|  |
| --- |
| IALA Guideline |

Gnnnn

Cyber security specifics in IALA domains

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 |
| March 2022 | First draft – joint task group on cybersecurity (ARM15 TG1.2.6) | n/a |
| October 2022 | Included input from ENG  Amended on VTS-specific cyber risks | n/a |
| September 2023 | Amendments and corrections on VTS-specific cyber risks | VTS54 silent approval on chapter 6 |
| September 2023 | Corrections following VTS54 silent approval  Amendments and corrections from DTEC1 | DTEC1 silent approval on chapters 4 and 5 |
|  |  |  |
|  |  |  |
|  |  |  |

1. Introduction 5

2. Purpose and scope of this document 5

3. available standards and guidance 5

3.1. Generic / IT 5

3.2. Operational technology (OT) 5

3.3. for the maritime domain 5

4. Considerations for ATON 6

4.1. Protection of ATON 7

4.2. Maintenance procedures 7

4.3. Communication with ATON 8

4.4. ATON INFORMATION MANAGMENT SYSTEMS 8

4.5. ATON-specific documents to consider 9

4.6. Potential gaps 9

5. Considerations for Maritime services in the context of e-navigation 9

5.1. IP/WEB based 9

5.2. Non IP/WEB based 9

5.3. MS-specific documents to consider 10

5.4. Potential Gaps 10

6. Considerations for VTS 10

6.1. General guidance for VTS 11

6.2. Sensors 12

6.3. Core VTS systems 13

6.4. Communication 13

6.5. VTS-specific documents 14

6.6. Potential gaps 14

7. Considerations for PNT 14

7.1. PNT-specific documents to consider: 15

7.2. Potential Gaps: 16

8. Further reading 17

9. Index 18

List of Tables

**Geen gegevens voor lijst met afbeeldingen gevonden.**

List of Figures

***Geen gegevens voor lijst met afbeeldingen gevonden.***

# Introduction

Cyber security is a relevant topic for all uses of digital technology, not only within IALA but everywhere around us. It cannot be considered as an add-on function, nor can it be handled separately from any work on digital systems; it should be incorporated in all technology, process and human behaviour.

Because of the broad spectrum of cyber security, many industry standards and best practices are available to address technical vulnerabilities, provide guidance on processes and raise awareness of these issues across the IALA domains, including Maritime Services in the Context of e-Navigation.

There are, however, specifics within these domains that are not covered by existing standards or best practices. This document aims to provide guidance by referencing existing standards, best practices and other guidance on the IALA-specific topics that are not addressed by ready available standards and best practices.

# Purpose and scope of this document

Purpose and scope of the rec and guideline

Cyber security awareness

Risk assessment

hazard detection and mitigation

Business continuity plans

Cyber attack response plan

# available standards and guidance

The IALA workshop on cyber security, held virtually in November 2021, produced a list of available standards for adoption by IALA members. The workshop report elaborates on these standards and they are summarized below.

## Generic / IT

* ISO/EIC 27001 series: IT Information Security and Privacy Management, providing requirements for an information security management system (ISMS)
* NIST Cybersecurity Framework: guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk
* NIST SP800-53: Security and Privacy Controls for Information Systems and Organizations

## Operational technology (OT)

* IEC 62443: Cyber security for Industrial Automation and Control Systems

## for the maritime domain

* IMO MSC-FAL.1/Circ.3-REV.2: Guidelines on Maritime Cyber Risk Management
* ISO/IEC 63173: Maritime navigation and radiocommunication equipment and systems, including SECOM
* Resolution MSC.428(98): MSC Maritime Cyber Risk Management in Safety Management Systems
* NISTIR 8323: Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services
* ISO 23806: Maritime Cyber safety standard
* BIMCO et al.: The Guidelines on Cyber Security Onboard Ships

# Considerations for ATON

An Aid to Navigation (AtoN) is a device, system or service, external to vessels, designed and operated to enhance safe and efficient navigation of individual vessels and/or vessel traffic. Some types of AtoNs are:

* Physical AtoN:
  + Visual AtoN: Lights, buoys, beacons, etc
  + Audible AtoN: Bells, horns, Mariner Radio Activated Sound Signals (MRASS), etc
  + Radar reflectors
* Electronic (Automatic Identification System (AIS) AtoN, radar responder (RACON) and radar target enhancer) and in the future the VDES (VHF Data Exchange System)
* Global Navigation Satellite Systems (GNSS)
* Vessel Traffic Service (VTS)

VTS and GNSS used for Position Navigation and Timing are discussed in separate chapters.

