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

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

Reference number
ISO/PAS 20858:2004(E)

© ISO 2004

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO 2004 – All rights reserved

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

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*.

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

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

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

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

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

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).

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

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)			

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

	Factors	Yes	No	Comments
21	Procedures for internal and external notifications for the following (if applicable): — bomb/terrorist 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.			
29	Security personnel patrols routinely cover all portions of the port facility, including all exterior and principal interior access points.			
30	Port facility has an organized/equipped security crisis management team or local community has an organized/equipped crisis management team.			
31	Procedures are in place to bring in additional security in an emergency or crisis situation.			
32	Liaison has been established between the port security officer and local government.			
33	Security personnel report their status to a designated contact during their security patrols.			
34	Security personnel assignments and patrol times and routes are varied to prevent predictability.			
35	Training records for security personnel are maintained.			
36	Armed security personnel are properly trained in the use of force and weapons and certified by appropriate authorities.			
37	Vehicles intended for use in security patrols are conspicuously marked.			
38	Only approved personnel are allowed to carry firearms.			
39	Security force inspects security barriers and clear zones at least monthly.			

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

	Factors	Yes	No	Comments
40	Records of security inspections are maintained and accessible to authorized personnel.			
41	If fitted, intrusion detection system signals are monitored at a central location and a security response can be initiated from that point.			
42	All external access points are guarded or secured and locked when not in use.			
43	Security measures are in effect to protect electrical power supplies and transmission facilities. (If equipped with an emergency generator, it should be within a restricted area.)			
44	Security measures are in effect to protect communications systems.			
45	Non-compliance with the security plan is noted and remedial action is promptly taken.			
46	Security measures are in place where water bodies form part of the perimeter barrier to prevent/detect illegal unauthorized access.			
47	Port facility has effective after-hours/weekend restricted area security checks.			
Access to the port facility				
48	Perimeter fencing is adequate to prevent unauthorized entry and meets recognized industry standards or government standards (explain which standard).			
49	If masonry or brick walls form part of the perimeter barrier, they are inspected regularly for effectiveness.			
50	Buildings, floors or roofs that form part of the perimeter barrier are complemented by intrusion-detection equipment.			
51	Perimeter fences/walls have a 3 m unobstructed zone on each side.			
52	Access points through the perimeter are kept to the minimum needed for safe and efficient operations.			
53	Gates provide equivalent level of security as perimeter fencing.			
54	Pass system is used to identify all personnel entering the port facility and indicate their degrees of access to portions of the port facility.			
55	Employees display passes when working in restricted areas.			
56	Security personnel certify passes of bearers upon entry.			
57	Personnel pass system is managed to prevent unauthorized issuance of passes.			
58	Lost passes are replaced with passes bearing different serial numbers.			
59	Passes are designed to enable security and other personnel to recognize individuals quickly and positively identify the authorizations and limitations applicable to the bearer.			
60	Pass procedures cover the resolution of queries by the pass checker.			
61	Procedures ensure the return or disablement of passes upon termination of employment or assignment.			
62	Procedures are in place to control the whereabouts of visitors.			
63	Procedures are in place to provide security for the port facility to meet international agreements on the humane treatment of ship crews.			
64	Truck drivers, vendors and other visitors are permitted access only to those areas required to conduct their business; only authorized personnel are permitted in warehouses.			

