IALA RECOMMENDATION

R0129 (R-129)

GNSS VULNERABILITY AND MITIGATION MEASURES

Edition 3.1

December 2012

urn:mrn:iala:pub:r0129

10, rue des Gaudines – 78100 Saint Germain en Laye, France
Tél. +33 (0)1 34 51 70 01 – Fax +33 (0)1 34 51 82 05 – contact@iala-aism.org
www.iala-aism.org
International Association of Marine Aids to Navigation and Lighthouse Authorities
Association Internationale de Signalisation Maritime

DOCUMENT HISTORY

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
December 2004	1st issue	
December 2008	Ed2. Whole document	Introduction of e-Navigation and eLoran
September 2012	Ed3. Whole document	Updated to reflect changes in GNSS since the original draft.
September 2020	Ed 3.1 Editorial Corrections	

THE IALA COUNCIL

NOTING the function of IALA with respect to Safety of Navigation, the efficiency of maritime transport and the protection of the environment;

NOTING ALSO that the IMO SOLAS Convention obliges administrations to provide such aids to navigation as the level of risk requires and the density of traffic justifies, but does not specify the type of systems to be provided;

NOTING FURTHER IMO resolutions A.915(22) on Maritime Policy for the Future Global Navigation Satellite System (GNSS), and A.953(23) on World Wide Radionavigation System;

RECOGNISING the increasing dependence of all classes of maritime users on GNSS services, and the vulnerability of such services to both intentional and accidental interference;

RECOGNISING ALSO that GNSS is a key element within e-Navigation;

RECOGNISING FURTHER the existence of conventional Aids to Navigation and VTS as alternative ground-based systems, available to all classes of maritime users;

HAVING CONSIDERED the proposals made as a result of the study contained in the Annex to this recommendation;

RECOMMENDS that:

1 National Members and other appropriate Authorities take account of the information in the annex and the other studies carried out on the options for alternative systems.

2 National Members and other appropriate Authorities conduct risk assessments, in terms of the various stages of a voyage relevant to their geographic areas of interest.

3 National Members and other appropriate Authorities maintain and improve liaison and partnerships between providers of GNSS.

4 National Members and other appropriate Authorities monitor parallel activities on vulnerability mitigation by other bodies and other modes of transport.

5 National Members and other appropriate Authorities encourage the transfer of mitigation technology from the military for civil use.

6 In co-operation with industry, National Members and other appropriate Authorities support the development of improved receiver performance standards.

7 National Members and other appropriate Authorities encourage the use of GNSS receiver equipment compliant with the latest performance standards.

8 National Members and other appropriate Authorities raise awareness among users about the vulnerability of GNSS and the need to maintain skills in the use of conventional aids.

9 National Members and other appropriate Authorities maintain and develop backup and contingency aids to navigation, which may include radio aids to navigation and conventional aids to navigation, appropriate to the identified level of risk.

ANNEX

TO

IALA RECOMMENDATION R0129 (R-129)

ON

GNSS VULNERABILITY AND MITIGATION MEASURES

ANNEX CONTENTS

List of Tables

1 INTRODUCTION

In 2001, the U.S. Department of Transportation Volpe Center carried out a study of the vulnerability to intentional and unintentional interference of the US transportation infrastructure relying on Global Positioning System (GPS) signals [1]. A similar study has been carried out for the Radiocommunications Agency in the UK [2]. Studies have also been carried out in Europe in preparation for the Galileo project [3] & [4]. A recent study by the Royal Academy of Engineering has investigated the level of reliance on and the vulnerabilities of GNSS [5]. These studies indicate that Global Navigation Satellite Systems (GNSS) have vulnerabilities to intentional and unintentional interference.

1.1 BACKGROUND

The IMO Strategy for e-Navigation contains a high level user need for data and system integrity that 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."*

In addressing the issue of Position Fixing, it can be defined as accurate and reliable electronic position, navigation and timing signals, with 'fail-safe' performance (probably provided through multiple redundancy, e.g. GNSS, differential transmitters, eLoran and defaulting receivers or onboard inertial navigation devices).

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 need for measures to counteract vulnerability has become particularly important with the phasing out of other systems and should be taken into account in the formulation of radio-navigation plans. In the aviation context, [6] indicates that the problem of GNSS vulnerability is manageable by the retention of existing terrestrial systems (VOR/DME, NDBs) as backups. Similar consideration is given here to the maritime environment.

