IALA GUIDELINE

GNNNN
CYBER SECURITY SPECIFICS FROM AN IALA PERSPECTIVE

Edition 1.0
June 2024

urn:mrn:iala:pub:gnnnn

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 REVISION

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

Date	Details	Approval
June 2024	First issue.	Council 80

CONTENTS

List of Figures

1. 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 into all technology, processes 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 the 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 directly addressed by readily available standards and best practices.

2. PURPOSE AND SCOPE OF THIS DOCUMENT

This document offers guidance on possible measures to be taken to mitigate cyber security risks in the IALA domain. Cyber security risk may be defined as:

"An effect of uncertainty on or within information and technology. Cyber security risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations and the Nation."

Definition based on ISO Guide 73 and NIST SP 800-60 Vol. 1 Rev. 1

The listing of referenced documents is meant to provide awareness, not serve as an all-inclusive list. This document is not meant as a replacement of existing guidance and standards as summarised in IALA *Recommendation R1024 Cyber security for the IALA domain*. Instead, this Guideline assumes the standards and best practices as referenced in the recommendation to be a generic basis to build upon, specifically for those assets and systems found in the IALA domain. Some parts of existing standards and best practices have been included though, if they are particularly important for the IALA domain or to provide necessary context.

2.1. SCOPE

This Guideline provides measures to mitigate cyber threats on assets and systems specific to the IALA domain and their properties. It is aimed at existing technology which may include legacy systems.

Technology that has not yet been developed or approved for use is not within the scope of this Guideline. Authors of guidance for new technologies are encouraged to include cyber resilience and mitigating measures against cyber risks in both the new technology itself and the respective documentation.

When updating existing documentation, authors are also encouraged to consider the inclusion of guidance on cyber security.

Some chapters include a paragraph on potential gaps which require extra attention apart from the measures or where no feasible measures are available.

2.2. INTENDED AUDIENCE

This Guideline is written for everyone in relevant authorities and providers of Marine Aids to Navigation (AtoN) as well as organizations providing technology used within the IALA domain, as cyber security should be embedded in everyone's day-to-day work. Some chapters do contain specifics for certain technology though that may not be applicable for all readers.

The document is not meant to be read and applied as a whole but rather as a reference with collected guidance on the different aspects of AtoN, including VTS and the Maritime Services in the context of e-Navigation.

2.3. LAWS AND REGULATIONS

Many countries, states and other (maritime) entities are developing or have developed laws and/or regulations on cyber security. Implementing measures set out in this Guideline will, in most cases, contribute to meeting local, regional, or global laws and regulations but users of this Guideline should make sure laws and regulations do not conflict with the guidance offered in this guidance.

3. PRINCIPLES AND BEST PRACTICES

Aside from the specific guidance that this Guideline offers, there are some general principles and best practices that every organization should practice as a basis for cyber security and resilience against cyber incidents.

3.1. RISK ASSESSMENT

Every asset, whether it is a single AtoN or a collection of systems comprising a VTS, should be assessed on the risk of cyber incidents to determine appropriate and proportional risk control(s) that Administrations should take. Cyber Risk is the combination of the likelihood of a cyber incident occurring and the severity of the consequences. In the context of cyber security, the disrupting event may be accidental or deliberate, the damage may be physical or digital and temporary or permanent. The damage to the assets and the navigational risks and/or economic impact on shipping should be incorporated in the risk analysis, as well as environmental impact. The consequence or damage caused by the cyber incident and its severity will help determine how Administrations should treat the risk and determine what mitigating measures could be taken.

Degradation of an asset may impact its availability and note that financial aspects may influence an acceptable risk level.

Sometimes, risk may be mitigated effectively, for example, by choosing a different (type) of component in an asset at the time it is acquired or bought.

The simplified risk assessment steps in the illustration below may be used as a basis for risk assessment of assets. This Guideline aims to offer possible mitigating measures as part of this process.