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

	Factors	Yes	No	Comments
65	Permanent records of visitors, vendors, and truck drivers entering the port facility are maintained and easily accessible by authorized personnel for a defined period.			
66	Random screening (at a minimum) of trucks for explosives and weapons are made of vehicles entering the port facility.			
67	If parking is allowed on the port facility, access to parking areas is supervised and restricted by a pass system for all vehicles.			
68	Parking-pass records that match personnel with pass number and motor vehicle identification are maintained.			
69	All vehicles are required to be parked in designated parking areas. Employees, vendors and visitors going to or from parking areas are required to pass through an area under the supervision of security personnel.			
70	Parking for employees, dockworkers and visitors is at least 15 m away from docks, wharfs and piers, and outside of fenced operational, cargo handling, and designated storage areas.			
71	Temporary parking passes are issued to vendors and visitors for parking in designated areas.			
72	All openings that permit access to the port facility (such as drainage ditches, tunnels, manholes for sewers and utility access, and sidewalk elevators) are properly secured.			
Restricted areas within the facility				
73	Restricted areas of the port facility have been designated in the port security plan by the port facility operator.			
74	All restricted-area access points are appropriately posted.			
75	All restricted areas have clearly marked perimeters.			
76	All restricted areas have pass systems and entrances and exits are guarded, controlled, or closed and secured.			
77	Only those personnel whose duties require access to information or equipment are allowed within restricted areas.			
78	Security personnel perform routine patrols of restricted areas.			
79	At Security Level 2, procedures are in place to — enhance the effectiveness of barriers or fencing surrounding restricted areas by using either patrols or automatic intrusion-detection devices, — reduce the number of access points to restricted areas and increase the controls applied at the remaining accesses; restrict parking adjacent to berthed ships, — increase supervision of personnel and cargo movement/storage in the restricted areas, — continuously monitor and record surveillance equipment, — enhance the number and frequency of patrols, including waterside patrols undertaken on the boundaries of restricted areas and within those areas, — establish and restrict access to areas adjacent to restricted areas, and — enforce restrictions on access by unauthorized craft to the waters adjacent to ships using the port facility			
80	At Security Level 3, procedures are in place to — set up additional restricted areas within the port facility in proximity to the security incident or potential location of the security threat to which access is denied, and — prepare for the searching of restricted areas as part of a search of all, or part, of the port facility			

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

	Factors	Yes	No	Comments
Handling of cargo				
81	The port facility has measures in place that — prevent cargo tampering, and — prevent cargo that is not meant for carriage from being accepted and stored within the port facility.			
82	Security measures in place include inventory-control procedures at access points to the port facility, once cargo within the port facility has been identified as having been checked and accepted for loading onto a ship or for temporary storage in a restricted area while awaiting loading. Cargo that does not have a confirmed date for loading is clearly identified as such, segregated from cargo to be loaded, or is prohibited from the port facility.			
83	At Security Level 1 — Cargo, cargo transport units, and cargo storage areas are routinely checked within the port facility prior to and during cargo handling operations. — Checks are performed to ensure that cargo entering the port facility matches the delivery notes or equivalent cargo documentation. — Vehicle screenings for explosives and weapons are conducted. — When cargo enters the port facility, and upon storage there, checks are conducted of the container seals that are used to prevent tampering.			
84	Restricted areas are designated for the safe inspection of cargo.			
85	Cargo stored in open areas within 3 m of a fence or port facility perimeter shall be spaced to enable security personnel to see between the perimeter barrier and the cargo, to minimize the use of stacked cargo to transit over the perimeter barrier.			
86	Cargo stored in warehouse facilities is properly stacked and placed so that security personnel may observe it. (This will minimize areas where people can hide.)			
87	Cargo information and delivery orders for cargo, cargo transport units, and containers are checked for accuracy and verified before acceptance.			
88	Access to areas where documentation is processed is limited to authorized personnel; ship documents are safeguarded from theft and documentation fraud.			
89	The placement of cargo on the port facility is controlled and all cargo can be readily identified by security and management personnel.			
90	Drivers entering the port facility are issued gate passes to control and identify those authorized to pick up or deliver cargo.			
91	Cargo is only released to drivers who have proper documentation and authorization.			
92	Before receiving a shipment, personnel processing delivery orders verify the identity of the trucker and trucking company.			
93	Cargo is moved directly from railcars or ships to storage facilities and directly from storage facilities to railcars and ships.			
94	The master flow and drain valves, and valves that would permit direct outward flow of a bulk liquid or gas storage tank contents to the surface, are securely locked in the closed position when in a non-operating or non-standby status.			
95	The starter controls on all bulk liquid and gas transfer pumps are locked in the “off” position, or located at a site accessible to authorized personnel only.			

