|  |
| --- |
| IALA Guideline |

1???

Resilient PNT (working draft)

Edition 1.0

Document date

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

|  |  |  |
| --- | --- | --- |
| Date | Page / Section Revised | Requirement for Revision |
| month/year approved by Council | aaaaa | aaaaaa |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1 INTRODUCTION 5

2 Sources of vulnerabitilies 5

2.1 real-life examples of jamming and spoofing 6

2.2 Space weather effects 6

3 Potential impact of the vulnerabilities on AtoN operations and a vessel's ability to navigate safely 9

3.1 Effect on maritime AtoN 9

3.2 Effect on shipborne equipment 9

3.3 Effect on future systems 12

4 Potential Interference/failure Detection 12

4.1 GNSS monitoring and integrity systems 12

4.2 13

4.3 Risk assessment 13

4.4 example risk assessment process 13

4.4.1 Identification of primary assets 13

4.4.2 Dependent systems 13

4.4.3 Classification of risk 13

4.4.4 Area affected 14

4.4.5 Duration of event 14

4.4.6 Probability of event 14

4.4.7 Impact of event 14

4.4.8 Severity of event (based on probability and impact) 14

4.5 Alerting 14

4.6 Potential Alerting options 14

5 Mitigation 14

5.1 fail safe design 15

5.2 use of multiple PNT options 15

5.3 updates to receivers and antennas 15

6 Potential Mitigation options 15

6.1 Platform based sensors 15

6.2 GNSS 16

6.3 Augmentation 18

6.4 Terrestrial systems 18

6.5 vISUAL aTOnS 18

6.6 External support 18

6.7 cyber security 18

6.8 Integrity 19

7 Implementation 19

7.1 User receiver 19

7.2 MSR &PNT Data Processor 19

7.3 Plausibility checks 19

7.4 Timing 20

7.5 Integrity monitoring 20

7.6 Training and monitoring 21

7.7 Scenarios 22

7.8 Scenario 1, vessel A, jamming threat 22

7.9 Scenario x, vessel x, threat x 22

8 DEFINITIONS 22

9 ACRONYMS 22

10 REFERENCES 22

1 Annex 2: Equipment comparisons (review of equipment and it's strengths and weaknesses) 24

List of Tables

Table 1 Example of a table with the significant information in the first column 3

Table 2 Example of a table with the significant information in the first row 3

Table 3 Example of a table with coloured rows 3

Table 4 Example table 3

List of Figures

Figure 1 Example figure caption 3

Figure 2 Another example figure caption 3

List of Equations

Equation 1 Geographical range 3

Equation 2 Theory of Special Relativity 3

# INTRODUCTION

Today’s vessels and many marine aids to navigation (AtoN) rely on GNSS for positioning, navigation and time (PNT). GNSS and other radionavigation and data services are vulnerable to interference and common failure modes.

A number of studies have been conducted into GNSS vulnerabilities (e.g. in the UK [2] & [5], in Europe [3] & [4]). These studies indicate that Global Navigation Satellite Systems (GNSS) have vulnerabilities to intentional and unintentional interference.

This Guideline considers how PNT systems can be made more resilient. 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 guidance in this document can be extended to other radionavigation and communication systems.

It is clear from the studies noted and the IMO e-Navigation requirement for resilience [noted below], that resilient PNT is required today to support the safe navigation of vessels and the correct operation of some marine AtoN. It is anticipated that the growth of autonomy and autonomous vessels will further increase the need for resilience and integrity.

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.”

# Sources of vulnerabitilies

Failure modes are common to all types of electronic navigation system including GNSS. While GNSS services continue to be enhanced and increasingly adopted by users, the fact remains that, contrary to many users’ understanding, GNSS signals have a high degree of vulnerability. The two main characteristics of the GNSS signal that result in vulnerabilities are related to signal strength and frequency bands.

Signal Strength

GNSS is particularly susceptible to accidental or malicious interference due to the extremely low level of the signal at the user receiver. Unintentional sources of interference or interruption in service include ionospheric variability, the effects of solar activity, and also strong signals, harmonics or intermodulation products from powerful transmitters operating in other bands or from sources close to GNSS receivers. Given that GNSS satellites are typically orbiting at about 20,000 kilometres, extremely low power levels of the satellites’ signals are available at the earth’s surface (minimum of -160 dBW for GPS signals or 10-16 W, -154 dBW for Galileo signals). Typically, a one-watt transmitter on a hilltop is sufficient to disrupt every GNSS receiver across the horizon.

