IALA

IALA GUIDELINE

G1180
RESILIENT POSITION, NAVIGATION AND TIMING (PNT)

Edition 1.0

Dec 2023

urn:mrn:iala:pub:g1180

10, rue des Gaudines - 78100 Saint Germain en Laye, France
Tél. +33 (0)1 34 51 70 01- Fax +33 (0)1 34 51 82 05 - contact@iala-aism.org
www.iala-aism.org

International Association of Marine Aids to Navigation and Lighthouse Authorities
Association Internationale de Signalisation Maritime

DOCUMENT REVISION

Revisions to this document are to be noted in the table prior to the issue of a revised document.

Date	Details	Approval
Dec 2023	1st edition	Council 79

CONTENTS

CONTENTS

List of Tables

List of Figures

1. INTRODUCTION

1.1. BACKGROUND

Today’s vessels and many Marine Aids to Navigation (AtoN) rely on electronic Position, Navigation, and Timing (PNT) information, which is predominantly derived from Global and Regional Navigation Satellite Systems (GNSS/RNSS). However, several studies indicate that GNSS signals are vulnerable to intentional and unintentional interference and common failure modes [1], [2]. RNSS which are based on similar technology as GNSS are facing the same vulnerabilities. However, to improve the readability of this Guideline, GNSS and RNSS are subsumed under the designation GNSS, since it is not relevant for the considerations here whether they are worldwide or only regionally receivable.

The International Maritime Organisation’s (IMO) e-Navigation strategy recognises the importance of resilience of electronic systems and mentions especially position fixing systems. The IMO’s e-Navigation strategy states [3]:

> “e-Navigation systems should be resilient and take into account issues of data validity, plausibility and integrity for the system to be robust, reliable and dependable. Requirements for redundancy, particularly in relation to position fixing systems, should be considered.”

The increasing reliance on GNSS in all types of position finding and navigation, including position and time inputs to Automatic Identification System (AIS), underlines the importance of an objective consideration of possible areas of vulnerability and a consideration of measures to reduce or mitigate such effects. The growth of autonomy and the introduction of autonomous vessels further highlights the importance of resilient PNT information.

Resilient PNT is defined as position, navigation, and timing services made resilient by building-in, or otherwise providing, standby capacity or by switching to alternative means [4]. It is best achieved by a combination of multiple dissimilar PNT sources. GNSS, terrestrial PNT services, augmentation services and ship-based sensors can be considered as candidates for resilient PNT system components.

The general responsibilities of Maritime Authorities related to the provision of PNT services may be derived from Chapter V of the IMO Safety of Life at Sea (SOLAS) convention, which states:

> Regulation 13 - Establishment and operation of aids to navigation
>
> 1. Each Contracting Government undertakes to provide, as it deems practical and necessary either individually or in co-operation with other Contracting Governments, such aids to navigation as the volume of traffic justifies and the degree of risk requires.
>
> 2. In order to obtain the greatest possible uniformity in aids to navigation, Contracting Governments undertake to take into account the international recommendations and guidelines when establishing such aids.
>
> 3. Contracting Governments undertake to arrange for information relating to aids to navigation to be made available to all concerned. Changes in the transmissions of position-fixing systems which could adversely affect the performance of receivers fitted in ships shall be avoided as far as possible and only be effected after timely and adequate notice has been promulgated.

1.2. SCOPE

This Guideline intends to help understanding PNT systems vulnerabilities and their potential impacts on AtoN services, vessel traffic services and users of these services, and to consider measures to increase PNT resiliency and mitigate associated risks. Because of the wide use of GNSS as a primary source of PNT information in the maritime domain, this Guideline is focused on GNSS vulnerabilities and possible mitigation measures for GNSS failures.

In this Guideline, Section 2 introduces sources of PNT vulnerabilities that can cause unavailability of reliable GNSS service. Section 3 discusses the impacts that the loss of reliable PNT information can cause to AtoN service and to vessel systems. Section 4 considers measures to identify risks, and Section 5 introduces options to mitigate the impacts of GNSS failures to achieve the required level of PNT service resilience.

2. SOURCES OF PNT VULNERABILITIES

2.1. GENERAL

Some vulnerabilities are common to all types of electronic navigation systems, including GNSS. These vulnerabilities are related to the general performance of communication links (e.g. signal strength, frequency bands), security (e.g. integrity and authenticity of signals) and hardware and software components. The service itself can fail, for example, because of deliberate or accidental damage to the service infrastructure, signal may be disrupted due to natural or man-made interference or may originate from a falsified source, or the user receiver can be malfunctioning.

2.2. SIGNAL INTERFERENCE

Radio signals can be affected or disrupted by natural events, such as space weather, natural or artificial obstacles or man-made interference. Effects of natural events may be observed in large areas and during any phase of navigation, whereas the risk of man-made interference as well as the presence of natural or artificial obstacles, is higher in coastal waters and ports. The majority of man-made interference is unintentional [5] and affects only limited line-of-sight areas, but the risk of intentional wide area man-made interference should also be recognised.

Given that GNSS satellites are typically orbiting at about 20,000 kilometres, only extremely low power levels of the satellites' signals are available at the earth's surface[1]. Therefore, the signals are particularly susceptible to interference.

2.2.1. NATURAL INTERFERENCE

The propagation of radio signals is affected by scattering, reflection, and attenuation caused by obstacles in the propagation path and the properties of propagation media. Observed effects vary depending on the signal frequency. International Telecommunication Union (ITU) publishes comprehensive guidance related to propagation effects [6], [7], [8].

GNSS signals travel from satellites to the receiver through the Earth's atmosphere, which comprehends four different layers or regions, being from the lower to the upper regions from Earth's surface: troposphere, stratosphere, mesosphere, and thermosphere [9]. The two upper layers, mesosphere and thermosphere (together also referred as the ionosphere), contain electrically charged particles (i.e. ions) as well as free electrons. The presence of these particles impacts the propagation speed of GNSS signals, resulting in a delay. The delay is not constant and depends on both the frequency of the signal and the existing electron density. The value of the electron density is fluctuating and depends on the time of day (i.e. day vs. night), time of the year, season and solar activity. The variability of the solar activity entails space weather events (e.g. solar flares, geomagnetic storms) that cause irregular spatial and temporal disturbances to GNSS signals in the ionosphere, which may cause delays, interference, and noise, leading to errors in PNT estimations or totally preventing the tracking of GNSS signals. The type and expected frequency of these ionospheric disturbances varies, for example, depending on the latitudes being also worsen in solar cycle maxima. Further information on the effects of space weather to GNSS is provided in ANNEX A.

[1] Minimum signal power level of -160 dBW for GPS signals and -154 dBW for Galileo signals.

The lowest atmospheric layer, troposphere, may also cause disturbances to the GNSS signals. The delays caused in this layer depend on the changing humidity, temperature and atmospheric pressure (as well as on the transmitter and receiver antenna locations). Unlike the ionospheric disturbances, the effect of this layer into the GNSS signals is not frequency dependent. The tropospheric delay has two main components [10]:

- The hydrostatic component, associated with the dry gases in the troposphere. The effects of this component vary with the local temperature and pressure. However, this delay component is quite predictable and can be modelled using the law of ideal gases. The error induced is between 2 to 10 meters.
- The wet component, caused by water vapour and condensed water (e.g. clouds). This delay component depends on the weather conditions and is therefore quite random and difficult to model. It is particularly prevalent in areas with high humidity, such as near coastlines, and during adverse weather conditions, such as heavy rain or snow. Fortunately, the delay induced is smaller than the hydrostatic one being about tens of centimetre.

There is a very common type of interference that affects GNSS receivers known as multipath. This phenomenon occurs when a satellite signal is received at the user GNSS receiver 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. Complementary to this phenomenon, there is another quite similar interference that also affects GNSS signals reception at the receivers. This undesired phenomenon is associated to the direct signal blockage of GNSS signals due to natural or man-made 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 the pseudorange measurement 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 [11].

The GNSS signals can also be totally blocked. This is not considered as signal interference but shall be taken into account when estimating possible disturbances on GNSS signals reception by the user. As it was introduced in the previous paragraph, 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 by the user. A situation, where the GNSS signal does not reach the receiver at all is referred to as shadowing or obstruction which will result into 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 which is related to the inaccuracy of the position measurement. The smaller the DOP value is the more precise position is calculated.

2.2.2. MAN-MADE INTERFERENCE

Man-made interference can be either unintentional or deliberately generated. The radio spectrum is in efficient use, and despite regulation and licensing, unintentional interference between radio transmissions cannot be totally avoided. Navigation signals may be accidentally or intentionally blocked by other high-power signals or lock into strong deliberately transmitted falsified signals.

2.2.2.1. Unintentional interference

Unintentional sources of man-made GNSS interference include strong RF signals, harmonics or intermodulation products from powerful transmitters operating in band or adjacent frequency bands or from emitting sources close to GNSS receivers. These can be for example television or radio broadcasting stations, microwave communication links or Vessel Traffic Service (VTS) surveillance radars. Onboard equipment like satellite uplinks and radars may also cause interference to vessel's own GNSS receiver or other GNSS receivers in the vicinity. Interference has also been noted from poorly designed consumer-grade equipment such as active TV antennas on the vessel itself or other vessels in its proximity [12]. This type of interference may temporarily prevent the receiver from tracking the satellite signals and provide a PNT solution.

2.2.2.2. Intentional interference

When interference is intentional, narrow-band or broad-band signals are radiated deliberately to prevent the reception of navigation signals. This type of GNSS interference is called jamming. Typically, a one-watt transmitter on a hilltop is sufficient to disrupt every GNSS receiver across the horizon [1]. Jamming activities have multiplied in the last years and the probability of these risks to materialise further has also grown significantly and may continue to grow for some time. The main causes are:

- Aim to avoid GNSS tracking for privacy or other reasons using individual unauthorised Personal Privacy Devices (PPDs)
- Availability of affordable commercial off-the shelf (COTS) technology
- Availability of free training materials and hacking guides on internet with minimum knowledge necessary to implement
- Growing number of events with the military character that lead to denial of service

When the jamming is done by individual persons, for example for privacy reasons, the initial intention is not to deny GNSS service from other users. Due to the low level of GNSS signal strength, negative effects on other nearby receivers are difficult to avoid.

Another type of intentional man-made GNSS signal interference, but also more complex of being implemented is the transmission of falsified signals. This type of activity is called spoofing. The intention is to get the receiver to lock into simulated or re-transmitted GNSS signals (i.e. meaconing). In this way, the receiver can be deceived to provide a false PNT solution or no PNT information at all [13]. 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 and could be led into danger.

Spoofing requires much more effort than jamming, however, spoofing events have been increasingly observed and reported in recent years.

2.3. SYSTEM AND EQUIPMENT MALFUNCTION

Both the provision and use of PNT signals rely on electronic equipment. These, like any electric equipment, can suffer either from hardware, software or configuration failures, which may affect the quality and/or availability of the service and the ability of the end user to obtain the correct PNT solution. Equipment can suffer from power failure, be physically damaged by external causes (e.g. extreme weather conditions, fire), individual components can fail, accidents or errors may happen during maintenance and service infrastructure can be a target to a cyber-attack.