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

	Factors	Yes	No	Comments
96	Loading and unloading connections of pipelines, loading arms, or transfer hoses are securely capped or blank-flanged when not in actual service or standby service.			
97	Security personnel are kept aware of locations of high-consequence and dangerous goods. The following is an indicative list of such goods: — Class 1, Division 1.1 explosives — Class 1, Division 1.2 explosives — Class 1, Division 1.3 Compatibility Group C explosives — Class 1, Division 1.5 explosives — Class 2.1, flammable gases in bulk — Class 2.3, toxic gases (excluding aerosols) — Class 3, flammable liquids in bulk of packing Groups I and II — Class 3 and Class 4.1, desensitized explosives — Class 4.2, goods of Packing Group I in bulk — Class 4.3, goods of Packing Group I in bulk — Class 5.1, oxidizing liquids in bulk of Packing Group I — Class 5.1, perchlorates, ammonium nitrate, and ammonium nitrate fertilisers, in bulk — Class 6.1, toxic substances of Packing Group I — Class 6.2, infectious substances of Category A — Class 7, radioactive material in quantities greater than 3 000 A1 (special form) or 3 000 A2, as applicable, in Type B or Type C packages — Class 8, corrosive substances of Packing Group I in bulk NOTE 1 For the purposes of this list, “in bulk” means transported in quantities greater than 3 000 kg or 3 000 litres in portable tanks or bulk containers. NOTE 2 For purposes of non-proliferation of nuclear material, the Convention on Physical Protection of Nuclear Material applies to international transport (supported by IAEA INFCIRC/225[Rev.4]). NOTE 3 For Class 7, A1 and A2 refer to maximum activity levels of radioactive materials. Specifically, A1 means the maximum activity of special-form radioactive materials permitted in a Type A package. A2 means the same for other than special-form radioactive materials. Special form means the material consists of materials of a certain minimum size (not likely to be distributed by wind).			
Delivery of ship stores, including a ship's spare and replacement parts				
98	Drivers entering the port facility obtain gate passes to control and identify those authorized to deliver ship’s stores.			
99	Procedures are in place to visually, physically, or electronically/chemically inspect ship's stores.			
100	Procedures are in place to prevent tampering with ship’s stores.			
101	Restricted areas are designated to perform inspections of ship's stores.			
102	Escorts are provided for delivery vehicles within the port facility where the PFSP requires it.			
103	Ship's stores are scheduled in advance of delivery and coordinated between the port facility and the ship.			
104	Measures are in place to confirm that stores presented for delivery are accompanied by evidence that they have been ordered by, or are expected by, ship personnel.			