Frequency Bands

The current GNSS signal structure that successfully addresses the requirement for systems interoperability has resulted in GNSS vulnerabilities that can be exploited deliberately or result in unintentional disruptions. That is, while there are radio frequency signals intentionally emitted for nefarious intent by purpose-built in-band jammers, there are many other threats to the GNSS signal that are unintentional and originate from sources such as radio, TV, wireless communication, and radars. Thus, the instance of unintentional interference to GNSS signals will undoubtedly continue to rise in an increasingly wireless world.

Intentional causes of interference also include the radiating of deliberate narrow-band or broad-band jamming signals. The Volpe Report[[1]](#footnote-1) also identifies as a hazard “spoofing” in which a false GNSS signal is radiated with the intention of deceiving the user.

In addition to the vulnerability of GNSS, failure of electronic 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. The measures to counteract these problems 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, it is quite common for more than one receiver for that system to be fitted to provide redundancy in the event of equipment failure.

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 [7].

The widespread adoption of GNSS has resulted in a tendency to rely heavily on electronic systems – ‘heads down’ navigation – with a perceived reluctance to use alternative means

## real-life examples of jamming and spoofing

GNSS intentional interference and spoofing activities have multiplied in the last years and the probability of these risks to materialize further has also grown significantly and will continue to grow for some time. The main causes are:

* Aim to protect privacy leading to use of individual unauthorized Personal Privacy Devices (PPDs)
* Availability of COTS technology for jamming / spoofing – Zeng et al. present in a proceedings paper a low cost spoofer based on Raspberry PI which costs less than 250 US dollars
* Training materials and hacking guides for jamming / spoofing freely available on internet with minimum knowledge necessary to implement
* Growing number of events with military character that lead to denial of service
* New features in satellite navigation systems that can improve at least partially the situation (like OS-NMA) will take time to adopt by the maritime environment as backwards compatibility is ensured, therefore no obligations on the user to change receiver.



## 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 system 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 similar to 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 (for phase fluctuations).

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

* At high latitudes the northern lights disrupts 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 [RD.8]) identifies the regions on the Earth where ionospheric scintillations are more/less frequent.



1. Scintillation frequency map.

Additionally, the scintillation activity also depends of 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.

# Potential impact of the vulnerabilities on AtoN operations and a vessel's ability to navigate safely

## Effect on maritime AtoN

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 these AtoNs may rely on GNSS as it can be used to accurately position floating AtoNs and to remotely monitor AtoNs’ positions during their operation.

Some AtoN services are directly relying on GNSS. 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.
* IALA Beacon DGNSS service which monitors and augments 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. The primary timing source for all AIS equipment is GNSS. Loss of GNSS might disturb the sharing of transmission time slots and thus cause problems for the system’s communication capability. Floating AIS AtoNs may also broadcast incorrect position information potentially resulting in conflicts with vessels’ radar information.

During a GNSS interference event, the DGNSS integrity monitoring system might set the station health indicator to unhealthy or unmonitored. When set unhealthy, corrections might not be available at all. In the case of unmonitored, faulty DGPS corrections might be broadcasted over the coverage area of the affected DGNSS site.

Loss of GNSS would also affect VTS operations. 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 vessel reports. 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.

## Effect on shipborne equipment

Modern bridge systems are interconnected and strongly dependent on GNSS. Integrated bridge systems assume vessels’ GNSS receivers are trustworthy when reporting a position fix from ambient GNSS signals. As such, GNSS is currently the main source of PNT information for maritime navigation and has essentially replaced traditional means of navigation.

If GNSS information is unavailable or falsified, vessels position, speed over ground and course over ground information could be missing or incorrect. This could lead vessels equipped with integrated bridge systems to undertake inadequate course and heading changes. The table below describes the extensive use of GNSS in many shipborne equipment and the impact that the loss of GNSS would have on each of the listed systems.



