No. 163 (Sep 2018)

Remote Update / Access

1 Introduction

1.1 General

Information and communications technology (ICT) is revolutionising shipping, bringing with it a new era – the ‘cyber-enabled’ ship. Many ICT systems on-board ships connect to remote services and systems on shore for monitoring of systems, diagnosis and remote maintenance, creating an extra level of complexity and risk. ICT systems have the potential to enhance safety, reliability and business performance, but there are numerous risks that need to be identified, understood and mitigated to make sure that technologies are safely integrated into ship design and operations.

This recommendation on Remote Update/Access aims to establish recommendations for control over remote access to onboard Information Technology (IT) and Operation Technology (OT) systems. Additionally, where remote maintenance is used clear procedures and protective measures, which include mechanisms for validating updates prior to their deployment and simply reverting to earlier revisions in the case of corruption, should be adopted.

1.2 Objective

This recommendation is intended to provide minimum recommendations/procedures for remote Update/Access.

1.3 Scope

This recommendation applies to new construction ships, and may be used as guidance for existing ships, which connect to remote services and systems on shore for: monitoring, diagnosis and remote maintenance.

These procedures are supplemental to IACS UR E22 “On Board Use and Application of Computer based systems” which apply to the use of computer based systems which provide control, alarm, monitoring, safety or internal communication functions which are subject to classification requirements extend to systems which may otherwise not be subject to classification requirements but which, when integrated with or connected to classed equipment or equipment with an impact on safety, can expose the vessel to cyber-risks and, have an impact on the safe and secure operation of the ship may be applied to additional systems at the request of the owner

2 References

For the purpose of application of this recommendation, the following standards can be used:

- UR E22 – On Board Use and Application of Computer based systems
- NIST SP 800 series – Computer security
- BIMCO – The Guidelines on Cyber Security onboard Ships
- ANSSI – Cyber security Assessment and protection of ship
- ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security controls

3 Remote Access

3.1 Ship to shore interface

For computer based systems on board that could be critical for the safety of navigation, power and cargo management (e.g. those performing functions such as:

- engine performance monitoring
- maintenance and spare parts management
- cargo, crane and pump management
- voyage performance monitoring)

the transmissions of data which can be critical to the safety of the ship should be protected against unauthorized access.

The system integrator, producers and service providers should have an updated cyber security company policy, which includes training and governance procedures for accessible IT and OT onboard systems.

OT should have the necessary capabilities to mitigate against the risks of remote access / update. The equipment should have the capability to terminate a connection from the on board terminal and immediately revert to the known and uncorrupted state.

Additionally, the Company should implement appropriate procedures for managing remote access / update.

Systems should have characteristic necessary to prevent interruptions to remote access sessions interfering with the integrity and availability of OT or the data OT uses.

The shipowner should include in contracts with system integrator, producers and service providers clauses to requiring evidence of their internal governance for cyber network security.

3.2 Configuration of network devices such as firewalls, routers and switches

Networks, that provide suppliers with remote access to allow upload of system upgrades or perform remote servicing of navigation and other OT system software on onboard, should be controlled (i.e. designed to prevent any security risks from connected devices by use of firewalls, routers and switches (reference IEC 61162-460)). Shoreside external access points of such connections should be secured to prevent unauthorised access.

3.3 Policy and procedures

The shipowner should establish policies and procedures for control of remote access to onboard IT and OT systems. Clear guidelines should identify who has permission to access, when they can access, and what they can access. Any procedures for remote access should include close co-ordination with the ship's master and other key senior ship personnel. Additionally, any remote access should be initiated and confirmed by a responsible person onboard, and it should be possible at all times to terminate the remote connection by the responsible personnel onboard.

All remote access occurrences should be recorded for review in case of a disruption to an IT or OT system. Systems, which require remote access, should be clearly defined, monitored and reviewed periodically.

Furthermore, the procedures for activities on board should include steps to:

- Document allowed methods of remote access to the information system;
- Establish usage restrictions and implementation guidance for each allowed remote access method;
- Monitor for unauthorized remote access to the information system;
- Authorize remote access to the information system prior to connection; and
- Enforce requirements for remote connections to the information system.

