|  |
| --- |
| IALA Guideline |

Gnnnn

RESILIENT PNT (WORKING DRAFT)

Edition x.x

Date (of approval by Council)

urn:mrn:iala:pub:gnnnn

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

|  |  |  |
| --- | --- | --- |
| Date | Details | Approval |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. INTRODUCTION 5

1.1. Background 5

1.2. Scope 6

2. SOURCES OF PNT VULNERABILITIES 6

2.1. Signal interference 6

2.1.1. Natural interference 6

2.1.2. Man-made interference 7

2.2. Equipment malfunction 7

3. IMPACT OF PNT FAILURES 8

3.1. Effect on maritime AtoNs 8

3.2. Effect on shipborne equipment 8

4. ENHANCING PNT RESILIENCE 10

4.1. Hazards identification 11

4.2. Risk assesment 12

4.3. Risk control options 12

4.3.1. Failsafe system/service design 13

4.3.2. Use of multiple PNT sources 15

4.3.3. Education and training 17

4.3.4. Monitoring and alerting 17

5. DEFINITIONS 17

6. ABBREVIATIONS 17

7. REFERENCES 18

8. FURTHER READING 19

9. INDEX 20

List of Tables

Table 1 Observed effects and possible impacts of GNSS loss to the vessel and its onboard systems 9

Table 2 Example of identifying PNT failure types and their characteristics 11

Table 3 Status of L5/E5a/B2a signals as of March 2020 13

List of Figures

Figure 1 Different systems affected by space weather (Source: Bell laboratories, Lucent Technologies) 21

Figure 2 Scintillation frequency map 23

# INTRODUCTION

## Background

Today’s vessels and many marine aids to navigation (AtoN) rely on electronic position, navigation, and time (PNT) information which is predominantly received from the global navigation satellite systems (GNSS). However, several studies indicate that GNSS services are vulnerable to intentional and unintentional interference and common failure modes [1], [2], [3], [4], [5].

IMO e-Navigation strategy recognizes the importance of resilience of electronic systems and mentions especially position fixing systems. The IMO e-Navigation strategy states:

“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 Systems (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 introduction of autonomous vessels further highlights the importance of resilient PNT information.

IALA Dictionary defines resilient PNT as follows:

"Position, Navigation and Timing services made resilient by building-in, or otherwise providing, standby capacity or by switching to alternative means."

Resilient PNT is best achieved by combination of multiple dissimilar PNT sources because no single PNT source is perfect. GNSS, terrestrial PNT services, augmentation services, vessel traffic services and ship-based sensors can be considered as candidates for resilient PNT system components. However, it is recognised from the start that no solution will ever be fully resilient and that the level of resilience achieved will be proportional to the overall cost.

The general responsibilities of Maritime Authorities related to the provision of PNT services may be derived from the Chapter V of IMO 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 guidelinesfootnote 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.

Footnote: Refer to the appropriate recommendations and guidelines of IALA and to SN/Circ.107 - Maritime buoyage system."

Maritime Authorities should evaluate the level of PNT resilience required in their responsibility area based on the risk assessment and arrange for the provision of appropriate services to ensure that the wanted level of resilience is achieved.

## Scope

This Guideline intends to help administrations to understand PNT system vulnerabilities and possible impacts of PNT failures to AtoN service and to vessel systems, and to consider measures to increase PNT resilience and mitigate the possible risks identified.

Because of the wide adaptation of GNSS as a primary source of PNT information in the maritime domain, this Guideline is focused on GNSS vulnerabilities and possible mitigation measures of GNSS failures. However, guidance in this document can be extended to other radionavigation and communication systems as well.

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

# SOURCES OF PNT VULNERABILITIES

Some vulnerabilities are common to all types of electronic navigation systems including GNSS. These vulnerabilities are related to 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, signals may not be received correctly due to natural or man-made interference or may originate from falsified source, or the user receiver can be malfunctioning.

## Signal interference

Radio signals can be affected by natural events, such as space weather or by 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 is higher in coastal waters and ports. Majority of the man-made interference is unintentional and affects only limited line-of-sight areas, but the risk of intentional wide area man-made interference should also be recognized.