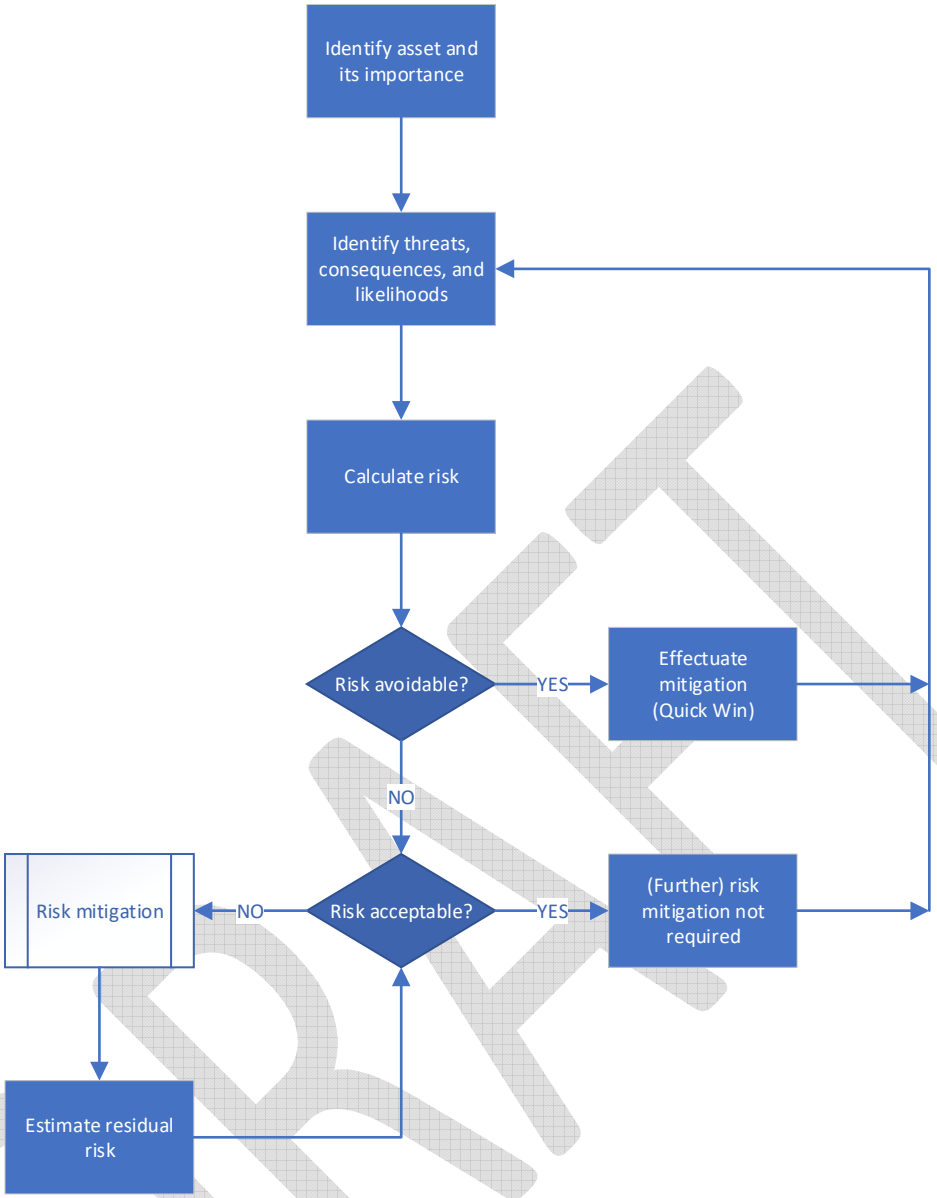

Figure 1 Basic risk assessment process flow

A cyber risk assessment should be repeated regularly to address the changes in the risk landscape, even if the asset itself is unchanged. In fact, cyber risk management should be an integral part of a risk management cycle as described in *Guideline G1018 Risk Management*.

Note that cyber security can require significant resources, both in human effort and costs. This should be proportional and supported by a thorough risk assessment that complements corporate risk management.

3.2. INCIDENT RESPONSE AND RECOVERY PLANNING

Almost every organization will be hit by a cyber incident at least once. For that reason, it is good to have incident response plans in place and practice these. Following risk assessments, organizations should be aware of the (residual) risk and possible gaps. Incident response plans should address these.

An incident response plan should at least consist of the following:

- a list of responsible persons and entities and their contact details.
- a list of prioritized actions to perform (or not to perform) immediately following a cyber incident.

