a jamming or spoofing attack and should be used with extreme caution (this refers to the other ships' positions that are likely to be affected by an attack, not the VHF AIS signal). **NOTE**: AIS virtual navigation aids position will be correct, since their position transmitted as a true static position which is not derived from GNSS signals.
- Use the parallel indexing method during coastal navigation to keep safe distances, identify if the vessel is drifting or setting towards shallow waters, and determine turning waypoints.
- If unable to ascertain position in relation to navigational hazards in the area, STOP the vessel to gain more time for safe reassessment. Use safe contingency anchorage, if available and contact the coastal state or port authorities to explain that you are doing so for safety reasons.
- Refer to Emergency Manual checklist for GNSS signal loss, if held. Keep the main engine ready.

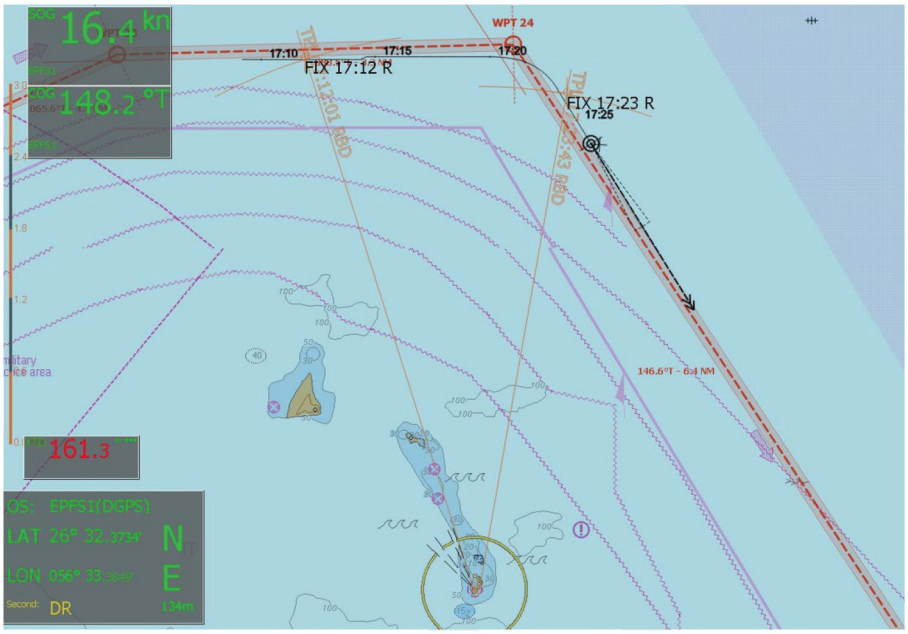


Figure 8: DR corrected by Manual Fix (ChartWorld)

When the situation is somewhat stable:

- Check the vessel's GNSS position and GNSS receivers frequently to detect when the service is available again.
- Report GNSS disruptions or anomalies to the authorities listed in *Appendix A: Reporting of jamming and spoofing events*.
- Record critical event information such as the actual location (latitude/longitude), date/time, and the duration of the outage or disruption.
- Keep recording the weather conditions, gyro and magnetic compass course, log speed values.
- When possible, provide photos or screenshots of equipment failures during a disruption to assist with investigation into the root and direct causes, aiding preparation of a report.
- Report the GNSS interference occurrence to your company and proper authorities: coastal state and Flag, noting that depending on the vessel position, UKMTO and MSCHOA should be notified.

When the GNSS position signal is back

When the GNSS signal is restored, it is still necessary to cross-check the position with manual fixes or radar overlay on ECDIS when in coastal range. Only upon satisfactory confirmation, select GNSS back as the primary position sensor but continue to closely monitor it.

Note that all time indicators (or clocks) on all GNSS-dependent instruments should be checked to make sure that time has correctly reset after recovering.

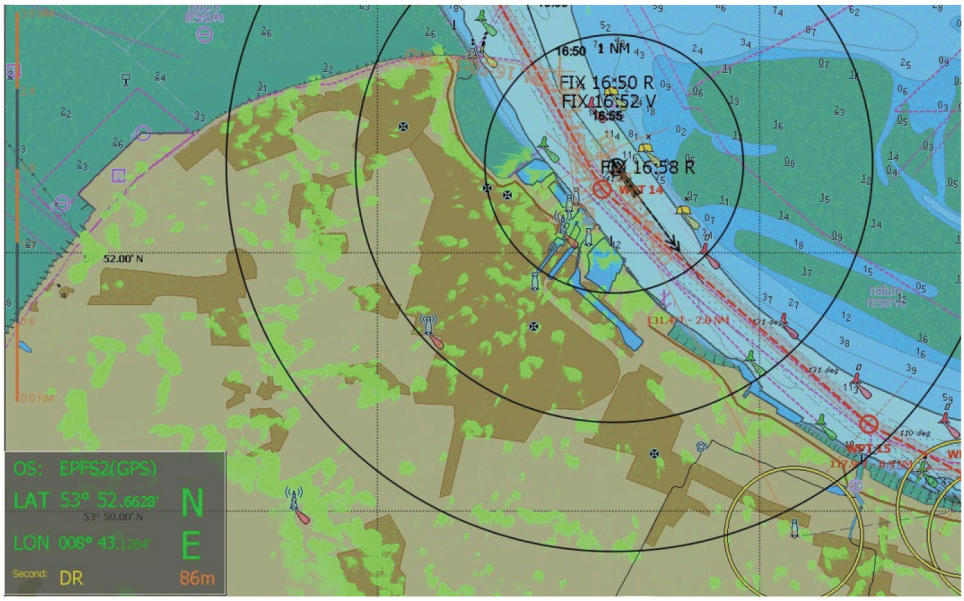


Figure 9: LOP fixes on Elbe River with radar overlay (ChartWorld)

For vessels using paper charts:
Continue plotting with alternate position fixing or DR. **NOTE**: Never rely on DR in coastal navigation and confined waters as this does not provide accuracy sufficient to support safe navigation in such areas. Radar and visual bearings and distances must be measured to establish a reliable and resilient navigational position enabling safe transit in restricted waters. Use parallel indexing techniques to monitor whether your vessel is not being set towards the shore and shallow waters.

During normal operation:
Periodically check ECDIS sensor input for position and source. Monitor GNSS receiver(s) working parameters. Refer to *APPENDIX C: GNSS receiver. Pocket guide on signal quality*.

Guide for the ship owner/manager

Bridge navigational equipment should comply with the latest regulations. New equipment installed should, as far as practicable, make use of the multi-system and multi-frequency GNSS, IALA Beacon differential services, and SBAS (Satellite Based Augmentation System). The system should utilise key elements of the MSC.401(95) and MSC.1/Circ.1575: *Guidelines for Shipborne Position, Navigation and Timing (PNT) Data Processing.* Ensure that primary and secondary ECDIS units have alarm management function(s) commensurate with the above equipment and that proper procedures are in place to manage these system utilities. Further protection may be gained through using the GNSS open signals which have Navigation Message Authentication (NMA).

NOTE: Some of the newer GNSS receivers can be operated as a fixed (non-portable) piloting units with real-time kinematics (RTK) required for vessels transiting Panama Canal from 1 October 2023. It is recommended to consult the manufacturer and ACP (Autoridad del Canal de Panama) website and verify the list of evaluated equipment to check on whether a particular GNSS receiver meets the ACP requirements and has been approved for such service.

Since most manufacturers continuously upgrade their GNSS receivers and harden them against adverse interference, it is recommended to have installed on the bridge the newest equipment type and software versions of the GNSS receiver that the company and their vessel(s) are using. Strong liaison and communication are encouraged to ensure the makers are aware how critical resilient GNSS receivers and stable GNSS positioning data are for safe navigation and loss prevention.

