Introduction

In today's increasingly interconnected maritime industry, cybersecurity has become a critical concern for ship-owners, surveyors, and auditors alike. Modern ships rely heavily on integrated digital systems for navigation, communication, cargo management, and machinery control, making them potential targets for cyberattacks.

As cyber, threats evolve in sophistication and frequency, the risks to vessel safety, environmental protection, and commercial operations have grown significantly. Regulatory bodies, including the IMO, have responded by introducing requirements for managing cyber risks as part of the ship's Safety Management System (SMS).

Consequently, understanding and implementing robust cybersecurity measures is now an essential component of safe and compliant vessel operation.

In this document, a list of onboard equipment that has been discussed by various IMO bodies as being at risk of cyberattacks has been compiled:

Shipboard Systems & Equipment to be Included in Ship Cybersecurity Plan

Bridge Systems

- ECDIS (Electronic Chart Display and Information System)
- GPS and GNSS receivers
- AIS (Automatic Identification System)
- Radar and ARPA systems
- VDR (Voyage Data Recorder)
- Integrated Navigation Systems (INS)
- BNWAS (Bridge Navigational Watch Alarm System)
- Autopilot systems

Communication Systems

- SATCOM terminals (Inmarsat, VSAT, Iridium, etc.)
- GMDSS equipment
- Ship-to-shore communication systems (email, fax, internet access)
- Crew and passenger internet services
- Internal shipboard LAN/Wi-Fi networks

Cargo Management Systems

- Cargo loading and stability software
- Ballast Water Management System (BWMS)
- Tank monitoring and valve control systems
- Integrated cargo control systems on tankers and gas carriers

Machinery and Power Management Systems

- Engine control systems (e.g., MAN, Wartsila engine automation)
- Power Management Systems (PMS)
- Auxiliary system controls (pumps, compressors, etc.)
- Alarm Monitoring and Control Systems (AMCS)

Safety Systems

- Fire detection and suppression systems
- Flooding detection systems
- Emergency shutdown systems
- Safety PLCs (Programmable Logic Controllers)
- Security monitoring systems (CCTV, access control)

Propulsion and Steering Systems

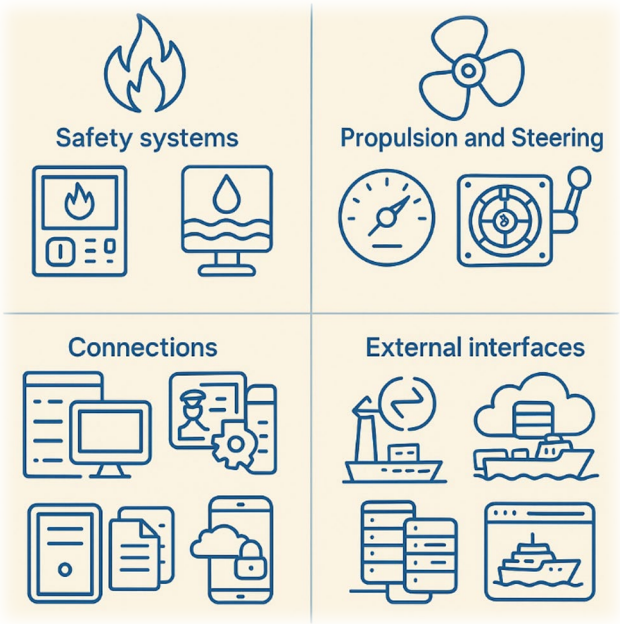
- Propeller pitch control systems
- Shaft RPM monitoring
- Steering gear control systems
- Thruster controls

Access and Administrative Systems

- Shipboard IT infrastructure (servers, switches, routers)
- Email and administrative systems (used by crew and officers)
- Shipboard applications (e.g., PMS software, HR systems)
- Portable devices (USBs, laptops, tablets)
- Remote access platforms for shore-based maintenance or diagnostics

External Interfaces

- Connections to shore-based maintenance systems
- Ship-port data exchange systems (e.g., Just-In-Time arrival, port clearance)
- Cloud-based platforms or remote monitoring services
- Online voyage and performance data submission systems



Threats concerning the equipment

Bridge Systems (e.g., ECDIS, GPS, AIS, Radar)

- **GPS Spoofing or Jamming**: Misleading ship's navigation position or causing loss of signal.
- **ECDIS Malware Infection**: Unauthorized chart manipulation or software corruption.
- **AIS Message Injection**: Sending false traffic info (e.g., ghost ships, fake collision alerts).
- **Radar Display Manipulation**: Creating false echoes or suppressing real targets.

Communication Systems (e.g., SATCOM, GMDSS, Email)

- **Phishing Emails**: Crew receives malicious emails leading to malware infection.
- **Unauthorized Remote Access**: Weak passwords on satellite terminals exploited.
- **Denial of Service (DoS)**: Disrupting SATCOM services, cutting off communication.
- **Man-in-the-Middle Attacks**: Interception of data between ship and shore.

Cargo Management Systems

- **Load Plan Manipulation**: Unauthorized access leads to unsafe cargo distribution.
- **Valve/Pressure Control Override**: Attackers control cargo or ballast tanks.
- **Ransomware on Cargo Software**: Freezes access to critical cargo management tools.

Machinery and Power Management Systems

- **PLC/SCADA System Hacking**: Modifies engine or generator behavior remotely.
- **Sensor Spoofing**: False readings from temperature, pressure, or flow sensors.
- **Command Injection**: Malicious code alters engine parameters or disables alarms.

Safety Systems

- **False Alarms or Alarm Suppression**: Attack disables fire detection or causes alarm floods.
- **Disabling Emergency Shutdown Systems**: Preventing the system from activating in emergencies.
- **CCTV Feed Tampering**: Disabling or manipulating onboard video surveillance.

Propulsion and Steering Control

- **Autopilot Hijack**: Unauthorized commands change course.
- **Steering System Override**: Causes loss of steering or erratic behavior.
- **Speed Control Manipulation**: Alters propeller pitch or engine RPM remotely.

Administrative and IT Systems

- **Data Theft or Leakage**: Extraction of crew data, HR files, or operational logs.
- **Ransomware Attacks**: Encrypting administrative documents and demanding payment.
- **Infected USB Devices**: Crew unintentionally introduce malware via portable media.

External Interfaces (e.g., Port, Remote Maintenance)

- **Compromised Vendor Access**: Vendors with remote login can introduce malware.
- **Port Data Manipulation**: False reporting of ETA, cargo data, or clearances.
- **Insider Threats**: Shore-based personnel misusing access privileges.

***