International Standard

ISO 23799

Ships and marine technology — Assessment of onboard cyber safety

First edition
2024-01

Reference number
ISO 23799:2024(en)

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

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

With the development of digitalization, intelligence and the networking of ships, an increasing number of control systems, communication and navigation systems, information management systems and equipment are constantly connected to the ship network to access external information. The hidden danger of shipborne equipment suffering from network threats is growing. Network security risk assessment uses scientific methods and means to systematically analyse the threats faced by ship borne systems and their existing vulnerabilities, assess the degree of harm that can be caused once the security time occurs, propose targeted countermeasures and measures, and control the risks at an acceptable level.

Based on the urgent need to enhance the awareness of network risk threats, this document brings together content from IEC 31010:2019, MSC-FAL.1/Circ 3. IACS Rec.171, IACS UR E26 and UR E27, to provide the elements of shipboard network security risk assessment and the basic criteria for assessment process, assessment preparation, security risk identification, security risk analysis and security risk assessment. The recommended method of shipboard network security risk assessment which is specified in this document can help improve the ship's network security defence capability, and provide assistance to stakeholders, including:

a) identifying onboard network security risks;

b) evaluating the consequences and possibility of shipboard network security risks;

c) prioritizing shipboard network security risk disposal.

Ships and marine technology — Assessment of onboard cyber safety

1 Scope

This document establishes the elements of onboard cyber risk assessment and specifies requirements for the assessment process, assessment preparation, risk identification, risk analysis and risk evaluation.

This document applies to the risk assessment of onboard cyber systems based on network technologies which mainly include bridge systems, cargo management systems, propulsion and machinery management and power control systems, access control systems, passenger or visitor servicing and management systems, passenger-facing networks, core infrastructure systems, administrative and crew welfare systems and communication systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000, *Risk management — Guidelines*

IEC 31010, *Risk management — Risk assessment techniques*

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
onboard cyber safety
situation where the hardware and software of the shipboard network system and the data in the system are protected from damage, alteration and leakage due to accidental or malicious reasons, and the system operates continuously, reliably and normally without interruption of network services

3.2
onboard cyber risk
combination of the likelihood and impact loss of a security incident

Note 1 to entry: In the onboard network system, damage can be caused to assets by taking advantage of the vulnerabilities that exist in the system and by adopting specific means to attack the onboard network so that the information in the onboard network is leaked, and the network functions are missing.

3.3
onboard cyber risk assessment
entire process of risk identification, risk analysis and risk evaluation

Note 1 to entry: An onboard cyber risk assessment is performed by establishing the value of information assets; identifying the existence (or potential existence) of applicable threats and vulnerabilities, existing controls and their impact on the identified risks; and determining potential consequences. Finally, derive risks are prioritized and ranked against the risk assessment guidelines in the environment creation.

3.4
onboard cyber risk identification
process of discovering, enumerating and describing the elements of *onboard cyber risks* (3.2)

Note 1 to entry: This involves identifying risk sources, the scope of impact, incidents and their causes and potential consequences that can have an impact on the ship's voyage. This helps to determine what can occur in onboard cyber systems that will result in potential loss, and also gives insight into how (threat identification), where (asset identification), and why (vulnerability identification, existing control measures identification) the potential loss will occur.

3.5
onboard cyber risk analysis
analysis of the likelihood and impact loss of consequences for the security incident onboard

3.6
onboard cyber risk evaluation
risk metrics for accident scenarios encountered by the ship to assess the risk level of the accident situation

3.7
onboard cyber asset
existing resources that are valuable to the system onboard

3.8
onboard cyber threat
potential causes of damage to the shipboard network system or environmental factors causing damage to the shipboard network

3.9
onboard cyber security incident
events that have an actual or potential negative impact on shipboard systems, networks and computers or the information they process, store, or transmit, and that require response measures to eliminate their consequences

3.10
impact loss of consequences of incident scenarios
damage caused by a security event to the software, hardware, functions and data of the onboard system, resulting in interruption of system operations

Note 1 to entry: The severity of such loss depends primarily on the cost of restoring the system to normal operation and eliminating the negative impact of the security incident.

4 Elements and process of risk assessment

4.1 Relationship of elements

The basic elements of risk assessment include assets, threats, vulnerabilities, and security measures. The relationship of the basic elements is shown in Figure 1.

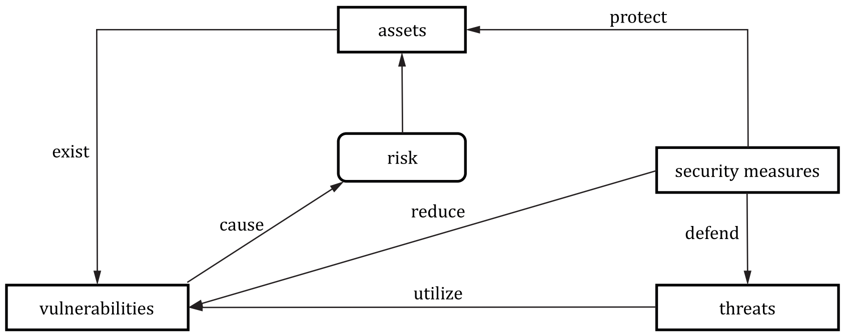

Figure 1 — Relationships of risk assessment elements

The core of the risk element is the asset, but assets are vulnerable. Security measures are used to make it more difficult for asset vulnerabilities to be exploited, to defend against external threats, and to achieve asset protection. Threats cause risk by exploiting vulnerabilities created by assets. When a risk is transformed into an onboard cyber security incident, it has an impact on the operational status of the asset.