In the future, regionally, there will be a possibility to use terrestrial components backing up the satellite positioning signals. In the Baltic, the R-Mode (Ranging) i.e. ship-to-shore distance measurements, is executed through regional campaigns in different Baltic Sea areas. The system consists of Medium Frequency (MF) and Very High Frequency Data Exchange System (VDES) R-Mode transmitters. While the system uses existing shore infrastructure, on the ship side the receiver can be integrated into a Portable Pilot Unit (PPU) to support Masters and pilots with alternative PNT data. Furthermore, the receiver enables the detection of GNSS distortions by comparing the R-Mode and GNSS measurements. This information can be fed into a newly developed coastal GNSS Interference Detection System (GIDS) to visualise overview on the current GNSS positioning performance and warn mariners in case of detected anomalies. In other words, watch officers on the bridge will be able to receive a warning from coastal stations in certain areas that the GNSS signal is distorted (or inaccurate), and that they should be on their guard. While this enhancement in navigational resilience is presently undergoing further tests and developments and remains geographically restricted to the Baltic Sea, it is possible more coastal states will become involved in the project and make "Ranging" possible in their waters. Other systems with a more global reach (e-Loran) are being developed and implemented to ensure navigational data resilience worldwide.

Safety Drills

It is recommended that regular GNSS failure drills are carried out to maintain familiarity with the handling of GNSS interference events. These should be different than ECDIS failure drills which have become standard for some companies and included in the Emergency Manual (Contingency Booklet) with relevant checklist for the bridge team. INTERTANKO recommends that a simple one-page, clear and concise procedure be developed for the OOW/Master to refer to when the GNSS signal is either confirmed lost, assumed lost or there are serious doubts as to its quality.

The drills could include situations where the GNSS signal is lost, or failed, and the ECDIS must be operated with manually inserted Line of Position(s) (LOPs) obtained through DR or EP mode, and through LOP or echo reference. Visual bearings should be exercised when in sight of the coast and in good visibility, with radar distances and bearings used when in coastal navigation. It is necessary for the Officer of the Watch (OOW) to identify the other equipment affected by GNSS sensor failure (for instance, AIS, digital selective calling – DSC, gyro, autopilot, and radar).

The aim of the drill is to develop competency in detection of GNSS jamming or spoofing and **gain confidence in safe navigation practices that are independent of GNSS**. The company should design a basic GNSS failure drill model, but the Masters should have freedom to tailor them to practise and improve the skills of their bridge team and therefore make a generic drill format more ship specific. Feedback should be collected from ships on lessons learned and identified room for improvement after each drill.

It is suggested that companies appreciate and recognise GNSS overreliance on the bridge is a modern problem which must be addressed to improve safety of navigation and prevent loss.

Training, coaching and mentoring

Navigation in a GNSS-compromised environment is considered a critical, yet vanishing, skill. Experienced Masters are encouraged to educate officers to reduce their dependence on satellite positioning systems and increase confidence they can navigate a ship when, for instance, GPS signal is lost but there are multiple – well identifiable – shore objects from which accurate bearing and distance measurements can be reliably made to determine a position.

New STCW Competence: Navigation in GNSS-compromised environment

Recognising that the GNSS signal feeds into the bridge equipment, particularly the ECDIS, has become a critical component upon which navigators rely upon to a great – perhaps too great – extent, during the STCW Convention review at the IMO, INTERTANKO proposed creation of a new competence to place navigation in a

GNSS-compromised environment firmly within the competences of all those undertaking a navigational watch. This submission was approved to be proceeded for the STCW review phase in 2025. The key competences defined by INTERTANKO's Nautical Sub-Committee (NSC) can be seen in the table below:

Competence	**Knowledge, understanding and proficiency**	**Methods for demonstrating competence**	**Criteria for demonstrating compliance**
Navigate safely in a Global Navigation Satellite System (GNSS) compromised environment.	Ability to recognise when GNSS has become unreliable including the monitoring of navigational notices. Knowledge of effects of unreliable GNSS input into bridge equipment such as AIS or ECDIS. Understands the actions to take if the GNSS position input becomes unreliable. Understanding of which navigational equipment is unaffected and use that to plot the ship's position and monitor the track of the ship. Understanding on various error and loss of GNSS in circumstances. Understanding on position verification in case unreliable date identified at sea and while in coastal water.	Examination and assessment of evidence obtained from both of the following methods: .1 approved training ship experience; and .2 approved simulator training.	Makes a full assessment of the information on electronic navigational equipment observing any significant difference between, a radar overlay, DR position and GNSS fix. Verification on indication of unreliability of GNSS data and output – Time/ loss of signals/ jamming. In coastal waters, monitors differences between expected depths and those indicated by echo sounder whilst monitoring track using methods such as parallel index and plotting using radar ranges and bearings. Ability to transfer position data from all available means, other means than position from primary means on ECDIS. Takes into account navigational notices warning of a GNSS compromised environments. Takes decisions to maintain safe navigation.

It was the NSC's view that the STCW competency review must be completed, and mandatory training implemented to address the contingency of temporary absence of GNSS signal – a new working environment in which navigators must be competent of obtaining position through either dead reckoning in deep sea, or dynamic visual and radar fixes in coastal navigation. Therefore, the NSC focus was on understanding consequences of a failed GNSS input to ECDIS and the ability to obtain position through terrestrial navigation, which are considered key competencies to be trained and safeguarded for the future.

Countermeasures

Jamming countermeasures

There are multiple mitigation strategies to help overcome interference:

- Utilise multi-frequency and multi-constellation GNSS receivers, accommodating the GPS, GLONASS, Galileo, and BeiDou. This allows for greater flexibility in terms of satellite availability and improves the robustness and accuracy of the navigational solution. **NOTE:** GNSS interference can still impact all these systems as they operate on similar frequencies.
- Install newest types of GNSS receivers the equipment maker(s) can provide, incorporating anti-interference mechanisms, stronger filtering capabilities, multi-frequency reception and better hardening.
- Aid eligible GNSS receivers with Inertial Measurement Unit (IMU).
- Consider using terrestrial component (E-Loran, Ranging) receivers if they become available.
- Always keep the GNSS receiver(s) software updated with the latest edition.
- Invest in adaptive antenna arrays CRPA (Controlled Reception Pattern Antennas).

