INTERNATIONAL STANDARD

ISO 20858

First edition
2007-10-15

Ships and marine technology — Maritime port facility security assessments and security plan development

Navires et technologie maritime — Évaluation de la sécurité des installations portuaires maritimes et réalisation de plans de sécurité

Reference number
ISO 20858:2007(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

1 Scope ... 1
1.1 General ... 1
1.2 Conformance ... 1

2 Terms and definitions ... 1

3 Performance of the security assessment ... 3
3.1 Overview of the security assessment ... 3
3.2 Personnel conducting the security assessment ... 4

4 Security assessment procedures ... 4
4.1 General ... 4
4.2 Scope of the security assessment ... 4
4.3 Current status of security at the port facility ... 5
4.3.1 Identification of assets and infrastructure ... 13
4.3.2 Consultations ... 13
4.4 Threat scenarios and security incidents ... 13
4.5 Classification of consequences ... 15
4.6 Classification of likelihood of security scenarios ... 15
4.7 Security incident scoring ... 15
4.8 Countermeasures ... 16
4.8.1 General ... 16
4.8.2 Countermeasure exceptions ... 16

5 Port Facility Security Plan (PFSP) ... 16
5.1 General ... 16
5.2 Prioritization of countermeasures ... 16
5.3 Port Facility Security Plan contents ... 17
5.3.1 General ... 17
5.3.2 Table of contents ... 17
5.3.3 Items in facility plot plan ... 17
5.3.4 Security administration and organization of the port facility ... 17
5.3.5 Port Facility Security Officer ... 17
5.3.6 Changes in security levels ... 18
5.3.7 Procedures for interfacing with ships ... 18
5.3.8 Declaration of Security (DoS) ... 18
5.3.9 Additional requirements for port facility receiving passenger ship at Security Level 1 ... 18
5.3.10 Communications ... 18
5.3.11 Security systems and equipment maintenance ... 18
5.3.12 Security measures for access control, including designated public access areas ... 18
5.3.13 Security measures for access control, including designated public access areas at Security Level 2 ... 20
5.3.14 Security measures for access control, including designated public access areas at Security Level 3 ... 20
5.3.15 Security measures for restricted areas ... 20
5.3.16 Access to restricted areas ... 20
5.3.17 Security measures for handling cargo at Security Level 2 ... 21
5.3.18 Security measures for delivery of ship's stores/spare parts and bunkers ... 22
5.3.19 Security measures for monitoring ... 22
5.3.20 Security incident procedures ... 22
5.3.21 Additional requirements for passenger and ferry port facilities ... 23
5.3.22 Additional requirements at cruise ship terminals ... 23
5.3.23 Audits and security plan amendments ... 24
5.3.24 Skills, knowledge and competencies of security and port facility personnel ... 24

5.3.25 Drills and exercises 26
5.4 Execution of the supply chain security plan 26
6 Documentation 26
6.1 Safeguarding the documents 26
6.2 Port Facility Security Assessment Report 26
6.3 Marine Port Facility Security Plan 27
6.4 Security operations and security training records 27
6.5 Retention of records 28
Annex A (informative) Guidance for obtaining advice and certification 29
A.1 General 29
A.2 Demonstrating conformance with ISO 20858 by audit 29
A.3 Certification of ISO 20858 by third party certification bodies 29

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 20858 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*.

This first edition of ISO 20858 cancels and replaces ISO/PAS 20858:2004, which has been technically revised.

Introduction

This International Standard addresses the execution of marine port facility security assessments, marine port facility security plans (including countermeasures) and the skills and knowledge required of the personnel involved. This International Standard is designed to ensure that the completed work meets the requirements of the International Maritime Organization (IMO) International Ships and Port Facility Security Code (ISPS) and the appropriate maritime security practices that can be verified by an outside auditor. Since other ISO standards may address non-marine port facilities the word “marine” usually appears before port facilities in this standard. This standard is intended to address port facilities as defined in the ISPS.