1. Use of electronic navigation in today's vessel system with the possible effects and consequences of loss of GNSS

| Vessel system | Effect of GNSS loss | Impact of GNSS loss |
| --- | --- | --- |
| GNSS positioning (incl. augmentation) | Loss of and DGPS input data for position fixing  Loss of the External Electronic Position Fixing System (EPFS) message |  |
| ECDIS & ECS | Loss of depth below keel info  Loss of speed and course over ground  Loss of heading and active waypoint lat-lon coord.  Loss of vessel’s position on the map |  |
| AIS | Display alarm status  Loss of vessel’ own’s position info for AIS transmission |  |
| Gyrocompass | Standby mode message  Heading maintained  Loss of position correction to derive true north. Error can reach 2 to 3 degrees in the Arctic if not corrected. |  |
| RADAR | Standby mode message  Loss of latitude & longitude and speed info  Loss of ground stabilisation info  Loss of water depth profile history  False Speed and Course over ground values  Range and bearing were relative to center of video circle instead of own’s ship’s position  Switch to Dead Reckoning mode |  |
| Digital Selective Calling (VHF/HF) | Loss of position and UTC timestamp information |  |
| Voyage Data Recorder | Loss of UTC timestamp information |  |
| GMDSS | Loss of satellite communication synchronization (SAT-C)  Loss of automatic update capabilities from last known position. Updated positions needed to be manually entered regularly. |  |
| Satellite Broadband Antenna | Loss of satellite lock |  |

When GNSS is disrupted or unavailable, some onboard vessel instruments respond almost instantly with sound alarms and screen messages indicating the loss of the GNSS feed. The high degree of interconnection among the different navigation systems onboard a vessel increases its vulnerability to GNSS outages and compromises bridge navigation system, GNSS-based timing systems and communication equipment. It should be noted that this would impact not only the means of navigation but also PNT information exchange between ships as with ship to shore PNT data communications (e.g. AIS reporting).

# Potential Interference/failure Detection

## GNSS monitoring and integrity systems

<include monitoring and integrity solutions, use of existing receivers to detect amonalies etc).

Services providers should consider the use of integrity information when conducting their risk assessment. Integrity information can be provided through different means.

A GNSS failure may be of such a nature that it is instantly perceived by the navigator. However, onboard systems like an Integrated Navigation System or using RAIM, GBAS, or SBAS can provide integrity warnings.

Service providers who operate IALA-DGPS infrastructure already provide integrity to the mariner. IALA and other relevant organizations have maintained appropriate recommendations for the system [14].

## Risk assessment

Understanding each system and looking deep into where time comes from.

## example risk assessment process

Need to check whether there is an IMO or BIMCO assessments available already?

### Identification of primary assets

* Capability to compute the vessel's position
* Capability to communicate vessel's position
* capability to know other vessels' positions
* capability to navigate with good weather conditions (good vis)
* capability to navigate with bad weather conditions (poor vis)
* 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)

### Dependent systems

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 1. 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.

### Classification of risk

* GNSS outages (planned or unplanned)
* DGNSS outages (planned or unplanned)
* SBAS outages (planned or unplanned)
* Interferences (unintentional)
* Attacks (spoofing, jamming)
* others

### Area affected

Phase of navigation: Ocean, Coastal, Port (or other restricted waters)

Local (<50nm), Regional (>50nm), Global

### Duration of event

Order of magnitude: Minutes, Hours, Days, Months

### Probability of event

* Very low (e.g. none in 20 years)
* Low
* Moderate
* High
* Very High (e.g. everyday)

### Impact of event

* Very low: minor delay
* Low: Delay without economic impact
* Moderate: Important delay with economic impact
* High: Accident without deaths
* Very high: Accident with deaths

### Severity of event (based on probability and impact)

## Alerting

* Raising awareness of the issues in general
* active monitoring and alarms
* Recognising interference/jamming/spoofing and reporting of incidents
* e-Navigation communications
* NtoM and Notices to shipping

## Potential Alerting options

* Training
* GNSS interference monitoring systems
* Dedicated services (e.g. SBAS maritime service that report system outages)
* Reporting lines
* Other PNT systems

# Mitigation

This subjective risk analysis helps to identify the threats that should be addressed by the user, particularly those with high probability, high consequences and low mitigation cost. The use of GNSS receiver equipment compliant with the latest performance standards will significantly reduce susceptibility to interference.

Awareness of the problem and changes in the design of future systems such as greater radiated power, increased receiver sophistication and added operating frequencies can serve to mitigate the impact of some of the threats to some degree. However, system vulnerability, particularly to deliberate attack, cannot be fully eliminated. This message was clear and repeated several times in the Volpe Report. Modification of the present systems can reduce the effect of natural and inadvertent sources of noise and interference. Calculated attempts to jam or otherwise deny the user community the positioning and timing services of GNSS will be far more difficult to anticipate and combat. Therefore maintenance and development of adequate alternative systems is essential.

