

**IMPLEMENTATIONS POLICY OF ISPS CODE AS IMO STANDARD
IN ORDER OF WORKSHOP ISPS CODE JICA – DGSC
IN SURABAYA**

By:
Drs. Cholik Kirom
Head of Sub Directorate of Port Order
Directorate Guard and Rescue
Directorate General of Sea Communication

A. INTRODUCTION

Some event/incident at sea continuously occurs against the cargo ship or war ship owned by the certain country around year 2000 and finally, while the building of WTC in New York, United State was attacked and bombed on September 11th 2001 and it became a starting moment of ISPS Code arisen.

International Maritime Organization (IMO) as the International Institution under United Nation Organization, who have full responsible in safety life at sea, held the Maritime Security Conference at London on December 9th and 13th 2002, the main focus of the meeting was determining the serious steps for security maritime, prevention and strict regulation against the terrorism

The IMO Contracting Government conference was resulting 11 resolutions, where the first of 2 (two) resolutions were the resolutions that adopting and effectiveness of the International Rule concerns the ship security and port facility, they are:

1. Resolution 1 is adoption of amendments to the annex to SOLAS 1974
2. Resolution 2 is adoption of the International Ship and Port Facility (ISPS Code)

B. INTERNATIONAL SHIP AND PORT FACILITY SECURITY

International Ship and Port Facility Security Code (ISPA Code), contains detailed security-related requirements for Government, port authorities and shipping companies in a mandatory section (Part A), together with a series of guideline is about how to meet the requirements in a second, non mandatory section (Part B). Each section comprises 19 sections which contain as follow:

- 1) Effectiveness
- 2) Responsible of Contracting Government
- 3) Ship Security
- 4) Port Facility Security

1. Effectiveness

ISPS Code was effectively working on July 1st 2004, towards:

1. The following types of ships engaged on International voyages
 - Passenger ships, including high speed passenger craft
 - Cargo ships, including high speed craft, of 500 gross tonnage and upwards, and
 - Mobile offshore drilling units, and
2. Port facilities serving such ships engaged on international voyages

2. Responsible of Contracting Government

The following responsible which should be accomplished by the Sea Communication Department on behalf of Indonesia Government in order to implementation of the Code, are:

1. Determining of Designated Authority
Designated Authority is an organization or recognized authority in the government country, as the responsible to ensure the implementation of this chapter related to Port Facility and ship/port interaction from port facility view.
2. Appointing of Recognized Security Organization (RSO)
RSO is an organization with appropriate expert in security site and with the appropriate acknowledge in ship and port operational, authorized by CG to conducting assessment, or verification or approval or certification, required by this chapter or section A from ISPS Code
3. Determining of Declaration of Security
 - Security level 1 = normal condition
 - Security level 2 = indication of threat
 - Security level 3 = threat existed
4. Adoption of Port Facility Security Assessment (PFSA) and Port Facility Security Plan (PFSP)
5. Adoption of Ship Security Plan
6. Verification and Certification
7. Deliver information to the International Maritime Organization (IMO)
8. Controlling

3. Ship Security

Such following stage which should be carried out that a ship is called complies with the ISPS Code requirement by issuing the International Ship Security Certificate (ISSC):

1. Determine company security officer and ship security officer
2. Conducting ship security assessment by CSO or appointed RSO
3. Review and approval of ship security assessment by DGSC or RSO
4. Make ship security plan by CSO or appointed RSO
5. Implementation of SSP: all relevant party such as CSO, SSO, Master and ship's crew
6. Verification and certification

Beside that, there are some another mandatory that should be complied by the ship in implementation and complying to the amendment 2002 SOLAS 74 related with ISPS CODE, are:

1. Marking of Ship identification number permanently (IMO number) in a visible place of ship's hull
2. Installing of Automatic Identification System (AIS)
3. Installing of Ship Security Alert System
4. Continuous Synopsis Record
5. other relevant documents: DOS, record of the last 10 port, pre arrival notification ship security and record of drill and exercises

4. Port Facility Security

Such stage that should be carried out by a port facility until the statement of compliance of port facility is issued, are as follow:

1. Determine port facility security officer
2. Conducting port facility security assessment (PFSA) by RSO
3. Review and approval of PFSA by DGSC
4. make port facility security plan (PFSP); by PFSO and assisted by RSO
5. Review and approval; by DGSC
6. Implementation PFSP; by relevant parties such as PSC, PSO, PFSO and others
7. Verification and certification

C. ISPS Code implementation in Indonesia

The policies which have been issued in implementation of ISPS Code in Indonesia may include:

1. Publishing of sea communication ministry decree KM.33/2003 dated august 2003 about the effectiveness of amendment SOLAS 74 regarding ISPS Code in Indonesia territory
2. publishing of sea communication ministry decree KM.3/2004 about appointing of DGSC as the Designated Authority in implementation of ISPS Code
3. DGSC decree No.KL.93/I/3-04 dated February 12,2004 regarding the guidance of determining the recognize security organization(RSO)
4. DGSC decree No.KL. 93/2/1-04 dated May 14th 2004 about directorate guard and security as the Implementation of ISPS Code responsible
5. Circular letter of DGSC:
 - a. Circular letter-No.UM-48/6/16-04 dated march 19th 2004, regarding the establishment of Port Security Committee
 - b. Circular letter-No.KL.933/3/7/DV-04 dated June 30th 2004, regarding the implementation of DOS arrangement and controlling entry/exit person, vehicle in port
 - c. Circular letter UM-933/3/20/DV-04 dated July 9th 2004 regarding the implementation of the pre arrival notification of ship security and Port State Control arrangement
 - d. Maritime court of DGSC no.327/phbl-04 dated December 24th 2004 regarding the use of frequency 156.675 (channel 73)
 - e. Circular letter no.KL.933/7/8/DV-04 dated September 27th 2004 regarding the port facility and ship verification
 - f. Circular letter no.KL.933/1/12/DV-05 dated January 4th 2004 regarding the verification follow up result of implementation ISPS Code onboard
 - g. Circular letter no.KL.933/2/1/DV-05 dated April 7th 2004 regarding the maintenance and enhance the implementation of ISPS Code for the port/ port facility have obtained the SoCPF

The latest condition of the advance ISPS Code implementation is as follow:

1. 181 port / port facilities included terminal obtain the permanent SoC, as detail as follow:
 - 26 general port
 - 151 special port, included terminal, floating storage, single buoy mooring
 - 4 port still in processing of complying permanent certificate

2. 359 ships have obtain ISSC permanent

Study of implementation the ISPS Code in Indonesia is being conducted at present by the Japan International Cooperation Agency (JICA) with the DGSC and all the costs are borne completely by JICA on behalf of Japan Government. The last target of this study is distribution of loan and grant in order to enhance security condition at the general port in Indonesia.

D. Problems in implementation of ISPS Code in Indonesia

Based on the result of verification done by DGSC and search result by JICA Study Team as well as DGSC Team against the implementation of ISPS Code, the following problems are identified in such port of Indonesia, that is:

- a. Lack of attention from the head of technical management unit in region to support the implementation of ISPS Code in their own working area, this thing is appeared where such port facility was still found in operational service with the international voyage have not implement yet or not comply yet to the requirement of ISPS Code
- b. Deficiency or mistake was still found in implementation of declaration of security (DoS) as the one of important element in ISPS Code, either at port / port facility have been complied and or not comply yet with the ISPS Code requirement
- c. Low standard of security devices, system and communication, the financial limitedness, human resources and minimum of patrol ship as well, so that impact to the un-optimum in implementation of ISPS Code at each port/port facility

E. Following instructions that should be taken by the Port Administrator, as below:

- a. Identifying and report each port/port facility serving the international voyages under their coordination which have not comply/implement yet with the requirement of ISPS Code to the DGSC, attention to directorate guard and rescue
- b. Conducting monitoring and give written notice to the port/port facility that carelessness in comply the ISPS Code requirement, especially the recommendations and revise of the PFSP, thus the delivery of SoCPF is postponed
- c. For the ports which have been complied with the ISPS Code (hold the SoCFP permanently) should conduct their obligation according to the ISPS Code part A.18 and part B. 18, to carry out drill once in three (3) months and exercise once in ten (10) months
- d. To be limited the publishing of declaration of security (DoS) as could as possible, except in emergency case and follow the steps in point 3.c, and if necessary enforce searching towards the ship side because they maybe not understand the Implementation of ISPS Code

- e. Furthermore that to maintain the condition in fulfillment of ISPS Code in every port, the intermediate verification will be conducted after 2,5 year the effective of SoCFP

Herewith the explanation that could given to all of you and hopefully can be useful for all us and thank you much for the kind attention.

DIRECTORATE GENERAL OF SEA COMMUNICATION

DR.Ir. TJUK SUKARDIMAN, MSi

JICA Study Team
JICA Study Team
JICA Study Team

**Training Session on
Implementation and
Management of Port Facility
Security Measures in
PELINDO**

jica

JICA Study Team
JICA Study Team
JICA Study Team

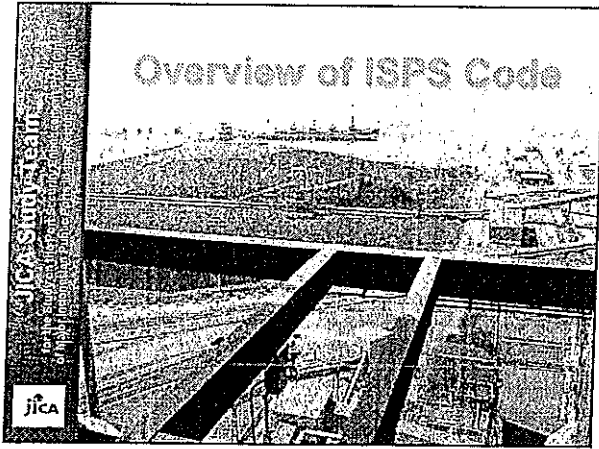
Course Time Table

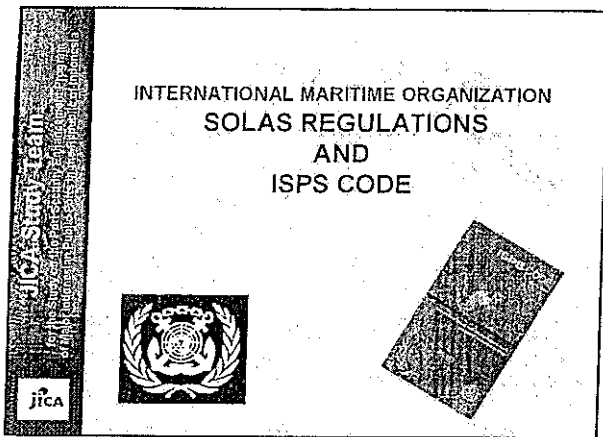
jica

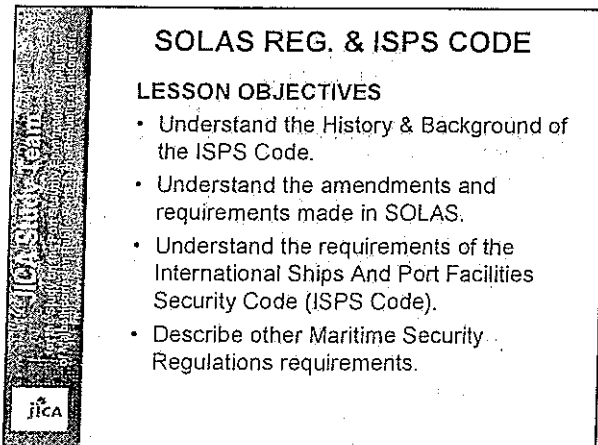
JICA Study Team
JICA Study Team
JICA Study Team

From	To	LESSONS	LECTURER
9:00	9:50	Overview of ISPS Code	Mr. Khoo
9:50	10:00	Coffee Break	
10:00	10:50	Overview of Maritime Security Threats	Mr. Khoo
10:50	11:00	Coffee Break	
11:00	11:50	Risk Analysis and Vulnerability Assessment	Mr. Khoo
11:50	12:10	Lunch	
12:10	14:00	Role of IMO	Mr. Khoo
14:00	14:10	Coffee Break	
14:10	15:00	Implementation and Management of Port Facility Security Measures	Mr. Hara
15:00	15:10	Coffee Break	
15:10	16:00	Security Self Assessment	Mr. Khoo
16:00	16:10	Coffee Break	

jica







SOLAS REG. & ISPS CODE

SCOPE

- Introduction
- History & Background of the ISPS Code
- Amendments To SOLAS
- International Ships And Facilities (Security Code & IS Code)
- Global Maritime Security Regulations
- Conclusion

JICA Study Team
Center for International Cooperation
Japan International Cooperation Agency

JICA

Surviving disaster – The Titanic and SOLAS

The infographic provides a comprehensive overview of the Titanic disaster and its impact on maritime safety. It includes details about the ship's construction, the iceberg collision, the sinking, and the subsequent international conference that led to the SOLAS convention. Key points include the ship's speed, the lack of lifeboats, and the role of the iceberg in the tragedy.

Background to the ISPS Code

11 September 2001 bombing of WTC
 IMO Secretary-General call for a review of the existing IMO instruments.

- to prevent and suppress terrorist acts against ships at sea and in port
- to improve security aboard and ashore
- to deter acts of violence and crime at sea
- TO ENHANCE MARITIME SECURITY

JICA Study Team
Center for International Cooperation
Japan International Cooperation Agency

JICA

JICA Study Team
 JICA Study Team
 for the Study on the Security of Maritime Transport
 at the Request of the Government of the Philippines
 JICA

Background to the ISPS Code

The following existing IMO instruments were specifically referred to:

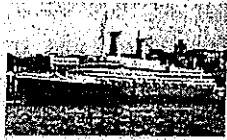
- 1985-Assembly Resolution A.584(14) titled "Measures to Prevent Unlawful Acts Which Threaten the Safety of Ships and the Security of their Passengers and Crew"
- 1986-MS/Circ.443, titled "Measures to Prevent Unlawful Acts against Passengers and Crew onboard vessel"
- 1988-"Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Convention (Rome 1988)", known as SUA Convention
- 1996-MS/Circ.754 titled "Passenger Ferry Security"

JICA Study Team
 JICA Study Team
 for the Study on the Security of Maritime Transport
 at the Request of the Government of the Philippines
 JICA

Background to the ISPS Code

The following existing IMO instruments were specifically referred to:

- 1985-Assembly Resolution A.584(14) titled "Measures to Prevent Unlawful Acts Which Threaten the Safety of Ships and the Security of their Passengers and Crew"
- Achille Lauro, Italian passenger ship with 400 passenger on board, Oct. 7 - Oct.9 in 1985 Off Alexandria (Mediterranean Sea). Ship seized at sea off the Egyptian coast by 4 Palestinian passengers who were accidentally discovered in their cabin by a steward while they were cleaning their weapons.




JICA Study Team
 JICA Study Team
 for the Study on the Security of Maritime Transport
 at the Request of the Government of the Philippines
 JICA

Background to the ISPS Code

The following existing IMO instruments were specifically referred to:

- 1985-Assembly Resolution A.584(14) titled "Measures to Prevent Unlawful Acts Which Threaten the Safety of Ships and the Security of their Passengers and Crew"
- 1986-MS/Circ.443, titled "Measures to Prevent Unlawful Acts against Passengers and Crew onboard vessel"
- The measures stress the need for port facilities and individual ships to have a security plan and appoint a security officer. The measures describe in detail the way in which security surveys should be conducted and the security measures and procedures which should be adopted.




JICA Study Team
 JICA Study Team
 of the Ministry of International Trade and Economic Relations
 of the Government of Japan

Background to the ISPS Code

The following existing IMO instruments were specifically referred to:

- 1985-Assembly Resolution A.584(14) titled "Measures to Prevent Unlawful Acts Which Threaten the Safety of Ships and the Security of their Passengers and Crew"
- 1986-MSC/Circ.443, titled "Measures to Prevent Unlawful Acts against Passengers and Crew onboard vessel"
- 1988-"Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Convention (Rome 1988)", known as SUA Convention.
 - Ensure that appropriate judicial action is taken against persons committing unlawful acts against ships.
 - It requires Contracting Governments either to extradite or prosecute alleged offenders.



jica

JICA Study Team
 JICA Study Team
 of the Ministry of International Trade and Economic Relations
 of the Government of Japan

Background to the ISPS Code

The following existing IMO instruments were specifically referred to:

- 1985-Assembly Resolution A.584(14) titled "Measures to Prevent Unlawful Acts Which Threaten the Safety of Ships and the Security of their Passengers and Crew"
- 1986-MSC/Circ.443, titled "Measures to Prevent Unlawful Acts against Passengers and Crew onboard vessel"
- 1988-"Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Convention (Rome 1988)", known as SUA Convention.
- 1996-MSC/Circ.754 titled "Passenger Ferry Security"

jica

JICA Study Team
 JICA Study Team
 of the Ministry of International Trade and Economic Relations
 of the Government of Japan

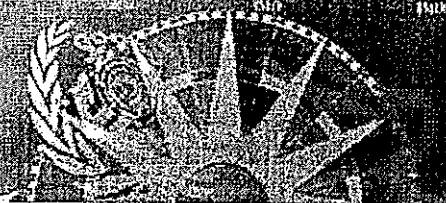
Background to the ISPS Code

The review process was initiated in February 2002, and produced a series of recommendations during:

- 1st Intercessional Working Group (ISWG) (11-15 Feb 02)
- Maritime Safety Committee MSC 75 (16-24 May 02)
- 2nd Intercessional Working Group (ISWG) (9-13 Sep 02)
- MSC 76 Diplomatic Conference (2-13 Oct 02)

jica

JICA Study Team
 JICA Study Team
 JICA Study Team



During the Diplomatic Conference on Maritime Security held in London in December 2002, IMO adopted new provisions in the International Convention for Safety of Life at Sea, 1974 and the ISPS code to enhance maritime security.




JICA

JICA Study Team
 JICA Study Team
 JICA Study Team

Maritime Security

```

  graph TD
    A[Maritime Security] --> B[Vessels]
    A --> C[Port Facilities]
    A --> D[Commercial]
  
```




JICA

JICA Study Team
 JICA Study Team
 JICA Study Team

Maritime Security

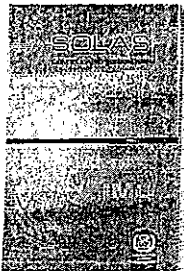
```

  graph TD
    A[Maritime Security] --> B[Vessels]
    A --> C[Port Facilities]
    A --> D[Commercial]
  
```

JICA

SAFETY
OF
LIFE
AT
SEA




JICA Study Team
International Policy Research Center
Japan International Cooperation Agency

JICA

Amendments to SOLAS

Chapter V
Chapter XI



Chapter XI-1
Special measures to
enhance maritime
SAFETY


Chapter XI-2
Special measures to
enhance maritime
SECURITY

JICA Study Team
International Policy Research Center
Japan International Cooperation Agency

JICA

SOLAS CHAPTER V

- Automatic Identification System (V/19)
 - All ships 300 GT and above (on int'l voyage)
 - not later than the first safety equipment survey after 1 July 2004 or by 31 December 2004
 - Maintain AIS in operation all times




JICA Study Team
International Policy Research Center
Japan International Cooperation Agency

JICA

SOLAS CHAPTER XI - 1
Special Measures to Enhance Maritime Safety

• Ship Identification Number (IMO Number) (XI-1/3)

- Permanently marked (200 mm)
- Visible on:
 - stern or side of hull or superstructure
 - horizontal surface for passenger vessels
- Contrasting color
- raised lettering or by cutting it into or center punching
- 1-July-2004



JICA Study Team
JICA Study Team
JICA Study Team

jica

SOLAS CHAPTER XI - 1
Special Measures to Enhance Maritime Safety

• Continuous Synopsis Record (XI-1/5)

- Basic diary of ship / historical record of ship
- Issued by Flag state and updated by company
- Information includes:
 - name of flag state & date of registry
 - ship's ID number
 - name of owners & name of registered demise charterers
 - name of shipping company
 - name of classification society(ies)
 - name of authorities or associations issuing certifications
- Left onboard with change of ownership or registry
- 01-July-2004





JICA Study Team
JICA Study Team
JICA Study Team

jica

SOLAS CHAPTER XI - 2
Special Measures to Enhance Maritime Security

Applies to ship engaged on international voyage (XI-2/2) :-

- Passenger Ships
- Cargo Ships => 500GT
- Mobile offshore Drilling Units
- Port facilities serving ships engaged in international voyages.


JICA Study Team
JICA Study Team
JICA Study Team

jica

SOLAS CHAPTER XI - 2
Special Measures to Enhance Maritime Security

Obligations Of Contracting Governments With Respect to Security (XI-2/3)

- Contracting Governments shall set Security Levels and provide security level information to its own ships and the ports in their own territory.
- Level 1 – Normal
- Level 2 – Heightened probability of a security incident
- Level 3 – When a security incident is probable or imminent.




JICA Study Team
for the Study of the
Introduction of the
ISPS Code to the
Philippines
JICA

SOLAS CHAPTER XI - 2
Special Measures to Enhance Maritime Security

Requirements for Companies and Ships (XI-2/4)

- Companies and ships shall comply with the requirements of chapter XI-2 and Part A of the Code using Part B as a guidance



JICA Study Team
for the Study of the
Introduction of the
ISPS Code to the
Philippines
JICA

SOLAS CHAPTER XI - 2
Special Measures to Enhance Maritime Security

Specific Responsibilities of Companies (XI-2/5)

Shall ensure that the master has available on board at all times information through which Flag and Port States officers can:-

- establish who has appointed the crew
- decided the employment of the ship
- who are the party(ies) to the charter party(ies).

JICA Study Team
for the Study of the
Introduction of the
ISPS Code to the
Philippines
JICA

SOLAS CHAPTER XI - 2
Special Measures to Enhance Maritime Security

Ship Security Alert System (XI-2/6)

- All ships shall be fitted with a security alert system. This may be combined with an existing radio installation. (A performance standard has been adopted by IMO by resolution MSC 136(76). SOLAS Chpt.IV)

The diagram illustrates the SSAS architecture. On the ship, there is a 'SECURITY ALERT SYSTEM' which is connected to a 'SECURITY ALERT UNIT'. This unit is linked to a 'SECURITY ALERT SYSTEM' on the shore, which is further connected to a 'SECURITY ALERT SYSTEM' on a satellite. The satellite is also connected to a 'SECURITY ALERT SYSTEM' on another shore-based station. The diagram shows the flow of information from the ship to the shore and back.

JICA Study Team
for the Study of the
of the Ministry of Public Safety, Japan

JICA

SOLAS CHAPTER XI - 2
Special Measures to Enhance Maritime Security

Threats to Ships (XI-2/7)

- In areas where there is a heightened risk against ships, coastal states are obliged to provide relevant information and points of contacts to ships in the area. EGC - NAVTEX

The image shows a dark silhouette of a ship on the water, likely at night or in low light conditions. The ship is positioned in the lower center of the frame, with a dark, textured background representing the sea and sky.

JICA Study Team
for the Study of the
of the Ministry of Public Safety, Japan

JICA

SOLAS CHAPTER XI - 2
Special Measures to Enhance Maritime Security

Master's Discretion for Ship Safety and Security (XI-2/8)

- Regulation make it absolutely clear that the master has the overriding responsibility for all safety and security matters on his ship.
- He has the right to make a professional judgment on what to do in case of a conflict between safety and security requirements.

JICA Study Team
for the Study of the
of the Ministry of Public Safety, Japan

JICA

SOLAS CHAPTER XI - 2
Special Measures to Enhance Maritime Security

Control and Compliance Measures (XI-2/9)

- Initially, there will be the 'normal' Port State control check of the ISSC.
- If there are clear grounds to believe that the ship is not in compliance, the control may go further.
- Non-compliance may include invalid ISSC, not properly implemented or no SSP.
- Control - inspected prior to entering the port or denied entry.
- Current security level vessel is operating in and record of security level in last 10 ports.

JICA Study Team
JICA
jica

SOLAS CHAPTER XI - 2
Special Measures to Enhance Maritime Security

Requirements for Port Facilities (XI-2/10)

- required to comply with the Code, including carrying out a Port Facility Security Assessment and establishing a Port Facility Security Plan.

Alternative Security Agreements (XI-2/11)

- Contracting Governments may enter into alternative security arrangements for ships on fixed routes between port facilities within their own territory. (To simplify security requirements for inland ferries.)

JICA Study Team
JICA
jica

SOLAS CHAPTER XI - 2
Special Measures to Enhance Maritime Security

Equivalent Security Arrangements (XI-2/12)

- Allows Contracting Governments to apply equivalent security arrangements.


Communication of Information (XI-2/12)

- This regulation summarizes the obligations of Contracting Governments to provide information to ships, to the IMO and other Contracting Governments.

JICA Study Team
JICA
jica

JICA Study Team
 International Ship and Port Facility Security Code

International Ship and Port Facility Security Code



jica

JICA Study Team
 International Ship and Port Facility Security Code

International Ship and Port Facility Security (ISPS) Code

- The International Ship and Port Facility Security (ISPS) code is a standalone instrument, put in force by an amendment to SOLAS chapter XI.
- It consists of a mandatory requirement part A and a recommendation part B.
- fundamental requirements of the Convention to detect and deter acts which threaten ships, ports and maritime trade.

jica

JICA Study Team
 International Ship and Port Facility Security Code

International Ship and Port Facility Security (ISPS) Code

ISPS Code - Part A (19 Sections)


- Responsibility Of Contracting Governments
- Obligation Of The Company
- Ship Security, Security Assessment, Security Plan, Ship And Company Security Officers
- Records
- Training And Drills
- Port Facility Security, Assessment, Port Facility Security Plan And Port Facility Security Officer
- Verification And Certification

jica

Sect. 2 - Definition

•Security Levels

- Level 1: Minimum appropriate security level maintained at all times
- Level 2: There is a heightened risk of a security incident
- Level 3: Limited period where a security incident is probable or imminent



JICA Study Team
for the
Preparation of the
Port Security
Regulation
JICA

Sect. 4 - Responsibilities of Contracting Governments


Specifying those responsibilities which **CANNOT** be delegated.

- setting of the applicable security level;
- approving a PFSA and subsequent amendments to an approved assessment and plan;
- determining the port facilities which will be required to designate a PFSO;
- exercising control and compliance measures pursuant to regulation XI-2/9; and
- establishing the requirements for a Declaration of Security.

JICA Study Team
for the
Preparation of the
Port Security
Regulation
JICA

Sect. 5 - Declaration of Security

- Declaration of Security means an agreement reached between a ship and either a port facility or another ship with which it interfaces specifying the security measures each will implement.
- This section explains the reasons for the Declaration of Security and the procedures for its use.



JICA Study Team
for the
Preparation of the
Port Security
Regulation
JICA


Sect. 5 - Declaration of Security

- Need for a DoS may be indicated by the results of the port facility security assessment.
- DoS may be initiated prior to ship/port interfaces that are identified in the approved PFSA as being of particular concern.
 - Examples - embarking or disembarking passengers, transfer, loading or unloading of dangerous goods or hazardous substances.
- PFSA may also identify facilities at or near highly populated areas or economically significant operations that warrant a DoS.

JICA Study Team
jica

Sect. 5 - Declaration of Security

- A ship may request for a DoS because it is operating at higher security level than the port facility.
- There is agreement between Contracting Governments covering certain international voyages or specific ships on those voyages.
- There is a security threat or incident involving ship or the port facility.



JICA Study Team
jica

Sect. 5 - Declaration of Security

- DoS must be acknowledged by the applicable port facility or ship.
- Copy of DoS must be kept by both the ship and the port facility.
- The DoS shall be made available to government authorities upon request.
- Contracting Government shall determine minimum period for which DoS shall be kept.

JICA Study Team
jica

International Ship and Port Facility Security (ISPS) Code


- Sect. 6 - Obligations of the Company
- Sect. 7 - Ship Security
- Sect. 8 - Ship Security Assessment
- Sect. 9 - Ship Security Plan

JICA Study Team
Japan International Cooperation Agency
 1-1-1 Higashi-Shinjuku 4-chome, Shinjuku-ku, Tokyo 162-8502, Japan
 TEL: 81-3-5288-5111 FAX: 81-3-5288-5112
 E-MAIL: jica@jica.go.jp

jica

Sect. 10 - Records

- Records are to be included in the SSP
 - training, drills and exercises
 - reports of security threats and incidents
 - reports of breaches of security
 - changes in security level
 - communications relating to the security of the ship
 - internal audits and reviews of security activities
 - periodic review of the security assessment
 - periodic review of ship security plan
 - implementation of any amendments to the plan
 - maintenance, calibration and testing of any security equipment



JICA Study Team
Japan International Cooperation Agency
 1-1-1 Higashi-Shinjuku 4-chome, Shinjuku-ku, Tokyo 162-8502, Japan
 TEL: 81-3-5288-5111 FAX: 81-3-5288-5112
 E-MAIL: jica@jica.go.jp

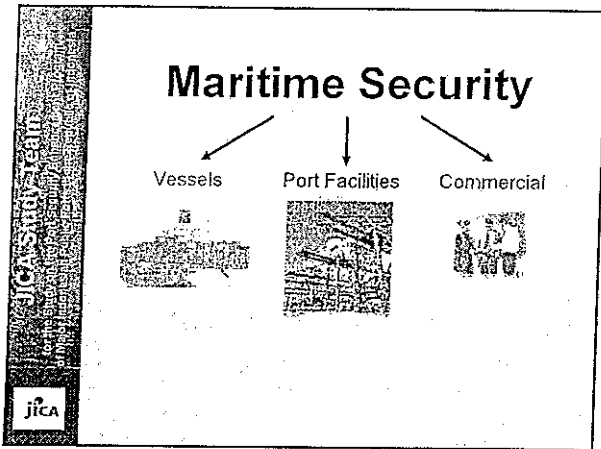
jica

International Ship and Port Facility Security (ISPS) Code

- Sect. 11 - Company Security Officer (CSO)
- Sect. 12 - Ship Security Officer (SSO)
- Sect. 13 - Trainings, drills and exercises on ship security


JICA Study Team
Japan International Cooperation Agency
 1-1-1 Higashi-Shinjuku 4-chome, Shinjuku-ku, Tokyo 162-8502, Japan
 TEL: 81-3-5288-5111 FAX: 81-3-5288-5112
 E-MAIL: jica@jica.go.jp

jica



Sect. 14 – Port Facility Security

- A port facility is required to act upon the security levels set by the Contracting Government within whose territory it is located.
- Security measures and procedures shall be applied at the port facility in such a manner as to cause a minimum of interference with, or delay to, passengers, ship, ship's personnel and visitors, goods and services



JICA Study Team
jica

Sect. 15 – Port Facility Security Assessment (PFSA)




- Is an essential and integral part of the process of developing and updating the port facility security plan.
- Shall be carried out by the Contracting Government within whose territory the port facility is located.
- May authorise a RSO to carry out the PFSA of a specific port facility located within its territory.

JICA Study Team
jica

Sect. 15 – Port Facility Security Assessment (PFSA) – cont 1

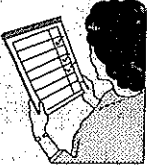


NOTE

- Port owners and operators with in-house capabilities may conduct the PFSA on their own. Such PFSA must be verified and endorsed by an appointed Recognised Security Organisation (RSO) before being submitted to the Maritime and Port Authority of Singapore.




Sect. 15 – Port Facility Security Assessment (PFSA) – cont 2

- PFSA shall periodically be reviewed and updated, taking account of changing threats and/or minor changes in the port facility and shall always be reviewed and updated when major changes to the port facility take place.

Sect. 16 – Port Facility Security Plan (PFSP)



- Shall be developed and maintained, on the basis of a PFSA, for each port facility, adequate for the ship/port interface.
- Shall make provisions for the three security levels.
- A RSO may prepare the PFSP of a specific port facility.
- The PFSP shall be approved by the Contracting Government.

Sect. 16 – Port Facility Security Plan (PFSP) – cont 1



PFSP should at least address:

- 1 measures designed to prevent weapons or any other dangerous substances from being introduced into the port facility or on board a ship;
- 2 measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility;
- 3 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface;



Sect. 16 – Port Facility Security Plan (PFSP) – cont 2

- 4 procedures for responding to any security instructions the Contracting Government, in whose territory the port facility is located, may give at security level 3;
- 5 procedures for evacuation in case of security threats or breaches of security;
- 6 duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects;
- 7 procedures for interfacing with ship security activities;

Sect. 16 – Port Facility Security Plan (PFSP) – cont 3

- 8 procedures for the periodic review of the plan and updating;
- 9 procedures for reporting security incidents;
- 10 identification of the port facility security officer including 24-hour contact details;
- 11 measures to ensure the security of the information contained in the plan;
- 12 measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility;

Sect. 16 – Port Facility Security Plan (PFSP) – cont 4

13. procedures for auditing the port facility security plan;

14. procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and

15. procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labor organizations.

JICA Study Team
 JICA
 SECURITY PLAN

Sect. 16 – Port Facility Security Plan (PFSP) – cont 5

- Personnel conducting internal audits, shall be independent, unless this is impracticable due to the size and the nature of the port facility.
- PFSA may be combined with, or be part of, the port security plan or any other port emergency plan or plans.
- Contracting Government shall determine which changes to the PFSP shall not be implemented unless the relevant amendments to the plan are approved by them.

JICA Study Team
 JICA
 SECURITY PLAN


Sect. 16 – Port Facility Security Plan (PFSP) – cont 6

- PFSP may be kept in an electronic format. Shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.
- The plan shall be protected from unauthorized access or disclosure.
- Contracting Governments may allow a port facility security plan to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar.

JICA Study Team
 JICA
 SECURITY PLAN

Sect. 17 – Port Facility Security Officer (PFSO)

- A port facility security officer shall be designated for each port facility.
- A person may be designated as the port facility security officer for one or more port facilities.



jica

Sect. 17 – Port Facility Security Officer (PFSO) – cont 2

Duties and responsibilities:

1. conducting an initial comprehensive security survey of the port facility taking into account the relevant port facility security assessment;
2. ensuring the development and maintenance of the port facility security plan
3. implementing and exercising the port facility security plan
4. undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures

jica

Sect. 17 – Port Facility Security Officer (PFSO) – cont 3

Duties and responsibilities:

5. recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account of relevant changes to the port facility
6. enhancing security awareness and vigilance of the port facility personnel
7. ensuring adequate training has been provided to personnel responsible for the security of the port facility

jica

Sect. 17 – Port Facility Security Officer (PFSO) – cont 4

Duties and responsibilities:

- 8. reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility
- 9. co-ordinating implementation of the port facility security plan with the appropriate Company and ship security officer(s);
- 10. co-ordinating with security services, as appropriate

JICA Study Team
 JICA
 JICA

Sect. 17 – Port Facility Security Officer (PFSO) – cont 5

Duties and responsibilities:

- 8. ensuring that standards for personnel responsible for security of the port facility are met
- 12. ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and
- 13. assisting ship security officers in confirming the identity of those seeking to board the ship when requested.

JICA Study Team
 JICA
 JICA


Sect. 18 – Training, drills and exercises on Port Security

PFSO and appropriate port facility security personnel shall have knowledge and have received training, taking into account the guidance given in part B of this Code

JICA Study Team
 JICA
 JICA


Sect. 18 – Training, Drills & Ex on Port Security – cont 2


Drills shall be carried out at appropriate intervals taking into account the types of operation of the port facility, port facility personnel changes, the type of ship the port facility is serving and other relevant circumstances

JICA Study Team


Sect. 18 – Training, Drills & Ex on Port Security – cont 3

PFSP shall ensure the effective coordination and implementation of the PFSP by participating in exercises at appropriate intervals




JICA Study Team


Recognized Security Organization (RSO)

Authorized by Contracting Government and acting on its behalf, such as:

- Approving of Ship Security Plan, or its amendments
- Verification and certification of compliance of ship
- Conducting Port Facility Security Assessment.

JICA Study Team


Recognized Security Organization (RSO)

May advise and provide assistance to companies or Port Facilities on security matters, such as:

- Ship Security Assessment (not approved by it)
- Ship Security Plan (not approved by it)
- Port Facility Security Assessment
- Port Facility Security Plan.

JICA Study Team
JICA

Maritime Security

Vessels Port Facilities Commercial


JICA Study Team
JICA

Voluntary Programs

Customs-Trade Partnership Against Terrorism (C-TPAT)

- An international initiatives to improve and enhance security arrangements throughout the supply chain.
- Businesses partner with U.S. Customs
- Conduct a comprehensive security self assessment
- Develop and implement a program to enhance security throughout their supply chains
- Communicate & promote C-TPAT guidelines to other companies in the supply chain
- In return, their goods and conveyances will receive expedited processing into the United States.

JICA Study Team
JICA

Voluntary Programs 


Container Security Initiative (CSI)

- To reduce the risk of global containerized cargos being exploited by terrorists.
- Target and screen containers at mega-port before container reaches port of final destination.
- Establish security criteria for identifying high-risk containers.
- Pre-screen containers before they are shipped to the U.S.
- Use technology to pre-screen high-risk containers
- Develop and use smart and secure containers

JICA Study Team
Japan International Cooperation Agency
JICA

U.S. Customs Service's Container Security Initiative

- U.S. Customs will place 4-12 inspectors in strategic overseas ports to assist in identifying high-risk containers.



JICA Study Team
Japan International Cooperation Agency
JICA

U.S. Customs Service's Container Security Initiative

Top 10 U.S. Ports of Import:

1) New York	6) Norfolk
2) Los Angeles	7) Houston
3) Long Beach	8) Oakland
4) Charleston	9) Savannah
5) Seattle	10) Miami

Advance inspection of containers destined for the U.S. should result in rapid Customs Clearance

JICA Study Team
Japan International Cooperation Agency
JICA

JICA Study Team
 Technical Assistance for Port Security Enhancement (Phase 2)
 Study on Port Security Enhancement (Phase 2)

U.S. Customs Service's Container Security Initiative

Top 20 Foreign Ports (Exports to U.S.)

1) Hong Kong	11) Antwerp, Belgium
2) Shanghai, China	12) Nagoya, Japan
3) Singapore	13) Le Havre, France
4) Kaohsiung, China	14) Hamburg, Germany
5) Rotterdam, Netherlands	15) La Spezia, Italy
6) Pusan, Republic of Korea	16) Felixstowe, United Kingdom
7) Bremerhaven, Germany	17) Algeciras, Spain
8) Tokyo, Japan	18) Kobe, Japan
9) Genoa, Italy	19) Yokohama, Japan
10) Yantian, China	20) Laem Chabang, Thailand

jica

JICA Study Team
 Technical Assistance for Port Security Enhancement (Phase 2)
 Study on Port Security Enhancement (Phase 2)

Other Security Related Information

ONI Worldwide Threat to Shipping

- This message service provides information on threat to and criminal action against merchant shipping worldwide.
 Link to official website -
http://164.214.12.145/onit/onit_j_main.html

The International Maritime Bureau (IMB)

- IMB publish a weekly piracy summary, based on reporting from the IMB Piracy Reporting Centre in Kuala Lumpur, Malaysia. Each week's report is published on Tuesday and may be accessed through their web page www.iccwbo.org.

jica

JICA Study Team
 Technical Assistance for Port Security Enhancement (Phase 2)
 Study on Port Security Enhancement (Phase 2)

What Happen After 1 July 2004


- Keep pace with Legislature Changes. Eg IMO Assembly, SOLAS, STCW, MSC Decisions and Circulars, Legal Provisions of other countries.
- Conduct Exercise, Training and Drill.
- Maintain Records. Eg DoS, Incident Reports, Change in Security Level etc.
- Continue to benchmark with other port facilities.
- Audit, Inspection and Amendments
- Update IMO

jica

SOLAS REG. & ISPS CODE

CONCLUSION

- Amendments To SOLAS
 - Chapter V
 - Chapter XI
- International Ships And Port Facilities Security Code (ISPS Code)
 - Part A & B
- Other Maritime Security Regulations



JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

Overview of Maritime Security Threats

Part B/18.1.12 & 18.2.1

The Port Facility Security Officer & Port facility personnel having specific security duties should have knowledge and receive training, in some of all of the following, as appropriate:...

..... knowledge of current security threats and patterns;

1

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

Scope

- Piracy & Armed attacks
- Terrorism
- Contraband smuggling
- Cargo theft

2

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

Piracy & Armed Attack

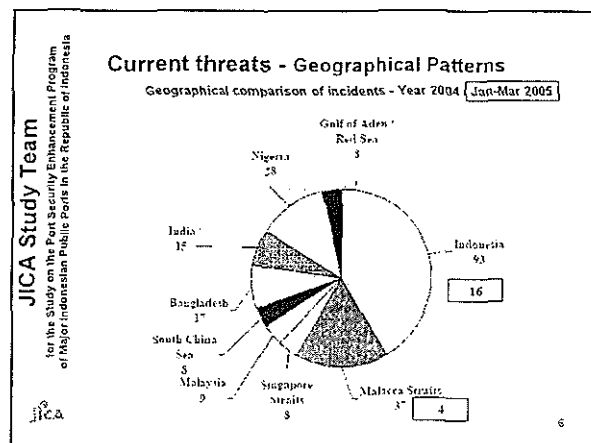
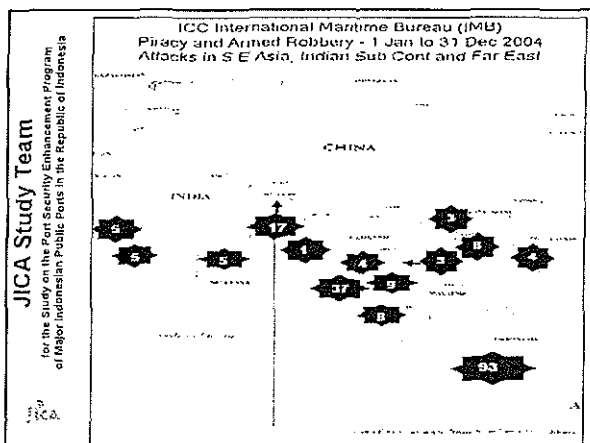
3

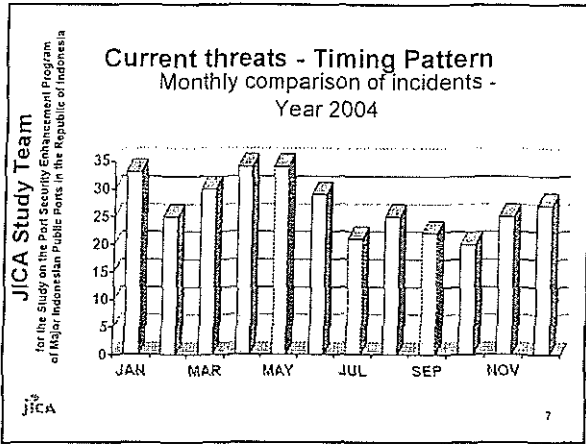
JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

Armed Attacks – Hijacking/Membajak

- Hijacking is usually done by highly organised, highly resourceful pirates with large network
- Targets are selected based on the value of the vessel and its cargo.
- The whole ship is seized, crew held hostage for ransom money, and the ship could be re-flagged and run as a 'Phantom Ship'.
- Pirates/Sea Robbers seems to have military background

4





Armed Attacks - Piracy and Hijacking

- Latest Trends – 2004 Report
- Attacked reduced from 445 (2003) to 325
- Violence (*kekerasan pertambahan*) continues to remain at high levels
- Number of crew killed increased to 30 from 21 (2003)
- Hijacking of tugs and barges
- Kidnapping (*penculikan*) increases
- Vessels being fired upon

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

JICA

Achille Lauro Hijacking
Oct 7, 1985

TERORISME

Four heavily armed Palestinian terrorists in October hijack the Italian cruise ship *Achille Lauro*, carrying more than 400 passengers and crew, off Egypt. The hijackers demand that Israel free 50 Palestinian prisoners. The terrorists killed a disabled American tourist, 69-year-old Leon Klinghoffer, and threw his body overboard with his wheelchair

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

JICA

Pan Am 103, Lockerbie Bombing,
December 21, 1988

Pan American Airlines Flight 103 was blown up over Lockerbie, Scotland, by a bomb believed to have been placed on the aircraft in Frankfurt, West Germany, by Libyan terrorists. All 259 people on board were killed.

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

JICA

1998 -U.S. Embassies, Kenya/Tanzania -
257 killed ;5,500 wounded

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

JICA

2000 USS Cole –19 killed; 37 wounded

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

MV Petro Ranger

Malaysian flag product tanker owned by a Singapore ship-owner, sailed from Singapore on 16 April 1998 for Vietnam with a cargo of gas oil and kerosene.

Nine hours later, 12-armed pirates boarded her. The crew was held hostage whilst the pirates sailed the vessel to Hainan island in China. The 21 crew members under control of the pirates were threatened with death and remained locked in the mess room for ten days. The Chinese authorities alleged that the ship was engaged in smuggling operations. They questioned the 12 alleged pirates who were carrying Indonesian travel documents. The authorities also detained and questioned the crew for over two weeks. However, on 16 October 1998, despite indisputable evidence, the pirates, who had committed a serious offence of hijacking a ship and attempting to sell the cargo, were simply sent back home without being prosecuted.

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

MV Alondra Rainbow -22/10/1999

The 8000-tonnes freighter Alondra Rainbow was hijacked when she set sail from with a compliment of 15 crew members and 7000 tonnes of aluminium ingot from port Kaula Tanjong in Indonesia on October 22. She was intercepted by the Indian Coast Guards off the Goa coast on November

JICA

14

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

MV Inabukwaw -15/03/2001

The vessel, MV Inabukwa, left the Indonesian port of Pangkalabalam for Singapore on the morning of the 15th March with a cargo of tin and white pepper. Armed pirates attacked that evening. They blindfolded the captain and the 22 crewmembers and forced them to leave the ship. The pirates then took the hostages to the deserted island of Pulau Sayap and abandoned them there. Cargo worth 2.2 million dollars.

JICA

15

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

6th Oct ULCC MT LIMBURG -1 killed ; 8 wounded



On 6th Oct 2002 ULCC MT Limburg 157,833 tons was damage by explosion at Yemen involving a small boat fitted with explosives. 1 crew member killed & 8 were hospitalised.

JICA

16

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

Container Ships – The Next Terrorist Weapon?

OCTOBER 25 2001
ITALIAN police were investigating last night why a suspected al-Qaeda hijacker would smuggle himself halfway around the world locked inside a shipping container with its own bed and toilet.

The bizarre discovery of an Egyptian carrying a Canadian passport was made on the dockside in Gioia Tauro in southern Italy, where detectives believe they may have foiled another hijacking. He was found with a laptop computer, two mobile phones, cameras, a Canadian passport, other identity documents and a certificate saying he is an aircraft mechanic.

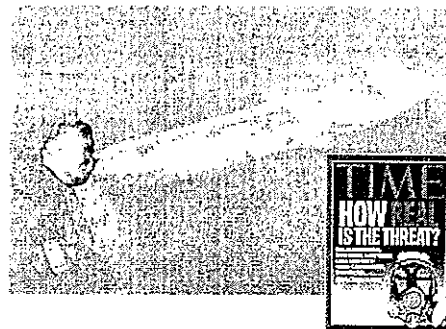


JICA

17

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

Another Likely Scenario?



JICA

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Public Ports in the Republic of Indonesia

Another 9/11 - Ship as a weapon?

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Public Ports in the Republic of Indonesia

WHAT A DIFFERENCE, A DAY MAKE

911 : ONE YEAR LATER

IMO adopted comprehensive maritime security measures in December 2002, including a new International Ship and Port Facility Security Code (ISPS Code)

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Public Ports in the Republic of Indonesia

Maritime Terrorism

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Public Ports in the Republic of Indonesia

Current Security Threats -Maritime Terrorism

- Terrorist attacks on maritime target are comparatively rare, only 2% of all terrorist incidents in the last 30 years.
- Most terrorists are land based with little experience in maritime environment
- However, there are some notable ones; eg al-Qaeda, The LTTE, Palestinian groups etc
- Examples of high profile attacks:
 - The seizure of the Achille Lauro in 1985
 - The Bombing of Philippine ferry in Feb 2000 (45 killed)
 - The suicide attack against USS Cole in Oct 2000 (19 killed)
 - The ramming of French oil tanker Limburg in Oct 2002

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Public Ports in the Republic of Indonesia

Current Security Threats -Maritime Terrorism

• Threat Matrix - Terrorist Behaviour and Target Selection

Motive
Revenge; Mass media coverage; Political alarms; Economic disruption

Opportunity
Un-policed areas; Lax port security; Ships with low security awareness and readiness

Capability
Intelligence; Weapons; Know-how; Equipment; Manpower

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Public Ports in the Republic of Indonesia

Maritime Terrorism- An Increasing Threat

- Maritime Terrorism is perceived to increase in the recent years due to the following:
 - **Opportunity**
 - Lax Port Security
 - Poor Coastal Surveillance
 - Profusion of Targets
 - trend towards 'skeleton crew'
 - **Motive**
 - Alternative venue for mass casualty attacks
 - LNG carriers/ terminals; oil refineries
 - Cruise ships; passenger liners
 - Precedent of successful attacks generated enormous political capital, and underscored vulnerability of ships and ports
 - Growing dependent of Global Trade on maritime choke points
 - **Capability**
 - Terrorists showing increased tactical and technical sophistication

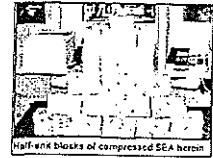
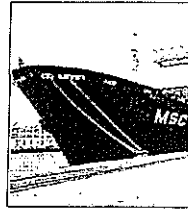
JICA

Maritime Terrorism- An Increasing Threat

- A vessel that is targeted by terrorists may be :
 1. a victim - when it is attacked by the terrorists, its crew/ passengers taken hostage (even killed), and the ship exploded;
 2. a means of transfer - when it is used to convey people, equipment or weapons; or
 3. a weapon - when it is used to cause collision, ramming, oil spill or even

25

Smuggling Penyelundupan



Half-ton blocks of compressed SEA bricks



26

Current Security Threat - Smuggling

- Drug Smuggling
- Human Smuggling
- Arms, Contraband and others

27

Drug Smuggling

- 'Containerised' Drug Smuggling
 - More in South East Asia
 - Import/ export companies or warehouses may be set up in source countries, or transit countries to smuggle/ store the drugs.
 - Names of these front companies change frequently.
 - Drugs are usually concealed within commercial cargo. Typically, one entire container filled with only low cost commodities.
 - Drugs are usually packed in cardboard cartons of the same size and weight as the other commodities.
 - Cartons containing the drugs are normally placed deep within the container

28

Drug Smuggling

- 'Containerised' Drug Smuggling- conti..
 - Usually less than 10 cartons of drugs are concealed among 600 to 1800 cartons of commercial cargo.
 - Pallets containing drug-laden cartons usually have different numbers or are marked in some distinguish ways.
 - Typically, the container that contain drugs are insured for more than the actual value of the commercial cargo - as much as 5 to 10 times.
 - Often drugs shipment transit a secondary port prior to the final destination.

- Source from DEA

29

Human Smuggling


- In the last decade, the process of globalisation has driven unprecedented amount of migrants from less developed countries of Asia, Africa, South America and Eastern Europe to Western Europe, North America and Australia.
- Growing evidence that transnational organised criminal groups are involved in human smuggling for financial gain.
- Such criminal network gain increasing control of the flow of migrants across borders.
- Known smuggling routes:
 - From Asia via southern CIS countries to Russia, then to Western Europe and US;
 - From Sub-Saharan region of Africa to Morocco, then to southern Spain via Strait of Gibraltar.



JICA Study Team
 for the Study on the Port Security Enhancement Program
 of Major Indonesian Public Ports in the Republic of Indonesia

Human Smuggling

- From Middle East and South Asia via Malaysia to Batam (Indonesia) then to Jakarta and Bali, and from there to west coast of Australia.
- From Asia to Central and South America, then via Mexico to North America. A new route for Asia migrants (particularly Chinese nationals) is via Africa to Western Europe.
- Trends
- It is established that Human smugglers are making higher profit in the recent years as they smuggle increasing number of migrants at the same time.
- The vessels are mostly insufficiently equipped with drinking water and food. Treatment of migrants by the crew and guards is extremely violent. Sick people are often thrown over board.




