**IACS UR E27 Guidance**

A person in a black hoodie

AI-generated content may be incorrect.

The [International Association of Classification Societies](https://iacs.org.uk/) (IACS) have introduced two new Unified Requirements (UR);

E26 “Cyber resilience of ships” and E27 “Cyber resilience of on-board systems and equipment”.

These apply to nearly all ships contracted for construction on or after 1st July 2024.

Contents

[Introduction 3](#_Toc192714843)

[Definitions: 5](#_Toc192714844)

[1.2.1 Terms and definitions 5](#_Toc192714845)

[Ship Cyber Security Levels 7](#_Toc192714846)

[Remote Access 8](#_Toc192714847)

[The Ship Asset Inventory is to contain all systems and devices 12](#_Toc192714848)

[SOC AND SIEM 14](#_Toc192714849)

[5.5.2 Account Management 14](#_Toc192714850)

[5.5.3 Installation and Upgrade 15](#_Toc192714851)

[7.0 Configuration Management 15](#_Toc192714852)

[5.6 Cloud Computing Management 15](#_Toc192714853)

# Introduction

The IAC 27 notation outlines specific cybersecurity requirements for vessel networks, focusing on the following areas:

1. **Risk Assessment and Management:**
   * Conduct a thorough cybersecurity risk assessment to identify vulnerabilities, threats, and potential impacts on vessel operations.
   * Develop a risk management plan to mitigate identified risks.
2. **Network Segmentation:**
   * Implement network segmentation to isolate critical systems (e.g., navigation, propulsion, and control systems) from non-critical systems (e.g., passenger Wi-Fi).
   * Ensure that communication between segments is controlled and monitored.
3. **Access Control:**
   * Enforce strict access control policies to limit access to critical systems and data.
   * Use strong authentication mechanisms (e.g., multi-factor authentication) and role-based access controls.
4. **System Hardening:**
   * Apply security patches and updates regularly to operating systems, software, and firmware.
   * Disable unnecessary services, ports, and protocols to reduce the attack surface.
5. **Monitoring and Detection:**
   * Implement continuous monitoring of network traffic and system activities to detect anomalies or potential cyberattacks.
   * Use intrusion detection systems (IDS) and intrusion prevention systems (IPS) to identify and respond to threats.
6. **Incident Response:**
   * Develop and maintain an incident response plan to address cybersecurity incidents effectively.
   * Conduct regular drills and exercises to test the effectiveness of the response plan.
7. **Training and Awareness:**
   * Provide cybersecurity training for crew members and shore-based personnel to raise awareness of cyber risks and best practices.
   * Ensure that personnel understand their roles and responsibilities in maintaining cybersecurity.
8. **Compliance with International Standards:**
   * Ensure that the vessel's cybersecurity measures comply with relevant international standards, such as the **IMO's Resolution MSC.428(98)** (cybersecurity risk management in safety management systems) and **IEC 62443** (industrial communication networks).
9. **Documentation and Auditing:**
   * Maintain detailed documentation of cybersecurity policies, procedures, and risk assessments.
   * Conduct regular audits to verify compliance with the IAC 27 requirements.

**Why IAC 27 is Important for Vessel Networks**

Maritime systems are increasingly interconnected and reliant on digital technologies, making them vulnerable to cyberattacks. Cyber incidents can disrupt vessel operations, compromise safety, and lead to financial losses or environmental damage. The IAC 27 notation provides a structured approach to managing these risks and ensuring the resilience of vessel networks.

# Definitions:

1.1.1.3 The on-board CBSs to which the requirements herein apply are the on-board Operation Technology (OT) systems using data to monitor or control physical processes of ships and devices that may be vulnerable to cyber incidents and, if compromised, could lead to dangerous situations for human safety, safety of the ship and/or threat to the environment.

1.1.1.7 **The networks considered in the Guidelines consist of the applicable systems and the networks supporting their stable, secure and reliable operations, including computing, security, storage, communication and network devices**.

### 1.2.1 Terms and definitions

1.2.1.1 **Access Control**: Selective limiting of the ability and means to interact with a system, to use system resources to handle information, to gain information and knowledge the system contains or to control system components and functions.

1.2.1.2 **Attack Surface**: *The set of all possible points where an unauthorized user can access a system and extract data. The attack surface comprises two categories: digital and physical.* **The digital attack surface** encompasses all the hardware and software that connect to an organization's network. These include applications, codes, ports, servers and websites. **The physical attack surface** comprises all endpoint devices that an attacker can gain physical access to, such as desktop computers, hard drives, laptops, mobile phones, removable drives and carelessly discarded hardware.