An AIS AtoN can be implemented in three ways, physical, synthetic, and virtual. A physical AIS AtoN Station is an AIS station located on an AtoN that physically exists. A synthetic AIS AtoN is a AtoN that physically exists but the location is transmitted from another AIS station located remotely, but in the close proximity of the physical AtoN. A virtual AIS AtoN broadcast is transmitted from an AIS station for an AtoN that does not physically exist. This virtual AIS AtoN is projected on Radar, ECDIS and ECS charts but cannot be found on that place it is projected.

AIS AtoN are, in essence, radio messages transmitted via computer programmable radios, which either augment a buoy or beacon or provide independent data of navigational significance.

Depending of the type of AIS AtoN the level of cyber security threat is different and should be taken into account accordingly. Type 1 AIS AtoN could be only vulnerable for PNT signals while more sophisticated have more vulneraries. A physical AtoN without Bluetooth/RF remote programing is seemingly cyber secure. However, AIS AtoN signals have corresponding data used to manage and maintain them as well as inform the mariner about hydrographic and Maritime Safety Information. Administrations/waterway authorities must ensure the integrity of their signals, and provide mariners a way to verify the authenticity of the signals. This chapter focusses on AtoN and the means to ensure that valid messages, whether AIS or visual/audible/radio, are transmitted. It also discusses AtoN information management systems used for program management by AtoN administrations.

The historical development of AtoN monitoring began with human observation, moved to a connected but closed solution, and now expanded to a convergence on IT, OT technology & IoT enabling with satellite monitoring almost from anywhere in the world. The use of these technologies has been progressed by AtoN operator and/or manager’s desire for remote and reliable monitoring, reduced preventative maintenance and aid availability targets[[1]](#footnote-1).

## Protection of ATON

AtoN are usually in publicly accessible areas, although often at sea or inland waterways where a vessel would be required to reach them. Physical security is an important component of cyber security. Administrations which provide physical, virtual and synthetic AIS AtoN signals may do so from network/internet connected AIS stations, necessitating network security in addition to physical security. Many lanterns use RF programming and can be accessed using a universal TV remote. More modern lanterns may use Bluetooth or WiFi technology providing another access point and potential remote connectivity.

Remotely monitored and programmable AtoN have both positive and negative implications with respect to cyber security. In one respect, remotely programmable AtoN allow additional access points and potential means for a cyber-attack. Conversely, remotely monitored AtoN offer administrations a method by which to more quickly identify an AtoN which is not operating as required and/or may have been subject to unauthorized modification by a nefarious actor.

The following measures should be taken into consideration:

1. Use locks on cabinets and casing where electronics or management interfaces are present. If possible use a sensor to be able to detect access to the cabinet/casing;
2. Modern AtoN may include digital systems that resemble (or are) a computer system, in which case best practices for hardening and protection of computer systems should be implemented;
3. Implement monitoring/detection of unusual behavior, including GNSS and physical properties. Note that monitoring and detection is not by definition a technical/automated system but may also be performed by means of human inspection;
4. If the AtoN uses GNSS for positioning and/or time synchronisation, apply measures to mitigate against jamming and spoofing of GNSS signals. See the chapter “Considerations for PNT”;
5. Use risk mitigation planning to make an informed decision when using remotely monitored and programmable AtoN equipment as it may become more susceptible to cyber-attacks. When remotely programmable AtoN equipment is used, provide authorized user identification and access protections measures
6. Whenever feasible, AtoN, systems used to conduct maintenance, maintain and transmit MSI related to AtoN should use cyber-secure electronics
7. Administrations should encourage public reporting of perceived electronic signal spoofing, jamming, or operation/behavior other than the advertised signal. This may include when the position of a physical buoy is significantly different than the position of its synthetic AIS AtoN signal, if so equipped.
8. Implement software/firmware updates and (security) patches on AtoN, but only after thorough acceptance testing;
9. Conduct periodic penetration tests and/or vulnerability scans on (representative) AtoN to validate cyber resilience.