- a description of the process to follow (which in many cases, will be a crisis management plan).
- a procedure for review and practice of the plan (which should be done regularly).

While incident response focus on damage control, incident recovery focus on the process of returning to normal operation. Incident recovery is often referred to as *disaster recovery*.

An incident recovery plan should at least include:

- check lists of tasks to complete before starting recovery.
- a list of prioritized actions for restoration of systems and services.
- a "plan-do-check-act" methodology to ensure correct restoration.
- a verified list of required resources, like installation media and backups.

Incident response and recovery plans may include sensitive information and should be considered to be confidential documents. Despite this, it is good practice to have a physical copy available, as computer systems may not be available or safe to use during a cyber incident.

Incident response and recovery are part of most available cyber security standards and best practices and specialised training may be offered.

3.3. BUSINESS CONTINUITY MANAGEMENT

While incident response and recovery address a cyber incident, Business Continuity Management (BCM) addresses operational processes during a period where normal operation is not possible, due to a variety of events, including cyber incidents. It may be combined with disaster recovery in a broader sense, as, for example, flooding may also be considered to be a disaster. It is important to note the difference in focus on either the origin or the operational process.

The process of Business Continuity Management should follow the following steps:

- identify (mission) critical processes in the organization;
- identify assets and processes supporting the (mission) critical processes;
- identify means of working around supporting systems and processes in case they are temporarily or permanently unavailable. This may also include alternative ways of working. It is recommended to do this for multiple timelines as workarounds may only be acceptable for a limited period;
- identify required assets for workarounds and alternative ways of working and make sure these are available and working; and
- practice, improve and review in accordance with the "plan-do-check-act" methodology.

Note that it is not necessary to work with incident/disaster scenarios. Assuming unavailability of a system or process will often catch any possible scenario.

BCM is part of most available cyber security standards and best practices.

Many organizations already have some kind of business continuity plan that is related to crisis management. It is suggested that existing plans are updated to include cyber security.

3.4. CYBER SECURITY AWARENESS

Research from many different organizations report that over 80% of data breaches have a contributing human element, with the majority of cyber incidents starting with phishing, either via communication media like e-mail/chat or physically. This may be summarised as "social engineering". It confirms that humans are the weakest link in cyber security and this requires specific action.

There are many companies offering commercial training and testing of employees' ability to recognize phishing and preach "cyber hygiene". Offering for systems and procedures used in the maritime domain is limited though. It is suggested that IALA members develop their own awareness campaigns, tailored for their organizations, or work with a commercial provider of awareness training offering tailored solutions.

Another factor of the human element in cyber security is deliberate sabotage by employees, either because they are unhappy with their employer, or they are blackmailed/offered money by criminals to perform malicious actions. Awareness of these risks is important. An organization's Human Resources department may be able to assist in mitigating against these risks especially in recruiting processes and personnel screening.

There are also technical solutions that help to mitigate risk from human error and malicious action, e.g. procedures that require multiple persons to always be involved or CCTV monitoring.

Specific training may be required for AtoN managers and technicians, VTS operators, supervisors and managers and training should be periodically repeated to keep awareness to the desired level and stay aligned with current cyber threats. Training should address:

- prevention of cyber incidents;
- recognition of cyber incidents and anomalies; and
- how to respond to cyber incidents, both technically and operationally, including what *not* to do.

3.5. INFORMATION SOURCES AND SHARING

Most governments have a cyber security department that shares news on cyber security topics, in particular newly discovered vulnerabilities that are published, along with recommended action if the vulnerability applies to you. Also, many vendors of systems offer cyber-related information for their products. It is good to selectively subscribe to newsletters that offer reliable information on such topics, so to be aware of trends and any new threats.

Information sharing between trusted parties helps organizations to prevent cyber-attacks at an early stage. To get early information on recent or emerging threats with the relevant indicators of compromise (IOCs) and tactics, techniques and procedure (TTPs) help organizations in early discovery of cyber-attacks and feeds an intrusion detection system (IDS) if present.

Furthermore, information sharing between trusted parties about recent experiences with cyber-attacks, discovered vulnerabilities and/or mitigation strategies for example helps others to thwart attacks at an early stage.