Through using an integrated PNT approach as part of the INS, it may be possible to indicate to the mariner the level of performance available (i.e. accuracy, integrity, continuity etc). Should the primary and redundant means of PNT become unavailable, the system could then indicate whether the primary or back-up requirements can be achieved, or not.

## fail safe design

## use of multiple PNT options

## updates to receivers and antennas

* hardening options
* plausibility checks

# Potential Mitigation options

## Platform based sensors

The concurrent use or comparison with another positioning or timing system can also help detect spoofing events. To illustrate this, validation with another source of actual navigation data can be achieved using an Inertial Measurement Unit (IMU) sensor. For timing consistency, a Chip Scale Atomic Clock (CSAC) can be used. A consistency check can be accomplished using external systems such as additional sensors or additional signals.

* Inertial navigation system (INS)

INS sensors are often used in dead reckoning applications where the signal may be lost momentarily. Dead reckoning navigation after a GNSS signal loss would require a known starting point, sensors for velocity (accelerometer), orientation (gyroscope, compass) and an estimation of the position error bound.

There are two families of inertial sensors: one based on **cold atom interferometry (quantum sensor)** and the second based on a **Micro-Electro-Mechanical Systems (MEMS)**.

* Depth sounder (Bathymetric Navigation)

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

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 (for example, 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.

* CSAC – Chip Scale Atomic Clocks

A receiver fitted with an additional onboard source of accurate time, such as a chip-scale atomic clock (CSAC) is capable of holding accurate time at sub-microseconds for hours after losing access to GNSS. The CSAC can achieve a better short-term stability than Rb, which results in a range error of 0.075 metres (a significant improvement to the TCXO range error of 0.3 metres). CSAC has other benefits such as reduced power consumption (less than a tenth of Rb oscillators) and is housed in a package with a footprint smaller than the currently available miniature Rb oscillators. Preliminary results related to short time periods confirm that there is a benefit related to the GNSS position solution, in the event of the loss of GNSS signals, by using CSAC instead of TCXO.

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.

* gyro compass
* ePelorus
* Radar

## GNSS

* Multiple constellations

With four GNSS constellations (GPS, Glonass, Galileo, BeiDou), becoming fully operational post 2020, and as more frequencies become available, multi GNSS 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 other 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 which is of critical importance for maritime navigation.

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 than a single one. 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.

* Multiple frequencies

Several GNSS signals may be allocated to different frequencies allowing 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.

**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.

As the GPS L5 signal is design to support safety-of-life applications, dual frequency receivers are likely to utilize this signal in addition to the legacy L1 signal that is currently widely employed for maritime navigation. The interoperable GPS L5 frequency (1176 MHz) is also shared with the GLONASS L5, the Galileo E5a and the BeiDou B2a signals. Development of the L5/E5a/B2a signal transmissions as of March 2020 is summarised below:

Table 23 – 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 |

* Integrity options
  + System level and user level

## Augmentation

* radiobeacon DGNSS
* Satellite Based Augmentation Systems (SBAS) - can be considered as a backup solution for DGNSS or as a complementary means to provide augmentation. Mariners can take advantage of the use of SBAS, which provide enhanced performance over the capabilities of GNSS and Regional Navigation Satellite System (RNSS) constellations. SBAS improves the accuracy and reliability of GNSS by correcting signal measurement errors and by providing information about the accuracy, integrity and availability of GNSS signals.

## to mariners. Recent navigation receivers installed on ships also generally utilize SBAS. Terrestrial systems

* eLoran
* R-Mode
* Locata
* STL
* radar absolute positioning

## vISUAL aTOnS

## External support

* VTS
* Sea Traffic Management (?)

## cyber security

* Authentication

## Integrity

* Consistency checks (multi-constellation, multiple systems, etc)
* External support information (VTS, Aton Information, etc)
* Autonomous PNT systems (Inertial, Compass, etc)
* Integrity Algorithms
* SBAS
* RAIM
* Single constellation RAIM
* M-RAIM
* etc.

(This is probably all now covered above somewhere)

# Implementation

## User receiver

It is noted that appropriate backup system user equipment would probably exist in a multi-modal form with a common output terminal (an integrated receiver). Such equipment has advantages with respect to monitoring the primary navigation system for interference, and using the last reliable primary data received as an initial position source for the backup receiver.