All GNSS consist mainly of three segments: (a) space segment, (b) control segment and (c) user segment. It is obvious that malfunctions can occur in all three segments.

2.3.1. MALFUNCTION IN THE SPACE AND CONTROL SEGMENT

GNSS constellations are designed to be very secure and robust. However, they may be considered as a target during times of war, can be impacted by space weather events or affected by human error. This could affect the performance of a single satellite, multiple satellites or result in a total system failure. Every GNSS has experienced such failures, for example, in January 2016, the United States Air Force (USAF) reported a Global Positioning System (GPS) constellation failure in which a -13µs timing offset was being transmitted through satellites in the L1 band for several hours (e.g. more than 12 hours). Regarding the European Global Satellite Navigation System (Galileo) constellation, a total system failure was reported in July 2019 for a total of 7 days [14]. Moreover, in April 2014, the Russian global navigation satellite system known as GLONASS experienced an outage for 10 hours [15].

Component failures may also cause malfunctions in the space segment, e.g. clock errors in the GNSS satellites. On 1st January 2004, for example, the clock on GPS satellite SV-23 drifted at a pseudo range error rate of 70.6 m/s for about 3 hours before the command centre was able to flag it as unhealthy. During this time, the pseudorange error increased from 0 to 285 km [16].

All these events may have caused failures or false PNT information for users.

2.3.2. Malfunction in the receiver segment

Failure of GNSS equipment onboard a vessel or AtoN equipment using GNSS signals is not uncommon due to power supply failure or to a fault, temporary or permanent, in the receiver or antenna. A less commonly observed failure mode is the permanent or temporary disablement of GNSS receiver antennae subjected to high power radar transmissions, owing to microwave damage to, or saturation of, internal components. GNSS receivers installed in floating AtoNs can be exposed to extremely harsh environmental conditions and may suffer from physical damage to the antenna or receiver itself.

Legacy GPS receivers may also face the problem of proper handling of the GPS week rollover which takes place every 1024 weeks (19.6 years). An unrecognised rollover may result in a jump back in the receiver time. The last rollover took place in April 2019. Additionally, some receiver may face internal time rollovers which can also result in a wrong receiver time [17]. GNSS receiver software updates are recommended to solve both issues.

3. IMPACT OF PNT FAILURES

3.1. MARINE AIDS TO NAVIGATION

Traditional marine AtoN service, which is provided for vessels via individual visual or radar aids, is not directly affected by GNSS failures. However, the maintenance of AtoNs may rely on GNSS as it may be used to accurately position floating AtoNs, and to remotely monitor AtoNs' positions during their operation.

Some AtoN services are directly relying on GNSS for time synchronisation and/or position fixing [18]. These may include:

- Synchronised lights which receive an accurate time reference from GNSS
- AtoNs using AIS technology and receiving an accurate time reference and, in case of floating AtoNs also an accurate position from GNSS
- IALA Beacon Differential GNSS (DGNSS) service which augments GNSS

Synchronised lights can be used along an approach channel to improve conspicuity. This operation requires that all the lights have a common precise time reference, which is usually obtained from GNSS. During a GNSS failure event, lights may not synchronise correctly leading to flashing characteristics contrary to that published and affecting the visual conspicuity to the pilot and mariner.

AIS system uses time division transmission technology where a common time reference is needed for synchronisation. Loss of GNSS may disturb the sharing of transmission time slots and thus cause problems for the system's communication capability and vessels' ability to receive AIS AtoN transmissions. Floating AIS AtoNs may also broadcast incorrect position information potentially resulting in conflicts with vessels' radar information or no position information at all. Furthermore, transmission of virtual AtoNs may be impacted and may be less useful as the mariner may not be able to determine their own position and, therefore, cannot determine the range and bearing to the AtoN.

AIS system can also be used to monitor AtoNs and provide information on their status. In case of GNSS failures, monitoring messages (6 and 21) may not be transmitted correctly. AtoN managers cannot check AtoN status and act if a fault occurs.

Floating AtoN may use GNSS to determine its position against the charted location. In cases of GNSS failure, such AtoN may provide false off-position alerts, potentially affecting AtoN over a large geographical area.

DGNSS IALA beacons are designed to meet Guideline G1112 [19]. Two architectures of DGNSS system design can be implemented and differ in their response to a GNSS failure, as described in Guideline G1129 [20].

- In a centralised system, corrections are computed within a centralised server or derived from Satellite Based Augmentation systems (SBAS). A loss of local GNSS signals doesn't impact corrections, but the integrity monitoring pre and post broadcast may be impacted.
- In a decentralised system, corrections are computed locally for each station from the GNSS position received by the local receivers. Loss of GNSS signals at the station does not allow the calculation of corrections. Vessels and users are notified that no corrections are available.

GNSS failures may also affect VTS. Vessels' AIS and Long-range Identification and Tracking (LRIT) equipment may lose their time reference and the source of accurate position. This could lead to vessels reporting faulty positions which conflict with information received from surveillance radars, electro optical systems and radio direction finders. Additionally, possible transmission slot collisions could block the normal reception of vessels' AIS reports.

3.2. SHIPBORNE EQUIPMENT

Modern bridge systems (also named Integrated Bridge Systems) are interconnected and strongly dependent on GNSS (Figure 1). The high degree of interconnection among the different systems onboard a vessel increases its vulnerability to, and the impact of, GNSS failures. GNSS failure or degradation can compromise bridge navigation systems as well as GNSS-based timing systems and communication equipment. It should be noted that GNSS failures could impact not only the means of navigation but also information exchange between ships as well as ship to shore data communications, as well as having implications on the Voyage Data Recorder (VDR) and Bridge Navigation Warning Alarm System (BNWAS) vessel engine operation.

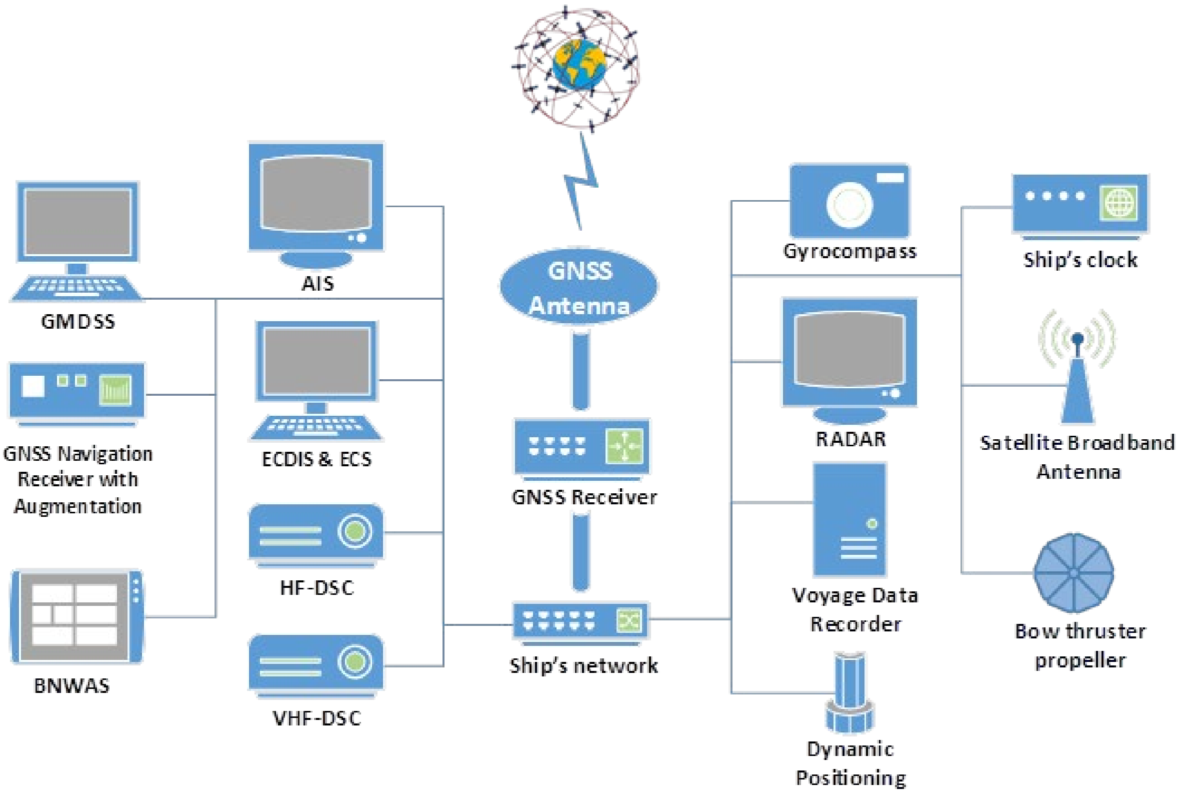

Figure 1 A general overview of various on-board systems which rely on GNSS to function in a proper manner.

When GNSS is unavailable, some onboard vessel instruments respond almost instantly with audible alarms and visual messages indicating the loss of the GNSS feed [21], but in case of falsified GNSS signals, the navigator may remain unaware of the error situation, especially if the error is relatively small or grows slowly.

If GNSS information is unavailable or falsified, a vessel's position, speed over ground (SOG) and course over ground (COG) information could be missing or incorrect. This could lead the vessel's navigator crew to undertake inappropriate course and heading changes.

ANNEX B gives examples of the effects that the loss of GNSS may have on the different onboard systems and which may affect the vessels' ability to navigate safely.

4. RISK EVALUATION

4.1. GENERAL

As already stated earlier, resilient PNT is best achieved by the combination of multiple dissimilar PNT sources, but the level of resilience achieved will be proportional to the overall cost. The general risk management process [22] should be followed when defining the target level of PNT service resilience in a particular area. Maritime authorities need to consider separately how [23]:

- AtoN services that use PNT information can be made more resilient;
- AtoN services that provide PNT information can be made more resilient; and
- AtoN services can support resilient PNT for the mariner.

General risk management process includes the following five steps [22]:

1 Hazard identification

2 Risk analysis

3 Risk control options

4 Cost-benefit assessment

5 Decision-making recommendations

For example, the Simplified IALA Risk Assessment method (SIRA) [24] may be applied to complete these steps for PNT information. It should be noted that risk management is an ongoing process, and the steps listed above should be repeated continually.

This section provides guidance and some examples on how to perform hazard identification and risk analysis related to PNT information. The risk analysis will provide the basis for further cost-benefit assessment, decision-making recommendations and possible deployment of risk control measures.

4.2. HAZARD IDENTIFICATION

Section 2 of this Guideline introduced the main sources of PNT failures. Maritime Authorities should identify and list the relevant PNT service failure types that may affect AtoN services and vessels based on general information provided in Section 2, observations of local conditions and expert knowledge. Some examples of possible GNSS related PNT failure types can be found in ANNEX C, Table 4.

The result of the hazard identification exercise can be a table listing identified failure types, their characteristics and an initial description of the estimated impact scenarios (Table 1). The purpose of hazard identification is to gather basic information about hazards to be used during the risk analysis and when estimating the probabilities and consequences of each identified hazard.