Ships and marine technology — Maritime port facility security assessments and security plan development

1 Scope

1.1 General

This International Standard establishes a framework to assist marine port facilities in specifying the competence of personnel to conduct a marine port facility security assessment and to develop a security plan as required by the ISPS Code International Standard, conducting the marine port facility security assessment, and drafting/implementing a Port Facility Security Plan (PFSP).

In addition, this International Standard establishes certain documentation requirements designed to ensure that the process used in performing the duties described above was recorded in a manner that would permit independent verification by a qualified and authorized agency (if the port facility has agreed to the review). It is not an objective of this International Standard to set requirements for a contracting government or designated authority in designating a Recognized Security Organization (RSO), or to impose the use of an outside service provider or other third parties to perform the marine port facility security assessment or security plan if the port facility personnel possess the expertise outlined in this specification. Ship operators may be informed that marine port facilities that use this document meet an industry-determined level of compliance with the ISPS Code.

Port infrastructure that falls outside the security perimeter of a marine port facility might affect the security of the facility/ship interface. This International Standard does not address the requirements of the ISPS Code relative to such infrastructures. State governments have a duty to protect their populations and infrastructures from marine incidents occurring outside their marine port facilities. These duties are outside the scope of this International Standard.

1.2 Conformance

While compliance with the ISPS Code is internationally mandated for all signatory countries, the use of this International Standard is voluntary. If a contracting government establishes requirements that preclude the use of this International Standard, local law takes precedence and compliance with this International Standard should not be claimed.

2 Terms and definitions

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

2.1
cargo
items that are placed on the ship to be transported to another port, such as boxes, pallets, cargo transport units, and bulk liquid and non-liquid matter

2.2
consequence
loss of life, damage to property or economic disruption, including disruption to transport systems that can reasonably be expected as a result of an attack on or at the marine port facility

2.3
International Maritime Organization
IMO
specialized agency of the United Nations whose purpose is “to provide machinery for cooperation among governments in the field of governmental regulation and practices relating to technical matters of all kinds affecting shipping engaged in international trade; to encourage and facilitate the general adoption of the highest practicable standards in matters concerning maritime safety, efficiency of navigation, and prevention and control of marine pollution from ships”

2.4
ISPS Code
international code for the security of ships and port facilities consisting of Part A (the provisions of which shall be treated as mandatory), and Part B (the provisions of which shall be treated as recommendatory), as adopted on 12 December 2002 by Resolution 2 of the Conference of Contracting Governments to the International Convention for the Safety at Sea, 1974, as may be amended by the Organization

2.5
likelihood
probability of a threat scenario becoming a security incident, considering the resistance the physical and operational security measures in place at the marine port facility

2.6
management system
organization’s structure for managing its processes or activities that transform inputs of resources into a product or service, which meet the organization’s objectives

NOTE It is not the intent of this document to specify a specific management system or require the creation of a separate security management system. ISO 9001 (Quality Management Systems), ISO 14001 (Environmental Management Systems), ISO 28000 (Supply Chain Security Management Systems) and the International Maritime Organization’s International Safety Management (ISM) Code are examples of management systems.

2.7
marine port facility
those areas of the port and harbour where the ship/port interface takes place

NOTE The ship/port interface means the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons and/or goods, or the provisions of port services to and from the ship. This includes areas such as anchorages, waiting berths, and approaches from seaward. The marine port facility extends landside to the security perimeter. Note that, for the purposes of this International Standard, there can be more than one marine port facility in a harbour. In that case, only the anchorages, waiting berths, and approaches from seaward that are used to service the marine port facility using this document are included. There can be areas of ports and harbours that are addressed in the ISPS Code, but that are not addressed in this International Standard.