## Maintenance procedures

Periodic maintenance should be performed on every ATON, both physical and electronic. The following suggestions will contribute to improved and consistent cyber resilience of ATON when applied in maintenance procedures:

1. Create and enforce a policy for physical key management for proper authorisation and logging;
2. Inventory and understand the means by which to program or modify the ATON equipment (e.g. LED lantern) providing the signal. Where feasible, consider use of methods such as password/pin or other means by which make unauthorized modification of the signal more difficult. If technically feasible, setup user accounts with minimum required permissions and/or use a central authentication database, like Radius or LDAP;
3. Where possible, create standardised maintenance instructions and templates including verification of measures to protect ATON against cyber risks. Having a second maintenance engineer check the work after maintenance provides additional verification and protect against possibly compromised personnel ("4-eyes principle"). An extra verification may partly be performed remote if technically feasible;
4. Ensure the cyber security of maintenance tools like engineering laptops and verify that no unnecessary data is stored on the device.
5. Verify the integrity of maintenance instructions to ensure that maintenance is conducted following the requirements;
6. Documentation of ATON information and configuration should continuously be verified to be accurate and up-to-date;
7. Ensure that backups of firmware, software and configuration are periodically made and that their integrity is verified, i.e. that backups can successfully be restored. Create new backups immediately after every change in software, firmware or configuration;
8. Ensure proper protection, with regards to Confidentiality, Integrity and Availability (“CIA”) of backup information and documentation. Standard IT best practices will in most cases be appropriate.

## Communication with ATON

Communication with ATON may be local, for programming and maintenance, or remote, usually via ATON management systems. ATON may also be used to transmit data, such as AIS ATON messages and/or VHF voice broadcasts.

Where IP-based communication is used, appropriate protection of the transmitted data should be implemented. In many cases the SECOM (IEC 63173-2) standard provides guidance. Where it does not, standard internet-based encryption and authentication technology may be applied.

The following additional measures may be considered:

1. Protect wireless management interfaces (Wireless LAN, RF, Bluetooth, Infrared) by disabling them while not in use;
2. If the (wireless) technology allows, apply (user) authentication and modern encryption for access to the ATON. Ensure that factory-set default passwords are changed and that passwords are rotated periodically;
3. If an ATON is remotely managed and monitored, apply authentication and encryption on the entire communication link to ensure integrity of the data transmitted. This may require an extra “layer” of security, i.e. the link from an ATON management system to a satellite system may be sufficiently secured, but the actual downlink to the ATON may not be.

## ATON INFORMATION MANAGeMENT SYSTEMS

Aside from the physical ATON itself ATON positioning systems may be connected to networks and internet and may double as OT/IT. ATON Administrations manage massive amounts of critical data related to the status and maintenance of the ATON. In many cases this data represents legal records related to the actions by the administration to provide and maintain the ATON which may be called upon in the event or marine incident which may have involved ATON. These systems and data are at risk from a variety of threat vectors including adversarial attack, system failure, data loss or corruption, and simple human error.

Recommended measures include:

1. Identify critical data and systems, networking connections, and access points. Consider forming a written IT cybersecurity policy for risk mitigation which incorporates data back-up, continuity of operations planning, and restoration management;
2. Identify what data requires additional control measures such as Personal Identifiable Information (PII);
3. Implement and maintain strict authorized user identification and access protection;
4. Where feasible use methods such as encryption, data segregation (e.g. by operational region) and or user role permission to protect data;
5. Limit the number of IT / OT network connections and data access points to only those necessary for routine and contingency operations;
6. Whenever possible, leverage data-management systems and programs which are user friendly and incorporate functions such as graphical displays that help prevent human error and allow users to recognize and correct errant or missing data.
7. Where possible, collect and save log files of all (sensor) information from ATON for at least 180 days to enable (forensic) inspection following abnormal behavior and cyber incidents.
8. If a communication link is established to provide automatic updates to hydrographic systems/organisations, apply appropriate preventative measures and monitoring to ensure the integrity of the data;
9. Conduct periodic penetration tests and/or vulnerability scans on ATON management systems to validate cyber resilience.

## ATON-specific documents to consider

## Potential gaps

# Considerations for Maritime services in the context of e-navigation

## IP/WEB based

Maritime services in the context of e-navigation are often based on IP and the application of web services. In those cases, the SECOM (IEC 63173-2) standard should be applied and additional measures from IT and/ot OT standards, like best practices for security monitoring, should be considered.

