

INTERNATIONAL STANDARD

ISO
23806

First edition
2022-11

Ships and marine technology — Cyber safety



Reference number
ISO 23806:2022(E)
Documents
Document Sharing Hub
© ISO 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the company	2
4.1 Understanding the company.....	2
4.2 Understanding interested parties.....	2
4.3 Determining the scope of the cyber safety risk assessment.....	3
5 Management	3
5.1 Commitment.....	3
5.2 Cyber risk management in the company safety and environmental protection policy.....	3
5.3 Company roles, responsibilities and authorities.....	4
6 Cyber risk exposure	4
6.1 General.....	4
6.2 Actions to identify cyber hazards and risks.....	4
7 Ongoing effectiveness of cyber risk assessment	4
8 Control of documented information	5
9 Implementation of protective measures	5
Bibliography	6

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.