GNSS signals are particularly susceptible to interference due to the extremely low level of the signal at the user receiver. 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]](#footnote-1).

### Natural interference

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 trough the Earth's atmosphere. Space weather events cause irregular spatial and temporal disturbances to the propagation path, especially to the ionosphere, which may cause GNSS signals to suffer from delays, interference, and noise, leading to errors in PNT estimations or totally preventing the tracking of GNSS signals. The type and expected frequency of atmospheric disturbances varies for example depending on the latitudes. Detailed information on the effects of space weather to the ionosphere and GNSS signals is provided in Appendix 1.

Something about multipath and its effects on GNSS signal reception added here?

### Man-made interference

Man-made interference can be ether 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.

Unintentional sources of man-made GNSS interference include strong RF signals, harmonics or intermodulation products from powerful transmitters operating in other frequency bands or from sources close to GNSS receivers. These can be for example television or radio broadcasting stations, microwave communication links or VTS 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 [9]. This type of interference may temporarily prevent the receiver from tracking the satellite signals and providing PNT solution.

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 materialize 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 unauthorized Personal Privacy Devices (PPDs)
* Availability of affordable COTS technology
* Availability of free training materials and hacking guides on internet with minimum knowledge necessary to implement
* Growing number of events with 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 signals, negative effects on other nearby receivers are however difficult to avoid.

Another type of intentional man-made GNSS signal interference is the transmission of falsified signals. This type of activity is called spoofing. Intention is to get the receiver to lock into simulated or genuine but delayed GNSS signals. In this way, the receiver can be deceived to provide false position solution or no position information at all [10]. Consequences of spoofing can be far more serious than 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 that jamming but unfortunately also spoofing events have been observed and reported in recent years. Spoofing is generally linked more to the military than to civil activities.

## 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 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, accident or errors may happen during maintenance and service infrastructure can be target to a cyber-attack.

GNSS constellations are designed to be very secure and robust. Failures of individual satellites are not unusual but total service outages or failures are very rare events. Nevertheless, every GNSS has experienced such failures (examples or reference from GMV?).

Failure of GNSS equipment on board a vessel is also 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 [11].

# IMPACT OF PNT FAILURES

## Effect on maritime AtoNs

Traditional maritime 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 however directly relying on GNSS for time synchronisation and/or position fixing. These include:

* Synchronized lights which receive an accurate time reference from GNSS
* AtoNs using AIS technology and receiving an accurate time reference and in case of floating aids also an accurate position from GNSS

Synchronized 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 synchronize correctly leading to flashing characteristics contrary to that published and affecting the visual conspicuity of the pilot.

AIS system uses time division transmission technology where 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.

GNSS failures would also affect Vessel Traffic Services. Vessels’ AIS 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. Additionally, possible transmission slot collisions could block the normal reception of vessels' AIS reports.

## Effect on shipborne equipment

Modern bridge systems are interconnected and strongly dependent on GNSS. The high degree of interconnection among the different systems onboard a vessel increases its vulnerability to GNSS failures, compromising bridge navigation system as well as GNSS-based timing systems and communication equipment. It should be noted that GNSS failures would impact not only the means of navigation but also information exchange between ships as well as ship to shore data communications (e.g. AIS reporting).

When GNSS is unavailable, some onboard vessel instruments respond almost instantly with sound alarms and screen messages indicating the loss of the GNSS feed but in case of falsified GNSS signals the navigator may remain unaware of the error situation.

If GNSS information is unavailable or falsified, vessels position, speed over ground (SOG) and course over ground (COG) information could be missing or incorrect. This could lead vessels equipped with integrated bridge systems to undertake inadequate course and heading changes.

Table 1 gives examples of the effects that the loss of GNSS may have on different onboard systems and the possible impacts on the vessels ability to navigate safely.