## Non IP/WEB based

Where no IP/Web based technology is used, especially in MSI radio systems like VHF, AIS, VDES and NAVTEX, the following suggestions may aid in the availability and integrity of the information. Note that many of these systems are meant to be public/broadcast and have a role in Maritime Safety Information (MSI). Although information transmitted may be confidential, no encryption is provided to enable all receiving parties to receive these.

1. While there are initiatives to implement authentication of messages in various MSI systems, there is currently no standardised solution. Instead, it is suggested to implement multiple different systems that may provide similar information, to be able to compare the information provided. If in doubt, human verification, for instance via VHF, may assist.
2. Monitor for unusual messages; commercial systems are available to monitor for spoofing and jamming, especially in AIS.
3. Have monitoring systems available for triangulation of invalid radio transmissions.

## MS-specific documents to consider

* IALA R1019: PROVISION OF MARITIME SERVICES IN THE CONTEXT OF E-NAVIGATION IN THE DOMAIN OF IALA **(recommendation)**
  + Covers general aspects of digitalisation: Resilience, security, identity and authentication by design
  + Availability, Integrity, Confidentiality
* IALA G1157: WEB SERVICE BASED S-100 DATA EXCHANGE **(technical guideline)**
  + Guidance on implementing MS with S-100 data
  + Recommends to use IP and TLS in combination with PKI
  + Local certificate store -> offline PKI
  + Sign data (+timestamp to avoid replay attacks)
* IEC 63173-2: Maritime navigation and radio communication equipment and systems – Data interface – Part 2: Secure exchange and communication of S-100 based products (SECOM) **(technical guideline)**
  + Standardises Interfaces used for S-100 online data exchange.
  + Provides some general guidance on how to utilize Identity Management and Service Discovery on the technical level
* IALA G1161: GUIDELINE ON THE EVALUATION OF PLATFORMS FOR THE PROVISION OF MARITIME SERVICES IN THE CONTEXT OF E-NAVIGATION **(generic guideline)**
  + Provides a framework to evaluate technologies/platforms for MS
  + Covers basic aspects of Cyber Security: Authentication, Authorization, Robustness, Efficiency, Confidentiality, Integrity, Availability, Non-repudiation
* (Technical Design Specification(s) for Maritime Services currently being drafted using SECOM)
* Maritime Connectivity Platform (MCP) as a framework for secure maritime data exchange:
  + Documentation on MCP PKI
  + Identity Management
  + Usage of MCP-MRNs
  + MMS as a secure low-bandwidth messaging service

## Potential Gaps

* Measures to provide authentication in existing systems like AIS and VDES are still in development.
* IALA GXXXX: Guideline on VDES VDL integrity monitoring (in development)

# Considerations for VTS

In VTS, cyber security risks focus on three main areas, namely the sensors, the VTS Core (presentation/processing) systems and the communication systems, all with their unique risks and potential mitigating measures.

Availability and reliability of the systems usually has the highest priority and cyber security measures may have an adverse effect on these. On the other hand, not taking measures against cyber risks may impact availability and reliability. Therefore, a good balance between security and reliability is required. A risk assessment is a good approach to find this balance.

With the intended increased provision of VTS Digital Services (S-210, S-212 ...), to some extent replacing provision via voice based communication, data integrity become a vital focus point against e.g. Liability issues. Furthermore all exchanged and provisioned data (services) need to be fully traceable, i.e. logged/archived as a function provisioned by the VTS System, beside voice and sensor data as should be in place already; the integrity and secure storage hereof will be essential within a VTS centre.

Besides the systems for VTS there are often administrative systems used. These are usually qualified as “standard” office systems and application and handled as appropriate in terms of cyber security.

## General guidance for VTS

Although mostly part of many existing standards, it is emphasised that attention is paid to the following topics when establishing or working on VTS systems:

1. **Documentation and procedures** are important to ensure consistent implementation and maintenance, in particular security procedures, especially as VTS systems may be spread over a large geographical area and/or difficult to visit.
2. Pay attention to **network segmentation[[2]](#footnote-2)** to lower the risk of an attacker reaching a VTS system when an office system is compromised. This also counts for networks within the VTS system itself; i.e. VHF systems should be separated from radar systems
3. Well established **maintenance procedures** contribute to a cyber secure system, especially well tested and timely applied security patches
4. **Remote access** should be minimised to absolutely necessary access by employees and/or third parties. Authentication and authorisation of users and technical monitoring/logging of all remote activity should be implemented and validated. Also time restriction in remote access should always be considered.
5. **Interfaces[[3]](#footnote-3)** with systems outside the VTS networks, for example for monitoring and predictive maintenance, should only be implemented after a risk assessment.
6. VTS personnel, both operational and technical should continuously be **educated** on cyber security awareness and detection of malicious activity within the VTS systems
7. Consider cyber security when establishing or renewing a VTS system, including risks introduced by using third party services, including private or public cloud services.
8. When implementing technical measures, consider the relation between cyber security and (physical) **safety**, including safety of navigation. These may complement each other, but one may also have a negative influence on the other.
9. A **Business Continuity Management plan** for VTS should be implemented to react to and recover from a cyber attack by management, operational and technical means in a structured way.