Table 1   Example of identifying PNT failure types and their characteristics

PNT failure type	Frequency of occurrence	Area affected	Duration of event	Impact
Description of each identified failure type on its own row.	Described verbally or numerically based on observations, literature or expert opinion.	Described, for example, by phase of navigation: – Ocean – Coastal – Port, other restricted water or by range: – Local (<50nm) – Regional (>50nm) – Global	Using agreed scale, for example: – Minutes – Hours – Days – Months	Verbal description of estimated impact mechanism. A separate impact column can be created for impact on AtoNs and impact on vessels.

4.3. RISK ANALYSIS

Risk analysis may consider both qualitative and quantitative issues. Qualitative analysis is subjective and aims to describe the severity of an event verbally. Quantitative analysis is objective and based on measurable numerical values.

The risk level of an unwanted event is defined by the probability of the event and its consequences, as shown in equation (1). The same equation can be used both for qualitative and quantitative assessment.

$$Risk = Probability * Consequence \tag{1}$$

The estimated probability may be based on past (monitored or reported) events. If there is numerical data available on the frequency of a specific event type, it is possible to define even quite accurate numerical value for probability. However, in most cases, the probability needs to be based at least partly on expert opinion and is best described using an agreed scale.

It is also possible to model the probability in more details by splitting it into several separate factors. This may be helpful when identifying the most efficient risk control options. For instance, probability can be expressed as the product of the probability of the unwanted event happening (threat) and the probability of it causing an unwanted impact on the system (vulnerability). Especially, in case of malicious events the threat can be further split into the motivation to do the harm (intent) and resources available to actually carry out the malicious act (capability) [25], [26]. Equation (1) can thus be expressed as below:

$$Risk = (Threat * Vulnerability) * Consequence \tag{2}$$

or further as below:

$$Risk = \big((Intent * Capability) * Vulnerability\big) * \ Consequence \tag{3}$$

The consequence can have a numerical monetary value but is more likely to be also described using an agreed scale describing the severity of the event. However, when considering the risk control options, it may be beneficial to have at least rough monetary estimates available.

When estimating the consequences of PNT failures, the following aspects may be considered:

- Capability to compute the vessel's (or AtoN's) own position
- Capability to communicate vessel's (or AtoN's) own position to other vessels and to the shore
- Capability to know (other) vessels' positions

- Capability to navigate safely in good weather conditions (good visibility)
- Capability to navigate safely in bad weather conditions (poor visibility)
- Capability to avoid collision in good weather conditions
- Capability to avoid collision in poor weather conditions
- Capability to arrive at destination on time (good weather)
- Capability to arrive at destination on time (poor weather)

A risk assessment scoring table is a practical tool to estimate the risk of individual PNT failure types and identify the high-risk areas by ranking failure types by their scores (ANNEX C, Table 4).

The purpose of the risk assessment is to identify events which have an unacceptable high-risk level and where risk control options (additional to those that may already be deployed) need to be considered.

5. RISK CONTROL OPTIONS

PNT service risk control options aim to decrease both the probability and the consequences of PNT failures. Generally, probability of a PNT failure can be best decreased by failsafe system design and using multiple alternative PNT sources. Consequences of PNT failures on the other hand can be best mitigated by education, training, monitoring, and alerting. Mitigation measures can also be divided into toughening, augmenting and protecting measures [26]. Toughening aims to increase PNT systems own resilience, augmenting aims to provide alternative PNT sources and protecting aims to eliminate the external sources of interference or other disturbances.

This section introduces different measures that may be used to mitigate the risk related to PNT failures. Because GNSS is the primary source of PNT information in the maritime domain, both for vessels and for AtoNs, the focus is on the risk controls towards GNSS failures. It is to be noted that when GNSS receiver is supporting AtoN service and installed in an AtoN with limited power source and space, number of potential risk control options may be reduced.

An overview of the identified mitigation measures and GNSS vulnerabilities they can mitigate is provided in ANNEX D of the document.

5.1. FAILSAFE SYSTEM/SERVICE DESIGN

PNT systems should be designed to detect and mitigate equipment failures. This applies both to the service infrastructure and user equipment and can be achieved by preventive maintenance, self-testing functionalities and duplication of equipment.

System design should also consider security aspects. Service infrastructure needs to be physically protected and countermeasures to protect service from possible signal interference from natural, unintentional, and intentional sources. Proper design will also consider measures to inform users in case of service failures. It is to be noted that Maritime Authorities can directly influence only the design of systems and services they are providing themselves.

5.1.1. SERVICE INFRASTRUCTURE

The infrastructure of all GNSS constellations is designed to be very secure and robust, and total system failures are rare (see Section 2.3.1). All GNSS service providers are also planning to provide countermeasures for different types of signal interference.

To enhance position accuracy, each GNSS provider has plans to provide or is already providing dual frequency service for public use. The new GPS L5 signal specifically designed for the safety of life services will be of interest to marine navigation in addition to the legacy L1 C/A signal already in use. Development status of GPS L5, GLONASS L5, Galileo E5a and BeiDou Navigation Satellite System (BDS) B2a signals is presented in Table 2. Using two or more frequencies, a GNSS receiver can remove all frequency-dependent errors and thereby improve its positional accuracy. This is an effective way to remove ionospheric error from the position calculation, which is a major contributor to the overall measurement error in the position calculation.

Table 2 Status of core GNSS signals at 1176.45 MHz as of May 2023

Signal	Status	Future deployment
GPS L5 [27]	L5 is broadcast from 17 satellites in pre-operational mode and is set to unhealthy until further monitoring capability are established on Block IIF and subsequent satellite blocks.	Planned to be available on 24 GPS satellites around 2027 (as of 2020).
GLONASS L5 [28]	L5 signal from the GLONASS-KM satellites currently in research phase.	Launch planned for 2030 beyond.
Galileo E5a [29], [30]	Galileo E5a has been available from 24 satellites. Following in-orbit testing of the initial service, the roll-out accessibility of the Galileo E5 signal will be assessed with the receiver manufacturers.	Initial service planned by the end of 2023.
BDS B2a [31]	BDS-3 B2a signals have been available from 3 Inclined Geosynchronous Satellite Orbit (IGSO) and 24 Medium Earth Orbit (MEO) satellites.	Full Operation Capabilities since 2020.

Following the evolution of GNSS constellations to provide navigation services in several frequencies (at least two), SBAS constellations are also evolving to provide augmentation and integrity information for additional frequencies and multiple constellations. In such a way, all SBAS constellations have planned to offer dual frequency multi constellation (DFMC) services in addition to the legacy SBAS L1 service currently provided. The DFMC SBAS service is subject to and mitigates threat in the same manner as L1 SBAS service, with the exception that differential ionosphere delay error is mitigated using the ionosphere-free pseudorange. The DFMC SBAS service implies several benefits:

- Provision of service in regions where active ionosphere affects L1 service availability.
- Augmentation of multiple constellations.
- Additional resilience to radio frequency interference and improved availability during ionospheric storms.
- Increased robustness against failure or degradations of one constellation.

The European GNSS service, Galileo, plans to provide a mechanism to authenticate the open navigation signals on the E1 band (i.e. Open Service - Navigation Message Authentication (OS-NMA)) [32]. The authentication is done by adding a digital signature to the unencrypted navigation message, allowing receivers to verify that the signal is coming from a trusted source and making signal spoofing more difficult. OS-NMA is an additional feature and does not impact legacy receivers.

GNSS constellations may also provide encrypted, more robust navigation signals for governmental and critical infrastructure related uses like, for example, VTS and AtoN services [33].

5.1.2. USER RECEIVER

The basic measures for users to counteract GNSS receiver equipment failures are duplication of equipment, the use of standby power supplies and following installation and fault-finding guidelines. The use of certified equipment ensures the reliable receiver performance. When installed on a floating AtoN, robust physical protection of the receiver and the antenna is also necessary.

5.1.2.1. Signal processing and antenna design and location

As previously mentioned in this Guideline, one of the main characteristics of GNSS signals is how weak they are in terms of power when they reach ground, with levels below thermal noise. This makes them prone to various types of interference that have an impact on the PNT performance, as discussed in Section 3. At the user level, it is possible to take advantage of system level improvements, where increasingly complex signals and greater frequency diversity play a key role in their robustness against interferences.

GNSS receiver manufacturers adopt these new features and may also implement internal countermeasures. These technologies can be used to protect the receiver from man-made interference like jamming and may be used to protect the receiver also from spoofing in some cases.

Receiver antennas may also be physically protected from interferences (e.g. reflections) by installing a metal plate under the antenna to block the unwanted signals. This may also help to eliminate jamming sources located below the receiving antenna installation height.

In some cases, having two antennas makes it possible to compare the information received from each antenna. Thus, some vulnerabilities such as spoofing, is possible to detect through the fact that the information is not consistent between the antennas.

5.1.2.2. Use of multiple GNSS constellations and frequencies

With four GNSS constellations becoming fully operational post 2020, and as more frequencies become available, multi-system multi-frequency receiver users will see a significant increase in accuracy, availability, and coverage, particularly in high latitudes including the Arctic.

A multi-constellation capable receiver can access signals from more than one GNSS constellation. The use of signals from several constellations results in the beneficial situation of having a larger number of satellites in the antenna field of view. Benefits include the fact that signal acquisition time is reduced, and position and time accuracy have a noticeable performance improvement. In addition, obstructions such as buildings, maritime structures, foliage, fjords, and urban canyons are less problematic. If a signal is blocked by an obstruction or in areas with shadowing, there is a very high likelihood that the receiver will simply pick up a signal from another constellation, therefore ensuring continuity.

It should be noted that additional satellites will not in themselves create the necessary level of robustness to mitigate jamming and spoofing. However, a receiver locked on satellites from two or more constellations is obviously much harder for the attacker to spoof. Each constellation operates independently from the others and can be seen as complementary to the navigation system. GNSS receivers must be specifically configured to access and use more than one constellation at the same time and manage the receiver power consumption as well as consistency and interoperability issues among GNSS systems such as clock biases.

As explained in Section 5.1.1 use of several GNSS signals allocated to different frequencies allow receivers to remove any frequency-dependent errors and thereby improve receiver accuracy. This is an effective way to remove ionospheric errors which are the main contributor to the overall measurement error in the position calculation.

Another advantage of dual-frequency receivers is that their levels of robustness and immunity are increased in the presence of single frequency jamming or single frequency spoofing. Frequency diversity provides some protection against simple jamming, especially if the receiver does not require L1 signals to initiate positioning. If reception is interrupted due to the influence of in-band jamming, the receiver can switch to another available frequency band and reception is maintained.

5.1.2.3. Receiver Autonomous Integrity Monitoring

GNSS services do not currently broadcast any information related to the integrity of the positioning calculation. It is possible for a GNSS satellite to broadcast incorrect information that will cause errors on the users' position, but there is no way for the receiver to determine this using standard techniques. Receiver Autonomous Integrity Monitoring (RAIM) algorithms were developed to overcome this problem.

RAIM algorithms use redundant GNSS signals to produce several GNSS position fixes and compare them, and statistically determine whether a fault can be associated with any of the GNSS signals. That is, when more satellites are available than needed to produce a position fix, the extra pseudo range measurements should all be consistent with the computed position. A pseudo range that differs significantly from the expected value may indicate a fault of the associated satellite or another signal integrity problem (e.g., ionospheric interference). This function of RAIM is known as fault detection (FD). To perform this function RAIM algorithm needs at least one additional satellite in view to the ones required to compute the navigation solution, this is at least five satellites in view. An enhanced version of RAIM allows also the exclusion of the faulty satellite in addition to the fault detection, which is known as fault detection and exclusion (FDE). This enhanced version requires a minimum of six satellites in view [34].

