|  |
| --- |
| 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) |  |
| October 2022 | Included input from ENG  Amended on VTS-specific cyber risks |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. Introduction 4

2. Purpose and scope of this document 4

3. available standards and guidance 4

3.1. Generic / IT 4

3.2. Operational technology (OT) 4

3.3. for the maritime domain 4

4. Considerations for ATON 5

5. Considerations for Maritime services in the context of e-navigation 6

5.1. MS-specific documents to consider: 6

5.2. Potential Gaps: 7

6. Considerations for VTS 7

6.1. Sensors 7

6.2. Presentation 8

6.3. Communication 9

6.4. Generic guidance FOR VTS 10

6.5. VTS-specific documents 10

6.6. Potential gaps 11

7. Considerations for PNT 11

7.1. PNT-specific documents to consider: 12

7.2. Potential Gaps: 12

8. Further reading 13

9. Index 14

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: 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

Request to all committees to review, comment and amend

* Physical ATON – Physical hardware – Data representing the signal – match required – transmission – fidelity – reproduction – redistribute (ECDIS etc)
* Is it a valid ATON? How to guarantee and verify that?
* Integrity of the ATON, its beheviour (light signal, placement etc) and its data
* AIS / virtual ATON – signal integrity and authenticated

ATON Administrations must ensure the integrity of their signals, and provide mariners a way thought which to verify the authenticity of the signals. ATON, systems used to conduct maintenance, maintain and transmit MSI related to ATON should use cyber-secure electronics. One approach to this would be to update appropriate IALA docs to incorporate existing cyber-security standards, protocols and best practices (i.e., CIRM's, BIMCO's, IMO's.)

Legacy ATON signals (buoys and beacons) seemingly have few cyber vulnerabilities. A physical ATON without Bluetooth/RF remote programing that requires manual programing is seemingly cyber secure. However, ATON signals have corresponding data used to manage and maintain them as well as inform the mariner about them through hydrographic and Maritime Safety Information products.

* Many lanterns use RF programming and can be accessed using a universal TV remote. More modern lanterns may use Bluetooth technology providing another access point and potential satellite connectivity.
* Aside from the physical ATON itself ATON positioning systems may be connected to networks and internet and may double as OT/IT. ATON Administration manage massive amounts of critical data related to the status and maintenance of the ATON.
* Administrations which provide virtual and synthetic AIS-ATON signals may do so from network/internet connected base stations. AIS-ATON signals are under significant additional threat of spoofing.

*As discussed by Jens Ohle during IALA Cyber Security 2021 Workshop*

*Excerpt from Report on Cyber Security Workshop 2021: Cyber security for ATON, Jens Ohle – Sealite*

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 and OT technology & IoT enabling satellite monitoring from anywhere in the world. The use of these developing technologies has been fueled by ATON operator or manager’s desire for remote and reliable monitoring, reduced preventative maintenance and aid availability targets.

The technology used for data transfer is subject to cyber threat: GSM, Bluetooth, PSTN, Wi-Fi, TCP, RF and different ways of data (and signal) corruption. Encryption is therefore needed to keep the risk of ATON operations as low as possible. Another risk to ATONs’ is accidental due to the human factor, data corruption and connectivity risk (interference). The reason for hacking were stressed being ransomware the most observed. Jens presented Iridium as the preferred technology for last mile communication and the data management platform to mitigate the risk permitting different capabilities and methodologies as part of the design considerations (encryption levels, segregation of Personally Identifiable Information (PII), authentication among others). Jens advised that good procedures could be to conduct penetration testing not only for system validation, but continuously, maintain backup and restore management and finally to start by forming a written IT cybersecurity policy for risk mitigation.

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

Request to all committees to review, comment and amend

* Problems emerging from trust: Different Stakeholders want to share different types of data, but need to make sure the other parties transmitting/receiving data can be trusted
  + No central point of trust / world-wide
  + Authenticity of Messages
  + Identity Management: Establishing PKI
  + Modelling complex trust relations: A dataset may be issued by a local authority, be forwarded to a coordinating authority, and then distributed to a mariner by a distribution service. Who needs to trust whom, how can it be modelled securely? -> verify chain of trust
* Communication Channels
  + Security of communication channels (dealing with insecure channels like AIS, VDES, NAVTEX, …)
  + Availability: Interrupted connection, network not available, data loss, …
  + Integrity of Messages / Man-in-the-middle
  + Implications for (physical) Safety
* Currently, MS focusing on more modern and commonly used (less domain specific) technologies and concepts like IP, REST, Service-oriented Architectures
  + Frequent monitoring of new exploits/vulnerabilities (e.g., CVE monitoring) required.
  + Attack surface is more “public” than in proprietary services, but also comes with standardized and well-established solutions for protection. -> Expected to see more of this in the future

## 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 ED1: Maritime navigation and radio communication equipment and systems – Data interface – Part 2: Secure exchange and communication of S-100 based products (SECOM) **(technical guideline)**
  + Standardizes 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 (?)
* IMO/BIMCO Documents (not specific to MS)
  + The Guidelines on Cyber Security onboard Ships - Version 4
  + MSC-FAL.1/Circ.3
  + Resolution MSC.428(98)

## Potential Gaps:

* How to operate a maritime service from the provider perspective (is it use-case specific?)
* Procedures for incidents, disaster recovery, risk mitigation (could be covered by a more general guideline also applicable to VTS & AtoN (?))
* How to model (decentralized) trust relations and implement them securely (WIP @ MCP consortium)
* Using low-bandwidth communication channels (like VDES) is currently a general gap for MS (not only for cyber security).

# Considerations for VTS

In VTS, cyber security risks focus on three main areas, namely the sensors, the presentation (VTS 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** 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 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.
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.

## 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 tools that not only monitor availability but also data integrity. Think of ways to validate that received data is valid and authentic. For instance, water level will, in normal situations not rise 10 meters in 1 minute and a ship on a radar will not move 100 meters in 3 seconds. Neither will an AIS message be received from a ship hundreds of miles away.
4. Awareness should be created amongst VTS personnel to recognise and respond appropriately to cyber incidents including (potential) integrity degradation of VTS information, including traffic image, data communication and voice communication. Training of VTS operators and maintenance staff is recommended.
5. 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.
6. 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.
7. Apply authentication where possible to be able to validate that data is actually originating from the device or system that it identifies itself as.
8. 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.
9. 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.
10. Create procedures for fast restoration and/or replacement of sensors.

## Presentation

The presentation systems the VTS operators work with are usually placed in a VTS centre. Some (back-end) 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 presentation systems that require an approach different than for standard IT systems;

1. Presentation 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 presentation systems are 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 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 operational systems should not be locked or logged out, there may also be unused/spare systems, 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, 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 systems should not have any internet access and be logically 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 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 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 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 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

Request to all committees to review, comment and amend

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:

* 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.
* 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.
* 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 channel, 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. For example, resilient PNT demonstration for ACCSEAS project could be found on https://www.youtube.com/watch?v=CNAr8eQQ\_9E
* Some AtoN 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.
* Authentication of PNT data is emerging with some GNSS constellations now developing authentication services (e.g. Galileo Open Service Navigation Message Authentication, OSNMA). The concept of authentication in the maritime sector is relatively novel and education as well as technical solutions are required.
* 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.
* For PNT systems, it may not be possible to remove the risk of system interference, whether natural or man-made. To mitigate such events, multiple position solutions should be employed, systems that are dissimilar in approach and failure modes as part of a system of systems approach. This is covered further in the Resillient PNT Guideline.

## 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
* IALA Guideline GNNNN RESILIENT PNT
* 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
* 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