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

	Factors	Yes	No	Comments
Handling of unaccompanied baggage				
105	Security measures are in place which ensure that unaccompanied baggage (i.e. any baggage, including personal effects that are not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening for weapons and explosives before being allowed access to the port facility. Unaccompanied baggage shall be screened before it is transferred between the port facility and the ship, at any time that such baggage is left uncontrolled before being loaded onto a ship.			
106	At security Levels 2 and 3, additional security measures are in place, including 100 % screening of all unaccompanied baggage for weapons and explosives.			
107	Unaccompanied baggage or personal effects are segregated from cargo in a secured area.			
108	Procedures are in place to restrict, suspend, or refuse to handle unaccompanied baggage.			
Monitoring the security of the facility				
109	Illumination of the port facility is adequate to allow for the ready detection of unauthorized personnel and is free of shadowed areas in which an unauthorized person would not be detected. Illumination meets recognized industry or government standards (explain which standards).			
110	The perimeter of the port facility is illuminated, and continuous or standby lighting with automatic activation is acceptable.			
111	The perimeters of all restricted areas are illuminated. (Continuous or standby lighting with automatic activation is acceptable.)			
112	All open access points are illuminated.			
113	All pedestrian entrances are illuminated. (Continuous lighting is required for all open pedestrian entrances. Pedestrian access points that are closed shall have standby or continuous lighting.)			
114	All docks, piers, wharfs and other working areas are illuminated in a manner that does not interfere with navigation. (Continuous lighting is required when there is any activity in these areas. However, during times of inactivity, standby lighting is acceptable.)			
115	All water approaches to dock, pier or wharfs are illuminated. (Continuous lighting is required when there is any activity in these areas. However, during times of inactivity, standby lighting is acceptable.)			
116	All parking lots on the port facility are evenly illuminated in a manner that prevents shadows and areas of poor illumination between vehicles.			
117	Protective perimeter lighting is arranged so that security force patrol personnel remain in comparative darkness.			
118	The port facility has an emergency backup power source for its protective lighting system.			
119	Lighting is provided from sunset to sunrise and during periods of low visibility.			
120	The port facility uses an intrusion detection system (IDS).			
121	The controls for all intrusion detection/surveillance systems are secured with key locks or screws and equipped with tamper-proof switches.			
122	There are alternative or independent power sources available for use on the system in the event of power failure.			
123	The IDS is inspected and/or tested at least monthly.			
124	The port facility security force has a reliable direct communication system between its designated security contact person and each security unit or post.			
125	There is an alternative means of security communication available.			

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

Factors		Yes	No	Comments
126	The designated security contact is in a physically secure location.			
127	The communication system is capable of rapidly transmitting instructions to all security forces and confirmation of reception is provided.			
128	All communications equipment is properly maintained.			
Name or location of the port facility being reviewed:				
Name(s) of person(s) conducting the performance review:				
Date(s) of the review:				

5.3.1 Identification of assets and infrastructure

In addition to the security performance review list, the following information shall be documented and considered during the assessment.

— Those critical assets within or adjacent to the port facility that, if damaged, could threaten the operation of the port facility.

— Those assets adjacent to the port facility that, if damaged, could cause harm to the port facility or could be used to cause harm to the port facility.

— National or prominent symbols within, or adjacent to, the port facility that, if attacked, could affect the operations of the port facility.

— Areas that can be used for illicit observation of the port facility.

— Areas adjacent to the port facility that could be used for diverting attention from security of the port facility.

5.3.2 Consultations

Contact with local law enforcement and other appropriate government officials shall be made concerning

— current and potential threats to the port facility,

— any aspects of the port facility, including the ship traffic using the facility, that make it likely to be the target of an attack,

— consequences of loss of life, damage to property, economic disruption, including disruption to transport systems, of a port facility attack,

— the capabilities and intentions of those likely to mount such an attack, and

— the types of possible attacks on the port facility.

The information received shall be documented and considered.

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

5.4 Threat scenarios and security incidents

The methodology used to conduct a security assessment shall, as a minimum, identify the threat scenarios and security incidents listed in Table 1.