As with existing primary navigation systems, it is considered essential that the user is notified of the status of both primary and backup navigation systems by means of obvious visual and audio alarms and messages.

The output of a backup navigation system should be in a recognised electronic format (i.e. IEC 61162) for input into electronic chart displays and GMDSS.

## MSR &PNT Data Processor

* MSN: IMO Resolution RESOLUTION MSC.401(95) on PERFORMANCE STANDARDS FOR MULTI-SYSTEM SHIPBORNE RADIONAVIGATION RECEIVERS
* PNT-DP: IMO MSC.1/Circ.1575 on GUIDELINES FOR SHIPBORNE POSITION, NAVIGATION AND TIMING (PNT) DATA PROCESSING

## Plausibility checks

Receivers could be designed to take into account the general dynamics of the vessel they are fitted to as a user configured entry. Receiver equipment and other relevant PNT data sources could be designed to take into account and compensate for the general dynamics of the vessel they are fitted to as a user configured entry. This is to mitigate the effect of the wind, swell and other sea states on the PNT data received or derived. On top of that it is recommended that the individual 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; and
* Checks that operative modes or states are consistent when they are reported by multiple sentences from a single sensor/source or function, GGA and VTG sentences reporting equal operative states of a single GNSS, for instance.

NOTE: Plausible range in terms of heading, for example, is 0 to 360 degrees.

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

## Timing

Timing is an information derived together with position and navigation information from a global or regional positioning system that can provide absolute position and time like GNSS, eLoran and R-Mode. On the ship it will be an output of the single system navigation receiver, the MSR or the PNT-DP processing unit. In case no navigation system for absolute positioning and timing is available build-in hold-over capabilities of the receivers or PNT-DP, most often a type of crystal oscillator, can provide accurate time information for a limited time. Atomic clocks can be used to increase the availability of accurate time and support plausibility checks and integrity monitoring.

## Integrity monitoring

The integrity of data should be monitored and verified automatically by the PNT data processing unit or integrated navigation display before being used or displayed onboard the vessels. The integrity of information should be verified by comparison of the data derived independently from at least two sensors and/or data sources, if available. The system should support manual or automatic means to select the most accurate method of integrity monitoring from available sensors and/or data sources. An indication of the sensors and data sources of the data selected for integrity monitoring should be provided. The system should provide a warning, if integrity verification is not possible or failed.

The results of integrity monitoring should be one of the followings:

* Passed: integrity verification passed;
* Failed: integrity verification not passed; or
* Doubtful: integrity verification not possible.

The following methods are examples of integrity monitoring that can be conducted onboard, but there may be other appropriate methods as defined by manufacturers, including incorporation of third sensor or data source or reference data for more thorough result. The maximum accepted threshold discrepancy values used for integrity monitoring can be defined by manufacturers for each type of PNT data.

Position

* Comparison between two EPFS; or
* Comparison between EPFS and dead reckoning using ship’s heading and SDME in the case where only a single EPFS is available for integrity monitoring.

Heading

* Comparison between two heading sensors.

Speed through water

* Comparison between two STW sensors; or

In the case where a single STW sensor is only available for integrity monitoring:

* Comparison with a SOG from SDME; or
* Comparison with a SOG from EPFS.

Speed and course over ground

* Comparison between two longitudinal/transversal ground speeds from SDME together with a heading; or

In the case where a single SOG/COG sensor is only available for integrity monitoring:

* Comparison with a STW sensor together with a heading sensor; or
* Comparison with a SOG and COG from EPFS

Depth

* Comparison between two depth sensors; or
* Comparison between depth data from depth sensor and the data from the latest available ENC in the case where a single depth sensor is only available for integrity monitoring.

Time

* Comparison between two EPFS; or
* Comparison with internal clock in the case where a single data source of time is only available for integrity monitoring.

Data which fails the integrity monitoring or data where integrity monitoring is not possible should be clearly indicated and should not be used for automatic control systems and functions.