This sharing of information is commonly facilitated by Information Sharing and Analysis Centres (ISACs). ISACs are non-profit organizations or cooperatives that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector.

IALA members are encouraged to participate in ISACs relevant for their region and/or sector. A national/governmental cyber security department can often inform about the availability of such ISACs.

4. CONSIDERATIONS FOR ATON

A Marine 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 include:

- 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) and supporting systems, e.g. PNT
- Vessel Traffic Service (VTS)

VTS and Position Navigation and Timing (PNT) are considered 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 an AIS overlay on the Radar, ECDIS and ECS charts but has no physical presence.

AIS AtoN are, in essence, radio messages transmitted via computer programmable radios, which augment a buoy, a beacon, or any other type of AtoN or provide independent data of navigational significance. AIS uses GNSS for position and time information, therefore it shares a GNSS vulnerability with other receivers. AIS AtoN can be used to share Maritime Safety Information such as Application Specific Messages (ASM) and/or data from mounted sensors (e.g. hydrographic).

Administrations/waterway authorities must ensure the integrity of their signals and provide mariners with 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 Information Technology (IT), Operational Technology (OT) and Internet of Things (IoT) enabling with satellite monitoring from almost 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.

4.1. 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 Wi-Fi 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 allows additional access points and potential means for a cyber-attack. Conversely, remotely monitored AtoN offers administrations a method to more quickly identify an AtoN which is not operating as required and/or may have been subject to unauthorized modification by a hostile actor.

The following measures should be taken into consideration:

- 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;
- 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;
- Implement monitoring/detection of unusual behaviour, 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;

- If the AtoN uses GNSS for positioning and/or time synchronization, apply measures to mitigate against jamming and spoofing of GNSS signals. See the chapter “Considerations for PNT”;
- 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 protection measures;
- Whenever feasible, AtoN systems used to conduct maintenance and transmit MSI related to AtoN should use cyber-secure electronics;
- Administrations should encourage public reporting of perceived electronic signal spoofing, jamming, or operation/behaviour 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;
- Implement software/firmware updates and (security) patches on AtoN, but only after thorough acceptance testing; and
- Conduct periodic penetration tests and/or vulnerability scans on (representative) AtoN to validate cyber resilience.

4.2. 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 authorization 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 standardized 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 protects 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.

4.3. COMMUNICATION WITH PHYSICAL ATON

Communication with physical 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:

- Protect wireless management interfaces (Wireless LAN, RF, Bluetooth, Infrared) by disabling them while not in use.
- 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.
- If an AtoN is remotely managed and monitored, apply authentication and encryption on the entire communication link to ensure the 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.

4.4. ATON INFORMATION MANAGEMENT SYSTEMS

Aside from the physical AtoN itself, AtoN may be connected to networks and the 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:

- Identify critical data and systems, network connections and access points. Consider forming a written IT cyber security policy for risk mitigation which incorporates data back-up, continuity of operations planning and restoration management.
- Identify what data requires additional control measures such as Personal Identifiable Information (PII). Standard IT data protection best practices should be implemented in this case.
- Implement and maintain strict authorized user identification and access protection.
- Where feasible use methods such as encryption, data segregation (e.g. by operational region) and or user role permission to protect data.
- Limit the number of IT / OT network connections and data access points to only those necessary for routine and contingency operations.
- 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.
- Where possible, collect and save log files of all (sensor) information from AtoN for at least 180 days to enable (forensic) inspection following abnormal behaviour and cyber incidents.

- If a communication link is established to provide automatic updates to hydrographic systems/ organizations, apply appropriate preventative measures and monitoring to ensure the integrity of the data, for example the use of unidirectional/one-way communication.
- Conduct periodic penetration tests and/or vulnerability scans on AtoN management systems to validate cyber resilience.

5. 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 have 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 (such as S-210, S-212) and to some extent replacing provision via voice-based communication, data integrity becomes a vital focus point. Furthermore, all exchanged and provisioned data (including voice and sensor data) should be fully traceable, i.e. logged and archived as a function provisioned by the VTS system. The integrity and secure storage hereof will be essential within a VTS centre.