1. Observed effects and possible impacts of GNSS loss to the vessel and its onboard systems

| Onboard system | Function and GNSS use | Observed effects | Possible impacts |
| --- | --- | --- | --- |
| 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. | * Display alarm status * Loss of vessel’ own’s position info for AIS transmission | [Collision] |
| Digital Selective Calling (VHF/HF) | Sending distress signal containing own’s ship location, MMSI number and other information. Core of the GMDSS system.  Uses GNSS position and time when making a DSC call. | * Loss of position and UTC timestamp information | [Loss of life] |
| ECDIS & 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 speed over ground (SOG), course over ground (COG) and position reference to map the vessel's own position on a chart. | * Loss of depth below keel info * Loss of SOG and COG * Loss of heading and active waypoint coordinates * Loss of vessel’s position on the map | [Collision, grounding] |
| GMDSS | Alert search and rescue organizations and nearby vessels that may be able to offer assistance.  Provide the vessel’s position to rescue authorities. | * Loss of satellite communication synchronization (SAT-C) * Loss of automatic update capabilities from last known position. Updated positions needed to be manually entered regularly | [Loss of life] |
| 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.  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 the External Electronic Position Fixing System (EPFS) message | [Collision, grounding] |
| 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[[2]](#footnote-2) | [Collision, grounding] |
| RADAR | 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 * 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 | [Collision, grounding] |
| 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 | [TBD] |
| Voyage Data Recorder | 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 synchronization to UTC are some of data logged in the VDR. | * Loss of UTC timestamp information | [TBD] |

# ENHANCING PNT RESILIENCE

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 [12] should be followed when defining the target level of PNT service resilience in particular area. Maritime authorities need to consider separately how:

* 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 [12]:

1. Identify hazards
2. Assess risk
3. Specify risk control options
4. Make a decision
5. Take action

It should be noted that risk management is continuous process and the steps listed above should be repeated in frequent intervals (e.g. every X year).

The sections 4.1 and 4.2 will give guidance on PNT service hazard identification and risk assessment respectively. The section 4.3 introduces possible risk control options. The risk assessment will provide basis for decision making and possible deployment of additional risk control measures.

## Hazards identification

Section 2 of this guideline introduced the main sources of PNT failures, which are signal interference (either natural, unintentional, or intentional) and equipment malfunction.

Maritime Authorities should identify and list the relevant PNT service failure types that may affect AtoN services or vessels respectively. The probability, duration and area affected for each of failure types may be initially estimated. Result can be a table listing identified failure types and their characteristics (Table 2).

1. Example of identifying PNT failure types and their characteristics

| PNT failure type | Probability | Area affected | Duration of event |
| --- | --- | --- | --- |
| Description of failure type (e.g. GNSS jamming) | Described verbally using agreed scale, for example:   * 1 = very low (e.g. none in 20 years) * 2 = low * 3 = moderate * 4 = high * 5 = very high (e.g. every day) | Described verbally, for example:   * Phase of navigation: Ocean, Coastal, Port (or other restricted water * Range: Local (<50nm), Regional (>50nm), Global | Described verbally for example:   * Order of magnitude: Minutes, Hours, Days, Months |
| Description of each failure type on its own row |  |  |  |

The impacts of each identified failure type should then be initially estimated. This initial review will help to identify those failure types that need to be analysed later in more detail via risk assessment. Impact may be described verbally using an agreed scale, for example for vessels:

* 1 = very low: minor delay
* 2 = low: delay without economic impact
* 3 = moderate: important delay with economic impact
* 4 = high: accident without deaths
* 5 = very high: accident with deaths

When estimating how PNT failures impact vessels, for example the following aspects can be considered:

* Capability to compute the vessel's own position
* Capability to communicate vessel's own position to other vessels and to the shore
* Capability to know other vessels' positions
* Capability to navigate with good weather conditions (good visibility)
* Capability to navigate with bad weather conditions (poor visibility)
* Capability to avoid collision with good weather conditions
* Capability to avoid collision with poor weather conditions
* Capability to arrive at destination on time (good weather)
* Capability to arrive at destination on time (poor weather)

[Similar lists for AtoNs?]

The result of this first assessment should be a list of PNT failure scenarios that are estimated to be able to cause the most severe impacts on AtoNs or vessels respectively.

## Risk assesment

Risk assessment 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 impact (Equation (1)). The same equation can be used both for qualitative and quantitative assessment.