Table 1 — Application examples for threat scenarios and incidents

Threat scenarios	Threat incidents	Application example
Intrude and/or take control of a target within the port facility	Intrude and/or take control of a target within the port facility and damage or destroy the target with explosives	Intruder plants explosives
	Intrude and/or take control of a target within the port facility and damage or destroy the target through malicious operations/acts	Intruder takes control of a ship and runs it aground or intentionally collides with something, or intruder intentionally opens valves to release dangerous substances, etc.
	Intrude and/or take control of a target within the port facility and create a hazardous or pollution incident without destroying the target	Intruder opens valves/vents to release toxic materials or releases toxic material brought along, or overrides interlocks leading to damage/destruction.
	Intrude and/or take control of a target within the port facility and take hostages/kill people	Goal of the intruder is to kill people.
Externally attack the port facility	Externally attack the port facility by moving explosives adjacent to the target from the waterside, the shoreside or subsurface	Car/truck bomb is used to damage/destroy the port facility.
	Externally attack the port facility by ramming a stationary target with a ship or a land-based vehicle	Intentional collision meant to damage/destroy/block operations of the port facility. (NOTE: Evaluate overall consequences from the collision, but only evaluate the vulnerabilities of the target and not the vulnerabilities of the ship/vehicle used to ram the target)
	Externally attack the port facility by launching or shooting weapons from a distance	Shooting at a target using a rifle, missile, etc.
Use the port facility as a means of smuggling	Use the port facility as a means of smuggling illegal weapons or explosives into or out of the country Use the port facility as a means of smuggling people into/out of the country	Moving people into or out of the country, concealed in ship, containers or otherwise hidden on/in a ship/train
Cyber tampering	Cyber tampering by locally or remotely gaining access to facility's or ship's computer systems for the purpose of disrupting operations or facilitating illegal activities	Hacking into a port facility's cargo documentation files for the purpose of determining which containers have dangerous goods or weapons contained within them. Or Hacking into the computer system that is used to route cargo flow at a refinery for the purpose of intentionally overfilling storage tanks.

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

Threat scenarios	Threat incidents	Application example
Cargo tampering/sabotage	Cargo tampering/sabotage to create a harmful situation.	Adding reactive chemicals to products being shipped. Rigging the cargo to discharge while in transit. Weakening the cargo restraints or containers so that they fail while being moved. Or Changing the origin of a cargo to avoid/reduce the probability of government inspections in order to smuggle devices intended to cause destruction. Or Changing the classification of cargo that causes harm or damage.
Unauthorized use	Unauthorized operations on a waterfront facility or ship other than those intended by management	Unauthorized personnel arranging to offload cargo at a waterfront facility from a ship without the knowledge of the waterfront facility management.
Others added by the contracting government, port facility management, or the security professional conducting the assessment		
NOTE The "targets" include the marine port facility, ships at the port facility, and ships in the approach channels.		

5.5 Classification of consequences

An evaluation of consequences shall consider potential loss of life and economic loss. The contracting government may also specify that facilities of symbolic value and/or the threat to government installations be taken into account when evaluating the consequence of a security incident. The consequences of each security incident evaluated at a marine port facility shall be classified as high, medium, or low. If a numerical system is used in the assessment process, the numerical results shall be converted into a qualitative system. Rationales for the classifications of consequences for each security incident shall be documented.

5.6 Classification of likelihood of security incidents

The status of physical and operational security measures at the port facility shall be taken into account in classifying potential security incidents. Physical security measures include objects that impede or detect unauthorized access to a target. Operational security measures include people and procedures that impede or detect unauthorized access to a target.

The likelihood of each security incident occurring at a particular marine port facility shall be evaluated as high, medium and low. Low likelihood should be used in cases where the security measures in place offer substantial resistance to the security incident occurring. Medium likelihood should be used when the security measures in place offer moderate resistance to the security incident occurring. High likelihood should be used when the security measures in place offer little resistance to the security incident occurring. If a numerical system is used in the assessment process, the numerical results shall be converted into this qualitative system. The rationale for the classification of likelihood assigned to each security incident shall be documented.

5.7 Security incident scoring

The following security incident scoring chart shall be used to determine when countermeasures shall be considered for specific security incidents.

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

	Consequences			
Likelihood		High	Medium	Low
	High	Countermeasures	Countermeasures	
	Medium	Countermeasures		
	Low			

Identification of countermeasures is required for security incidents that score high in both likelihood and consequences, as well as for those scoring at medium likelihood and high consequences. Other security incidents need not include countermeasures, unless they are considered advisable by the evaluator. The person assessing the security shall list each security incident required to be considered for countermeasures.