1.2 SCOPE

This document considers all types of GNSS vulnerability within the maritime field, and the mitigation measures that may be used to overcome them.

The effect on marine navigation of interruptions to GNSS will be significant. Where natural events, such as space weather, affect GNSS signal reception, it is likely that the effects will be observed over large areas and during any phase of navigation. Man-made interference is most likely to arise within coastal waters, since the sources of man-made interference are likely to be land-based and will be restricted to line-of-sight. However, the possibility of deliberate shipborne or airborne jamming cannot be ruled out.

It is accepted as good practice that all available sources of positioning information should normally be used.

2 DEFINITIONS & ACRONYMS

The following additional acronyms are used within this document:

ASF	Additional Secondary Factors
dBW	decibels relative to One (1) Watt
DME	Distance Measuring Equipment
ECDIS	Electronic Chart Display
EGNOS	European Geostationary Navigation Overlay System
ENC	Electronic Navigational Chart
GLONASS	Global Navigation Satellite System

GMDSS	Global Maritime Distress and Safety System
IEC	International Electro-technical Commission
IMO	International Maritime Organization
LBS	Location Based Services
Loran	Long Range Navigation
NDB	(Aeronautical) Non-Directional Beacon
PNT	Position, Navigation & Timing
SOLAS	Safety of Life at Sea (Convention)
UMTS	Universal Mobile Telecommunications System
VOR	VHF Omnidirectional Ranging
WAAS	Wide Area Augmentation System

3 SOURCES OF VULNERABILITY

Some failure modes are common to all types of electronic navigation system. The system itself can fail, for example because of deliberate or accidental damage to the ground infrastructure. Given the military nature of present GNSS – GPS & GLONASS, it may be assumed that security levels are high and that standby equipment is provided. Experience with GPS bears this out and system failure can be assumed to be a very rare event. Security measures for Galileo are comparable to those for GPS, with the exception that the satellites are not hardened to resist electro-magnetic pulses from nuclear explosions. Failure of individual GPS satellites is not unusual, although the Mean-Time-To-Repair is less than 48 hours.

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

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 for position verification, as recommended by the International Maritime Organization (IMO).

3.1 INTERFERENCE SOURCES

Unintentional interference may come from natural or man-made sources.

Ionospheric variability and the effects of solar activity on radionavigation systems have been the subject of research for many years. Reference [8] reports the effect of scintillation of GPS signals. The effects of ionospheric variability are to increase errors of position fixes and these may exceed the limits laid down in the relevant IMO Resolution [9] and may even lead to failure of the receiver to lock onto satellites’ signals.

The Galileo (and future GPS) Integrity System should detect large ionospheric disturbance effects and provide warnings.

Sources of shore-based unintentional man-made interference may include television broadcasts, microwave communications - both fixed links and satellite uplinks – and VTS radars. Interference from television broadcasts and microwave fixed links can be especially serious as it can affect all vessels within a significant area or on a particular waterway.

Interference from onboard equipment such as satellite uplinks and radars can be minimised by correct installation practices. However, such interference may originate on board other vessels in the vicinity. In that case, it becomes difficult or impossible to do anything about it. This could be a very serious problem in harbours and harbour approaches.

INMARSAT frequencies are close to those of GNSS and GNSS antenna installations should take account of the variation of signal elevation with latitude, where steerable dish antennas are used.

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 [10].

Electromagnetic Compatibility plans are an IMO requirement for all systems on SOLAS ships, but the thoroughness with which they are applied may vary because they can be costly to implement. Measurement and analysis of onboard interference sources is a specialised subject about which there is a shortage of knowledge and training. Space limitations on masts often make it difficult to achieve the ideal antenna installation for any system (not just GNSS).

3.2 JAMMING & SPOOFING

Jamming of GNSS signals can be achieved quite easily using relatively low-cost equipment. This is because of the extremely low power levels of the signals at the earth's surface (minimum -160 dBW for GPS, -154 dBW for Galileo). Spread spectrum signals such as those of GPS are less vulnerable to a single frequency jammer than to a broadband one. Since all the GPS satellites transmit on one frequency, a single jammer normally takes out every satellite. Frequency division systems such as GLONASS could, in theory, still give a service when a narrow band jammer takes out one or two satellites' signals. On the other hand, it is easy to design a jammer that transmits on several frequencies simultaneously, considering the low power levels required for efficient jamming. Galileo will have the advantage of time for the development of counter-measures and a security board will oversee such matters as interruption in time of war.