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 verbally using an agreed scale. In case of malicious events, the probability could be estimated as the product of capacity, opportunity, and motivation [13].

Impact can have a numerical monetary value but is more likely to be described verbally 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.

Risk assessment may use a risk matrix to visualize level of risk that can or cannot be accepted (Figure X).

[Figure X with Risk Matrix using Impact scale 1-5 and Probability scale 1-5, and defining Acceptable, Acceptable with caution and Unacceptable risk levels to be added here, ref. G1018?)

Risk assessment will identify events with have an unacceptable high-risk level and where risk control options (additional to those already deployed) need to be considered.

## Risk control options

PNT service risk control options aim to decrease both the probability and the consequences of PNT failures. Probability of an 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.

[Table that gathers all mitigation options and indicates which vulnerabilities they mitigate could be added here?]

This chapter introduces measures that may be used to mitigate the risk of 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.

### Failsafe system/service design

PNT systems should be designed to detect and tolerate 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 need to be physically protected and countermeasures to protect service from possible signal interference from natural, unintentional, and intentional sources need to be considered. Proper design will also consider measures to inform users in case on service failures. It is to be noted that Maritime Authorities can directly influence only the design of systems and services they are providing themselves.

#### Service infrastructure

The infrastructure of all GNSS constellations is designed to be very secure and robust and total system failures are rare (see Section 2.2). 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 dual frequency service for public use in near future (Table 3). Several GNSS signals allocated to different frequencies will allow receivers to benefit from multi-frequency signal processing for the removal of any frequency-dependent errors on the signals and thereby improving receiver accuracy. This is an effective way to remove ionospheric error from the position calculation such as scintillation effects that are the main contributor to the overall measurement error in the position calculation.

1. Status of L5/E5a/B2a signals as of March 2020

| Signal | Current status | Future deployment |
| --- | --- | --- |
| GPS L5 | L5 is broadcast from 12 satellites in pre-operational mode and is set to unhealthy until further monitoring capability are established (GPSIII and OCX). | Planned to be available on 24 GPS satellites in 2027. |
| GLONASS L5 | L5 signal from the GLONASS-KM satellites currently in research phase. | Launch scheduled planned for 2025-2030. |
| Galileo E5a | Full Operation Capabilities in 2020 on 24 satellites. | Next generation satellites planned for 2025. |
| BeiDou B2a | BDS-3 B2a signals are planned to be available from 3 IGSO and 24 MEO satellites. | Full Operation Capabilities to be established by 2035. |

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)) [14]. The authentication is done by adding 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.

#### User receiver

[Can we add something specific about the PNT equipment installed (and used) in AtoNs and how they can be made more reliable?]

For vessel equipment, the measures to counteract GNSS receiver equipment failures are the same as for other onboard systems - the use of standby power supplies (required for SOLAS vessels) and following installation and fault-finding guidelines. Although the IMO carriage requirement is for a single Electronic Position Fixing System (EPFS), it is quite common for more than one navigation receivers to be fitted to provide redundancy in the event of equipment failure.

Further, it is recommended that the individual PNT receivers or data sources should be capable of checking the plausibility of the data to ensure that the data values are within the normal range. In this respect, two types of checks for plausible magnitudes can be carried out:

* Checks that the value is within plausible range as defined by manufacturers (e.g. plausible range in terms of heading, for example, is 0 to 360 degrees).
* Checks that operative modes or states are consistent when they are reported by multiple sentences from a single sensor/source or function (e.g. NMEA messages GGA and VTG are reporting equal operative states of a single GNSS).

Data which has failed the plausibility checks should not be used by the system and should not affect functions not dependent on these data.

[Something about interference protection using signal processing and antenna design to be added here]

##### 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 a 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.

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 band and reception is maintained.

##### Receiver Autonomous Integrity Monitoring

GNSS services do not broadcast any information about the integrity of their signals. 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 pseudorange measurements should all be consistent with the computed position. A pseudorange that differs significantly from the expected value may indicate a fault of the associated satellite or another signal integrity problem (e.g., ionospheric interference). It is to be noted that RAIM can function only if there are enough satellites in view (more than X).

GNSS integrity information can also be provided via external augmentation services (e.g. IALA Beacon DGNSS, SBAS).