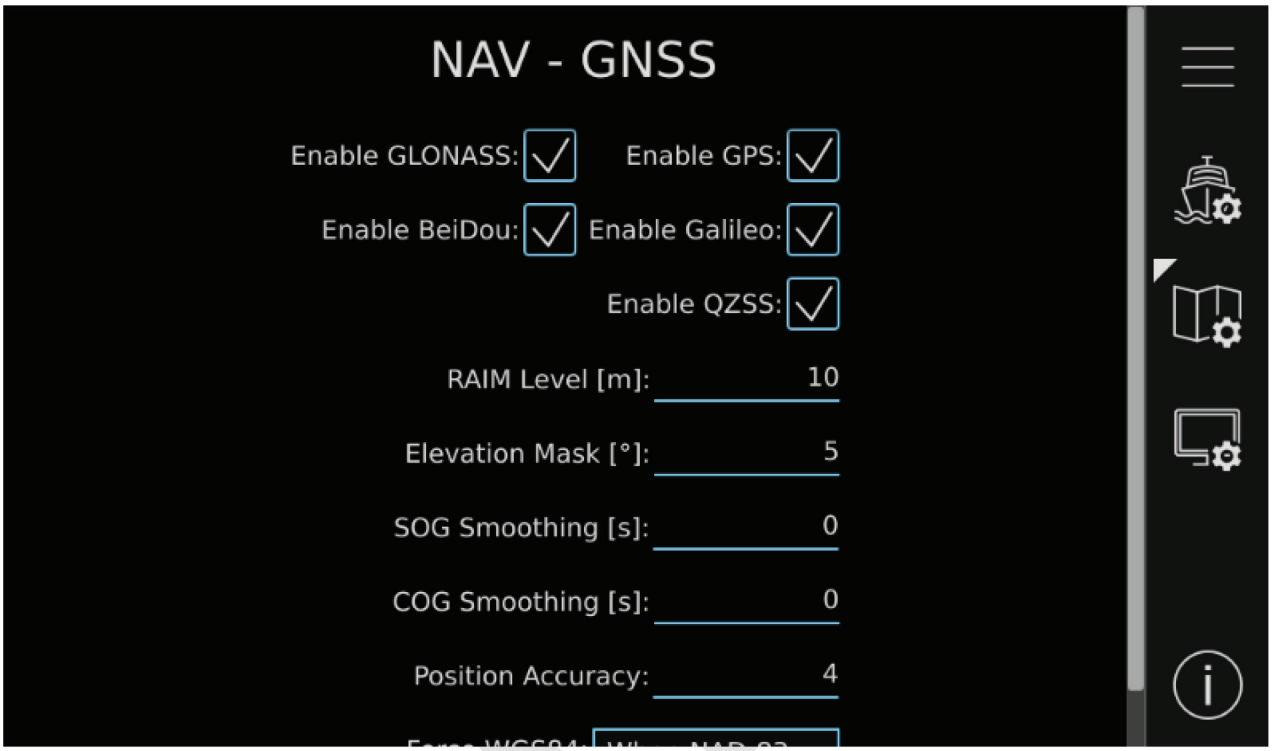


Figure 10: Multi-system GNSS Receiver (Saab TransponderTech R6 NAV)

With respect to jamming, various GNSS systems deliver different services at different frequencies. For the open service used for type-approved maritime equipment, all receivers are tested against IEC 61108-x series test and performance standards. The Galileo standard (IEC61108-3) offers multi-frequency reception of Galileo E1 (1.559-1.610 MHz) and E5 (1.164-1.215 MHz) signals. Using different frequencies will to some extent mitigate against an attack, since most attacks focus on the GNSS E1 frequency. Multi-frequency jamming attacks can still be successful, though, and most GNSS receivers continue to use single frequencies at present, although plans are in place to upgrade them soon.

Aiding the GNSS receiver with an IMU (Inertial Measurement Unit) and appropriate alarm management plan would improve the ability to detect an attack and manage poor GNSS signal quality, or temporary signal loss. The IMU can support GNSS receiver with measurements of the unit acceleration and angular velocity. While the

IMU can sometimes "take over" during GNSS outage, usings its sensors to track movement and orientation to perform what could arguably be called "digital dead-reckoning", **the user must be aware of the errors which IMU can introduce** (especially over time) – such as bias and drift – and factor them in the position calculations. The manufacturer's manual should be consulted so that equipment limitations are known and all officers made aware of them.

Spoofing countermeasures

Viable countermeasures against spoofing include the use of Controlled Reception Pattern Antennas (CRPA), which is adaptive and generally larger than that of typical GNSS antennas. The CRPAs work by exploiting so-called spatial diversity, utilising the fact that the desired satellite signals, and the unwanted spoofing and jamming signals, generally arrive from different directions. In simple terms, you create a spatial filter, one of which removes signals that arrive from a particular direction but letting through signals from other directions. To achieve this, rather than use a single antenna, an array of antenna elements can be used. Additional cost must be factored in when installation of CRPAs is considered, but their efficiency has been proven in operation.

However, when considering vessels with multiple GNSS antennas to support different functions, the question may arise which antenna, or system, is to be protected as priority. Should all antennas be replaced with a CRPA, or should we CRPA-protect only GNSS receiver(s) used to feed GNSS data to all ship systems, especially ECDIS? The answer is not straightforward, and the extra cost must be considered.

Against very simple spoofing attacks, the monitoring of certain GNSS receiver Key Performance Indicators (KPI) can be successful, such as monitoring for clock jumps, unusual or implausible signal-to-noise density ratios, or differences between code and carrier measurements. It is recommended to check with the equipment manufacturer how their equipment, or hardware and software updates, can mitigate risks and solve these issues.

Advanced cryptographic techniques can be effective. GNSS providers Galileo and GPS will soon provide Navigation Message Authentication (NMA), which involves a signal consisting of encrypted data stream that cannot be generated by a spoofer.

Other measures exist but will require adequate software and hardware to support them (for example, software for ECDIS systems and the new GNSS receiver). These measures include:

- Flywheel algorithms to prohibit the system from immediate jumps in location and time in the GNSS Receiver (ECDIS or external PNT software).
- Similarly to jamming preventative actions, aid the receiver with an IMU. Even a low-cost IMU could be very effective in operation.
- Consider using Loran/E-Loran and/or Ranging (R-Mode) receivers as terrestrial navigational systems, where and when they become available.

Meaconing countermeasures

Against meaconing which includes the use of signal repeaters, similar countermeasures apply as for spoofing. The only exception is that cryptographic techniques, or encrypted navigational messages, which spread code generation by cryptographic means and NMA, do not always help against meaconing, depending on the GNSS receiver's architecture and anti-replay features. This is because unlike in the spoofing attacks, the GNSS repeater does not need to know the structure of the GNSS signal it re-transmits.

APPENDIX A: Reporting of jamming and spoofing events

There are systems in place that allow ships and managers to report GNSS-related problems, including suspected jamming and spoofing attacks. The international working group IDM (Interference Detection and Mitigation Task Force) has been set up to coordinate international efforts in detection and mitigation of GNSS interferences. However, a uniform international reporting mechanism has not been established yet, although such a system would be desirable and useful to be set-up in the future.

Reporting systems known to INTERTANKO at the time of print are detailed as follows.

GPS problem reporting

United States Coast Guard Navigation Centre welcomes all reports regarding service degradations, disruptions, or other incidents or anomalies. All personal data is kept private and will only be used when more information is needed or if further clarification required. It is requested that submissions are as complete as possible when reporting an incident. Navigation Centre: US Coast Guard (NAVCEN) recommends that the steps below are followed before a GPS problem is reported:

- Reset the device by cycling power to the unit.
- Confirm the settings for the GPS unit or GPS application.
- Refer to the equipment manual.
- Update the equipment software or firmware.
- Contact the equipment manufacturer for additional assistance.
- For more information, refer to the GPS Frequently Asked Questions page.

To submit a report to NAVCEN, please fill in the form on the following link:
https://www.navcen.uscg.gov/contact/gps-problem-report

Another valuable resource for guidance on resilience measures can be found from the Cybersecurity and Infrastructure Security Agency (CISA at **www.cisa.gov**) and their Positioning, Navigation, and Timing (PNT) team.

The PNT team can be contacted by the following email: **NRMC@hq.dhs.gov**

www.cisa.gov/topics/risk-management/positioning-navigation-and-timing (PNT / Risk Management)

Masters can use 24/7 watch's email **NAVCENWatch@uscg.mil** if they need additional support and guidance.

Galileo incident report form

The European GNSS Service Centre (GSC) welcomes reports on Galileo system performance degradations, disruptions, interferences or any other incident. Inputs will be processed and the incident investigated.

Some fields are required for submission, but all personal data will be kept private only to be used if more information is needed or if further clarification is required. It is requested that submissions are as complete as possible when reporting an incident.