Spoofing is more difficult to achieve, as it is necessary to simulate the signals in order to make the receiver lock on to the false signals. However, GPS signal simulators are readily available items of industry test equipment. Furthermore, the consequences of spoofing are far more serious than those of jamming. If the false signals are indistinguishable from the real ones and give a position close enough to be believable, then the user may not be aware of the deception and could be led into danger. An authentication service, such as that proposed for Galileo, could be an effective counter measure to spoofing.

Given the relative difficulties of jamming and spoofing, jamming is more likely to be encountered. There have been several recorded incidents of deliberate jamming by military authorities. The maritime world is highly vulnerable to jamming effects on navigation, AIS and GMDSS equipment. AtoN provision can be affected, with regard to DGNSS, VTS and GNSS-synchronised lights [Ref. [11]]. Additionally, the implementation of e-Navigation is expected to result in an increased reliance on timing-dependent communications systems, which may utilise GNSS.

Malicious jamming of GNSS may be thought of as analogous to attacking computers with viruses, and likely to appeal to the same kinds of perpetrator. Many Internet sites give details of how to achieve it. The sort of area that could be affected with a simple jammer would not be just a single port approach. GNSS service could be denied over the whole of an area of high traffic density such as the Straits of Dover or the Straits of Malacca.

Jamming countermeasures are already available in the form of directional antennas and tuneable filters on military receivers. Jamming will become more difficult as more frequencies become available, but it will still

be possible. The slightly higher power levels of Galileo and GPS III will reduce vulnerability and the combination of multiple GNSS will be better than one system alone. However, susceptibility to jamming cannot be eliminated.

An important consideration is the duration of the jamming event. The consequences of brief interruptions are clearly less serious than a prolonged denial of service. Measures to deal with jamming would also depend on its duration. Providing technical personnel to track down jammers would be justified and effective if long periods of jamming were to be expected, but could be ineffective against "hit and run" jamming. In fact, many countries already have teams and resources allocated to deal with jamming and interference. It is important that they are made aware of the threat to safety of life services posed by the possible interruption of GNSS.

3.3 RISK ANALYSIS

Analysing the risk of losing GNSS is difficult. The user may note that the signal has been lost for a period and has then returned, but has no way of knowing the cause, be it external or onboard interference, accidental or intentional.

Consequences to navigation applications may range from complete loss of signal, false position information or intermittent loss to degradation of accuracy. Consequences to timing applications may include failure due to loss of synchronisation.

Table 1 gives subjective assessments of the different risks in terms of their perceived probability of occurrence, consequences and the difficulty and cost of mitigation. It is emphasised that these are subjective judgements, based on expert opinions. A quantitative risk analysis should be carried out if possible.

Table 1 Risk Assessments

Event	Probability of Occurrence	Consequences	Mitigation difficulty/cost
GNSS Service failure	L	H	H
Power supply failure	M	H	L
Receiver/antenna failure	M	H	L
Onboard interference	M	M	L
External interference	L	H	M
Ionospheric	L	M	M
Jamming	L	H	M
Spoofing	L	H*	H
Radar burn-out	L	H	L

H = High. High probability means likely to be encountered more than once a year. High consequence means complete loss of use of the system. High difficulty or cost of mitigation means it is unlikely to be achieved.

M = Medium. Medium probability means likely to be encountered less than once a year. Medium consequence means system still usable, but degraded. Medium difficulty or cost means achievable at significant cost.

L = Low. Low probability means unlikely to be encountered. Low difficulty or cost means mitigation should be achieved.

* notes the more serious implications of spoofing (see section 3.2).

3.4 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.

3.5 ALTERNATIVE SYSTEMS

Alternative means of navigation may be provided at various levels; fully redundant, backup and contingency[1].

- 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.

3.5.1 Redundant System

Fully redundant systems should provide equivalent performance levels in terms of positioning and timing accuracy, integrity, availability and continuity. GLONASS represents a potential redundant system for GPS, with additional systems such as BEIDOU and Galileo due to become fully operational by 2020.