Additionally, this policy and procedures for control over remote access should at least define:

- Roles and responsibilities of:
  - Shipowner,
  - onboard personnel,
  - shoreside personnel,

- Awareness and training (security awareness training, role-based security training, and training records) – should be tailored to appropriate level for:
  - onboard personnel,
  - shoreside personnel who support the management and operation of the ship,

- Identification and Authentication:
  - user identification and authentication,
  - device identification and authentication,
  - identifier management,
  - authenticator management,

- Access control, IT/OT security measures:
  - account management,
  - separation of duties,
  - least privilege,
  - session lock,
  - information flow enforcement, and
  - session termination,

- Configuration management:
  - baseline configuration,
  - configuration change control,
  - security impact analysis,
  - least functionality, and
  - software usage restrictions,

- Controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance
- Records management monitoring, the reinforced control of remote maintenance and information sharing,
- The outline of a plan ensuring the ship's operational continuity,
- The preparedness for any foreseeable resulting dangerous situations.

Policy and procedures should be documented, maintained, and made available to all users who need them.

No. 163 (Cont)

4 Remote maintenance

IT or OT support personnel will often need remote maintenance access to quickly provide assistance to users without having to physically go to the user location (i.e. on board).

Clear procedures and protective measures shall be implemented to regulate this type of operations. The Owner company's policy should define the limits of this remote maintenance.

Where remote maintenance is used, access monitoring and control must be reinforced.

A maintenance plan should be developed by the Owner, and made available to all stakeholders involved.

The Owner should implement the following safeguards for remote maintenance:

- A permit to work system, like the one in use for hot work on board.
- The connection for remote maintenance should always be initiated by the local IT or OT system. This can be accomplished by having the target systems call the remote maintenance location or by using an automatic call-back function.
- All activities during remote maintenance should be monitored by in-house trained and designated IT or OT personnel. It should be possible at all times to cancel remote maintenance locally.
- The external maintenance personnel should authenticate when beginning the maintenance session. Passwords should not be transmitted in unencrypted form. If systems cannot provide encryption, tunneling traffic through an encrypting virtual private network (VPN) should be adopted.
- To the extent possible, remote access credentials should be personal, not shared (e.g. by a vendor's technical support team). If this is not possible, one-time passwords should be used and reset after the session ended.
- Procedures should be in place to ensure the remote maintenance process is ended safely, once completed.
- Remote maintenance shall be logged. Logging information should at least contain the start and end time, persons involved during the remote maintenance and content of the maintenance.

Furthermore, the Owner should consider the following additional functions for remote maintenance of the computer based system on board:

- Activation of a lock-out period in the event of failed access attempts.
- Blocking of the remote maintenance feature during normal operation and express approval for a precisely defined period of time.
- Maintenance personnel should not be granted full administrator rights and should only have access to the data and directories requiring maintenance; graduated administration of rights shall be implemented.
- When possible, maintenance personnel should have a user ID for performing all maintenance work that is separate from their regular, non-privileged user ID.
- If the connection to the remote maintenance location is disrupted for some reason, access to the system shall be terminated by an automatic logout function.

No.
163
(Cont)

5 Validating Updates

The Owner should ensure that the following recommendations are taken into account:

1. Patches and updates should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated. They should also be prevented from installation unless signed with recognized and approved certificates.

2. Where practicable, malicious code should be detected and removed by appropriate scanning software. To enable detection of newer malicious code, the scanning software should always be kept up to date.

3. Data validation plan for updates needs to be established. A data validation plan describes procedures for checking the updates for signs of corruption before the update process, including the number and types of validation, criteria and action recommendation.

4. Robust procedures for validating updates prior to their deployment should be established, including the ability to revert simply to earlier revisions in the case of corruption.

5. The following consideration should be included in the procedure for validating updates:
   - Remote update should only be carried out by authorised personnel;
   - Update signatures ensure the integrity and authenticity of the update;
   - Update data transfer protection (encryption or cyclic redundancy check - CRC) to prevent exposure of software image;
   - Update data decryption or CRC;
   - Malware scanning;
   - Update data validation ensures update integrity;
   - Post-update verification ensures that the system is performing appropriately.

6. Rollback strategy should be determined prior to updating process and previous versions of software should be stored and available to be installed in emergency situations. The system should have the ability to revert simply to earlier revisions in the case of corruption.

7. A log should be provided for all information needed to successfully audit system activity.

8. Software and update versions should also be stored and log which records the:
   - versions that are in use,
   - versions that were in use, and
   - versions that are stored.

9. The procedure for validating updates should be documented and made available to all stakeholders involved.

End of
Document