Another function that RAIM algorithms can perform, taking advantage of the pseudo range measurements redundancy, is the computation of the so-called Protection Levels. The Protection Level is the radius of a circle which describes the region that is assured to contain the indicated position. In the maritime field, particularly the horizontal protection is considered, so the Protection Level in this case is called Horizontal Protection Level (HPL). The HPL value is used to compare with a Horizontal Alert Limit (HAL) in order to establish whether to trigger an alarm [35].

The classical RAIM algorithms were initially only applicable to a single constellation and a single frequency. Currently, different new RAIM algorithms have been proposed that provide enhanced performances such as the possibility to use them for multiple constellations and multiple frequencies. In addition, the progress of these algorithms also makes it possible to reduce the size of the protection levels, which allows for higher integrity in contexts where the accuracy level is more demanding. The aviation industry is at the forefront of the development of these algorithms (e.g. Advanced Receiver Autonomous Integrity Monitoring (ARAIM)), although proposals and studies are appearing to adapt these algorithms also to the maritime sector.

5.1.2.4. GNSS Augmentation systems

The reliability and accuracy of GNSS receiver performance can be enhanced by using information provided by some external augmentation system. The GNSS augmentation systems can provide integrity information and/or corrections to increase the reliability and accuracy of the positioning calculation. They can provide support to one or more GNSS constellations. There are a number of commercial augmentation services with different service levels available for maritime use [36]. Additionally, there are public free of charge services available, including SBAS (e.g. European Geostationary Navigation Overlay Service (EGNOS), WAAS) and IALA Beacon DGNSS, to support users in different domains where augmentation and integrity is required.

The integrity concept relies on the use of ground reference stations, which receive data from the GNSS satellites and compute integrity and correction data. In case of IALA Beacon DGNSS, augmentation information is transmitted via medium frequency (MF) radio link to the vessels’ DGNSS receivers. In the case of SBAS, information is uploaded to the SBAS geostationary orbit (GEO) satellites, which then relay this information to SBAS-capable receivers through the SBAS Signal in Space (SIS) transmissions. The receivers acquire and apply this data to determine the integrity and improve the accuracy of the computed navigation solution. The SBAS integrity service is based on a large network of ground stations and should protect the user from:

- Failures of GPS satellites (drifting or biased pseudo ranges) by detecting and excluding faulty satellites through the measurement of GPS signals.
- Transmission of erroneous or inaccurate differential corrections which may be induced from either undetected failure in the ground segment and/or processing of reference data corrupted by the noise induced by the measurement and algorithmic process.

In addition to the provision of SBAS corrections and integrity via SIS, data can be provided also by other channels. For instance, EGNOS provides ground-based access by enabling a dedicated internet domain where authorised users are allowed to retrieve real time or historical EGNOS data. A similar approach is followed also by many other GNSS augmentation service providers [37], [38].

5.1.2.5. Signal Authentication

A receiver with authentication capability can detect the veracity of the signal received and increase user's confidence in the receiver reported position. In terms of GNSS navigation message, authentication is established when it can be confirmed that the message received is identical to the satellite message transmitted and the source of the signal transmitted can be trusted. The Galileo currently operates a free of charge authenticated service. GPS is developing an authenticated service [39].

Using a receiver equipped with authentication features will improve its resilience against spoofing signals but not protection against jamming.

5.2. USE OF MULTIPLE PNT SOURCES

Use of more than one PNT source provides means to validate the integrity of PNT data by comparing information coming from different sources. This may help to identify, for example, GNSS spoofing events. Using PNT sources with dissimilar failure types may also prevent the total loss of PNT information. When one service fails, others may still provide PNT information with acceptable accuracy.

In case of AtoNs that use PNT information, it might be challenging to use multiple PNT sources, for example, due to limited power supply. However, possibilities for deploying backup systems should be considered whenever possible. In case of vessels, the primary PNT source is generally GNSS. Secondary, alternative PNT sources include onboard sensors, terrestrial PNT services, visual AtoNs and external support (e.g. by VTS).

Alternative PNT sources may provide information at various levels; fully redundant, backup and contingency as follows [40]:

- A redundant system provides the same functionality as the primary system, allowing a seamless transition with no change in procedures.
- A backup system ensures continuation of the navigation application, but not necessarily with the full functionality of the primary system and may necessitate some change in procedures by the user.
- A contingency system allows safe completion of a manoeuvre but may not be adequate for long-term use.

Where the risk assessment concludes that a backup system is necessary, suggested minimum maritime user requirements for such a system are listed in APPENDIX 1. There is currently no single backup system to GNSS that can meet requirements of all the maritime navigation phases. However, a combination of various backup systems considering their respective areas of operation can improve PNT information resiliency.

It is expected that the development of space-based LEO-PNT systems will provide ocean coverage and meet the meter level accuracy requirement for port navigation in the near future.

Some terrestrial-based backup systems (e.g. eLoran) can meet the 10m navigation requirements for coastal and port approach phases at the regional level. Some commercial systems (e.g. Locata [41]) can meet the 1m requirement for port and harbour navigation.

In addition, traditional means of navigation such as dead-reckoning and radar positioning should also be considered.

The argument for a backup system will be dependent on the perceived threat to the primary system and the likely duration of primary system outages.

5.2.1. LEO-BASED SYSTEMS

In recent years, multiple satellite constellations in the Low Earth Orbits (LEO) providing global broadband communication services (e.g. OneWeb, Starlink), Earth observation capabilities (e.g. Iceye), maritime communication services such as VDE-SAT (e.g. Space Norway, Spire, Sternula) or other institutional initiatives (e.g. ESA) has emerged. There may be potential to use LEO satellites also for PNT purposes (e.g. STL [42], Pulsar [43]).

This application area is currently being studied by the research community world-wide. At least three different options are being studied [44]:

- Using existing LEO signals as signals of opportunity (SOOP).
- Modification of existing LEO signals to better support positioning.
- New LEO signals optimised for PNT.

LEO satellites orbit the Earth at an altitude of less than 2000 km, significantly lower than current GNSS (MEO) and SBAS (GEO) satellites. LEO-based PNT services have the potential to support GNSS positioning by enhancing the satellite geometry and providing stronger signal levels (Figure 2).

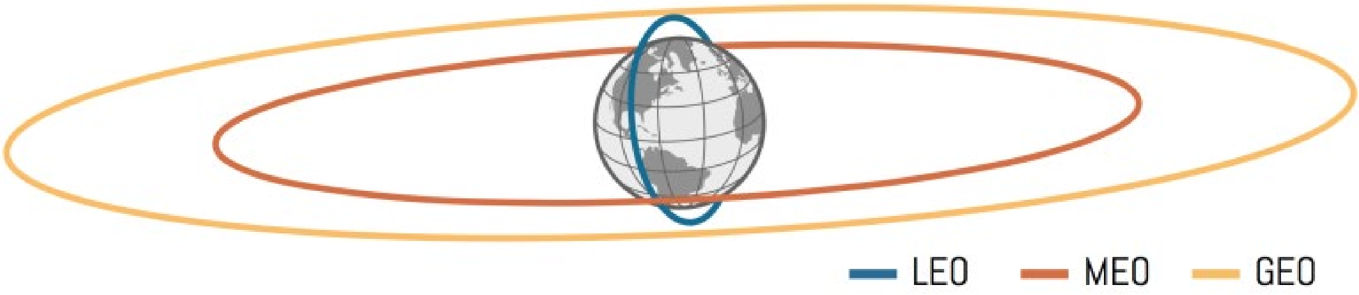

Figure 2 Typical LEO, MEO and GEO orbits [45]

LEO constellations would be able to use new RNSS frequency bands (e.g. UHF, K-band, C-band), complementing and providing alternative PNT solutions to those already used today in L-band GNSS systems. Having greater diversity in the spectrum and having greater geometric diversity allows for the application of a large number of navigation techniques that complement MEO L-band based GNSS systems, leading to improved PNT resiliency. LEO systems could be also considered as an interesting solution for high latitude areas or to offer functionalities such as 2-way ranging for position verification. It is not yet clear if some LEO-based PNT services would be provided as public, free of charge services or if all these services would be commercial.

5.2.2. TERRESTRIAL-BASED SYSTEMS

The growing demand for reliable PNT information in navigation systems, together with the increased understanding of GNSS vulnerabilities, have led to efforts to find alternative ways to provide PNT services to vessels using ground-based transmissions. Different terrestrial-based PNT systems may operate in different frequency bands and use different power levels, these particularities along with other factors, will determine their coverage and their positioning accuracy. Technologies operating in a higher frequency band provide better accuracy but will have a shorter range and thus will require investment in a denser transmitter network to cover a large area (see Table 3 below).

Table 3 Frequency band, typical coverage and expected ranging accuracy of different terrestrial-based PNT systems.

Terrestrial-based systems	Frequency band	Coverage	Ranging accuracy
eLoran	100 kHz	1000-1600 km	10-20 m (in differential mode)
MF R-Mode	300 kHz	200-300 km	10-20 m
VDES R-Mode	160 MHz	40 km	10-20 m

5.2.2.1. Enhanced Loran (eLoran)

The Loran radio navigation system is based on high power, low-frequency signal broadcasts from terrestrial transmitters. Loran technology evolved from the Loran-A system of the 1950's to the Loran-C system widely utilised from the 1970's through the first decade of this century. Loran systems have proved invaluable to the global transportation sector through the provision of positioning, navigation and timing (PNT) services. The name Loran is abbreviation from long range navigation. The low transmission frequency (about 100 kHz for Loran-C) which propagates as ground wave enables the large service coverage area.

Enhanced Loran (eLoran), which has been developed from mid 1990's could be considered as an ideal GNSS backup system because it is independent of satellite technologies and dissimilar yet complementary to GNSS. With the application of differential corrections, eLoran timing accuracy exceeds 100 ns and it is capable of providing 10-metre positioning accuracy in differential mode. As such, eLoran meets IMO performance requirements for PNT services such as maritime harbor entrance and approach maneuvers, aviation non-precision instrument approaches as well as timing requirements for the telecommunications, energy and financial sectors.

5.2.2.2. Ranging Mode (R-Mode)

The underlying idea of the Ranging Mode (R-Mode) technology is the addition of a timely synchronised ranging signal to a radio signal of opportunity that results in an alternative terrestrial position, navigation and timing technology completely independent of GNSS.

R-Mode adds ranging signals superimposed on typical transmitted signals from existing maritime radio infrastructure which includes many DGPS transmitters in operation globally. Utilising the existing maritime radio beacon system avoids the substantial costs associated with procuring and installing transmitters and antennas in order to establish a GNSS backup functionality. Moreover, in the case of existing radio infrastructures, the relevant broadcast frequencies are already available and protected, and the beacons are well-positioned along shipping corridors.

R-Mode configurations can utilise MF DGNSS or VDES signals [49] or a combination of these signals as well as the signals in combination with eLoran. Following the completion of feasibility studies, initial proof-of-concept trials have been performed with encouraging results [50], [51]. The development and standardisation of R-Mode system is still in progress and vessel equipment are not yet commercially available.