### Use of multiple PNT sources

Use of more than one PNT sources 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.

[Can we say something about the multi-PNT options for AtoNs?]

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:

* 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.

For any GNSS constellation, only another GNSS constellation can be considered to provide a fully redundant system. However, GNSS backup can be provided by terrestrial radionavigation services like eLoran, radar AtoNs and R-Mode. Ships own sensors, visual AtoNs and external assistant from VTS are examples of contingency system.

Where the risk assessment concludes that a backup system (i.e. a system ensuring continued operation, but not necessarily with the full functionality of the primary system) is necessary, suggested minimum maritime user requirements (derived from IMO Resolution A.915(22)) for such a system are listed at Appendix 2. It may however be impractical to expect backup systems to achieve some of these standards, such as global coverage in the ocean phase of navigation or metre level accuracy in the port phase. In these cases, it might be necessary to navigate the ocean phase by dead-reckoning, or delay port manoeuvres until the primary navigation system is restored. The argument for a backup system may be dependent on the perceived threat to the primary system and the likely duration of primary system outages.

#### Onboard sensors

The integrity of 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 an alternative source of PNT information (in addition to GNSS) include:

* Inertial Navigation System (INS)
* Depth sounder
* Vision system
* Atomic clock
* Gyro compass
* ePelorus
* Radar

INS may provide dead reckoning position and navigation data when the GNSS signal is momentarily lost. INS consist of an Inertial Measurement Unit (IMU) and computational unit. IMU usually contains accelerometers, gyroscopes and may contain magnetometers, providing velocity, orientation and heading information respectively. Dead reckoning navigation requires a known starting point after which a high-quality INS can provide good position accuracy for several minutes [15].

Bathymetric navigation uses a depth sounder and the contours of the seabed to determine a position in the absence of GNSS or in some cases in addition to it. It is a technique that is generally applicable to offshore navigation and consists of deriving a position fix from the superimposition of a line of sounding measurements onto a seabed map. By matching this with a database, the vessel’s position may be inferred. Bathymetric navigation is also known as bottom-contour navigation (BCN). This satellite-free navigation technique requires accurate up-to-date charts, and it will, of course, have a limited use in areas that have shifting or less contoured seabed profiles. The level of performance for this technique depends on the terrain height variation and sensor resolution. The highest resolution sensors can measure more than 10,000 points simultaneously. The positioning accuracy can be as good as one metre but is typically around 10 metres for underwater vehicles/vessels. Surface vessel positioning may be less precise because the sensor will be further away from the seabed, although noise-like errors may be smoothed out through integration with dead reckoning. With the limitations above, bathymetric navigation can be considered a resilient improvement solution to some but not all navigation phases.

Vision systems are a sensor suite, generally used for collision avoidance, including, for example, a LiDAR that includes visible and infrared cameras and a radar. The information fed by these sensors can be fused and/or used for self-learning intelligent systems (e.g. Simultaneous localization and mapping (SLAM)) or feature matching. This kind of system is only useful for navigation in consistent (unchanging), constrained waters and would be utilized in situations like the docking of a ferry. A vision system is neither a navigation system nor a positioning system but can provide additional resiliency in very specific situations.

For timing consistency, an atomic clock can be used. A receiver fitted with an additional onboard source of accurate time, such as a chip-scale atomic clock (CSAC) can hold accurate time at sub-microseconds for hours after losing access to GNSS. GNSS receivers with a higher frequency stability clock such as a CSAC oscillator enhance the navigation solution in terms of low satellite visibility positioning accuracy, signal recovery (holdover), multipath and jamming mitigation and spoofing attack detection.

[Some text on gyro compass, ePelorus and radar to be added here]

#### Terrestrial systems

Existing and future:

* eLoran, PNT
* radar AtoNs (including radar absolute positioning), PN
* R-Mode; PNT
* Commercial services (e.g. Locata STL), PNT?

#### Visual AtoNs

#### External support

* VTS

### Education and training

An important measure to mitigate impacts of possible PNT failures is to raise the 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. [IMO's and/or the Nautical Institute's role in educating mariners?]