5.8 Countermeasures

5.8.1 General

Using the methods specified in this Publicly Available Specification, each countermeasure shall be assessed for effectiveness in lowering the likelihood or consequences (or a combination of them) until the security incident no longer requires that countermeasures be considered. The countermeasure achieving this is considered to be effective, and shall be listed in the PFSP.

5.8.2 Countermeasure exceptions

If the contents of a sealed container or cargo transport unit are judged to present a risk requiring countermeasures according to the methodology used, the marine port facility is not required to establish countermeasures, unless the Customs Administration of the contracting government prescribes countermeasures. If no such measures are specified, the port facility shall notify their Customs Administration of the findings of their security assessment in regard to sealed containers. A statement that notification has been made shall be included in the Port Facility Security Assessment Report.

The IMO recognized the role of Customs Administrations in controlling the international movement of closed cargo-transport units [in Conference Resolution 9 attached to the SOLAS ISPS and entitled, “Enhancement of Security in Co-operation with the World Customs Organization (Closed Cargo Transport Units)”] and has requested measures to be developed. If the contracting government develops such measures, they shall be incorporated into the port facility countermeasures list and security plan.

6 Port Facility Security Plan

6.1 General

A marine Port Facility Security Plan (PFSP) shall be developed to ensure the application of measures designed to protect the personnel, marine port facility, ships at berth, cargo, cargo transport units, and ship's stores/spare parts within the port facility from the risks of a security incident.

6.2 Prioritization of countermeasures

The countermeasures identified in 5.8 shall be implemented, in priority order, to achieve maximum benefit as judged by the port facility operator, unless the contracting government sets other priorities. Countermeasures selected for implementation shall be incorporated into the Port Facility Security Plan in the appropriate section.

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

6.3 Port Facility Security Plan contents

6.3.1 General

The following items shall be incorporated into the PFSP.

6.3.2 Table of contents

A table of contents shall be provided, that at a minimum identifies all the items listed in this subclause that are applicable.

6.3.3 Items in facility plot plan

The facility perimeters or areas covered by this security plan are as follows:

— all gates and access points (functional or otherwise);

— restricted areas on the port facility;

— ship berths;

— emergency equipment and emergency shutdown controls;

— parking areas;

— security checkpoints;

— building/structures within the facility;

— traffic flow, including emergency vehicle lanes;

— storage areas for dangerous materials (unless cargo is intermixed with non-dangerous materials, which should be noted);

— critical port facility assets.

6.3.4 Security administration and organization of the port facility

A description of the security organizational structure, including an explanation of duties and responsibilities of each person in the security organizational structure shall be provided.

A minimal breakdown of security duties should extend to the following levels:

— management;

— port facility security officer (PFSO);

— security personnel;

— personnel handling documentation related to cargo or ships' stores;

— any contractor with security duties.

6.3.5 Port Facility Security Officer

Provide the name of the Port Facility Security Officer (PFSO) and how the officer can be contacted at any time.

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

6.3.6 Changes in security levels

Define procedures for accomplishing the following.

— Ensuring that the facility operates in compliance with the required security level in effect for the port.

— Ensuring that all additional security requirements are being met, including notifying ships at berths and inbound when there has been an increase in the security level.

— At Security Levels 2 and 3, ensuring that the PFSO informs all port facility personnel about identified threats, emphasizing reporting procedures and the need for increased vigilance.

6.3.7 Procedures for interfacing with ships

Define measures for interfacing with ships at all security levels.

6.3.8 Declaration of Security (DoS)

Define procedures for requesting a DoS and for handling DoS requests from a ship.

6.3.9 Additional requirements for port facility receiving passenger ship at Security Level 1

Define procedures taken prior to the arrival of a ship at the facility, in which the PFSO, master, and Ship Security Officer (SSO) (or their designated representatives) coordinate security needs and procedures while the ship is at the facility.