JICA

JICA Study Team
 for the Study on the Port Security Enhancement Program
 of Major Indonesian Public Ports in the Republic of Indonesia

Arms Smuggling

- Usually by highly organised criminals or terrorists, some with state support.
- Weapon continues to be in high demand throughout the world.
- Transporting illicit arms by sea allows smugglers to move large amount of weaponry among legitimate cargo, and within legitimate transportation infrastructure.
- The full extend of maritime arms smuggling is unknown.
- Identifying illicit arms shipments become increasingly difficult as the volume of commercial seaborne trade triples.
- Container ships are the most commonly used means of maritime arms smuggling.



JICA

JICA Study Team
 for the Study on the Port Security Enhancement Program
 of Major Indonesian Public Ports in the Republic of Indonesia

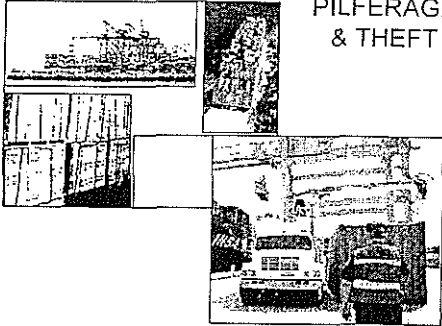
Contraband and other smuggling

- Tobacco
- Oil
- Antiques
- Vehicles and vehicle parts
- Electrical appliances

JICA

JICA Study Team
 for the Study on the Port Security Enhancement Program
 of Major Indonesian Public Ports in the Republic of Indonesia

PENYEROBOTAN DAN PENCURIAN PILFERAGE & THEFT



JICA

JICA Study Team
 for the Study on the Port Security Enhancement Program
 of Major Indonesian Public Ports in the Republic of Indonesia

Current Security Threat - Theft of Cargo

- Multi-million dollar cargoes stolen by Organised criminal groups who operate vessels.
- ❖ Often offer bargain freight rates to shippers. After obtaining cargoes, discharge them at ports other than the originally contracted ones. Cargoes often sold illegally at reduced price.
- ❖ Cargoes targeted are those that are easily disposed off.
- ❖ Chances of recovering the stolen cargoes are minimal.
- ❖ Identity of such vessels change very frequently, even at sea.
- ❖ A possible resurgence of ship deviations from ports.
- ❖ The first 3 such cases reported at Eastern Mediterranean (Sep 02), North Africa (Nov 02), and West Africa (Dec 02).

JICA

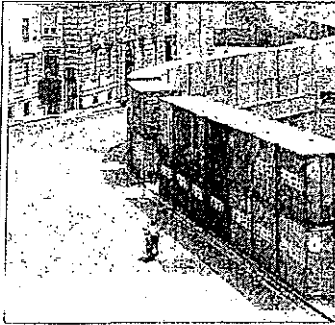
JICA Study Team
 for the Study on the Port Security Enhancement Program
 of Major Indonesian Public Ports in the Republic of Indonesia

Security measures taken by some countries

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

Extreme Security Measures?



G-8 FACE-OFF



Italian security personnel has hardened off the summit venue, with the red zone cut off bounds to the protesters. More than 16,000 riot police and 3,000 army troops are being deployed in the port city to deal with the expected clashes as the leaders of the US, Russia, Japan, Germany, France, Italy, Britain and Canada meet.

Security measures in Gama include these containers stacked on board as to they protect them from rioters on piles in the street below

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

Shallow Water Intruder Detection System Programme

- ZAK, a 170 kg California sea lion patrols the San Diego harbour.
- ZAK is trained to locate swimmers near piers, ships, and suspicious objects.


Part of US' Space and Naval Warfare Systems Centre's Shallow₃₈ Water Intruder Detection System programme.

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

Swimmer Detection Radar Network

for All-Case Port Surveillance



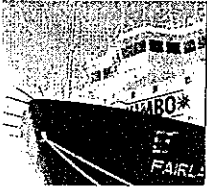
A radar network of 2000 is being installed in the port area to detect swimmers and suspicious objects. The network will be installed in the port area and will be used to detect swimmers and suspicious objects. The network will be installed in the port area and will be used to detect swimmers and suspicious objects.

JICA


JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

DECK PROTECTION

SecureShip System



Sentor Vision



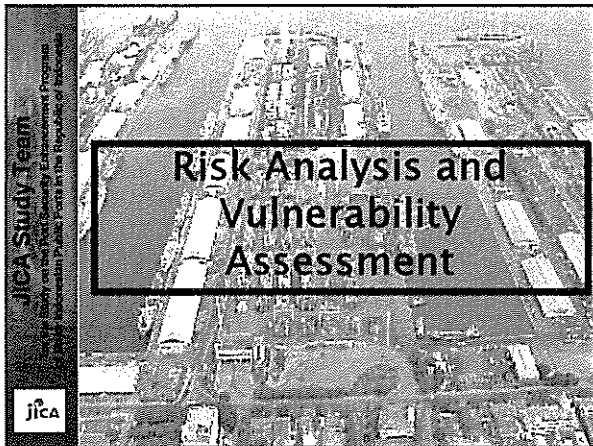
JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

Thank you

JICA

41



Risk and Vulnerability Assessment

Security is more art than science. Few formulas will cover all organizations, situations and needs, and that is the beauty and challenge of our profession. We are about probabilities.

- Richard D.Sem, CPP
Are These Truths Self-Evident?
Security Management, March 1998

Risk and Vulnerability Assessment

LESSON OBJECTIVE

- Conduct a Threat Evaluation & Risk Assessment

Port Facility Security Assessment (PFSA)

- A process that identifies weakness that may lead to a security breach and may suggest options to eliminate or mitigate those weakness.
- PFSA is an essential and integral part of the process of developing PFSP.

Port Facility Security Assessment (PFSA)

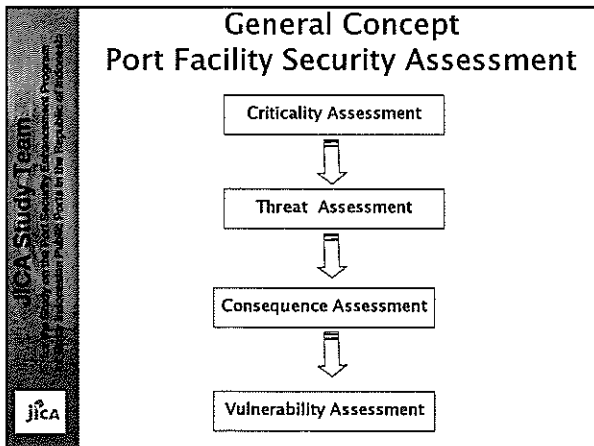
According to ISPS Code Part A/15, PFSA shall at least include the following elements:

- 1 Identification and evaluation of important assets and infrastructure it is important to protect;
- 2 Identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures;
- 3 Identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability; and
- 4 Identification of weaknesses, including human factors in the infrastructure, policies and procedures.

Port Facility Security Assessment

The PFSA should address the following elements within a port facility (ISPS Code Part B15.3):

- Physical security
- Structural integrity
- Personnel protection systems
- Procedural policies
- Radio/Comm systems
- Relevant transportation infrastructure
- Utilities
- Other areas that may, if damaged pose a risk to operations within the port facility



General Concept Port Facility Security Assessment

CRITICALITY ASSESSMENT

Identify critical operations and infrastructure

Identify those specific infrastructure that support critical operations of the port.

All identified should be included. Those considered but dismissed for evaluation should be documented for future reference.

General Concept Port Facility Security Assessment

CRITICALITY ASSESSMENT

Target	Mission	Effect of Target Destruction	Ability to Recover	Criticality
<i>Bridge Ulliy Pier Tunnel Waterway Other</i>	<i>Public Health Commerce Safety / Defense Transportation Communications Other</i>	<i>Loss of Life Economic Impact Environmental Impact Public Safety / Defense Symbolic Significance</i>	<i>Excellent Good Fair Poor None</i>	<i>Critical Moderate Marginal</i>

General Concept Port Facility Security Assessment

THREAT ASSESSMENT

Define Scenarios
List the Scenarios.

An attack scenario consists of a potential threat to a unique target or target class under specific circumstances.

It is important that the developed scenario or scenarios are within the realm of possibility and, must address known capabilities and intents as evidenced by past events and available intelligence.

General Concept Port Facility Security Assessment

THREAT ASSESSMENT

Typical Types of Scenarios.

- Intrude and/or take control of the target
 - With explosive
 - Through malicious ops
 - Create hazardous or pollution
- Externally attack the target
 - Moving explosives adjacent to target
 - Ramming a stationary target
 - Launching weapons from a distance
- Use the target as a means of transferring
 - Contraband/people

General Concept Port Facility Security Assessment

CONSEQUENCE/VULNERABILITY ASSESSMENT

Conduct consequence and vulnerability assessment for each scenario

Document Assessments.
Evaluate each target/attack scenario combination in terms of the potential consequences of the attack and the vulnerability of the target to the attack.

**General Concept
Port Facility Security Assessment**

CATEGORIZING TARGET/SCENARIO COMBINATION

Document Prioritization.

Determine which scenarios should have mitigation strategies, and also document why other scenarios did not need mitigation strategies, based on the consequence and vulnerability assessment.

JICA Study Team
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program

JICA

**General Concept
Port Facility Security Assessment**

DETERMINING MITIGATION STRATEGIES
/IMPLEMENTATION METHODS

Develop mitigation

Prevention and Mitigation

List a tiered and scalable security procedures to be developed and it is likely to be a combination of voluntary and mandatory procedures that will be the shared responsibility of the country, vessels and facilities operating in the port.

JICA Study Team
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program

JICA

Threat Evaluation & Risk Assessment

Risk Based Analysis Process

The analysis process consists of 5 steps:

Navigation and Vessel Inspection Circulars
NVIC 11-02: Security Guidelines for Facilities

JICA Study Team
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program

JICA

Threat Evaluation & Risk Assessment

Risk can be represented as the product of the probability and consequence of a given security breach.

$$R = P * C$$

where

R = risk score for a given security breach

P = probability – probability of a security breach. The probability of a security breach can further be defined as the product of threat (T) and vulnerability (V).

C = consequence – the sum of possible consequences associated with a successful security breach. Consequences may be based on impacts to life, economic security, symbolic value, and national defense.

JICA Study Team
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program

JICA

Threat Evaluation & Risk Assessment

Risk management principles acknowledge that while risk generally cannot be totally eliminated, it can be reduced by adjusting operations to reduce

consequence (C?),
threat (T?), or
vulnerability (V?).

Generally it is easier to reduce vulnerabilities than to reduce consequences or threats.

JICA Study Team
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program

JICA

Threat Evaluation & Risk Assessment

The final goal of risk management is to achieve an adequately low and consistent level of risk.

The goal for maritime security is to ensure

Threat (T)

Consequence (C), Vulnerability (V)

JICA Study Team
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program
JICA Study Team for the Security Assessment Program

JICA

Threat Evaluation & Risk Assessment

Example:
A port may decide to increase security checks (V?) after receiving a bomb threat (T?).

↑

Threat (T)

Vulnerability (V)

↓

Threat Evaluation & Risk Assessment

- Step 1: Selecting potential threat scenario
- Step 2: Determine facility's consequence Level
- Step 3: Determine if the scenario requires a mitigation strategy
- Step 4: Assess impact of mitigation strategy (protective measures)
- Step 5: Implement mitigation strategy

STEP 1: Selecting Potential Threat Scenario

- Consider attack scenario(s), potential threat to the facility under specific circumstances.
- Possible security threats need not be too detailed.
- Brainstorming session, there is no standard answer.
- Use the standard list of possible threat scenarios as mentioned in the ISPS Code, Part B, 15.11

STEP 1: Selecting Potential Threat Scenario

ISPS Code, Part B, 15.11

- Damage by explosive devices, arson, sabotage or vandalism;
- hijacking or seizure of the ship or of persons on board;
- tampering with cargo, ship equipment or ship's stores;
- unauthorized access or use, including stowaways;
- smuggling weapons or equipment, including weapons of mass destruction;
- Use of the ship to carry those intending to cause a security incident and/or their equipment;
- use of the ship itself as a weapon or as a means to cause damage or destruction;
- blockage of port entrances
- nuclear, biological and chemical attack

STEP 1: Select Potential Threat Scenario

Step 1 Possible Threat & Scenario	Step 2 Consequence Score	Step 3 Vulnerability			Step 4 Mitigation Needed?
		Accessibility	Organic Security	Total	
Damage to, or destruction of port facility					
Hijacking ship interfaces with port facility					
Tampering of cargoes					
Smuggling weapons					
Use the ship itself as weapon					

STEP 2: Determine Consequence Level

- Each scenario should be evaluated in terms of the consequence level

Consequence Level	
3	Facilities that transfer, stores, or otherwise handle a certain dangerous cargoes
2	Facilities that store other than dangerous cargoes, receive vessel that are certificated to carry more than 150 passengers and receive vessel on international voyages
1	Facilities other than those above

STEP 2: Determine Consequence Level

Consequence Calculation			
Death & Injury	Economic	Environmental	Highest Consequence
2	2	1	2


use highest figure

Consequence Score	
3	CATASTROPHIC : numerous loss of life or injuries; major national or long term economic impact; complete destruction of multiple aspects of the eco-system over a large area
2	SIGNIFICANT : multiple loss of life or injuries; major regional economic impact; long-term damage to a portion of the eco-system
1	MODERATE : little or no loss of life or injuries; minimal economic impact; some environmental damage

STEP 2: Determine Consequence Level

Possible Threat & Scenario	Consequence Score	Step 3			Mitigation Needed?
		Accessibility	Organic Security	Total	
Damage to, or destruction of port facility	2				
Hijacking ship interfaces with port facility	2				
Tampering of cargoes	2				
Smuggling weapons	2				
Use the ship itself as weapon	2				

STEP 3: Determine Vulnerability



VULNERABILITY FACTORS

- Availability
- Accessibility
- Organic security
- Facility hardness

STEP 3: Determine Vulnerability

- Availability
 - The facility presence and predictability as it relates to the ability to plan an attack.
- Facility hardness
 - The ability of the facility to withstand the specific attack based on the complexity of the facility design and material construction characteristics

STEP 3: Determine Vulnerability

- Accessibility
 - Accessibility of the facility to the attack scenario. This relates to physical and geographic barriers that deter the threat independently of organic security.
- Organic Security
 - The ability of the security personnel to deter the attack. It includes having in place security measures and plans, communication capability, guard force, intrusion detection systems, and timeliness of outside law enforcement to prevent attack.

STEP 3: Determine Vulnerability

Vulnerability Score		
Accessibility	Organic Security	Total Score
2	3	5

Total

Vulnerability Score	
Accessibility	Organic Security
3 No deterrence (e.g. unrestricted access to vessel and unrestricted external movement)	No deterrence capability (e.g. no plan, no guard force, no emergency communication, outside law enforcement not available for timely prevention, no detection capability)
2 Good deterrence (e.g. single substantial barrier; unrestricted access to within 100 yards of vessel)	Good deterrence capability (e.g. minimal security plan, some communications, armed guard force of limited size relative to the vessel, outside law enforcement not available for timely prevention, limited detection systems)
1 Excellent deterrence (expected to deter attack; access restricted within 500 yards of vessel, multiple physical/geographical barriers)	Excellent deterrence capability expected to deter attack; covert security elements that represent additional elements not visible or apparent

STEP 3: Determine Vulnerability

Possible Threat & Scenario	Step 1	Step 2	Step 3			Step 4
	Consequence Score	Accessibility	Vulnerability		Mitigation Needed?	
			Organic Security	Total		
Damage to, or destruction of port facility		2	2	3	5	
Hijacking ship interfaces with port facility		2	2	3	5	
Tampering of cargoes		2	2	3	5	
Smuggling weapons		2	2	3	5	
Use the ship itself as weapon		2	2	3	5	

- STEP 4: Assess Impact of Mitigation Strategy**
- Determine which scenarios require mitigation strategies (protective measures) to be implemented.
 - 3 Mitigation categories:
 - Mitigate
 - Consider
 - Document
 - Based on the consequences and vulnerability assessment scores.

- STEP 4: Assess Impact of Mitigation Strategy**
- Mitigation categories:
- Mitigate :**
Develop a protective measures and/or procedures to reduce risk for that scenario.
 - Consider :**
Scenario should be considered and mitigation strategies should be developed on a case-by-case basis.
 - Document :**
Scenario may not need a mitigation measure at this time and therefore needs only to be documented.

STEP 4: Assess Impact of Mitigation Strategy

Table 4 - Mitigation Score

Consequence	Mitigation Score				
	Total Vulnerability Score				
	2	3	4	5	6
3	Consider	Consider	Mitigate	Mitigate	Mitigate
2	Document	Consider	Consider	Mitigate	Mitigate
1	Document	Document	Document	Consider	Consider

STEP 4: Assess Impact of Mitigation Strategy

Possible Threat & Scenario	Step 1	Step 2	Step 3			Step 4
	Consequence Score	Accessibility	Vulnerability		Mitigation Needed?	
			Organic Security	Total		
Damage to, or destruction of port facility		2	2	3	5	M
Hijacking ship interfaces with port facility		2	2	3	5	
Tampering of cargoes						
Smuggling weapons						
Use the ship itself as weapon						

Consequence	Mitigation Score				
	Total Vulnerability Score				
	2	3	4	5	6
3	Consider	Consider	Mitigate	Mitigate	Mitigate
2	Document	Consider	Consider	Mitigate	Mitigate
1	Document	Document	Document	Consider	Consider

- STEP 5: Implement Mitigation Strategy**
- Determine which scenarios require mitigation to reduce vulnerabilities.
 - The overall desire is to reduce the risk associated with the identified scenario.
 - Generally it is easier to reduce vulnerabilities than to reduce consequences.
 - In determining if a mitigation strategy should be implemented, there are two factors to consider:
 - Effectiveness
 - Feasibility

STEP 5: Implement Mitigation Strategy (Effectiveness)

- Highly effective: implementation lowers the mitigation category.

Mitigation Score						
Total Vulnerability Score						
Consequence	2	3	4	5	6	
3	Consider	Consider	Document	Document	Document	Document
2	Document	Document	Consider	Consider	Document	Document
1	Document	Document	Document	Consider	Consider	

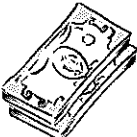
STEP 5: Implement Mitigation Strategy (Effectiveness)

- Partially effective : lower overall vulnerability score when implemented by itself or with one or more other strategies.

Mitigation Score						
Total Vulnerability Score						
Consequence	2	3	4	5	6	
3	Consider	Consider	Document	Document	Document	Document
2	Document	Document	Consider	Consider	Document	Document
1	Document	Document	Document	Consider	Consider	

STEP 5: Implement Mitigation Strategy (Feasibility)

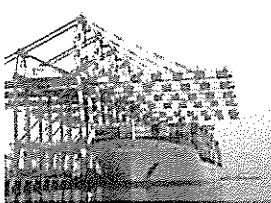
- Feasible : little operational impact or funding relative to the prospective reduction in vulnerability.
- Partially feasible : Requires significant changes or funding relative to the prospective reduction in vulnerability.
- Not feasible : if its implementation is extremely problematic or is cost prohibitive.



STEP 5: Implement Mitigation Strategy

Possible Threat & Scenario	Mitigation Strategy	Step 5		Step 4 Mitigation Needed?
		Residual Consequence	Residual Vulnerability	
Damage to, or destruction of port facility	Access Control, ID Checks and restrict free access for ship crew	2	4	C
Hijacking ship Interfaces with port facility	Monitoring sea approaches	2	4	C
Tampering of cargoes	Supervise Cargo Ops and proper documentation	2	4	C
Smuggling weapons	Access Control personnel, vehicles & ships	2	4	C
Use the ship itself as weapon	ETA ships and comms	2	4	C

Port Facility Security Assessment Example



Threat Evaluation & Risk Assessment

- Step 1: Selecting potential threat scenario
- Step 2: Determine facility's consequence Level
- Step 3: Determine if the scenario requires a mitigation strategy
- Step 4: Assess impact of mitigation strategy (protective measures)
- Step 5: Implement mitigation strategy

Port Facility Security Assessment Example

- Facility: International Multi-purposes Terminal
- Type of ships calling at this facility: Container Ships/ Large Passenger Ships
- Accessibility to Facility: Limited barriers and fencings have been set up to prevent access.
- Organic Security: There is no organic armed security forces deployed in the whole facility.

STEP 1: Select Potential Threat Scenario

Possible Threat & Scenario	Step 2 Consequence Score	Step 3 Vulnerability			Step 4 Mitigation Needed?
		Accessibility	Organic Security	Total	
Damage to, or destruction of port facility					
Hijacking ship interfaces with port facility					
Tampering of cargoes					
Smuggling weapons					
Use the ship itself as weapon					

STEP 2: Determine Consequence Level

Consequence Calculation			
Death & Injury	Economic	Environmental	Highest Consequence
2	2	1	2

use highest figure

Consequence Score	
3	CATASTROPHIC : numerous loss of life or injuries; major national or long term economic impact; complete destruction of multiple aspects of the eco-system over a large area
2	SIGNIFICANT : multiple loss of life or injuries; major regional economic impact; long-term damage to a portion of the eco-system
1	MODERATE : little or no loss of life or injuries; minimal economic impact; some environmental damage

STEP 2: Determine Consequence Level

Possible Threat & Scenario	Step 2 Consequence Score	Step 3 Vulnerability			Step 4 Mitigation Needed?
		Accessibility	Organic Security	Total	
Damage to, or destruction of port facility	2				
Hijacking ship interfaces with port facility	2				
Tampering of cargoes	2				
Smuggling weapons	2				
Use the ship itself as weapon	2				

STEP 3: Determine Vulnerability

Vulnerability Score		
Accessibility	Organic Security	Total Score
2	3	5

total

Vulnerability Score	
Accessibility	Organic Security
3	No deterrence capability (no plan, no guard force, no emergency comms, outside law enforcement not available for timely prevention no detection capability)
2	Good deterrence capability (e.g. some security plan, some comms, armed guard force of fair of size relative to ship / port, outside law enforcement not available for timely prevention limited detection systems)
1	Excellent deterrence capability - should deter attack; covert security elements that represent additional elements not visible or apparent)

STEP 3: Determine Vulnerability

Possible Threat & Scenario	Step 2 Consequence Score	Step 3 Vulnerability			Step 4 Mitigation Needed?
		Accessibility	Organic Security	Total	
Damage to, or destruction of port facility	2	2	3	5	
Hijacking ship interfaces with port facility	2	2	3	5	
Tampering of cargoes	2	2	3	5	
Smuggling weapons	2	2	3	5	
Use the ship itself as weapon	2	2	3	5	

STEP 4: Assess Impact of Mitigation Strategy

Table 4 – Mitigation Score

Mitigation Score					
Consequence	Total Vulnerability Score				
	2	3	4	5	6
3	Consider	Consider	Mitigate	Mitigate	Mitigate
2	Document	Consider	Consider	Mitigate	Mitigate
1	Document	Document	Document	Consider	Consider

STEP 4: Assess Impact of Mitigation Strategy

Step 1	Step 2	Step 3			Step 4																																			
Possible Threat & Scenario	Consequence Score	Vulnerability			Mitigation Needed?																																			
		Accessibility	Organic Security	Total																																				
Damage to, or destruction of port facility	2	2	3	5																																				
Hijacking ship interfaces with port facility	2	2	3	5																																				
Tampering of cargoes	<table border="1"> <thead> <tr> <th colspan="6">Mitigation Score</th> </tr> <tr> <th rowspan="2">Consequence</th> <th colspan="5">Total Vulnerability Score</th> </tr> <tr> <th>2</th> <th>3</th> <th>4</th> <th>5</th> <th>6</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>Consider</td> <td>Consider</td> <td>Mitigate</td> <td>Mitigate</td> <td>Mitigate</td> </tr> <tr> <td>2</td> <td>Document</td> <td>Consider</td> <td>Consider</td> <td>Mitigate</td> <td>Mitigate</td> </tr> <tr> <td>1</td> <td>Document</td> <td>Document</td> <td>Document</td> <td>Consider</td> <td>Consider</td> </tr> </tbody> </table>					Mitigation Score						Consequence	Total Vulnerability Score					2	3	4	5	6	3	Consider	Consider	Mitigate	Mitigate	Mitigate	2	Document	Consider	Consider	Mitigate	Mitigate	1	Document	Document	Document	Consider	Consider
Mitigation Score																																								
Consequence	Total Vulnerability Score																																							
	2	3	4	5	6																																			
3	Consider	Consider	Mitigate	Mitigate	Mitigate																																			
2	Document	Consider	Consider	Mitigate	Mitigate																																			
1	Document	Document	Document	Consider	Consider																																			
Smuggling weapons	3	Consider	Consider	Mitigate	Mitigate																																			
Use the ship itself as weapon	2	Document	Consider	Consider	Mitigate																																			

STEP 4: Assess Impact of Mitigation Strategy

Step 1	Step 2	Step 3			Step 4																																			
Possible Threat & Scenario	Consequence Score	Vulnerability			Mitigation Needed?																																			
		Accessibility	Organic Security	Total																																				
Damage to, or destruction of port facility	2	2	3	5	M																																			
Hijacking ship interfaces with port facility	2	2	3	5																																				
Tampering of cargoes	<table border="1"> <thead> <tr> <th colspan="6">Mitigation Score</th> </tr> <tr> <th rowspan="2">Consequence</th> <th colspan="5">Total Vulnerability Score</th> </tr> <tr> <th>2</th> <th>3</th> <th>4</th> <th>5</th> <th>6</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>Consider</td> <td>Consider</td> <td>Mitigate</td> <td>Mitigate</td> <td>Mitigate</td> </tr> <tr> <td>2</td> <td>Document</td> <td>Consider</td> <td>Consider</td> <td>Mitigate</td> <td>Mitigate</td> </tr> <tr> <td>1</td> <td>Document</td> <td>Document</td> <td>Document</td> <td>Consider</td> <td>Consider</td> </tr> </tbody> </table>					Mitigation Score						Consequence	Total Vulnerability Score					2	3	4	5	6	3	Consider	Consider	Mitigate	Mitigate	Mitigate	2	Document	Consider	Consider	Mitigate	Mitigate	1	Document	Document	Document	Consider	Consider
Mitigation Score																																								
Consequence	Total Vulnerability Score																																							
	2	3	4	5	6																																			
3	Consider	Consider	Mitigate	Mitigate	Mitigate																																			
2	Document	Consider	Consider	Mitigate	Mitigate																																			
1	Document	Document	Document	Consider	Consider																																			
Smuggling weapons	3	Consider	Consider	Mitigate	Mitigate																																			
Use the ship itself as weapon	2	Document	Consider	Consider	Mitigate																																			

STEP 3: Determine Vulnerability

Step 1	Step 2	Step 3			Step 4
Possible Threat & Scenario	Consequence Score	Vulnerability			Mitigation Needed?
		Accessibility	Organic Security	Total	
Damage to, or destruction of port facility	2	2	3	5	
Hijacking ship interfaces with port facility	2	2	3	5	
Tampering of cargoes	2	2	3	5	
Smuggling weapons	2	2	3	5	
Use the ship itself as weapon	2	2	3	5	

STEP 3: Determine Vulnerability

Step 1	Step 2	Step 3			Step 4
Possible Threat & Scenario	Consequence Score	Vulnerability			Mitigation Needed?
		Accessibility	Organic Security	Total	
Damage to, or destruction of port facility	2	2	3	5	
Hijacking ship interfaces with port facility	2	2	3	5	
Tampering of cargoes	2	2	3	5	
Smuggling weapons	2	2	3	5	
Use the ship itself as weapon	2	2	3	5	

We are going to implement security measures to reduce vulnerability

STEP 5: Implement Mitigation Strategy

Step 1	Step 2	Step 3	Step 4	
Possible Threat & Scenario	Mitigation Strategy	Revised Consequence	Revised Vulnerability	Mitigation Needed?
		2	5	
Damage to, or destruction of port facility		2	5	M
Hijacking ship interfaces with port facility		2	5	M
Tampering of cargoes		2	5	M
Smuggling weapons		2	5	M
Use the ship itself as weapon		2	5	M

STEP 5: Implement Mitigation Strategy				
Step 1	Step 5	Step 3	Step 4	Step 4
Possible Threat & Scenario	Mitigation Strategy	Revised Consequence	Revised Vulnerability	Mitigation Needed?
Damage to, or destruction of port facility	Access Control, ID Checks and restrict free access for ship crew	2	4	C
Hijacking ship interfaces with port facility		2	5	M
Tampering of cargoes		2	5	M
Smuggling weapons		2	5	M
Use the ship itself as weapon		2	5	M

STEP 5: Implement Mitigation Strategy				
Step 1	Step 5	Step 3	Step 4	Step 4
Possible Threat & Scenario	Mitigation Strategy	Revised Consequence	Revised Vulnerability	Mitigation Needed?
Damage to, or destruction of port facility	Access Control, ID Checks and restrict free access for ship crew	2	4	C
Hijacking ship interfaces with port facility	Monitoring sea approaches	2	4	C
Tampering of cargoes		2	5	M
Smuggling weapons		2	5	M
Use the ship itself as weapon		2	5	M

STEP 5: Implement Mitigation Strategy				
Step 1	Step 5	Step 3	Step 4	Step 4
Possible Threat & Scenario	Mitigation Strategy	Revised Consequence	Revised Vulnerability	Mitigation Needed?
Damage to, or destruction of port facility	Access Control, ID Checks and restrict free access for ship crew	2	4	C
Hijacking ship interfaces with port facility	Monitoring sea approaches	2	4	C
Tampering of cargoes	Supervise Cargo Ops and proper documentation	2	4	C
Smuggling weapons	Access Control personnel, vehicles & ships	2	4	C
Use the ship itself as weapon	ETA ships and comms	2	4	C

RISK ANALYSIS TABLE				
1	2	3	4	5
Threats (Article 15.11 of Part B of the ISPS Code)	Order these threats as they concern you, highest to lowest	Assets of High Value or Critical to your Operations Affected by Threats	Existing Safeguards or Apparent Weaknesses	Possible Corrective Measures to Address Weaknesses
Damage to, or destruction of, the port, port facility or a ship alongside, e.g. by explosive devices, arson, sabotage, suicide bombing or vandalism.	Example HIGH MEDIUM LOW	Example 1. Electrical Sub-stations 2. Dangerous Goods (DG) Yard 3. Computer Room 4. Control Station	Example 1a. Electrical Sub-stations are fenced off around 1b. Security personnel patrol electrical sub-stations regularly 2. Nil 3. Nil 4. Regular patrol by security personnel	Example 1. Nil Required 2a. Installing CCTV to monitor DG Yards. 2b. Security personnel to patrol DG yard regularly 3. Increase security patrols to monitor computer room 4. Nil required.

RISK ANALYSIS TABLE				
1	2	3	4	5
Threats (Article 15.11 of Part B of the ISPS Code)	Order these threats as they concern you, highest to lowest	Assets of High Value or Critical to your Operations Affected by Threats	Existing Safeguards or Apparent Weaknesses	Possible Corrective Measures to Address Weaknesses
Hijacking or seizure of port/port facility, ship alongside, service vessels or of persons on board.	Example HIGH MEDIUM LOW	Example 1. Electrical Sub-stations 2. Dangerous Goods (DG) Yard 3. Computer Room 4. Control Station	Example 1a. Electrical Sub-stations are fenced all around 1b. Security personnel patrol electrical sub-stations regularly 2. Nil 3. Nil 4. Regular patrol by security personnel	Example 1. Nil Required 2a. Installing CCTV to monitor DG Yards. 2b. Security personnel to patrol DG yard regularly 3. Increase security patrols to monitor computer room 4. Nil required.

RISK ANALYSIS TABLE				
1	2	3	4	5
Threats (Article 15.11 of Part B of the ISPS Code)	Order these threats as they concern you, highest to lowest	Assets of High Value or Critical to your Operations Affected by Threats	Existing Safeguards or Apparent Weaknesses	Possible Corrective Measures to Address Weaknesses
Tampering with cargo, baggage, ship's stores, essential port/port facility equipment or systems (including security or communications systems).	Example HIGH MEDIUM LOW	Example 1. Electrical Sub-stations 2. Dangerous Goods (DG) Yard 3. Computer Room 4. Control Station	Example 1a. Electrical Sub-stations are fenced all around 1b. Security personnel patrol electrical sub-stations regularly 2. Nil 3. Nil 4. Regular patrol by security personnel	Example 1. Nil Required 2a. Installing CCTV to monitor DG Yards. 2b. Security personnel to patrol DG yard regularly 3. Increase security patrols to monitor computer room 4. Nil required.

RISK ANALYSIS TABLE				
1	2	3	4	5
Threats (Article 15.11 of Part B of the ISPS Code)	Order these threats as they concern you, highest to lowest	Assets of High Value or Critical to your Operations Affected by Threats	Existing Safeguards or Apparent Weaknesses	Possible Corrective Measures to Address Weaknesses
Unauthorised access to the port/port facility including presence of stowaways on board a ship alongside.	Example HIGH MEDIUM LOW	Example 1.Electrical Sub-stations 2.Dangerous Goods (DG) Yard 3.Computer Room 4.Control Station	Example 1a. Electrical Sub-stations are fenced all around 1b. Security personnel patrol electrical sub-stations regularly 2.Nil 3.NIL 4. Regular patrol by security personnel	Example 1. Nil Required 2a.Installing CCTV to monitor DG Yards. 2b. Security personnel to patrol DG yard regularly 3. Increase security patrols to monitor computer room 4. Nil required.

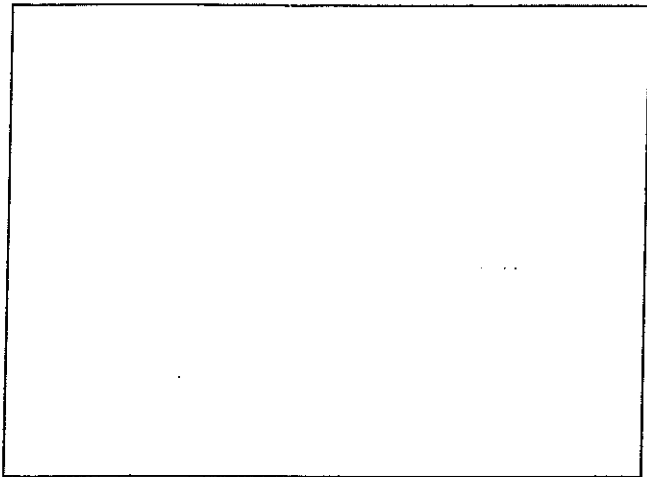
RISK ANALYSIS TABLE				
1	2	3	4	5
Threats (Article 15.11 of Part B of the ISPS Code)	Order these threats as they concern you, highest to lowest	Assets of High Value or Critical to your Operations Affected by Threats	Existing Safeguards or Apparent Weaknesses	Possible Corrective Measures to Address Weaknesses
Smuggling weapons or equipment, including weapons of mass destruction	Example HIGH MEDIUM LOW	Example 1.Electrical Sub-stations 2.Dangerous Goods (DG) Yard 3.Computer Room 4.Control Station	Example 1a. Electrical Sub-stations are fenced all around 1b. Security personnel patrol electrical sub-stations regularly 2.Nil 3.NIL 4. Regular patrol by security personnel	Example 1. Nil Required 2a.Installing CCTV to monitor DG Yards. 2b. Security personnel to patrol DG yard regularly 3. Increase security patrols to monitor computer room 4. Nil required.

RISK ANALYSIS TABLE				
1	2	3	4	5
Threats (Article 15.11 of Part B of the ISPS Code)	Order these threats as they concern you, highest to lowest	Assets of High Value or Critical to your Operations Affected by Threats	Existing Safeguards or Apparent Weaknesses	Possible Corrective Measures to Address Weaknesses
Use of the ship to carry those intending to cause a security incident and their equipment.	Example HIGH MEDIUM LOW	Example 1.Electrical Sub-stations 2.Dangerous Goods (DG) Yard 3.Computer Room 4.Control Station	Example 1a. Electrical Sub-stations are fenced all around 1b. Security personnel patrol electrical sub-stations regularly 2.Nil 3.NIL 4. Regular patrol by security personnel	Example 1. Nil Required 2a.Installing CCTV to monitor DG Yards. 2b. Security personnel to patrol DG yard regularly 3. Increase security patrols to monitor computer room 4. Nil required.

RISK ANALYSIS TABLE				
1	2	3	4	5
Threats (Article 15.11 of Part B of the ISPS Code)	Order these threats as they concern you, highest to lowest	Assets of High Value or Critical to your Operations Affected by Threats	Existing Safeguards or Apparent Weaknesses	Possible Corrective Measures to Address Weaknesses
Use of a ship alongside as a weapon or as a means to cause damage or destruction.	Example HIGH MEDIUM LOW	Example 1.Electrical Sub-stations 2.Dangerous Goods (DG) Yard 3.Computer Room 4.Control Station	Example 1a. Electrical Sub-stations are fenced all around 1b. Security personnel patrol electrical sub-stations regularly 2.Nil 3.NIL 4. Regular patrol by security personnel	Example 1. Nil Required 2a.Installing CCTV to monitor DG Yards. 2b. Security personnel to patrol DG yard regularly 3. Increase security patrols to monitor computer room 4. Nil required.

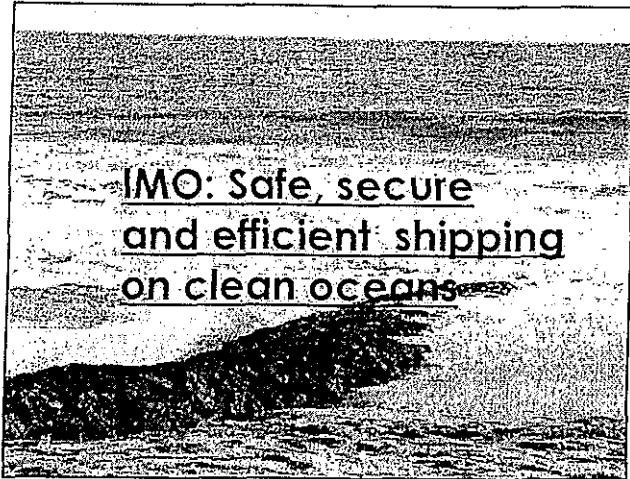
RISK ANALYSIS TABLE				
1	2	3	4	5
Threats (Article 15.11 of Part B of the ISPS Code)	Order these threats as they concern you, highest to lowest	Assets of High Value or Critical to your Operations Affected by Threats	Existing Safeguards or Apparent Weaknesses	Possible Corrective Measures to Address Weaknesses
Blockage of port entrances, locks, approaches to the port/port facility, etc.	Example HIGH MEDIUM LOW	Example 1.Electrical Sub-stations 2.Dangerous Goods (DG) Yard 3.Computer Room 4.Control Station	Example 1a. Electrical Sub-stations are fenced all around 1b. Security personnel patrol electrical sub-stations regularly 2.Nil 3.NIL 4. Regular patrol by security personnel	Example 1. Nil Required 2a.Installing CCTV to monitor DG Yards. 2b. Security personnel to patrol DG yard regularly 3. Increase security patrols to monitor computer room 4. Nil required.

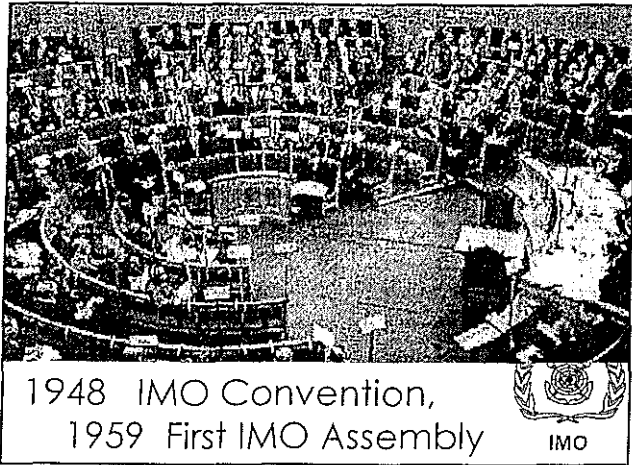
RISK ANALYSIS TABLE				
1	2	3	4	5
Threats (Article 15.11 of Part B of the ISPS Code)	Order these threats as they concern you, highest to lowest	Assets of High Value or Critical to your Operations Affected by Threats	Existing Safeguards or Apparent Weaknesses	Possible Corrective Measures to Address Weaknesses
Nuclear, biological and chemical attack against the port/port facility or ship alongside.	Example HIGH MEDIUM LOW	Example 1.Electrical Sub-stations 2.Dangerous Goods (DG) Yard 3.Computer Room 4.Control Station	Example 1a. Electrical Sub-stations are fenced all around 1b. Security personnel patrol electrical sub-stations regularly 2.Nil 3.NIL 4. Regular patrol by security personnel	Example 1. Nil Required 2a.Installing CCTV to monitor DG Yards. 2b. Security personnel to patrol DG yard regularly 3. Increase security patrols to monitor computer room 4. Nil required.



INTRODUCTION TO IMO

- ### Module Objectives
- Role of IMO
 - Structure of IMO
 - Decision-making process









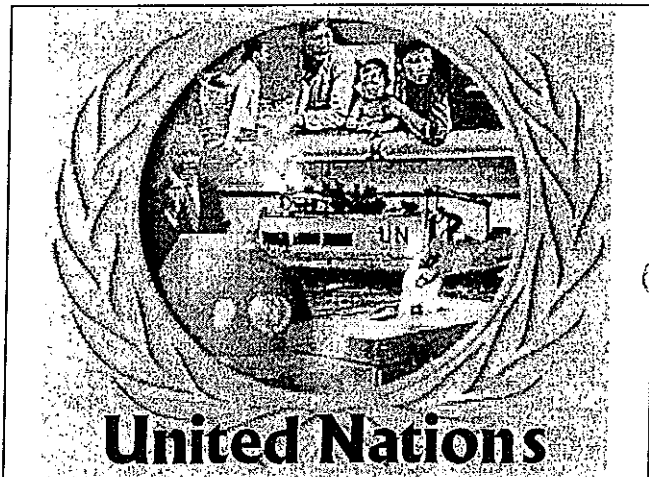
Potentially dangerous

Mid 19th century onwards –
some international treaties

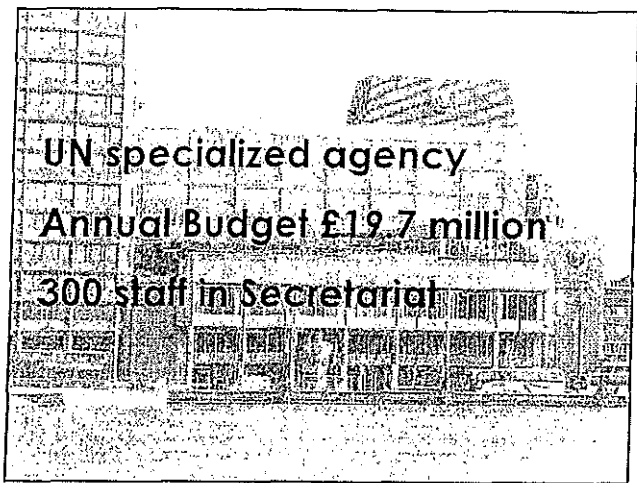


First SOLAS convention
adopted 1914

Titanic disaster 1912



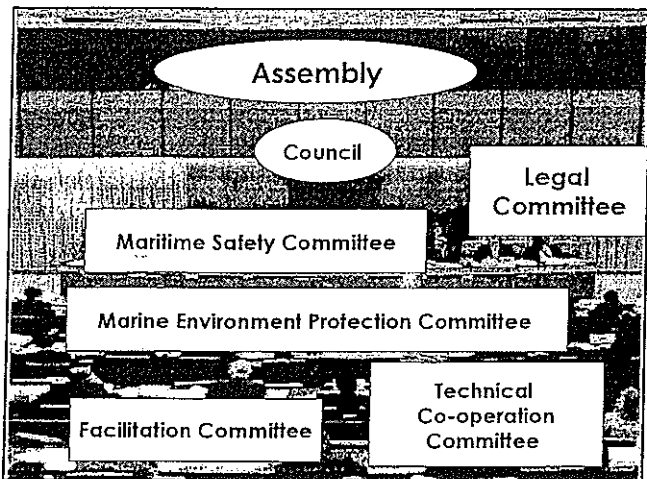
United Nations

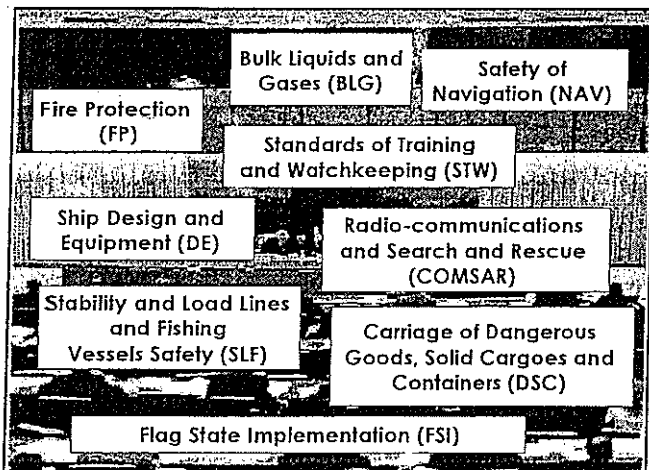


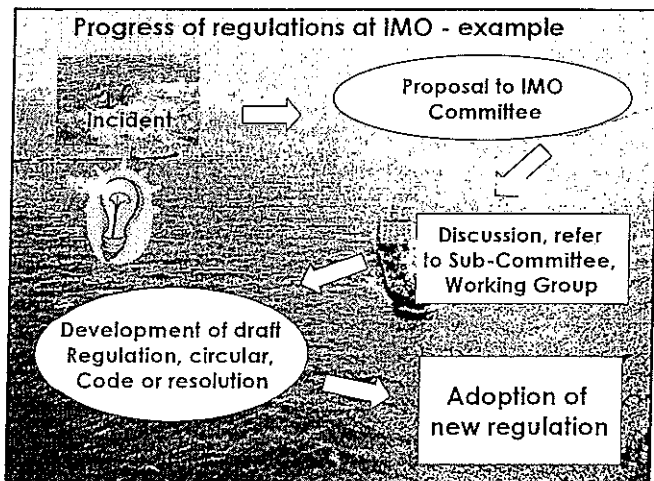


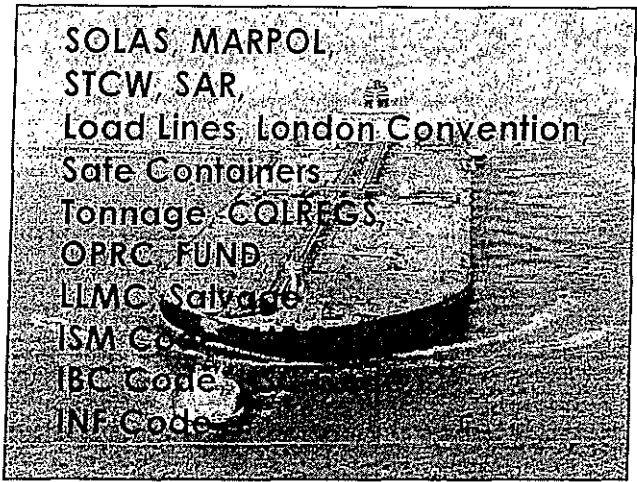
IMO contributors to budget - top 10

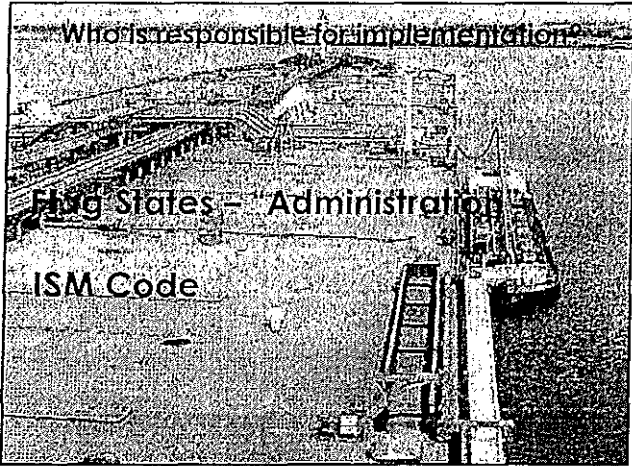
Country	Amount (£ million)	% of total
Panama	2.90	15.80
Liberia	1.86	10.17
Japan	0.96	5.23
Bahamas	0.81	4.36
Greece	0.80	4.32
USA	0.76	4.12
Malta	0.73	3.96
Cyprus	0.72	3.91
Norway	0.71	3.86
Singapore	0.61	3.31