To submit a report to the GSC, please fill in the form on the following link:
https://www.gsc-europa.eu/contact-us/galileo-incidents-report-form

Tracking of events: NATO Shipping Centre (NSC)

The NSC is the link between NATO and the merchant shipping community. It is the primary point of contact for the exchange of merchant shipping information between NATO's military authorities and the international shipping community, facilitating communication and cooperation. The NSC is permanently manned by NATO personnel and is located at NATO Maritime Command (MARCOM).

As GNSS disturbances must be regarded as a serious threat to safety of navigation, the respective NAVAREA Coordinators are responsible for promulgating warnings and keeping track of incidents. NATO is strongly concerned about GNSS interferences and requests assistance with reporting which can aid constructing a comprehensive picture of this activity and help to assess full impact to the maritime domain. The NATO Shipping Centre (NSC) remains the point of contact for merchant vessels and shipping companies.

Please report the following:

/1/DTG (DATA TIME GROUP)/UNIT LAT/ LONG POSITION AT REPORTING TIME//

/2/TRACK WHILE OBSERVING INTERFERENCES/FROM LAT/LONG-TO LAT/ LONG//

/3/DURATION WHILE OBSERVING INTERFERENCES- START AND END TIME//

/4/INTERFERENCE TYPE (SYSTEMS AFFECTED AND HOW)//

/5/ASSESSED DIRECTION OR COVERAGE AREA OF INTERFERENCE//

/6/NAVIGATION – SECONDARY MODES OF NAVIGATION USAGE AND ACCURACY VS GPS SYSTEMS//

/7/COMMUNICATIONS SYSTEMS AFFECTED

/8/OVERALL ASSESSMENT OF OBSERVATIONS – PROVIDE FREE TEXT COMMENT ON THE EVENT AND ADDITIONAL INFORMATION THAT CAN BE CONSIDERED INTERESTING.

Please submit reports to NSC by email to: **info@shipping.nato.int**

NATO Shipping Centre (Duty Officers)

Atlantic Building

Northwood Headquarters, UK

Telephone +44 (0) 1923-956574 (24 hours)

Fax +44 (0) 1923-956575

Sandy Lane, Middlesex

HA6 3HP Northwood, UK

https://www.mc.nato.int
https://shipping.nato.int/nsc

APPENDIX B: Types of Satellite Positioning Systems

GNSS is a worldwide position, time and velocity radio determination system comprising space, ground and user segments (IMO A.915). For maritime users, Class will recognise a GNSS as a system which meets the carriage requirements for position-fixing equipment for a Worldwide Radio Navigation System (WWRNS) as per the IMO Resolution A.1046 (27). However, regional (non-global) positioning systems exist to either provide independent position signal in the region they serve, and/or augment the existing GPS/GNSS signal accuracy and stability.

Global

GNSS types include the USA's NAVSTAR Global Positioning System (GPS), Russia's Global'naya Navigazionnaya Sputnikovaya Sistema (GLONASS), Europe's Galileo, and China's BeiDou Navigation Satellite System.

The performance of GNSS is assessed using four criteria:

1. Accuracy: the difference between a receiver's measured and real position, speed or time.
2. Integrity: a system's capacity to provide a threshold of confidence and, in the event of an anomaly in the positioning data, an alarm.
3. Continuity: a system's ability to function without interruption.
4. Availability: the percentage of time a signal fulfils the above accuracy, integrity and continuity criteria.

USA's NAVSTAR Global Positioning System (GPS)

The GPS is a US-owned utility that provides users with positioning, navigation, and timing (PNT) services and global coverage. The US Air Force develops, maintains, and operates the space and control segments. There is an ongoing modernisation program adding further civilian and military signals capacity to GPS. The first satellite to support L2C (second civilian GPS signal at 1227 MHz, designed specifically to meet commercial needs) was launched in 2005. L2C was reported to be currently available on 25 satellites. Further modernisation is ongoing with the newer L5C (1176.45 MHz reserved almost exclusively for aviation) and the new L1C signal (1575.42 MHz broadly used for navigation) with an expected fully operational phase by 2030 and the replacement of all GPS Block II satellites by Block III ones supporting all new signals. GPS III will broadcast a similar signal and navigation scheme as Galileo and enable civilian multi-frequency use, as well as similar authentication modes. The system is expected to provide a Navigation Message Authentication service soon (see the later section on *Navigation Message Authentication (NMA)*).

Russia's Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS)

GLONASS is a satellite navigation system operating in the radionavigation-satellite service. It provides an alternative to GPS and is the second navigational system in operation with global coverage and is of comparable precision.

The GLONASS satellite designs have undergone several upgrades, with the latest version, GLONASS-K2, scheduled to enter service soon. Its first satellite was successfully launched on 7 August 2023. The K2 satellites are informed to use a novel navigation signal with a code-protected selection transmitting three signal types, including two in the L1 and L2 frequencies for military users, and one channel in the L1 range accessible to the civilian users.

GLONASS utilises what is called a frequency division multiple access method (FDMA), whereas GPS and Galileo use a code division multiple access (CDMA) technique. However, the modernisation plan which is presently in progress will also have CDMA included.

Galileo: The European global satellite-based navigation system

Galileo is Europe's GNSS, providing improved services related to the use of dual and/or multi-frequency processing. Galileo has made significant progress in recent years and has been declared fully operational since 2024. The program is designed to be compatible with all existing and planned GNSS. Further to this, Galileo already includes Navigation Message Authentication (see the later section on *Navigation Message Authentication (NMA)*).

Galileo offers several free of charge open services on E/L1, E5a/b and E6 frequencies, including a new high accuracy service (Galileo HAS) since 2024. Galileo provides a public regulated service (PRS) with encrypted signals and high accuracy, comparable to GPS military codes. The PRS is dedicated for administrations, police, military and SAR/disaster control units. The merchant fleet will most likely use open services from different frequencies with high accuracy service and message authentication in the future.

Spoofing capabilities are high on the list of priorities for Galileo. The Open Service Navigation Message Authentication (OS-NMA) is already transmitted, which offers some limited spoofing protection. Active works are in progress on introduction of encrypted Controlled Access Service (CAS) signal, which will give stronger protection against spoofing, but not jamming. For governmental users the Public Regulated Service will soon be available, offering the strongest level of protection, but this is only available to EU Member State-authorised entities.

Galileo has been offering E1/E5 dual-frequency capabilities for many years, and in fact has a third frequency, E6, which is also operational (used for the Galileo High Accuracy Service (HAS) and CAS)).

All Galileo services are provided free of charge.

China's BeiDou Navigation Satellite System (BDS)

The third generation of the BDS system (BeiDou-3) was reported as operational from July 2020 with the launch of its last satellite, although the final pair of back-up BDS satellites was informed as being sent to orbit in September 2024.

BDS offers a similar signal and message structure as Galileo as GNSS signals are based on the CDMA modulation. BDS is informed to consist of space segment with a hybrid constellation of satellites in three kinds of orbits. In comparison with other navigation satellite systems, BDS operates more satellites in high orbits, allegedly to offer better anti-shielding capabilities, which is particularly observable in terms of performance in the low-latitude areas.

BDS provides navigational signals of multiple frequencies and can improve service accuracy by using combined multi-frequency signals. Also, BDS is reported to allow navigation and communication function, possessing multiple service capabilities, including PNT, short message communication, international search and rescue, satellite-based augmentation, ground augmentation and "precise point positioning".

A more ubiquitous, integrated and intelligent, comprehensive national PNT system is scheduled to be established by 2035. Unsurprisingly, it will be named Beidou-4.

Augmentation systems

Augmentation systems are available in different ways. On one hand, regulated terrestrial services are provided by a lot of administrations all around the world, often referred to as IALA (International Organization for Marine Aids to Navigation) Beacon Network.