2.8
Port Facility Security Plan
PFSP
plan to ensure the application of measures designed to protect the people, port facility, ships, cargo, cargo transport units, and ship stores within the port facility from the risks of a security incident

2.9
risk
chance of injury, damage or loss postulated by considering the consequence of a threat and the likelihood of its occurrence

2.10
security
resistance to intentional, unauthorized acts designed to cause harm or damage to ships and ports

2.11
security crisis management team
group of people who have the knowledge and authority to bring the necessary resources to bear in the event of an imminent security threat or actual security incident

2.12
security incident
suspicious act or circumstance threatening the security of a ship or port facility

2.13
security personnel
individuals who have assigned security duties defined in the port facility and who may or may not be employees

2.14
ship's stores
supplies and spare parts intended for use by a ship calling on a marine port facility

2.15
target
personnel, ships, cargo, physical assets, and control/documentation systems within a marine port facility

2.16
security threat scenario
means by which a potential security incident might occur

NOTE Because attack methods are nearly infinite, several general postulated security threat scenarios are specified to address the full range of attack scenarios. Local authorities, port facility management and personnel conducting the security assessment could add more specific security threat scenarios to the list of general security threat scenarios, depending on local circumstances.

3 Performance of the security assessment

3.1 Overview of the security assessment

The port facility implementing this International Standard shall conduct a security assessment or draw upon existing security assessments that are valid, documented and meet the requirements of this International Standard. The assessment shall consider security threat scenarios, consequences of a successful attack on the port facility, and the likelihood of each security threat scenario being successful given the security measures in place. Based on these considerations, a determination shall be made if additional security countermeasures are required.

NOTE The authorized maritime security group convened to compose the PFSA needs to be collectively knowledgeable in port/facility operations, security and the potential security threats that could occur at the specific site. From their experience and training, they review current conditions (using a provided Performance Review) and produce a realistic list of security threat scenarios that could adversely affect the facility. These potential security incidents are thoroughly studied, and then charted with regard to the likelihood of an occurrence and subsequent consequences, if it occurs. The resultant security risk chart for each of these incidents indicates which are of such gravity as to need effective human and/or physical countermeasures. The formulating team will increasingly apply these countermeasures until the identified risk is reduced to an acceptable level (meeting with the approval of the contracting government).

At this stage, the PFSA evolves into the PFSP. The aforementioned process is dealt with in more detail within this document, and forms the route toward a site-specific facility plan. Although basically stated, nothing here is intended to oversimplify the effort needed to construct a comprehensive quality plan. The above sequence will establish a plan for effective security for the standard Security Level 1, following which the group will reapply the countermeasures required for the higher Security Levels 2 and 3, as described herein. The contracting government reviews and approves the prepared plan for submission to the IMO.

3.2 Personnel conducting the security assessment

Those involved in a Port Facility Security Assessment (PFSA) shall be able to draw upon expert assistance relative to:

— knowledge of current security threats and patterns;

— recognition and detection of weapons, dangerous substances, and devices;

— recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

— techniques used to circumvent security measures;

— methods used to cause a security incident;

— effects of explosives on structures and port facility services;

— port business practices;

— contingency planning, emergency preparedness, and response;

— physical security measures (e.g. fences);

— radio and telecommunications systems, including computer systems and networks;

— transport and civil engineering;

— ship and port operations;

— maintenance of appropriate measures to avoid unauthorized disclosure of, or access to, sensitive security material;

— knowledge of the requirements in Chapter XI-2 and part A of the ISPS Code and relevant national and international legislation and security requirements;

— knowledge of security and surveillance equipment and systems, as well as their operational limitations.

All personnel involved in a PFSA, including those called on to provide the expertise listed above, shall be listed in the Port Facility Security Assessment Report as specified in 6.2.

4 Security assessment procedures

4.1 General

A security assessment provides the basis for developing the Marine Port Facility Security Plan. The methodology used in the assessment is not specified in this International Standard. However, the methodology used in the assessment shall meet the requirements of this International Standard.

4.2 Scope of the security assessment

The scope of the assessment extends to those port facilities and port infrastructures that could be threatened or be used to threaten maritime trade.

The port facility security assessment shall include, as a minimum, all areas

— where port facility/ship operations are conducted within the port facility,

— where cargo is staged, stowed or handled before/following marine transportation within the port facility,

— where cargo documentation for marine transportation is handled/accessible within the port facility,

— attached to the port facility without an intervening security perimeter, and

— including ship channels used to approach the port facility.