1.2.1.3 **Authentication**: Provision of assurance that a claimed characteristic of an identity is

1.2.1.4 **Compensating Countermeasure**: An alternate solution to a countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.

1.2.1.5 **Computer Based System** (CBS): A programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBS on-board include IT and OT systems. A CBS may be a combination of subsystems connected via network. CBS on-board may be connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBS and/or other facilities.

1.2.1.6 **Computer Network**: A connection between two or more computers for the purpose of communicating data by means of agreed communication protocols.

1.2.1.7 **Cyber Security:** Characteristics of *confidentiality, integrity and availability* of information stored, transmitted and processed in a cyber environment.

1.2.1.8 **Cyber Attacks:** Any type of offensive operation that targets IT and OT systems, computer networks, and PC devices and attempts to access, compromise or destroy company and/or Page 3 Guidelines for Ship Cyber Security ship systems and data.

1.2.1.9 **Cyber Incident:** An act or incident that affects the integrity, availability and/or confidentiality of a system caused by malicious threats in breach of security policies.

1.2.1.10 **Cyber Resilience:** The capability to reduce the occurrence and mitigating the effects of cyber incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the ship and/or threat to the environment.

1.2.1.11 **Defense in Depth**: Information security policy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

1.2.1.12 **Demilitarized Zone (DMZ)**: A physical or logical perimeter network segment that contains and exposes an organization's external-facing services to an external network. Its purpose is to enforce the internal network's security policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

1.2.1.13 **Denial of Service (DoS):** A type of cyber attack designed to prevent legal and authorized users from accessing information typically by means of server buffer overflow. Distributed DoS refers to a DoS through controlling multiple computers and/or servers by a cyber attacker.

# Ship Cyber Security Levels

**1.3.1 Ship Cyber Security Levels and Class Notations Ship Cyber Security Levels**

1.3.1.1 S/N There are five ship cyber security levels. Ship Cyber Security Levels Level

Table 1.3.1.1 Defensive Capability

1. **SL0 Defense capability meeting minimum security requirements (UR E26) 2**
2. **SL1 Defense against occasional cyber incidents 3**
3. **SL2 Defense against cyber incidents initiated with a small amount of resources 4**
4. **SL3 Defense against cyber incidents initiated with a great amount of resources 5**
5. **SL4 Defense against well-organized and targeted cyber incidents**

A close-up of a document

AI-generated content may be incorrect.

A close-up of a document

AI-generated content may be incorrect.

### Remote Access

A white and black text on a white background

AI-generated content may be incorrect.

2.3.1.5 Restricted data flow

A list of information on a computer

AI-generated content may be incorrect.

A close-up of a checklist

AI-generated content may be incorrect.

A close-up of a document

AI-generated content may be incorrect.

A close-up of a text

AI-generated content may be incorrect.

A black and white text on a white background

AI-generated content may be incorrect.

A close-up of a document

AI-generated content may be incorrect.

A close-up of a security requirements

AI-generated content may be incorrect.

A close-up of a document

AI-generated content may be incorrect.

A document with text on it

AI-generated content may be incorrect.

A close-up of a document

AI-generated content may be incorrect.

A close-up of a document

AI-generated content may be incorrect.

## The Ship Asset Inventory is to contain all systems and devices

A diagram of a ship asset inventory

AI-generated content may be incorrect.

(3) Network Topology Diagram, which is a block diagram that identifies the physical or logical connections between the various on-board CBSs and between the CBSs and external devices or networks. The Network Topology Diagram is to be able to clearly mark the security zone and the physical location of each CBS.