The IALA Beacon transmitters provide differential correction data for GNSS receivers. The differential beacon services have been recognised by IMO since 1996, and they have been an integral part of safe navigation ever since. IALA Beacon transmissions provide local correction data to improve accuracy for single-frequency GNSS receivers, as well as consistency and integrity information to enable failure warnings to the user.

On the other hand, Satellite-Based Augmentation Systems (SBAS) can enhance regional position accuracy and integrity. Those systems are managed by regional agencies. The EUSPA (EU Agency for the Space Program) in Europe provides the European Geostationary Navigation Overlay Service (EGNOS) for Europe and its surrounding seas, while the USA provides the Wide Area Augmentation System (WAAS), Japan the Multifunctional Satellite Augmentation System (MSAS), Russia the SDCM (System for Differential Corrections and Monitoring), while China is operating the BeiDou Satellite Based Augmentation system (BDSBAS) and India the GPS Aided Geo Augmented Navigation system (GAGAN).

Most modern GNSS receivers obtain SBAS data directly, without any further modifications or external receivers needed.

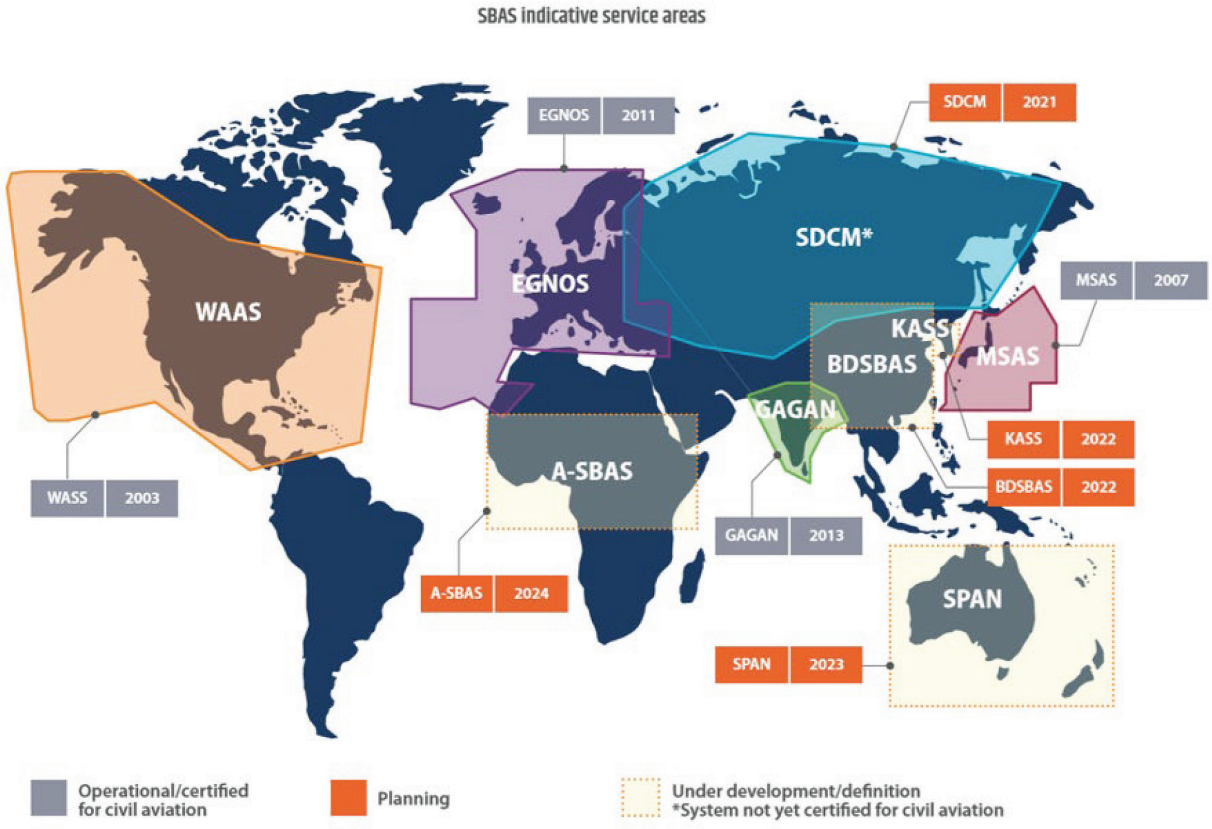


Figure 11: SBAS indicative service areas, Oct 2020 (source: SBAS IWG 36 meeting)

Regional

There are ongoing developments and employments of regional satellite-based systems such as the Japanese Quasi Zenith Satellite System (QZSS) and India's Regional Navigation Satellite System (IRNSS). These regional systems are recognised by IMO and may act like supporting systems for the global ones to improve the availability, accuracy and reliability of satellite navigation in local areas.

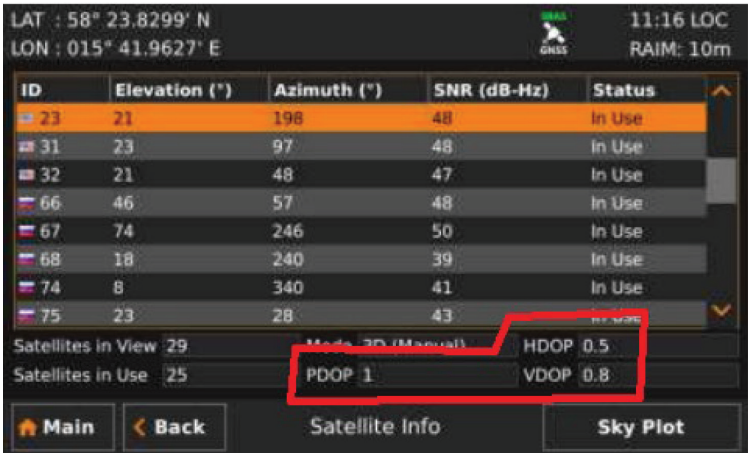
Quasi-Zenith Satellite System (QZSS)

It is worth noting that Japan's MSAS has been transitioned to being transmitted via the QZZS, a regional satellite navigation system designed to enhance accuracy, integrity and availability of GNSS signals. QZZS can now offer its own independent positioning services and augments GNSS signal, providing higher elevation angles in the Asia-Oceania region.

India's Regional Satellite Navigation System (IRNSS): NavIC (Navigation with Indian Constellation)

Designed to provide accurate positioning and timing services to users in India and a surrounding region extending up to approximately 1,500km beyond its borders, the system consists of a constellation of seven satellites, with two additional satellites on standby. Plans have been made to extend the system range to a 3,000km "buffer zone" around India. The development of NavIC was driven by India's need for an independent regional navigation system, particularly after experiencing some limitations with relying solely on GPS in the past.

APPENDIX C: GNSS receiver: Pocket guide on signal quality



Saab will display various DOP values in the status panel

Quick GPS/GNSS receiver reference guide

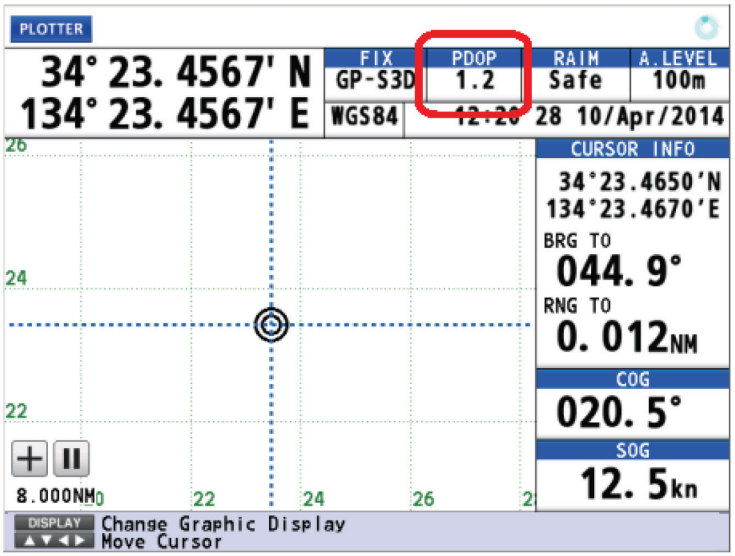
What navigators should know about their units

GNSS receivers are modern navigational aids, but they still rely on the operator's ability to comprehend, process and monitor the information provided. As with all navigational aids, navigators must be familiar with their limitations. Here is a list of things that each navigator should be aware of when navigating a vessel with the help of a GNSS receiver.

