PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 20858

First edition
2004-07-01

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/PAS 20858:2004(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

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.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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/PAS 20858 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, Subcommittee SC 11, *Intermodal and short sea shipping*.

Introduction

This Publicly Available Specification addresses the execution of marine port facility security assessments, development of marine port facility security plans (including countermeasures), and skills and knowledge required of the personnel involved. This Publicly Available Specification is designed to ensure that the completed work meets the requirements of the ISPS Code and appropriate maritime security practices that can be verified by an outside auditor.

Users of this Publicly Available Specification are encouraged to submit their comments and revision suggestions.

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

1 Scope

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

In addition, this Publicly Available Specification 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 Publicly Available Specification to set standards 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 party to perform the marine port facility security assessment or security plan if the port facility personnel possess the expertise outlined in this specification.

A port infrastructure that falls outside the security perimeter of a marine port facility might affect the security of the facility/ship interface. This Publicly Available Specification does not address the requirements of the ISPS Code relative to such infrastructures. However, ship operators may be informed that ports receiving cargo from other ports that do use this Publicly Available Specification meet an industry-determined level of adequate security and the ISPS Code. 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 Publicly Available Specification.

2 Conformance

While compliance with the International Ship and Port Facility Security (ISPS) Code is internationally mandated for all signatory countries, the use of this Publicly Available Specification is voluntary. If a contracting government establishes requirements that preclude the use of this Publicly Available Specification, local law takes precedence and compliance with this Publicly Available Specification should not be claimed.

3 Terms and definitions

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

3.1
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

3.2
consequence
likely loss of life, damage to property, economic disruption (including disruption to transport systems) caused by an attack on or at the marine port facility

3.3
International Maritime Organization
IMO
a 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.”

3.4
ISPS Code
the 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

3.5
likelihood
probability of a threat scenario becoming a security incident, considering the resistance that physical and operational security measures in place at the marine port facility provide

3.6
marine port facility
those areas of the port and harbour where the ship/port interface takes place

NOTE 1 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. It should be noted that, for the purposes of this Publicly Available Specification, 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 Publicly Available Specification are included. There can be areas of ports and harbours that are addressed in the ISPS Code, but that are not addressed in this Publicly Available Specification.

NOTE 2 This Publicly Available Specification specifically addresses the marine port facility. Because other standards may address non-marine port facilities and ship security, “marine” usually appears before port facilities in this Publicly Available Specification.

3.7
Port Facility Security Plan
PFSP
a 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

3.8
risk
a level of consequence and likelihood of occurrence of a security incident

3.9
security
resistance to intentional, unauthorized acts designed to cause harm or damage to ships and ports

3.10
security crisis management team
a 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

3.11
security incident
any suspicious act or circumstance threatening the security of a ship or port facility

3.12
security personnel
individuals who have assigned security duties defined in the port facility and who may or may not be employees

3.13
ship's stores
supplies and spare parts intended for use by a ship calling on a marine port facility

3.14
target
personnel, ships, cargo, physical assets, and control/documentation systems within a marine port facility

3.15
threat scenario
potential means by which a security incident might occur. Because attack methods are nearly infinite, several general postulated threat scenarios are specified to address the full range of attack scenarios. Local authorities, port facility management, and personnel conducting the security assessment may add more specific threat scenarios to the list of general threat scenarios, depending on local circumstances

4 Performance of the security assessment

4.1 Overview of the security assessment

The principle intent of this clause is to provide informative guidance for the drafters, and later the users, of PFSAs and their accompanying plans (PFSPs), to illustrate flow logic, originating from the conceptual need to assess existing security, and produce a viable and threat-reducing plan.

The authorized maritime security group convened to compose the PFSA shall be collectively knowledgeable in port/facility operations, security and the potential threats that could occur at the specific site. From their experience and training, they shall review current conditions (using a provided Performance Review) and produce a realistic list of threat scenarios that could adversely affect the facility. These potential security-incidents shall be thoroughly studied, and then charted with regard to the likelihood of an occurrence and subsequent consequences, should it occur. The resultant risk chart for each of these incidents shall indicate 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 shall review and approve the prepared plan for submission to the IMO.

4.2 Classification of consequences

Care should be taken in establishing values of “high”, “medium” and “low” consequences. The use of excessively low threshold values may result in the requirement that countermeasures be considered for more threat scenarios than are needed. However, using excessively high threshold values may omit countermeasures for threat scenarios involving consequences that the port facility or nation cannot afford.

A “high” consequence classification may be considered as a consequence that would be unacceptable in all but low likelihood situations.

A “medium” classification of consequence may be considered as a consequence that would be unacceptable in a high likelihood situation.

A “low” classification of consequence may be considered as a consequence that is normally acceptable.

Acceptability should not be confused with desirability or approval. Rather, acceptability could be considered as a judgment of the amount of possible damage that a port facility or port state is willing to accept under certain conditions related to probability. A nation may determine that the possibility of a certain level of damage may be undesirable yet acceptable. The relative affluence of a port state can affect its acceptable threshold of consequences. A less affluent nation might be unable to recover from the same level of damage than a more affluent nation could, thus it would have a lower damage threshold. A more affluent nation may demand lower threshold values for issues because of public opinion, for example, potential damage to the environment. A developing nation may have to accept higher threshold values in spite of potential environmental damage.

4.3 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 behavioral 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.

5 Security assessment procedures

5.1 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 Publicly Available Specification. However, the methodology used in the assessment shall meet the requirements of this Publicly Available Specification.

5.2 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.

5.3 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 all-inclusive, nor does a negative indication concerning any specific factor indicate that security is inadequate. Some items on the list are not appropriate for certain port facilities. 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 the following Performance Review List, 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).

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 governments' 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			
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)			