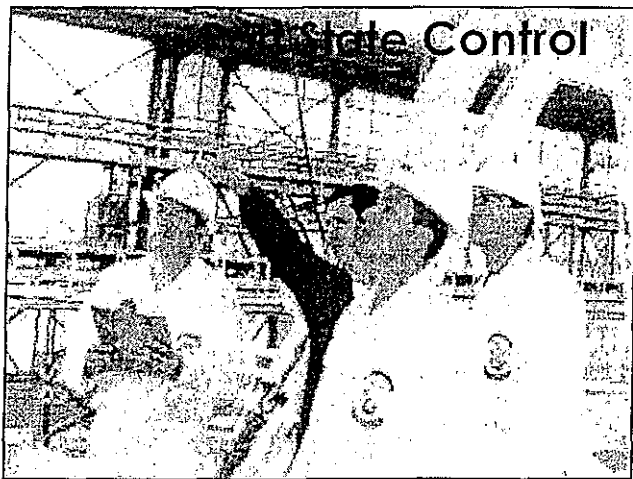


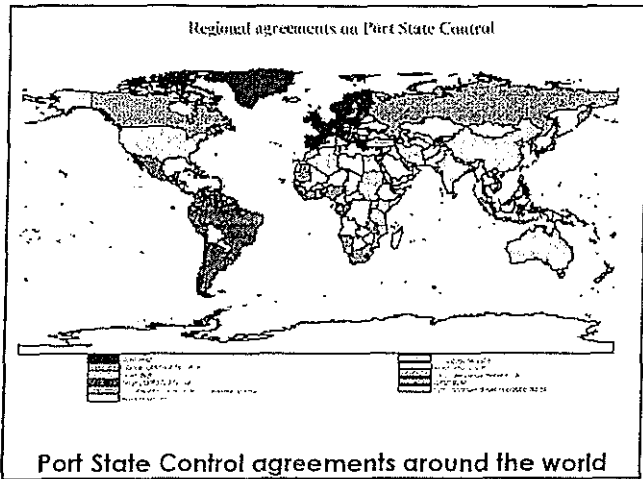




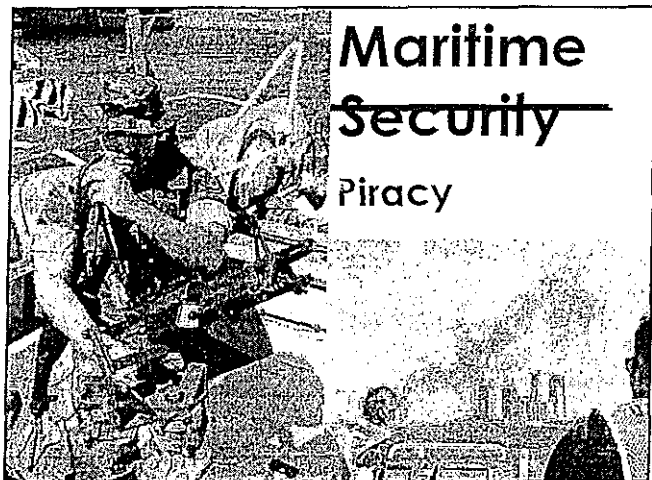




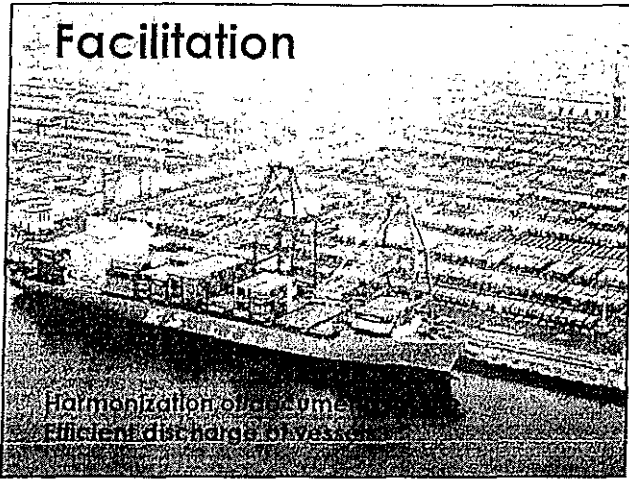






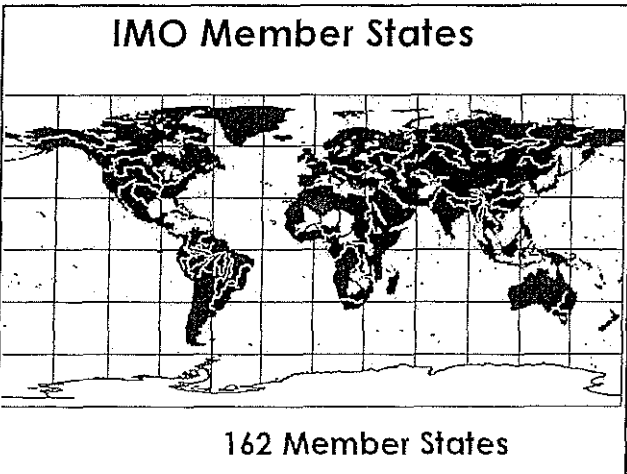


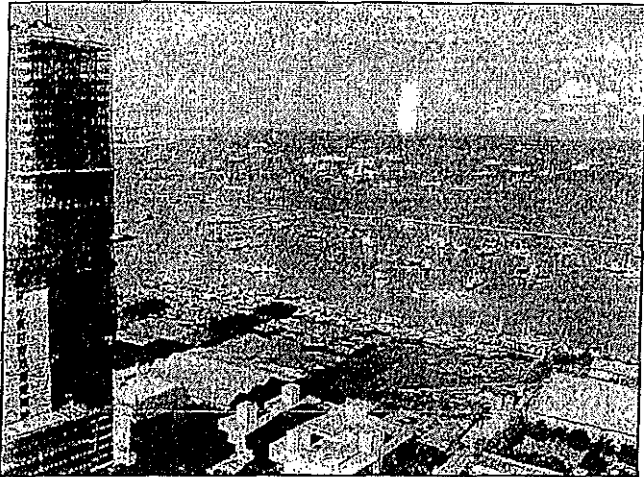
Facilitation

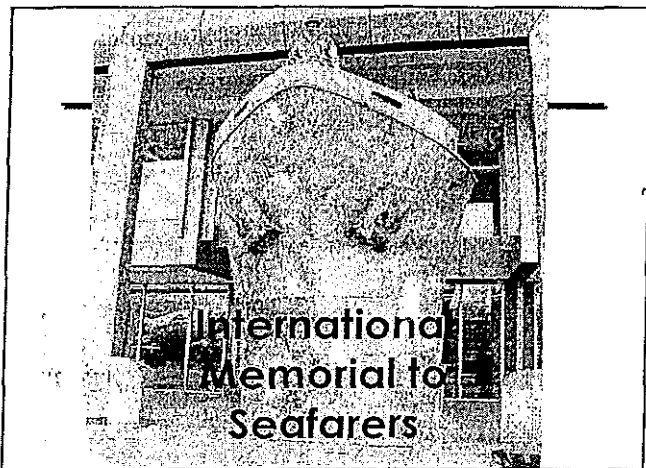




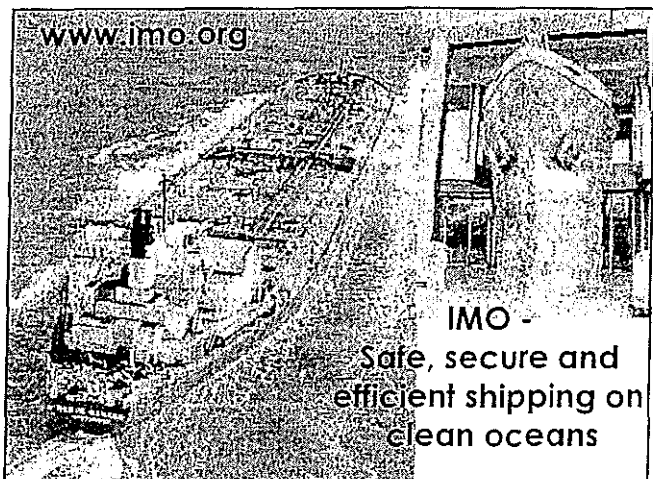
IMO Member States







International
Memorial for
Seafarers

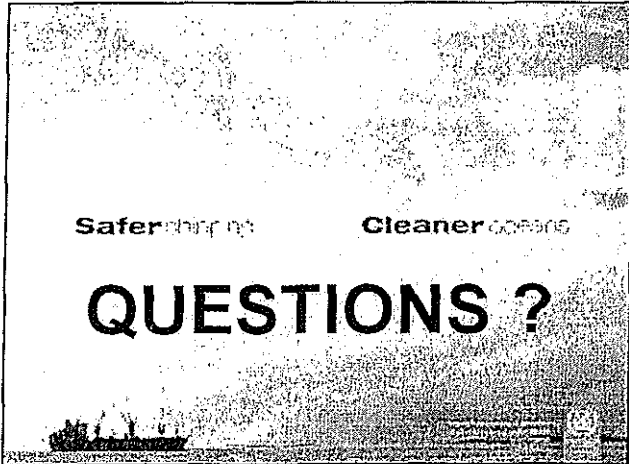


www.imo.org

IMO -
Safe, secure and
efficient shipping on
clean oceans

Module Summary

- Role of IMO
- Structure of IMO
- Decision-making process



Implementation and Management of Port Facility Security Measures

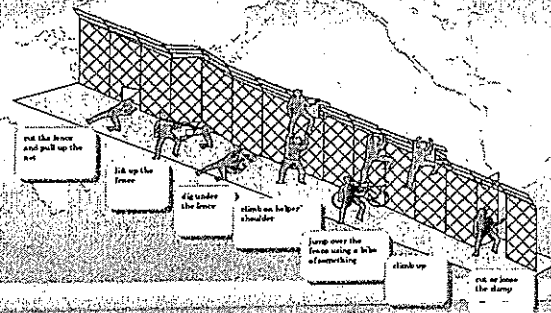
JICA Study Team on the Port Security Enhancement Program of Major Indonesian Public Ports

1. Settle a restricted area
2. Fence off the area and set gates
3. Set necessary security facilities
4. Monitor the boundaries
5. Conduct access control

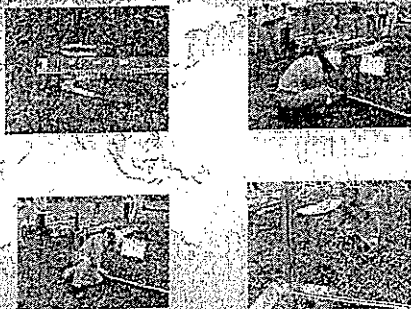
1. Setting a restricted area

- Minimize the area as small as possible
- Separate the area from non-compliance ships (domestic ships, fishing ships, etc.) as much as possible

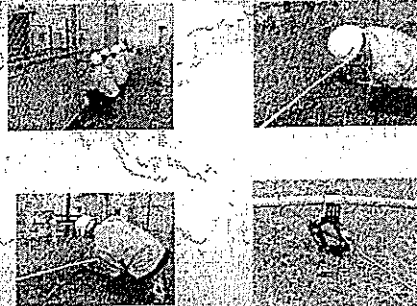
2. Fence and Gates (1) Intrusion scenario

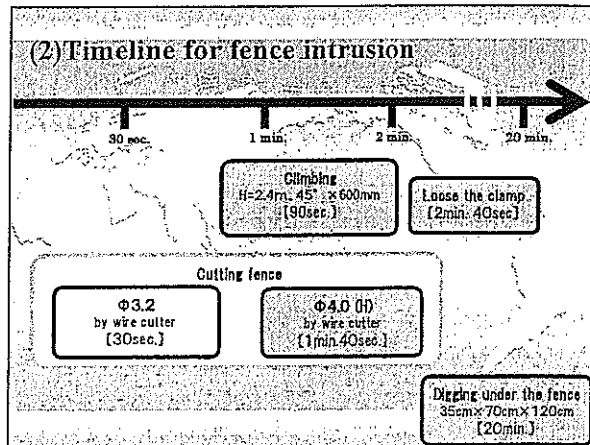
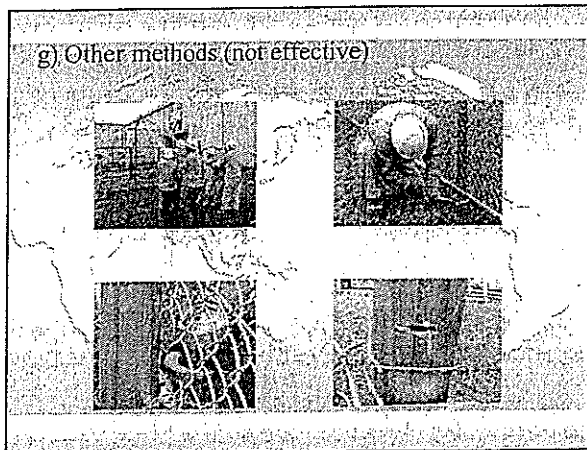
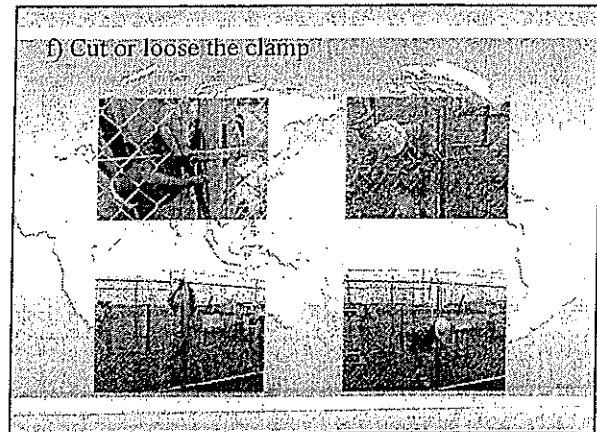
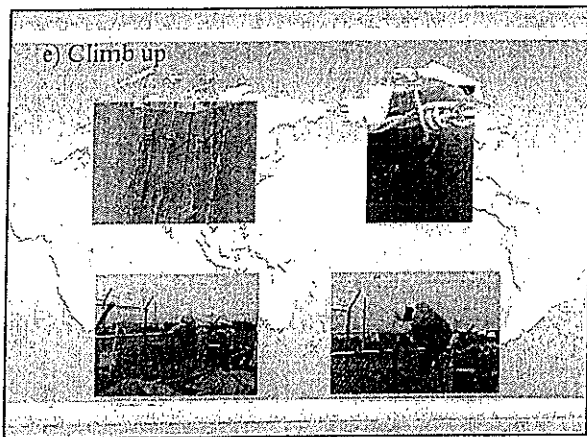
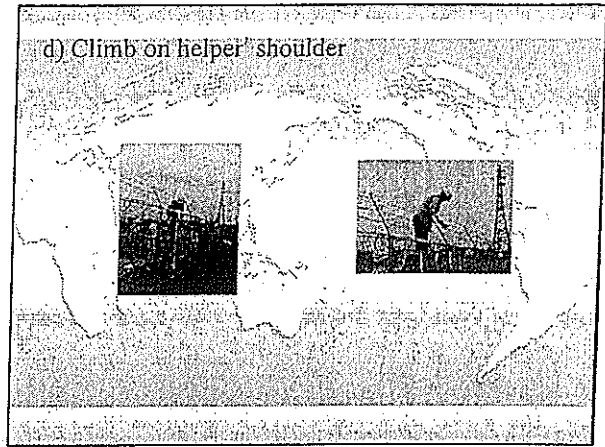
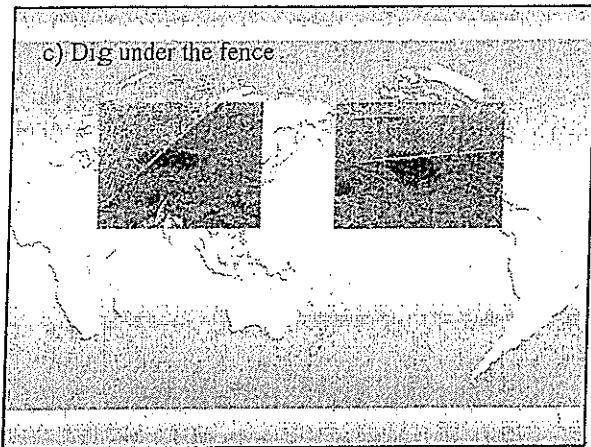


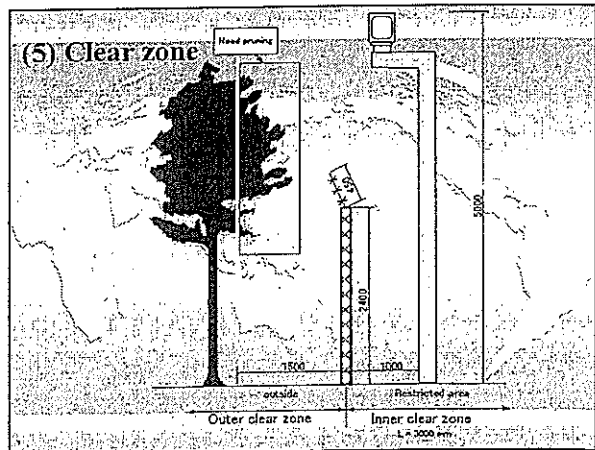
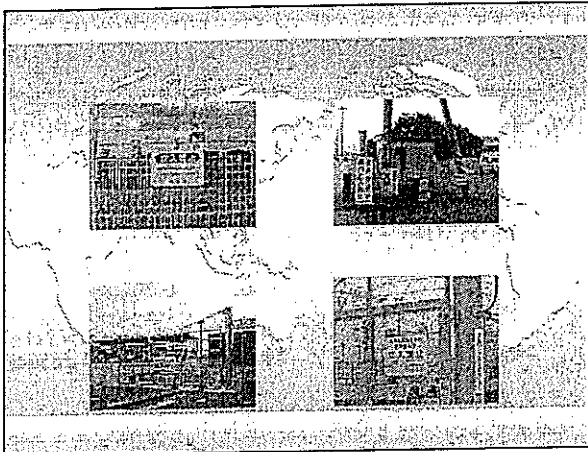
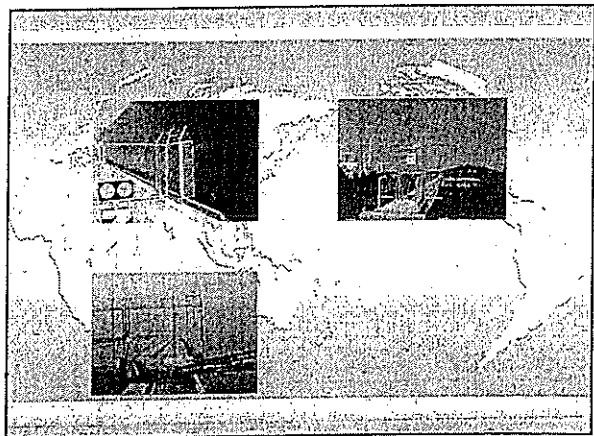
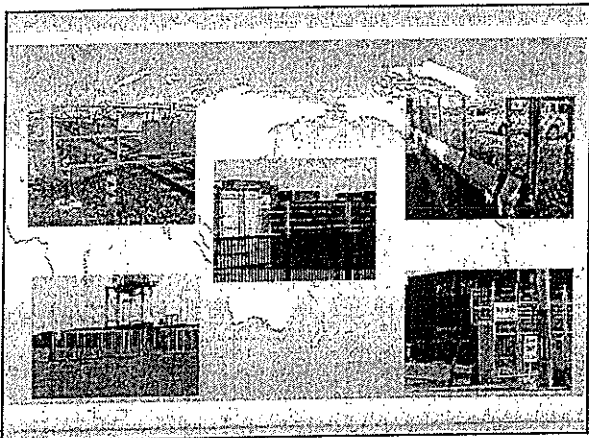
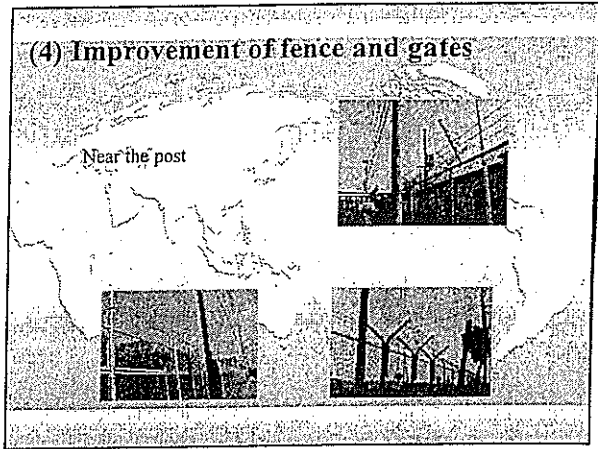
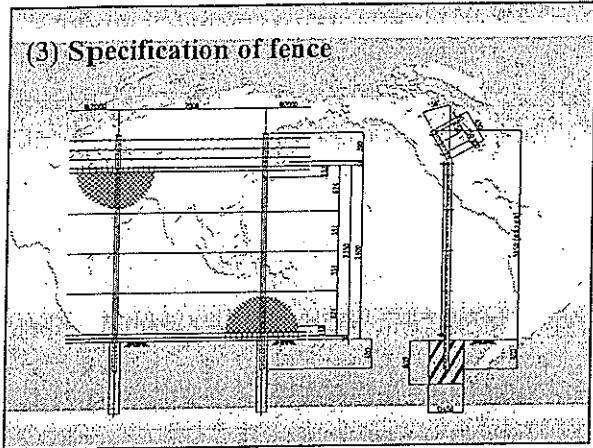
a) Cut the fence and pull up the net



b) Lift the fence



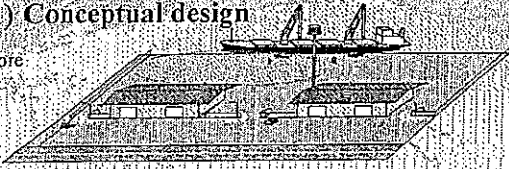




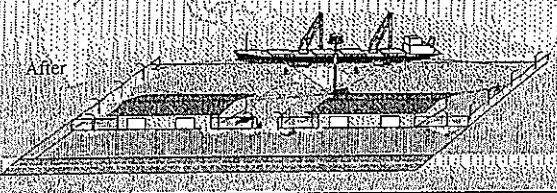
3. Set up necessary facilities

(1) Conceptual design

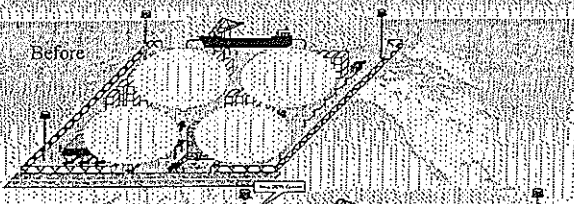
Before



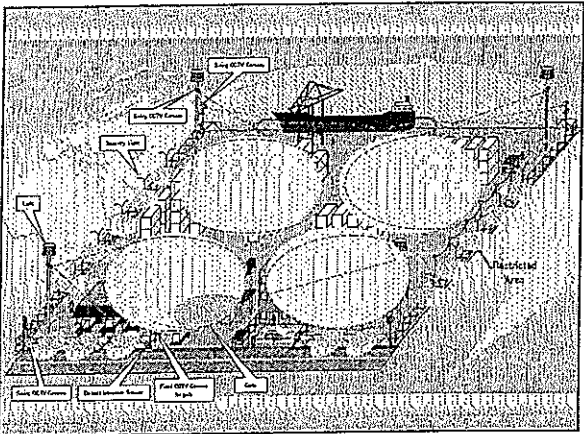
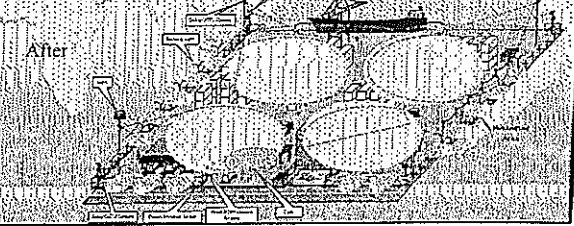
After



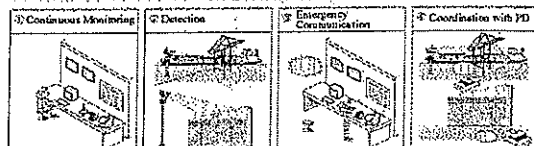
Before



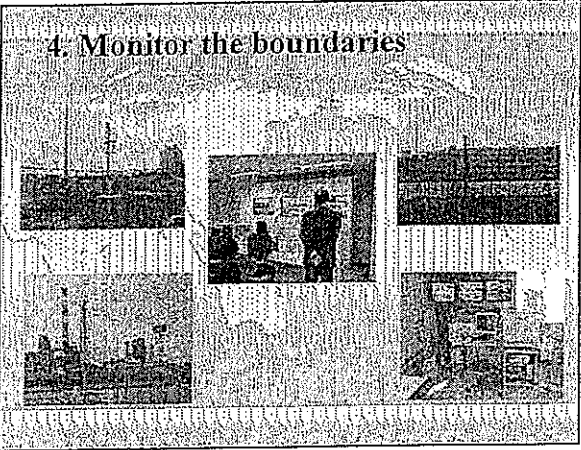
After



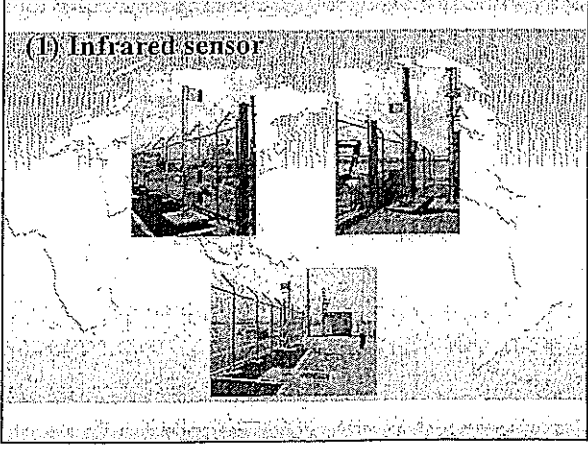
(2) Make effective use of security facilities

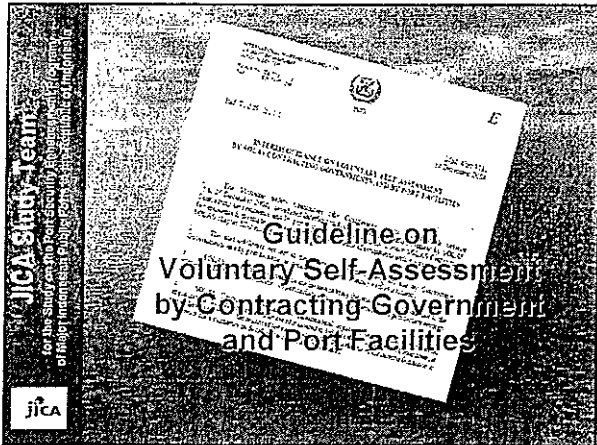


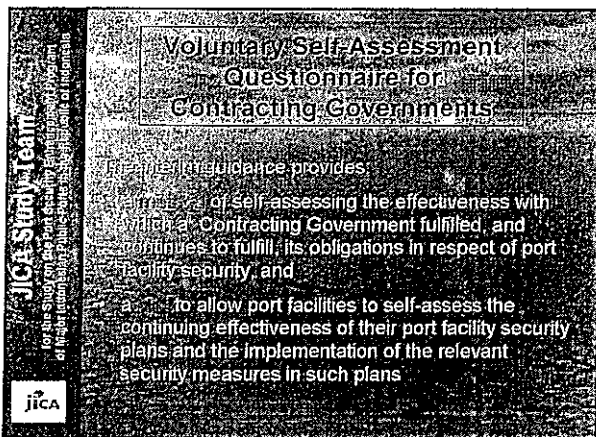
4. Monitor the boundaries

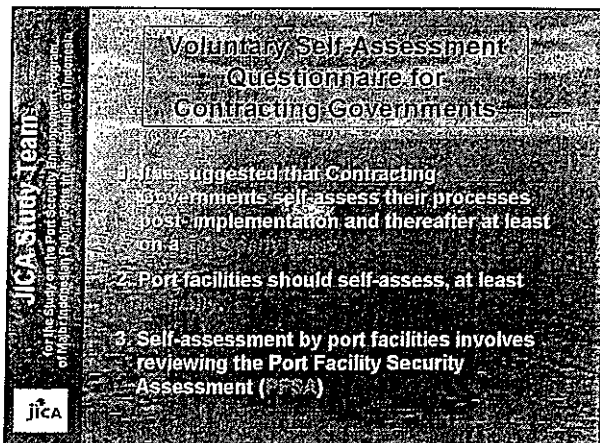


(1) Infrared sensor









JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports (Phase 1) (Indonesia)

**Voluntary Self-Assessment
Questionnaire for
Contracting Governments**

Qualification

Anyone undertaking the self-assessment should, at least, have knowledge of:

- 1. The requirements of SOLAS Chapter XI-2 and the ISPS Code;
- 2. general security principles, and
- 3. the operation of port facilities

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports (Phase 1) (Indonesia)

**Voluntary Self-Assessment
Questionnaire for
Contracting Governments**

The questionnaire is intended for those conducting the voluntary self-assessment to document the Contracting Government's strategy in its implementation of the provisions in SOLAS Chapter XI-2 and the ISPS Code relating to port facility security.

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports (Phase 1) (Indonesia)

**Voluntary Self-Assessment
Questionnaire for
Contracting Governments**

The questionnaire has six (6) sections:

1. The implementation process
2. Port Facility Security Assessment (PFSA)
3. Port Facility Security Plan (PFSP)
4. Security Levels
5. Declaration of Security (DOS)
6. Delegation of Tasks and Duties

JICA

JICA Study Team
 for the Study on the Port Security Enhancement of Major Indonesian Public Ports to Strengthen the Resilience of Infrastructure

JICA

Implementation – XI-2-4.1

Contracting Government

1. What is the designated authority? (SOLAS regulation XI-2/1.1)
2. What is the national legislative basis for the implementation of the ISPS Code? (SOLAS regulations XI-2/2 and XI-2/10)
3. What guidance to industry was released to implement the ISPS Code? (SOLAS regulations XI-2/2 and XI-2/10)
4. What is the means of communication with port facilities regarding ISPS Code implementation? (SOLAS regulations XI-2/3 and XI-2/10)
5. What processes are in place to document initial and subsequent compliance with the ISPS Code? (SOLAS regulation XI-2/10.2)
6. What is the Contracting Government’s definition of a Port Facility? (SOLAS regulation XI-2/1.1)

JICA Study Team
 for the Study on the Port Security Enhancement of Major Indonesian Public Ports to Strengthen the Resilience of Infrastructure

JICA

Implementation – XI-2-4.1

Contracting Government

7. What are the procedures used to determine the extent of compliance with the ISPS Code for port facilities? (When does compliance with the ISPS Code start? With particular reference to those port facilities that are to fully serve ships on international voyages?) (SOLAS regulations XI-2/1, XI-2/2.2)
8. Has the Contracting Government concluded in writing bilateral or multi-lateral agreements with other Contracting Governments on alternative security agreements? (SOLAS regulation XI-2/11.1)
9. Has the Contracting Government allowed a port facility or group of port facilities to implement equivalent security arrangements? (SOLAS regulation XI-2/12.1)
10. Who has the responsibility for notifying and updating the IMO with information in accordance with SOLAS regulation XI-2/13? (SOLAS regulation XI-2/13)

JICA Study Team
 for the Study on the Port Security Enhancement of Major Indonesian Public Ports to Strengthen the Resilience of Infrastructure

JICA

Port Facility

Contracting Government

11. Who conducts PFSAs? (SOLAS regulation XI-2/10.2.1, ISPS Code section A/15.2 and A/15.3)
12. How are PFSAs conducted and approved? (ISPS Code sections A/15.2 and A/15.4)
13. What minimum skills are required for persons conducting PFSAs? (ISPS Code section A/15.3)
14. Are PFSAs used for each Port Facility Security Plan? (ISPS Code section A/15.1)
15. Do single PFSAs cover more than one port facility? (ISPS Code section A/15.6)

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Ports within the Security of Indonesia

Port Facility Security
Contracting

1. What is the process of approval of the PFSA and the single PFSA cover the relevant area? (ISPS Code section A/16.5)
2. What national guidance has been developed to assist with the completion of PFSA's? (SOLAS regulation XI-2/10.2.1)
3. What procedures are in place for determining when re-assessment takes place? (ISPS Code section A/16.4)
4. What procedures are in place for protecting the PFSA's from unauthorized access or disclosure? (ISPS Code section A/16.7)

jica

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Ports within the Security of Indonesia

Port Facility Security
Contracting

1. How are Port Facility Security Officers designated? (ISPS Code section A/17.1)
2. What are the minimum training requirements that have been set by the contracting government for PFSOs? (ISPS Code section A/18.1)
3. What procedures used to determine the individuals/organizations responsible for the preparation of the PFSP? If yes, please describe.
4. Are procedures in place to protect PFSPs from unauthorized access? (ISPS Code sections A/16.7 and A/16.8)
5. What procedures are in place for approval and subsequent amendments of the PFSPs? (ISPS Code section A/16.9)

jica

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Ports within the Security of Indonesia

Security Level
Contracting

1. Who is the authority responsible for setting the security level for port facilities? (SOLAS regulation XI-2/3.2)
2. What are the procedures for communicating security levels to port facilities by the responsible authority? (SOLAS regulation XI-2/3.2)
3. What are the procedures for communicating port facilities' security levels to ships? (SOLAS regulations XI-2/4.3 and XI-2/7.1)
4. What are the contact points and procedures for receiving ships' security level information in the Contracting Government and for notifying ships of contact details? (SOLAS regulation XI-2/7.2)

jica

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Public Ports, the Republic of Indonesia

Declaration of Security Contracting

1. Which procedures are used to determine when a Declaration of Security is required? (SOLAS Regulation XI-2/10.3, ISPS Code section A/5.1)
2. What is the minimum time frame that a Declaration of Security is required to be retained? (ISPS Code section A/5.6)

jica

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Public Ports, the Republic of Indonesia

Declaration of Security Contracting

1. What tasks and duties have the contracting government delegated to Recognized Security Organizations (RSOs) or others? (ISPS Code section A/4.3)
2. To whom have these tasks and duties been delegated? What oversight procedures are in place? (SOLAS regulation XI-2/13.2)

jica

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Public Ports, the Republic of Indonesia

Voluntary Self-Assessment

jica

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Ports (Phase 1) (JICA/JICA/JICA)

Voluntary Self-Assessment Tool for Port Facility Security

The self-assessment tool can be used to examine the status of ISPS Code implementation.

The tool will help identify any aspects of the ISPS Code that the port facility/port facility security officer (PFSO) or AS Contracting Government (Designated Authority) can address to enhance the ISPS Code implementation process.

If amendment to the approved Port Facility Security Plan is needed the changes may have to be submitted to the Designated Authority for its approval.

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Ports (Phase 1) (JICA/JICA/JICA)

Voluntary Self-Assessment Tool for Port Facility Security

Port Facility Information

- Name of port facility
- Name of operator/authority
- Name of Port, if applicable
- Name of PFSO
- Average number of SOLAS vessels handled per annum

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program of Major Indonesian Ports (Phase 1) (JICA/JICA/JICA)

Voluntary Self-Assessment Tool for Port Facility Security

Port Facility Information

- Is a tender ship
- Ro/ro/containers terminal
- Oil/ gas
- Oil/ gas refinery / terminal
- LPG, LNG or petrol storage
- Other dangerous goods
- Near military installation
- Military vessels
- Embarkation of military personnel or cargo
- Other (describe)

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Ports in the Republic of Honduras

Volume 1: Self-Assessment Tool for Port Facility Security

There are nine (9) sections:

1. Ensuring the performance of port facility security duties
2. Controlling access to the port facility;
3. Monitoring of the port facility, including anchoring and berthing area(s);
4. Monitoring of restricted areas;
5. Supervising the handling of cargo;
6. Supervising the handling of ship's stores;
7. Ensuring security communication is readily available;
8. Training, drills and exercises, and
9. Miscellaneous

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Ports in the Republic of Honduras

Volume 1: Self-Assessment Tool for Port Facility Security

Each section has sub-sections relating to:

- the mandatory requirements in Part A of the ISPS Code, and
- the guidance provided in Part B of the Code.

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Ports in the Republic of Honduras

Volume 1: Self-Assessment Tool for Port Facility Security

Ensuring the performance of port facility security duties (ISPS Code sections A/16.2.1 and A/16.3, Part A.14)

1. Does the port facility have means of ensuring the performance of all security duties meet the requirements set out in the RFSP for security alert plans 2? (ISPS Code section A/14.2.1)
2. Does the port facility established measures to prohibit weapons or any other dangerous substances and devices intended for use against persons, ships, or the port, from entering the facility? (ISPS Code section A/16.3.1)
3. Has the port facility established evacuation procedures in case of security threats or breaches of security? (ISPS Code section A/16.3.5)
4. Has the port facility established procedures for response to an activation of a ship security alert system? (ISPS Code section A/16.3.14)

JICA

JICA Study Team
For the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports, with Support from Indonesia

Initial Self-Assessment Tool for Port Facility Security

1. Has the port facility established their security organization? (ISPS Code paragraph B/16.8.1)

2. Has the port facility established the role and structure of the security organization? (ISPS Code paragraph B/16.8.1)

3. Has the port facility established the duties and responsibilities for personnel with security roles? (ISPS Code paragraph B/16.8.2)

4. Has the port facility established the training requirements for personnel with security roles? (ISPS Code sections A/18.1, A/18.2, A/18.3 and paragraph B/16.8.2)

5. Has the port facility established the performance measures needed to assess the individual effectiveness of personnel with security roles? (ISPS Code paragraph B/16.8.2)

JICA

JICA Study Team
For the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports, with Support from Indonesia

Initial Self-Assessment Tool for Port Facility Security

6. Has the port facility established their security organization's link with other national or local authorities with security responsibilities? (ISPS Code paragraph B/16.8.3)

7. Has the port facility established procedures and practices to protect security sensitive information held in paper or electronic format? (ISPS Code paragraph B/16.8.6)

8. Has the port facility established procedures to assess the continuing effectiveness of security measures and procedures? (ISPS Code paragraph B/16.8.7)

9. Has the port facility established procedures to assess security equipment, to include identification of, and response to, equipment failure or malfunction? (ISPS Code paragraph B/16.8.7)

10. Has the port facility established procedures governing submission and assessment of reports relating to possible breaches of security or security concerns? (ISPS Code paragraph B/16.8.8)

JICA

JICA Study Team
For the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports, with Support from Indonesia

Initial Self-Assessment Tool for Port Facility Security

11. Has the port facility established procedures to maintain and control records of dangerous goods and hazardous substances in the handling area of the port facility? (ISPS Code paragraph B/16.8.9)

12. Has the port facility established a means of alerting and obtaining the services of waterside patrols and search teams, to include command and underwater specialists? (ISPS Code paragraph B/16.8.12)

13. Has the port facility established procedures for assisting, when requested, Ship Security Officers in confirming the identity of those seeking to board the ship? (ISPS Code paragraph B/16.8.13)

14. Has the port facility established the procedures for facilitating shore leave for ship's crew members or personnel changes? (ISPS Code paragraph B/16.8.14)

15. Has the port facility established the procedures for facilitating visitor access to the ship, to include representatives of seafarers' welfare and labour organizations? (ISPS Code paragraph B/16.8.14)

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Ports in the Republic of Indonesia

16 **Control Access to the Port Facility (ISPS Code sections A/12.4, A/14.2.2 and A/14.3) Part A (1)**

16 **Does the port facility's means of controlling access to the port facility meet the requirements set out in the PFSP for security level 1 and 2?**

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Ports in the Republic of Indonesia

17 **Control Access to the Port Facility (ISPS Code sections A/12.4, A/14.2.2 and A/14.3) Part B (1)**

17 **Has the port facility identified the appropriate location(s) where security measures can be applied to restrict prohibited access? These should include all access points identified in the PFSP at security level 1 and 2? (ISPS Code paragraphs B/16.11, B/16.19.1)**

17 **Does the port facility specify the type of restrictions or prohibitions and the means of enforcement to be applied at all access points identified in the PFSP at security level 1 and 2? (ISPS Code paragraphs B/16.11, B/16.19.2, B/16.19.3)**

17 **Has the port facility established measures to increase the frequency of searches of people, personal effects, and vehicles at security level 2? (ISPS Code paragraph B/16.19.4)**

17 **Has the port facility established measures to deny access to visitors who are unable to provide verifiable justification for seeking access to the port facility at security level 2 (ISPS Code paragraph B/16.19.5)**

JICA

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Ports in the Republic of Indonesia

18 **Control Access to the Port Facility (ISPS Code sections A/12.4, A/14.2.2 and A/14.3) Part C (1)**

18 **Does the port facility have the means to differentiate the identification of permanent, temporary, and visiting individuals? (ISPS Code paragraph B/16.12)**

18 **Does the port facility have the means to verify the identity and legitimacy of passenger boarding passes, tickets, etc? (ISPS Code paragraph B/16.12)**

18 **Has the port facility established provisions to ensure that the identification systems are regularly updated? (ISPS Code paragraph B/16.12)**

JICA

JICA Study Team
 for the study on the Port Security Enhancement Program
 of Major Indonesian Ports by the Government of Indonesia

Voluntary Self-Assessment Tool for Port Facility Security
 11. Does the port facility establish provisions to permit disembarking actions against those who remain in the identification system procedure? (ISPS Code paragraph B/16.12)

12. Has the port facility created procedures to deny access and deny boarding to individuals who are unwilling or unable to establish their identity or purpose for visit to the PFSP and to the national or local authorities? (ISPS Code paragraph B/16.13)

13. Does the port facility identified a location(s) for searches of persons, personal effects, and vehicles that facilitates continuous operation, regardless of prevailing weather conditions? (ISPS Code paragraph B/16.14)

14. Does the port facility have procedures established to directly transfer persons, personal effects, or vehicles subjected to search to the restricted holding, embarkation, or vehicle loading area? (ISPS Code paragraph B/16.14)

JICA Study Team
 for the study on the Port Security Enhancement Program
 of Major Indonesian Ports by the Government of Indonesia

Voluntary Self-Assessment Tool for Port Facility Security
 15. Has the port facility established separate locations for embarking and disembarking passengers, ship's personnel, and their effects to ensure that unchecked persons do not come in contact with checked persons? (ISPS Code paragraph B/16.15)

16. Does the PFSP establish the frequency of application of all access controls? (ISPS Code paragraph B/16.16)

JICA Study Team
 for the study on the Port Security Enhancement Program
 of Major Indonesian Ports by the Government of Indonesia

Voluntary Self-Assessment Tool for Port Facility Security
 17. Does the PFSP establish control points? (ISPS Code paragraph B/16.17)

18. Does the PFSP establish control points for restricted areas bounded by fencing or other barriers to a standard which is approved by the national government? (ISPS Code paragraph B/16.17.1)

19. Does the PFSP establish the identification of and procedures to control access points not in regular use which should be permanently closed and locked? (ISPS Code paragraph B/16.17.7)

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Ports (Phase 1) - Surabaya and Semarang, Indonesia

JICA

Voluntary Self-Assessment Tool for Port Facility Security

12. **Monitoring of the port facility, including anchoring and berthing area(s)** (ISPS Code paragraphs A/14.2.3 and A/14.3) Part A (1)

Does the facility's means of monitoring the port facility including berthing and anchorage area(s) meet the requirements set out in the PFSP for security level 1 and 2?

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Ports (Phase 1) - Surabaya and Semarang, Indonesia

JICA

Voluntary self-assessment tool for Port Facility Security

13. **Monitoring of the port facility, including anchoring and berthing area(s)** (ISPS Code paragraph B/16.49) Part B (6)

13.1. Does the port facility have the capability to continuously monitor on land and water the port facility and its nearby approaches? (ISPS Code paragraph B/16.49)

13.2. Which of the following means are employed to monitor the port facility and nearby approaches? (ISPS Code paragraph B/16.49)

- A. Patrols by security guards
- B. Patrols by security vehicles
- C. Patrols by watercraft
- D. Automatic intrusion-detection devices
- E. Surveillance equipment

14. If automatic intrusion-detection devices are employed, do they activate an audible and/or visual alarm(s) at a location(s) that is continuously monitored? (ISPS Code paragraph B/16.50)

15. Does the PFSP establish procedures and equipment needed at each security level? (ISPS Code paragraph B/16.51)

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Ports (Phase 1) - Surabaya and Semarang, Indonesia

JICA

Voluntary Self-Assessment Tool for Port Facility Security

16. **Monitoring of the port facility, including anchoring and berthing area(s)** (ISPS Code paragraphs B/16.53, B/16.54, B/16.55, B/16.56, B/16.57 and B/16.58)

Does the port facility established measures to increase the security measures at security level 1 and 2?

- A. Increase intensity and coverage of lighting and surveillance equipment
- B. Increase frequency of foot, vehicle & waterborne patrols
- C. Assign additional personnel
- D. Surveillance


17. Does the PFSP establish procedures and equipment necessary to ensure that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather or power disruptions? (ISPS Code paragraph B/16.51)

JICA Study Team
For the Study on the Port Security Improvement of Major International Public Ports (Subsidiary Technical Interview)

Voluntary Self-Assessment Tool for Port Facility Security

14. Identification of port facility (ISPS Code section A/14.1 and paragraph B/16.29)(A/14.1)

Does the port facility have adequate illumination to allow for detection of unauthorized persons at or approaching access points, the perimeter, restricted areas and ships, at all times including the night hours and periods of limited visibility? (ISPS Code paragraph B/16.49.1)




JICA Study Team
For the Study on the Port Security Improvement of Major International Public Ports (Subsidiary Technical Interview)

Voluntary Self-Assessment Tool for Port Facility Security

Marking of restricted areas (ISPS Code sections A/14.2.4 and A/14.3)

15. Does the port facility's means of limiting and controlling access to restricted areas meet the requirements of the PFSP for security level 1 and 2? (ISPS Code sections A/14.2.4 and A/14.3)



JICA Study Team
For the Study on the Port Security Improvement of Major International Public Ports (Subsidiary Technical Interview)


Voluntary Self-Assessment Tool for Port Facility Security

Establishment of restricted areas (ISPS Code Paragraph B/16.21)

16. Are restricted areas identified within the port facility? (ISPS Code paragraph B/16.21)

Which of the following elements are identified for restricted areas in the PFSP? (ISPS Code paragraph B/16.21)

- A. Extent of area
- B. Times of application
- C. Security measures to control access to areas
- D. Security measures to control activities within areas
- E. Measures to ensure restricted areas are swept before and after establishment



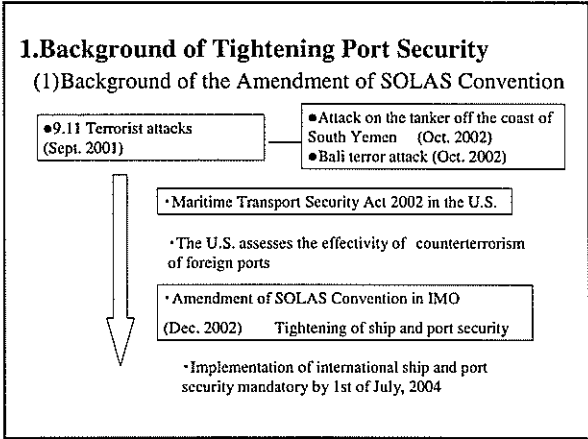
**Port of Benoa
East Berth**

Port Facility Security

**JICA Study Team on the Port Security
Enhancement Program of
Major Indonesian Public Ports**

Table of Contents

1. Background of Tightening Port Security
2. PFSA for Benoa Port, East Berth
3. PFSP for Benoa Port, East Berth
 - (1) Restricted Area for Each Pier
 - (2) Port Security Facilities to be provided
 - (3) Access Control to be conducted at Gates
 - (4) Maintenance Work
 - (5) Procedure of Emergency Management Plan
 - (6) Evacuation Route
 - (7) Emergency Contact List
 - (8) Contrast Chart for ISPS Code and PFSP



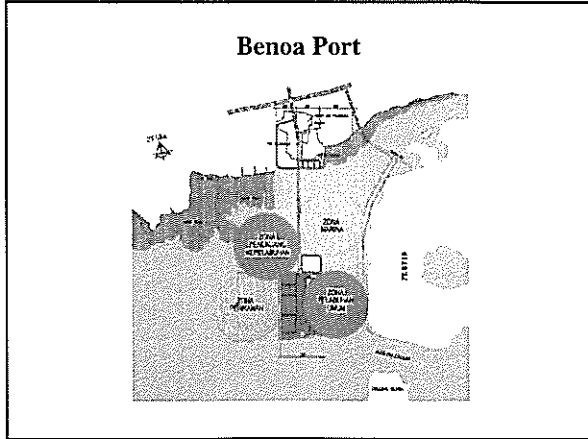
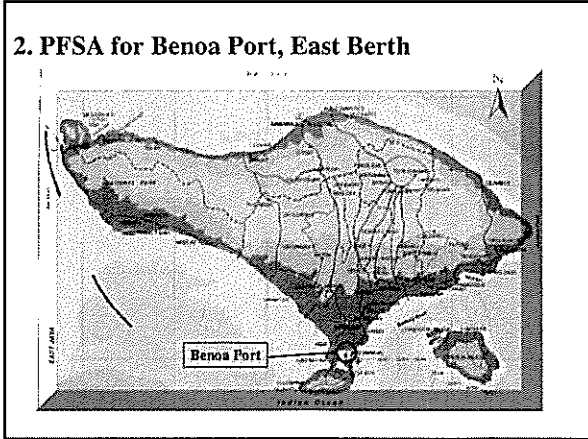
(2) What is SOLAS Convention?