1. HDOP (PDOP/GDOP)

This term stands for Horizontal (Position/Geometric) Dilution of Precision and describes the position error influenced by how well the satellites are "spaced out" in the sky. Just like with the visual fixes, satellites should not be bunched up together as that may introduce errors or positional inaccuracies. The value is usually presented on a scale from 0.1 to 20. **The lower the value, the better**. However, the unit should be set to alarm the user if HDOP value starts to exceed 5 or 6. In the open ocean, HDOP shall not exceed 2.

The typical GNSS unit might also display VDOP (Vertical Dilution of Precision) – a measure of limited value to mariners, since altitude accuracy has not been proven critical to surface navigation.



Furuno displays PDOP value by default. PDOP will automatically change to HDOP if the receiver is in 2D mode.

You should be able to understand and demonstrate the following:

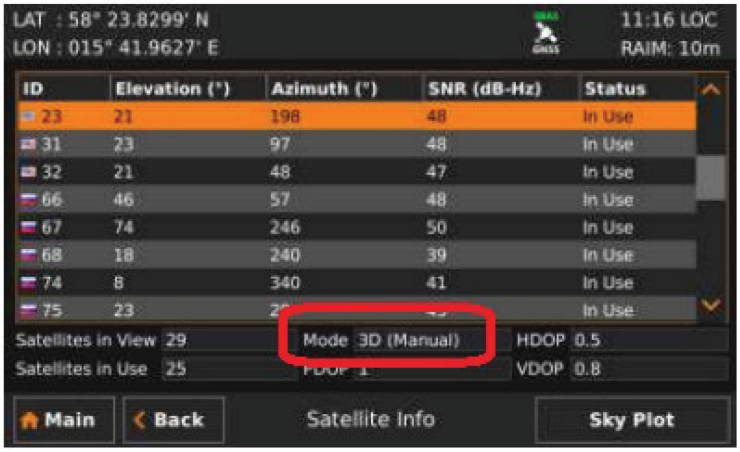
- **How to display DOP values on your receiver.**
- **Know what HDOP alarm settings are and how to set them.**

2. 2D vs 3D

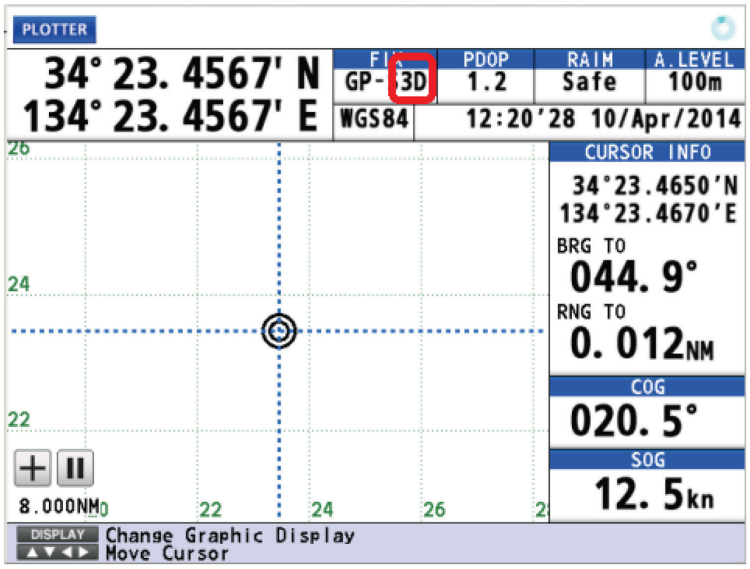
All GNSS receivers have the ability to display vessel's position in 2-dimensional (Lat + Long) or 3-dimension "plane" orientation (Lat + Long + Altitude). The key difference is that to plot the position in two dimensions, GNSS receivers need three satellites, and for the third dimension minimum of four satellites are necessary. In most situations, the receiver can be safely set to 3D without any issues. It is only closer to the polar regions where satellites might be scarce and when the receiver should be switched over to 2D to maximise availability of satellites, to be manually focused on accurate and stable 2D position data. Beware that when using GNSS receivers in 2D mode, the antenna height must be set correctly in the settings as the wrong value may result in position errors.

You should be able to demonstrate the following:

- **How will receiver present 2D or 3D display mode.**
- **How to amend this setting.**
- **How to set the antenna height.**



SAAB will display the fix mode in the satellite status panel.



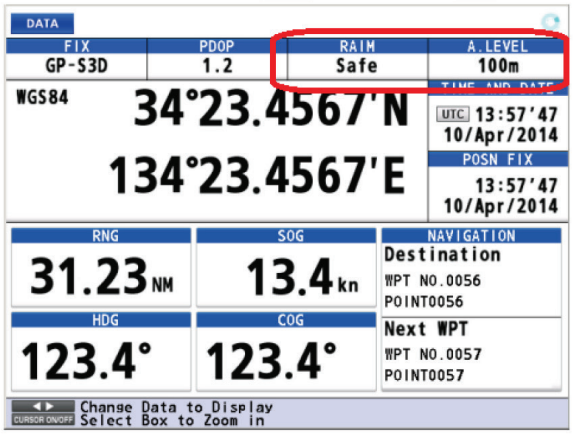
Furuno displays the plotting mode on the default screen in the "Fix" tab. It will either state 3D or 2D

3. RAIM

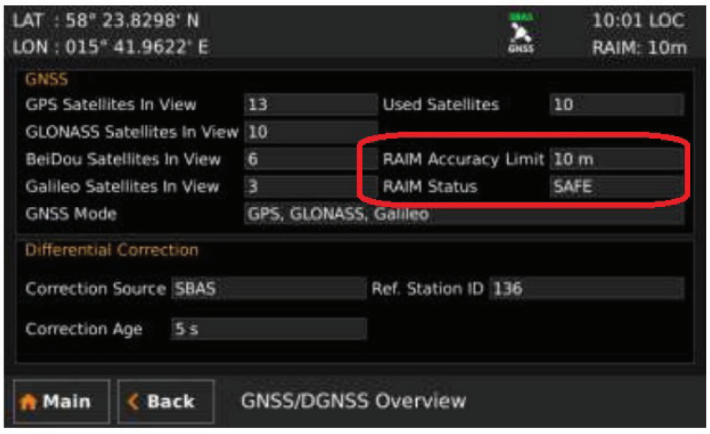
RAIM (Receiver Autonomous Integrity Monitoring) is a function independently verifying the accuracy of position displayed by the receiver. To fix a vessel's position, only three or four satellites are required, but usually, many more are visible. While the GNSS receiver selects the best-fit satellites automatically, RAIM will utilise the unused satellites to plot "alternative" positions, which, despite being viewed as "suboptimal", should obtain a position of comparable accuracy. The alarm margin of error can be selected by the user and is usually indicated in metres. RAIM has three main indications of its positioning status: SAFE, UNSAFE and Caution. When "**Safe**" informs that all positions are within the margin of error, "**Unsafe**" alarms that some of the positions are being plotted outside of the indicated margin of error. The user will see "**Caution**" when the RAIM functionality cannot be used (not enough visible satellites or when RAIM functionality is turned off).