It must also be noted that such similar systems may also have common failure modes. For example a jammer or interference source could deny multiple GNSS services, since it is very likely that the two systems will use the same frequency bands. It is also expected that most receivers will employ both systems; thus an attack on one may affect both. Counter-measures against jamming and interference are being developed and are likely to be quite effective by the time Galileo and later generations of GPS become operational.

3.5.2 Backup Systems

Backup systems may include existing or planned terrestrial systems such as:

- Loran C;
- Enhanced Loran (eLoran);
- Radar and radar aids to navigation;

1 As defined in various studies conducted by Booz-Allen & Hamilton on behalf of the US Federal Aviation Administration.

- Cellular telephone based systems;
- Ranging from DGNSS/AIS (R-Mode)[2].

Loran is the only existing candidate as a terrestrial radionavigation alternative and provides a position sentence usable with electronic charting and other onboard systems. Loran provides independent position, navigation and timing with dissimilar failure modes to GNSS, however the coverage is limited. For example in European waters it is restricted at present to the north-western part, while in North America the decision was made to switch the service off in 2010. Loran receivers are not a required fit and very few vessels outside North American waters carry them.

eLoran has demonstrated comparable accuracy to GNSS [12]. In order to make eLoran into an effective redundant or backup system, receivers would need to be carried and there is little motivation for voluntary fitting of backup receiving equipment as long as GNSS continues to work well.

Although receivers for Loran are not a specific carriage requirement, they would be covered by the SOLAS Chapter V requirement for an Electronic Position Fixing System, suitable for the whole voyage, in the case of regional traffic. The current IEC test specification for the type approval of Loran receivers is based on out of date technology and may need to be revised.

Loran also has vulnerabilities to failure of onboard equipment or power supplies, damage to the ground infrastructure, loss of synchronisation due to interruption of communication systems and interference from ionospheric effects or power lines, which can carry both low frequency alternating current and higher frequency data signals.

Radar can be used for position-fixing, but it does not generally provide a compatible input to an electronic charting system; therefore different procedures are necessary for its use. However, radar is a required fit on SOLAS vessels and radar map-matching (echo referencing) techniques are well developed and used in waters such as the archipelagos between Sweden and Finland. The most serious limitation of radar as a backup is in areas with low-lying, featureless coastlines, for example in Europe those of Northern France, Belgium and the Netherlands or the East coast of England. In order to make radar a universal backup, such areas would need to be marked with sufficient radar aids to navigation.

This would not provide the same level of positioning service as Loran, nor would it give an alternative timing reference. However, this option could justify further investigation in regions where Loran is not a realistic option. Radar and radar beacons also have vulnerabilities to failure of equipment or power supplies, multipath, rain and sea clutter and masking effects.

Another possible backup in the future may be positioning using the Universal Mobile Telecommunications System (UMTS). This is the third generation cellular system and the first networks became operational in 2002. One of the main features of 3G cellular will be Location Based Services (LBS) in which location of the user will be achieved either by GNSS (vulnerable to the same failure modes as the ship's GNSS receiver) or by systems that employ the cellular base-stations themselves. Such systems include cell identification (cell ID) and tri-lateration of signals at multiple base-stations. Deployment of such networks is likely to start with the more densely populated areas and coverage of coastlines is unlikely to be a priority; however, it may be possible to use multiple base-station techniques as a backup in some areas, such as estuaries. The use of these systems as a viable alternative has still to be proven; accuracy would not be as high as with GNSS and it is unlikely that such equipment would ever be type-approved for use on SOLAS vessels. These systems are likely to depend increasingly on GNSS for their timing and synchronisation, therefore they could be affected by any loss of GNSS. Cellular, radio and television signals could also be used within a Signals Of Opportunity type approach, where signals provided for alternative uses are used for ranging. While there are advantages of this approach, it is unlikely to achieve the level of service integrity required for navigation applications as the signals are provided for a different purpose and therefore may be altered or cease without notice.

2 During the e-Navigation test bed project ACCSEAS, tests concerning the R-Mode (DGPS/AIS) as an alternative back-up system will be carried out in the North Sea Region. The results of those tests can be expected in early 2015.

Another possible future backup is the use of ranging signals from existing DGNSS or AIS infrastructure (R-Mode) [13]. Both systems have widespread distribution and maritime standards already exist for onboard equipment. The new functionality of R-Mode is the provision of timing information from shore to ship. The shipboard radio receiver may then calculate a distance (range) to the transmitter. Using several such calculations from a number of different transmissions, the shipboard equipment is able to calculate the ship position. Coverage, geometry and interference questions would need to be investigated.

