INTERNATIONAL STANDARD

**ISO 23806**

First edition
2022-11

# Ships and marine technology — Cyber safety



Reference number
ISO 23806:2022(E)



ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

# Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

# Introduction

This document has been prepared to provide requirements for identification and assessment of cyber hazards and risks affecting the safe and environmentally sound operation of ships throughout their operational life. This document provides specifications for procedures designed to be included or referenced in the company safety management system (SMS) in order to support effective cyber risk management as defined in MSC-FAL.1/Circ.3 on Guidelines for Maritime Cyber Risk Management[1], as well as any additional requirements of the company or other identified stakeholder.

Operational technology (OT) includes devices, sensors, software and associated networking that monitor and control onboard systems required to safely and efficiently operate the ship. OT includes, but is not limited to, navigation, main and auxiliary machinery, propulsion management and cargo management systems.

The risks associated with OT differ from those associated with information technology (IT). In general, the risks associated with OT have the potential for physical impacts affecting the safety of the ship, the personnel and cargo onboard, and the marine environment. The risks associated with IT generally relate to business and other non-physical impacts which are not safety-critical. Where IT and OT systems are integrated for particular functions, there is a potential for IT to contribute to safety-critical impacts.

The information security management system (ISMS) recommended by ISO/IEC 27000 addresses the preservation of the confidentiality, integrity and availability (CIA) of information and data stored and processed by IT systems. This document uses CIA but focuses on risks associated with the loss of availability or integrity of OT systems and data which are necessary for the safe and environmentally sound operation of a ship.

The objective of the company security management system (SMS) required by SOLAS[3] chapter IX and the ISM Code[4] is to provide a safe working environment by establishing appropriate safe practices and procedures based on an assessment of all identified risks to the ship, personnel and the environment.

The loss of availability or integrity of safety critical systems and data, and disruption of safety related operational technology (OT) is expected to have physical consequences for the safe operation of ships and prevention of pollution. Consequently, it is essential that cyber risk management be incorporated into the company's overall approach to safety management and compliance with the requirements of SOLAS chapter IX and the ISM Code, and as required by resolution MSC.428(98)[5]. The IMO has recognized that aspects of cyber risk management, including physical security aspects of cyber security, should be addressed in ship security plans under the ISPS Code[6]; however, this should not be considered as requiring a company to establish a separate cyber security management system operating in parallel with the company safety management system.

# Ships and marine technology — Cyber safety

## 1 Scope

This document gives requirements and recommendations for establishing, implementing, maintaining and continually improving a cyber risk assessment system within the context of a company's security management system (SMS).

All the elements for compliance with this document can therefore be traceable within the SMS by direct inclusion or reference.

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

**3.1**
**company**
owner of the ship or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the shipowner and, who on assuming such responsibility, has agreed to take over all the duties and responsibility imposed by the *International Safety Management Code* (3.3)

**3.2**
**cyber incident**
occurrence which potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences

**3.3**
**International Safety Management Code**
**ISM Code**
code providing an international standard for the safe management and operation of ships and for pollution prevention, drafted by the International Maritime Organization

Note 1 to entry: This Code is mandatory for all ships under the International Convention for the Safety of Life at Sea (SOLAS), chapter IX, Management for the Safe Operation of Ships.

**3.4**
**operational technology**
**OT**
hardware and software used to manage physical processes through monitoring and/or control of physical devices

Note 1 to entry: These may be items like pumps, valves, engines, machinery or systems such as bridge, cargo handling and management, machinery management, propulsion and power management, safety systems, access control passenger serving and management, passenger facing public networks, administration and crew welfare, communications and navigation systems.

**3.5**
**safety management system**
**SMS**
procedures and processes which document and implement how a *company* (3.1) approaches all elements of safety

Note 1 to entry: See also 4.1 below.

# 4 Context of the company

## 4.1 Understanding the company

The company is required to incorporate cyber risk management into their security management system (SMS). An SMS is one which conforms to the requirements of the ISM Code and ensures:

— consideration of rules and regulations;

— consideration of applicable codes, guidelines (such as Reference [7]) and standards recommended by the IMO, administrations, classification societies, maritime industry organizations and other items to which the company subscribes.

The company shall determine how cyber risk management is incorporated into an SMS. Administrations, recognized organizations or other bodies carry out verification audits of the company SMS. These include verification that the company has identified and assessed cyber safety risks to its ships, personnel and the environment, and established appropriate safeguards.

The cyber safety risk profile of a company is specific to:

— the company;

— the types of ship operated by the company, taking into account the OT installed and the degree of integration and connectivity of OT systems and between OT and IT onboard.

## 4.2 Understanding interested parties

It is expected that companies consider rules and regulations, applicable recommended codes, guidelines and standards, as well as obligations for cyber risk management imposed by contractual obligations with interested parties.