6.3.10 Communications

Define the means by which the PFSO can effectively notify facility personnel of changes in security conditions. The system shall allow effective and continuous communications among the port facility security personnel, ships interfacing with the facility, the PFSO, and national and local authorities with security responsibilities.

At each active facility access point, a means of contacting police, security control, or an emergency operations centre by telephone, cellular phone or portable radios (or equivalent means) shall be provided. Facility communications systems shall have backups for internal and external communications.

6.3.11 Security systems and equipment maintenance

Define procedures to ensure that the following requirements are met:

— security systems and equipment shall be in good working order and inspected, tested, calibrated and maintained according to manufacturers' recommendations;

— security system deficiencies shall be corrected promptly and the results recorded. Procedures for identifying and responding to security system and equipment failures or malfunctions shall be included.

6.3.12 Security measures for access control, including designated public access areas

6.3.12.1 Introduction

Define security measures to

— deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, ships, facilities or ports,

— secure dangerous substances and devices that are authorized by the appropriate authority to be on the facility,

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

— control access to the facility,

— identify authorized and unauthorized persons at any security level,

— allow temporary or continuing access for facility personnel and visitors, including seafarers' chaplains and union representatives, through the use of a badge or other system to verify their identities,

— allow certain long-term, frequent vendor representatives to be issued non-temporary passes that meet the requirements specified for employee passes,

— establish the frequency of application of any access controls,

— screen persons, baggage (including carry-on items), personal effects, and vehicles, including delivery vehicles, for dangerous substances and devices at the rate specified in the approved PFSP for Security Level 1,

— deter unauthorized access to the facility and to designated restricted areas within the facility,

— screen by hand, or with devices such as X-rays, all unaccompanied baggage prior to loading onto a ship,

— secure unaccompanied baggage in a designated restricted area, after screening, and maintain security control during transfers between the facility and a ship,

— require the checking of identification of any person seeking to enter the facility, including ship passengers and crew, facility employees, vendors, personnel duly authorized by the cognizant authority, and visitors,

— deny or revoke a person's authorization to be on the facility if a person is unable or unwilling to be identified or account for his or her presence. This procedure shall include methods of reporting this situation.

6.3.12.2 Additional security measures for access control, including designated public access areas

The PFSC shall define or establish procedures to address the following.

— Ensure that a system is established for checking the identification of facility personnel or other persons seeking access to the facility that identifies access points that shall be secured or attended in order to deter unauthorized access.

— Establish the means of identification required to allow access to the facility and for individuals and vehicles to remain on the facility without requiring challenges.

— Identify the locations where screenings of people, personal effects, and vehicles are to be conducted. The designated screening areas should be covered to provide for continuous operations, regardless of weather conditions.

— Identify locations within which restrictions or prohibitions that prevent unauthorized access are applied for each security level. Each location with means of access to the facility shall be addressed.

— Identify the types of restrictions or prohibitions to be applied and the means of enforcing them.

— Specify regular updating of the security plan.

— Define disciplinary measures to discourage violations of the security plan.

— Specify the conspicuous posting of signs that describe security measures in effect and clearly state the following:

  — entering the facility is deemed as consent to screening or inspection;

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

  - failure to submit to screening or inspection will result in denial or revocation of authorization to enter the ship.

- Designate restricted areas and provide appropriate access controls for these areas.

6.3.13 Security measures for access control, including designated public access areas at Security Level 2

Define additional security measures to be taken at Security Level 2.

6.3.14 Security measures for access control, including designated public access areas at Security Level 3

Define additional security measures to be taken at Security Level 3.

6.3.15 Security measures for restricted areas

The security plan shall define the restricted areas at the port facility. As a minimum, the restricted areas shall include the following:

- shore areas immediately adjacent to each ship moored at the facility;
- areas containing sensitive security information, including cargo documentation;
- areas containing security and surveillance equipment and systems and their controls as well as lighting system controls;
- areas containing critical facility infrastructure, including
  - water supplies,
  - telecommunications, and
  - electrical systems;
- access points for ventilation and air-conditioning systems;
- manufacturing or processing areas and control rooms;
- locations in the facility to which access by vehicles and personnel is restricted;
- areas designated for loading, unloading, or storage of cargo and stores;
- areas containing cargo consisting of dangerous goods.