➢ Formally each shipping nation had its own maritime laws. However in response to the Titanic disaster, which resulted in death of 1,500 passengers and crew out of over 2,000, treaty for international maritime safety was concluded in 1914

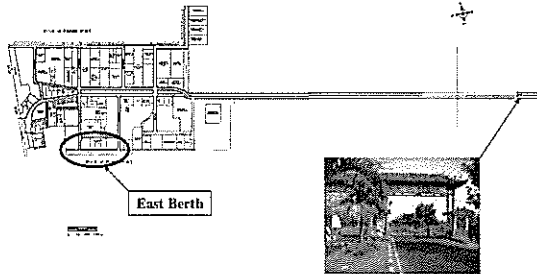
(3) Outline of Amendment of SOLAS Convention

➢ To improve the reliability of international sea transportation system by having the ship owner, the port operator and port administrator take security measures

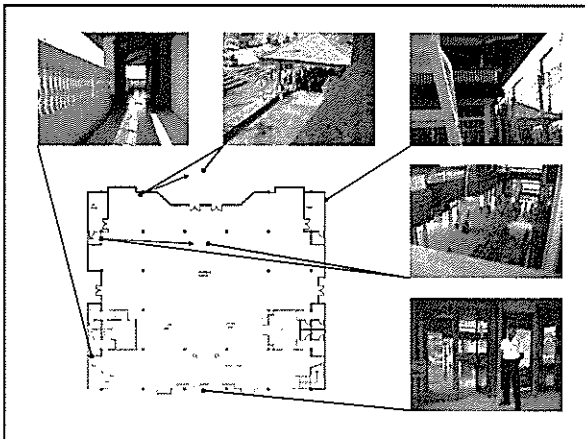
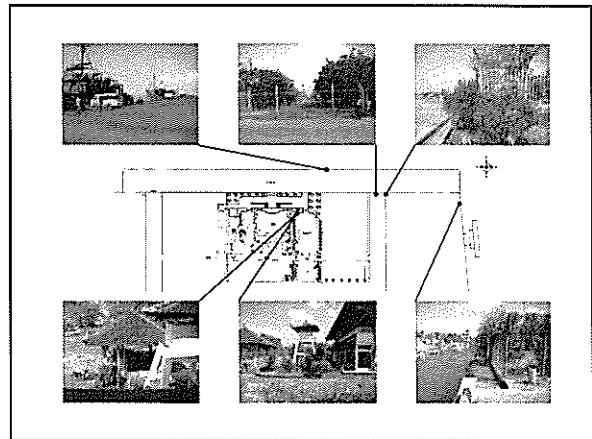
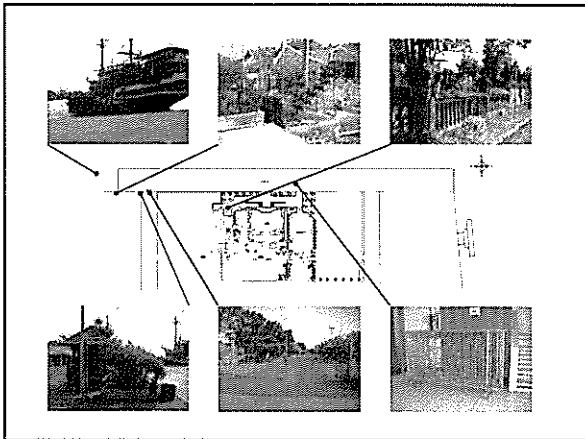
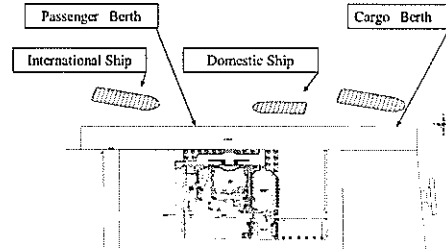
➢ To prevent an unlawful act related to international sea transportation by not admitting a ship identified to be a threat to enter the port



(1) Layout of Benoa Port



East Berth



(2) Current situation of East Berth

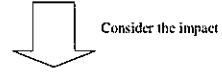
- No access control conducted
- Various ships are using the same wharf
 - International Passenger Ships
 - Domestic Passenger Ships
 - Cargo Ships(Domestic)
- Difficult to set restricted area for international ships
 - 45 international calls / year
 - Berthing wharf is depending on the size of vessel
 - Setting of fence will interfere the activities of cargo handling and so on

(3) Important Assets and Infrastructures

- Passenger Terminal
- Containers Terminal (domestic)

(4) Risk Evaluation

- Bali terror attack (Oct. 2002)



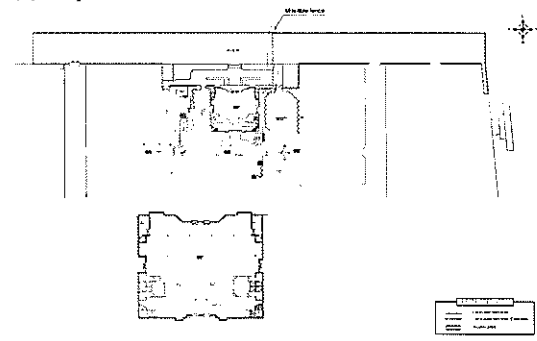
- "Social" and "Economic Activities"
- "Symbolic" and "Port Activities"

(5) Recommendations

- Access control system(Gate) of the restricted area
- Fence surrounding the restricted area
- Lighting system within the restricted area
- Communication system
- X-ray inspection system in the passenger terminal
- Security equipments such as a metal detector
- Use temporary fence and minimize the interference of port service
- Establish a procedure of international ship's calling
- Type of temporary fence
- Decide the number of security guards
- Deployment of security guards
- Area of temporary restricted area

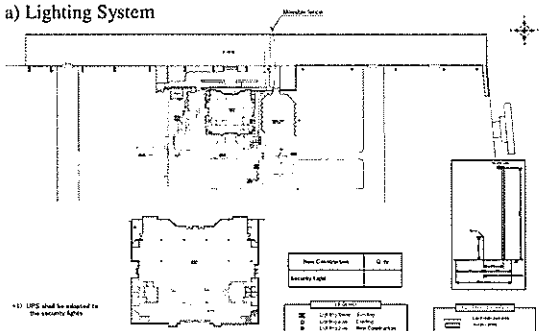
3. PFSP for Benoa Port, East Berth

(1) Proposed Restricted Area

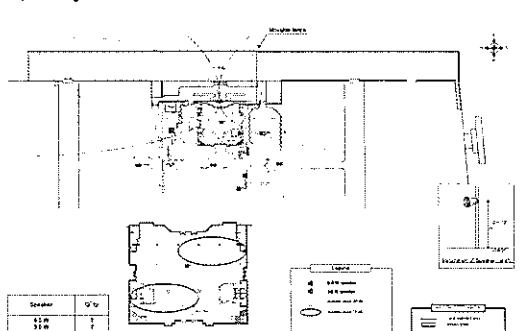


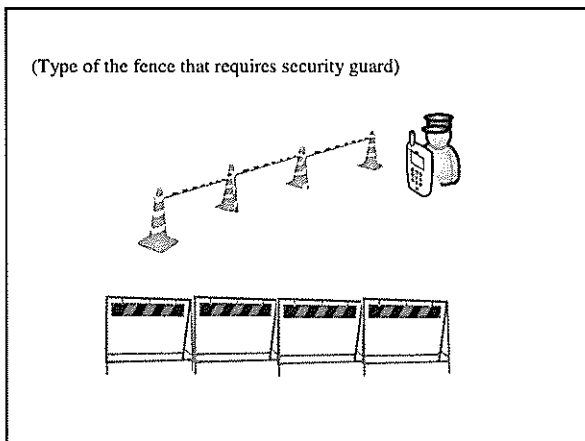
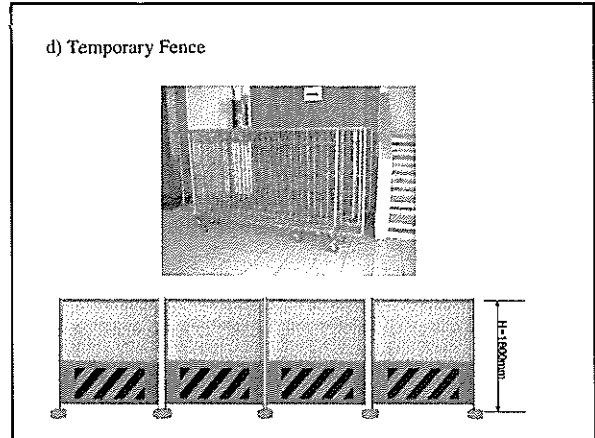
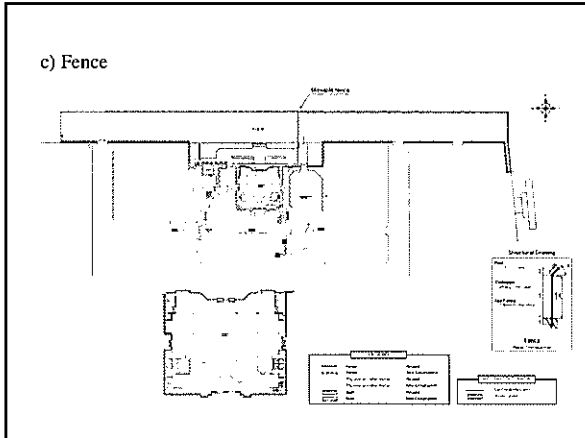
(2) Port Security Facilities to be Provided at East Berth

a) Lighting System



b) PA System





(3) Access Control to be Conducted at Gates

a) Access Control for Customs and ISPS Code

- Different Purpose
 - Customs
 - Avoid smuggling
 - Avoid goods BEING TAKEN out illegally
 - EXIT CONTROL
 - ISPS
 - Avoid Suspicious Person/Goods inside the Restricted Area
 - Protect from Terrorism
 - ENTRY CONTROL

- b) Category of Entrance
- Port User (by foot or otherwise)
 - Container Truck
 - Construction/Maintenance Vehicle
 - Ships Stores/Equipment
 - Ships Crew
 - Taxi
 - Emergency Service Vehicle

Port User (by foot or otherwise)

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Foot or Vehicle Entry	•Request to stop •Ask for ID card all those wishing to enter	•Same as on the left •Check ID photo and the face for 10 out of every 100	•Do not admit entry
Baggage	•Check appearance of baggage	•Confirm contents of baggage for 10 out of 100	•Do not admit entry

Container Truck			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Confirm documents	•Same as on the left	•Do not admit entry
Driver	•Ask for ID card for 10 out of every 100	•Ask all drivers for ID card	•Do not admit entry
Helper	•Admit entrance on guarantee of driver	•Same as on the left	•Do not admit entry
Full Container	•Check documents and appearance	•Same as on the left	•Do not admit entry
Empty Container	•Check documents and confirm inside	•Same as on the left	•Do not admit entry

Cargo Truck			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Confirm documents	•Same as on the left	•Do not admit entry
Driver	•Ask for ID card for 10 out of every 100	•Ask all drivers for ID card	•Do not admit entry
Helper	•Admit entrance on guarantee of driver	•Same as on the left	•Do not admit entry
Freight	•Check Documents & appearance of cargo	•Inspect and confirm cargo against documents	•Do not admit entry

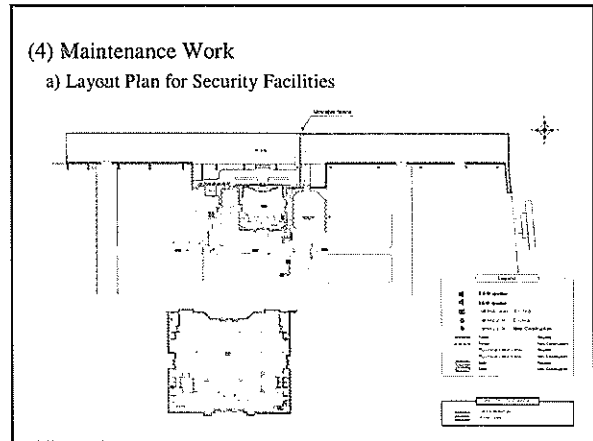
Construction/Maintenance Vehicle			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Confirm approval with PFSO	•Same as on the left	•Do not admit entry
Driver	•Ask all drivers for ID card	•Ask all drivers for ID card •Check ID photo and the face for 10 out of every 100 •Request to fill in form and issue temporary pass when there is no ID card	•Do not admit entry
Passenger/ Workmen	•Admit entrance on guarantee of driver/foreman	•Same as above	•Do not admit entry
Cargo	•Check appearance	•Inspect contents	•Do not admit entry

Ship's Stores/Equipment			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Check documents	•Request to stop •Confirm documents	•Do not admit entry
Driver & Passenger	•Ask all drivers/Passengers for ID card •Check ID photo and face for 50 out of every 100	•Ask all drivers/Passengers for ID card •Check ID photo and the face for all those wishing to enter	•Do not admit entry
Cargo	•Not necessary to check when under escort •Confirm customs report or work order when there is no escort	•Confirm contents of cargo for 50 out of every 100	•Do not admit entry

Ships Crew's Exit and Return Entry			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Ships Crew exit	•Confirm shore pass or ID issued by the ship	•Same as on the left	•Do not admit entry
Ships Crew entry/go on board	•Same as above •Confirm an embarkation order, seamen's book or passport or confirm with the ship	•Same as on the left	•Do not admit entry
Baggage	•Check appearance of baggage	•Confirm contents of baggage for 10 out of 100	•Do not admit entry

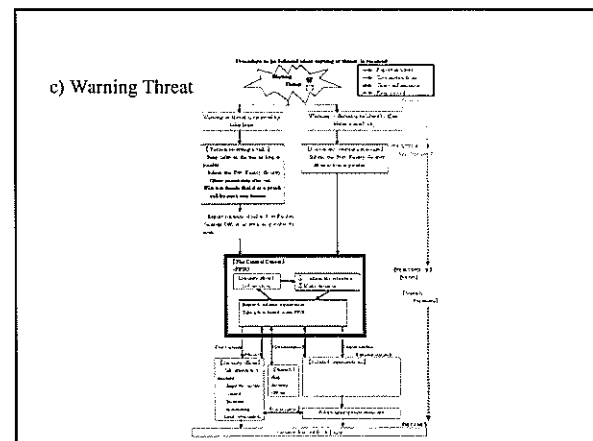
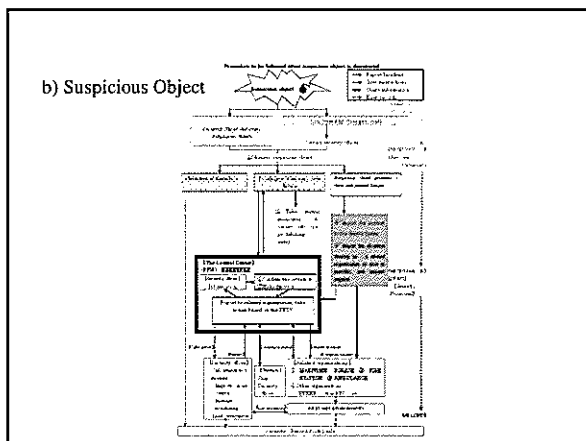
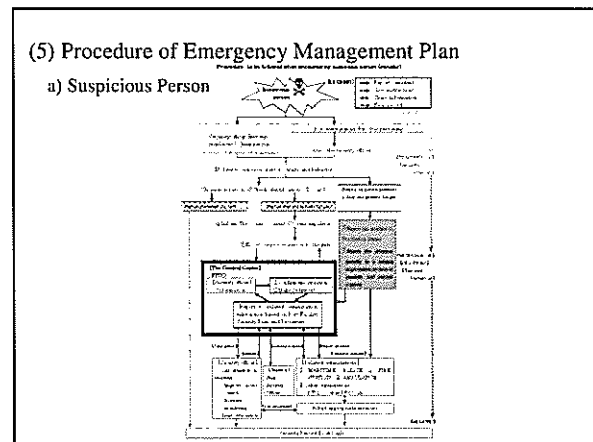
Taxi			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop	•Request to stop •Inspect trunk	•Do not admit entry
Driver	•Ask all drivers for ID card	•Ask all drivers for ID card •Check ID photo and the face for 10 out of every 100	•Do not admit entry
Passenger	•Same as above	•Same as above •Ask destination	•Do not admit entry
Baggage	•Check appearance of baggage	•Confirm contents of baggage for 10 out of 100	•Do not admit entry

Emergency Service Vehicle	
Security level	Security level 1,2 and 3 (Emergency Service personnel not required to have ID)
Vehicle	<ul style="list-style-type: none"> •Confirm the type of vehicle •Record time of entry into record book
Driver	•Confirm by the type of vehicle
Vehicle Crew	•Same as above



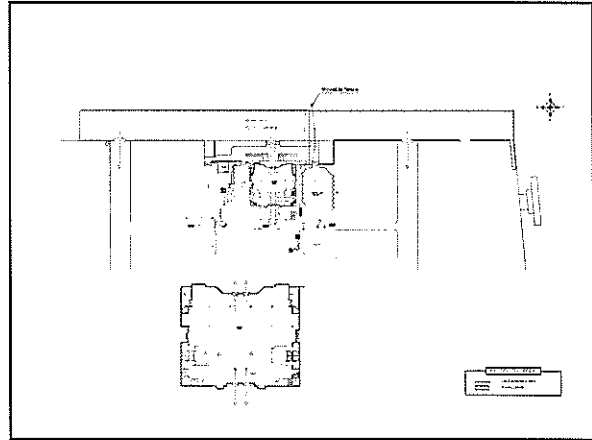
b) Inspection Procedure

Description	Items to be Checked	Daily Inspection	Periodical Inspection
Fence and Gate		*Visual inspection during patrol (repair, reinforce, or replace if necessary)	*Conduct monthly *Sway and confirm net is not loose
Security Light	Road Light	*Ensure that all security lights are illuminated by visual inspection during patrol	*Conduct annually *Check mounting of lamp fitting *Clean the cover *Check cables and switch box
Monitoring System	CCTV Camera Monitor	*Check operating range of camera platform *Check brightness of the graphics	*Conduct annually by the supplier *Cleaning, adjustment, and change consumables
Communication System	VHF Radio Telephone Fax	*Check in daily usage	*Conduct annually by the supplier *Cleaning adjustment, and change consumables



(6) Evacuation Procedure

- Evacuate following the instruction of PFSO
- Direct the gate number when evacuating from the restricted area
- Direct the name of facility when evacuating to the building
- PFSO may direct, navigate and confirm that no one fail to escape



(7) Emergency Contact List

Security Officer			
Organization/Title	Tel.	Name	Remarks
PFSO			
Deputy PFSO			

Port of Benoa			
Organization/Title	Tel.	Name	Remarks
ADPEL			
KPLP/PISO			
KPPP			
PORT HEALTH			
Fire Department			

(8) Contrast Chart for ISPS Code and PFSP

ISPS Code	PFSP
1.1	1.1
1.2	1.2
1.3	1.3
1.4	1.4
1.5	1.5
1.6	1.6
1.7	1.7
1.8	1.8
1.9	1.9
1.10	1.10
1.11	1.11
1.12	1.12
1.13	1.13
1.14	1.14
1.15	1.15
1.16	1.16
1.17	1.17
1.18	1.18
1.19	1.19
1.20	1.20
1.21	1.21
1.22	1.22
1.23	1.23
1.24	1.24
1.25	1.25
1.26	1.26
1.27	1.27
1.28	1.28
1.29	1.29
1.30	1.30
1.31	1.31
1.32	1.32
1.33	1.33
1.34	1.34
1.35	1.35
1.36	1.36
1.37	1.37
1.38	1.38
1.39	1.39
1.40	1.40
1.41	1.41
1.42	1.42
1.43	1.43
1.44	1.44
1.45	1.45
1.46	1.46
1.47	1.47
1.48	1.48
1.49	1.49
1.50	1.50
1.51	1.51
1.52	1.52
1.53	1.53
1.54	1.54
1.55	1.55
1.56	1.56
1.57	1.57
1.58	1.58
1.59	1.59
1.60	1.60
1.61	1.61
1.62	1.62
1.63	1.63
1.64	1.64
1.65	1.65
1.66	1.66
1.67	1.67
1.68	1.68
1.69	1.69
1.70	1.70

1.1	1.1	1.1
1.2	1.2	1.2
1.3	1.3	1.3
1.4	1.4	1.4
1.5	1.5	1.5
1.6	1.6	1.6
1.7	1.7	1.7
1.8	1.8	1.8
1.9	1.9	1.9
1.10	1.10	1.10
1.11	1.11	1.11
1.12	1.12	1.12
1.13	1.13	1.13
1.14	1.14	1.14
1.15	1.15	1.15
1.16	1.16	1.16
1.17	1.17	1.17
1.18	1.18	1.18
1.19	1.19	1.19
1.20	1.20	1.20
1.21	1.21	1.21
1.22	1.22	1.22
1.23	1.23	1.23
1.24	1.24	1.24
1.25	1.25	1.25
1.26	1.26	1.26
1.27	1.27	1.27
1.28	1.28	1.28
1.29	1.29	1.29
1.30	1.30	1.30
1.31	1.31	1.31
1.32	1.32	1.32
1.33	1.33	1.33
1.34	1.34	1.34
1.35	1.35	1.35
1.36	1.36	1.36
1.37	1.37	1.37
1.38	1.38	1.38
1.39	1.39	1.39
1.40	1.40	1.40
1.41	1.41	1.41
1.42	1.42	1.42
1.43	1.43	1.43
1.44	1.44	1.44
1.45	1.45	1.45
1.46	1.46	1.46
1.47	1.47	1.47
1.48	1.48	1.48
1.49	1.49	1.49
1.50	1.50	1.50
1.51	1.51	1.51
1.52	1.52	1.52
1.53	1.53	1.53
1.54	1.54	1.54
1.55	1.55	1.55
1.56	1.56	1.56
1.57	1.57	1.57
1.58	1.58	1.58
1.59	1.59	1.59
1.60	1.60	1.60
1.61	1.61	1.61
1.62	1.62	1.62
1.63	1.63	1.63
1.64	1.64	1.64
1.65	1.65	1.65
1.66	1.66	1.66
1.67	1.67	1.67
1.68	1.68	1.68
1.69	1.69	1.69
1.70	1.70	1.70

Port of Banjarmasin Trisakti Terminal

Port Facility Security

JICA Study Team on the Port Security
Enhancement Program of
Major Indonesian Public Ports

Table of Contents

1. Background of Tightening Port Security
2. PFSA for Banjarmasin Port, Trisakti Terminal
3. PFSP for Banjarmasin Port, Trisakti Terminal
 - (1) Restricted Area for Each Pier
 - (2) Port Security Facilities to be provided
 - (3) Access Control to be conducted at Gates
 - (4) Maintenance Work
 - (5) Procedure of Emergency Management Plan
 - (6) Evacuation Route
 - (7) Emergency Contact List
 - (8) Contrast Chart for ISPS Code and PFSP

1. Background of Tightening Port Security

(1) Background of the Amendment of SOLAS Convention

●9.11 Terrorist attacks
(Sept. 2001)

●Attack on the tanker off the coast of
South Yemen (Oct. 2002)
●Bali terror attack (Oct. 2002)

• Maritime Transport Security Act 2002 in the U.S.

• The U.S. assesses the effectivity of counterterrorism
of foreign ports

• Amendment of SOLAS Convention in IMO
(Dec. 2002) Tightening of ship and port security

• Implementation of international ship and port
security mandatory by 1st of July, 2004

(2) What is SOLAS Convention?

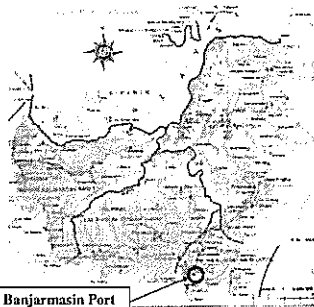
➤ Formally each shipping nation had its own maritime laws. However in response to the Titanic disaster, which resulted in death of 1,500 passengers and crew out of over 2,000, treaty for international maritime safety was concluded in 1914

(3) Outline of Amendment of SOLAS Convention

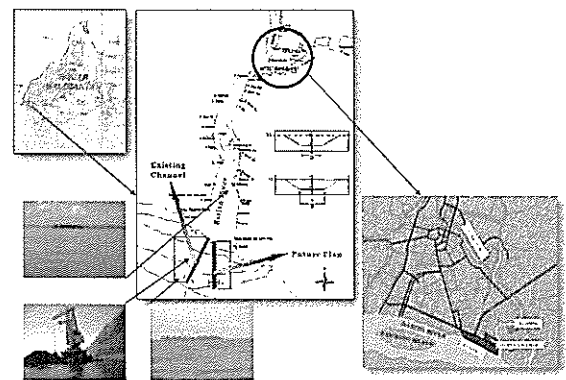
➤ To improve the reliability of international sea transportation system by having the ship owners, the port operator and port administrator take security measures

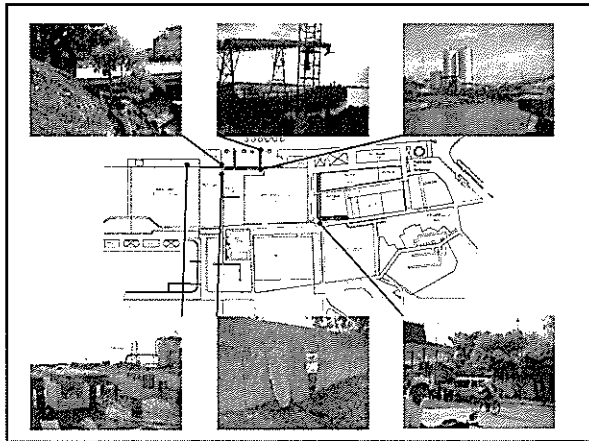
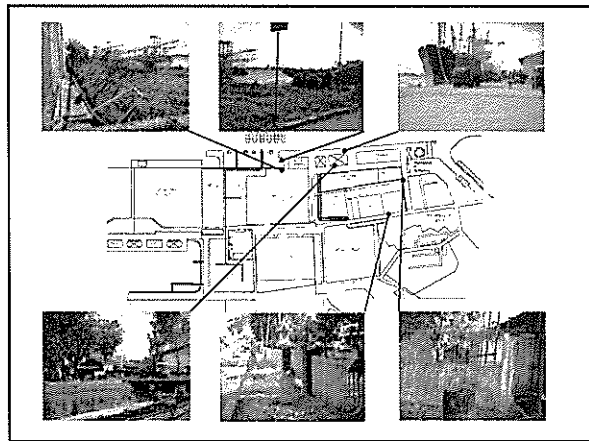
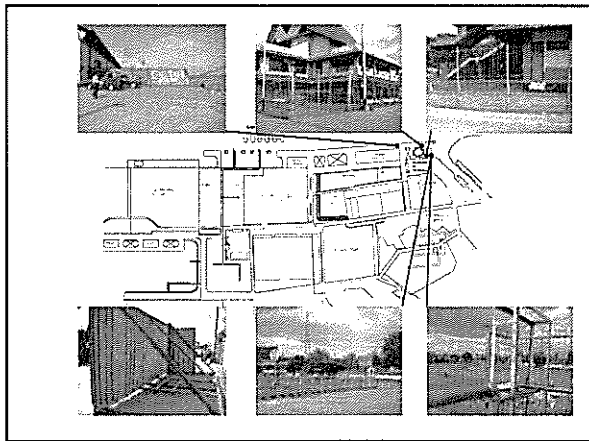
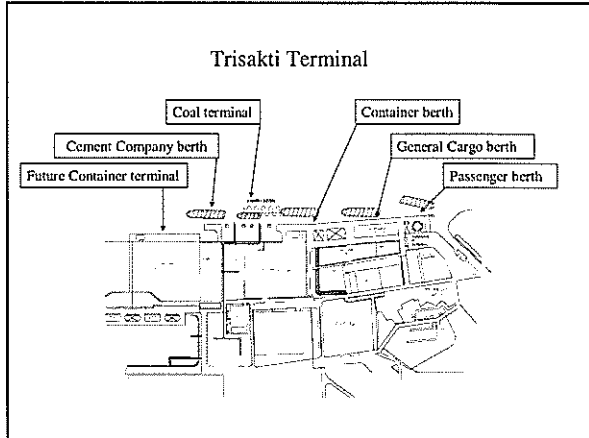
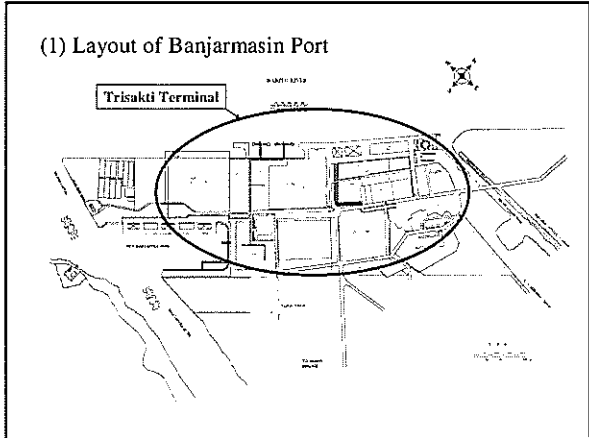
➤ To prevent an unlawful act related to international sea transportation by not admitting a ship identified to be a threat to enter the port

2. PFSA for Banjarmasin Port, Trisakti Terminal



Banjarmasin Port





- (2) Current situation of Trisakti Terminal
- No access control conducted
 - Various ships are using the same wharf
 - International Ships
 - Domestic Ships
 - Domestic Passenger Ships
 - Difficult to set restricted area for international ships
 - Berthing wharf is depending on the occasion
 - Setting of fence will interfere the activities of cargo handling and so on
 - Cargoes are transshipped at the mouth of Barito River

(3) Important Assets and Infrastructures

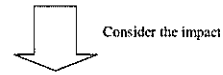
- New Container Terminal will open in (Jan.)2006

- Containers will be handled at the new CT in the future

- Passenger Terminal (domestic)

(4) Risk Evaluation

- The biggest port in south Kalimantan



- “Social” and “Economic Activities”
- “Symbolic” and “Port Activities”

(5) Recommendations

Trisakti Terminal

- Access control system(Gate) of the restricted area
- Fence surrounding the restricted area
- CCTV system and Lighting system within the restricted area
- Communication system
- Security equipment such as metal detector
- Use temporary fence and minimize the interference of port service
- Establish the procedure of international ship's calling
 - Type of temporary fence
 - Decide the number of security guards
 - Deployment of security guards
 - Area of temporary restricted area

(5) Recommendations

At the mouth of Barito River

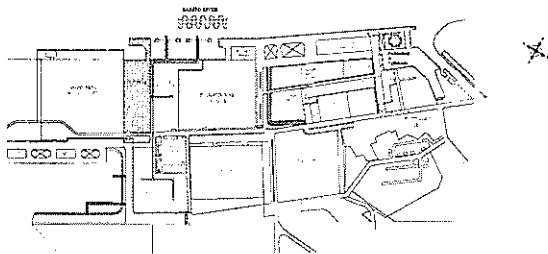
- Conduct patrol at the cargo handling point
- Ask for authority's presence when transshipping

Barito River

- Provide self-security assessment check list and fill tug boat security log

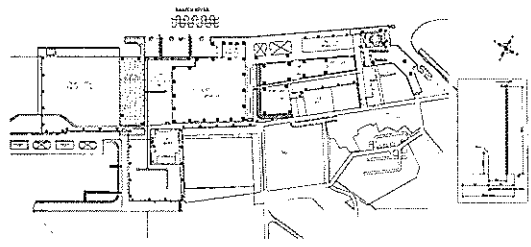
3. PFSP for Banjarmasin Port, Trisakti Terminal

(1) Proposed Restricted Area



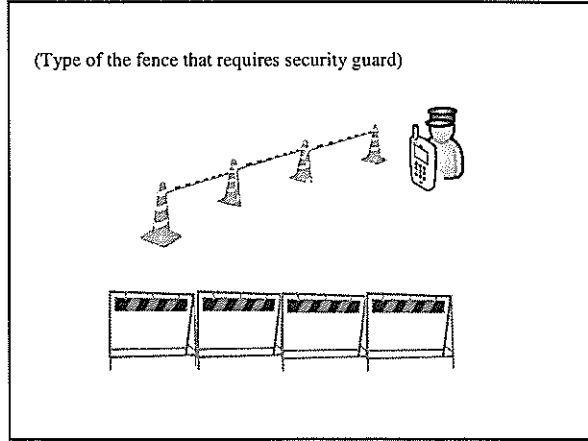
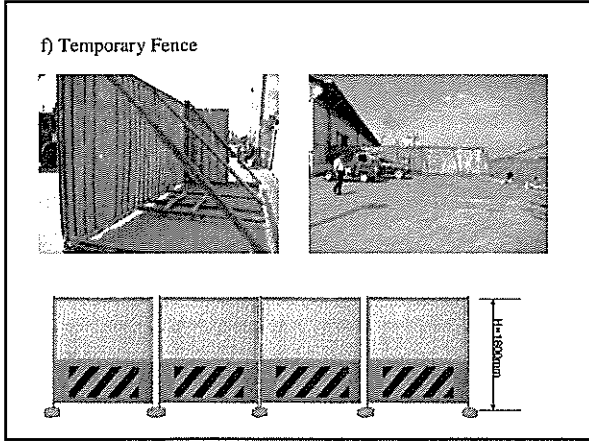
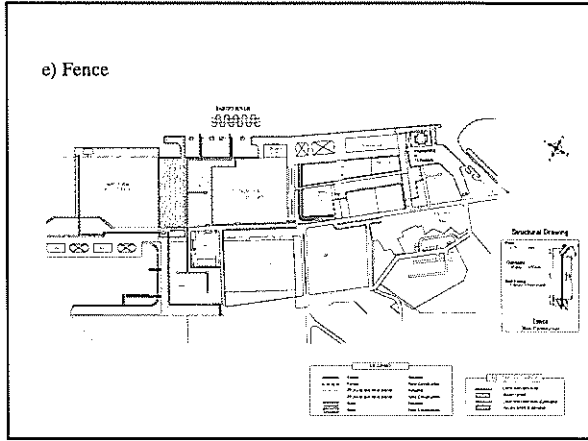
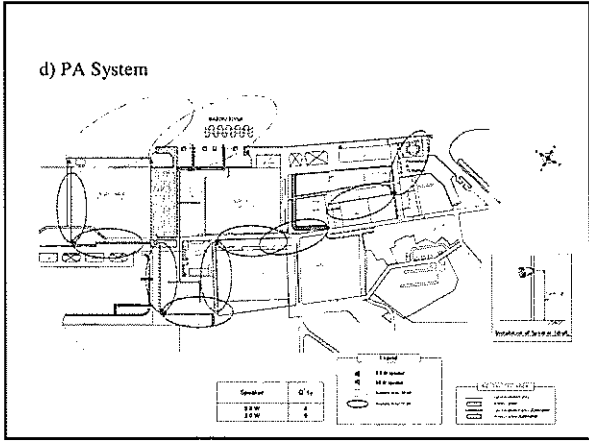
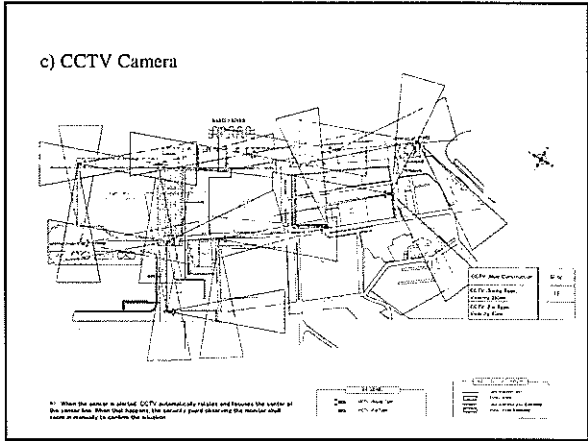
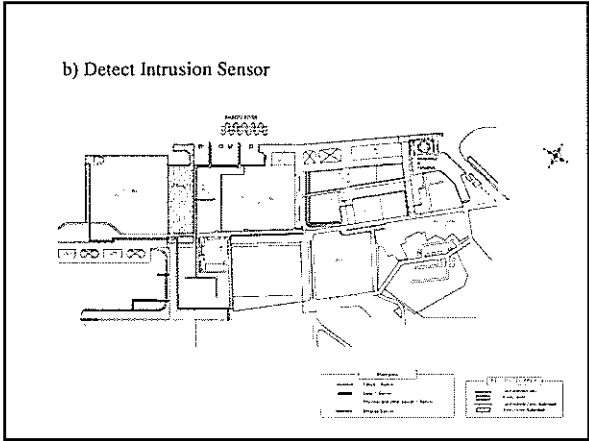
(2) Port Security Facilities to be Provided at Trisakti Terminal

a) Lighting System



11. LPS shall be placed in the main 1 light
 12. More than 3 set Photocell shall be provided for CCTV monitoring area

Lighting System	0.00
Security System	0.00



(3) Access Control to be Conducted at Gates

a) Access Control for Customs and ISPS Code

- Different Purpose
 - Customs
 - Avoid smuggling
 - Avoid goods BEING TAKEN out illegally
 - EXIT CONTROL
 - ISPS
 - Avoid Suspicious Person/Goods inside the Restricted Area
 - Protect from Terrorism
 - ENTRY CONTROL

b) Category of Entrance

- Port User (by foot or otherwise)
- Container Truck
- Construction/Maintenance Vehicle
- Ships Stores/Equipment
- Ships Crew
- Taxi
- Emergency Service Vehicle

Port User (by foot or otherwise)

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Foot or Vehicle Entry	•Request to stop •Ask for ID card all those wishing to enter	•Same as on the left •Check ID photo and the face for 10 out of every 100	•Do not admit entry
Baggage	•Check appearance of baggage	•Confirm contents of baggage for 10 out of 100	•Do not admit entry

Container Truck

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Confirm documents	•Same as on the left	•Do not admit entry
Driver	•Ask for ID card for 10 out of every 100	•Ask all drivers for ID card	•Do not admit entry
Helper	•Admit entrance on guarantee of driver	•Same as on the left	•Do not admit entry
Full Container	•Check documents and appearance	•Same as on the left	•Do not admit entry
Empty Container	•Check documents and confirm inside	•Same as on the left	•Do not admit entry

Cargo Truck

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Confirm documents	•Same as on the left	•Do not admit entry
Driver	•Ask for ID card for 10 out of every 100	•Ask all drivers for ID card	•Do not admit entry
Helper	•Admit entrance on guarantee of driver	•Same as on the left	•Do not admit entry
Freight	•Check Documents & appearance of cargo	•Inspect and confirm cargo against documents	•Do not admit entry

Construction/Maintenance Vehicle

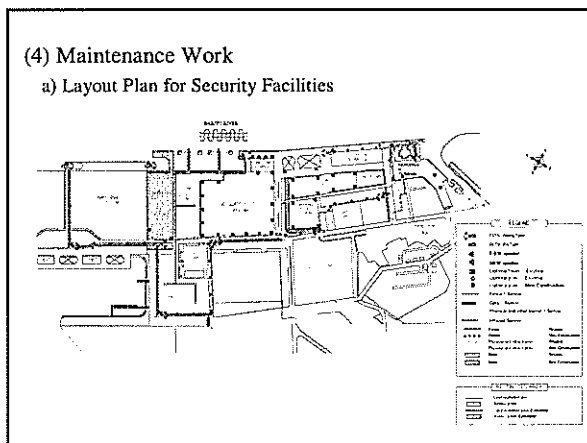
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Confirm approval with PFSO	•Same as on the left	•Do not admit entry
Driver	•Ask all drivers for ID card	•Ask all drivers for ID card •Check ID photo and the face for 10 out of every 100 •Request to fill in form and issue temporary pass when there is no ID card	•Do not admit entry
Passenger/ Workmen	•Admit entrance on guarantee of driver/foreman	•Same as above	•Do not admit entry
Cargo	•Check appearance	•Inspect contents	•Do not admit entry

Ship's Stores/Equipment			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Check documents	•Request to stop •Confirm documents	•Do not admit entry
Driver & Passenger	•Ask all drivers/Passengers for ID card •Check ID photo and face for 50 out of every 100	•Ask all drivers/Passengers for ID card •Check ID photo and the face for all those wishing to enter	•Do not admit entry
Cargo	•Not necessary to check when under escort •Confirm customs report or work order when there is no escort	•Confirm contents of cargo for 50 out of every 100	•Do not admit entry

Ships Crew's Exit and Return Entry			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Ships Crew exit	•Confirm shore pass or ID issued by the ship	•Same as on the left	•Do not admit entry
Ships Crew entry/go on board	•Same as above •Confirm an embarkation order, seamen's book or passport or confirm with the ship	•Same as on the left	•Do not admit entry
Baggage	•Check appearance of baggage	•Confirm contents of baggage for 10 out of 100	•Do not admit entry

Taxi			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop	•Request to stop •Inspect trunk	•Do not admit entry
Driver	•Ask all drivers for ID card	•Ask all drivers for ID card •Check ID photo and the face for 10 out of every 100	•Do not admit entry
Passenger	•Same as above	•Same as above •Ask destination	•Do not admit entry
Baggage	•Check appearance of baggage	•Confirm contents of baggage for 10 out of 100	•Do not admit entry

Emergency Service Vehicle	
Security level	Security level 1,2 and 3 (Emergency Service personnel not required to have ID)
Vehicle	•Confirm the type of vehicle •Record time of entry into record book
Driver	•Confirm by the type of vehicle
Vehicle Crew	•Same as above

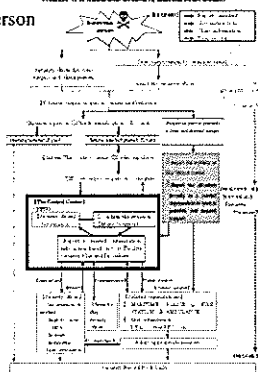


b) Inspection Procedure

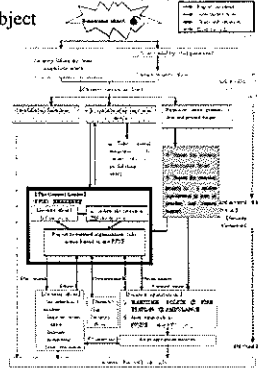
Description	Items to be Checked	Daily Inspection	Periodical Inspection
Fence and Gate		•Visual inspection during patrol (repair, reinforce, or replace if necessary)	•Conduct monthly •Sway and confirm net is not loose
Security Light	Road Light	•Ensure that all security lights are illuminated by visual inspection during patrol	•Conduct annually •Check mounting of lamp fitting •Clean the cover •check cables and switch box
Monitoring System	CCTV Camera Monitor	•Check operating range of camera platform •Check brightness of the graphics	•Conduct annually by the supplier •Cleaning, adjustment, and change consumables
Communication System	VHF Radio Telephone Fax	•Check in daily usage	•Conduct annually by the supplier •Cleaning adjustment, and change consumables

(5) Procedure of Emergency Management Plan

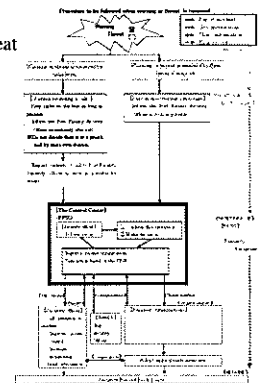
a) Suspicious Person



b) Suspicious Object



c) Warning Threat



(6) Evacuation Procedure

- Evacuate following the instruction of PFSO
- Direct the gate number when evacuating from the restricted area
- Direct the name of facility when evacuating to the building
- PFSO may direct, navigate and confirm that no one fail to escape

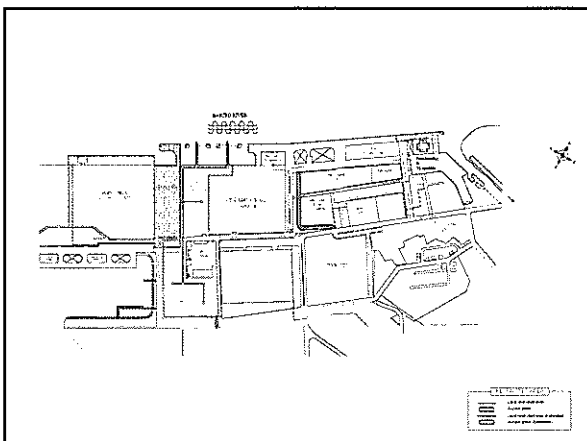
(7) Emergency Contact List

Security Officer

Organization/Title	Tel.	Name	Remarks
PFSO			
Deputy PFSO			

Port of Banjarmasin

Organization/Title	Tel.	Name	Remarks
ADPEL			
KPLP/PSO			
KPPP			
PORT HEALTH			
Fire Department			



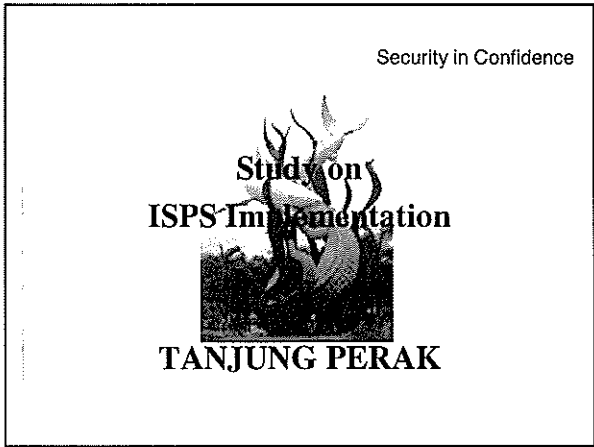
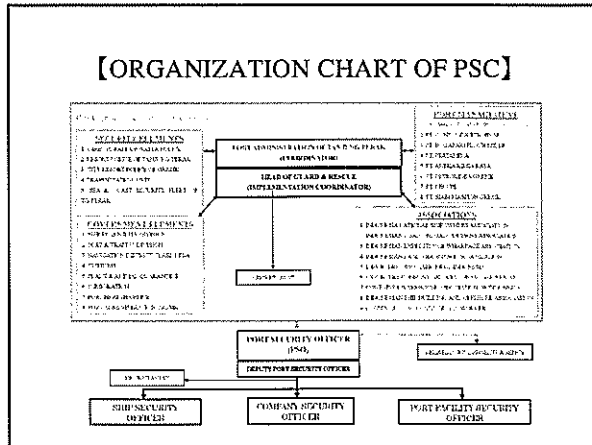
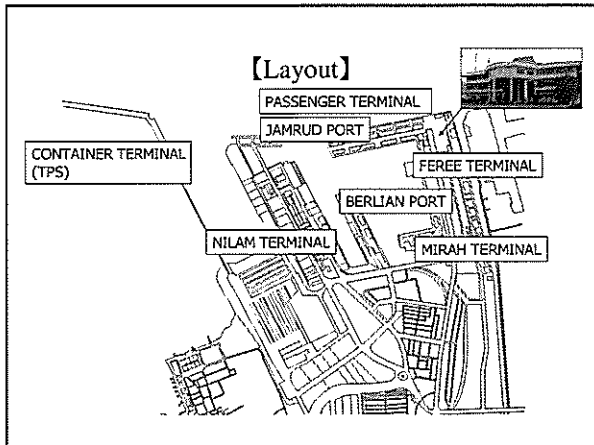
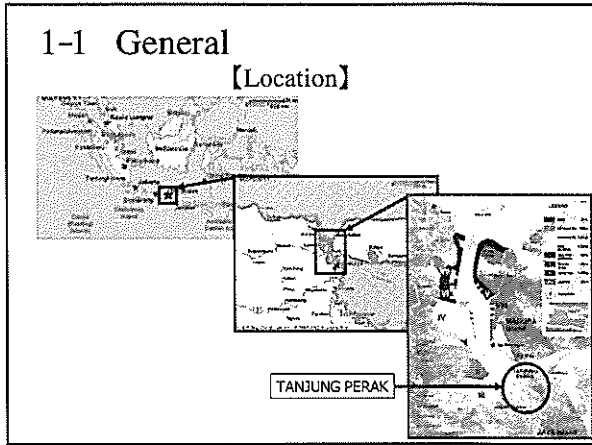


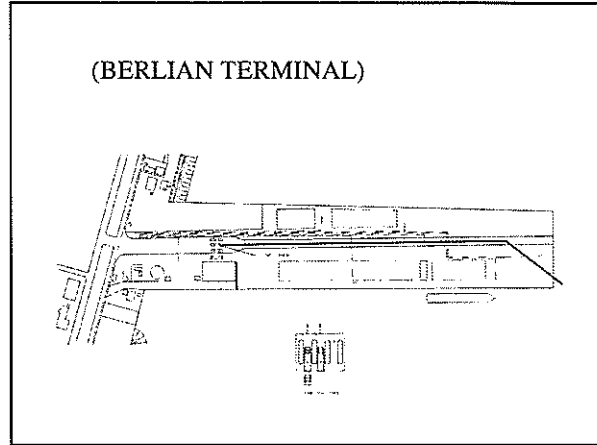
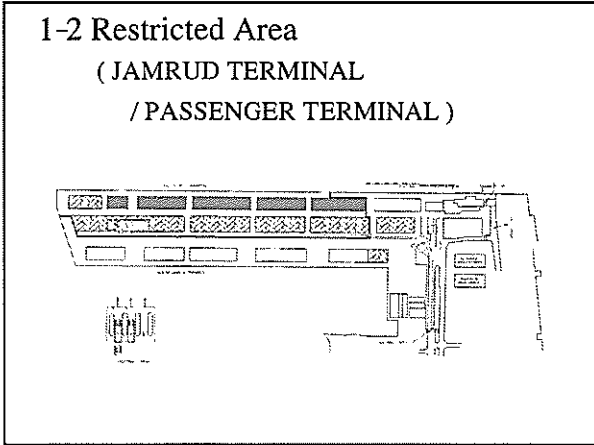
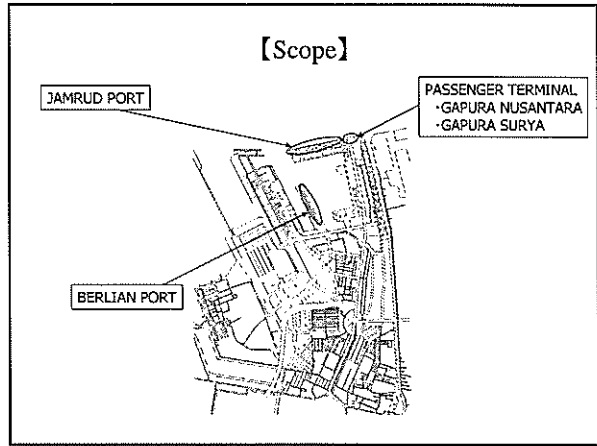
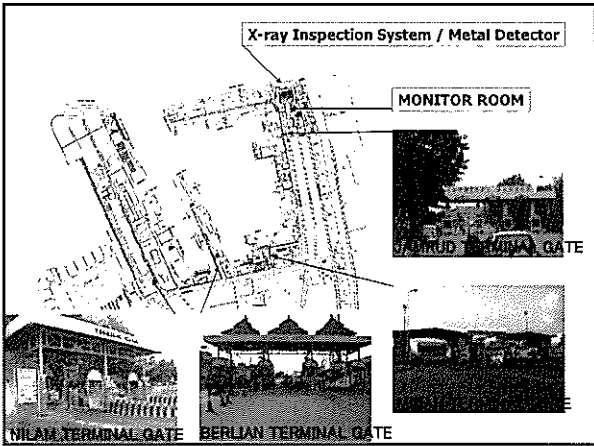
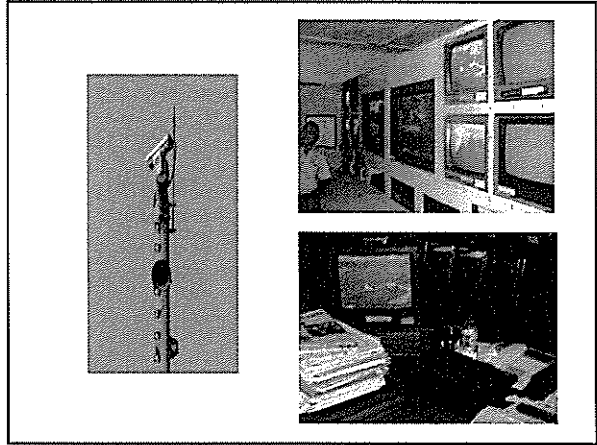
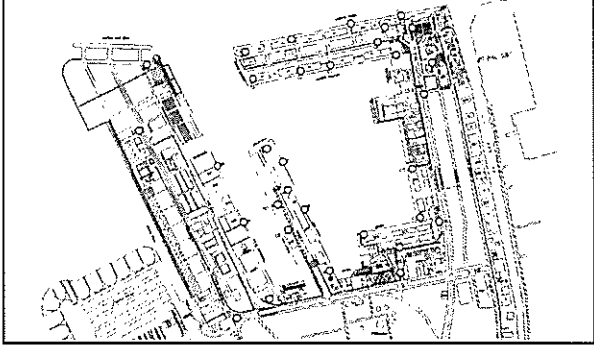
Table of Contents

- 1 Implementation
 - 1-1 General
 - 1-2 Restricted Area
 - 1-3 Important Facilities to be Protected
 - 1-4 Observation
 - 1-4-1 Access Control at the Gate
 - 1-4-2 Barrier
 - 1-4-3 Communication System
 - 1-4-4 Patrol in the Water Area
- 2 Recommendation
 - 2-1 Barrier and Gate
 - 2-2 Access Control
 - 2-3 Procedure of Monitoring Security
 - 2-4 Maintenance Work
 - 2-5 Procedure of Emergency Management Plan

1 Implementation



【CCTV (Closed-Circuit Television) SYSTEM】



1-3 Important Facility

1 Access point area and entrance gate

(1) Land area

- ① Port entrance gate
- ② Main gate and Post
- ③ Access road going outside the terminal

(2) Sea area

- ① Buoy 2 entrance groove
- ② Outside anchorage area
- ③ Movement area
- ④ Berth area

2 Restricted area including are:

(1) Cargo handling facility, terminal, storage area, and cargo handling equipments, like a:

- ① Warehouses
- ② Storage area
- ③ Passenger Terminal

(2) Electric distribution system, communication system and radio, include networks & computer system.

(3) Power plant, cargo removal piping and water installation system.