Actions and procedures in situations, where the primary PNT source is lost or is providing false information should be trained regularly.

The IALA World-Wide Academy (WWA) addresses the importance of uninterrupted PNT and the vulnerabilities of GNSS in the AtoN managers training modules on Marine AtoN, GNSS and e-Navigation. The aim is to highlight that an uninterrupted determination of such service is essential to e-Navigation.

### 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.

A GNSS failure may be of such a nature that it is 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 recognizing the GNSS events and secondly, informing mariners and solving the high levels of ambiguity during the event.

[Something about how to monitor and alert AtoN related GNSS faults to be added?]

Dedicated GNSS signal monitoring stations or network of stations could be established for monitoring and detecting GNSS failures. This type of monitoring could cover large areas or just some critical areas where incorrect PNT information is estimated to cause especially severe consequences.

# DEFINITIONS

The definitions of terms used in this Guideline can be found in the *International Dictionary of Marine Aids to Navigation* (IALA Dictionary) at <http://www.iala-aism.org/wiki/dictionary> and were checked as correct 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.

# ABBREVIATIONS

AIS

ATON

BCN

COG

COTS

CSAC

DGNSS

DSC

ECDIS

ECS

EGNOS

EPFS

GGA

GLONASS

GMDSS

GNSS

GPS

HF

IMO

IMU

INS

ITU

MMSI

NMEA

PNT

PPD

SAT-C

SBAS

SLAM

SOC

SOLAS

TV

UTC

VDR

VHF

VTG

VTS

WAAS

# REFERENCES

1. John A. Volpe National Transportation Systems Center, Vulnerability assessment of the Transportation Infrastructure relying on the Global Positioning System. Final report, August 2001. (John A. Volpe National transportation systems Center, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," 29 Aug 2001. [Online]. Available: https://www.navcen.uscg.gov/pdf/vulnerability\_assess\_2001.pdf. [Accessed Oct 2018]).
2. 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.
3. GNSS 2 High Level Group 3 on Security and Defence issues, 1999.
4. The Galileo System Security Board (GSSB) – Galileo Threats and Vulnerabilities, 2001.
5. Global Navigation Space Systems: reliance and vulnerabilities, The Royal Academy of Engineering, ISBN 1-903496-62-4, March 2011.
6. Handbook on radiometeorology
7. Handbook on ground wave propagation
8. Handbook on the ionosphere and its effects on radiowave propagation
9. J.R. Clynch, A.A. Parker, R.W. Adler, W.R. Vincent, P. McGill, G. Badger. GPS World, January 2003. The Hunt for RFI – Unjamming a Coast Harbor.
10. Above us only stars - report
11. A.Grant, P.Williams, N.Ward & S.Basker, GPS Jamming and the Impact on Marine Navigation. GNSS Vulnerabilities and Solutions Conference, Royal Institute of Navigation. September 2008.
12. IALA Guideline 1018 on Risk Management
13. IALA Cyber security workshop, presentation by Dr. Jose M. Fernandez
14. <https://www.euspa.europa.eu/newsroom/news/tests-galileo-osnma-underway>
15. <https://www.vectornav.com/resources/inertial-navigation-articles/what-is-an-ins>

# FURTHER READING

1. TBD….

# INDEX

**No index entries found.**

1. 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 the Earth is known as space weather event. Bursts of electromagnetic energy can result in radio blackouts; bursts of high energy particles can increase ionising radiation and affect space craft performance; and bursts of magnetised plasma can result in the degradation and potential loss of radionavigation signals on Earth.



1. Different systems affected by space weather (Source: Bell laboratories, Lucent Technologies)

The amount of solar activity is linked with 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. Storms with the strength to affect everyday operations are very infrequent, with the most extreme storms referred to as once in 300- or 500-year events. However, it is important to note that they are stochastic in nature and as such could occur at any time.

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.

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 GPS 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 systems 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 types 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 characterized by the level of two scintillation parameters: S4 (for amplitude fluctuations) and σ\_φ (for phase fluctuations).

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

* At high latitudes the northern lights disrupt GNSS signals and magnetics storms in which blobs of different electron contents swept over the polar cap from the dayside onto the night side.