Note that this general guidance does not replace the established standards and these should also be followed to implement other measures, such as anti-malware and password/identity management, for example.

## Sensors

When referring to sensors in the context of VTS, we mean the systems collecting data to enable VTS operators to have situational awareness. Examples are radars, CCTV cameras, hydrographic sensors, meteorologic sensors and AIS listeners/base stations. Their common attribute is that they are usually placed outside the actual VTS centres, often in publicly accessible areas. This makes them vulnerable to physical influences, both deliberate (vandalism, break-in, manipulation, disruption) and accidental (weather, natural disasters). Also the communication links are more vulnerable, whether these are (buried) cables or wireless connections.

The following measures for improving resilience against deliberate and accidental cyber risks may be considered:

1. Part of the cyber security for sensors will be formed by physical security. Consider qualitative locks, thorough building, fences, security cameras, door/window alarms, smoke detectors, leakage detectors, climate control and emergency power systems. Many of these will already be in place for availability purposes and addressing accidental influences. Additional measures may be needed to detect and prevent deliberate access attempts and the consequential cyber risks of that.
2. Related to physical security, make sure authorisation for entering the site is controlled. Who has the keys? Is it a shared location?
3. Implement monitoring/detection tools that not only monitor availability[[4]](#footnote-4) but also data integrity[[5]](#footnote-5). Think of ways to validate that received data is valid and authentic. This may be caused by accident or deliberately via radio communication or using communication links, via the network. .
4. Turn off unnecessary features of systems. A hydrographic sensor may be programmable by Bluetooth. Make sure the Bluetooth is disabled when not programming the sensor and make sure it is documented so it is repeatable for the next sensor. Also, any unused (network) interfaces should be disabled at unmanned locations.
5. Apply encryption on communication links, whether they are wired (copper/fiber), wireless (beam/laser/LTE/Satcom), public (Internet/site2site service), or private (own cables) to make sure eavesdropping and manipulation of the data is prevented as much as possible.
6. Apply authentication where possible to be able to validate that data is actually originating from the device or system that it identifies itself as.
7. Take measures to assure that if one sensor is compromised, this will not imply that all sensors may be compromised, e.g. as a result of identical passwords or other configuration.
8. For business continuity reasons, apply redundancy. A single (or even 2 or 3) compromised sensors should not lead to VTS operators being unable to perform their tasks.
9. Create procedures for fast restoration and/or replacement of sensors.

## Core VTS systems

The Core VTS systems, including the presentation systems the VTS operators work with are usually placed in a VTS centre. Some (back-end and processing) systems may be placed in an (internal) data centre. They collect and process the data from the sensors and present them to the VTS operator to create situational awareness. In most cases these systems are more or less standard IT systems, like computer workstations and servers and security measures for computer systems may be applied as is done for office computers.

There are, however, unique properties for VTS Core systems that require an approach different than for standard IT systems;

1. VTS Core systems may not require user authentication – VTS operators man these systems 24/7 and a locked or logged-out system prevents them from having a continuous overview of the traffic situation
2. As VTS workstations are often used 24/7 there may not be maintenance windows to install updates and patches
3. Because of the availability and reliability requirements, system administrators may be hesitant to install updates and patches as they may cause instability or unexpected behaviour.