- ① Power plant substation

3 Services ships like a Tugboat, Pilot boat, and lighter have the shape of:

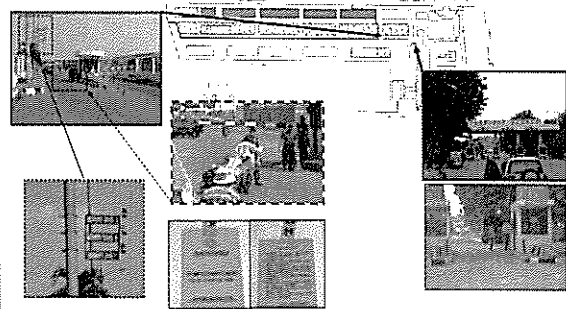
- ① Tugboat
- ② Pilot boat
- ③ Supply vessels

4 System & security equipment or monitoring, shape of:

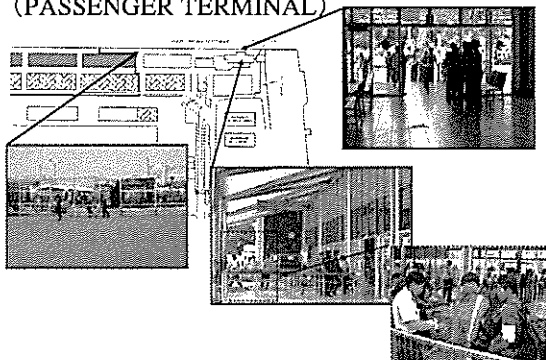
- ① System & CCTV cameras.
- ② Lightings
- ③ Fencing

1-4 Observation

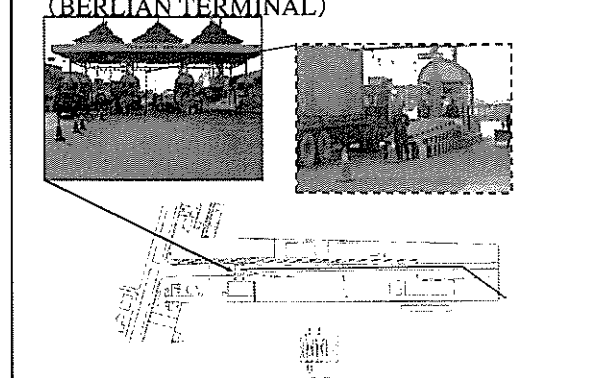
1-4-1 Access Control at the Gate (JAMRUD TERMINAL)

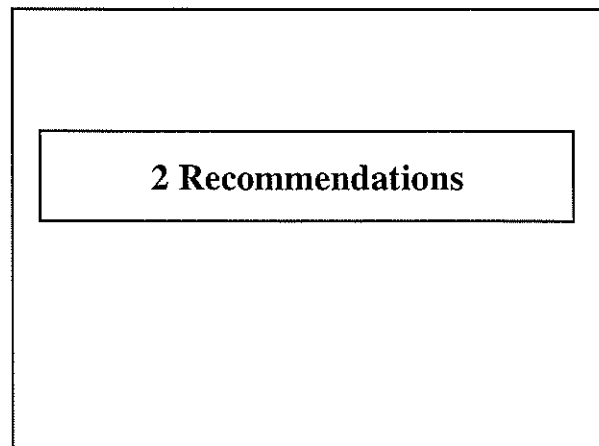
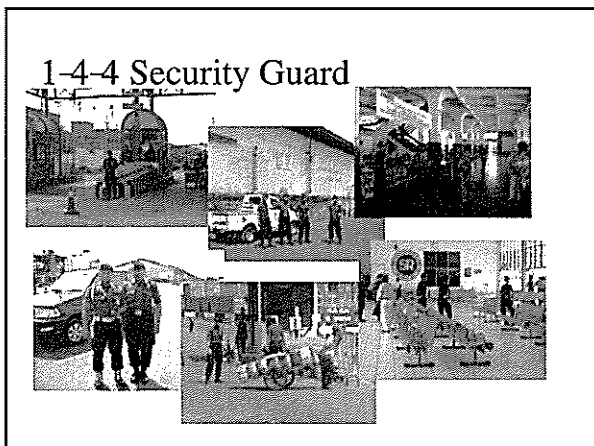
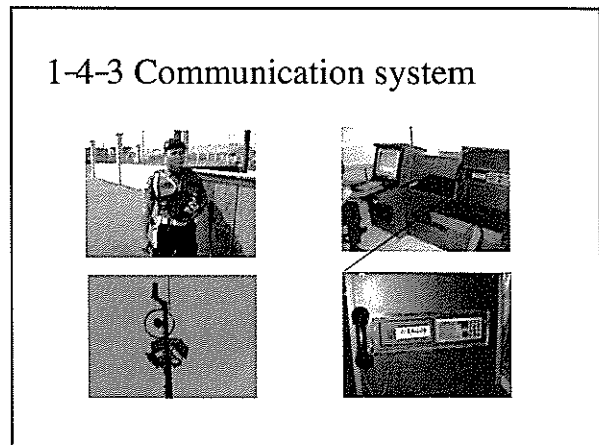
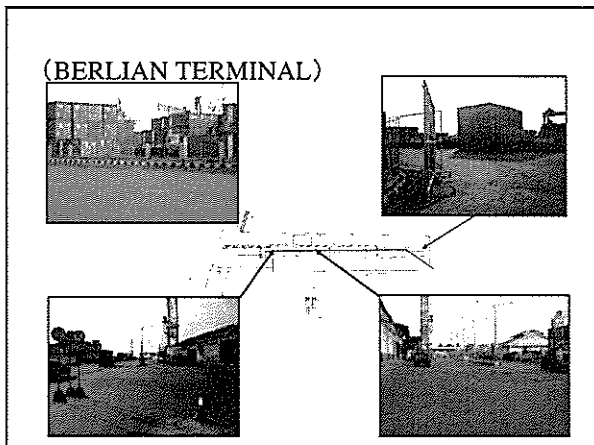
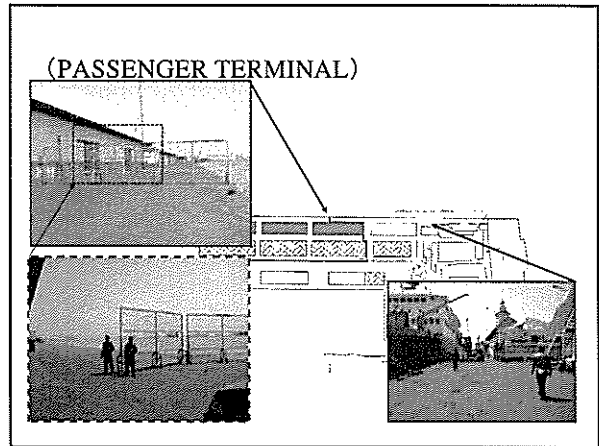
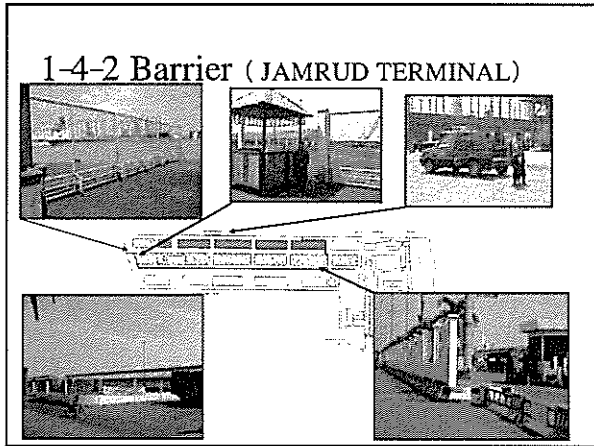


(PASSENGER TERMINAL)

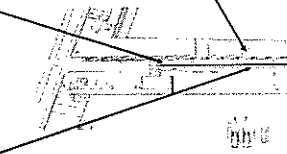
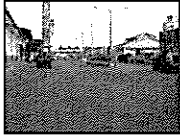
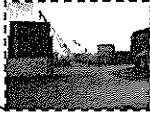


(BERLIAN TERMINAL)





2-1 Barrier and Gate



2-2 Access Control

Access Control Procedure

Port User (by foot or otherwise)

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Foot or Vehicle Entry	<ul style="list-style-type: none"> Request to stop Ask for ID card all those wishing to enter 	<ul style="list-style-type: none"> Same as on the left Check ID photo and the face for XX out of every 100 	<ul style="list-style-type: none"> Do not admit entry
Baggage	<ul style="list-style-type: none"> Check appearance of baggage 	<ul style="list-style-type: none"> Confirm contents of baggage for 10 out of 100 	

Container Truck

Continue

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	<ul style="list-style-type: none"> Request to stop Confirm documents 	<ul style="list-style-type: none"> Same as on the left 	<ul style="list-style-type: none"> Do not admit entry
Driver	<ul style="list-style-type: none"> Ask for ID card for XX out of every 100 	<ul style="list-style-type: none"> Ask all drivers for ID card 	
Helper	<ul style="list-style-type: none"> Admit entrance on guarantee of driver 	<ul style="list-style-type: none"> Same as on the left 	
Full Container	<ul style="list-style-type: none"> Check documents and appearance 	<ul style="list-style-type: none"> Same as on the left 	
Empty Container	<ul style="list-style-type: none"> Check documents and confirm inside 	<ul style="list-style-type: none"> Same as on the left 	

Cargo Truck

Continue

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	<ul style="list-style-type: none"> Request to stop Confirm documents 	<ul style="list-style-type: none"> Same as on the left 	<ul style="list-style-type: none"> Do not admit entry
Driver	<ul style="list-style-type: none"> Ask for ID card for XX out of every 100 	<ul style="list-style-type: none"> Ask all drivers for ID card 	
Helper	<ul style="list-style-type: none"> Admit entrance on guarantee of driver 	<ul style="list-style-type: none"> Same as on the left 	
Freight	<ul style="list-style-type: none"> Check Documents & appearance of cargo 	<ul style="list-style-type: none"> Inspect and confirm cargo against documents 	

Construction/Maintenance Vehicle

Continue

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	<ul style="list-style-type: none"> Request to stop Confirm approval with PFSO 	<ul style="list-style-type: none"> Same as on the left 	<ul style="list-style-type: none"> Do not admit entry
Driver	<ul style="list-style-type: none"> Ask all drivers for ID card 	<ul style="list-style-type: none"> Ask all drivers for ID card Check ID photo and the face for XX out of every 100 Request to fill in form and issue temporary pass when there is no ID card 	
Passenger/ Workmen	<ul style="list-style-type: none"> Admit entrance on guarantee of driver/foreman 	<ul style="list-style-type: none"> Same as above 	
Cargo	<ul style="list-style-type: none"> Check appearance 	<ul style="list-style-type: none"> Inspect contents 	

Ship's Stores/Equipment				continue
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO	
Vehicle	*Request to stop *Check documents	*Request to stop *Confirm documents	*Do not admit entry	
Driver & Passenger	*Ask all drivers/Passengers for ID card *Check ID photo and face for XX out of every 100	*Ask all drivers/Passengers for ID card *Check ID photo and the face for all those wishing to enter		
Cargo	*Not necessary to check when under escort *Confirm customs report or work order when there is no escort	*Confirm contents of cargo for XX out of every 100		

Ships Crew's Exit and Return Entry				Continue
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO	
Ships Crew exit	*Confirm shore pass or ID issued by the ship	*Same as on the left	*Do not admit entry	
Ships Crew entry/go on board	*Same as above *Confirm an embarkation order, seamen's book or passport or confirm with the ship	*Same as on the left		
Baggage	*Check appearance of baggage	*Confirm contents of baggage for XX out of 100		

Taxi				Continue
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO	
Vehicle	*Request to stop	*Request to stop *Inspect trunk	*Do not admit entry	
Driver	*Ask all drivers for ID card	*Ask all drivers for ID card *Check ID photo and the face for XX out of every 100		
Passenger	*Same as above	*Same as above *Ask destination		
Baggage	*Check appearance of baggage	*Confirm contents of baggage for XX out of 100		

Emergency Service Vehicle		Continue
Security level	Security level 1,2 and 3 (Emergency Service personnel not required to have ID)	
Vehicle	*Confirm the type of vehicle *Record time of entry into record book	
Driver	*Confirm by the type of vehicle	
Vehicle Crew	*Same as above	

2-3 Procedure of Monitoring Security

(1) By Manpower			
Security Level	Level 1	Level 2	Level 3
By Manpower: Mutual monitoring (security guard and workers in the restricted area)	(Method)		
	*monitoring hours:	operation hours	*Same as on the left
	*monitoring location:	one's working place	*Same as on the left
	*boundary:	suspicious person and/or goods	*In addition, follow the instruction from the Port Security Committee
	*gate:	suspicious person and/or goods	
	*within the yard	aisle, warehouse, light and etc.	
	*alongside the quay:	intruders sneak in ship from ladder, mooring rope, etc.	

(2) By CCTV Camera

Security Level	Level 1	Level 2	Level 3
By equipment (CCTV system)	<p>(Method)</p> <ul style="list-style-type: none"> • monitoring hours: round-the-clock (24hours) • monitoring location: in monitor room by security guard <p>(Items)</p> <ul style="list-style-type: none"> • set up for equipment: pre-set CCTV detectable area for sensor • boundary: suspicious person and/or goods • gate: suspicious person and/or goods • within the yard: aisle, warehouse, light and etc. • alongside the quay: intruders sneak in ship from ladder, mooring rope, etc. 	<ul style="list-style-type: none"> • Same as on the left 	<ul style="list-style-type: none"> • Same as on the left • In addition, follow the instruction from the Port Security Committee

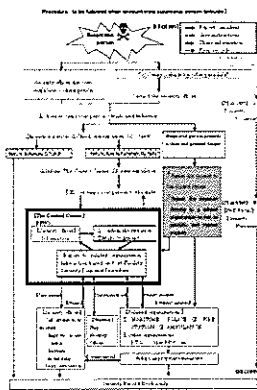
2-4 Maintenance Work

(2) Inspection Procedure

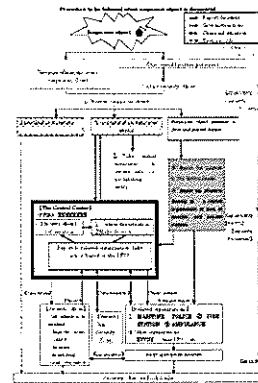
Description	Items to be Checked	Daily Inspection	Periodical Inspection
Fence and Gate		<ul style="list-style-type: none"> • Visual inspection during patrol (repair, reinforce, or replace if necessary) 	<ul style="list-style-type: none"> • Conduct monthly • Sway and confirm net is not loose
Security Light	Road Light	<ul style="list-style-type: none"> • Ensure that all security lights are illuminated by visual inspection during patrol 	<ul style="list-style-type: none"> • Conduct annually • Check mounting of lamp fitting • Clean the cover • check cables and switch box
Monitoring System	CCTV Camera Monitor	<ul style="list-style-type: none"> • Check operating range of camera platform • Check brightness of the graphics 	<ul style="list-style-type: none"> • Conduct annually by the supplier • Cleaning, adjustment, and change consumables
Communication System	VHF Radio Telephone Fax	<ul style="list-style-type: none"> • Check in daily usage 	<ul style="list-style-type: none"> • Conduct annually by the supplier • Cleaning adjustment, and change consumables

2-5 Procedure of Emergency Management Plan

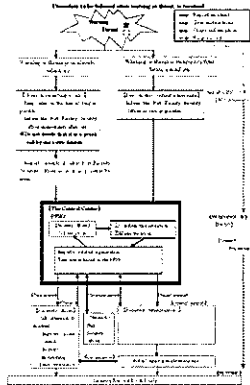
(1) Suspicious Person



(2) Suspicious Object



(3) Warning Threat



Port of Bitung Samudera Terminal Pier 1~3

Ver. 1.0

Port Facility Security

Table of Contents

1. Background of Tightening Port Security
2. PFSP for Bitung Port, Samudera Terminal
3. Access Control to be constructed at Gates
4. Maintenance Work
5. Procedure of Emergency Management Plan
6. Evacuation Route
7. Emergency Contact List
8. Contrast Chart for ISPS Code and PFSP

1. Background of Tightening Port Security

(1) Background of the Amendment of SOLAS Convention

• 9.11 Terrorist attacks (Sept. 2001)

• Attack on the tanker off the coast of South Yemen (Oct. 2002)
• Bali terror attack (Oct. 2002)



• Maritime Transport Security Act 2002 in the U.S.

• The U.S. assesses the effectivity of counterterrorism of foreign ports

• Amendment of SOLAS Convention in IMO (Dec. 2002) Tightening of ship and port security

• Implementation of international ship and port security mandatory by 1st of July, 2004

(2) What is SOLAS Convention?

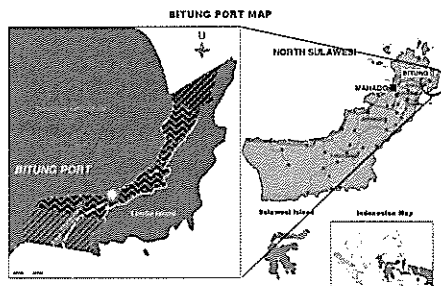
➤ Formally each shipping nation had its own maritime laws. However in response to the Titanic disaster, which resulted in death of 1,500 passengers and crew out of over 2,000, treaty for international maritime safety was concluded in 1914

(3) Outline of Amendment of SOLAS Convention

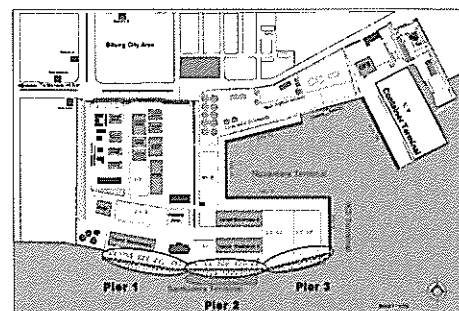
➤ To improve the reliability of international sea transportation system by having the ship owners and the port authorities take security measures

➤ To prevent an unlawful act related to international sea transportation by not admitting a ship identified to be a threat to enter the port

2. PFSP for Bitung Port, Samudera Terminal



(1) Layout of Bitung Port



(2) Specific Usage of Samudera Terminal

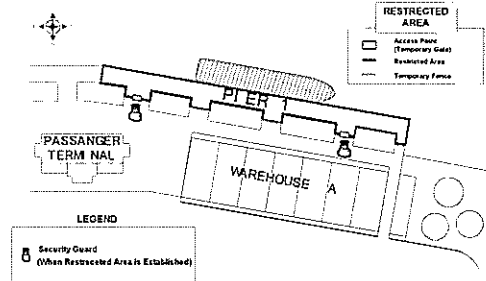
- Domestic vessels
- 5 international calls / month
- Includes passenger terminal
- Anchoring wharf is depending on the size of vessel



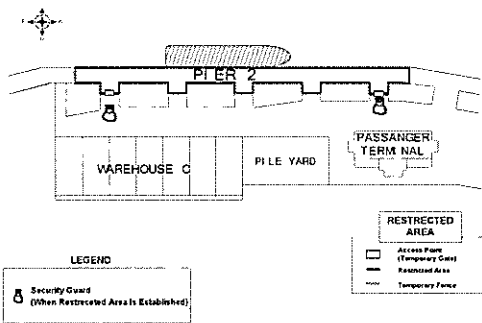
- Temporary Fence
- Individual Barrier

(3) Restricted Area for Each Pier

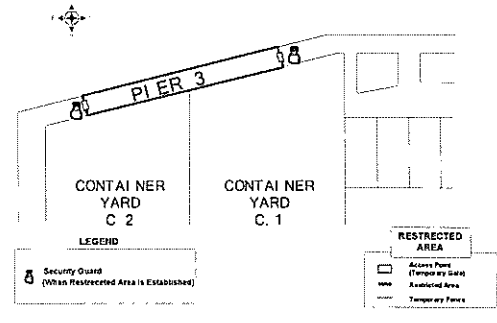
a) Pier 1



b) Pier 2

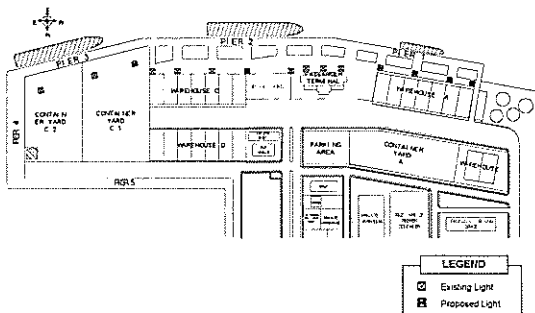


c) Pier 3

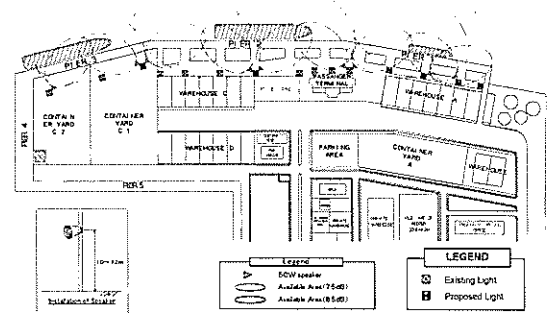


(4) Port Security Facilities to be Provided at Samudera Terminal

a) Lighting System



b) PA System



3. Access Control to be Conducted at Gates

(1) Access Control for Customs and ISPS Code

- Different Purpose
 - Customs
 - Avoid smuggling
 - Avoid goods taking out illegally
 - EXIT CONTROL
 - ISPS
 - Avoid Suspicious Person/Goods inside the Restricted Area
 - Protect from Terrorism
 - ENTRY CONTROL

(2) Category of Entrance

- Port User (by foot or otherwise)
- Container Truck
- Construction/Maintenance Vehicle
- Ships Stores/Equipment
- Ships Crew's Exit and Return Entry
- Taxi
- Emergency Service Vehicle

Port User (by foot or otherwise)

Security Level	Level 1	Level 2	Level 3 (after the area is secured by inspection)
Foot or Vehicle Entry	<ul style="list-style-type: none"> • Request to stop • Ask for ID card all those wishing to enter 	<ul style="list-style-type: none"> • Same as on the left • Check ID photo and the face for 10 out of every 100 	<ul style="list-style-type: none"> • Request to stop • Ask for ID card all those wishing to enter • Check ID photo and the face for all those wishing to enter
Baggage	<ul style="list-style-type: none"> • Check appearance of baggage 	<ul style="list-style-type: none"> • Confirm contents of baggage for 10 out of 100 	<ul style="list-style-type: none"> • Open and inspect all baggage with consent of owner

Container Truck

Security Level	Level 1	Level 2	Level 3 (after the area is secured by inspection)
Vehicle	<ul style="list-style-type: none"> • Request to stop • Confirm documents 	<ul style="list-style-type: none"> • Same as on the left 	<ul style="list-style-type: none"> • Same as on the left • Record car number
Driver	<ul style="list-style-type: none"> • Ask for ID card for 10 out of every 100 	<ul style="list-style-type: none"> • Ask all drivers for ID card 	<ul style="list-style-type: none"> • Ask all drivers for ID card • Check ID photo and the face for all drivers
Helper	<ul style="list-style-type: none"> • Admit entrance on guarantee of driver 	<ul style="list-style-type: none"> • Same as on the left 	<ul style="list-style-type: none"> • Do not admit entrance
Full Container	<ul style="list-style-type: none"> • Check documents and appearance 	<ul style="list-style-type: none"> • Same as on the left 	<ul style="list-style-type: none"> • Same as on the left
Empty Container	<ul style="list-style-type: none"> • Check documents and confirm inside 	<ul style="list-style-type: none"> • Same as on the left 	<ul style="list-style-type: none"> • Same as on the left

Cargo Truck

Security Level	Level 1	Level 2	Level 3 (after the area is secured by inspection)
Vehicle	<ul style="list-style-type: none"> • Request to stop • Confirm documents 	<ul style="list-style-type: none"> • Same as on the left 	<ul style="list-style-type: none"> • Same as on the left • Record car number
Driver	<ul style="list-style-type: none"> • Ask for ID card for 10 out of every 100 	<ul style="list-style-type: none"> • Ask all drivers for ID card 	<ul style="list-style-type: none"> • Ask all drivers for ID card • Check ID photo and the face for all drivers
Helper	<ul style="list-style-type: none"> • Admit entrance on guarantee of driver 	<ul style="list-style-type: none"> • Same as on the left 	<ul style="list-style-type: none"> • Do not admit entrance
Freight	<ul style="list-style-type: none"> • Check Documents & appearance of cargo 	<ul style="list-style-type: none"> • Inspect and confirm cargo against documents 	<ul style="list-style-type: none"> • Same as on the left

Construction/Maintenance Vehicle

Security Level	Level 1	Level 2	Level 3 (after the area is secured by inspection)
Vehicle	<ul style="list-style-type: none"> • Request to stop • Confirm approval with PFSO 	<ul style="list-style-type: none"> • Same as on the left 	<ul style="list-style-type: none"> • Same as on the left • Record car number
Driver	<ul style="list-style-type: none"> • Ask all drivers for ID card 	<ul style="list-style-type: none"> • Ask all drivers for ID card • Check ID photo and the face for 10 out of every 100 • Request to fill in form and issue temporary pass when there is no ID card 	<ul style="list-style-type: none"> • Ask all drivers for ID card • Check ID photo and the face for all drivers • No ID, no entry
Passenger/ Workmen	<ul style="list-style-type: none"> • Admit entrance on guarantee of driver/foreman 	<ul style="list-style-type: none"> • Same as above 	<ul style="list-style-type: none"> • Same as above
Cargo	<ul style="list-style-type: none"> • Check appearance 	<ul style="list-style-type: none"> • Inspect contents 	<ul style="list-style-type: none"> • Open and inspect the cargo with consent of the driver

Ship's Stores/Equipment			
Security Level	Level 1	Level 2	Level 3 (after the area is secured by inspection)
Vehicle	•Request to stop •Check documents	•Request to stop •Confirm documents	•Admit entrance only by escort by representative of ships
Driver & Passenger	•Ask all drivers/Passengers for ID card •Check ID photo and face for 50 out of every 100	•Ask all drivers/Passengers for ID card •Check ID photo and the face for all those wishing to enter	•Same as on the left
Cargo	•Not necessary to check when under escort •Confirm customs report or work order when there is no escort	•Confirm contents of cargo for 50 out of every 100	•Confirm contents of all entry against ships initial order

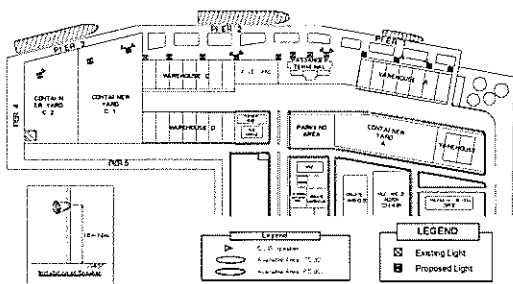
Ships Crew's Exit and Return Entry			
Security Level	Level 1	Level 2	Level 3 (after the area is secured by inspection)
Ships Crew exit	•Confirm shore pass or ID issued by the ship	•Same as on the left	•Confirm shore pass or ID issued by the ship or if without photo request to be escorted by a representative of the ship
Ships Crew entry/go on board	•Same as above •Confirm an embarkation order, seaman's book or passport or confirm with the ship	•Same as on the left	•Same as above •Confirm an embarkation order, seaman's book or passport or confirm with the ship
Baggage	•Check appearance of baggage	•Confirm contents of baggage for 10 out of 100	•Open and inspect all baggage with consent of owner

Taxi			
Security Level	Level 1	Level 2	Level 3 (after the area is secured by inspection)
Vehicle	•Request to stop	•Request to stop •Inspect trunk	•Do not admit entrance
Driver	•Ask all drivers for ID card	•Ask all drivers for ID card •Check ID photo and the face for 10 out of every 100	•Same as above
Passenger	•Same as above	•Same as above •Ask destination	•Check ID photo of all those wishing to enter •Ask destination
Baggage	•Check appearance of baggage	•Confirm contents of baggage for 10 out of 100	•Open and inspect all baggage with consent of owner

Emergency Service Vehicle	
Security level	Security level 1,2 and 3 (Emergency Service personnel not required to have ID)
Vehicle	•Confirm the type of vehicle •Record time of entry into record book
Driver	•Confirm by the type of vehicle
Vehicle Crew	•Same as above

4. Maintenance Work

(1) Layout Plan for Security Facilities

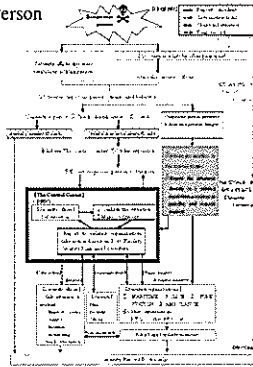


(2) Inspection Procedure

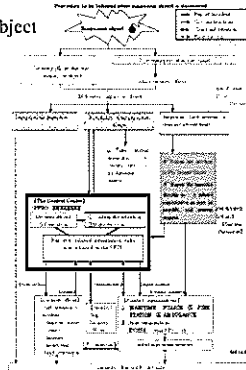
Description	Items to be Checked	Daily Inspection	Periodical Inspection
Security Light	Road Light	•Ensure that all security lights are illuminated by visual inspection during patrol	•Conduct annually •Check mounting of lamp fitting •Clean the cover check cables and switch box
Communication System	VHF Radio Telephone Fax	•Check in daily usage	•Conduct annually by the supplier •Cleaning adjustment, and change consumables

5. Procedure of Emergency Management Plan

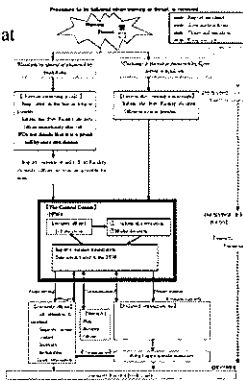
(1) Suspicious Person



(2) Suspicious Object



(3) Warning Threat



6. Evacuation Procedure

(1) Evacuation Procedure

- Evacuate following the instruction of PFSO
- Direct the gate No. when evacuating from the restricted area
- Direct the name of facility when evacuating to the building
- PFSO may direct, navigate and confirm that no one fail to escape

7. Emergency Contact List

Security Officer

Organization/Title	Tel.	Name	Remarks
PFSO			
Deputy PFSO			

Port of Tanjung Instan

Organization/Title	Tel.	Name	Remarks
ADPEL			
KPLP/PFSO			
KPPP			
PORT HEALTH			
Fire Department			

8. Contrast Chart for ISPS Code and PFSP

ISPS Code	ISPS Code	PFSP
1.1.1	1.1.1	1.1.1
1.1.2	1.1.2	1.1.2
1.1.3	1.1.3	1.1.3
1.1.4	1.1.4	1.1.4
1.1.5	1.1.5	1.1.5
1.1.6	1.1.6	1.1.6
1.1.7	1.1.7	1.1.7
1.1.8	1.1.8	1.1.8
1.1.9	1.1.9	1.1.9
1.1.10	1.1.10	1.1.10
1.1.11	1.1.11	1.1.11
1.1.12	1.1.12	1.1.12
1.1.13	1.1.13	1.1.13
1.1.14	1.1.14	1.1.14
1.1.15	1.1.15	1.1.15
1.1.16	1.1.16	1.1.16
1.1.17	1.1.17	1.1.17
1.1.18	1.1.18	1.1.18
1.1.19	1.1.19	1.1.19
1.1.20	1.1.20	1.1.20
1.1.21	1.1.21	1.1.21
1.1.22	1.1.22	1.1.22
1.1.23	1.1.23	1.1.23
1.1.24	1.1.24	1.1.24
1.1.25	1.1.25	1.1.25
1.1.26	1.1.26	1.1.26
1.1.27	1.1.27	1.1.27
1.1.28	1.1.28	1.1.28
1.1.29	1.1.29	1.1.29
1.1.30	1.1.30	1.1.30
1.1.31	1.1.31	1.1.31
1.1.32	1.1.32	1.1.32
1.1.33	1.1.33	1.1.33
1.1.34	1.1.34	1.1.34
1.1.35	1.1.35	1.1.35
1.1.36	1.1.36	1.1.36
1.1.37	1.1.37	1.1.37
1.1.38	1.1.38	1.1.38
1.1.39	1.1.39	1.1.39
1.1.40	1.1.40	1.1.40
1.1.41	1.1.41	1.1.41
1.1.42	1.1.42	1.1.42
1.1.43	1.1.43	1.1.43
1.1.44	1.1.44	1.1.44
1.1.45	1.1.45	1.1.45
1.1.46	1.1.46	1.1.46
1.1.47	1.1.47	1.1.47
1.1.48	1.1.48	1.1.48
1.1.49	1.1.49	1.1.49
1.1.50	1.1.50	1.1.50
1.1.51	1.1.51	1.1.51
1.1.52	1.1.52	1.1.52
1.1.53	1.1.53	1.1.53
1.1.54	1.1.54	1.1.54
1.1.55	1.1.55	1.1.55
1.1.56	1.1.56	1.1.56
1.1.57	1.1.57	1.1.57
1.1.58	1.1.58	1.1.58
1.1.59	1.1.59	1.1.59
1.1.60	1.1.60	1.1.60
1.1.61	1.1.61	1.1.61
1.1.62	1.1.62	1.1.62
1.1.63	1.1.63	1.1.63
1.1.64	1.1.64	1.1.64
1.1.65	1.1.65	1.1.65
1.1.66	1.1.66	1.1.66
1.1.67	1.1.67	1.1.67
1.1.68	1.1.68	1.1.68
1.1.69	1.1.69	1.1.69
1.1.70	1.1.70	1.1.70
1.1.71	1.1.71	1.1.71
1.1.72	1.1.72	1.1.72
1.1.73	1.1.73	1.1.73
1.1.74	1.1.74	1.1.74
1.1.75	1.1.75	1.1.75
1.1.76	1.1.76	1.1.76
1.1.77	1.1.77	1.1.77
1.1.78	1.1.78	1.1.78
1.1.79	1.1.79	1.1.79
1.1.80	1.1.80	1.1.80
1.1.81	1.1.81	1.1.81
1.1.82	1.1.82	1.1.82
1.1.83	1.1.83	1.1.83
1.1.84	1.1.84	1.1.84
1.1.85	1.1.85	1.1.85
1.1.86	1.1.86	1.1.86
1.1.87	1.1.87	1.1.87
1.1.88	1.1.88	1.1.88
1.1.89	1.1.89	1.1.89
1.1.90	1.1.90	1.1.90
1.1.91	1.1.91	1.1.91
1.1.92	1.1.92	1.1.92
1.1.93	1.1.93	1.1.93
1.1.94	1.1.94	1.1.94
1.1.95	1.1.95	1.1.95
1.1.96	1.1.96	1.1.96
1.1.97	1.1.97	1.1.97
1.1.98	1.1.98	1.1.98
1.1.99	1.1.99	1.1.99
1.1.100	1.1.100	1.1.100

Port of Samarinda

Port Facility Security

Ver. 1.0

JICA Study Team

on the Port Security Enhancement Program
of Major Indonesian Public Ports

Table of Contents

1. Background of Tightening Port Security
2. PFSA for Samarinda Port
3. PFSP for Samarinda Port
 - (1) Restricted Area
 - (2) Access Control at Gate
 - (3) Emergency Contact List
- (4) Contrast Chart for ISPS Code and PFSP

1. Background of Tightening Port Security

(1) Background of the Amendment of SOLAS Convention

9.11 Terrorist attacks (Sept. 2001)

Attack on the tanker off the coast of South Yemen (Oct 2002)
Bali terror attack (Oct. 2002)



Maritime Transport Security Act 2002 in the U.S.

The U.S. assesses the effectivity of counterterrorism of foreign ports

Amendment of SOLAS Convention in IMO (Dec. 2002) Tightening of ship and port security

Implementation of international ship and port security mandatory by 1st of July, 2004

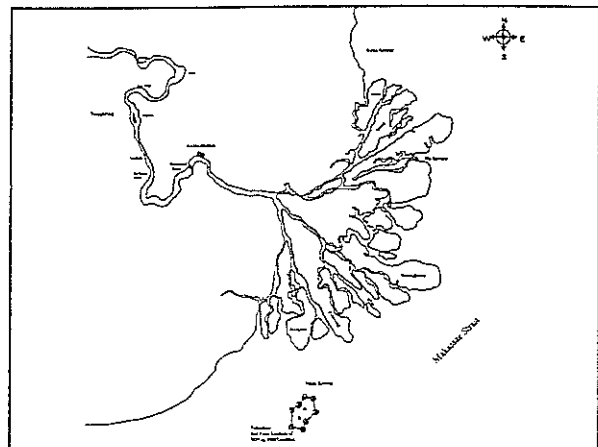
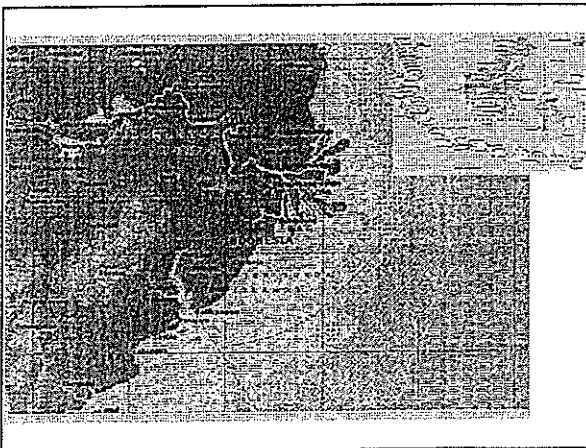
(2) What is SOLAS Convention?

> Formally each shipping nation had its own maritime laws. However in response to the Titanic disaster, which resulted in death of 1,500 passengers and crew out of over 2,000, treaty for international maritime safety was concluded in 1914

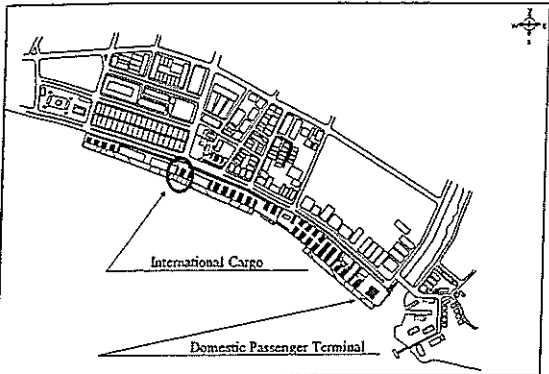
(3) Outline of Amendment of SOLAS Convention

> To improve the reliability of international sea transportation system by having the ship owners and the Port Operator and Port Administrator take security measures

> To prevent an unlawful act related to international sea transportation by not admitting a ship identified to be a threat to enter the port



2. PFSA for SAMARINDA PORT



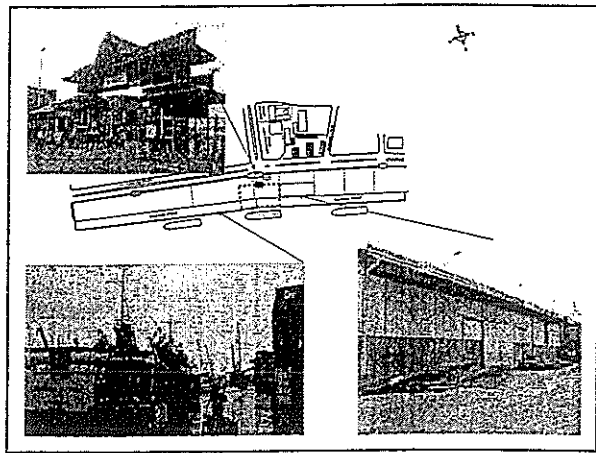
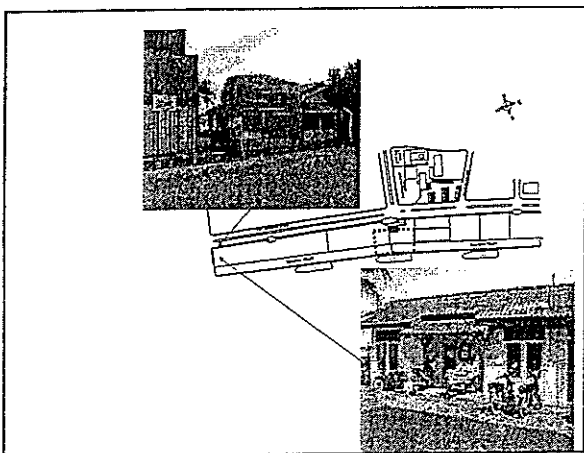
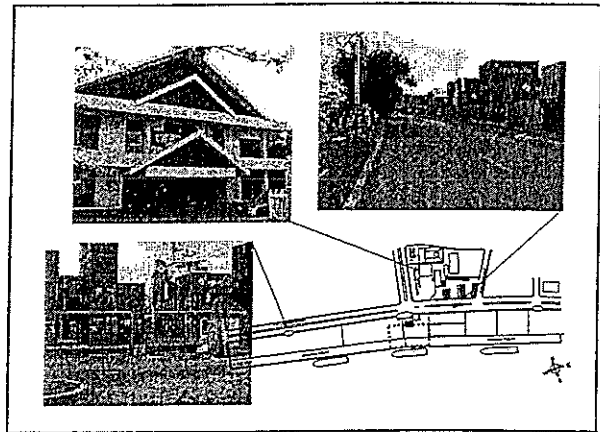
(1) Difficulty

Difficult to set restricted area for international ships

- Few international vessel calls a year
- Setting of fence around international berth will interfere the activities of cargo handling

(2) Current situation of security measure

- Fence and Gate
- Access control at the gate conducted by KPLP
 - International berth
 - Domestic berth
 - Passenger berth



(3) Important Assets and Infrastructures

- Berth and Handling Yard
- Cargo Handling Machine
- Vessel
- Anchorage area and waterway

(4) Result of Assessment

One of the biggest port in Karimantan



Consider the impact

“Social” and “Economic” → “High”

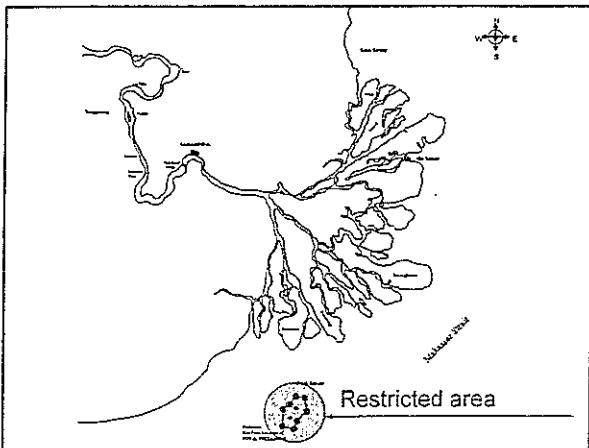
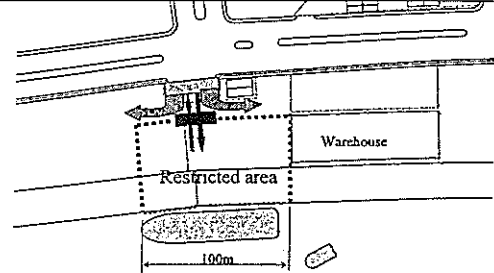
“Symbolic” → “Low”

(5) Recommendations

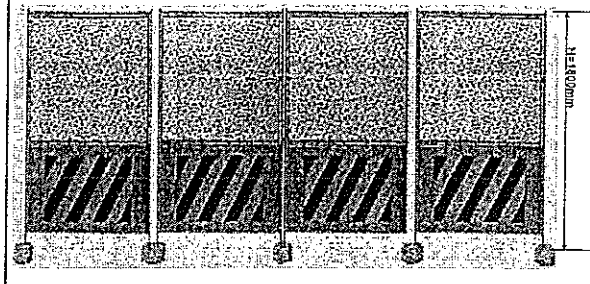
- Use temporary fence and minimize the interference of port service
- Establish a procedure of access control and security patrol before and while international ship’s call
 - Type of temporary fence
 - Decide the number of security guards
 - Area of temporary restricted area

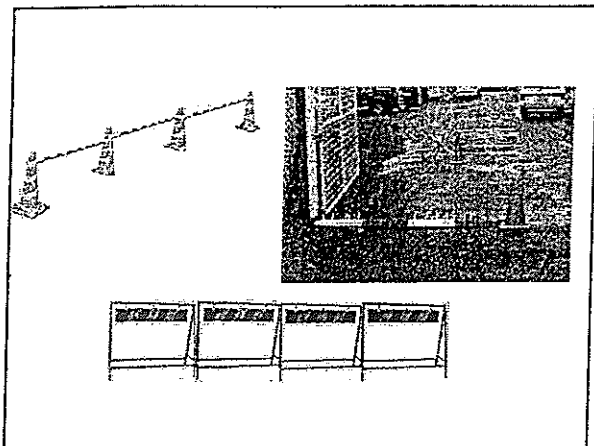
2. Port Facility Security Plan for international port for Samarinda

(1) Restricted Area



Temporary Fence





(2) Access Control to be Conducted at Gates

a) Access Control for Customs and ISPS Code Different Purpose

– Customs/Quarantine

- Avoid smuggling/Stowaway
- Avoid goods BEING TAKEN out illegally
- Others

ISPS Code

- Avoid Suspicious Person/Goods inside the Restricted Area
- Protect from Terrorism/others

b) Category of Entrance

- Port User (by foot or otherwise)
- Cargo Truck
- Ship Stores/Equipment
- Ship Crew
- Emergency Service Vehicle

Port User (by foot or otherwise)

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Foot or Vehicle Entry	•Request to stop •Ask for ID card all those wishing to enter	•Same as on the left •Check ID photo and the face for XX out of every 100	•Closed
Baggage	•Check appearance of baggage	•Confirm contents of baggage for XX out of 100	•Closed

Cargo Truck

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Confirm documents •Check Sticker	•Same as on the left	•Closed
Driver	•Ask for ID card for XX out of every 100	•Ask all drivers for ID card	•Closed
Helper	•Admit entrance on guarantee of driver	•Same as on the left	•Closed
Freight	•Check Documents & appearance of cargo	•Inspect and confirm cargo against documents	•Closed

Ship's Stores/Equipment

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Check documents •Check sticker	•Request to stop •Confirm documents •Check sticker	•Closed
Driver & Passenger	•Ask all drivers/Passengers for ID card •Check ID photo and face for XX out of every 100	•Ask all drivers/Passengers for ID card •Check ID photo and the face for all those wishing to enter	•Closed
Cargo	•Not necessary to check when under escort •Confirm customs report or work order when there is no escort	•Confirm contents of cargo for XX out of every 100	•Closed

Ships Crew's Exit and Return Entry			
Security Level	Level 1 Conducted by PFSSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Ships Crew exit	•Confirm shore pass or ID issued by the ship	•Same as on the left	•Closed
Ships Crew entry/go on board	•Same as above •Confirm an embarkation order, seaman's book or passport or confirm with the ship	•Same as on the left	•Closed
Baggage	•Check appearance of baggage	•Confirm contents of baggage for XXout of 100	•Closed

Emergency Service Vehicle	
Security level	Security level 1,2 and 3
Vehicle	•Confirm the type of vehicle •Record time of entry into record book
Driver	•Confirm by the type of vehicle
Vehicle Crew	•Same as above

(3) Emergency Contact List

Security Officer

Organization/Title	Tel.	Name	Remarks
PFSSO			
Deputy PFSSO			

Port Security Committee

Organization/Title	Tel.	Name	Remarks
PSO			
KPLP			
KPPP			
CUSTOMS			
Immigration			
Quarantine			
Port Health			
Fire Department			
Any other PFSSO			

(4) Contrast Chart for ISPS Code and PFSP

ISPS Code	PFSP
1.1.1.1	1.1.1.1
1.1.1.2	1.1.1.2
1.1.1.3	1.1.1.3
1.1.1.4	1.1.1.4
1.1.1.5	1.1.1.5
1.1.1.6	1.1.1.6
1.1.1.7	1.1.1.7
1.1.1.8	1.1.1.8
1.1.1.9	1.1.1.9
1.1.1.10	1.1.1.10
1.1.1.11	1.1.1.11
1.1.1.12	1.1.1.12
1.1.1.13	1.1.1.13
1.1.1.14	1.1.1.14
1.1.1.15	1.1.1.15
1.1.1.16	1.1.1.16
1.1.1.17	1.1.1.17
1.1.1.18	1.1.1.18
1.1.1.19	1.1.1.19
1.1.1.20	1.1.1.20
1.1.1.21	1.1.1.21
1.1.1.22	1.1.1.22
1.1.1.23	1.1.1.23
1.1.1.24	1.1.1.24
1.1.1.25	1.1.1.25
1.1.1.26	1.1.1.26
1.1.1.27	1.1.1.27
1.1.1.28	1.1.1.28
1.1.1.29	1.1.1.29
1.1.1.30	1.1.1.30
1.1.1.31	1.1.1.31
1.1.1.32	1.1.1.32
1.1.1.33	1.1.1.33
1.1.1.34	1.1.1.34
1.1.1.35	1.1.1.35
1.1.1.36	1.1.1.36
1.1.1.37	1.1.1.37
1.1.1.38	1.1.1.38
1.1.1.39	1.1.1.39
1.1.1.40	1.1.1.40
1.1.1.41	1.1.1.41
1.1.1.42	1.1.1.42
1.1.1.43	1.1.1.43
1.1.1.44	1.1.1.44
1.1.1.45	1.1.1.45
1.1.1.46	1.1.1.46
1.1.1.47	1.1.1.47
1.1.1.48	1.1.1.48
1.1.1.49	1.1.1.49
1.1.1.50	1.1.1.50
1.1.1.51	1.1.1.51
1.1.1.52	1.1.1.52
1.1.1.53	1.1.1.53
1.1.1.54	1.1.1.54
1.1.1.55	1.1.1.55
1.1.1.56	1.1.1.56
1.1.1.57	1.1.1.57
1.1.1.58	1.1.1.58
1.1.1.59	1.1.1.59
1.1.1.60	1.1.1.60

1.1.1.1	1.1.1.1	1.1.1.1	1.1.1.1
1.1.1.2	1.1.1.2	1.1.1.2	1.1.1.2
1.1.1.3	1.1.1.3	1.1.1.3	1.1.1.3
1.1.1.4	1.1.1.4	1.1.1.4	1.1.1.4
1.1.1.5	1.1.1.5	1.1.1.5	1.1.1.5
1.1.1.6	1.1.1.6	1.1.1.6	1.1.1.6
1.1.1.7	1.1.1.7	1.1.1.7	1.1.1.7
1.1.1.8	1.1.1.8	1.1.1.8	1.1.1.8
1.1.1.9	1.1.1.9	1.1.1.9	1.1.1.9
1.1.1.10	1.1.1.10	1.1.1.10	1.1.1.10
1.1.1.11	1.1.1.11	1.1.1.11	1.1.1.11
1.1.1.12	1.1.1.12	1.1.1.12	1.1.1.12
1.1.1.13	1.1.1.13	1.1.1.13	1.1.1.13
1.1.1.14	1.1.1.14	1.1.1.14	1.1.1.14
1.1.1.15	1.1.1.15	1.1.1.15	1.1.1.15
1.1.1.16	1.1.1.16	1.1.1.16	1.1.1.16
1.1.1.17	1.1.1.17	1.1.1.17	1.1.1.17
1.1.1.18	1.1.1.18	1.1.1.18	1.1.1.18
1.1.1.19	1.1.1.19	1.1.1.19	1.1.1.19
1.1.1.20	1.1.1.20	1.1.1.20	1.1.1.20
1.1.1.21	1.1.1.21	1.1.1.21	1.1.1.21
1.1.1.22	1.1.1.22	1.1.1.22	1.1.1.22
1.1.1.23	1.1.1.23	1.1.1.23	1.1.1.23
1.1.1.24	1.1.1.24	1.1.1.24	1.1.1.24
1.1.1.25	1.1.1.25	1.1.1.25	1.1.1.25
1.1.1.26	1.1.1.26	1.1.1.26	1.1.1.26
1.1.1.27	1.1.1.27	1.1.1.27	1.1.1.27
1.1.1.28	1.1.1.28	1.1.1.28	1.1.1.28
1.1.1.29	1.1.1.29	1.1.1.29	1.1.1.29
1.1.1.30	1.1.1.30	1.1.1.30	1.1.1.30
1.1.1.31	1.1.1.31	1.1.1.31	1.1.1.31
1.1.1.32	1.1.1.32	1.1.1.32	1.1.1.32
1.1.1.33	1.1.1.33	1.1.1.33	1.1.1.33
1.1.1.34	1.1.1.34	1.1.1.34	1.1.1.34
1.1.1.35	1.1.1.35	1.1.1.35	1.1.1.35
1.1.1.36	1.1.1.36	1.1.1.36	1.1.1.36
1.1.1.37	1.1.1.37	1.1.1.37	1.1.1.37
1.1.1.38	1.1.1.38	1.1.1.38	1.1.1.38
1.1.1.39	1.1.1.39	1.1.1.39	1.1.1.39
1.1.1.40	1.1.1.40	1.1.1.40	1.1.1.40
1.1.1.41	1.1.1.41	1.1.1.41	1.1.1.41
1.1.1.42	1.1.1.42	1.1.1.42	1.1.1.42
1.1.1.43	1.1.1.43	1.1.1.43	1.1.1.43
1.1.1.44	1.1.1.44	1.1.1.44	1.1.1.44
1.1.1.45	1.1.1.45	1.1.1.45	1.1.1.45
1.1.1.46	1.1.1.46	1.1.1.46	1.1.1.46
1.1.1.47	1.1.1.47	1.1.1.47	1.1.1.47
1.1.1.48	1.1.1.48	1.1.1.48	1.1.1.48
1.1.1.49	1.1.1.49	1.1.1.49	1.1.1.49
1.1.1.50	1.1.1.50	1.1.1.50	1.1.1.50



JICA Study Team
Study on the Port Security Enhancement Program
to Strengthen Public Ports in the Republic of Indonesia

WORKSHOP

Issues on Implementation of Port Facility Security Measures in

Port of Makassar

Indonesian Port Corporation IV






PT (Persero) PELABUHAN INDONESIA IV
CABANG Makassar

1

JICA Study Team
Study on the Port Security Enhancement Program
to Strengthen Public Ports in the Republic of Indonesia

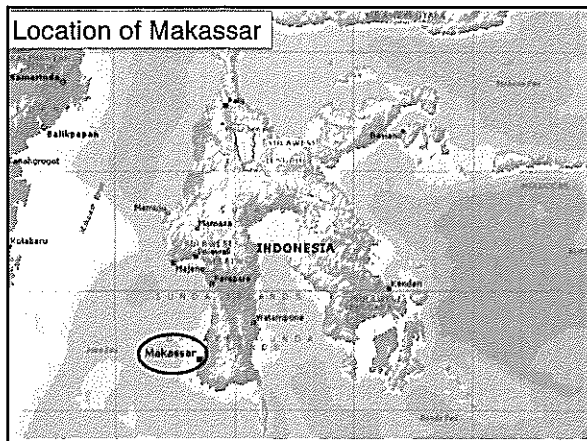
Acknowledgement

- We, the study team would like to thank the Port Administrator, GM, PSO, PFSO and staff of PELINDO IV is assisting in our observation and study in the implementation of ISPS Code in your Port Facility.
- We apologize in the areas of ignorance and/or misunderstanding with regards to your operations and procedures.