5.2.2.3. Radar Aids to Navigation

In general, a ship's captain will consider the ship's radar system as being the most important equipment of all the electronic navigation instruments available on the bridge. Radar provides the capability to safely maneuver a ship even in zero visibility and during adverse weather conditions. Radar has traditionally been used in two ways in the maritime environment; for relative positioning to other objects and for situational awareness. Radars scan the surroundings and provide bearing and distance from the radar echo of other ships, terrains, buoy retroreflectors and obstacles. It is important to note that the traditional ship's radar is not a positioning device, nor does it rely on GNSS to function.

In cases where the radar echo is not sufficient or is blurred into clutter, active radar transponders, such as a radar beacon (racon), can be used to mark and identify lighthouses, navigation buoys, bridges, centre lines, turning points, offshore oil platforms and other structures. Racons are important aids to navigation for enhancing collision avoidance and safe navigation at sea. When a racon receives a radar pulse, it responds with a signal on the same frequency that results in a Morse dots and dashes line on the sending radar display.

Radar can also be used to calculate absolute position solutions. Absolute radar positioning can be realised using one of the two following methodologies; 1) active transponders or 2) passive returns employing map and feature matching.

A system known as Enhanced Radar Positioning System (ERPS) uses active transponders. The system uses enhanced racons, called eRacons, with enhanced radars, called eRadars to allow automatic calculation of absolute position information. The eRacons provide their accurate, surveyed position to eRadars, encoded on their response signals. Using response signals from one or more eRacons, eRadar can calculate its own vessel's position [46]. Trials have demonstrated the high potential of radar-based absolute positioning from eRacons and eRadars on ships without the need for GNSS or externally provided information to operate effectively [47]. This technology is not able to provide timing information and would be limited to areas within Racon coverage. Standardisation of the technology is not finalised, and no vessel equipment are yet commercially available.

Map and feature matching is an alternative approach to absolute position determination using radar data. There are a number of potential approaches as discussed in [48], but the general concept is that the radar matches measured terrain features to a database of features and calculates absolute positions. This technique is a candidate for resilient positioning. Although the technique does not necessarily require racons, racons can be included in terrain features databases and may be required where there are insufficient radar returns, for example in areas of low-lying coastline.

5.2.2.4. Cellular technology positioning

Like R-Mode, cellular positioning is based on using signals from existing communications systems. Multiple different positioning technologies have been developed to allow the localisation of user equipment by the cellular network infrastructure but also to allow the user equipment to position itself using signals from the network. There are few different ways that cellular network radio signal can be used for positioning [52]:

- Based on the timing of signals received from multiple cell-sites.
- Based on the power of received signals.
- Based on the angle of arrival of the signals.

These technologies may, in the future, provide support also for maritime applications (including AtoNs) requiring position and timing information. PNT services provided via cellular technologies are expected to be commercial and involve a user fee.

5.2.3. ON-BOARD SENSORS

The integrity of vessels PNT information should be verified by comparison of the data derived independently from at least two sensors and/or data sources, if available. Onboard sensor systems that may provide alternative PNT sources of information include:

- Inertial Navigation System (INS) position and navigation data.
- Depth sounder depth information which together with accurate bathymetric information, may provide position and navigation data.
- Atomic clock timing data.
- Gyro compass true north to be used for heading and rate of turn information.
- Vision system (e.g. ePelorus) relative bearings to charted and visually identifiable objects which can provide vessel's position.
- Radar and LiDAR range and bearing to nearby objects. Using range and bearing information related to known charted objects can provide vessel's position.

5.2.4. VISUAL AIDS TO NAVIGATION

Traditional visual AtoNs form the foundation of safe navigation for all vessel types. Charted AtoNs assist navigators to determine their own position, indicate the safe fairway area and warn of nearby dangers. To support navigation in reduced visibility conditions (e.g. during night-time), many AtoNs are fitted with light and/or radar aids.

Excluding a few exceptions mentioned in Section 3.1, visual AtoNs provide navigation services totally independent from GNSS.

5.2.5. EXTERNAL SUPPORT

In areas covered with VTS, vessels can request navigational support. If a vessel is unsure of its position and course due to, for example, navigational equipment failure, VTS may provide it with the following information [53]:

- Range and bearing from fixed objects, fairway/channel or waypoints.
- Proximity to navigational hazards.
- Information related to navigating into a channel/fairway/lane (i.e., track is parallel/diverging/converging with/from/to reference line).

However, navigational support by VTS is provided only to assist vessel in shipboard decision-making process in various situations.

When a GNSS receiver is installed in a floating AtoN solely for remote off-position monitoring purposes, the accuracy of the reported position can be enhanced by post processing. This requires the availability of nearby reference sites where estimated position corrections can be calculated and stored. Post-processing can remove some position errors introduced by GNSS signal interference.

5.3. EDUCATION AND TRAINING

An important measure to mitigate the impacts of possible PNT failures is to raise awareness of PNT service vulnerabilities, especially related to the GNSS services. GNSS provides normally very accurate information and can easily be taken for granted. However, users should stay alert, be aware of possible causes and signs of PNT failures and continuously validate the primary PNT source against other available PNT sources either manually or assisted by onboard equipment. Actions and procedures in situations, where the primary PNT source is lost or is providing false information should be included in regular training.

The IALA World-Wide Academy (WWA) addresses the importance of uninterrupted PNT and the vulnerabilities of GNSS in the AtoN manager's Level one Model Course on GNSS and e-Navigation [54]. The aim is to highlight that an uninterrupted determination of such service is essential to e-Navigation.

5.4. MONITORING AND ALERTING

Generally, misleading PNT information will cause more severe consequences than having no PNT information at all. Thus, monitoring, detection, and indication/alerting of PNT error situations is one of the most important risk control measures.

The nature of a GNSS failure may be instantly perceived by the navigator and onboard equipment may be capable of detecting and indicating some GNSS failures by comparing information from different PNT sources or by using the RAIM algorithms. However, additional shore-based monitoring, detection and alerting options should be considered when conducting the risk assessment. Integrity information can be provided to vessels through different means. For example, IALA Beacon DGNSS service or SBAS, such as WAAS and EGNOS, may carry integrity messages. In addition, VTS operators would be critical in first recognising the GNSS failure events and, secondly, informing mariners and solving the high levels of ambiguity during the event.

Dedicated RF spectrum monitoring stations and network of stations could be established for monitoring and detecting interference events in GNSS frequencies. This type of monitoring could cover large areas or just some critical areas where incorrect PNT information is estimated to cause severe consequences.

Technologies to allow global scale GNSS interference monitoring and localisation from space using special payloads on LEO satellites is being explored [55], [56]. If the technology proves to be reliable, near real time information and warnings of GNSS interference events may be available for maritime users during all phases of the voyage.

6. DEFINITIONS

The definitions of terms used in this Guideline can be found in the *International Dictionary of Marine Aids to Navigation* (IALA Dictionary), which were still valid at the time of going to print. Where conflict arises, the IALA Dictionary should be considered as the authoritative source of definitions used in IALA documents.

7. ABBREVIATIONS

AGC	Automatic Gain Control
AIS	Automatic Identification System
ARAIM	Advanced Receiver Autonomous Integrity Monitoring
ARP	Absolute Radar Positioning
ATON	Aids to Navigation
BCN	Bottom-contour Navigation
BDS	BeiDou Navigation Satellite System
BNWAS	Bridge Navigation Warning Alarm System
BOC	Binary Offset Carrier
BTW	Bow Thruster Propeller
CIS	Commonwealth of Independent States
COG	Course over Ground
COTS	Commercial off the shelf
CRPA	Controlled Radiation Pattern Antennas
CSAC	Chip-scale Atomic Clock
DFMC	Dual frequency multi-constellation
DGNSS	Differential GNSS
DOP	Dilution of Precision
DP	Dynamic Positioning
DSC	Digital Selective Calling
ECDIS	Electronic Chart Display and Information System
ECS	Electronic Chart System
EGNOS	European Geostationary Navigation Overlay Service
ELORAN	Enhanced Long Range Navigation
EPFS	Electronic Position Fixing System
ERPS	Enhanced Radar Positioning System
FD	Fault Detection
FDE	Fault Detection and Exclusion
GALILEO	European Global Satellite Navigation System
GEO	Geostationary Orbit
GLONASS	Russian Global Navigation Satellite System
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HAL	Horizontal Alert Limit

HAS	High Accuracy Service
HF	High Frequency
HPL	Horizontal Protection Level
IGSO	Inclined Geosynchronous Satellite Orbit
IMO	International Maritime Organisation
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
ISL	Inter-satellite link
ITU	International Telecommunication Union
LEO	Low Earth Orbit
LIDAR	Light Detection and Ranging
LRIT	Long-range Identification and Tracking
MEO	Medium Earth Orbit
MF	Medium Frequency
MMSI	Maritime Mobile Service Identity
NLOS	non line of sight
NT	New Technology
OS	Open Service
OS-NMA	Open Service Navigation Message Authentication
PLL	Phase Lock Loop
PNT	Position, Navigation and Timing
PPD	Personal Privacy Device
RACON	Radar Beacon
RAIM	Receiver Autonomous Integrity Monitoring
RF	Radio Frequency
R-Mode	Ranging-Mode
RNSS	Regional Navigation Satellite System
SBAS	Satellite Based Augmentation Service
SIRA	Simplified IALA Risk Assessment
SIS	Signal in Space
SLAM	Simultaneous Localisation and Mapping
SOG	Speed over Ground
SOLAS	Safety of Life at Sea
SOOP	Signal of Opportunity
SV	Space Vehicle
TEC	Total Electron Content
TV	Television
UERE	User Equivalent Range Error
UHF	Ultrahigh Frequency
UKC	Under Keel Clearance
USAF	United States Air Force
UTC	Universal Time Coordinated

VDES	VHF Data Exchange System
VDE-SAT	VDES Satellite component
VDR	Voyage Data Recorder
VHF	Very High Frequency
VTS	Vessel Traffic Service
WAAS	Wide Area Augmentation System
WWA	IALA World-wide Academy

8. REFERENCES

[1] John A. Volpe National Transportation Systems Center. (2001) Vulnerability assessment of the Transportation Infrastructure relying on the Global Positioning System. Final report. Available online: https://rntfnd.org/wp-content/uploads/Vople_vulnerability_assess_2001.pdf (Accessed Nov 2022).

[2] The Royal Academy of Engineering. (2011) Global Navigation Space Systems: reliance and vulnerabilities. ISBN 1-903496-62-4.

[3] IMO. (2008) MSC 85/26/Add.1, Annex 20, Strategy for the Development and Implementation of e-Navigation.

[4] IALA. Dictionary: Resilient PNT. https://www.iala-aism.org/wiki/dictionary/index.php/Resilient_PNT.

[5] Towlson, O., Payne, D., Eliardsson, P., Manikundalam, V. (2019) Standardisation of GNSS threat reporting and receiver testing through international knowledge exchange, experimentation and exploitation (STRIKE3); D6.2: Threat database analysis report.

[6] ITU. (2013) Handbook on radiometeorology.

[7] ITU. (2014) Handbook on ground wave propagation.