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

5.1. GENERAL GUIDANCE FOR VTS

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

- Documentation and procedures are important to ensure consistent implementation and maintenance, in particular security procedures, especially as VTS equipment may be spread over a large geographical area and/or difficult to visit.
- Pay attention to network segmentation[1] 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.
- Well established maintenance procedures contribute to a cyber secure system, especially well tested and timely applied security patches.
- Remote access should be minimized to absolutely necessary access by employees and/or third parties. Authentication and authorization of users and technical monitoring/logging of all remote activity should be implemented and validated. Time restriction in remote access should also be considered.
- Interfaces[2] with systems outside the VTS networks, for example for monitoring and predictive maintenance, should only be implemented after a risk assessment.
- VTS personnel, both operational and technical, should continuously be educated on cyber security awareness and detection of malicious activity within the VTS systems.

1 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.

2 An interface is a communication channel between systems and may both be physical or logical, line a TCP port or rest API.

- Cyber security should be considered when establishing, updating or renewing a VTS system. Moreover, risks introduced by using third party services, as well as private or public cloud services should be included.
- 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.
- 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.

5.2. 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 receivers/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 (e.g. vandalism, break-in, manipulation, disruption) and accidental (e.g. weather, natural disasters). Also, the communication links are more vulnerable, whether these are (buried or open-air) cables or wireless connections.

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

- 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.
- Related to physical security, make sure authorization for entering the site is controlled. Who has the keys? Is it a shared location?
- Implement monitoring/detection tools that not only monitor availability[3] but also data integrity[4]. 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.
- 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.
- 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.
- Apply authentication where possible to be able to validate that data is actually originating from the device or system that it identifies itself as.
- 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.

3 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.

4 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.

- 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.
- Create procedures for fast restoration and/or replacement of sensors.

5.3. 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. These systems 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 core VTS systems that require a different approach than for standard IT systems:

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

The following measures for improving resilience, considering core VTS system's unique properties should be considered:

- 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.
- 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.
- Apply monitoring mechanisms, other than a user login, to validate user actions. Maybe security cameras may be suitable or other biometric identification may be possible. These will not prevent deliberate manipulation but will enable alerting and forensic investigations.
- 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, i.e. by performing background checks.
- Disable all functionalities on VTS systems that is not needed for the VTS operation process. Users should not be able to start any unnecessary application or start an internet browser. Especially all USB devices, other than Human Interface Devices like mice and keyboard, should not work.
- Limit network access to the minimum necessary; Core VTS 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.
- Create procedures for fast restoration and/or replacement of Core VTS systems or have cold spares[5] available. Hot spares[6] are often good for availability but may be hit by cyber-attacks. Cold spares will not be hit.

[5] A cold spare is a spare system that is turned off. It may be installed/configured to replace a live system, or may be factory default.

[6] A hot spare is a running system configured to (instantly) replace a live system or it's functionality. It is also sometimes referred to as a redundant system.

- Awareness should be created amongst VTS personnel to recognize and respond appropriately to cyber incidents with (potential) integrity degradation of VTS information, including traffic image, data communication and voice communication. Training of VTS operators and maintenance staff is recommended to increase this awareness.

5.4. COMMUNICATION

VTS communication systems include VHF communication, AIS messaging and, depending on the specific VTS centre, telephone and other communication means.

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. However, in most cases that will not be an option in the maritime industry.

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

- Deploy methods for detection and localisation of disruptive signals or contract a competent third party to do so. Usually, a technique like triangulation could be suitable. This may assist in quickly mitigating disruption and malicious transmissions.
- Implement technical measures or procedures to disable any disruptive sources of radio signals. For instance, AIS/NAVTEX may be disabled as a source for VTS systems in case of disruption or spoofing, if instead radar is available. VTS operators should be able to perform their duties with only radar information.
- 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.
- Have alternative communication methods available. Telephone or megaphone may replace VHF in emergency situations and navigational warnings (MSI) 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.
- While there are initiatives to implement authentication of messages in various MSI systems, there is currently no standardized 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.
- Monitor for unusual messages; commercial systems are available to monitor for spoofing and jamming, especially in AIS.
- Where communication is digitalised, it is often based on IP with the application of web services. In those cases and in particular for the provision of S-100 based data services, the SECOM (IEC 63173-2) standard should be applied and additional measures from IT and OT standards, like best practices for security monitoring, should be considered.
- As resources allow, implement multiple different dissemination systems that provide similar information to enable comparison. Provide readily discoverable methods for mariners to validate information when in doubt (e.g. human verification via VHF communications to the authoritative source).