You should be able to demonstrate the following:

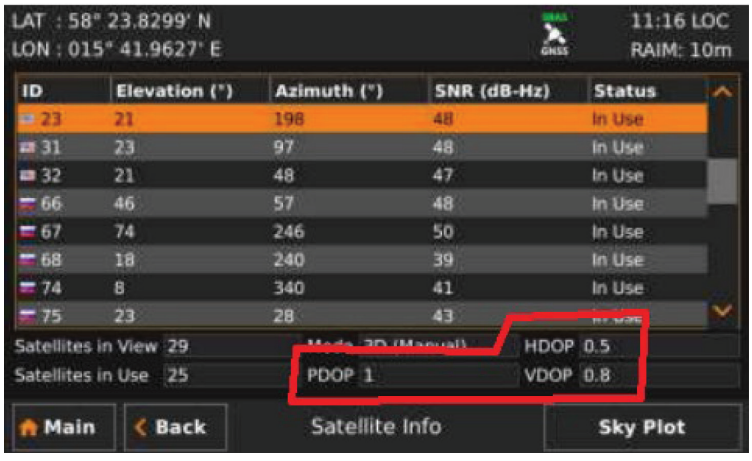
- **How to confirm RAIM is ON and what is the positioning status.**
- **How to turn RAIM on and off and how to change the desired margin of error.**



Furuno displays RAIM status and the set accuracy level on the default screen. Accuracy level can be changed manually in the settings panel.



SAAB will display RAIM status with a coloured LED on the receiver (Red, Yellow, Green) and in the Satellite status menu.

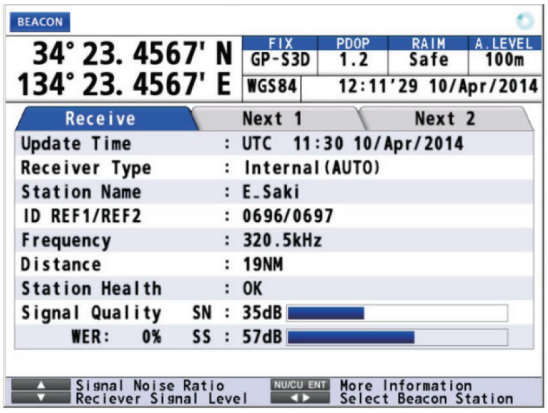


4. DGNSS (DGPS)

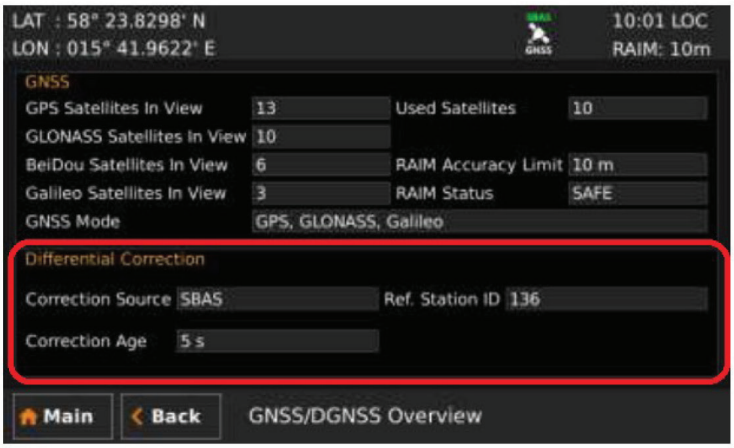
DGNSS (or DGPS) is a differential GNSS system which uses fixed terrestrial stations (which geographical is position is well known) to fine-tune vessel position through transmission of GNSS position corrections to all vessels in the vicinity. Correction quality generally decreases with distance to the terrestrial station. DGNSS corrections are transmitted via VHF and require a separate unit/ antenna to receive them. DGPS should only be turned on when DGNSS stations are available as the receiver may alarm if DG signal is unavailable when the functionality is on.

You should be able to demonstrate the following:

- **How to turn on/off the DGNSS (DGPS).**
- **How to manually select DGNSS (DGPS) stations.**
- **Where would you find information about DGNSS (DGPS) stations.**



Furuno DGPS status is displayed in the default "Fix" panel with notation "GP-D3D" where D stands for differential, as well as in Beacon settings



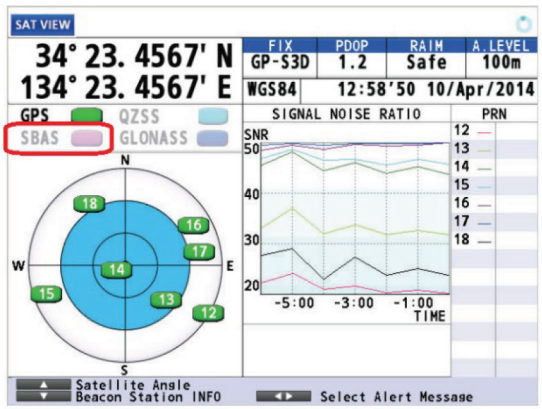
SAAB will display beacon status below the GNSS status panel. Note that SBAS and Beacon status are displayed in the same spot and are mutually exclusive.

5. SBAS

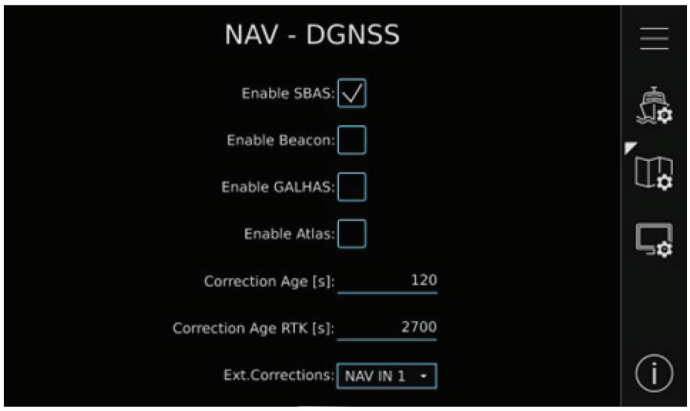
SBAS is the Satellite Based Augmentation System which works similarly to the DGNSS (DGPS). Fixed ground stations are comparing their real positions with GNSS indications, but instead of relaying corrections directly to vessels via VHF, they are transmitted to geostationary satellites which transmit them back to the vessels. The main SBAS systems are: WAAS (USA), EGNOS (EU), MSAS (Japan), QZSS (Japan) and GAGAN (India). Not all receivers will be able to accept SBAS corrections from each system. SBAS, just like DGPS, can be most valuable in coastal navigation.