The following measures for improving resilience, considering VTS Core system’s unique properties may be considered:

1. Physical security may partly make up for lower cyber security. Implement proper access procedures for the VTS centre and -rooms and if possible, put the actual systems in a locked cabinet.
2. Implement user authentication with a suitable policy. While VTS workstations should not be locked or logged out, there may also be unused/spare workstations, and they should not be freely accessible. An automatic locking mechanism may be suitable if set to several hours of inactivity timeout.
3. Apply monitoring mechanisms, other than a user login, to validate user actions. Maybe security cameras may be suitable or other biometric identification is possible. These will not prevent deliberate manipulation but will enable alerting and forensics.
4. Implement social control – make sure no-one is ever alone in a VTS centre or associated data centre, if the situation permits. Also take measures to validate the integrity of personnel
5. Disable all functionality on VTS systems that is not needed for the VTS operation process. Users should not be able to start any unnecessary applications or start an internet browser. Especially all USB devices, other than Human Interface Devices, should not work.
6. Limit network access to the minimum necessary; VTS Core systems should not have any internet access and be logically or physically separated from office systems. Make sure both inbound and outbound network traffic is blocked.
7. Create procedures for fast restoration and/or replacement of VTS Core systems, of have cold spares available. Hot spares are often good for availability but may be hit by cyber attacks. Cold spares will not be hit.

## Communication

VTS communication systems include VHF communication, AIS/VDES messaging and, depending on the specific VTS centre, telephone, and other communication means, even AtoN like lights.

All communication with ships is wireless and thus vulnerable to deliberate and incidental disruption and often eavesdropping or manipulation (spoofing). Communication systems, especially VHF/AIS/VDES systems, may be physically placed outside an actual VTS centre and therefore share the same vulnerabilities as sensors.

Most measures in communication focus on business continuity as reliability can often not be improved with the communication systems, apart from choosing alternative technology, but that will, in most cases, not be an option in the maritime industry.

The following measures are available for mitigating the cyber risks in VTS communication systems:

1. Deploy methods for detection and localisation of disruptive signals or contract a competent third party to do so. Usually, a technique like triangulation is suitable. This will assist in quickly mitigating disruption and malicious transmissions.
2. Implement technical measures or procedures to disable any disruptive sources of radio signals. For instance, AIS/VDES/NAVTXT may be disabled in case of disruption or spoofing, if also radar is available. VTS operators must be able to perform their duties with only radar information.
3. Depending on the communication method, special radio hardware (antennas) may be available that are less sensitive for disruption from directions other that where ships may be expected to be.
4. Have alternative communication methods available. Telephone or megaphone may replace VHF in emergency situations and notices to mariners may be sent out to mention a phone number or to inform that the VTS will not communicate verbally at all.

## VTS-specific documents

* IALA G1111 is a common source of information to assist competent authorities and VTS providers in the preparation and establishment of functional and performance requirements for VTS systems. Cyber Security requirements should be considered in this process
* SECOM (IEC 63173-2) specifies technology en measures for Secure communication between ship and shore. The implementation of an identity registry and PKI may be provided by the Maritime Connectivity Platform (MCP)

## Potential gaps

* Specific training may be required for VTS operators, supervisors and managers, and training should be periodically repeated to keep awareness on the desired level and stay aligned with current cyber threats. Training should address:
  + Prevention of cyber incidents
  + Recognition of cyber incidents and anomalies
  + How to respond to cyber incidents, both technically and operationally, including what *not* to do

# Considerations for PNT

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

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

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

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

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

"Regulation 13 - Establishment and operation of aids to navigation

1 Each Contracting Government undertakes to provide, as it deems practical and necessary either individually or in co-operation with other Contracting Governments, such aids to navigation as the volume of traffic justifies and the degree of risk requires.

2 In order to obtain the greatest possible uniformity in aids to navigation, Contracting Governments undertake to take into account the international recommendations and 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."

Available measures to mitigate against PNT spoofing and jamming are:

1. Awareness of the potential impact is important, without considering what any data manipulation or denial may look like, it will be difficult to understand if such an event is occurring.
2. Monitoring – where possible the system should have some form of monitoring capability to ensure the information provided is reliable – this is commonly known as integrity and may have performance targets depending on the system.
3. Some GNSS constellations offer authentication services which could be considered for implementation
4. It
5. GNSS signals usually originate from satellites, which should be well above the horizon. Antennas are available that attenuate signals that originate from lower than ~5 degrees above the horizon, that may assist in effective blocking of jamming or spoofing signals, that are mostly send from the ground.
6. Make use of the SBAS and GBAS systems/information services to alert about jamming and/or spoofing of GNSS signals.
7. Make use of the provisions in AIS and VDES to mitigate jamming and/or spoofing.
8. For the mariners use the physical AtoNs to check the reliability of PNT.