(4) The Manual of Network Security Design shall at least include the following:

① Clearly identify the security zone and each CBS contained in the network topology diagram;

② Describe the security zone and the CBS contained therein of the network topology diagram;

④ Describe the communication and characteristics between the security zone and untrusted networks, including serial communication and IP-based communication purposes and characteristics (such as protocol and data flow), zone boundary devices, and traffic allowed through zone boundaries (such as firewall rules);

⑬ The effectiveness of network isolation should be demonstrated by disconnecting all networks that cross the boundaries of the security zone, demonstrating that the CBS in the security zone can maintain adequate operational functionality without network communication with other security zones or networks;

⑤ Wireless network design, explaining the wireless network design scheme, including how to achieve a separate security zone, zone boundary equipment and the traffic allowed to pass through the zone boundary (such as firewall rules);

⑥ Physical access control measures, for the CBS that needs immediate access, if its human machine interface is already located in the physical access control area, there is no need to carry out identification and authentication. Such equipment shall be described in this document;

⑦ Malicious code protection mechanism, outline the malicious code protection mechanism used by each CBS, for the installation of anti-malicious code software for CBS, should explain how to keep the software updated ⑧ Describe remote access control and communication. Each CBS shall be identified to determine whether it can be accessed remotely or communicate with untrusted networks through secure zone boundaries and, if so, shall indicate compliance with the relevant requirements of Chapter 4, Paragraphs 4.3.15 and 4.3.16 of the guidelines;

⑮ **When connecting to an untrusted network**, the relevant requirements applicable to Section 3 of Chapter 2 of the Guidelines for connecting to an untrusted network should be met and can be analyzed *using a protocol analysis too*l;

⑯ **When remote users conduct remote access**, the following should be verified:

a) Multi-factor identity authentication;

b) Limit the number of login failures. When a remote user establishes a session, there should be a prompt message;

c) Remote connection after confirmation by the person in charge of the ship;

d) The remote connection may be terminated manually by the personnel on board, or automatically after a period of inactivity;

e) The remote session should form an audit log, the log content is referred to Chapter 2, Section 3, Article 2.3.1.2 (8) of the Guide; f) Relevant suppliers shall provide operating manuals and procedures.

### SOC AND SIEM

The management activities of CBS and network anomalies, including the discovery and identification of abnormal activities, the examination of security auditable records, and the description or procedure for detecting events, can be managed together with the incident response;

⑨ Test and regular maintenance management of security functions in CBS and network; ⑩ Incident response plan shall at least:

a) Describe who, when and how to respond to cyber incidents;

b) Describe procedures or instructions for local/manual control;

c) Describe procedures or instructions for isolating security zones;

d) Describe the expected behavior of CBS in the event of a network incidents.

⑪ Incident recovery and backup plan shall including at a minimum:

a) Describe who, when, and how to recover from a cyber incident;

b) A specified backup plan, including backup frequency, backup maintenance and testing, taking into account acceptable downtime, alternative controls, vendor support and the importance of CBS; c)

5.1.2.3 Procedure manual for performing backup, shutdown, reset, restore and restart of CBS.

### 5.5.2 Account Management

(1) Different roles are to be assigned for the management and use of network and application systems, and the responsibilities and privileges of each role are to be clarified;

(2) Account application, account establishment and account deletion are to be controlled, and the accounts and access privileges are to be regularly reviewed. Users are only allowed access to networks and network services that they are explicitly authorized for use, and the assignment and use of privileges are to be restricted and controlled.

### 5.5.3 Installation and Upgrade

(1) Devices and software are to be installed, configured, updated, upgraded and patched by trained and appropriately authorized personnel. The device and software installed are to be approved and a log is to be generated after successful operation. The installation, configuration and operation manuals are to be formulated, and the security configuration and optimized configuration are to be carried out according to the manuals;

(2) Vulnerabilities and patch releases are to be closely monitored, software installation, upgrades and patch management are to be strictly enforced, and professional technical institutions are to be entrusted with security assessment and testing verification before software upgrades and patch installation for critical OT systems;

(3) Before installation, configuration, renewal, upgrade and patching, a plan is to be formulated to restore when necessary.

### 7.0 Configuration Management

Basic configuration information is to be recorded and saved, including network topology, software/components installed on each device, version and patch information of software/components, configuration parameters of each device or software/component, etc.;

(2) The change of basic configuration information is to be included in the scope of change, the change of configuration information is to be controlled, and the basic configuration information base is to be updated in time.

### 5.6 Cloud Computing Management

5.6.1 A confidentiality agreement is to be signed with the cloud service provider who is required not to disclose the cloud service customer data.

5.6.2 The security incident information or security threat information of the supply chain is to be communicated to the cloud service customers in a timely manner.

5.6.3 Important changes of suppliers are to be communicated to cloud service customers in a timely manner, and the security risks caused by the changes are to be evaluated and measures are to be taken to control the risks.

5.6.4 The selection of O&M locations for the cloud computing platform and the implementation of O&M operations are to take into account the regulations of regulatory authorities and relevant organizations.