[8] ITU. (1998) Handbook on the ionosphere and its effects on radiowave propagation.

[9] UCAR, Center for Science Education. Webpage: https://scied.ucar.edu/learning-zone/atmosphere/ionosphere.

[10] Sanz Subirana J., Juan Zornoza J.M., Hernández-Pajares M. (2013) European Space Agency (ESA TM-23/1), GNSS Data Processing, Volume I: Fundamentals and Algorithms. ISBN 978-92-9221-886-7. Available online: https://gssc.esa.int/navipedia/GNSS_Book/ESA_GNSS-Book_TM-23_Vol_I.pdf.

[11] McGraw G.A., Groves P.D., Benjamin W. Ashman B.W. (2021) Robust Positioning in the Presence of Multipath and NLOS GNSS Signals.

[12] Clynch J.R., Parker A.A., Adler R.W., Vincent W.R., McGill P., Badger G. (2003) GPS World: The Hunt for RFI – Unjamming a Coast Harbor.

[13] C4ADS. (2019) Above us only stars. Available online: https://c4ads.org/reports/above-us-only-stars/ (Accessed Jan 2023).

[14] Inside GNSS. (2019) Lessons to be Learned from Galileo Signal Outage. Available online: https://insidegnss.com/lessons-to-be-learned-from-galileo-signal-outage/.

[15] Inside GNSS. (2014) GLONASS Suffers Temporary Systemwide Outage; Multi-GNSS Receiver Overcomes Problem (updated). Available online: https://insidegnss.com/glonass-suffers-temporary-systemwide-outage-multi-gnss-receiver-overcomes-problem-updated/.

[16] Eastlack, H. (2004). Second Space Operations Squadron, US Air Force, Washington, D.C: SVN-23/PRN-23 Integrity Failure of 1 January 2004.

[17] FURUNO Norge. Webpage: https://www.furuno.no/en/aktuelt/furuno-gps-recievers-affected-by-gps-rollover-02-01-2022/.

[18] Grant, A., Williams, P., Ward, N., Basker, S. (2008) GNSS Vulnerabilities and Solutions Conference, Royal Institute of Navigation: GPS Jamming and the Impact on Marine Navigation.

[19] IALA. Guideline G1112 on the Performance and Monitoring of DGNSS Services in the Frequency Band 283.5 – 325 kHz.

[20] IALA. Guideline G1129 on the Retransmission of SBAS Corrections Using MF-Radio Beacon and AIS.

[21] Williams, A. (2013) YouTube video: ACCSEAS Resilient PNT Demonstration. Available online: https://www.youtube.com/watch?v=CNAr8eQQ_9E.

[22] IALA. Guideline G1018 on Risk Management.

[23] IALA. Guideline R1017 on Resilient Position, Navigation and Timing (PNT).

[24] IALA. Guideline G1138 on the Use of the Simplified IALA Risk Assessment method (SIRA).

[25] Fernandez, J.M. (2021) IALA Cyber security workshop: Threats and challenges in Maritime Cybersecurity.

[26] Resilient Navigation and Timing Foundation. (2016) White Paper: Prioritising Dangers to the United States from Threats to GPS; Ranking Risks and Proposed Mitigations. Available online: https://rntfnd.org/wp-content/uploads/12-7-Prioritizing-Dangers-to-US-fm-Threats-to-GPS-RNTFoundation.pdf.

[27] National Coordination Office for Space-Based PNT. (2023) GPS.GOV: New Civil Signals. Available online: https://www.gps.gov/systems/gps/modernization/civilsignals/#L5.

[28] CIS. (2019) Main directions (plan) of the development of radio navigation CIS member states for 2019–2024. Available online: https://rntfnd.org/wp-content/uploads/CIS-Russia-Radionav-Plan-2019-2024.pdf.

[29] European Union. (2021) European GNSS (Galileo) Open Service SIS ICD issue 2.0. Available online: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.0.pdf.

[30] Pont, G., Falcone, M., Mantiega Bautista, M. (2023) GPS World: Directions 2023: Galileo Offers New Services. Available online: https://www.gpsworld.com/directions-2023-galileo-offers-new-services/.

[31] China Satellite Navigation Office. (2017) BeiDou Navigation Satellite System Signal In Space (SIS) Interface Control Document (ICD) Open Service Signal B2a (version 1.0). Available online: http://en.beidou.gov.cn/SYSTEMS/ICD/201806/P020180608518432765621.pdf.

[32] ESA. Navipedia: Galileo Open Service Navigation Message Authentication. https://gssc.esa.int/navipedia/index.php/Galileo_Open_Service_Navigation_Message_Authentication.

[33] ESA. Navipedia: Galileo Public Regulated Service (PRS). https://gssc.esa.int/navipedia/index.php/Galileo_Public_Regulated_Service_(PRS).

[34] Zabalegui P., De Miguel G., Pérez A., Mendizabal J., Goya J., Adin I. (2020) A Review of the Evolution of the Integrity Methods Applied in GNSS.

[35] IEC. (2010) IEC 61108-3 Maritime navigation and radiocommunication equipment and systems – Global navigation satellite systems (GNSS) – Part 3: Galileo receiver equipment – Performance requirements, methods of testing and required test results.

[36] Khatun, A., Thombre, S., Bhuiyan, M.Z.H., Bilker-Koivula, M., Koivula, H. (2021) Preliminary Study on Utilising GNSS-based Techniques for Enhanced Height Estimation for Vessels in Finnish Waterways. ISBN 978-952-317-854-0.

[37] European GNSS Agency (GSA). (2021) EGNOS Safety of Life (SoL) Service Definition Document (SDD), Issue 3.4. ISBN N 978-92-9206-051-0.

[38] EU Agency for the Space Programme (EUSPA). (2022) EGNOS Data Access Service (EDAS) Service Definition Document Issue 2.3 ISBN 978-92-9206-063-3.

[39] Petovello, M. (2018) Inside GNSS: GNSS solutions: Q: What is navigation message authentication? Available online: https://insidegnss.com/wp-content/uploads/2018/04/janfeb18-SOLUTIONS.pdf.

[40] IALA. Recommendation R1029 on GNSS Vulnerability and Mitigation Measures.

[41] Locata. Webpage: https://www.locata.com/.

[42] Satelles. Webpage: https://satelles.com/technology/reliable-and-secure-pnt-service/.

[43] XONA Space Systems. Webpage: https://www.xonaspace.com/pulsar.

[44] Prol, F.S., Morales Ferre, R., Saleem, Z., Välisuo, P., Pinell, C., Lohan, E.S., Elsanhoury, M., Elmusrati, M., Islam, S., Çelikbilek, K., Selvan, K., Yliaho, J., Rutledge, K., Ojala, A., Ferranti, L., Praks, J., Bhuiyan, M.Z.H., Kaasalainen, S., Kuusniemi, H. (2022) IEEEAccess: Position, Navigation, and Timing (PNT) Through Low Earth Orbit (LEO) Satellites: A Survey on Current Status, Challenges, and Opportunities. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9840374.

[45] Aerospace security. Webpage: https://aerospace.csis.org/aerospace101/earth-orbit-101/.

[46] IALA. Guideline G1147 the Use of Enhanced Radar Positioning Systems.

[47] Kashiwa, T. (2017) e-Navigation Underway 2017: Trials of e-Radar/e-Racon Positioning System at Singapore port. Available online: https://www.iala-aism.org/content/uploads/2016/09/1555-Takuo-Kashiwa-Trials-of-e-Radar-e-Racon-positioning-system-at-Singapore-Port-final.pdf.

[48] Hargreaves, C., et al. (2023) Position fixing using marine radar.

[49] IALA. Guideline G1158 VDES R-Mode.

[50] Grundhöfer,L., Giacomo Rizzi, F., Gewies, S., Hoppe, M., Bäckstedt, J., Dziewicki, M., Del Galdo, G. (2021) Journal of the Institute of Navigation: Positioning with medium frequency R-Mode. DOI: https://doi.org/10.1002/navi.450.

[51] Wirsing, M., Dammann, A., Raulefs, R. (2021) International Journal of Satellite Communications and Networking: VDES R-Mode performance analysis and experimental results. DOI: https://doi.org/10.1002/sat.1424.

[52] 5G Positioning. Webpage: https://www.5gpositioning.com/cellular-network-positioning-technologies/.

[53] IALA. Guideline G1089 Provision of a VTS.

[54] IALA. Model Course C1004 on Aids to Navigation Management Training Level 1 – Global Navigation Satellite Systems and e-Navigation.

[55] Pojani, G., Ellis, P., Irisov, V., Breeze, C. (2022) NAVISP EL2-117 Final Presentation: GNSS Interference Monitoring from LEO. Available online: https://navisp.esa.int/uploads/files/documents/NAVISP%20EL2-117%20Presentation%20Final.pdf.

[56] Fernandez, F.A. (2021) GNSS Interference Monitoring from Space. Available online: https://www.unoosa.org/documents/pdf/icg/IDM/IDM9/2021_IDM_workshop_02.pdf.

[57] The Royal Academy of Engineering. (2013) Extreme space weather: impacts on engineered systems and infrastructure. ISBN 1-903496-95-0.

[58] Space Studies Board, Division on Engineering and Physical Sciences. (2009) Workshop report: Severe Space Weather Events – Understanding Societal and Economic Impacts. ISBN 978-0-309-13811-6. Available online: https://nap.nationalacademies.org/read/12643/chapter/4#8.

[59] Kintner, P.M., Humphreys, T., Hinks, J. (2009) Inside GNSS: GNSS and Ionospheric Scintillation, How to Survive the Next Solar Maximum. Available online: https://www.insidegnss.com/auto/julyaug09-kintner.pdf.

[60] IALA. Recommendation R0129 GNSS Vulnerability and Mitigation Measures.

9. FURTHER READING

1. S.J.Harding, Study into the impact on capability of UK Commercial and Domestic Services Resulting from the loss of GPS Signals. Qinetiq Report for the UK Radiocommunications Agency, 2001.
2. Konovaltsev, A. & Marcos, E. & Caizzone, S. & Yinusa, K. & Meurer, M. (2018) Characterisation of Radio Frequency Interference for GNSS Maritime Applications.
3. ICAO. (2017) Navigation Systems Panel, Fourth meeting (NSP/4-Flimsy/13): DFMC SBAS Key Concepts.
4. Walter T., Blanch J., Joerger M., Pervan B. (2016) Determination of Fault Probabilities for ARAIM.

ANNEX A SPACE WEATHER EFFECTS

Modern society depends on a variety of technologies that are susceptible to the extremes of space weather and severe disturbances of the upper atmosphere and of the near-Earth space environment that are driven by the magnetic activity of the Sun. The Sun continuously releases random bursts of energy and highly charged particles. The impact of these emissions on Earth is known as a space weather event. Bursts of electromagnetic energy can result in radio blackouts; bursts of high energy particles can increase ionising radiation and affect satellite performance; and bursts of magnetised plasma can result in the degradation and potential loss of radionavigation signals on Earth.