PT (Persero) PELABUHAN INDONESIA IV
CABANG Makassar

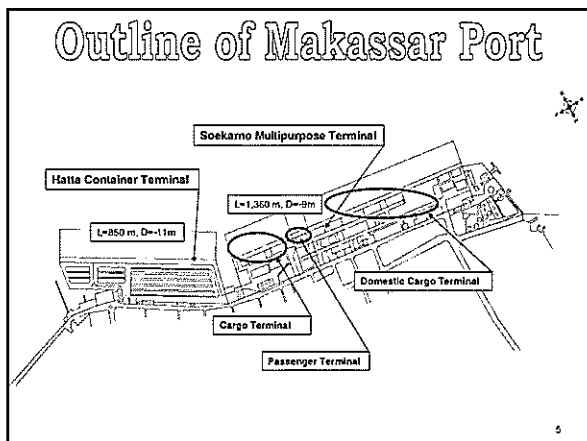
2



Scope

- Outline of Makassar Port
- Gates of Makassar Port
- Soekarno Multipurpose Terminal
- Hatta Container Terminal
- Cargo Terminal
- Passenger Terminal
- Conclusion

4



Outline of Makassar Port

Ship Calls

	1999	2000	2001	2002	2003	2004
Ocean going	297	355	407	367	309	289
Domestic	2,695	2,867	3,004	3,421	3,379	3,518
Traditional Ships	1,860	1,976	1,925	1,982	1,701	1,184
Total	4,852	5,198	5,336	5,770	5,389	4,991

Cargo Flow

Unit: ton

	1999	2000	2001	2002	2003	2004
Domestic unloading	2,955,554	3,200,552	3,073,474	3,665,427	4,016,075	4,303,801
Domestic loading	1,106,932	1,600,108	1,704,505	2,107,810	2,487,163	2,711,308
Import	488,691	628,688	451,746	620,797	637,017	708,689
Export	669,431	923,687	1,510,363	1,028,516	1,138,219	1,241,077
Total	5,220,598	6,353,035	6,740,088	7,442,772	8,278,474	8,964,875

Outline of Makassar Port

Container Flow

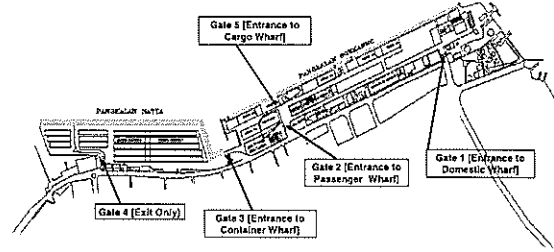
Unit: TEU

	1999	2000	2001	2002	2003	2004
Export	8,792	10,682	10,167	7,671	8,604	9,783
Import	178	41	1,035	2,318	1,536	1,957
Domestic	119,917	154,228	166,214	197,496	222,014	238,104
Total	128,887	164,951	177,416	207,485	232,154	249,844

Passenger Flow

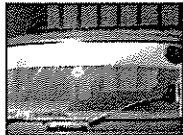
	1999	2000	2001	2002	2003	2004
Embarkation	779,726	721,655	676,171	613,897	478,537	420,008
Debarcation	556,890	535,098	507,033	516,612	386,990	329,487
Total	1,336,616	1,257,923	1,183,204	1,190,509	865,527	749,495

Gates of Makassar Port



Soekarno Multipurpose Terminal

Access point to Port via GATE 1



Vehicle Pass for entry to Port



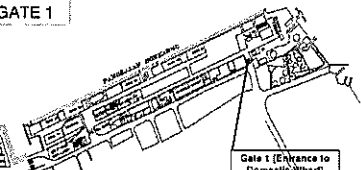
Purchase of Coupon for access



Pedestrian Access



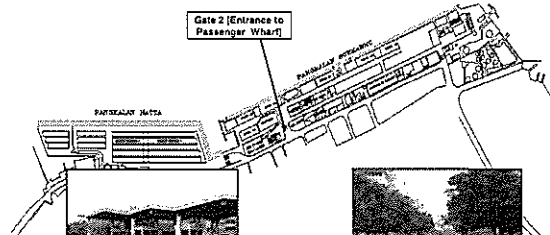
Access by Truck, Vehicles and Motorcycle



Gate 1 (Entrance to Domestic Wharf)

Soekarno Multipurpose Terminal

Gate 2 (Entrance to Passenger Wharf)

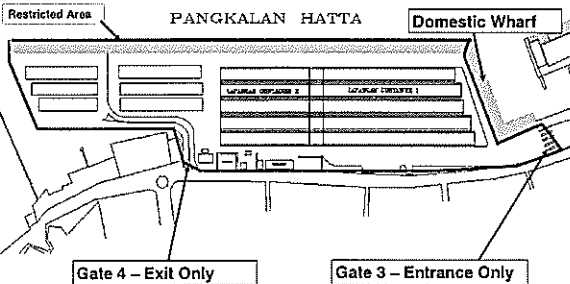


Inside view of Gate 2



From Gate 2 leading to Passenger and PELINDO IV Office

Hatta Container Terminal



Hatta Container Terminal

KPPP police random patrol in port facility

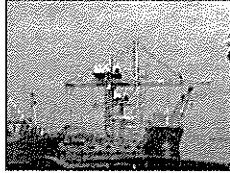
Security post at end of wharf

Perimeter fencing in container wharf

Purchase of ticket for entry into port

Hatta Container Terminal

- The whole area within the container wharf has been classified as restricted area
- Access control measure are applied to container wharf
- Authorized truck will display disc on front of windscreen
- Daily temporary truck drivers do not have authorized disc displayed prominently.
They will purchase tickets before entrance
- Security personnel will record all trucks entering into the wharf

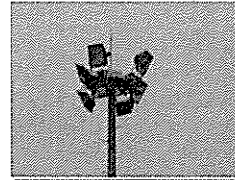


View from Cargo Wharf to Container Terminal

13

Hatta Container Terminal

- Good security lightings in wharf area. During operations, security personnel will station at area



Lightings

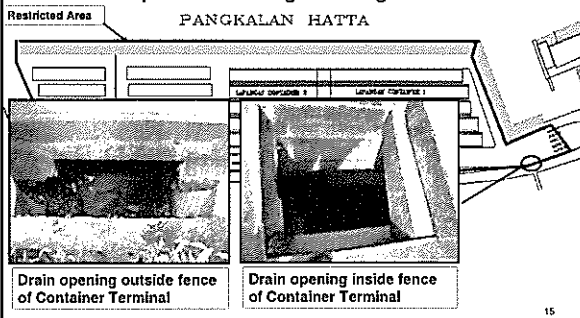


Lightings In Container Yard

14

Hatta Container Terminal

- Drain opening should be covered as access via outside is possible through underground drain



Drain opening outside fence of Container Terminal

Drain opening inside fence of Container Terminal

15

Hatta Container Terminal

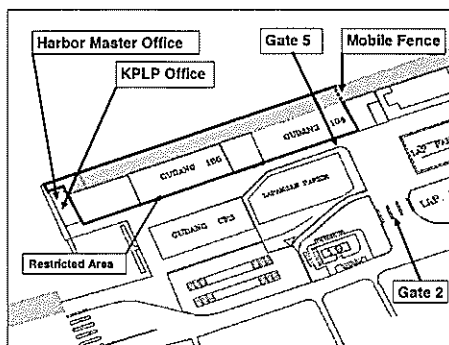
- It is easy to climb over the fence because of rough mesh of fence and lack of top guard.



Fence structure of Container Terminal

16

Cargo Terminal

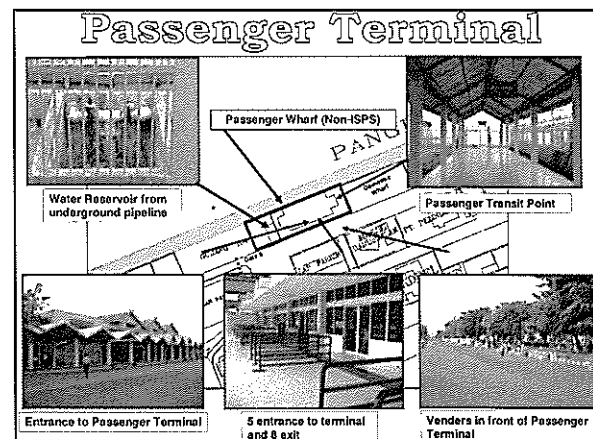
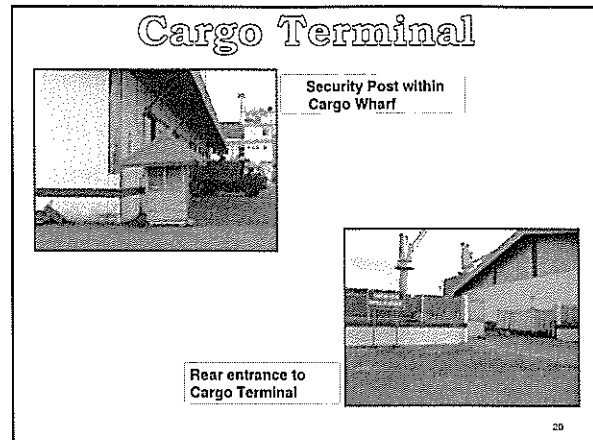
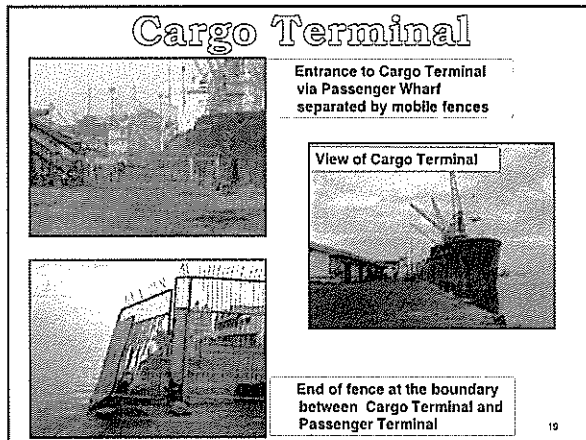


17

Cargo Terminal

- Soekarno Cargo Terminal is used by Cargo Vessels, Bag and Bulk Cargo
- The berthing area is close to the domestic passenger terminal
- It is separated by a mobile fence that is placed when passenger ships call

18



Passenger Terminal

- The passenger wharf is Makassar Port is mainly for domestic use only. An average of 50 calls per month is made to the wharf.
- Entrance to the passenger wharf is via Gate 2.
- Mode of transportation is by taxi, public bus and by foot.
- During arrival and departure of passenger vessels, hawkers are allowed to display and sell their products. If there are no passenger vessels, they are not allowed into the port area.
- There is no security equipment in the passenger wharf. Checks are done manually by custom officials.
- Each passenger is allowed 30 kg of luggage weigh. Any access, an additional charge.
- Custom official conducts random checks on passenger and baggage.

23

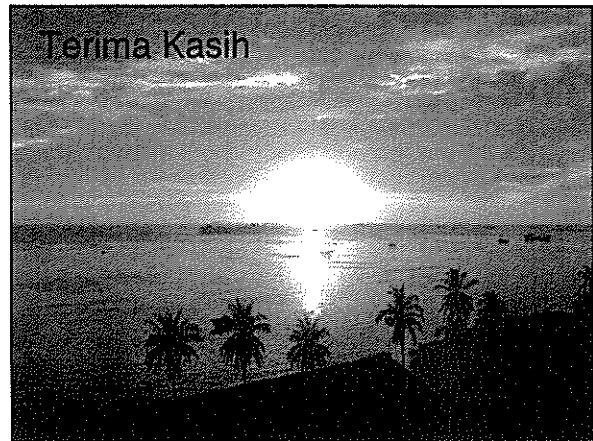
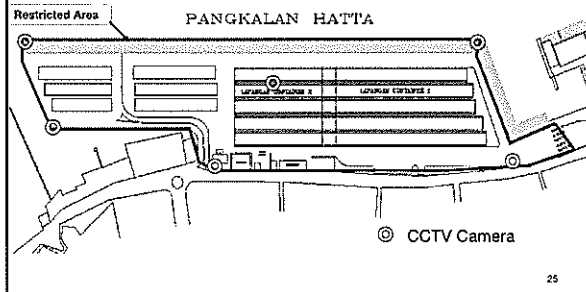
Conclusion

- Port of Makassar has a security procedure and plan in place.
- The container and the cargo wharf are ISPS compliant. However, it is recommended that the PFSO request for the Declaration of Security (DoS) with non-ISPS compliant vessels calling at the container wharf. This is to prevent any contamination with ISPS compliant ships calling at this wharf.
- The drainage at the container wharf should be covered to prevent unauthorized personnel from entering the port.
- It also observed that there are many people walking in the port area without being checked. These are people looking for odd jobs on a daily basis. PFSO should enforce security measures to these people who are entering the port facilities.
- They should be given visitor pass in exchange for their identification.

24

Conclusion

- It is preferable to install the CCTV camera monitoring system in the Container Terminal to secure the terminal security.



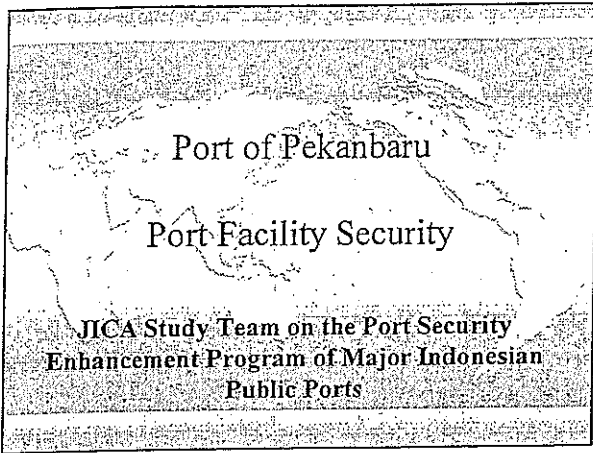
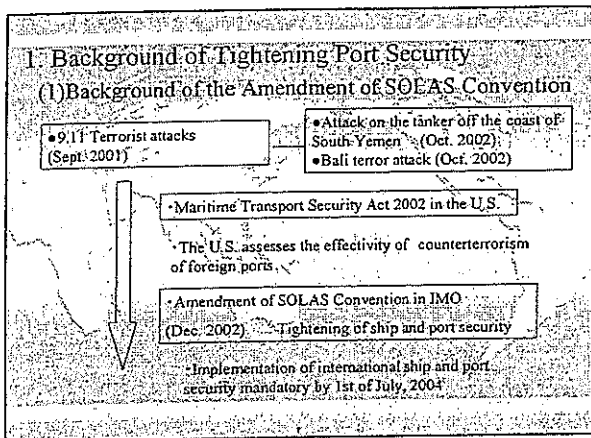


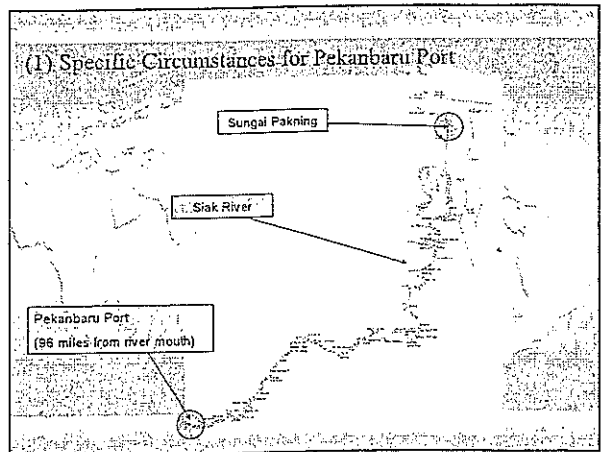
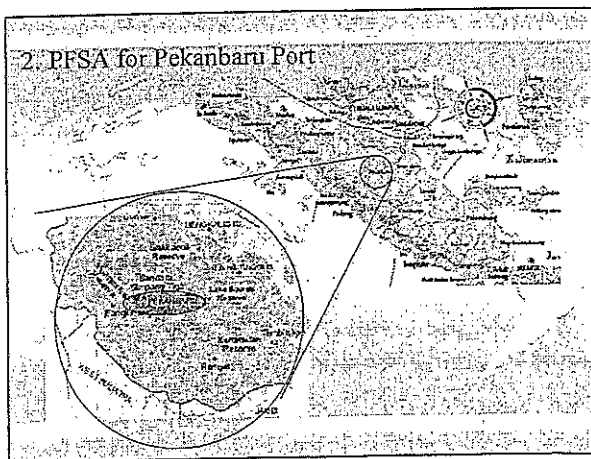
Table of Contents

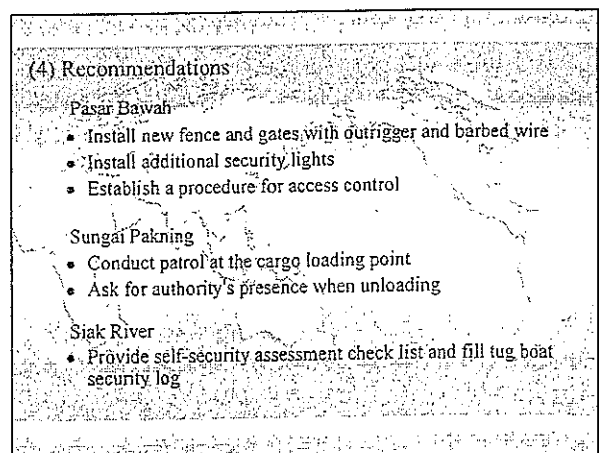
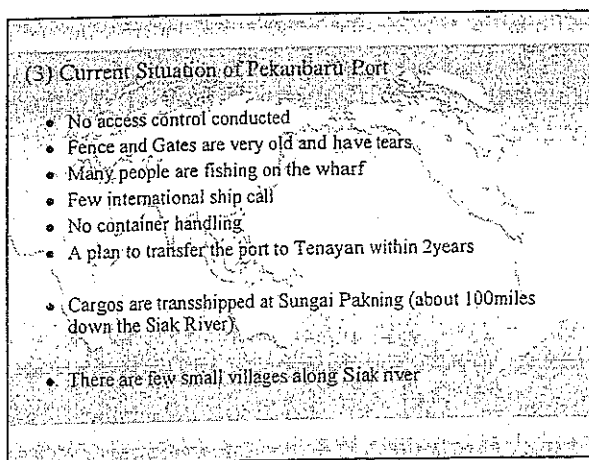
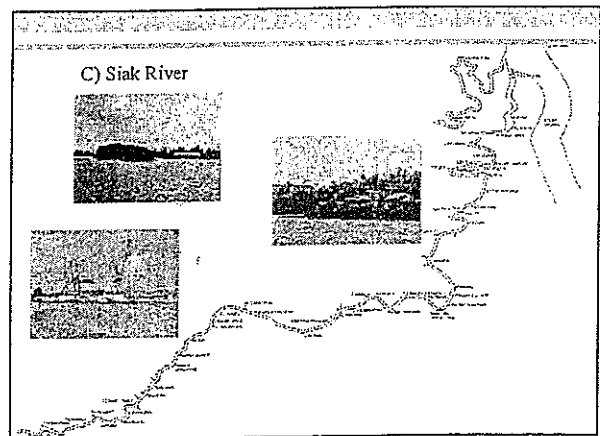
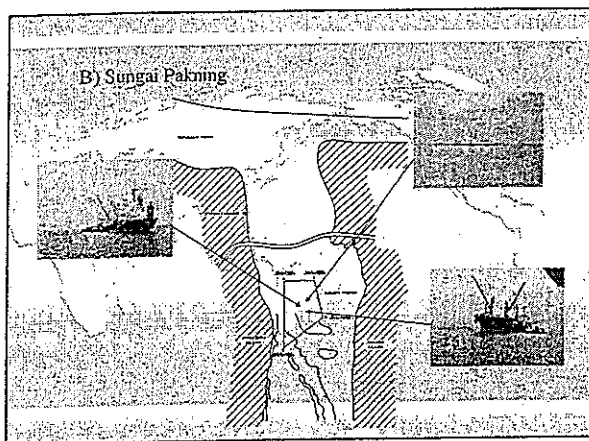
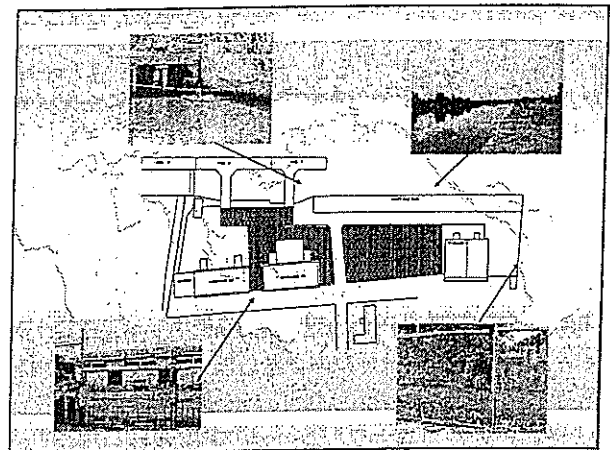
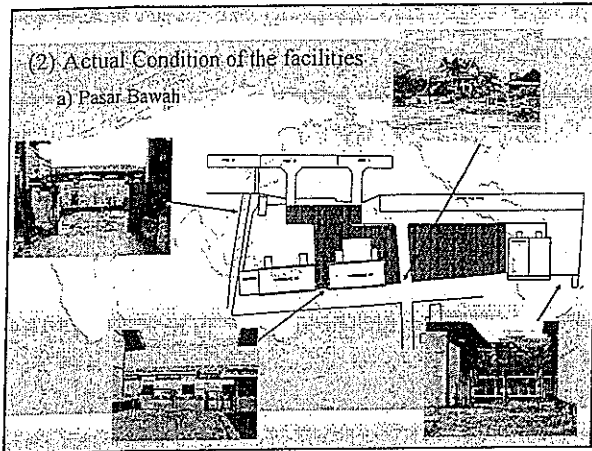
1. Background of Tightening Port Security
2. PFSP for Pekanbaru Port
3. Access Control to be Conducted at Gates
4. Maintenance Work
5. Procedure of Emergency Management Plan
6. Evacuation Route
7. Emergency Contact List
8. Contrast Chart for ISPS Code and PFSP

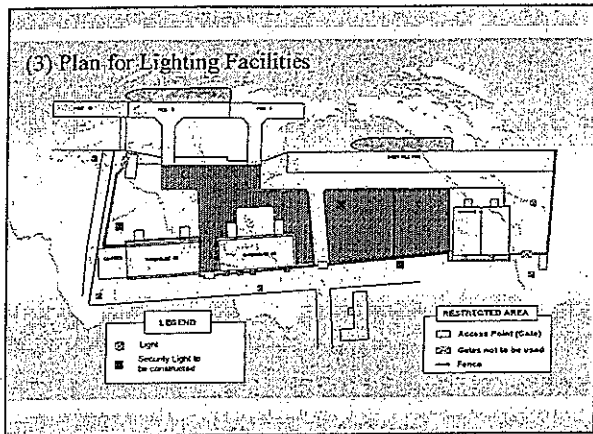
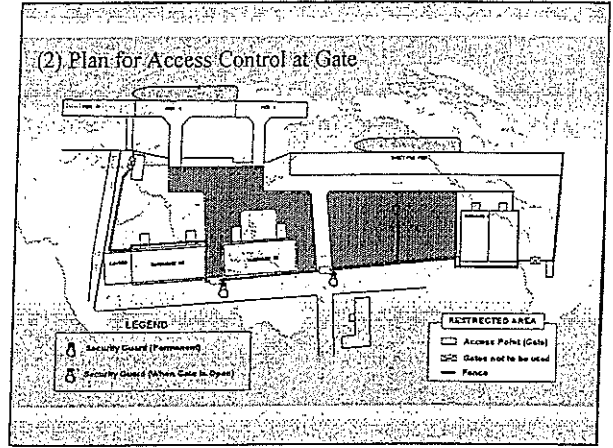
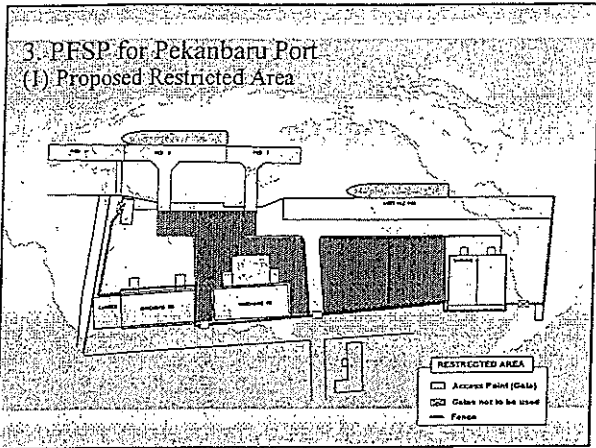


(2) What is SOLAS Convention?
 > Formally each shipping nation had its own maritime laws. However in response to the Titanic disaster, which resulted in death of 1,500 passengers and crew out of over 2,000, treaty for international maritime safety was concluded in 1914

(3) Outline of Amendment of SOLAS Convention
 > To improve the reliability of international sea transportation system by having the ship owners, the port operator and port administrator take security measures
 > To prevent an unlawful act related to international sea transportation by not admitting a ship identified to be a threat to enter the port







(4) Access Control to be Conducted at Gates

a) Access Control for Customs and ISPS Code

- Different Purpose
 - Customs
 - Avoid smuggling
 - Avoid goods taking out illegally
 - EXIT CONTROL
 - ISPS
 - Avoid Suspicious Person/Goods inside the Restricted Area
 - Protect from Terrorism
- ENTRY CONTROL

b) Category of Entrance

- Port User (by foot or otherwise)
- Container Truck
- Construction/Maintenance Vehicle
- Ships Stores/Equipment
- Ships Crew
- Taxi
- Emergency Service Vehicle

Port User (by foot or otherwise)

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PFO	Level 3 Conducted by PSO
Foot or Vehicle Entry	<ul style="list-style-type: none"> • Request to stop • Ask for ID card all those wishing to enter 	<ul style="list-style-type: none"> • Same as on the left • Check ID photo and the face for 10 out of every 100 	<ul style="list-style-type: none"> • Do not admit entrance
Baggage	<ul style="list-style-type: none"> • Check appearance of baggage 	<ul style="list-style-type: none"> • Confirm contents of baggage for 10 out of 100 	

Container Truck			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PFO	Level 3 Conducted by PSO
Vehicle	-Request to stop -Confirm documents	-Same as on the left	-Do not admit entrance
Driver	-Ask for ID card for 10 out of every 100	-Ask all drivers for ID card	
Helper	-Admit entrance on guarantee of driver	-Same as on the left	
Full Container	-Check documents and appearance	-Same as on the left	
Empty Container	-Check documents and confirm inside	-Same as on the left	

Cargo Truck			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PFO	Level 3 Conducted by PSO
Vehicle	-Request to stop -Confirm documents	-Same as on the left	-Do not admit entrance
Driver	-Ask for ID card for 10 out of every 100	-Ask all drivers for ID card	
Helper	-Admit entrance on guarantee of driver	-Same as on the left	
Freight	-Check Documents & appearance of cargo	-Inspect and confirm cargo against documents	

Construction/Maintenance Vehicle			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PFO	Level 3 Conducted by PSO
Vehicle	-Request to stop -Confirm approval with PFSO	-Same as on the left	-Do not admit entrance
Driver	-Ask all drivers for ID card	-Ask all drivers for ID card -Check ID photo and the face for 10 out of every 100 -Request to fill in form and issue temporary pass when there is no ID card.	
Passenger/Workmen	-Admit entrance on guarantee of driver/foreman	-Same as above	
Cargo	-Check appearance	-Inspect contents	

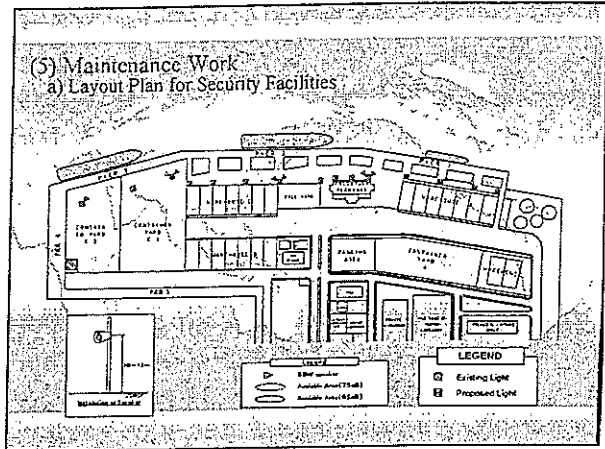
Ship's Stores/Equipment			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PFO	Level 3 Conducted by PSO
Vehicle	-Request to stop -Check documents	-Request to stop -Confirm documents	-Do not admit entrance
Driver & Passenger	-Ask all drivers/Passengers for ID card -Check ID photo and face for 50 out of every 100	-Ask all drivers/Passengers for ID card -Check ID photo and the face for all those wishing to enter	
Cargo	-Not necessary to check when under escort -Confirm customs report or work order when there is no escort	-Confirm contents of cargo for 50 out of every 100	

Ships Crew's Exit and Return Entry			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PFO	Level 3 Conducted by PSO
Ships Crew exit	-Confirm shore pass or ID issued by the ship	-Same as on the left	-Do not admit entrance
Ships Crew entry on board	-Same as above -Confirm an embarkation order, seaman's book or passport or confirm with the ship	-Same as on the left	
Baggage	-Check appearance of baggage	-Confirm contents of baggage for 10 out of 100	

Taxi			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PFO	Level 3 Conducted by PSO
Vehicle	-Request to stop	-Request to stop -Inspect trunk	-Do not admit entrance
Driver	-Ask all drivers for ID card	-Ask all drivers for ID card -Check ID photo and the face for 10 out of every 100	
Passenger	-Same as above	-Same as above -Ask destination	
Baggage	-Check appearance of baggage	-Confirm contents of baggage for 10 out of 100	

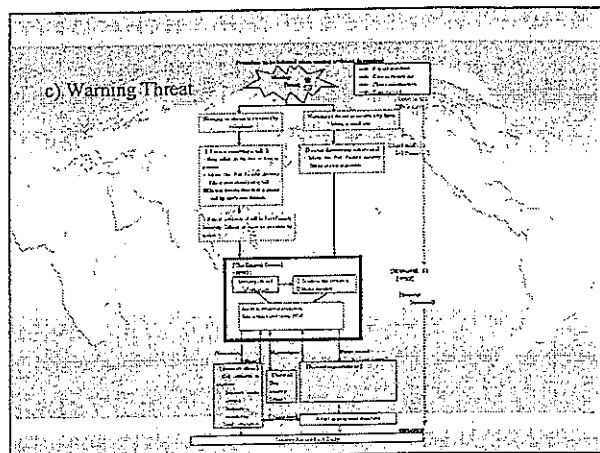
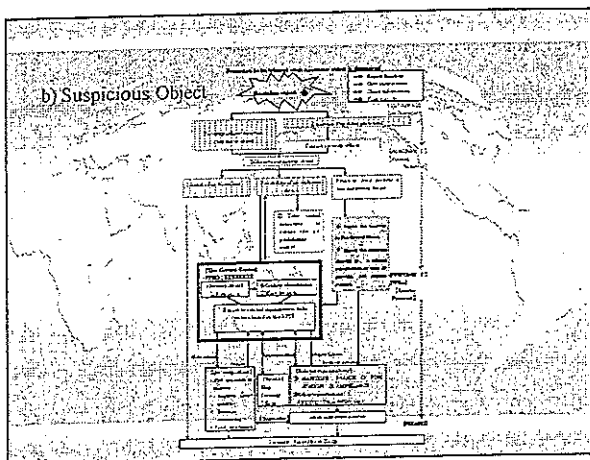
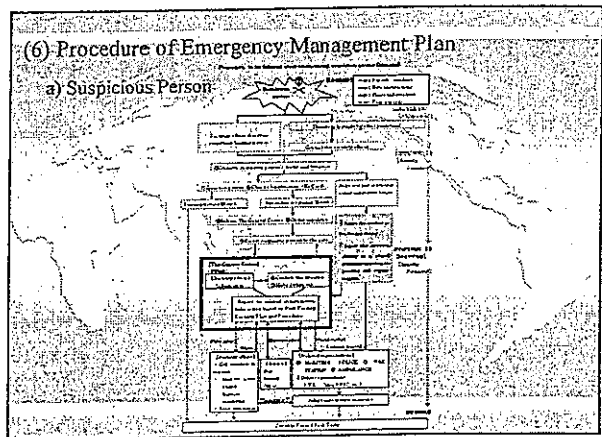
Emergency Service Vehicle

Security level	Security level 1, 2 and 3 (Emergency Service personnel not required to have ID)
Vehicle	• Confirm the type of vehicle • Record time of entry into record book
Driver	• Confirm by the type of vehicle
Vehicle Crew	Same as above



b) Inspection Procedure

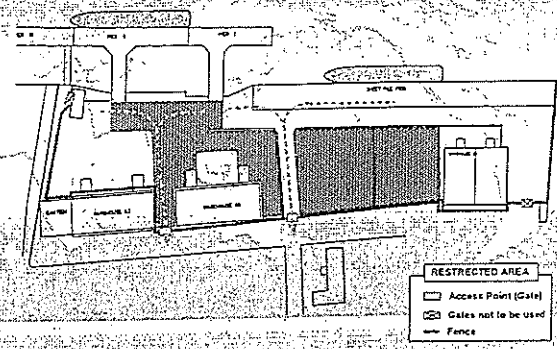
Description	Items to be Checked	Daily Inspection	Periodical Inspection
Security Light	Road Light	• Ensure that all security lights are illuminated by visual inspection during patrol	• Conduct annually • Check mounting of lamp fitting • Clean the cover check cables and switch box
Communication System	VHF Radio Telephone Fax	• Check in daily usage	• Conduct annually by the supplier • Cleaning, adjustment, and change consumables



(7) Evacuation Procedure

- Evacuate following the instruction of PFSO
- Direct the gate No. when evacuating from the restricted area
- Direct the name of facility when evacuating to the building
- PFSO may direct, navigate and confirm that no one fail to escape

Evacuation Route



(8) Emergency Contact List

Security Officer

Organization/Title	Tel.	Name	Remarks
PFSO			
Deputy PFSO			

Port of Pekanbaru

Organization/Title	Tel.	Name	Remarks
ADPEL			
KPLP/PSO			
KPPP			
FORT HEALTH			
Fire Department			

(9) Contrast Chart for ISPS Code and PFSP

ISPS Code	PFSP
1.1.1.1.1.1	1.1.1.1.1.1
1.1.1.1.1.2	1.1.1.1.1.2
1.1.1.1.1.3	1.1.1.1.1.3
1.1.1.1.1.4	1.1.1.1.1.4
1.1.1.1.1.5	1.1.1.1.1.5
1.1.1.1.1.6	1.1.1.1.1.6
1.1.1.1.1.7	1.1.1.1.1.7
1.1.1.1.1.8	1.1.1.1.1.8
1.1.1.1.1.9	1.1.1.1.1.9
1.1.1.1.1.10	1.1.1.1.1.10
1.1.1.1.1.11	1.1.1.1.1.11
1.1.1.1.1.12	1.1.1.1.1.12
1.1.1.1.1.13	1.1.1.1.1.13
1.1.1.1.1.14	1.1.1.1.1.14
1.1.1.1.1.15	1.1.1.1.1.15
1.1.1.1.1.16	1.1.1.1.1.16
1.1.1.1.1.17	1.1.1.1.1.17
1.1.1.1.1.18	1.1.1.1.1.18
1.1.1.1.1.19	1.1.1.1.1.19
1.1.1.1.1.20	1.1.1.1.1.20
1.1.1.1.1.21	1.1.1.1.1.21
1.1.1.1.1.22	1.1.1.1.1.22
1.1.1.1.1.23	1.1.1.1.1.23
1.1.1.1.1.24	1.1.1.1.1.24
1.1.1.1.1.25	1.1.1.1.1.25
1.1.1.1.1.26	1.1.1.1.1.26
1.1.1.1.1.27	1.1.1.1.1.27
1.1.1.1.1.28	1.1.1.1.1.28
1.1.1.1.1.29	1.1.1.1.1.29
1.1.1.1.1.30	1.1.1.1.1.30
1.1.1.1.1.31	1.1.1.1.1.31
1.1.1.1.1.32	1.1.1.1.1.32
1.1.1.1.1.33	1.1.1.1.1.33
1.1.1.1.1.34	1.1.1.1.1.34
1.1.1.1.1.35	1.1.1.1.1.35
1.1.1.1.1.36	1.1.1.1.1.36
1.1.1.1.1.37	1.1.1.1.1.37
1.1.1.1.1.38	1.1.1.1.1.38
1.1.1.1.1.39	1.1.1.1.1.39
1.1.1.1.1.40	1.1.1.1.1.40
1.1.1.1.1.41	1.1.1.1.1.41
1.1.1.1.1.42	1.1.1.1.1.42
1.1.1.1.1.43	1.1.1.1.1.43
1.1.1.1.1.44	1.1.1.1.1.44
1.1.1.1.1.45	1.1.1.1.1.45
1.1.1.1.1.46	1.1.1.1.1.46
1.1.1.1.1.47	1.1.1.1.1.47
1.1.1.1.1.48	1.1.1.1.1.48
1.1.1.1.1.49	1.1.1.1.1.49
1.1.1.1.1.50	1.1.1.1.1.50

ISPS Code	PFSP
1.1.1.1.1.51	1.1.1.1.1.51
1.1.1.1.1.52	1.1.1.1.1.52
1.1.1.1.1.53	1.1.1.1.1.53
1.1.1.1.1.54	1.1.1.1.1.54
1.1.1.1.1.55	1.1.1.1.1.55
1.1.1.1.1.56	1.1.1.1.1.56
1.1.1.1.1.57	1.1.1.1.1.57
1.1.1.1.1.58	1.1.1.1.1.58
1.1.1.1.1.59	1.1.1.1.1.59
1.1.1.1.1.60	1.1.1.1.1.60
1.1.1.1.1.61	1.1.1.1.1.61
1.1.1.1.1.62	1.1.1.1.1.62
1.1.1.1.1.63	1.1.1.1.1.63
1.1.1.1.1.64	1.1.1.1.1.64
1.1.1.1.1.65	1.1.1.1.1.65
1.1.1.1.1.66	1.1.1.1.1.66
1.1.1.1.1.67	1.1.1.1.1.67
1.1.1.1.1.68	1.1.1.1.1.68
1.1.1.1.1.69	1.1.1.1.1.69
1.1.1.1.1.70	1.1.1.1.1.70
1.1.1.1.1.71	1.1.1.1.1.71
1.1.1.1.1.72	1.1.1.1.1.72
1.1.1.1.1.73	1.1.1.1.1.73
1.1.1.1.1.74	1.1.1.1.1.74
1.1.1.1.1.75	1.1.1.1.1.75
1.1.1.1.1.76	1.1.1.1.1.76
1.1.1.1.1.77	1.1.1.1.1.77
1.1.1.1.1.78	1.1.1.1.1.78
1.1.1.1.1.79	1.1.1.1.1.79
1.1.1.1.1.80	1.1.1.1.1.80
1.1.1.1.1.81	1.1.1.1.1.81
1.1.1.1.1.82	1.1.1.1.1.82
1.1.1.1.1.83	1.1.1.1.1.83
1.1.1.1.1.84	1.1.1.1.1.84
1.1.1.1.1.85	1.1.1.1.1.85
1.1.1.1.1.86	1.1.1.1.1.86
1.1.1.1.1.87	1.1.1.1.1.87
1.1.1.1.1.88	1.1.1.1.1.88
1.1.1.1.1.89	1.1.1.1.1.89
1.1.1.1.1.90	1.1.1.1.1.90
1.1.1.1.1.91	1.1.1.1.1.91
1.1.1.1.1.92	1.1.1.1.1.92
1.1.1.1.1.93	1.1.1.1.1.93
1.1.1.1.1.94	1.1.1.1.1.94
1.1.1.1.1.95	1.1.1.1.1.95
1.1.1.1.1.96	1.1.1.1.1.96
1.1.1.1.1.97	1.1.1.1.1.97
1.1.1.1.1.98	1.1.1.1.1.98
1.1.1.1.1.99	1.1.1.1.1.99
1.1.1.1.1.100	1.1.1.1.1.100

JICA Study Team
 for the Study on the Port Security Enhancement Program
 of Major Indonesian Public Ports in the Republic of Indonesia

WORKSHOP

Issues on Implementation of Port Facility Security Measures in

Port of Belawan

Indonesian Port Corporation I

**PT (Persero) PELABUHAN INDONESIA I
CABANG BELAWAN**

1

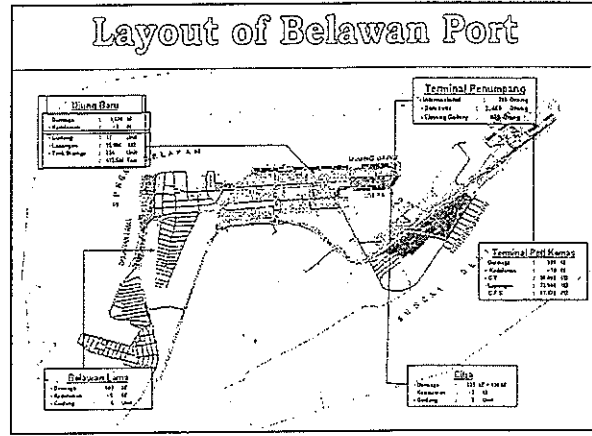
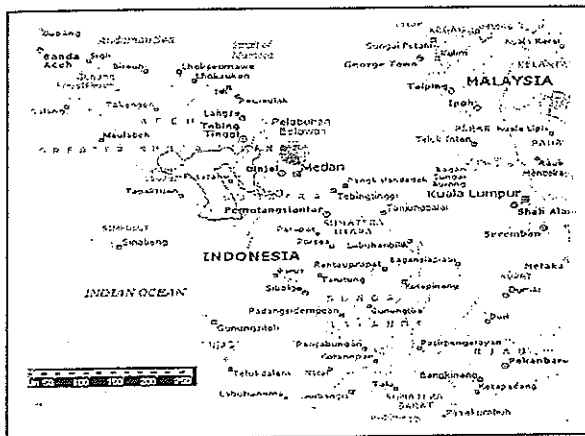
JICA Study Team
 for the Study on the Port Security Enhancement Program
 of Major Indonesian Public Ports in the Republic of Indonesia

Acknowledgement

- We, the study team would like to thank the Port Administrator, GM, PSO, PFSO and staff of PELINDO I is assisting in our observation and study in the implementation of ISPS Code in your Port Facility.
- We apologize in the areas of ignorance and/or misunderstanding with regards to your operations and procedures.

**PT (Persero) PELABUHAN INDONESIA I
CABANG BELAWAN**

2

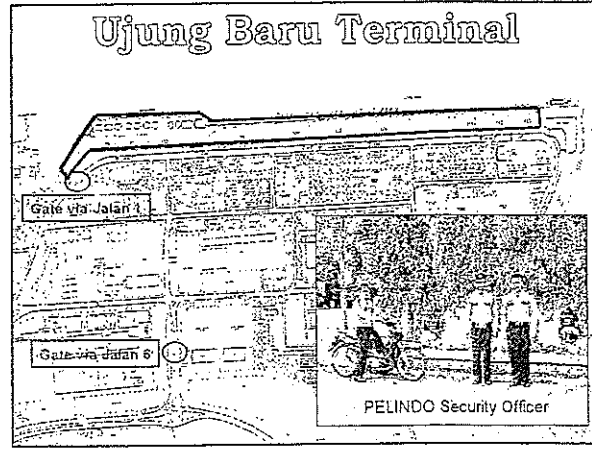


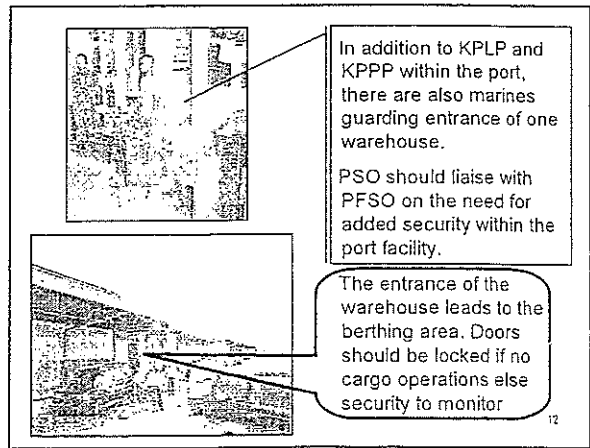
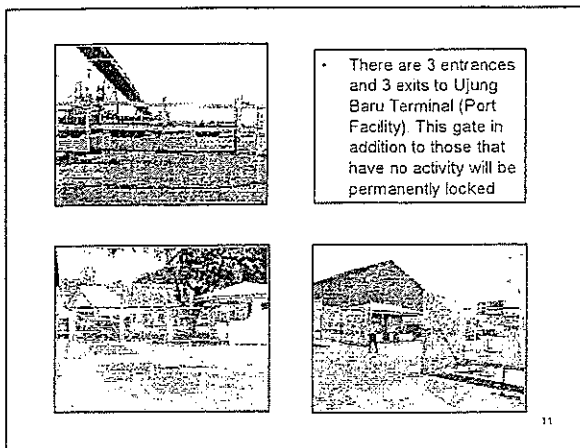
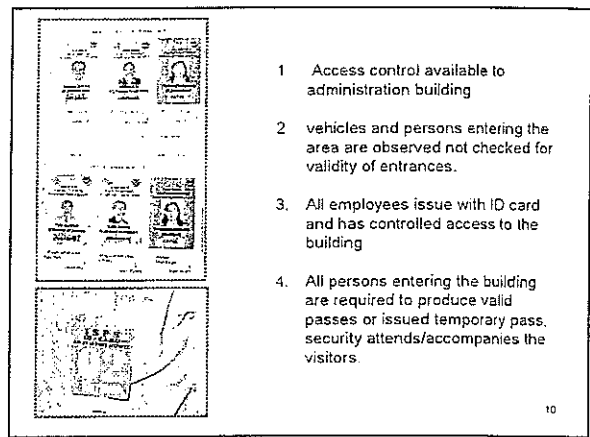
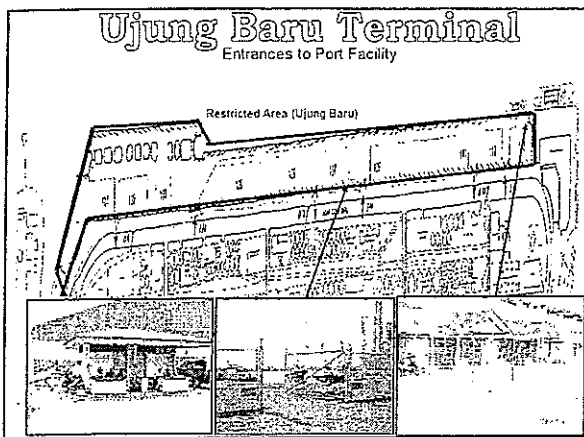
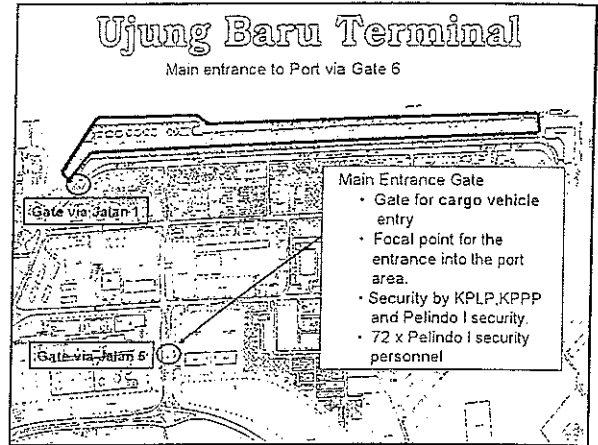
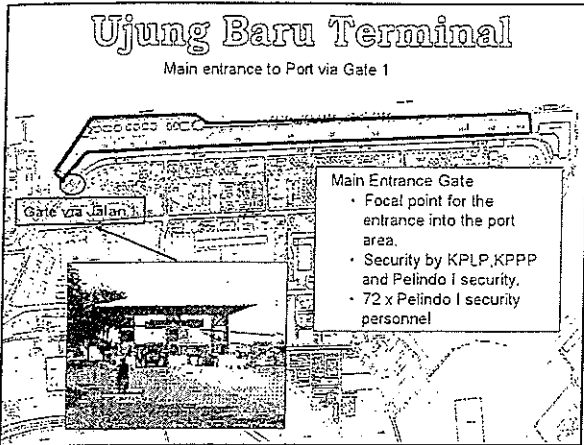
JICA Study Team
 for the Study on the Port Security Enhancement Program
 of Major Indonesian Public Ports in the Republic of Indonesia

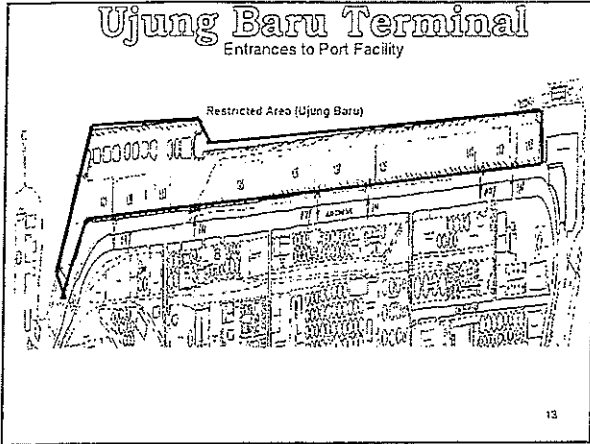
Scope

1. Port Facility Security Duties
2. Access Control
3. Monitoring of Port Facility, including anchoring and berthing area(s)
4. Monitoring of Restricted Areas
5. Supervising the Handling of Cargo
6. Supervising the Handling of Ship's Store
7. Ensuring Security Communication is readily available
8. Training, Drills and Exercises
9. Conclusion

5







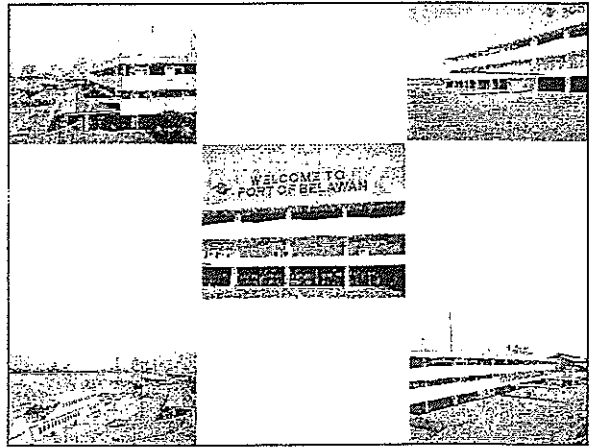
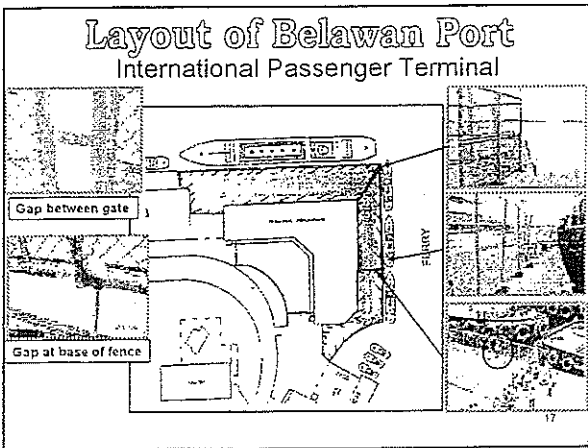
Assets & Infrastructure to be protected Ujung Baru Terminal

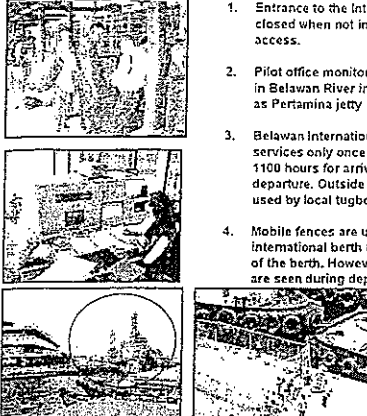
- Wharf
- Storage / Warehouse
- Administration Building
- Berthing Area

14

- Berthing area where conveyor belt is located has poor visibility in the night
- Recommend to install flood lighting
- CCTV to monitor berth and perimeter

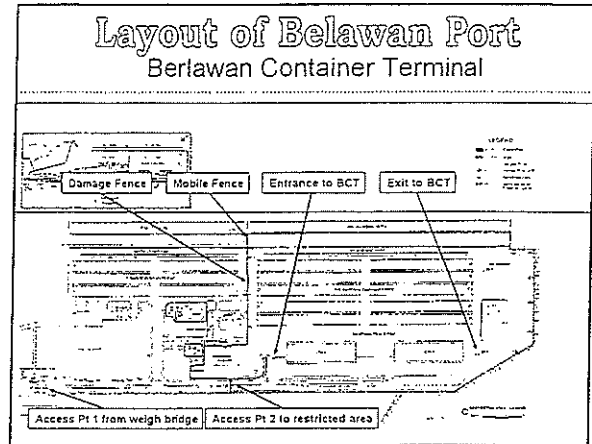
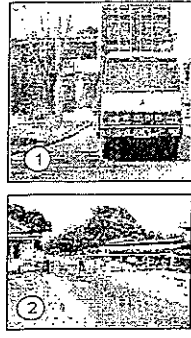
15





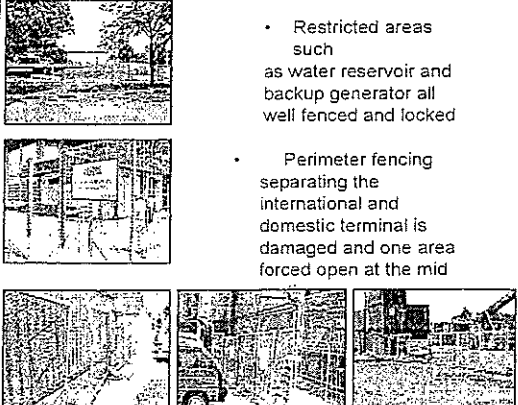
1. Entrance to the International Ferry Terminal is closed when not in use. Ticket is required for access.
2. Pilot office monitoring movement of all vessels in Belawan River including container terminal as Pertamina jetty
3. Belawan International Ferry Terminal provides services only once a day. The ferry schedule is 1100 hours for arrival and 1400 hours for departure. Outside this period, the berth is used by local tugboats as temporary berth.
4. Mobile fences are used to separate international berth from domestic at both side of the berth. However, no security personnel are seen during departure of passenger vessel.