You should be able to demonstrate the following:

- **What SBAS systems your receiver can use.**
- **How to turn SBAS corrections on and off.**
- **How do you know SBAS corrections are being received?**



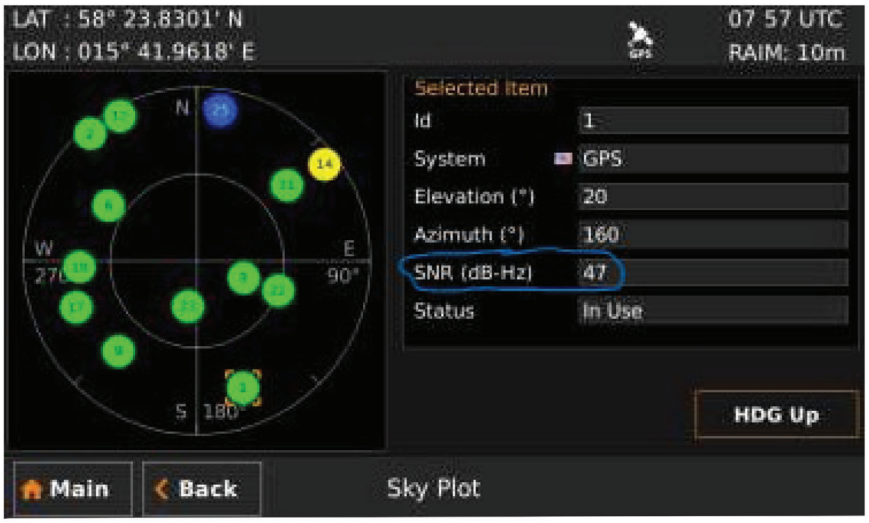
Furuno SBAS satellites can be viewed in the Sky View panel. The Fix tab will also indicate SBAS enhancement with an "S" prefix i.e "GP-S3D"



SAAB receiver with its GNSS SBAS enabled (ON)

6. Signal-to-Noise Ratio (SNR)

Signal-to-noise ratio (SNR) which depicts signal strength relative to noise is a crucial indicator of GNSS signal quality. A high SNR signifies a clear signal with minimal interference, while a low SNR suggests a weak or obstructed signal. All GNSS receiver manufacturers design their receivers to optimise SNR for accurate positioning.



SAAB receiver with SNR value

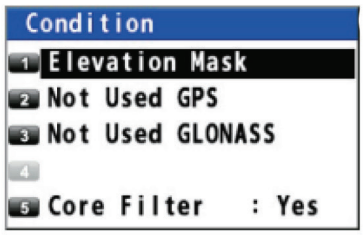
For this manufacturer, depending on how good the signal (SNR) received from a satellite is, shows the target items changing colour from green to yellow or blue. However, the alarms and status symbols may look different for other manufacturers. Mariners must consult the equipment maker manual to verify which warning is generated for this GNSS receiver type.

7. Elevation Mask

Elevation mask allows the filtering out of satellites that are too low on the horizon, "instructing" the receiver NOT to use them. The lower on the horizon a satellite is, the more atmospheric distance the GPS signal has to travel before it reaches the receiver, which increases errors. The typical default value is five degrees, but that may be reduced in very high latitudes due to lower levels of satellites being available.

You should be able to demonstrate the following:

- **What your elevation mask setting is.**



Furuno Elevation Mask settings can be set in Condition settings panel

Furuno Elevation mask settings are visually indicated with blue circle on the Sky Plot. SAAB elevation mask settings can be accessed in General Settings

References

- IALA Guideline G1180: Resilient Position, Navigation and Timing (PNT)
- MSC.1/Circ.1575 - Guidelines for Shipborne Position, Navigation and Timing (PNT) Data Processing
- MSC.401(95) – Performance Standards for Multi-System Shipborne Radionavigation Receivers
- Satellite-derived Time and Position: A Study of Critical Dependencies; Report, UK Government
- The economic impact on the UK of a disruption to GNSS; Report, London Economics
- GNSS Jamming and Spoofing: Hazard or Hype? Alexander Rügamer, Jan Wendel
- Quantum Navigation, Dr Alan Bury, Liverpool John Moores University (Nautical Institute)

APPENDIX D: Bridge procedure for GNSS Spoofing and Jamming

NAVIGATIONAL PROCEDURES **(Company Name)**

GNSS Jamming or Spoofing .....

Navigational Officer to perform this procedure

- ☐ Actions to detect GNSS interference or poor signal
- ☐ Use secondary ECDIS positioning method through independent radar and visual verification (LOP, EP, ER)
- ☐ Continuously monitor discrepancies and "accuracy jumps" between ECDIS primary and secondary positioning method
- ☐ Active use and monitoring of radar overlay on ECDIS (if fitted)
- ☐ Comparison of COG and Gyro Course
- ☐ Comparison of SOG and Log Speed
- ☐ Monitor GNSS receiver working parameters: SNR, HDOP, RAIM, SBAS, DGPS status
- ☐ Check GNSS Receiver Jamming/Spoofing status, if available
- ☐ Check and monitor GNSS time data to confirm no time spoofing is taking place

If Jamming or Spoofing is detected

- ☐ Select secondary position sensor (independent from GNSS): DR, LOP, EP or ER
- ☐ A: Confirm if all GNSS receivers are affected
- ☐ B: If one of GNSS receivers is unaffected by attack, manually switch to this receiver
- ☐ C: If one of GNSS global systems (GPS, GLONASS, Galileo, Beidou) is unaffected by attack, switch to this system
  NOTE: If the switch to automatic ECDIS data feed from unaffected GNSS receiver or system is not possible, keep manually plotting position displayed by them on ECDIS
- ☐ If actions B and C are unable to provide reliable satellite position, stick to DR or EP mode
  NOTE: Never rely on other ship's AIS position signal since that, too, can be unreliable Inform the Master. Call lookout to the bridge if not present
- ☐ Make sure Autopilot is working normally. Change to hand steering if required
- ☐ De-activate AIS overlay feature on ECDIS and ARPA/radars
- ☐ If fitted, activate radar overlay on ECDIS if in confined waters and **verify position basis radar bearing(s) and/or distance(s)**. Monitor the position and plot it frequently
- ☐ Use STW (Speed Through Water) and COW (Course Over Water) with trails activated on ARPA/radars
- ☐ Assess distance to closest navigational danger and plan to give it very wide berth (big CPA)
- ☐ If the GNSS receiver is equipped with IMU, use it with caution to continue navigation
  NOTE: IMU limitations must be known to OOW and due to possibility of introducing significant errors over time, this must be done directly under Master supervision

Continues opposite...

If Jamming or Spoofing is detected Continued...

- ☐ Record speed log, gyro and magnetic gyro values, wind speed, current/tide
- ☐ Use parallel indexing techniques to control set and drift in coastal navigation
- ☐ **Frequently verify position** through:
  - ☐ Radar and visual measurements in coastal navigation
  - ☐ Dead-reckoning in deep sea (using recorded values of log, speed, gyro, weather)
  - ☐ Celestial observations, if equipped with a sextant and in good weather
- ☐ Inform the Company. **Inform the engine team** and keep updating them on situation
  NOTE: If necessary, STOP the ship to gain more time for safe situation reassessment
- ☐ Make passage plan to safe anchorage in case it was needed (keep it on stand-by)
- ☐ Have the main engine ready for immediate manoeuvring and rapid speed changes
- ☐ Record evidence of GNSS interference (signal loss) occurrence for future learnings
- ☐ Report event to coastal state, UKMTO, Flag and NATO Shipping Centre (NSC)
- ☐ Check Gyro for speed/latitude corrections. Manually feed GNSS position if required
- ☐ Check GNSS input for GMDSS, ODME, Autopilot and insert position manually if possible
- ☐ Verify GNSS time data to ensure correct time is being used

INTERTANKO London
St Clare House
30-33 Minories
London EC3N 1DD
United Kingdom
Tel: +44 20 7977 7010
london@intertanko.com

INTERTANKO Oslo
Nedre Vollgate 8
7th floor
PO Box 761 Sentrum
N-0106 Oslo
Norway
Tel: +47 22 12 26 40
oslo@intertanko.com

INTERTANKO Asia
70 Shenton Way
#20-04 Eon Shenton
079118
Singapore
Tel: +65 6333 4007
singapore@intertanko.com

INTERTANKO North America
801 North Quincy Street – Suite 500
Arlington, VA 22203
USA
Tel: +1 703 373 2269
washington@intertanko.com

INTERTANKO Athens
Spaces, 5th Floor
Ermou 56
Athens 105 63
Greece
Tel: +30 218 219 0430/0431
athens@intertanko.com

www.intertanko.com

INTERTANKO