6. CONSIDERATIONS FOR PNT

Today's vessels and many 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. RNSS which are based on similar technology as GNSS face the same vulnerabilities. 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 available.

Cyber security includes aspects such as GNSS jamming (likened to a denial of service) and spoofing (likened to data manipulation). The International Maritime Organization'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**Error! Reference source not found.**:

> *"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 related equipment underscores 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.

PNT is used within AtoNs to support positioning and timing aspects such as synchronising lights and communications. For example, within AIS systems, 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.

PNT data can also be used in areas where it may not immediately be obvious. During GPS jamming trials conducted by a GLA buoy tender, it was discovered by accident that the main GPS receiver feeding the bridge also provided time throughout the vessel. For additional reference, the resilient PNT demonstration for ACCSEAS project video link is under the IALA test bed area for the ACCSEAS project which is found at: https://www.iala-aism.org/technical/planning-reporting-testbeds-maritime-domain/accseas/

PNT information is subject to natural and deliberate interference (jamming) and data manipulation (spoofing). GNSS vulnerability is common across various different satellite constellations that broadcast on similar frequencies and so are likely to be affected by the same interference source(s). It may not be possible to remove the risk of GNSS interference, whether natural or man-made. As referenced in Chapter V of IMO Safety of Life at Sea (SOLAS) convention, 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. This provision can be interpreted to refer to both GNSS and traditional physical AtoN, which are in and of themselves a resilient back-up to GNSS disruption.

Available measures to mitigate against PNT spoofing and jamming are:

- Consider in advance what potential impacts of data manipulation or denial may look like to help identify when such an event is occurring.
- Monitor – 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.
- Implement GNSS constellation authentication services.
- Utilize integrity warning services provided by Satellite Based Augmentation Systems (SBAS) and/or Ground Based Augmentation Systems (GBAS).

- Mitigate risk of disruption - To mitigate such events on critical ports and waterways, multiple and where possible dissimilar position solutions should be employed as part of a system of systems approach. This may include sufficient physical ATON to enable a continuity of port/waterway operations where the degree of risk/consequence of GNSS disruptions warrants.
- Encourage use of antennas that are shielded from terrestrial based jamming and spoofing signals. 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, which may assist in effective blocking of jamming or spoofing signals, which are mostly sent from the ground.
- Encourage mariners to use physical AtoNs to check the reliability of PNT information received and report discrepancies to the responsible authority.

7. KNOWN VULNERABILITIES IN WIRELESS COMMUNICATION

The maritime industry relies heavily on wireless communication. Many wireless communication systems do not implement authentication (authentication, in the context used here, is the ability to ensure that a message or file is authentic). Most well-known are VHF voice communication and AIS, but it applies to many GMDSS technologies and other wireless communication used in the maritime industry. They offer no technical means to validate that the source of a message is actually the sender it identifies itself as.

Authentication of these means of communication requires manual (human) verification.

8. FURTHER READING

[1] IALA Guideline G1111 Establishing Functional Performance Requirements, 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.

[2] IALA Recommendation R1019 Provision of Maritime Services in the context of e-Navigation in the domain of IALA

- Covers general aspects of digitalisation: Resilience, security, identity and authentication by design
- Availability, Integrity, Confidentiality

[3] IALA Guideline G1157 Web Service based S-100 data exchange

- Guidance on implementing MS with S-100 data
- Recommends using IP and TLS in combination with PKI
- Local certificate store -> offline PKI
- Sign data (+timestamp to avoid replay attacks)

[4] 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) (standard)

- 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

[5] IALA Guideline G1161 The evaluation of platforms for the provision of Maritime Services in the context of E-navigation

- Provides a framework to evaluate technologies/platforms for MS

- Covers basic aspects of Cyber Security: Authentication, Authorization, Robustness, Efficiency, Confidentiality, Integrity, Availability, Non-repudiation

[6] 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

[7] IALA Guideline G1018 Risk Management

- IALA Risk Management processes