6.3.16 Access to restricted areas

The security plan shall specify or define procedures to

- determine which persons other than facility personnel are authorized to have access,
- determine the conditions under which that access may take place,
- define the extent of any restricted areas,
- define the times when access restrictions apply,

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

— control the entry, parking, loading, and unloading of vehicles,

— control the movement and storage of cargo and ship's stores,

— control unaccompanied baggage or personal effects,

— deter cargo tampering,

— prevent cargo that is not meant for carriage from being accepted and stored at the facility,

— identify cargo that is approved for loading onto ships interfacing with the facility,

— identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up,

— restrict the entry of cargo that does not have an appropriate, confirmed date for loading,

— ensure that cargo is released to the carrier specified in the cargo documentation,

— coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures,

— create, update and maintain a continuous inventory, including locations of all dangerous goods or hazardous substances, from receipt to delivery within the facility,

— check cargo entering the facility for dangerous substances and devices at the rate specified in the approved PFSP; means for checking cargo include

  — visual examination,

  — physical examination, and

  — detection devices, such as scanners or canines,

— ensure routine checks of cargo, cargo transport units and cargo storage areas within the facility before and during cargo handling operations in order to deter tampering,

— ensure that cargo, containers, or other cargo transport units entering the facility match the delivery notes or equivalent cargo documentation,

— screen vehicles and personnel at the rate specified in the approved PFSP,

— when vehicles or persons enter the facility, and upon storage within the facility, check all seals and other methods used to prevent tampering with cargo.

6.3.17 Security measures for handling cargo at Security Level 2

6.3.17.1 General

Define additional security measures to be taken at Security Level 2.

6.3.17.2 Security measures for handling cargo at Security Level 3

Define additional security measures to be taken at Security Level 3.

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved

6.3.18 Security measures for delivery of ship's stores/spare parts and bunkers

6.3.18.1 Introduction

Define the security procedures relating to the delivery of ship's stores/spare parts as follows

— check ship's stores for package integrity;

— prevent ship's stores from being accepted without inspection;

— deter tampering;

— screen ship's stores at the frequency specified in the approved PFSP;

— require advance notification of ship's stores or bunkers delivery, including a list of stores, delivery vehicle driver information, and vehicle registration information;

— screen delivery vehicles at the frequencies specified in the approved PFSP;

— escort delivery vehicles within the facility at the rate specified by the approved PFSP.

6.3.18.2 Security measures for delivery of ship's stores/spare parts and bunkers at Security Level 2

Define additional security measures to be taken at Security Level 2.

6.3.18.3 Security measures for delivery of ship's stores/spare parts and bunkers at Security Level 3

Define additional security measures to be taken at Security Level 3.

6.3.19 Security measures for monitoring

6.3.19.1 General

For the facility and its approaches on land and water, define the security measures that provide continuous monitoring through a combination of lighting, security guards, waterborne patrols, and automatic intrusion-detection devices, or surveillance equipment, including the following:

— restricted areas within the facility;

— ships at the facility and areas surrounding the ships.

6.3.19.2 Security measures for monitoring at Security Level 2

Define additional security measures to be taken at Security Level 2.

6.3.19.3 Security measures for monitoring at Security Level 3

Define additional security measures to be taken at Security Level 3.

6.3.20 Security incident procedures

Define the procedures which ensure that the PFSO and facility security personnel are able to

— respond to security threats or breaches of security and maintain critical facility and ship-to-facility interface operations,

STANDARDSISO.COM : Click to view the full PDF of ISO/PAS 20858:2004

© ISO 2004 – All rights reserved