It is important to point out that 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.

It is important to point out that 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 next figure (from Reference?) identifies the regions on the Earth where ionospheric scintillations are more/less frequent.



1. Scintillation frequency map

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

* Scintillations' activity is generally higher in periods of high solar activity.
* Scintillations´ effect are generally stronger during the equinoctial months.
* Scintillations generally occur between sunset and midnight, and occasionally continue until dawn.

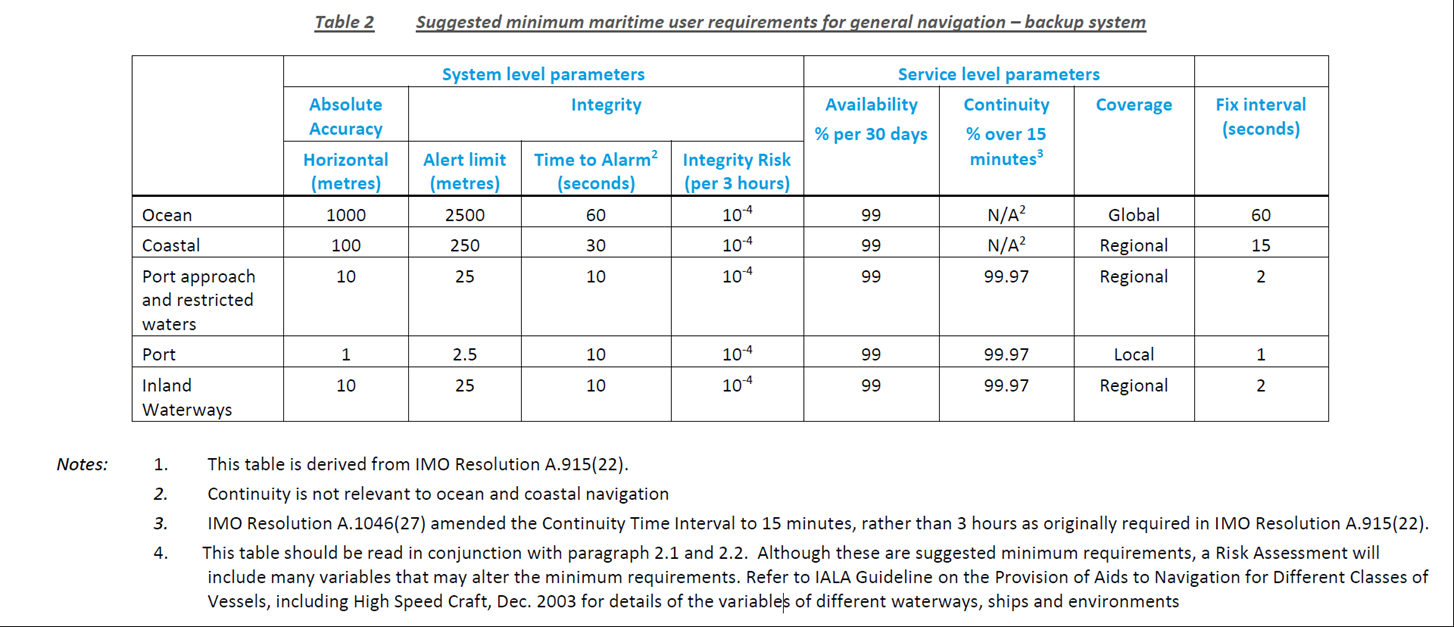
Scintillations can mainly affect GNSS signal in two ways:

* Producing severe radio signal disruptions (and thus leading to signal losses).
* Increasing the error of the user range (i.e. increasing the corresponding 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. We talk about signal fades.

Phase fluctuations due to scintillation are also problematic since they can lead to a 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.

1. SUGGESTED MINIMUM MARITIME USER REQUIREMENTS FOR GENERAL NAVIGATION – BACKUP SYSTEM



1. Minimum signal power level of -160 dBW for GPS signals and -154 dBW for Galileo signals. [↑](#footnote-ref-1)
2. Error can reach 2 to 3 degrees in the Arctic if not corrected. [↑](#footnote-ref-2)