4.2 Process of risk assessment

Onboard cyber risk assessment shall comply with ISO 31000 and IEC 31010, which includes four processes: assessment preparation, risk identification, risk analysis and risk evaluation (see Figure 2).

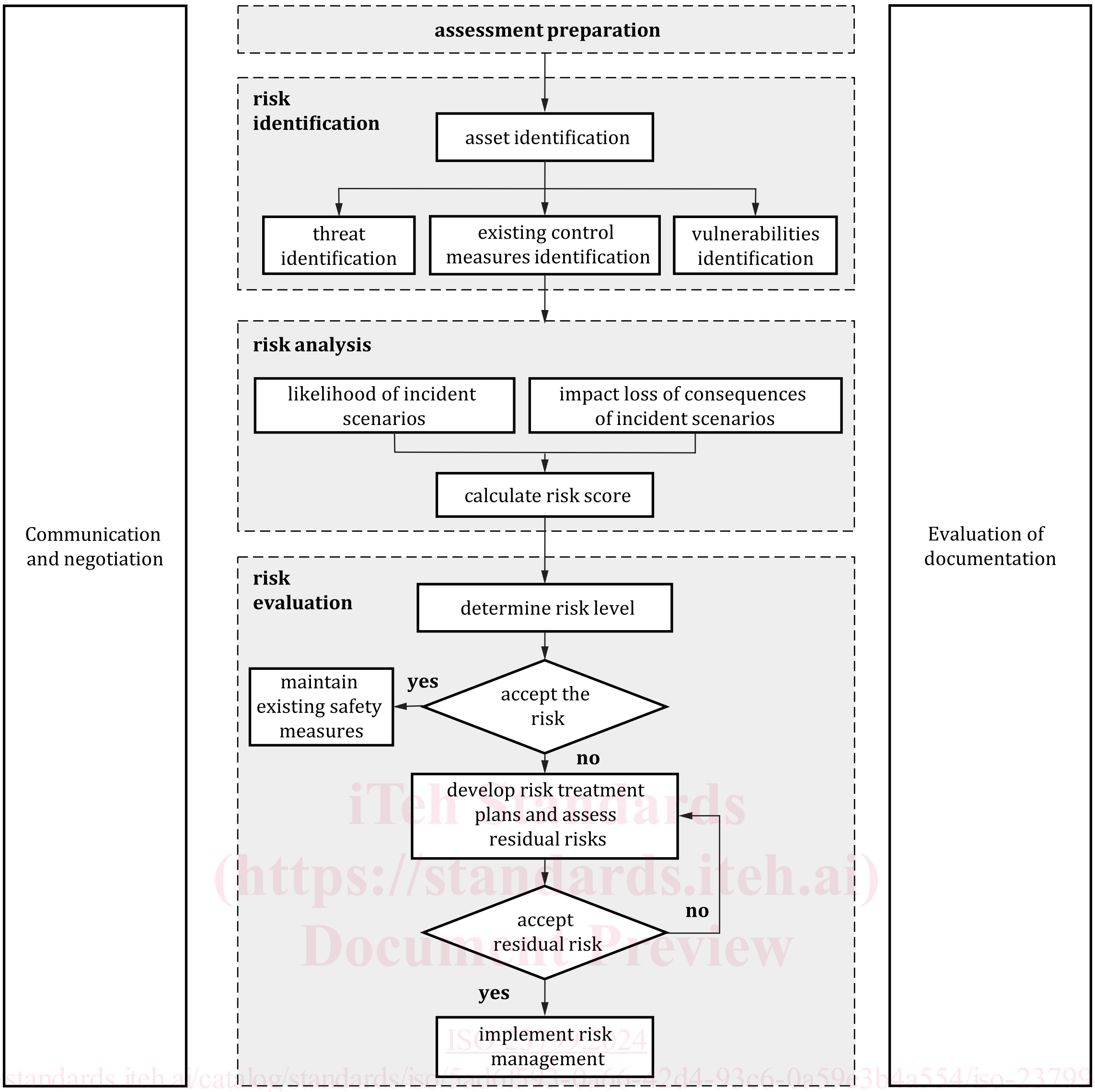
assessment preparation
risk identification
asset identification
threat identification
existing control measures identification
vulnerabilities identification
risk analysis
likelihood of incident scenarios
impact loss of consequences of incident scenarios
calculate risk score
risk evaluation
determine risk level
accept the risk
yes
maintain existing safety measures
no
develop risk treatment plans and assess residual risks
accept residual risk
no
yes
implement risk management
Communication and negotiation
Evaluation of documentation

Figure 2 — Process of onboard cyber risk assessment

Assessment preparation includes the development of an assessment work plan, the formation of an assessment team according to the needs of the assessment work, and the clarification of the responsibilities of each party.

Risk identification includes carrying out asset identification, threat identification, identification of existing security measures and vulnerability identification.

Risk analysis includes the calculation of risk values based on the results of identification.

Risk evaluation includes determining the risk level based on risk evaluation guidelines.

Communication, negotiation, and evaluation of documentation for the evaluation process should be carried out throughout the entire risk assessment process.

During the risk assessment, in the absence of relevant statistical data, experts are required to make judgements based on experience for the process of risk identification and risk analysis. A judgement matrix or other methods can be used to analyse whether the consistency of expert judgement meets the requirements.

Risk assessment is an ongoing activity, and should be conducted again when the policy environment, external threat environment, business objectives and security objectives of the assessment target change.