## Training and monitoring

* Training of personal

The IALA World-Wide Academy (WWA) hosted a training course on an Introduction to e-Navigation and GNSS on May 2017 at the IALA Headquarters mainly dedicated to aids to navigation manager to gain an understanding on the matter. The modules on PNT and GNSS were addressed focusing on the idea that an uninterrupted determination of such service is essential to e-Navigation. The following topics were included:

Module on PNT:

* **Need for Resilient PNT** 
  + e-Navigation
  + ECDIS and other dependent systems
  + IMO WWRNS Requirements
  + GNSS
  + Characteristics & systems
  + Alternative PNT systems and augmentation for GNSS
* **Resilient PNT Plans**
  + Timeline for Resilient PNT
  + e-Navigation solutions
  + IALA WWRNP

Module on GNSS:

* + GNSS Introduction
  + GNSS architecture
  + GNSS systems (core constellation)
  + Augmentation systems
  + GNSS applications
  + GNSS evolution/Future scenarios:
  + GNSS Vulnerabilities

A small participation attended the course but the need to build awareness and effective services and means supporting the Resilient PNT system of systems deployments remains a priority for the competent authorities. The WWA is currently updating the technical content and reviewing the course as the progress on this matter have increased exponentially from 2017. The WWA is seeking at this stage for inputs and ideas to develop and enlarge the content on a more operational and technical approach.

* Monitoring of resilient PNT

## Scenarios

## Scenario 1, vessel A, jamming threat

## Scenario x, vessel x, threat x

# DEFINITIONS

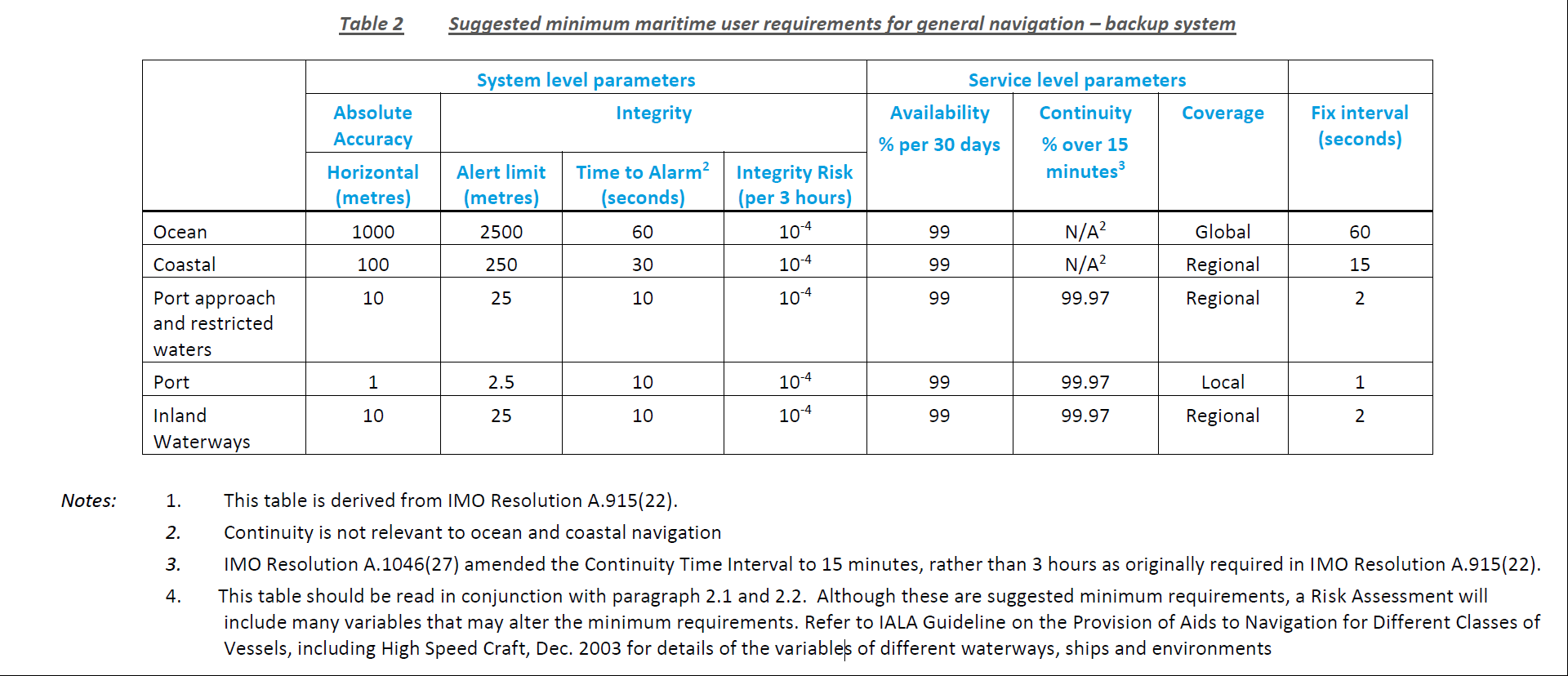
*Suggested text:* The definitions of terms used in this IALA Guideline can be found in the International Dictionary of Marine Aids to Navigation (IALA Dictionary) at <http://www.iala-aism.org/wiki/dictionary> and were checked as correct at the time of going to print. Where conflict arises, the IALA Dictionary should be considered as the authoritative source of definitions used in IALA documents.