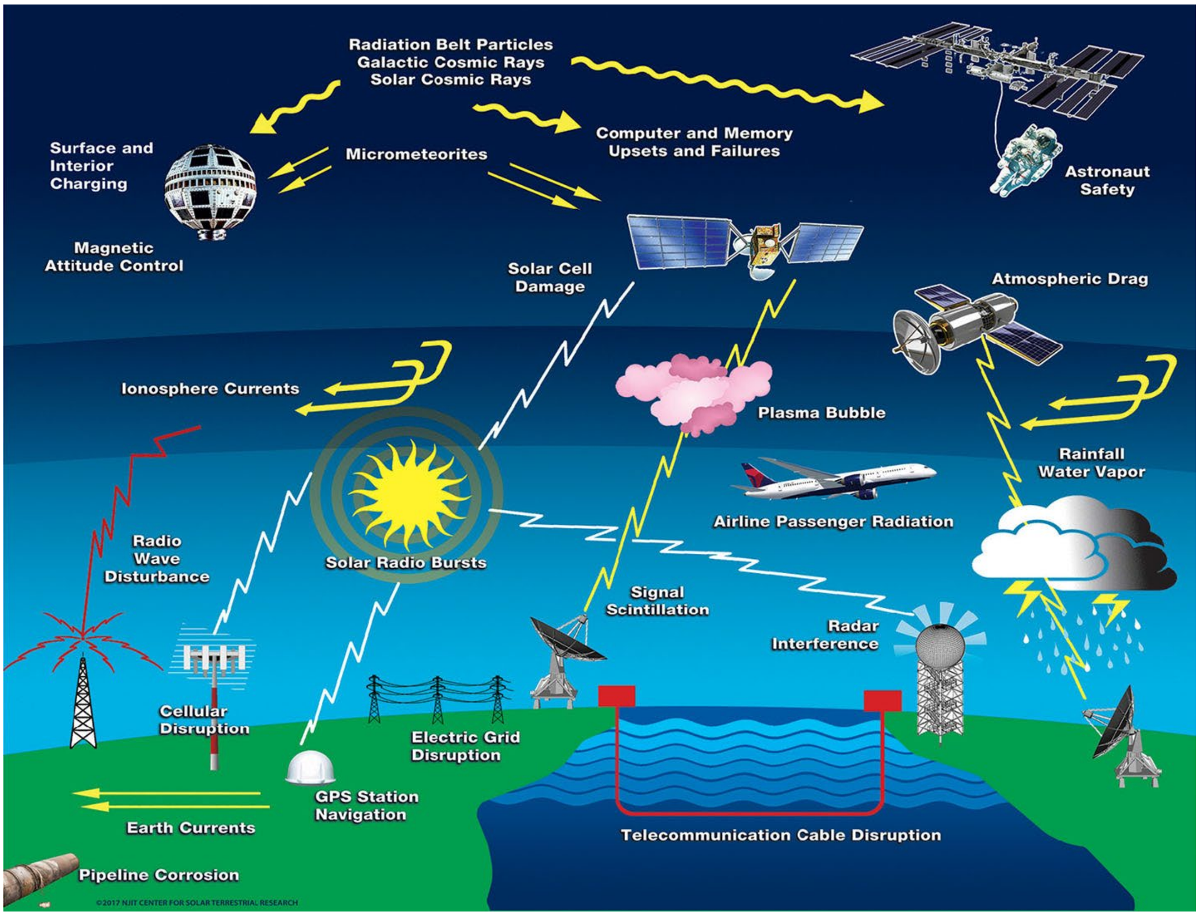

Figure 3 Different systems affected by space weather [57].

The amount of solar activity is linked to the natural sunspot cycle, which shows that the number of sunspots peak approximately every 11 years. Sunspots occur almost continuously, but normally give rise to weak solar events that generally go by unnoticed. The most intense storm ever encountered until today is the 1859 Carrington Event geomagnetic storm which happened during solar cycle 10, a few months before the solar maximum. The impact of a geomagnetic storm of this magnitude today would render GNSS satellites inoperable, compromise cell phone reception and create extended outages of the electric power grid system. Fortunately, such major event has not been repeated yet, but less severe storms continue to be recorded by the experts such as the 2003 Halloween solar storm which affected numerous satellites, aircrafts, satellite communications and electric power grid systems. During the Halloween storm, the SBAS Wide Area Augmentation System (WAAS) was also disabled for 30 hours [58]. In 2006, solar flares from the sun were reported to disrupt mariners and aircraft landing systems. In 2011 Global Positioning System (GPS) users with dynamic positioning on the daylight side of the Earth were impacted for 8 minutes and in 2014 satellite navigation was disrupted in part of Europe for 15 minutes. However, it is important to note that these events are stochastic in nature and thus unpredictable.

Space weather events could affect GNSS derived position, navigation, and timing information by affecting the satellite's operation or position, the GNSS signals characteristics, along with affecting the user's ability to receive the transmitted signals. At the most extreme, the receiver's tracking of GNSS signals could be lost due to interference and noise. Similar effects are also present in RNSS systems and services.

There are several ways in which space weather can affect GNSS and other radio signals. GNSS radio signals travel from the satellite to the receiver on the ground, passing through the Earth's ionosphere. The charged plasma of the ionosphere bends the path of the GNSS radio signal like the way a lens bends the path of light.

The ionosphere is one of the major error sources that affect the position estimation. Therefore, its study and characterisation is of paramount importance to minimise the user errors through models or other techniques. The ionosphere general behaviour and its long-term changes are quite well known. This knowledge together with the use of double frequency solutions (which almost corrects the influence of the ionosphere) reduce the impact on the GNSS signals and focus the ionosphere research on its fast changes and irregularities, the so-called scintillations.

Ionospheric scintillation is a form of space-based multipath. A planar electromagnetic signal wave goes through a volume of ionospheric irregularities, which is formed by regions with different electron density. Scintillations affects GNSS signals in two ways: refraction and diffraction. Both of these cause group delay and phase advance of the GNSS signals as they interact with free electrons along their transmission path. The number of ionospheric free electrons is usually expressed as Total Electron Content (TEC).

Signal refraction takes place when large-scale variations in TEC along the signal path through the ionosphere cause a group delay and a phase advance. Signal diffraction is more complicated. Ionospheric irregularities with scale lengths of about 400m scatter GNSS signals, so the radio wave reaches the receiver through multiple paths. Both are called scintillations, although diffractive scintillations can seriously challenge GNSS receivers causing deep power fades and fast phase variations.

Ionospheric scintillations mainly affect the amplitude and phase of the signals at the receiver, and their behaviour is usually characterised by the level of two scintillation parameters: S4 (for amplitude fluctuations) and $\sigma_{\Delta\phi}$ (for phase fluctuations).

Ionospheric scintillation does not homogenously affect all regions of the Earth:

- At high latitudes the northern lights disrupt GNSS signals and magnetic storms in which blobs of different electron contents swept over the polar cap from the dayside onto the night side. The polar scintillations mainly produce fluctuations in the phase of the receiver signals.
- At tropical latitudes the ionosphere creates its own storms that typically form after sunset and last for several hours. This tropical behaviour is more intense at the equinoxes. The equatorial scintillations mainly produce fluctuations in the amplitude of the receiver signals.
- At mid-latitudes the threat comes during magnetic storms. Although there is a low level of ionospheric activity at mid-latitudes it should not be assumed that no activity exists there.

The Figure 4 identifies the regions on the Earth where ionospheric scintillations are more/less frequent.

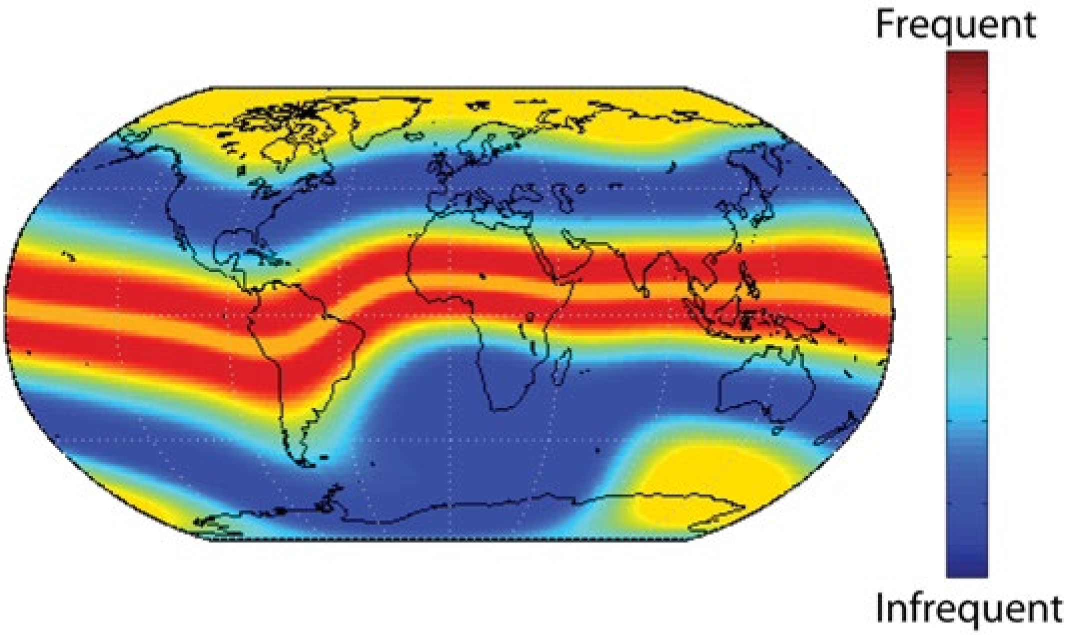

Figure 4 Scintillation frequency map [59].

Additionally, the scintillation activity also depends on several temporal scales:

- Scintillations’ activity is generally higher in periods of high solar activity.
- Scintillations´ effects are generally stronger during the equinoctial months.
- Scintillations generally occur between sunset and midnight and occasionally continue until dawn.

Scintillations can mainly affect GNSS signal in two ways:

- Producing severe radio signal disruptions (and thus leading to signal losses).
- Increasing the error of the user range (i.e. increasing the corresponding User Equivalent Range Error (UERE) values).

From a physical point of view, scintillation is a perturbation of the phase fronts of the transmitted signal that modifies the magnitude and phase at the receiver depending on the recombination of the signal. When the phase recombination is destructive, the loss of signal power at the receiver level can be large enough to lead to a cycle slip, a loss of carrier tracking or even a loss of code and carrier tracking.

Phase fluctuations due to scintillation are also problematic since they can lead to a receiver Phase Lock Loop (PLL) loss of lock. In the equatorial regions, this phenomenon is of second order after the signal fades. In Polar Regions, however, the phase fluctuations may become large enough for the receiver to lose the satellite tracking.

ANNEX B OBSERVED EFFECTS OF GNSS LOSS TO ON-BOARD SYSTEMS

Table in this Appendix introduces observed effects of GNSS loss to onboard systems, additional to the audible alarms and visual information and warning messages.