19

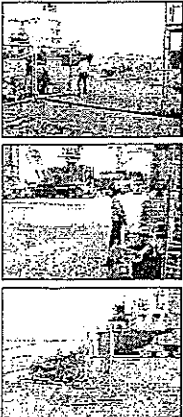
- There 2 access points to the container terminal. The first access point with Weigh Bridge allows vehicle access to domestic and international terminal.
- The 2nd access point is controlled for access only to international terminal.
- All container trucks and vehicles are inspected before access is granted.

21



- Restricted areas such as water reservoir and backup generator all well fenced and locked
- Perimeter fencing separating the international and domestic terminal is damaged and one area forced open at the mid

22



1. The international berth is 500m in length while the domestic berth is 350m.
2. A mobile fence is used to facilitate movement within the 2 area during cargo operations.
3. One of the international berths is used for domestic operations frequently due to space constraint. However, security personnel will be there at all times to ensure no unauthorized access to the international terminal.

23

WORKSHOP
Issues on Implementation
of Port Facility Security
Measures in
Port of Dumai
Indonesian Port Corporation I

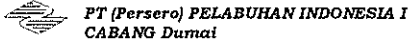
 PT (Persero) PELABUHAN INDONESIA I
 CABANG Dumai




1

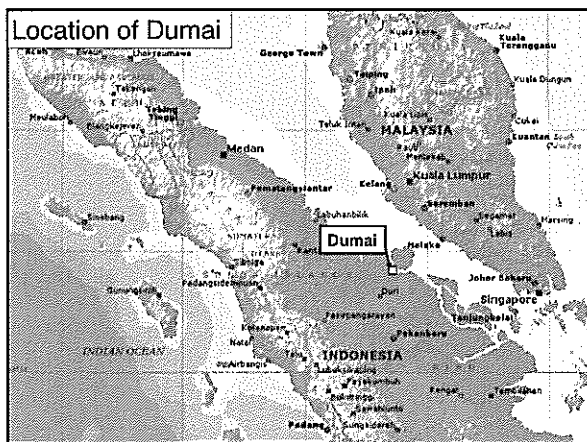
Acknowledgement

- We, the study team would like to thank the Port Administrator, GM, PSO, PFSO and staff of PELINDO I is assisting in our observation and study in the implementation of ISPS Code in your Port Facility.
- We apologize in the areas of ignorance and/or misunderstanding with regards to your operations and procedures.

 PT (Persero) PELABUHAN INDONESIA I
 CABANG Dumai



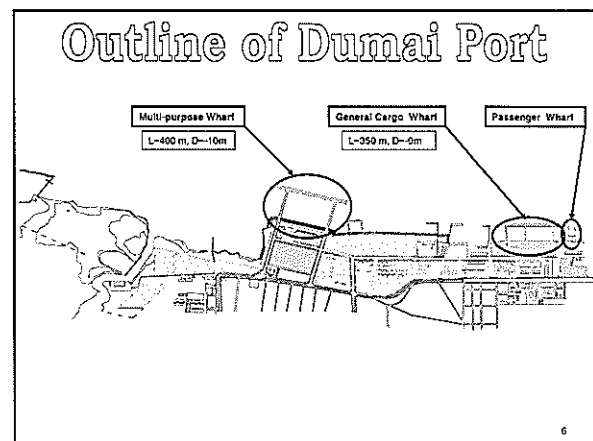
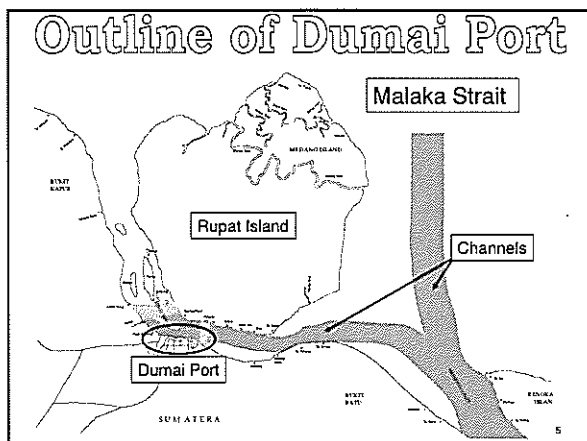
2



Scope

- Outline of Dumai Port
- Gates of Dumai Port
- Multi-purpose Wharf
- General Cargo Wharf
- Passenger Wharf
- Access Control
- Conclusion

4



Outline of Dumai Port

Ship Calls

Type of Ships	2000	2001	2002	2003	2004
Special Ships for CPO	505	457	494	538	779
Ferry	3,477	3,498	3,385	3,157	3,300
Other Ships	2,834	3,001	2,541	2,468	2,297
Total	6,816	6,956	6,420	6,163	6,376

7

Outline of Dumai Port

Cargo Volume

Unit: ton

Trade Type	2000	2001	2002	2003	2004	
Non Oil & Gas Commodity	Export	2,393,399	2,756,918	3,144,644	3,858,016	4,130,476
	Import	329,957	278,678	365,133	387,907	387,398
	Loading (Dom.)	625,936	552,578	298,920	178,883	467,722
	Unloading (Dom.)	736,891	845,061	878,893	869,800	991,003
	Sub-total	4,086,183	4,433,235	4,687,590	5,294,606	5,976,599
Oil & Gas Commodity	Export	16,868,385	17,168,144	14,916,352	13,163,728	12,500,980
	Import	0	44,038	10,939	33,795	99,339
	Loading (Dom.)	16,580,900	14,856,894	13,429,590	12,605,808	14,312,120
	Unloading (Dom.)	1,323,036	1,558,279	1,868,414	1,430,864	1,078,556
	Sub-total	34,772,321	33,627,355	30,225,295	27,234,195	27,990,995
Total	38,858,504	38,060,590	34,912,885	32,528,801	33,967,594	

8

Outline of Dumai Port

Crude Palm Oil & Its Derivative Volume

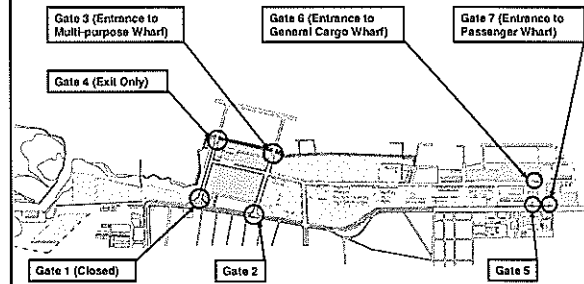
Unit: Ton

	2000	2001	2002	2003	2004
Crude Palm Oil (CPO)	1,792,878	1,706,203	1,739,679	1,817,495	3,742,066
The derivatives	1,548,390	1,940,891	2,117,001	2,584,031	1,228,480
Total	3,341,268	3,647,094	3,856,680	4,401,526	4,970,546

Passenger Flow

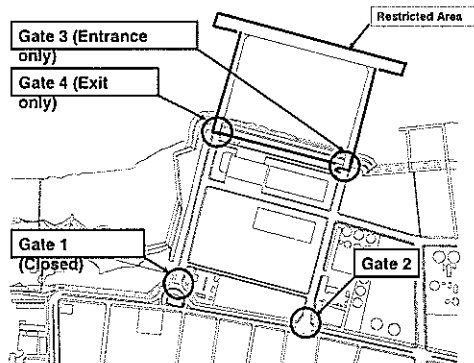
		2000	2001	2002	2003	2004
Domestic	Embarkation	280,002	319,844	262,387	263,802	242,977
	Disembarkation	279,811	317,835	351,610	303,210	260,527
	Sub-total	559,813	637,679	613,997	567,012	503,504
International	Embarkation	141,178	177,368	188,928	180,337	148,373
	Disembarkation	151,370	143,392	209,604	125,054	147,003
	Sub-total	292,548	320,760	398,532	305,391	295,376
Total	852,361	958,439	1,012,529	872,403	798,880	

Gates of Dumai Port



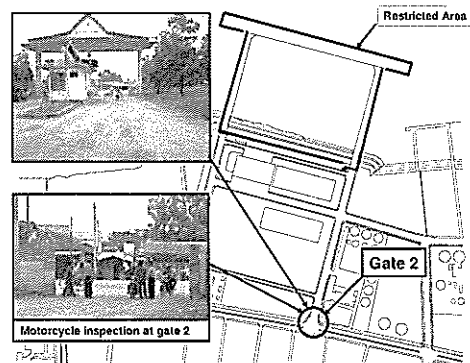
10

Multi-purpose Wharf

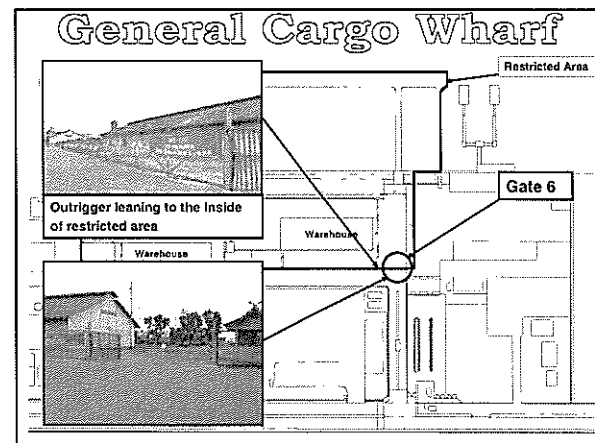
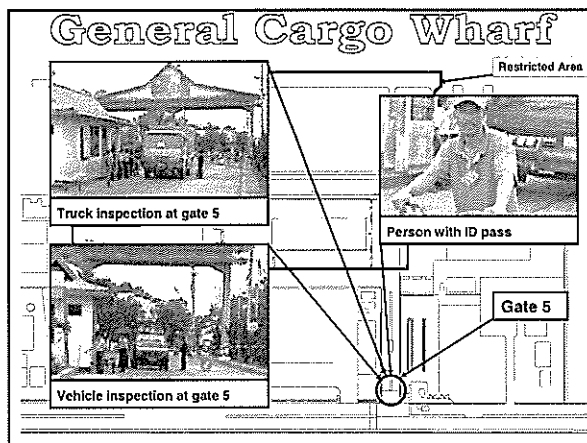
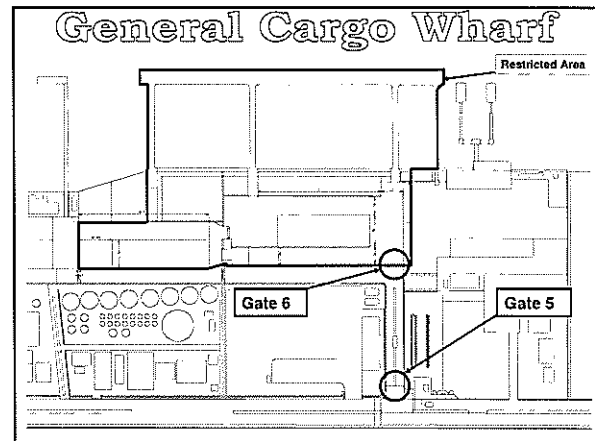
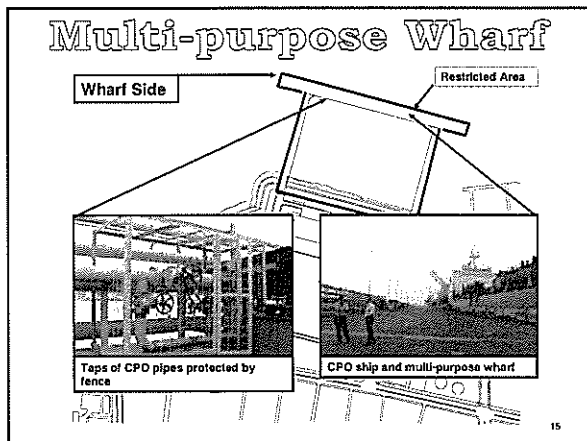
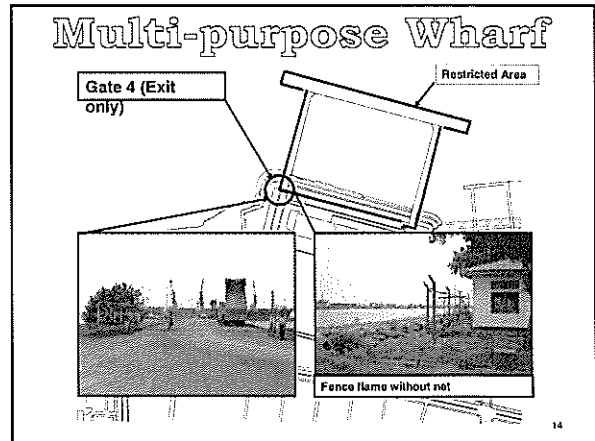
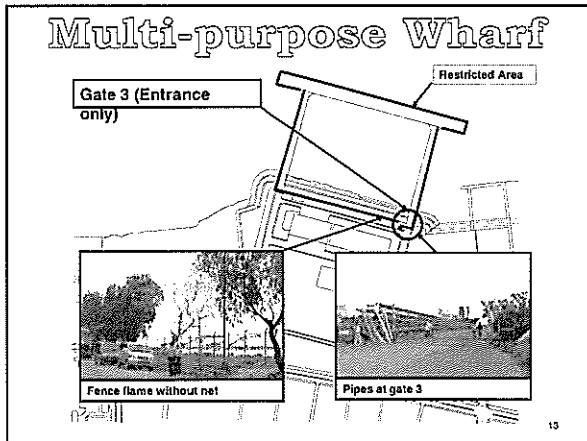


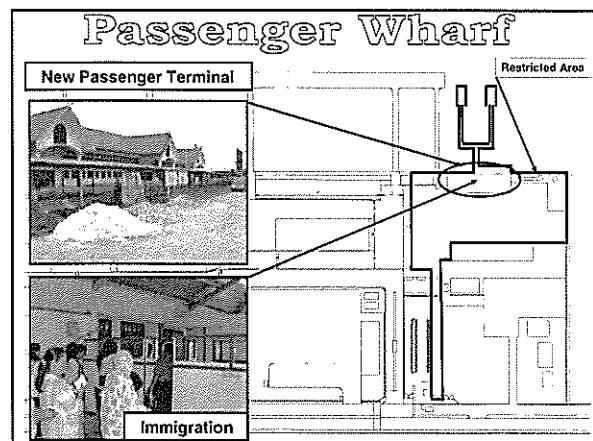
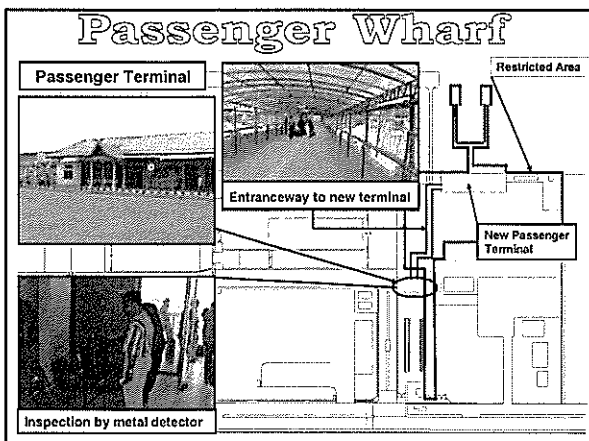
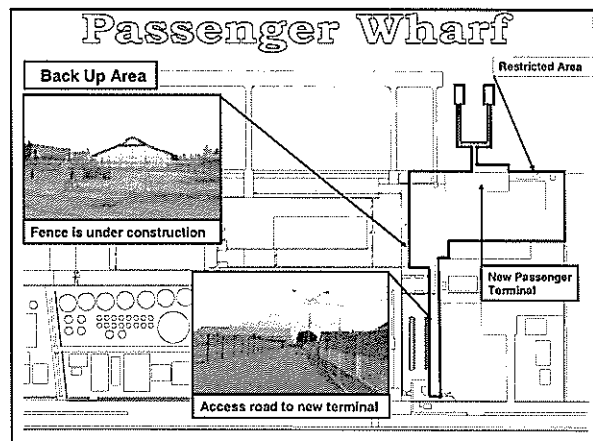
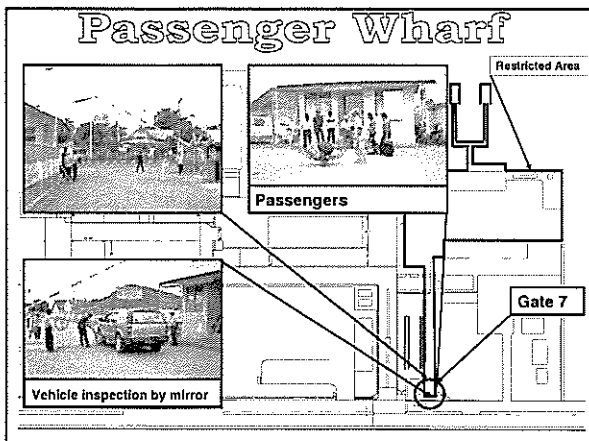
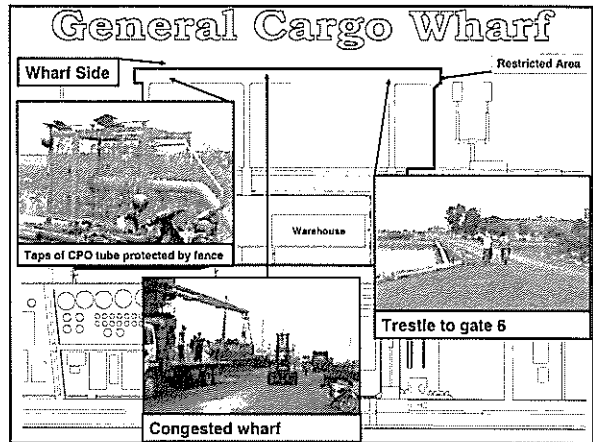
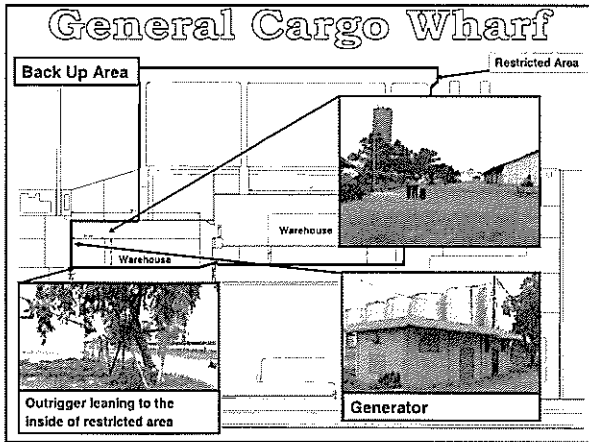
11

Multi-purpose Wharf



12





Access Control

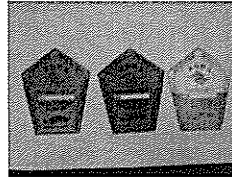
ID Card



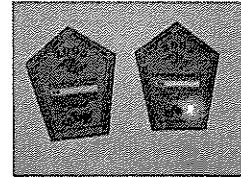
25

Access Control

ID Sticker



ID Sticker for Vehicle



ID Sticker for Motorcycle

26

Conclusion

- Port of Dumai has a security procedure and plan in place.
- The multi-purpose, general cargo and passenger wharves are ISPS compliant.
- The fence and a entrance gate should be installed in the multi-purpose wharf. The four security lightings and 2 speakers as a communication system should be installed. In addition, it is preferable to install the CCTV camera monitoring system in the multi-purpose wharf to secure the terminal security.
- The fence and entrance gate should be installed in the general cargo wharf. Especially, since the outrigger of existing fence leans to the inside of restricted area, its leaning should be improved to the outside of restricted area. The several security lightings and 4 speakers as a communication system should be installed. In addition, it is preferable to install the CCTV camera monitoring system in the general cargo wharf and passenger wharf to secure the terminal security.

27

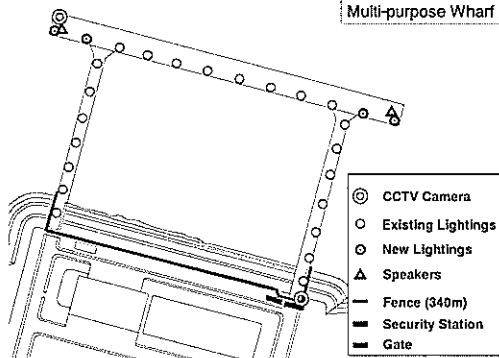
Conclusion

- The 6 CCTV cameras, a x-ray inspection system and a walk-through type metal detector should be installed in the passenger terminal. At least, 1 speaker as a communication system should be installed.
- It is also observed that there are many people walking in the restricted areas without being checked. These are people looking for odd jobs on a daily basis. PFSO should enforce security measures to these people who are entering the port facilities.
- They should be given visitor pass in exchange for their identification.

28

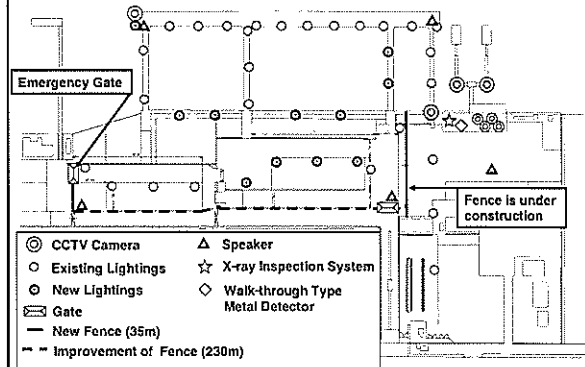
Conclusion

Multi-purpose Wharf

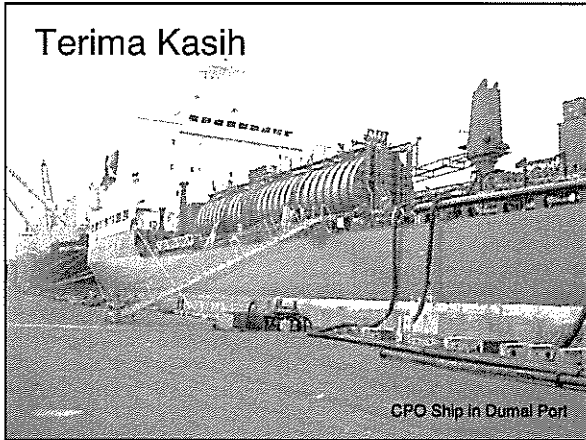


29

Conclusion



Terima Kasih



JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

WORKSHOP

Issues on Implementation of Port Facility Security Measures in Port of Palembang







Indonesian Port Corporation II

JICA Study Team
for the Study on the Port Security Enhancement Program
of Major Indonesian Public Ports in the Republic of Indonesia

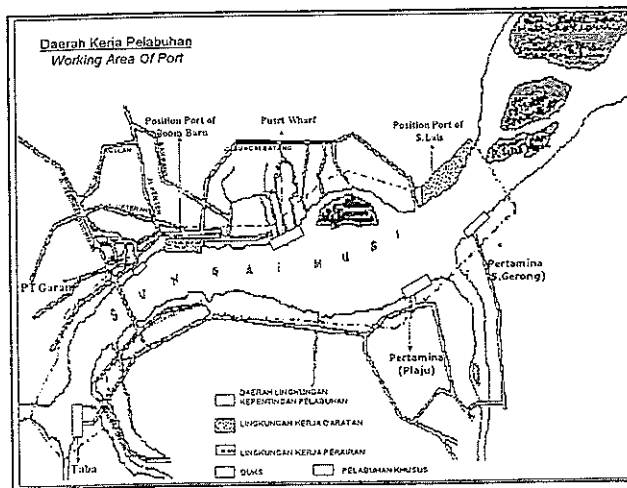
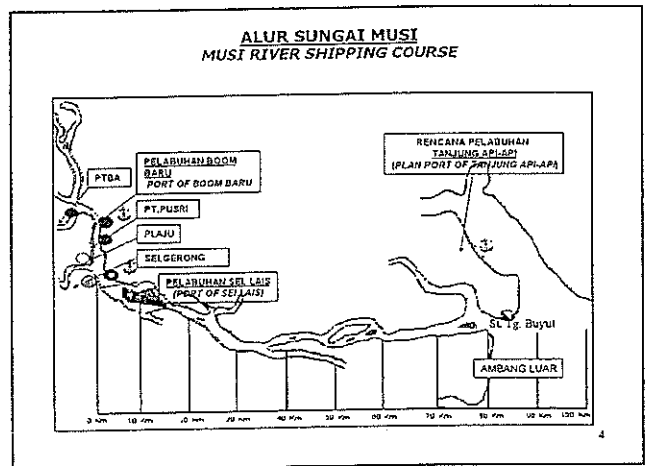
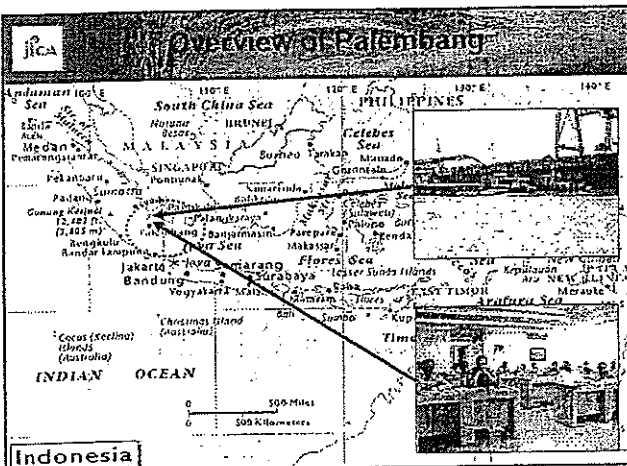
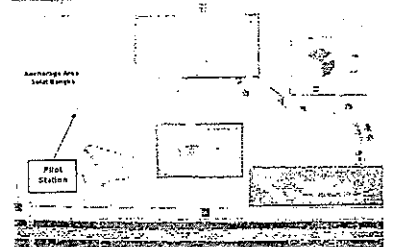
Acknowledgement

- We, the study team would like to thank the Port Administrator, GM, PSO, PFSO and staff of PELINDO II is assisting in our observation and study in the implementation of ISPS Code in your Port Facility.
- We apologize in the areas of ignorance and/or misunderstanding with regards to your operations and procedures.

PT (Persero) PELABUHAN INDONESIA II
CABANG PALEMBANG

2

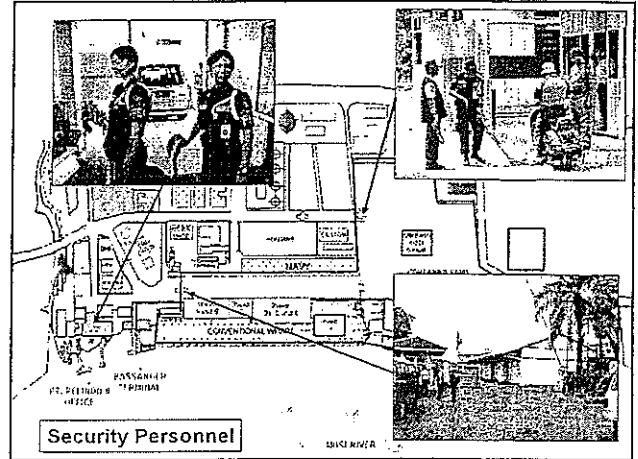
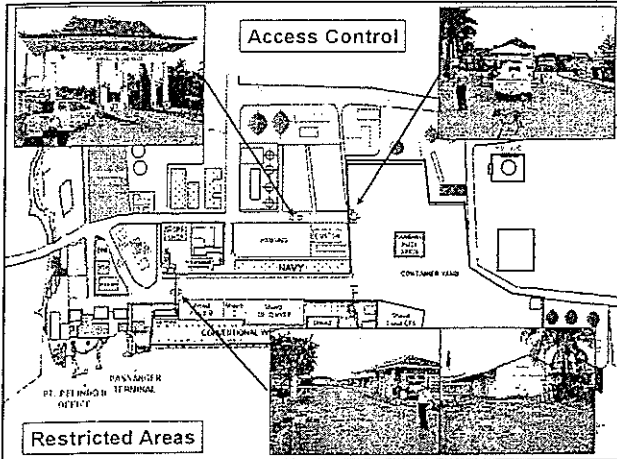
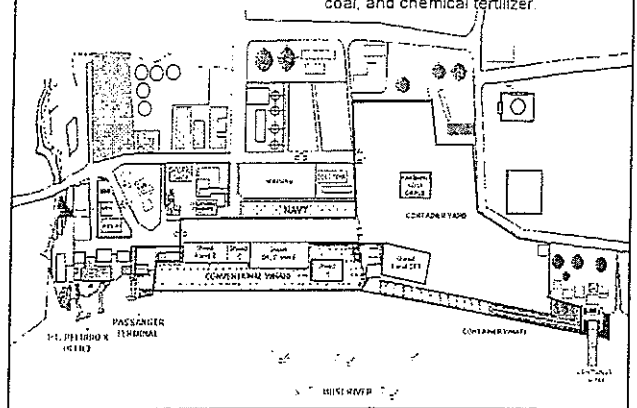

- The anchorage area is 108 km from Palembang Port
- Has incident of sea robbery
- Some ship owners will contract security personnel to be onboard when sailing in to Musi River.
- Domestic anchorage area in Sungai Lais is about 6 km from Palembang Port for small ships to anchor.
- Area patrolled by Water Police (POLAIRUD) & KPLP

Scope

1. Port Facility Security Duties
2. Access Control
3. Monitoring of Port Facility, including anchoring and berthing area(s)
4. Monitoring of Restricted Areas
5. Supervising the Handling of Cargo
6. Supervising the Handling of Ship's Store
7. Ensuring Security Communication is readily available
8. Training, Drills and Exercises
9. Conclusion

Site Plan of Palembang Port

Main exports consist of crude palm oil, rubber, coffee, plywood, cement, coal, and chemical fertilizer.

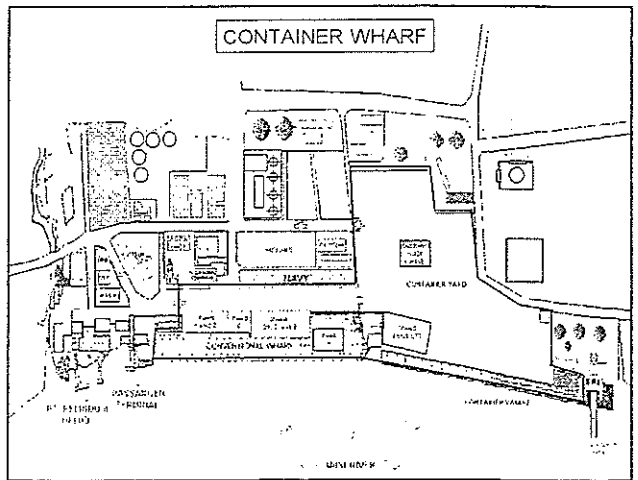



Main Gate

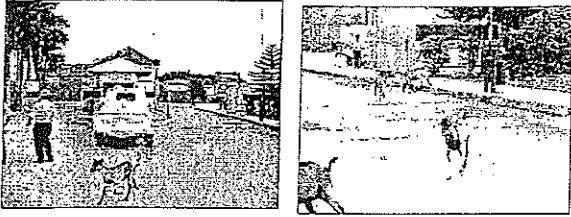
This is the main gate to enter the port area.

- It has a security post with no guards
- Limited access control on people or vehicles entering and leaving the port.

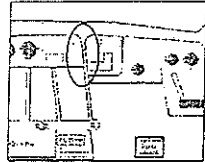
11



Container Terminal Gate



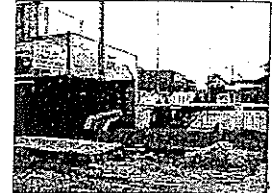
- Entrance to container terminal
- Security personnel at post
- Access to this gate via another route?



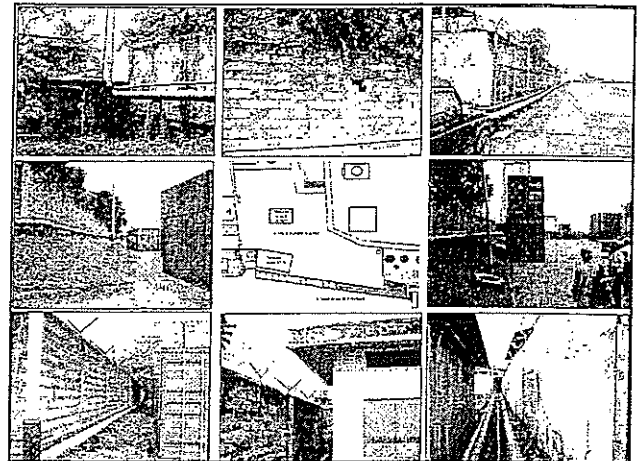
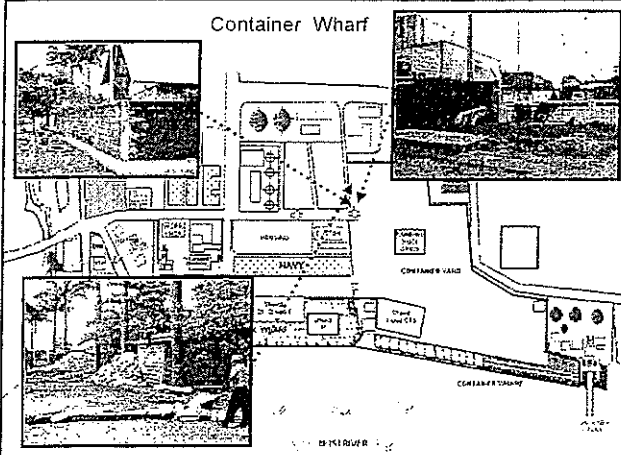
Exterior of Container Terminal



- Outside perimeter of container terminal
- Stalls outside wall fencing
- Right side of entrance to container terminal
- Pipeline above ground level



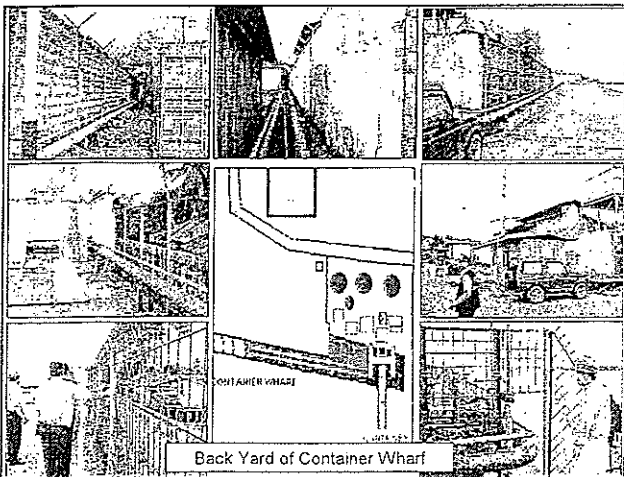
Container Wharf

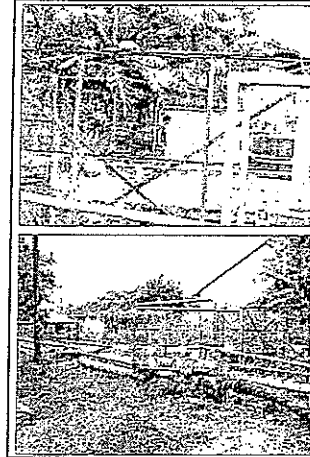
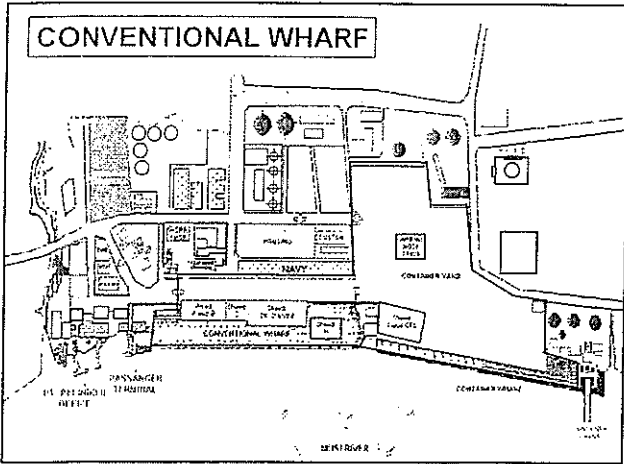
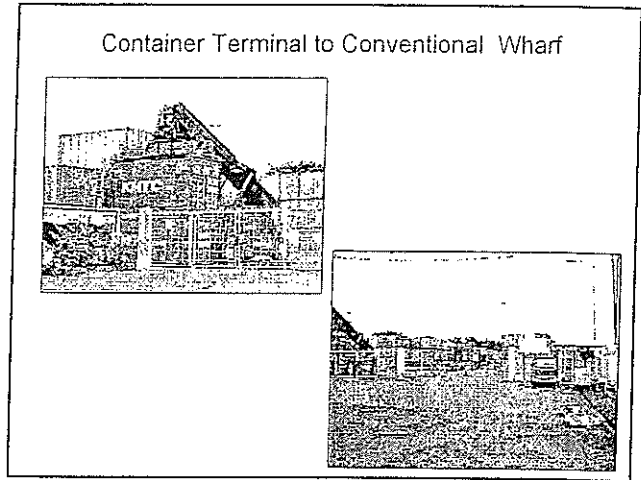
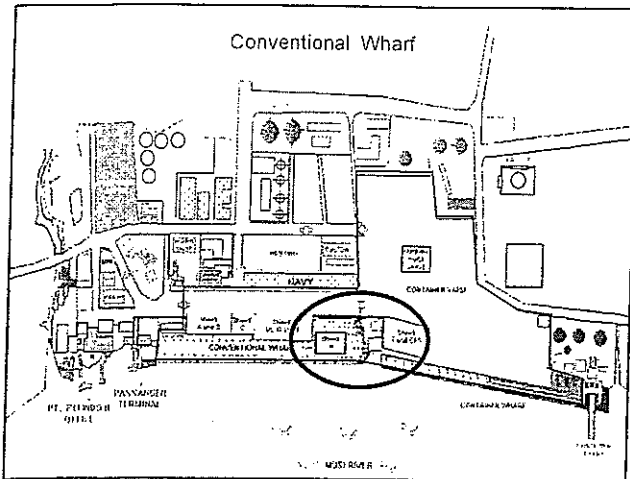


Recommendation

1. Clear hazardous waste or materials from restricted area
2. Pipeline within facility to have contingency plan
3. Daily temporary truck drivers to have authorized disc displayed prominently at the front of the truck.
4. Daily temporary truck driver to wear a security pass.
5. Too many trucks and people waiting at the yard area without identification.
6. Access from container terminal to conventional terminal to improve access control to conventional wharf
7. Right edge of berth at container terminal separating from neighbor is too wide. Easy for intruders to sneak in even when there is a lock.

Back Yard of Container Wharf





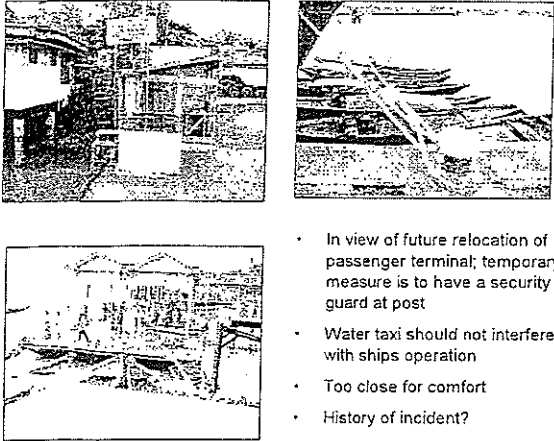
- Access control from seaward to be monitored or controlled
- Remove debris or unnecessary materials
- Fences to show boundary between container terminal and conventional wharf



- Security personnel to station at existing guard post during bunkering operation or in accordance with PFSP
- Port Facility under responsibility of PFSP – any security elements inside should coordinate with PFSP with regards to role and responsibility



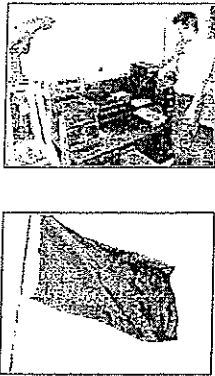
- Security to monitor area for intrusion
- Proposed canteen for future development as current practice pose risk
- Safety hazard during rainy days?



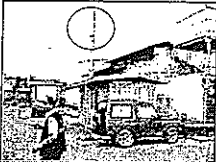
- In view of future relocation of passenger terminal; temporary measure is to have a security guard at post
- Water taxi should not interfere with ships operation
- Too close for comfort
- History of incident?

25

Communication System



- communications systems in Palembang pilot office received information regarding ships visit from the pilot office in Tg Buyut which is located near the mouth of musi river towards the Bangka Straits anchorage.
- Security personnel do not have operational VHF systems.
- Good communication method for security level 1 to 3.



26

TERIMAH KASIH

THANK YOU

27

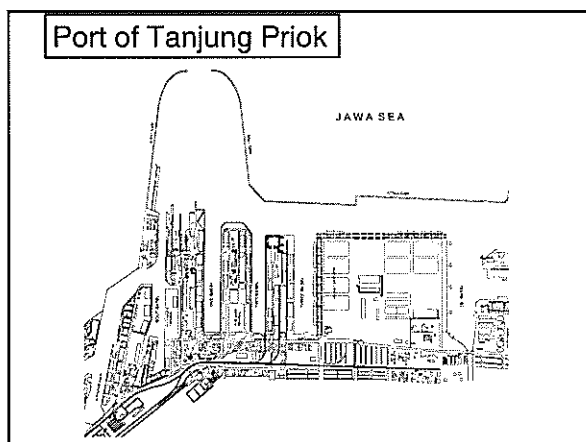
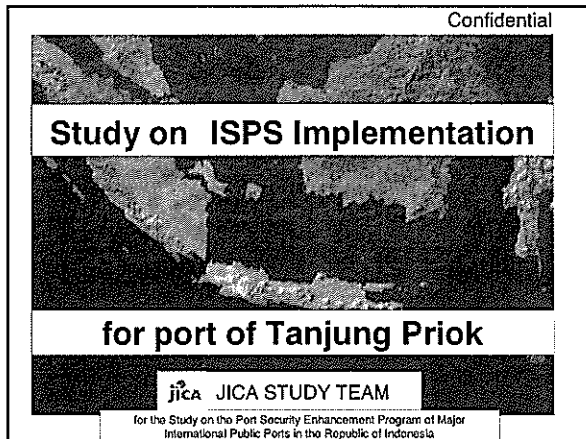


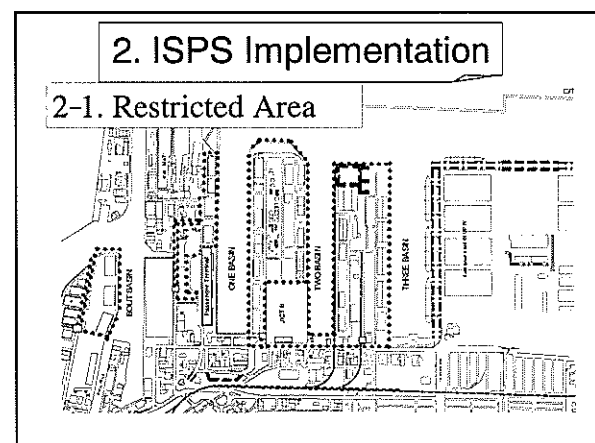
Table of Contents

1. Port of Tanjung Priok
2. Implementation of PFSP in Tanjung Priok PORT
 - 2-1 Restricted Area
 - 2-2 Observation
 - 2-2-1 Gate
 - 2-2-2 Fence
 - 2-2-3 Security Guard
 - 2-2-4 Patrol in the Water Area
3. Recommendation
 - 3-1 Gate and Fence
 - 3-2 CCTV Camera System
 - 3-3 Patrol Boat
 - 3-4 Procedure of Monitoring Security
 - 3-5 Maintenance Work
 - 3-6 Contingency Plan

1. Port of Tanjung Priok

Four International Trade Ports in Tanjung Priok Port

- 1). **PELINDO's Tanjung Priok Port**
- 2). JICT
- 3). KOJA
- 4). MTI (No Compliance)



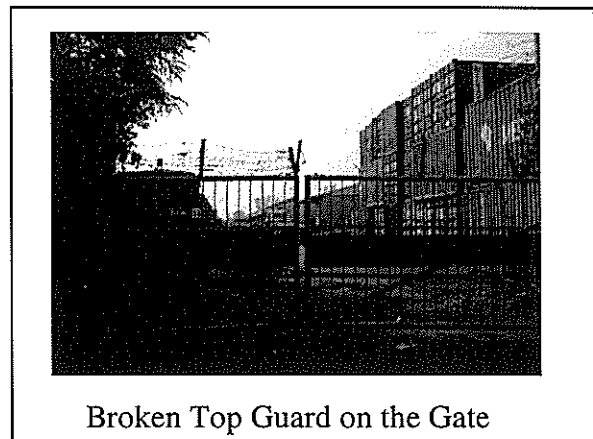
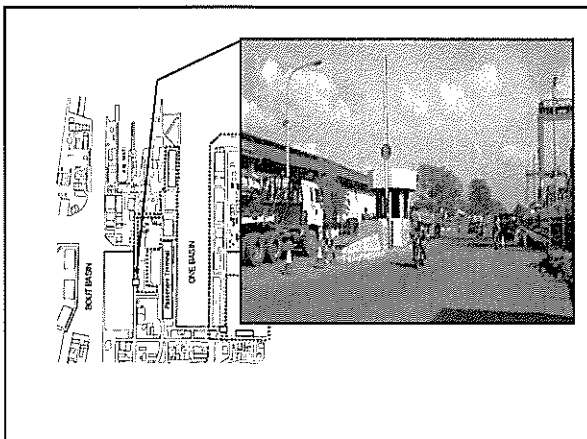
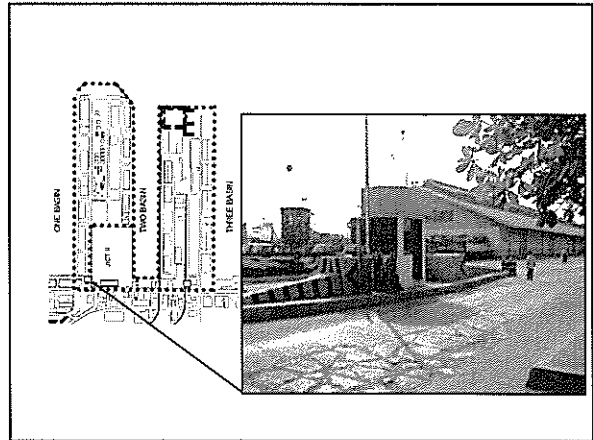
2-2 Observation

2-2-1 Gate

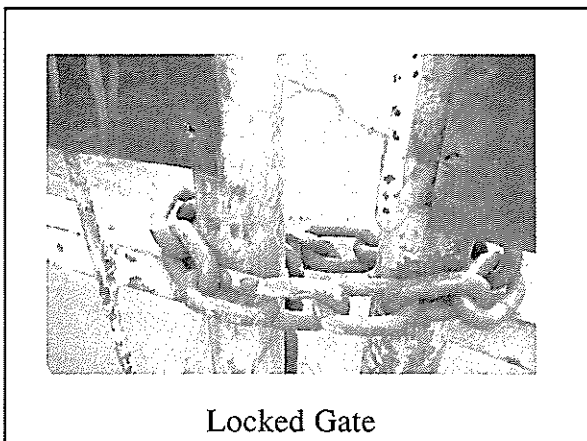
Car stopper should be closed while car is not entering

Access Control Procedure

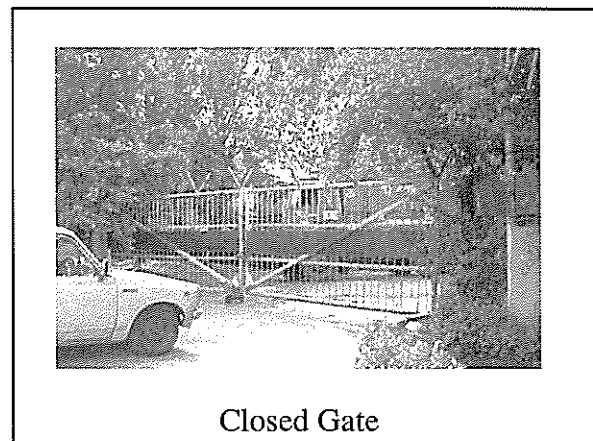
- Security guard should check a sticker of entering car
- Security guard should be check document



Broken Top Guard on the Gate

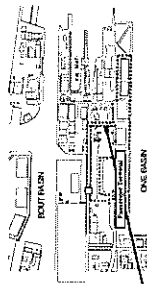
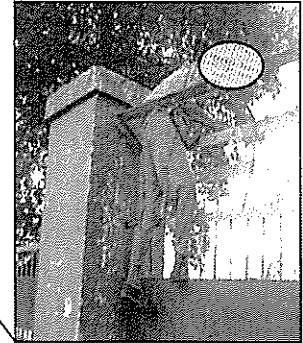
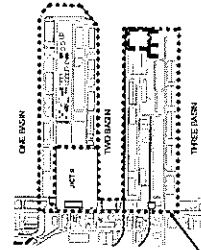
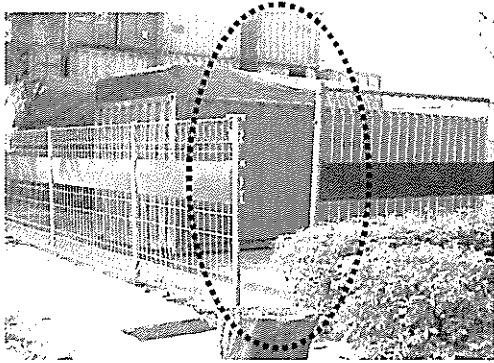


