No. 164 Communication and Interfaces

(Nov 2018)

1 Introduction

1.1 General

Shipboard information flows enable the automation systems found in shipboard Information and Operational Technology (IT/OT). Communications among components, and the system interfaces and protocol converters that allow those components to exchange information, are critical to systems and ship success.

Because communications capabilities and flows enable operations in the IT/OT supporting crews and ship systems, these functions must be safeguarded to ensure proper, authorized operations. Communications faults or failures may cause operational disconnects, improper decisions or actions. This is especially true for highly-automated vessels or systems, and their communications paths must be kept secure for the safety of ship, crew and the environment. All these communications and interfaces increase the possibility of computer system faults and extend the fault from one system to another system.

It is necessary to consider recommendations relating to the permitted and prohibited interconnections, regulating and managing access across interfaces, potential protective functions to safeguard external and internal protective functions and testing of communication paths for functional and security purposes. This Recommendation on Communication and Interfaces aims to establish recommendations for control over communication paths and connections to onboard Information Technology (IT) and Operation Technology (OT) systems.

1.2 Objective

This Recommendation is intended to provide minimum recommendations/procedures for Communications and Interfaces protection and management in order to:

- Develop criteria that help define which interconnections / interfaces are permitted or prohibited.

- Develop methods for safe communication and interface between computer-based systems.

- Develop recommendations for testing of communication paths for functional and security purposes.

- Develop recommendations relating to the application of suitable logs for periodic validation and continuous update of all routes into the systems in order to assess the acceptability of modifications and review appropriate procedures for addressing the associated risks.

1.3 Scope

This Recommendation provides guidance on communication paths and onboard IT/OT systems for existing ships that provide connections to computer-based services and systems ashore, and to new construction ships with integrated systems provided by the builder or integrator.

Shipboard equipment and associated integrated systems to which these recommendations

No. 164 (Cont)

apply can include, but are not limited to:

- Ship control networks;
- Critical systems that may not always be connected (e.g., navigation systems);
- Propulsion networks;
- Safety-critical systems;
- Cargo management systems and networks;

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
- IEC 61162 – Maritime navigation and radio communication equipment and systems – Digital interfaces. Part 450: Multiple talkers and multiple listeners – Ethernet interconnection. Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security
- IEC 62443-3-3 Industrial communication networks – Network and system security. Part 3-3: System security requirements and security levels
- ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security controls
- ISO 16425 – Ships and marine technology – Guidelines for the installation of ship communication networks for shipboard equipment and systems

3. Policy and procedures

The ship-owner should establish policies and procedures for control of communications and system interfaces to onboard IT and OT systems, including communications methods originating from company or affiliated organization shore side locations. Clear guidelines should identify who has permission to access, when they can access, and what they can access through shipboard communication and networking paths. Policies must implement company or organizational security and privacy requirements, and procedures should be developed to implement the policies, working in close collaboration with ship masters, officers and crews.

Access policy for any communications or system interfaces should include

- Processes by which the company will manage and inventory assets, especially in use of Recommendation PC17009 of this series;

- Processes by which the company will manage personnel and machine identities as part of access management and control of assets;

- Documentation and training of systems, their performance and operations, and how networks and communications bring systems to higher levels of performance for the crews;

- Failure modes and indicators of problematic behaviors in case performance or safety is affected;

No. 164 (Cont)

- Usage restrictions and controls put into place to ensure proper uses are encouraged, and improper uses are prevented; and

- Periodic training for care, diligence and operational habits and safeguards around the communications paths that serve shipboard systems.

Additionally, this policy and procedures for control over communications or system interfaces should at least define:

- Roles and responsibilities of:
  - Ship-owner,
  - Onboard personnel,
  - Shore side personnel, and
  - Personnel escorting and monitoring third party vendors or service providers.

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

Company policy and procedures should be documented, maintained, regularly trained to crews and company personnel, and made available to all personnel.

4 Communications integrity and content protection

The owner or operator should manage and monitor the normal performance of systems connecting to shipboard data paths and communications nodes and also check their activity and health for data integrity, considering that sensors and reporting systems may be installed in areas detrimental to data (e.g. areas with high electromagnetic interference (EMI); with open access to sea and sun; and sometimes with potential for human interference or mischief).

4.1 System integrity

Asset integrity – managing systems to ensure they perform and operate as expected and as required – is vital to gathering, using and operating with data from sensors and systems. If sensors are critical to emissions or discharge compliance reporting, it's important to ensure those sensors' output is accurate and 'clean' for the owner and crew to have best results. This includes the transmission paths, access interfaces (human-usable or machine-accessible), and the systems that communicate with such sensors. Communication path integrity, including the protection of communications and transmission lines or links, is also important to understand and maintain if the owner and crew are to have the best opportunity to gain accurate data from the reporting devices or systems.

Personnel access to communication paths and interface devices can challenge the integrity and credibility of data originating with systems located on those communications paths. The owner or operator should assess relative risks associated with systems that have exposed communications paths, open data links or available interfaces to determine if prudent action might include concealing or protecting the paths, links or interfaces from potential interfering influences.

No. 164 (Cont)

4.2 System fault tolerance

The ship's communications systems may not be available continuously while the ship is operating. When installing new systems, the owner and operator must both remain aware of those systems critical to operational safety, and their communications requirements and dependency on other systems by updating systems inventory list (detailed information regarding inventory list is available in Recommendation # 9 [section 4]).

Fault tolerance is important for every safety-critical and operationally-critical system aboard. The other Recommendations in this series emphasize asset inventory, backup procedures, and training to alternative methods of operation, among other recommended practices; these factors are especially important if communications links fail and cannot support critical system operations.

5 Security and monitoring

The owner should consider monitoring methods that increase confidence in data path quality and also increase likelihood of recognizing interference, nuisances, and mischief or illegal activity on networks.

- Transmission paths should be protected from routine shipboard environment (Nature), shipboard operation and potential random damage, and from human contact.

- Physical connections between systems and networks should be marked for the network to which they connect, and labelled with 'tell-tales' that indicate when connections have been broken or changed (e.g., frangible tapes applied to connectors).

- Test Access Points (TAP) or Switch Port Analyzers (SPAN) connections to the ship's main switch may provide valuable information about transmission path content and bandwidth usage, such that the owner or operator may adjust usage for best economy while managing security across the SATCOM path.

- Each individual enclave or segment of the ship's networks should have its own monitoring methods implemented, matching the amount of effort and data collection to the relative criticality, importance to safety, or vital contribution to ship operations or safety of that enclave or segment.

- Non-critical systems, such as sensor networks put into place for performance monitoring, should be segmented by themselves to minimize the potential for interference with critical systems, and to more easily manage the devices and their data flows.

- Security and performance monitoring complement each other, when properly implemented. Either can indicate system faults or errors, whether through software fault, system errors, or human errors or deliberate actions. It's important for the owner and operator to understand how to read logs and reports to determine where possible flaws in operations can point to impending problems for ship or crew.

End of Document