Onboard system	Function and GNSS use	Observed effects/ potential impact
Automatic Identification System (AIS)	Reporting system that automatically provides updates of surrounding vessel's position and other voyage data to avoid collision. Uses GNSS position for position reports transmitted to other vessels and shore. Uses GNSS timing to transmission synchronisation.	– Loss of vessel's own position for AIS transmission (and therefore the situational awareness of the proximity of other reported AIS targets)
Digital Selective Calling, VHF/HF (DSC)	Sending distress signal containing own's ship location, Maritime Mobile Service Identity (MMSI) number and other information. Core of the GMDSS system. Uses GNSS position and time when making a DSC call.	– Loss of position and Universal Time Coordinated (UTC) timestamp information
Electronic Chart Display and Information System (ECDIS) & Electronic Chart System (ECS)	ECDIS complying to IMO regulations and the ECS provide continuous position and navigational safety information and alarm when the vessel is in proximity to navigation hazards such as shallow waters. Uses GNSS for SOG, COG and position reference to map the vessel's own position on a chart.	– Loss of vessel's position on the chart – Loss of Under Keel Clearance (UKC) monitoring – Loss of SOG and COG – Loss of heading and active waypoint coordinates
Global Maritime Distress and Safety System (GMDSS)	Alert search and rescue organisations and nearby vessels that may be able to offer assistance. Provide the vessel's position to rescue authorities.	– Loss of automatic update capabilities from last known position. Updated positions needed to be manually entered regularly
Global Navigation Satellite System (GNSS) navigation receiver with augmentation	Provides positioning accuracy and integrity required for entrances and harbour approaches and other waters where freedom of manoeuvre is limited. Provides the accurate timing information. Uses GNSS for calculating position solution and augmentation system for enhancing position accuracy and for integrity.	– Loss of GNSS and DGNSS input data for position fixing – Loss of ability to provide the Electronic Position Fixing System (EPFS) message and timing information – Possibly provision of wrong navigation data
Gyrocompass	Used for determining vessel's heading by finding true north and for calculating the rate of turn component. Uses GNSS for vessel speed error correction and latitude correction.	– Standby mode message – Heading maintained – Loss of position correction to derive true north

Onboard system	Function and GNSS use	Observed effects/ potential impact
Radar display	Provides collision avoidance and search and rescue localisation. The range and bearing are non-GNSS dependent but directly dependent of the distance and the quality of the return signal from a known target. Uses GNSS for vessel latitude and longitude, SOG and COG reference.	– Standby mode message – Loss of latitude, longitude – Loss of ground stabilisation info – Loss of water depth profile history from depth sounder – False SOG and COG values – Range and bearing relative to centre of video circle instead of own's ship's position – Switch to Dead Reckoning mode
Satellite Broadband Antenna	Provide Internet connectivity at sea. Assist the vessel's satellite antenna(s) in locating and tracking satellite position.	– Loss of satellite lock
Voyage Data Recorder (VDR)	Records information of all interconnected systems on a vessel assisting in incident investigation, performance analysis, vessel tracking, preventive maintenance, etc. Vessel GNSS position, COG, SOG, AIS, Radar targets, Gyroscope and timing synchronisation to UTC are some of data logged in the VDR.	– Loss of UTC timestamp information
Dynamic Positioning (DP)	Maintain vessel's position and heading to remain in a fixed location usually for offshore drilling vessels or keep track as for pipe or cable laying vessels.	– Loss of position, SOG and COG reference to assist the system in calculating the required steering angle and thruster output to maintain the vessel's position leading to inability to maintain DP mode
Ship's clock	Accurate time is required by law during voice communication on a ship.	– Loss of time reference since GNSS timing information is used to synchronise the ship's clock.
Bridge Navigational Watch Alarm System (BNWAS)	BNWAS is a monitoring and alarm system which notifies other navigational officers or master of the ship if the officer on watch does not respond, or he/she is incapable of performing the watch duties efficiently. To avoid this, BNWAS is installed on the bridge which acts similar to a dead man alarm in the engine room. The BNWAS is automatically activated when the vessel is navigating by means of heading or track control system (autopilot/trackpilot) and inhibited as the heading/track control system is deactivated. GNSS is an input to activate automatically the BNWAS	– Loss of position, SOG and COG reference to automatically activate the BNWASS

Onboard system	Function and GNSS use	Observed effects/ potential impact
Bow thruster propeller (BTP)	The bow thrusters are used to help manoeuvrability of the vessel at lower speeds. An input data of SOG using the GNSS source is fitted in the BTP to deactivate it when the SOG value exceeds a set value.	– Loss of SOG reference to automatically deactivate the BTP

ANNEX C EXAMPLE OF GNSS RISK ASSESSMENT SCORING TABLE

Table 4 provides an example on the use of Risk Scoring table. The purpose of the table is to compare the level of risk that different identified hazard types may impose to the PNT uses under evaluation. It helps to identify the high-risk areas where additional risk control options should be considered.

Table 4 Estimated total risk to GNSS services by various hazards, adapted from [26].

	Risk Vector	Vulnerability	Consequence	Threat*		Risk Score**
				Intent	Capability	
I. Natural & II. Accidental	1. Built structure obstruction	1	2	5		10
	2. Terrain obstruction	1	2	5		10
	3. Foliage (pines, heavy canopy)	1	1	5		5
	4. Solar activity - mild	1	1	5		5
	5. Solar activity - moderate	3	2	4		24
	6. Solar activity - powerful	5	5	2		50
	7. Human error/software	5	1-5***	3		15-75
	8. Satellite malfunction	1	1	4		4
	9. Control segment failure	5	5	1		25
	10. Space debris	1	4	2		8
	11. Unintentional RF	5	1-4***	5		25-100
III. Malicious	12 Privacy seeker (1 event)	5	3	5	5	75
	13. Criminal jamming (1 event)	5	3	5	5	75
	14. Criminal + Privacy 1 Yr Total	5	5	5	5	125
	15. Criminal spoofing (1 event)	4	3	4	4	48
	16. Terrorist jamming	5	5	5	5	125
	17. Terrorist spoofing	4	4	3	4	56
	18. Military-style jamming	5	5	5	5	125
	19. National agent spoofing	3	4	4	4	48
	20 Attack on satellites	5	5	1	1	25
	21. Attack on control segment	1	1	1	2	1.5
	22. Cyber-attack on control segment	2	5	3	2	25

* For Natural and Accidental hazards Thread is expressed as a single value. For Malicious hazards Thread is expressed by two separate parameters (Intent and Capacity) and the Thread for the Risk Score calculation is defined as the arithmetic mean of the two values.

** Risk Score is calculated as product of Vulnerability, Consequence and Thread.

*** If required, Risk parameters can be described by a range of values with lower and upper limit. Risk Score is calculated based on both limits.

The value of Risk Score parameters in Table 4 is estimated in scale from 1 to 5 [26].

For Vulnerability:

1	Low	Risk vector able to impact less than 5% of users
2	Moderate	Difficult for this risk vector to impact overall GPS service, or more than 10% of users
3	Significant	Fairly easy for this vector to impact many unsophisticated users and high performance users
4	High	Fairly easy for this vector to impact all or most users
5	Severe	Very easy for this vector to impact all or most users

For Consequence:

1	Low	No noticeable economic losses, unlikely impact to safety of life
2	Moderate	Probable economic losses, possible safety of life impacts
3	Significant	Documented economic losses, probable safety of life impacts
4	High	Economic losses > $1B, injuries, probable loss of life
5	Severe	Economic losses > $5B, and/or loss of life

For Threat of Natural and Accidental events:

1	Low	Probability/history of occurrence < once every 100 years
2	Moderate	Probability/history of occurrence > once every 100 years
3	Significant	Probability/history of occurrence > once every 50 years
4	High	Probability/history of occurrence > once every 10 years
5	Severe	Probability/history of occurrence > once every year

For Threat of Malicious acts:

For Intent:

1	Low	No expressed desire or interest
2	Moderate	Rarely expressed desire or interest
3	Significant	Repeat expressions of interest, some attempts, possible successes
4	High	Repeat expressions of interest, some attempts, some successes
5	Severe	Repeat expressions of interest, many attempts, many successes

For Capability:

1	Low	No known ability to access and use this method
2	Moderate	Available to some nations & sophisticated actors (global criminal networks, terrorist organisations)
3	Significant	Available to all nations & sophisticated actors
4	High	Available to moderately sophisticated actors (individual technologists, criminals, etc.)
5	Severe	Available to unsophisticated actors (low cost, easy to access or build and use)

ANNEX D GNSS VULNERABILITIES VS. MITIGATION MEASURES

The table in this Appendix provides a general overview of the identified mitigation measures and GNSS vulnerabilities they can mitigate.

Legend:

- + Significantly mitigates the vulnerability
- O Mitigates the vulnerability in some cases
- - Does not mitigate the vulnerability

	GNSS Vulnerabilities						
	Signal Interference					System Faults	
	Natural Interference		Man-made Interference				
				Intentional interference			
Mitigation measures*	**Multipath/NLOS etc.**	**Space Weather Events**	**Unintentional Interference**	**Jamming**	**Spoofing**	**Space Segment**	**User receiver segment**
Service design	**-**	**o**	**+**	**o**	**+**	**+**	**-**
Dual frequency service	-	o	+	o	o	+	-
Navigation message authentication	-	-	-	-	+	-	-
User receiver	**+**	**+**	**+**	**o**	**+**	**+**	**+**
Duplication of equipment, backup power, etc.	-	-	-	-	o	-	+
Signal processing, antenna design and location	o	-	+	o	o	-	-
Multi-constellation receiver	o	o	o	o	o	+	-
Multi-frequency receiver	o	o	+	o	o	-	-
RAIM	+	+	+	o	o	o	-
GNSS augmentation systems	o	o	-	-	-	+	-
Signal authentication detection	-	-	-	-	+	-	-
Use of multiple PNT sources	**+**	**+**	**+**	**+**	**+**	**+**	**+**
LEO-based systems	o	o	+	+	+	+	+
Terrestrial-based systems	+	+	+	+	+	+	+
Onboard sensors	+	+	+	+	+	+	+
Visual AtoNs	+	+	+	+	+	+	+
External support	+	+	+	+	+	+	+
Monitoring and alerting	**+**	**+**	**+**	**+**	**+**	**+**	**-**

* Some of the mitigation measures listed include more than one technology (e.g. Terrestrial-based includes eLoran, R-Mode etc.). In these cases, the assessment has been done according to the option that gives the best mitigation result.

ANNEX E SUGGESTED MINIMUM MARITIME USER REQUIREMENTS FOR GENERAL NAVIGATION – BACKUP SYSTEM

The Table in this Annex is copied from [60].

	System level parameters				Service level parameters			
	Absolute Accuracy	Integrity			Availability % per 30 days	Continuity % over 15 minutes[3]	Coverage	Fix interval (seconds)
	Horizontal (metres)	Alert limit (metres)	Time to Alarm[2] (seconds)	Integrity Risk (per 3 hours)				
Ocean	1000	2500	60	10^{-4}	99	N/A[2]	Global	60
Coastal	100	250	30	10^{-4}	99	N/A[2]	Regional	15
Port approach and restricted waters	10	25	10	10^{-4}	99	99.97	Regional	2
Port	1	2.5	10	10^{-4}	99	99.97	Local	1
Inland Waterways	10	25	10	10^{-4}	99	99.97	Regional	2

Notes:

1. This table is derived from IMO Resolution A.915(22).
2. Continuity is not relevant to ocean and coastal navigation
3. IMO Resolution A.1046(27) amended the Continuity Time Interval to 15 minutes rather than 3 hours as originally required in IMO Resolution A.915(22).