3.5.3 Contingency Systems

The most obvious contingency system, allowing safe completion of a manoeuvre is the system of lights and buoys already provided in most parts of the world. Visual aids serve two specific functions, hazard-warning and position-fixing. They are not necessarily deployed in such a way as to allow for continuous navigation, except in the case of channel markers. Accuracy levels depend on the relative position of the visual aids and the scope of their movement in the case of floating marks, but accuracy could be expected to be considerably below that provided by GNSS. Visual (and radar) Aids to Navigation provide an essential alternative to GNSS although it is accepted that they are now a secondary means of relative position verification. They also form an essential safety function in physically marking hazards and in allowing the mariner to develop critical spatial and environmental awareness. These functions need to be borne in mind when users and service providers are assessing the continuing need for visual aids. It is considered essential that skills in the use of conventional aids to navigation should be maintained. Lights and buoys have limited visibility and achieving high levels of reliability represents a significant maintenance burden. In poor visibility and in the absence of Loran or radar, another system would be needed.

A future contingency system could be the inertial navigation system. These installations have previously been too expensive for non-military vessels, but lower cost devices with acceptable short-term performance are now becoming available. Integrated with a GNSS receiver, an inertial navigation system could provide continuity of service to electronic charts and autopilots, but only for a period limited by the rate of drift. It would be very important that the user was made aware of the change of position input from GNSS to an inertial navigation system and the consequent degradation with time in the confidence to be placed in positional accuracy.

Dead-reckoning is a contingency method of navigation. It relies on the use of onboard instruments, principally the compass and the log, for estimating speed and course and hence position. Accuracy depends on the quality of the last fix and degrades with time at a rate depending on the accuracy of the equipment and the sea and weather conditions.

Other onboard instruments can contribute to position-fixing, in particular the depth sounder, which is a mandatory fit on SOLAS vessels and very widely carried by non-SOLAS craft.

Use of manual intervention would require adequate warnings and the necessary skills and experience. These skills should include training and experience of overriding the dependency of the primary system from other bridge equipment.

Where electronic systems are used for contingency, the performance requirements will likely fall between the primary and back up requirements, however in the case of inertial systems or dead reckoning, they may only be reliable for a short period of time due to drift.

The duration that a contingency system remains adequate for use will depend on:

- the navigation application being performed;
- the weather conditions;
- the risk of collision or grounding (based on traffic situation and location restrictions);
- the equipment fit of the vessel.

3.5.4 Dependent Systems

In addition to providing the primary navigation data, the GNSS on a modern bridge supplies position, navigation and timing inputs to other systems, including AIS, ECDIS and GMDSS. Loss of GNSS would render

AIS unusable for positioning, however it should not make an ECDIS unusable, as it should be possible to input visual or radar bearings. Manual input of position would be needed for GMDSS. Contingency systems would be of no use in this case – only a similar satellite navigation system such as Galileo or a compatible backup system such as Loran could provide a direct position input. This will become an increasing problem as reliance on these systems grows. AIS is being seen as an aid to security in addition to safety and in that role the incentive to jam the system providing the position input may become much greater.

GNSS vulnerabilities also extend to AtoN provision with regard to DGNSS, VTS and GNSS-synchronised lights. Additionally, the implementation of e-Navigation is expected to result in an increased reliance on timing-dependent communications systems based on GNSS.

3.5.5 Integrity Systems

A number of systems are provided to monitor the integrity of GNSS, for example the IALA beacon Differential GNSS service, which is standardised for maritime use. Satellite Based Augmentation Systems, such as WAAS and EGNOS, carry integrity messages and enhanced forms of Loran such as Eurofix also perform this function, but these are not internationally approved for maritime use. Navigational warning systems, such as Navtex and Safetynet can also provide integrity warnings, but there may be delays in delivering such warnings by these methods. It should be noted that augmentation systems are dependent on GNSS for position indication and are not standalone services. They are therefore subject to interference, jamming and spoofing of GNSS, but may be able to provide a warning of malfunction. Modern GNSS receivers incorporate Receiver Autonomous Integrity Monitoring (RAIM), which may be able to provide a warning of malfunction.

It may be feasible to utilise AIS to monitor GNSS anomalies by analysing position reports and comparing with previous reports and/or other data sources such as VTS.