ENG is working on a Guideline to support resilient PNT. This GL discusses a number of vulnerabilities and options to achieve resilient PNT, and while it mentions cyber security it is not captured in detail.

We need to be clear on whether cyber security includes aspects such as GNSS jamming (likened to a denial of service) and Spoofing (likened to data manipulation).

The technical advice provided in the reference documents should be considered and referenced where possible, but for PNT the following considerations are noted:

* PNT is used within AtoNs to support positioning and timing aspects. Both support the use of the AtoN, although in different context. As an example, within AIS, timing information from GNSS is used to synchronise the data channels, while GNSS derived positioning information is used to measure the vessel’s proximity to other targets. GNSS timing is also used to support synchronised lights and communications.
* PNT data can also be used in areas where it may not immediately be obvious. During GPS jamming trials conducted by the GLAs on a buoy tender, it was discovered by accident that the main GPS receiver feeding the bridge also provided time throughout the vessel. The resilient PNT demonstration for ACCSEAS project could be found on https://www.youtube.com/watch?v=CNAr8eQQ\_9E
* Some (physical) AtoN can provide PNT information and it’s important to consider the impact of cyber security aspects for them too. Corrupting the provision of data could have significant implications, whether that’s providing false position information or integrity data.
* Overall security mitigation measures will depend on the type of AtoN and how the PNT data is used or generated. Physical security is a key component, whether that’s preventing access to a shore site or simply preventing a seemingly innocent phone charger from being plugged into a device. Networked devices should be planned and not added in an ad-hoc manner and air gaps should be used where relevant to prevent any hacker from gaining access to all/sensitive areas.

## PNT-specific documents to consider:

The following documents may need to be reviewed to ensure cyber security aspects are suitably considered.

* IALA Recommendation R1017 Resilient position navigation and timing (PNT)
* IALA Recommendation R0129 GNSS vulnerability and mitigation measures
* IALA Recommendation R1020 Terresterial radionavigation systems
* IALA Recommendation R1011 Performance and monitoring of eLORAN services in the frequency band 90-110 kHz
* IALA Recommendation R1011 Performance and monitoring of DGNSS services in the frequency band 283.5-325 kHz
* IALA Guideline G1112 Performance and monitoring of DGNSS services in the frequency band 283.5-325 kHz
* IALA Recommendation R0135 Future of DGNSS
* IALA Guideline G1060 Recapitalization of DGNSS
* IALA Recommendation R0150 DGNSS service provision, upgrades and future uses
* IALA Guideline G1158 VDES R-mode
* S-201 Aids to Navigation Information
* S-240 DGNSS Station Almanac
* S-245 eLoran ASF Data
* S-246 eLoran Station Almanac
* S-247 Differential eLoran Reference Station Almanac

## Potential Gaps:

* Training of personnel on ship and shore
* Review of impact to MASS as a special consideration (also drones where used)
* Human factors implications
* Authentication of the signal
* Environmental implications
* Infrastructure for monitoring / reporting / warning is being removed (IALA beacons)

**------ After here only placeholders for additional content ------**

# Further reading

Any texts that are recommended to the reader without direct reference in the text should be listed within this section using the same syntax as the reference list. Sources should be listed using the **Further reading** style.

1. Einstein, A. (1905) Relativity: The Special and General Theory of Relativity
2. Idle, E. (1984) The Galaxy Song

# Index

**No index entries found.**

1. Example of appendix Title (Head 1) style

1. Example of Annex title (Head 1) style

1. As discussed during the IALA Cyber Security 2021 Workshop [↑](#footnote-ref-1)
2. Segmentation is a term that is often used in Cyber Security and refers to the splitting (or even isolating) networks into smaller networks and implement inspection, such as a firewall or malware protection in between, allowing only the necessary network traffic between the networks. [↑](#footnote-ref-2)
3. An interface is a communication channel between systems and may both be physical or logical, line a TCP port or rest API. [↑](#footnote-ref-3)
4. Data availability pertains to jamming of radio signals and communication. This may be accidental or deliberate and can happen with any type of wireless communication resulting in unavailability of the wireless signals or creation of many false signals. [↑](#footnote-ref-4)
5. Data integrity pertains to the manipulation of sensor data. Examples are false AIS messages (“spoofing”), unauthorised VHF voice messages and altered measurement data from hydrographic/meteorologic sensors. [↑](#footnote-ref-5)