4.3 Current status of security at the port facility

The person(s) conducting the security assessment shall review all current security operations and emergency plans used by the port facility. All reviewed plans shall be listed. The person(s) conducting the security assessment shall, in addition, conduct an on-site review of the port facility and surrounding vicinity. As a minimum, the person(s) conducting the security assessment should examine and document items in the following performance review list during the port facility security assessment.

This performance review list is not exhaustive. Some items on the list are not applicable to certain port facilities and a negative indication concerning any specific factor does not mean that security is inadequate. The performance review list is a generalized method for assessing the current status of a port facility's security; it is not intended to set security requirements.

A copy of the completed performance review list shall be included in the assessment report.

In Table 1, if the factor indicated is in effect at the port facility, the "yes" block should be checked. If the factor is not in effect, the "no" block should be checked. If the factor is not applicable, put "NA" in the "Comments" column (additional comment pages may be added as needed).

Table 1 — Performance review list

Factors		Yes	No	Comments
Do the current port facility security documents address the following?				
1	Security organization of the port facility			
2	Organization's links with other relevant authorities and the necessary communication systems to enable an effective, continuous operation of the organization and its links with others, including ships in port			
3	Basic Security Level 1 measures, both operational and physical, that will be in place			
4	Additional security measures that will enable the port facility to progress without delay to Level 2 and, when necessary, to Level 3			
5	Regular reviews or audits of the PFSP or its amendments in response to current experiences or changing circumstances			
6	Reporting procedures, including lists of appropriate contracting government's contact points			
7	Role and structure of the port facility security organization			
8	Duties, responsibilities and training requirements of all port facility personnel who have security roles, and the performance measures needed to assess their effectiveness			
9	Port facility security organization's links with other national or local authorities with security responsibilities			
10	Communication systems provided to enable effective and continuous communication among port facility security personnel, ships in port and, when appropriate, with national or local authorities with security responsibilities			

	Factors	Yes	No	Comments
11	Procedures or safeguards necessary to enable such continuous communications to be maintained at all times			
12	Procedures and practices to protect security-sensitive information held in paper or electronic format			
13	Maintenance frequency of security equipment and procedures to assess the continuing effectiveness of security measures and equipment, including identification of, and responses to, equipment failures or malfunctions			
14	Procedures that require submission and assessments of reports relating to possible breaches of security or security concerns			
15	Procedures relating to traffic flow within the facility			
16	Procedures covering the delivery of spare parts and ship's stores			
17	Procedures to maintain and update records of dangerous goods and hazardous substances, including their location within the port facility			
18	Means of alerting and obtaining the services of waterside patrols and specialist search teams, including bomb searches and underwater searches			
19	Procedures for assisting ship security officers in confirming the identity of those seeking to board the ship when requested			
20	Procedures for facilitating shore leave for ship personnel or personnel changes, as well as access of visitors to the ship (including representatives of seafarers, welfare and labour organizations)			
21	Procedures for internal and external notifications for the following (if applicable): — bomb/terrorist security threats; — an actual explosion or detonation; — fire on the port facility or berthed ship; — hostage situation; — civil disturbance/violent labour dispute; — emergency evacuation; — informing employees to/not to report to work; — accounting for all personnel on the port facility, including their names; — specific safety guidance on the proper use of fire arms by authorized personnel in the port facility.			
22	Sketches of the port facility, access points, working areas, cargo stowage areas			
23	Security organization of the port facility			
Are the following true for the organization and performance of port facility security duties?				
24	Security force is as described in the PFSP's "Security Force" and is adequately equipped with vehicles to patrol, respond to alarms and emergencies and maintain supervision			
25	Personnel with security roles or access to restricted areas have passed background checks performed at the time of employment and periodically thereafter. This has been documented and the process used explained			
26	Security personnel are provided with security updates at the beginning of each work shift			
27	Security force orders are reviewed monthly and revised as needed			
28	Security personnel wear distinct/authoritative uniforms			