# ACRONYMS

IMO International Maritime Organization (Acronym style)

# REFERENCES

1. Abcd
2. Efgh
4. SUGGESTED MINIMUM MARITIME USER REQUIREMENTS FOR GENERAL NAVIGATION – BACKUP SYSTEM



1. Annex 2: Equipment comparisons (review of equipment and it's strengths and weaknesses)

re GMV e-mail. A chance to list equipment and review how each system works, which threats they are able to detect and those they can't etc.

1. PERMITTED COLOUR PALETTE

The IALA colour palette is divided in 3 palettes of different level of hierarchy that has to be respected.

Corporate colours (Not shown)

IALA’s corporate colour palette is directly inspired from the colours in our logotype:

* dark blue
* white
* yellow
* gradient blue

Primary & secondary colours

The primary colours are to be applied in complement with the corporate colours.

This second level of colours gives rhythm and helps to segment our publications.

The secondary colours are used to highlight information, titles in a minor proportion only.

These colours can’t be replaced by other tints.

**PANTONE PROCESS CYAN C CMYK :** C 100

**RGB :** R 0 - G 159 - B 223

**CMYK : 50 % OF THE TONE RGB :** R 131 - G 208 - B 245

**CMYK : 50 % OF THE TONE RGB :** R 148 - G 217 - B 213

**CMYK : 50 % OF THE TONE RGB :** R171 - G 219 - B 233

**CMYK : 50 % OF THE TONE RGB :** R 178 - G 193 - B 237

**PANTONE 326C CMYK :** C 81 - Y 39

**RGB :** R 0 - G 175 - B 170

**PANTONE 7703 C**

**CMYK :** C 79 - M 2 - Y 10 - K 11

**RGB :** R 0 - G 181 - B 208

**PANTONE 660 C CMYK :** C 88 - M 50

**RGB :** R 64 - G 126 - B 201

**CMYK : 20 % OF THE TONE RGB :** R 212 - G 237 - B 252

**CMYK : 20 % OF THE TONE RGB :** R 213 - G 240 - B 237

**CMYK : 20 % OF THE TONE RGB :** R 216 - G238 - B 245

**CMYK : 20 % OF THE TONE RGB :** R 218 - G 223 - B 246

**PANTONE 258 C CMYK :** C 51 - M 79

**RGB :** R 153 - G 80 - B 159

**CMYK : 50 % OF THE TONE RGB :** R 201 - G 169 - B 208

**CMYK : 50 % OF THE TONE RGB :** R 183 - G214 - B 155

**CMYK : 50 % OF THE TONE RGB :** R 246 - G 174- B 135

**CMYK : 50 % OF THE TONE RGB :** R 157 - G 157 - B 156

**PANTONE 739 C**

**CMYK :** C 78- Y 95- K 5

**RGB :** R82 - G 174 - B 50

**PANTONE 2347 C**

**CMYK :**M 88 - Y 100

**RGB :** R 230 - G 56 - B 17

**PANTONE COOL GRAY 11 C CMYK :** K 100

**RGB :** R 87 - G 87 - B 86

**CMYK : 20 % OF THE TONE RGB :** R 232 - G 221 - B 288

**CMYK : 20 % OF THE TONE RGB :** R226 - G 238 - B 217

**CMYK : 20 % OF THE TONE RGB :** R 253 - G 224- B 208

**CMYK : 20 % OF THE TONE RGB :** R218 - G 218 - B 218

**CMYK : 10 % OF THE TONE RGB :** R 237 - G 237 - B 237

Guideline

Recommendation

Model Course

PRIMARY COLOURS

SECONDARY COLOURS

1. 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] [↑](#footnote-ref-1)