4 ACTION PLAN

To respond to these concerns, an action plan is provided that includes carrying out a Risk Assessment to identify requirements for a back-up navigational system and the user receiver architecture that would need to be provided.

4.1 Risk Assessment

Aids to Navigation authorities should conduct an assessment of risks to traffic within areas of interest. The type and level of Aid to Navigation (AtoN) systems required should be determined by the levels of risk and dependence on GNSS. Whatever systems or procedures are deployed must be looked at in terms of the various stages of a voyage i.e. Ocean, Coastal, Port approach and restricted waters, Port, Inland Waterways. For example in the middle of the Pacific Ocean a suitable alternative could consist of celestial navigation, dead reckoning and estimating position. The alternative system required in critical areas such as the Dover Straits or Straits of Malacca needs to be significantly more robust as many vessels may be using integrated navigation systems in close proximity.

In evaluating the need for an alternative system, the transition from GNSS to alternative systems must also be considered from a practical and watchkeeping point of view. Visual AtoN provide a ‘reality check’, however integrating position verification into existing electronic systems is not always straightforward and will inevitably rely on good continuation training and situational awareness by mariners.

It must be recognised that a loss of operational capabilities currently available with GNSS is acceptable providing the safety of the vessel is not compromised.

4.2 Requirements for a Backup Navigation 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 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.

4.3 GNSS Integrity Warning System

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].

4.4 User Receiver Architecture

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.

5 CONCLUSIONS

The following conclusions were identified through studies carried out on GNSS Vulnerability:

1 A thorough risk analysis is needed to determine the probability of loss or degradation of GNSS and the likely duration and area affected.

2 Greater reliance on GNSS will increase the consequences of its loss or degradation.

3 Current developments in GNSS are expected to provide a fully redundant PNT system.

4 Future GNSS are expected to have similar vulnerabilities as currently identified for GPS.

5 Vulnerability of future GNSS will be reduced by additional signals and higher transmitter powers.

6 eLoran could provide an effective backup, but has its own vulnerabilities and coverage and equipment carriage is limited.

7 Radar can provide a limited backup to GNSS, but does not meet all the PNT requirements.

8 Low-cost inertial systems may provide an onboard backup system in the future.

9 Ranging mode (R-mode) implemented within DGNSS and/or AIS may provide a backup system in the future.

10 Visual and other AtoN, including VTS, are essential to complement GNSS for marine users.

11 In poor visibility radar and dead-reckoning are the present alternatives, both have limitations.

12 Taking account of the results of the risk assessment noted in (1) an effective, compatible backup to GNSS may be needed to support dependent systems (AIS, ECDIS).

6 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.

[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] ICAO. Draft 11th ANC Secretariat Paper. Task 3. Mitigation of GNSS Vulnerabilities, Oct. 2002.

[7] S.Williams. Commercial GPS Susceptibility. RTCM 2004 Annual Assembly Proceedings.

[8] P.H. Doherty et al. ION GPS-2000, Sept. 2000, p. 662.

[9] International Maritime Organization (IMO), 2003. World-Wide Radionavigation System Resolution A.953(23).

[10] 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.

[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] eLoran. Securing Positioning, Navigation and Timing for Europe's Future. European eLoran Forum. April 2008.

[13] German Federal Waterways and Shipping Administration. Contribution to the IALA World Wide Radio Navigation plan, IALA eNAV 4, February 2008.

[14] IALA, Recommendation R0121 (R-121), "The Performance and Monitoring of DGNSS Services in the Frequency Band 283.5 – 325 kHz", Edition 1, 2004.

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

Table 2 Suggested minimum maritime user requirements for general navigation – backup system

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

Notes:

1. This table is derived from IMO Resolution A.915(22).
2. Continuity is not relevant to ocean and coastal navigation
3. IMO Resolution A.1046(27) amended the Continuity Time Interval to 15 minutes, rather than 3 hours as originally required in IMO Resolution A.915(22).
4. This table should be read in conjunction with paragraph 2.1 and 2.2. Although these are suggested minimum requirements, a Risk Assessment will include many variables that may alter the minimum requirements. Refer to IALA Guideline on the Provision of Aids to Navigation for Different Classes of Vessels, including High Speed Craft, Dec. 2003 for details of the variables of different waterways, ships and environments