Company procedures should also identify third parties with relevant information on the OT systems onboard and their integration. This should include information on flows of data between OT and other systems, including systems ashore.

### 4.3 Determining the scope of the cyber safety risk assessment

The company shall determine the scope of the cyber safety risk assessment, taking into account:

— the OT identified by the company as being installed on its ships and which is critical to the ship's safe and environmentally sound operation, security of shipping and protection of the marine environment;

— the extent to which OT is used in shipboard operations;

— the degree of integration between OT systems, and between OT and IT;

— the requirements referred to in 4.1 and 4.2;

— interfaces and dependencies between activities performed by the company, and those performed by other parties;

— existing policies, procedures and protection measures;

— software outside the control of the shipowner;

— trusted users on their vessels;

— third-party vendors accessing the vessel's software systems.

The scope shall be documented. The scope shall recognize the rate of change of technologies, software developments and threats.

## 5 Management

### 5.1 Commitment

The senior management of the company shall demonstrate leadership and commitment to incorporating cyber risk management into its SMS, and implementing appropriate protective measures, by:

— ensuring the company establishes, implements and maintains a cyber risk policy within the defined scope of the SMS safety and environmental protection policy (see 5.2);

— ensuring that cyber risk identification, and the evaluation, planning, implementation and control of protective measures are appropriately resourced by competent personnel (see Clauses 7 and 8);

— ensuring that personnel observe the policies and procedural protective measures implemented by the company;

— ensuring defined levels of cyber management authority and lines of communication between, and among, shore and shipboard personnel (see 5.3);

— ensuring that cyber risk management is integrated into the internal audit and management review requirements in the SMS and its continuous improvement procedures (see Clause 7);

— providing cyber risk procedures to prepare for and respond to emergency situations;

— providing adequate and appropriate training and awareness for all personnel (see Clause 7).

### 5.2 Cyber risk management in the company safety and environmental protection policy

The senior management of the company should have a safety and environmental protection policy which:

— includes a commitment to supporting safe and secure shipping, which is operationally resilient to cyber risks;

— establishes objectives for cyber risk management or provides the framework for setting cyber risk management objectives;

— demonstrates a commitment to holistic governance of both IT and OT;

— demonstrates a commitment to satisfy requirements for identifying and managing cyber risks;

— includes an action plan in the SMS for containing cyberattacks;

— includes a commitment to incorporating cyber risk assessment into the continual improvement of the company's SMS.

### 5.3 Company roles, responsibilities and authorities

The senior management of the company should ensure that the responsibilities and authorities for personnel involved in cyber risk assessment; the evaluation, planning, implementation and control of protective measures; and the monitoring of effectiveness, are assigned, communicated and documented.

## 6 Cyber risk exposure

### 6.1 General

Companies are required to identify cyber risks affecting the safety and security of shipping for the ships they operate and protection of the marine environment, and to establish appropriate safeguards.

A company's risk exposure is company specific, reflecting its organizational, operational and technical characteristics and operations (see Clause 4). In identifying and assessing the risks to ships operated by the company, a generic risk assessment based on the prevailing organizational, operational and technical characteristics of the fleet should provide the company with an understanding of its cyber risk exposure. However, where ships or groups of ships within a company's fleet have materially different operational and technical characteristics, additional ship-specific risk assessments shall be carried out.

### 6.2 Actions to identify cyber hazards and risks

The cyber risk management system shall identify cyber hazards and risk, including actions necessary to detect and report cyber-events in a timely manner.

## 7 Ongoing effectiveness of cyber risk assessment

The company should periodically evaluate the effectiveness of the SMS, including the cyber risk management policies and procedures, in accordance with the procedures established by the company for that purpose. The evaluation of the effectiveness of cyber risk management policies and procedures should take into account actual or potential changes in the company's risk exposure arising from:

— the life cycle stage of OT;

— changes in the OT or in the degree of integration of OT with other systems;

— changes in the training and awareness of personnel;

— material changes in common threats affecting ships operated by the company;

— change of technologies and software developments.

Evaluating the effectiveness of the SMS should enable continuous improvement of its cyber risk related elements, in accordance with the procedures established by the company for this purpose.

## 8 Control of documented information

Documented information required by the safety management system should be controlled to ensure it is:

a) available and suitable for use, where and when it is needed;

b) adequately protected (e.g. from confidentiality, availability, or integrity).

## 9 Implementation of protective measures

The company shall evaluate, plan, implement and control the technical and procedural protection measures identified as cost-effective in accordance with the procedures established by the company including:

— implementation of risk control processes and measures, and contingency planning to protect against a cyber event and ensure continuity of shipping operations;

— development and implementation of activities and plans to prepare, respond and provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber incident;

— identification of measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber event.