Locked Gate

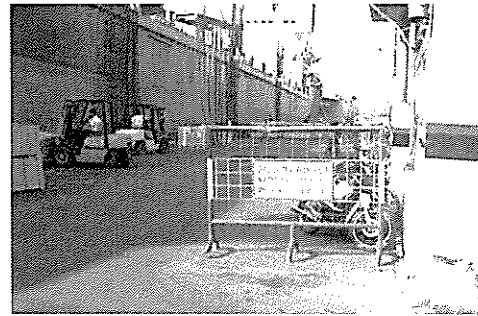


Closed Gate

2-2-2 Fence



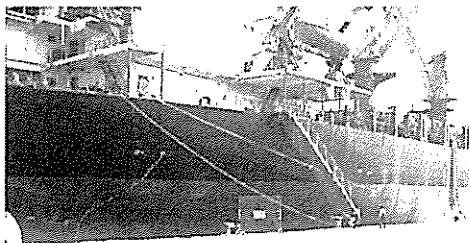
No clearance beside the fence



2-2-3 Security Guard

KPLP Security Personnel are deployed at the gate and patrol in handling yard

Security Guards from private security company are employed by the operator



Mobile fence which partitions off berth into international and domestic area

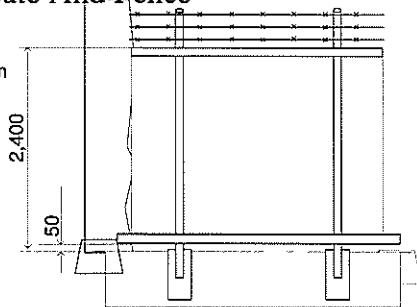
2-2-4 Patrol in the Water Area

Seaward security patrols are carried out by KPLP with two boats, but frequency is not adequate

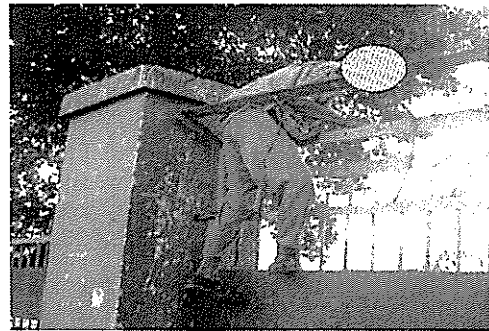
3 Recommendation

3-1 Gate And Fence

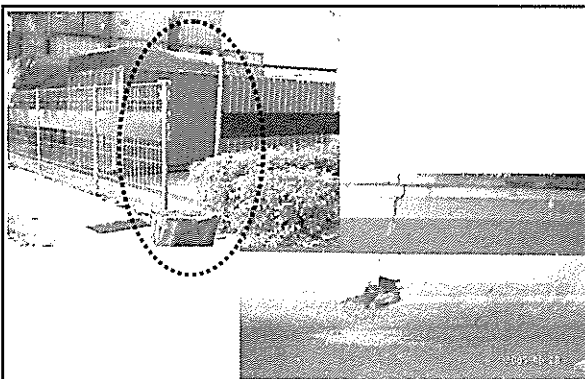
Unit: mm



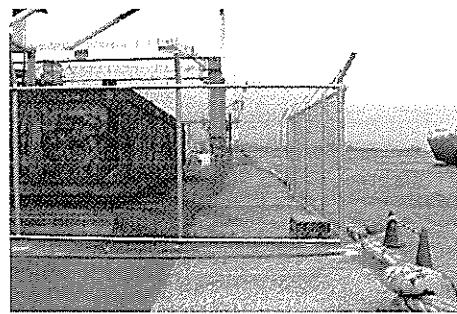
Clearance from gate to ground should be less than 5cm



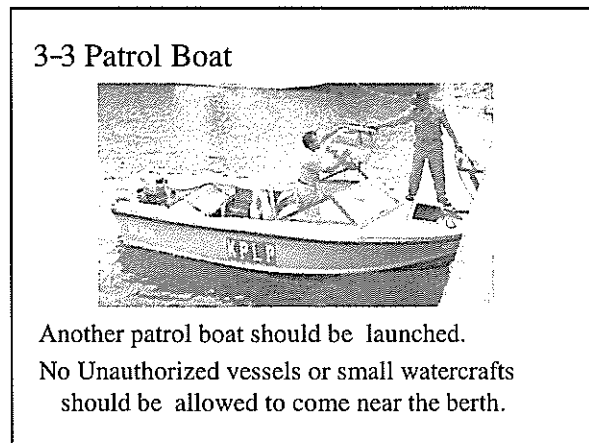
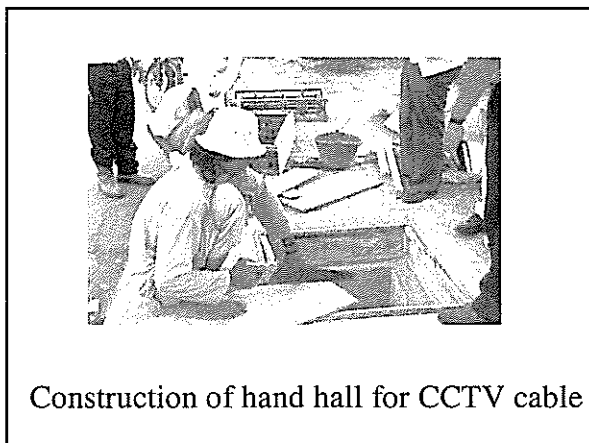
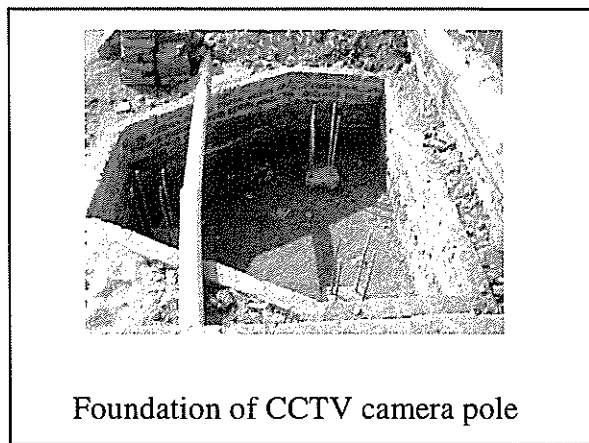
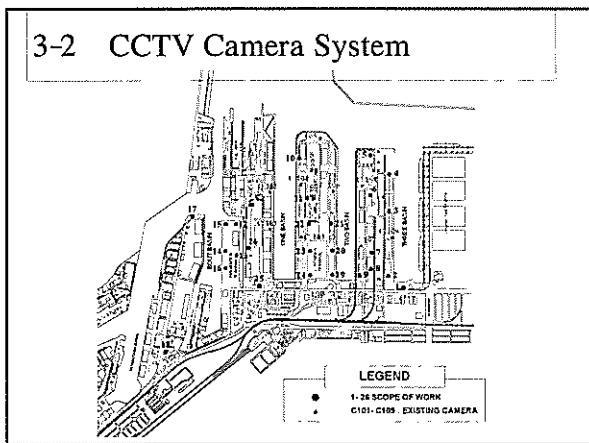
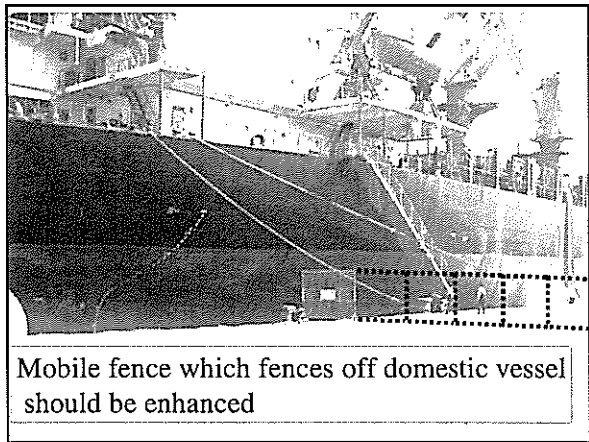
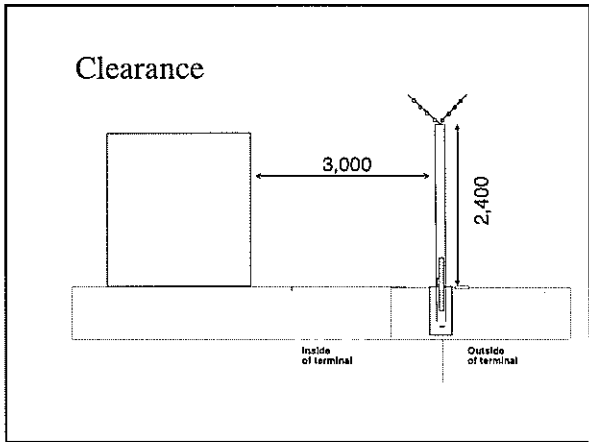
Gate should not be Climbed Over easily



Fence should be fixed partially



Sufficient clearance along the fence



3-4 Procedure of Monitoring Security

3-4-1 By Manpower

Security Level	Level 1	Level 2	Level 3
By Manpower: Mutual monitoring (security guard and workers in the restricted area)	(Method) *monitoring hours: operation hours *monitoring location: one's working place (items) *boundary: suspicious person and/or goods *gate: suspicious person and/or goods *within the yard aisle, warehouse, light and etc. *alongside the quay: intruders sneak in ship from ladder, mooring rope, etc.	*Same as on the left	*Same as on the left *In addition, follow the instruction from the Port Security Committee

3-4-2 By CCTV Camera

Security Level	Level 1	Level 2	Level 3
By equipment (CCTV system)	(Method) *monitoring hours: round-the-clock (24hours) *monitoring location: in monitor room by security guard (items) *set up for equipment: pre-set CCTV detectable area for sensor *boundary: suspicious person and/or goods *gate: suspicious person and/or goods *within the yard aisle, warehouse, light and etc. *alongside the quay: intruders sneak in ship from ladder, mooring rope, etc.	*Same as on the left	*Same as on the left *In addition, follow the instruction from the Port Security Committee

3-5 Maintenance Work

Maintenance Inspection Procedure

Description	Items to be Checked	Daily Inspection	Periodical Inspection
Fence and Gate		*Visual inspection during patrol (repair, reinforce, or replace if necessary)	*Conduct monthly *Sway and confirm act is not loose
Security Light	Road Light	*Ensure that all security lights are illuminated by visual inspection during patrol	*Conduct annually *Check mounting of lamp fitting *Clean the cover check cables and switch box
Monitoring System	CCTV Camera Monitor	*Check operating range of camera platform *Check brightness of the graphics	*Conduct annually by the supplier *Cleaning, adjustment, and change consumables
Communication System	VHF Radio Telephone Fax	*Check in daily usage	*Conduct annually by the supplier *Cleaning adjustment, and change consumables

3-6 Contingency Plan

- Evacuate following the instruction of PFSO
- Announce gate No. when evacuating from the restricted area
- Announce the name of facility when evacuating to a building
- PFSO directs evacuation and confirms that no one has been left behind

Emergency Contact List

Security Officer of PELINDO's Port

Organization/Title	Tel.	Name	Remarks
PFSO			
Deputy PFSO			

Port Security Committee

Organization/Title	Tel.	Name	Remarks
ADPEL			
PSO			
KPLP			
KPPP			
Custom			
Fire Department			
Others			

TERI MA KASIH

ARIGATOU
GOZAIMASITA

DGSC-JICA Workshop ISPS Code in PLINDO III

Date: July 18-20, 2005
Place: PELINDO III Headquarter meeting room
Participants: about 50

(July 18, 2005)

1. The policy and current issues of port security measures in Indonesia (Cholik)

Q1) How do we allocate international vessels which comply with the ISPS Code to wharves in a port where port facilities are insufficient?

In Tg.Perak port, international ships which comply with the ISPS Code often cannot use the international passenger terminal which comply with the ISPS Code because domestic vessels occupy the terminal when the port is congested.

A1) In foreign countries, international ships which comply with the ISPS Code cannot berth at wharves which do not comply with the ISPS Code. In Indonesian ports such as Tg.Perak international ships which comply with ISPS Code often cannot berth at the international passenger terminal which complies with ISPS Code because many domestic vessels use the terminal. In these cases, the following problems might happen. Therefore it is desirable that the port facility should comply with the ISPS Code as soon as possible if liner passenger ship comes to wharves.

(1) International ships which comply with ISPS Code do not want to use port facilities which do not comply with the ISPS Code.

(2) If an international ship berths at the wharf, extra security measures which are the same as that of security level 2 are requested and the port management body has to bear the cost.

Q2) How does the Contracting Government decide security levels?

(1) Procedures to show security threats in a port facility

(2) Methods to detect security threats without delay (such as terrorist activity)

(3) Procedures to convey information when a security threat occurs

A2) (1) The National Security Committee composed of relevant security organizations including Government Intelligence, Navy, Police should be established to implement effective security measures. At present each port has to tackle with port security incidents.

(2) For example, we can obtain intelligence information. We had an experience in which we prepared to introduce measures for security level 2 when we obtained information that an Australian ship carrying explosive bomb would enter Tg.Priok port.

(3) In order to take action against terrorism, one of the important issues is communication between the National Security Committee and regional Port Security Committees. We have to establish proper communication system based on coordination with relevant organizations.

Q3) How do we conduct Drills and Exercises which are needed by ports complying with the ISPS Code?

A3) It is impossible for a single port management body to conduct them. We suggest you to involve many relevant organizations and to make good use of RSO's experience.

Q4) What are the contents of Port Facility Security Assessment including physical security measures,

structural standard and scope?

(1) Are illegal drugs included in security objectives?

(2) How does the Contracting Government regard the vulnerability which is caused by carelessness of forwarders and consignees?

A4) (1) As you know, security threats are composed of nine items. Illegal drugs are not included in the security threats.

(2) Although it is difficult, efforts to meet each region are needed. Comprehension of forwarders and consignees is quite important to realize the ISPS Code.

Q5) I would like to provide new information obtained at an international conference in which representatives will come to the related ports to strengthen security measures of vessels which plan to visit ports in the US.

A5) Thank you for your information. It is difficult to obtain the understanding of the public concerning security in ordinary ports. It takes a lot of time to enhance security measures in Indonesia which has many complicated problems and various social cultures.

Q6) Banjarmasin port has a long channel and financial support is needed to comply with the ISPS Code for that.

A6) It may take a long time to obtain consent from relevant organizations. Revision of tariff is one of the alternatives.

Q7) We want to know the concrete security measures for Benoa Port (Bali Island) at security level 1 (at normal time)

(1) Who decides the duration of security level 1? At present, KPPP escorts vehicles full-time in the port. Such responses are needed only in security level 2. Extra cost is needed.

(2) Can we obtain specific supports including training and port security equipment from JICA to enhance security measures?

A7) (1) A port authority and a PFSO are responsible for security measures at security level 1. It is needed to strengthen the status of PSC and PFSOs.

(2) The DGSC hopes that JICA will give training and education and guidance on how to use security equipment such as CCTV and metal detectors. Recently JICA provided CCTV cameras to Tg.Priok, Tg.Perak and Batam.

2. Introduction of Japanese experience in port facility security measures (Yamaguchi)

Q1) How do we monitor by CCTV camera surveillance system? Who is responsible for management of the CCTV camera surveillance system?

A1) In principle, you monitor ship/port interface and fence areas to detect intruders. The PFSO is responsible for that.

Q2) What are the specifications of the CCTV camera? How much coverage can the CCTV camera provide?

A2) It can rotate 360 degrees horizontally, 20 degrees in the upper direction and 70 degrees in the lower direction and its visibility range is 360 meters.

Q3) How do you monitor the sea side by CCTV camera surveillance system in Japan?

A3) On wharves in Japan vessel width plus 30 meters is designated as a restricted area and it is usually monitored by CCTV system. In the case of security level 2, a patrol boat surveys the area.

from the viewpoint of safety as well as security.

(July 19)

1. Overview of ISPS Code and Quiz (Khoo)
2. Overview of Maritime Security Threats (Khoo)
4. Role of IMO (Khoo)
6. Security Self-assessment (Khoo)

Q1) Some international ships alongside berth that is non-ISPS compliant and they do not complain nor request for exchange of DoS.(PFSO)

A1) The master of the ship has the final say with regards to safety and security of the ship. ISPS Code Part A/5.2.4 states that DoS can be requested based on this scenario. Part B/9.51 also advises that the SSP should establish details of the procedures and security measures the ship should apply when interfacing with a port facility that does not need to comply.

Q2) Do we have to include goods that are transferred from a non-ISPS port facility to as an ISPS compliant port facility in our PFSP? (SATPAM)

A2) Yes, please refer to Part B/16.38 which should be included in your PFSP.

Q3) Who is responsible for the port facility security? If it is the PFSO why do the police need to be stationed in the port facility? (SATPAM)

A3) Port Facility is under the responsibility of the PFSO at level 1. At level 2, it will be supervised by PSO based on your existing PSC guidelines. Police presence may be requested for law enforcement but it is temporary only. PFSO should discuss these issues with PSO. Please do not confuse the difference between port security and port facility security. One is covered under the ILO-IMO Code of Practice and the other is under the IMO ISPS Code.

Q4) There are villagers that live inside the port area. They have been living there for many years and their houses are next to the fences of the port facility. (DGSC-Planning)

- a. Do we need to relocate them? Their houses are within restricted area designated by the RSO.
- b. They are a threat as we do not know who is living there.

A4) This is a sensitive issue that needs to be addressed by your local authority. The houses shouldn't be covered in your PFSP as a restricted area, else you have to assign security patrol and also you will intrude into the privacy of the villagers. My advice is to contact the village head and discuss such issues. If there is a plan for relocation than temporary measures should be in place. Perhaps, all residents should be accounted for and any visitors to the house should exchange their ID with photo for a visitor pass. Village chief should hold periodic discussions and inform the residents that they have a part to play in protecting the port. If the port is affected, all staying there will be evicted. Therefore, villages should be educated and encouraged to report any suspicious activity or person.

Q5) How do we defend against an underwater attack by divers or submarine? (KPLP)

A5) Risk Analysis and Vulnerability Assessment will decide the importance of the port facility and threats from underwater. There is no need to have the latest diver detection sonar system if it doesn't warrant it. However, security measures such as patrolling along berthing area and using torchlight to check for any activities or ropes should be introduced. Lights should also be bright enough for the water area so that intruder shadows may be reflected at the walls and also easy for security personnel to detect. The lighting glare should be towards the water and not at the wharf. However, lighting should not affect the safety of navigation

Q4) How long does it take for security guards to go reach the scene after a sensor detects an intruder and CCTV camera captures him/her.

A) It is estimated that it takes 3-5 minutes when security guards always stay in the terminal area and about 15 minutes when security guards are not in terminal area.

Q5) How is the interval of lighting decided?. How much does it cost to install lighting shown in the distributed document?

A5) Minimum illumination intensity is nearly 3 luxes when CCTC camera is installed. Therefore lighting has to be installed at 50 meter intervals. The cost is not calculated.

Q6) In case that CCTV cameras are installed in Japan, how many security guards are deployed in one terminal?

A6) In principle, only control persons for monitoring system are deployed. Six persons are needed for three shifts in a day. CCTV cameras are installed to reduce security personnel as labor costs are high in Japan.

Q7) How long does it take and how much does it cost to introduce CCTV cameras as security measures included in the presentation material?

A7) It takes 0.4 million US dollars and 3-4 months.

Q8) In Indonesia many public including vendors come into a port area, making it difficult to take port security measures. How many ordinary people stay in a port area in Japan?

A8) In Japan ordinary people seldom enter the port area.

Q9) In the case of security level 3 in Japan, what are security guards requested to do?

A9) Security guards request the police to come to the port area without delay. Security staff does not have weapons and has no authority to make an arrest.

3. Port facility security assessments and port facility security plans for the Port of Benoa (Ono)

Q1) How much does it cost to take security measures including installation of security equipment?

A1) We have not calculated the cost yet.

4. Port facility security assessments and port facility security plans for the Ports of Banjarmasin (Iinuma)

Q1) Bajarmasin port is a river port and its water depth is shallow. Therefore foreign cargo is transhipped to barges at an anchorage and transported to the port as domestic cargo. In this case, how do we treat the anchorage and wharf in the PSFP?

A1) The study team is now discussing with DGSC this case where an anchorage is far from a wharf and international cargo is handled at the anchorage.

5. The issues on implementation of port facility security measures in the Port of Tg. Perak (Ono)

Q1) In Tg.Perak, many relevant organizations are involved in monitoring water area. It is difficult to coordinate the organizations. Do you have any idea for smooth coordination?

A1) Many vessels lay at anchor in Tg.Perak. It is needed to introduce navigation surveillance system

Q6) We always focus on international vessels that are 500 GT and above based on ISPS Code. What about domestic vessel such as bunkers, tug and barges? They are a threat too as historically speaking we have had instances of domestic terrorism.(Port Master)

A6) This is something the CG is studying now. Access control from seaward is important. Unauthorized sampan should not be allowed near international ships berthed at the port facility. There should be a response patrol boat on standby for activation if the need arises. Port Administrator should encourage vessels to report any suspicious craft or activities. In Singapore, we have harbour craft transponder systems for vessels below 300 GT. This technology is inexpensive and uses GPRS technology.

3. Risk Analysis & Vulnerability Assessment (Kado)

Q1) It is said that impact and feasibility of security measures should be carried out when planning a security plan. Is there any matrix or something like that which shows the relation between security measures and their feasibility?

A1) We do not have such a matrix.

Q2) When assessing threats and risks, scores of consequence and vulnerability have only three steps. In other cases more steps such as five steps are adopted. Don't you think that assessment by more than three steps is needed?

A2) A general concept on risk evaluation is explained in the presentation. It is one of the examples. Other cases will be explained later.

5. Implementation and Management of Port Facility Security Measures (Hiura)

No question

DGSC-JICA Workshop ISPS Code in PLINDO IV

Date: July 21-22, 2005
Place: Gran Puri Hotel (Manado)
Participants: 72

(July 21)

1. The policy and current issues of port security measures in Indonesia (Cholik)

2. Introduction of Japanese cases on port facility security measures (Yamaguchi)

Q1) Is an X-ray detector no used for cargo in Japan? (Customs)

A1) This is the responsibility of Customs. Therefore port management bodies do not own it.

Q2) What problems does Bitung port have concerning port security from the viewpoint of a Japanese expert? What the counter measures do you think are necessary?

A3) We will discuss this at the other session.

3. Port Facility Security Assessment and Port Facility Security Plan for Bitung Port (Hiura)

Q1) Can we introduce the Japanese security system in Bitung port?

A1) It may be difficult to introduce Japanese security system in the present Bitung port where international and domestic cargo are handled at the same berth. However, if the new container berth is used only for international trade, you could introduce the Japanese security system there.

Q2) What problems will we face when applying the ISPS Code to Bitung port?

A2) The problem is that temporary fence may not be placed when an international vessel berths at the designated area even though the use of such a fence is required in the PFSP.

4. Port Facility Security Assessment and Port Facility Security Plan for Samarinda Port (Sasa)

Q1) How many security guards are needed in the restricted area which is separated from other areas by movable fence?

A1) Two security guards are deployed at a gate and another two in the restricted area. In addition two persons for traffic regulation are also needed.

Q2) Are there any differences in security measures between Makassar and Samarinda ports? Do we have to introduce extra security measures for a river port?

A2) We will explain the security measures in Makassar port. Samarinda port is a river port and has anchorages around the river mouth area which are far from wharves. Therefore it may be possible that anchorages and channel are exposed to threats.

However, since cargo transhipped at an anchorage in Samarinda port is domestic, the anchorage does not have to comply with the ISPS Code. But I think that patrol vessels have to be deployed in high-risk situations.

Q3) Anglers enter the port area. How do we cope with this?

A3) Vendors sell food and other items in the passenger terminal at Samarinda port. Vendors, who are

thought to be needed in the passenger terminal, should be permitted to do business at an appropriate area and the passenger terminal must be surely separated from other area by fence. Fishing in a restricted area must be strictly prohibited.

5. Implementation and Management of Port Facility Security Measures (Hiura)

Q1) As to the CCTV surveillance camera system, how do you cope with electric power failure?

A1) Electric power is maintained for ten minutes by uninterruptible power source (UPS). During the 10 minutes, initial measures can be engaged.

Q2) Do the sensor use high voltage?

A2) No. The sensor is a device to detect intruders with CCTV cameras.

Q3) How do you monitor the water area?

A3) We keep necessary illumination intensity along a wharf and monitor water area. In case of the security level 2 in Japan, patrol vessels are deployed.

Q4) I want know the specifications of a fence.

A4) Class A fence is 2.4 meters high, has a 30 degree inclination from the vertical toward the outward and 45 cm outrigger with barbed wire. Class B is 1.8 meters high and others are the same as Class A. In Japan, CCTV cameras and sensors are installed only for a Class A port. Class A stands for international container, RORO, passenger and dangerous goods berths Class B is for all ports other than Class A.

(July 22)

1. The issues on Implementation of Port Facility Security Measures in Makassar Port (Kado)

No question

1. Overview of ISPS Code and Quiz (Khoo)

2. Overview of Maritime Security Threats (Khoo)

4. Role of IMO (Khoo)

6. Security Self-assessment (Khoo)

Q1) Hand carry luggage tends to get lost in ferry terminals. Also, there may be a risk where a potential smuggler may pretend to exchange baggages in hope that the wrong person will be caught. Then, once outside the building they will exchange back the baggages. Do we need a system that all hand luggage needs to be tag as like in airport? (Custom Officer)

A1) Current practice by airport is similar with passenger ferry. Only check in luggage is tagged and linked to the passenger concern. Hand luggage is the responsibility of any individual. CCTV plays an important part here as well as signage to advise against unattended luggage. Part B/16.30 to B/16.48 provides some guidelines. However, this guideline (which should be in your PFSP) should go together with your existing custom procedures.

Q2) There are no clear guidelines as to who is responsible if a ship is on fire while alongside the berth. Do we release the ship to float or do we fight the fire (Navy Officer)?

A2) You do have an existing Emergency Response Procedure for Fire as well as other incidents. Please refer to it as it is your national regulations. Tug boat should be on standby in the

event a ship is not under command. She may pose a navigation and safety hazard.

Q3) There is a tank farm that is opposite the port facility. The RSO says we do not need to include the tank farm in our PFSP as it is outside the port facility. Do we need to be concerned (and yes to your questions, there is a pipeline that links it to our berthing area.) (PFSP)

A3) If the tank farm is destroyed or on fire, will it affect your operations? (Yes). Then it should be addressed in your PFSP or referred to in any of your existing Emergency Shutdown Procedures etc... The tank farm is close to your port facility and may pose a hazard. Remember risk analysis is not only within. It is necessary to look into your external surroundings and the resulting impact on your port facility in the event of an accident.

Q4) In a particular port, there are ships that use the anchorage for transloading with international vessels. At this anchorage the international vessel does interface with both ISPS and non-ISPS compliant vessels. The international vessel doesn't seem to mind. Your comment? (PELINDO)

A4) Not advisable. The Master of the Ship may have to answer for it in the next port of call. Please refer to Part A/5.2.5, B/4.38, B/9.51. We have to ask your CG to comment on it. All port facilities with international interface will have to comply with the ISPS Code.

DGSC-JICA Workshop ISPS Code in PLINDO I

Date: July 25-26, 2005
Place: Emerald Garden Hotel
Participants: about 50

(July 25)

1. The policy and current issues of port security measures in Indonesia (Cholik)
2. Introduction of Japanese cases on port facility security measures (Hiura)
No question
3. Port Facility Security Assessment and Port Facility Security Plan for Pekanbaru Port (Hiura)

Q1) How do we ensure security in an anchorage at the river mouth?

A1) You have two alternatives. One is to take measures so that only the anchorage area as the ship-port interface where cargo is transshipped complies with the ISPS Code. Another is so that both the anchorage area and the wharf are in compliance. In the latter case, a captain of a tug boat takes responsibility for cargo while sailing in a river. The captain is also requested to fill in a check list and describe incidents in a report.

Q2) Who is responsible for the management of rivers?

A2) PELINDO

Q3) What security regulations have been drafted for the river mouth?

A3) None.

4. The issues on Implementation of Port Facility Security Measures in Belawan Port (Khoo)
No question

5. The issues on implementation of port facility security measures in the Port of Dumai (Kado)

Q1) At the port of Dumai, both PELINDO I and a private company operator have facilities in the port. How should security measures be implemented in this case? (PFSO of Dumai port)

A1) While PSO has responsibility for the entire port area, we also think it is necessary for PELINDO I, the private company and members of the PSX to cooperate in order to implement the various security measures.

Q2) Concerning the plan to install a CCTV monitor on the multipurpose wharf, we are concerned that the camera will hinder handling operations if it is placed on the seaside of the wharf. Would it be possible to move it a little further back?

A2) The CCTV camera's key focal points are the ship/port interface and the area surrounding the fence. That is why we chose to position it at the seaside of the wharf. However, if it will hinder operations, it can probably be moved a little closer to the land side.

(July 26)

1. Overview of ISPS Code and Quiz (Khoo)
2. Overview of Maritime Security Threats (Khoo)
4. Role of IMO (Khoo)
6. Security Self-assessment (Khoo)

Q1) Sometimes Intelligence and Security personnel enter our port facility without informing us. When challenged they say they are on cover operations or surveillance. Is that allowed under the ISPS code?

A1) Using MSC 80 Circ 1156 as a guide, I would suggest the CG provide guidelines to the port facility. If the operations need to be covert, then perhaps the GM or PFSO should be informed to prevent any incident from happening in the port facility. The security personnel on duty may request visual identification and verify with PFSO.

Q2) Sometimes before an international ferry arrives, many visitors, mainly family and friends of people on board, enter a restricted zone of the passenger terminal. What should we do about this?

A2) Existing immigration and customs procedures do not allow visitors to congregate at restricted areas. As such, PFSO should liaise with immigration and customs officers to announce over the PA system that entering such areas is prohibited. This is an internal problem that DGSC must deal with.

Q3) Do we need to control cargo coming into the port facility by rail? We don't know what is being brought in and some items may pose a risk.

A3) Yes, ISPS Code Part B/16.30 to B/16.48 provides some guidelines.

3. Risk Analysis & Vulnerability Assessment (Kado)
No question

5. Implementation and Management of Port Facility Security Measures (Hiura)
No question

DGSC-JICA Workshop ISPS Code in PLINDO II

Date: July 28-29, 2005
Place: PELINDO III Headquarter meeting room
Participants: 74

(July 28)

1. The policy and current issues of port security measures in Indonesia (Cholik)
2. Introduction of Japanese cases on port facility security measures (Hiura)

Q1) In Japan, both fixed and revolving type CCTV monitors are used. Where are they generally placed?

A1) It depends on what is being monitored. For gates and the passenger terminal, a fixed monitor is used. A revolving camera is used to observe the fence line and restricted areas. And different types of cameras have different ranges, i.e., can capture objects 100m away, 350 m away, or even 1000 m away.

3. The issues on Implementation of Port Facility Security Measures in Palembang Port (Khoo)
No questions

4. The issues on implementation of port facility security measures in the Port of Tg. Priok (Kado)

Q1) In Indonesian ports, in terms of the apron to yard ratio, the apron is higher. Is the same situation seen in Japan.

A1) Generally the width of the apron is 30 m, while the yard stretches some 350 m.

Q2) During level I, how often should patrols of the water area be conducted?

A2) At least twice a day.

(July 29)

1. Overview of ISPS Code and Quiz (Khoo)
2. Overview of Maritime Security Threats (Khoo)
4. Role of IMO (Khoo)
6. Security Self-assessment (Khoo)

Q1) If there is a need to go to level 2 or 3 due to an emergency situation, do we wait for CG approval before executing security measures required by level 2 or 3?

A1) The CG decides on when to raise the level from 1 to 2 or from 2 to 3. However, in the event of an emergency, the port facility, on advice from PSC, may implement measures of level 2 while awaiting CG decisions. The port facility is technically still at level 1 but with level 2 security measures in place.

Q2) What do we do if we receive a phone call saying that there is a bomb somewhere. Do we evacuate immediately?

A2) Your existing PFSP should have addressed this procedure. In addition, office personnel should

also be trained bomb incident management. Your PFSP should be incorporated in your existing fire evacuation plan. Security personnel should be trained in first level bomb sweeping. Assembly area should be swept before allowing personnel to evacuate and assemble here. Bomb incident management is a course by itself.

Q3) There are some pipelines in the port facility that do not belong to us. They are linked from the nearby CPO plant. These pipes carry crude palm oil, which are not dangerous cargoes. Do we still need to be concerned?

A3) The main issue is if the pipeline is damaged or bursts, will the oil spill affect the operation of the port facility? If yes, safety and security are at stake. As such, the port facility should coordinate with the owner and promulgate an emergency procedure which includes roles, responsibilities and the contact person.

Q4) If a pilot is onboard a ship and level 2 or 3 is declared by a flag state, do we get rid of the pilot or do we keep him onboard?

A4) MSC 80 Circ 1156 gives guidance on the access of public authorities, emergency response services and pilots on board ships to which SOLAS chapter XI-2 and the ISPS code apply. It should be noted that safety of the ship is the top priority. The Captain of the ship has the final say taking safety into consideration.

Q5) How long do we need to renew declaration of the security level?

A5) When the CG raises the security level to the next higher stage. Perhaps you should follow how Palembang Port communicates the security level to all staff and visitors in the port- by having the flag and windsock flying with the respective color and security level.

Q6) How do you propose we protect against a domestic vessel or one that is below 300 GT since such vessels do not need to install the AIS system?

A6) This is something that CG is studying now. Access control from seaward is important. Unauthorized sampan should not be allowed near international ships berthed at the port facility. There should be a response patrol boat on standby for activation if the need arises. Port Administrator should encourage vessels to report any suspicious craft or activities. In Singapore, we have the harbour craft transponder systems for vessels below 300 GT. This technology is inexpensive and uses GPRS technology.

3. Risk Analysis & Vulnerability Assessment (Kado)

Q1) How do you appropriately position the CCTV monitors?

A1) Provided that the container terminal is not too large, cameras should be positioned at the 4 corners of the facility and should be focused on the Ship/Port interface, fence, and restricted area.

Q2) Where should the CCTV monitoring system be installed.

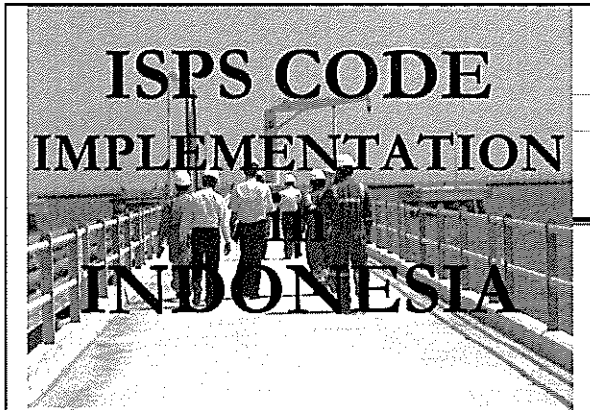
A2) Basically in the container terminal, hazardous materials terminal, and the passenger terminal.

Q3) What are the specifications of a CCTV camera?

A3) The specs vary. Basic camera has a range of 350 m.

5. Implementation and Management of Port Facility Security Measures (Hiura)

No question



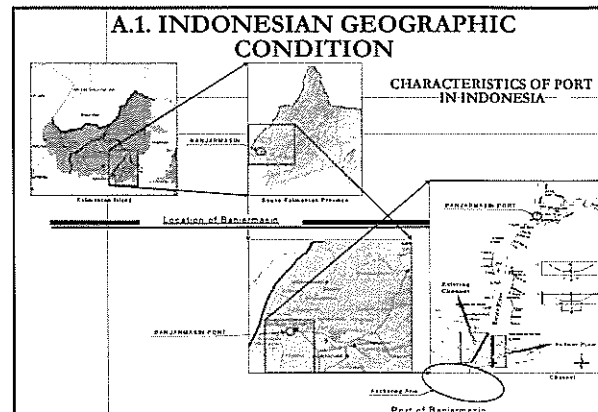
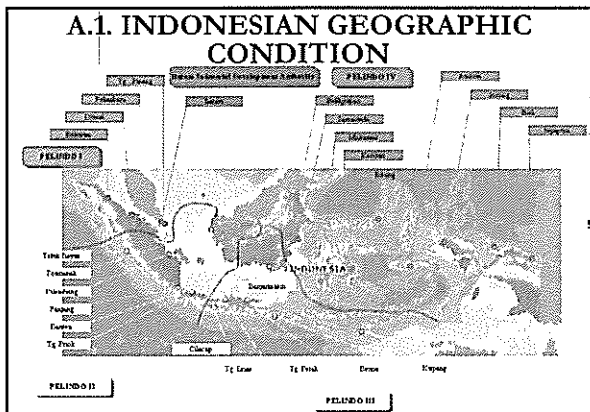
Problem and Future Plan
 By
Directorate of Guard and Rescue
Directorate General of Sea and Transportation

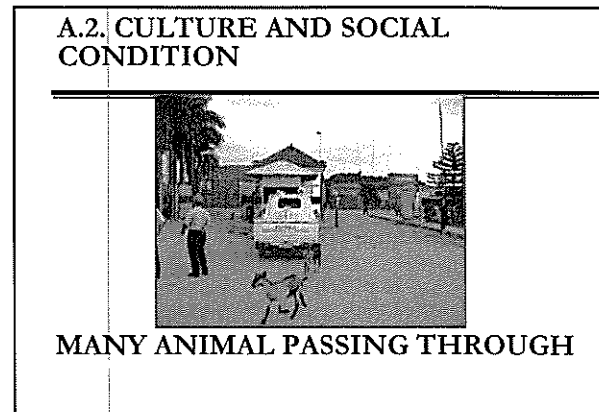
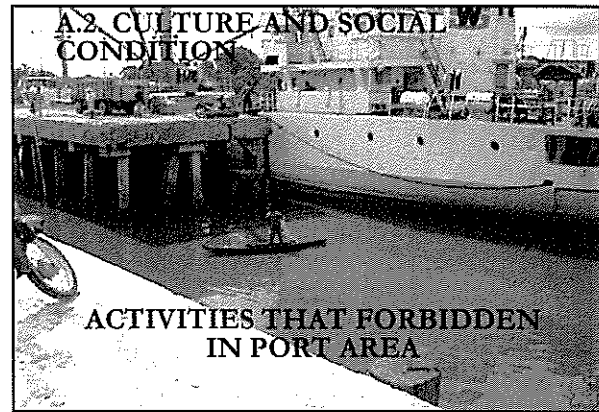
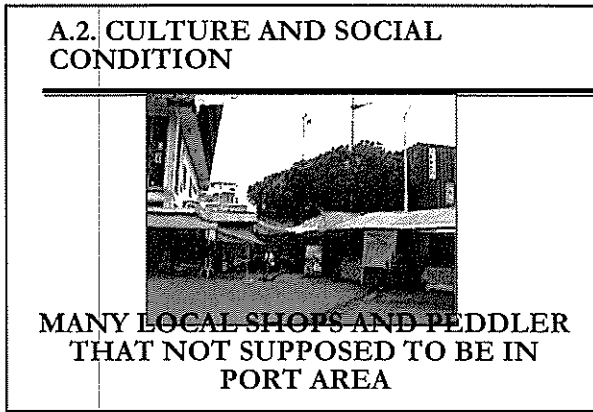
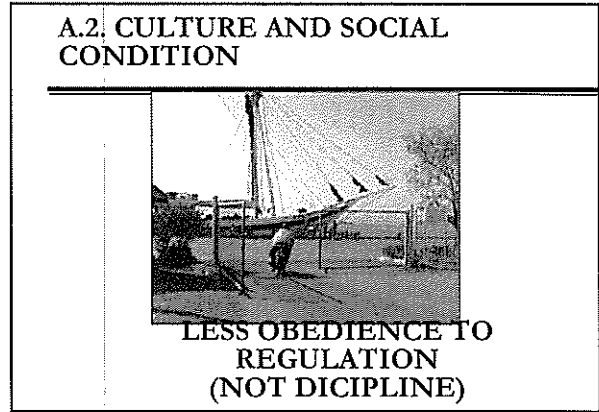
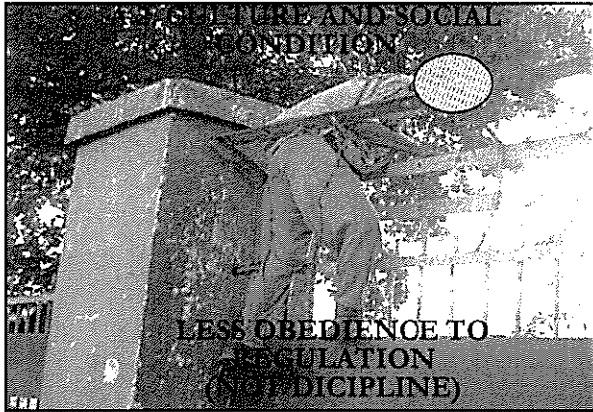
SYSTEMATICS

- A. Introduction**
- B. Pre-Implementation**
- C. Realization**
- D. Future Plan**

A. INTRODUCTION

- A.1. Indonesian Geographic**
- A.2. Condition of Social, Culture, Economic, and Politics**
- A.3. Technology and System**
- A.4. Human Resources**
- A.5. Fund**
- A.6. Other**





A.3. TECHNOLOGY AND SYSTEM

Most of port (especially public port) still using old technology, even using manual system for the operational.

A.4. HUMAN RESOURCES

General Problem (cliché)

A.5. FUND

General Problem (cliché)

B.1. PROBLEM

- There is some of government agency that handles port security.
- Plenty of port for international trading.
- Budget for supplying port security facility is finite/ limited.
- Organization which responsible for security in the port is not establish yet.
- Entrance Channel for international ship and domestic ship is limited (become one).

B.1. PROBLEM

Government Agency in Port Area

Government: Sailing Safety (safety)

Custom
Immigration
Quarantine
Security

SECURITY

Service Company

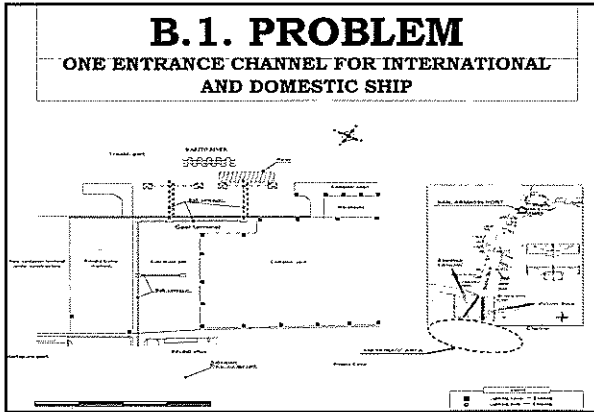
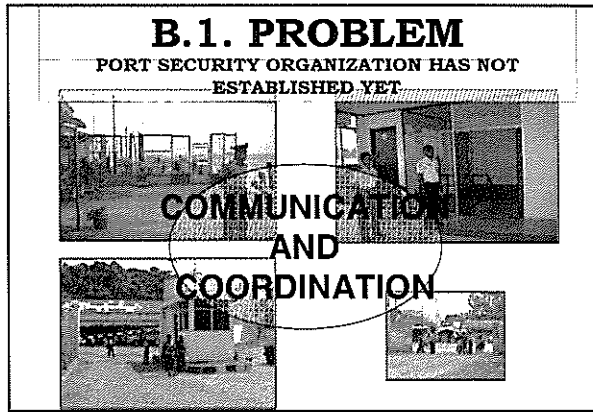
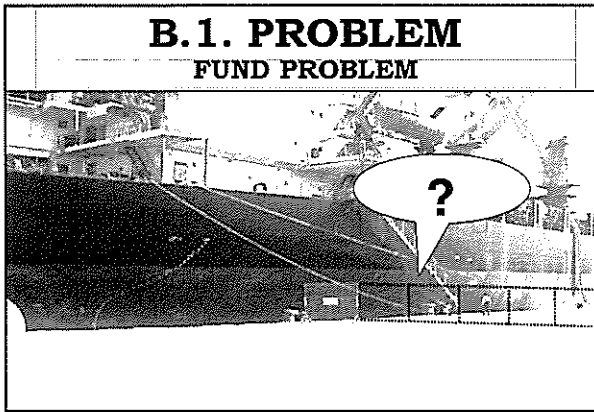
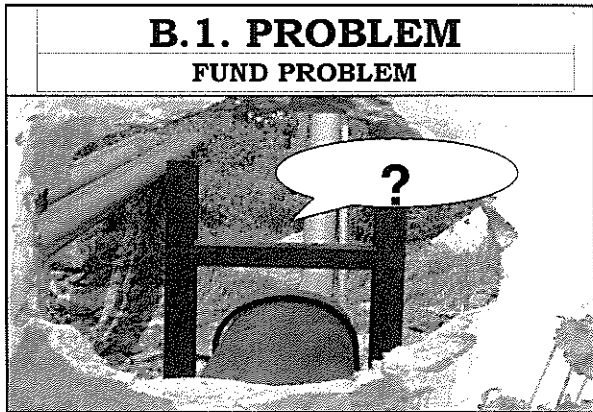
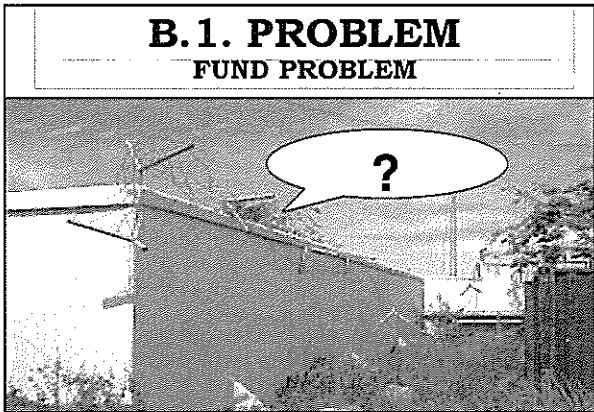
Main : ship service; cargo and passenger

Supporting : Warehouse, land, etc

B.1. PROBLEM

TOTAL OF PORTS IN INDONESIA

TYPE OF PORT	OPEN, INTERNATIONAL TRADING	DOMESTIC	TOTAL
1. PUBLIC PORT			
a. UPT	10	513	523
b. PT PELINDO	85	56	111
2. SPECIAL PORT	46	1.366	1,412
TOTAL	141	1.905	2,046



B.2. SOCIALIZATION

In order to introducing ISPS Code to officer and related party, some of ISPS Code socialization has performed by DGST or with other party (international and domestic), as follow:

ISPS CODE SOCIALIZATION

A. With Expert Party / International

- ISPS Code Workshop – IMO – IMO (Jakarta & Surabaya)
Cooperation between DGST and IMO
Participants: Stake Holder, Port Administration and related party.
- ISPS Code Workshop – Singapore
Cooperation DGST and MPA Singapore in Jakarta.
Participants: Stake Holder, Port Administration and Related party.
Cooperation DGST and BPMIGAS (3 generation) in Surabaya.
- ISPS Code Workshop – Australia (Jakarta, Ktr Pusat)
Cooperation DGST and Australian Transportation Department
Participants: DGST, Custom, and related party
- ISPS Code One Day Seminar – Japan (Jakarta)
Cooperation DGST and Japan COAST Guard (JCG)

B. With Expert Party / Domestic

- ISPS Code One Day Seminar – Jakarta (July 2004)
 - ✦ Cooperation DGST and INNI
 - ✦ Participants: Stake Holder, Port administration, Port Office, and related party.
- Workshop PFSO ISPS Code – BATAM (March 2004)
 - ✦ Cooperation DGST and Batam Port Administration
 - ✦ Participants: Stake Holder, Port Administration, Port Office, and related party.
- Workshop PFSO ISPS Code – BANTEN (March 2004)
 - ✦ Cooperation DGST and Banten Port Administration
 - ✦ Participants: Stake Holder, Port Administration, Port Office, and related party.
- ISPS Code One Day Seminar – Jakarta (March 2004)
 - ✦ Cooperation DGST and LITBANG Transportation Department.
 - ✦ Participants: Stake Holder, Port Administration, Port Office, RSO and related party.

continued ...

- Workshop PFSO ISPS Code – BALIKPAPAN (April 2004)
 - ✦ Cooperation DGST and Balikpapan Port Administration
 - ✦ Participants: Stake Holder, Port Administration, Port Office, and related party.
- Workshop PFSO ISPS Code – PALEMBANG (April 2004)
 - ✦ Cooperation DGST and Palembang Port Administration
 - ✦ Participants: Stake Holder, Port Administration, Port Office, and related party.
- Workshop PFSO ISPS Code – BANTEN (May 2004)
 - ✦ Cooperation DGST and Fleet of PLP Tg. Priok
 - ✦ Participants: UPT DGST and related party.

B.3. POLICY

1. Decree of Ministry of Transportation KM.33/2003, 14 August 2003 about the validity of SOLAS Amendment 1974 about ISPS Code in Indonesia zone.
2. Decree of Ministry of Transportation KM. 3/2004 about DGST assignment as Designated Authority for ISPS Code implementation

INSTRUCTION FOR ISPS CODE IMPLEMENTATION

1. Decree of Directorate General of Sea and Transportation Number KL. 93/1/3-04, 12 February 2004 about Guidance of Organization Decree that accredited (RSO).
2. Decree of Directorate General of Sea and Transportation Number KL. 93/2/1-04, 14 May 2004, about Assignment for Director of Guard and Rescue to responsible for ISPS Code Implementation.

CIRCULAR LETTER: IMPLEMENTATION GUIDELINE

- a. SE – Number UM-48/6/16-04, 19th March 2004, about Port Security Officer Establishment.
- b. SE – Number KL.933/3/7/DV-04 30th June 2004, about DoS Working System and discipline of people and vehicle entrance/exit on the port.
- c. SE – Number UM-933/3/20/DV-04 on 9th July 2004, about Pre-Arrival Notification of Ship Security Implementation and Port State Control Working System.
- d. Mapel of DGST No. 327/Phbl-04, on 24th December 2004, about utilization of freq.156.675 MHz (Channel 73).
- e. SE – No. KL.933/7/8/DV-04, on 27th September 2004, about Preparation of Port Verification/ Port and Ship Facility.
- f. SE – No. KL.933/1/12/DV-05, on 4th January 2005, about Follow up action In Verification Result of ISPS Code Implementation on ship.
- g. SE – No. KL.933/1/12/DV-05, on 7th April 2005, about Maintenance and Upgrading of ISPS Code Implementation for Port/ Port Facility, which has got SoCPF.

POLICY: RSO REQUIREMENTS

- ♦ Indonesian Legal Company that formed as Limited Corporation which specially established for RSO business.
- ♦ Have the Tax ID Number (NPWP).
- ♦ Have, at least employee as follow:
 - 1 person/ expert in security.
 - 1 person/ expert in shipping and wharves.
 - 1 person/ expert for intelligent agent.
 - 1 person/ expert in risk management.
- ♦ Those experts may only registered in 1 (one) RSO Company.

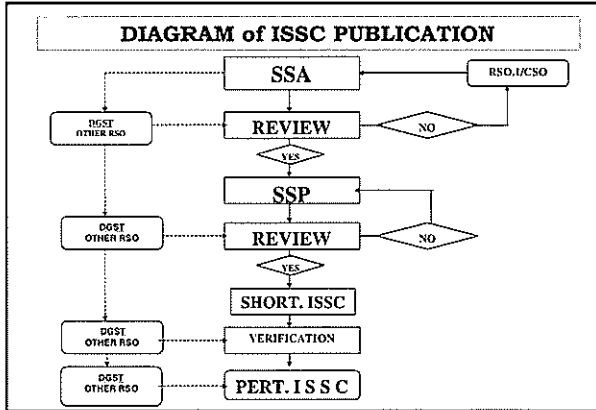
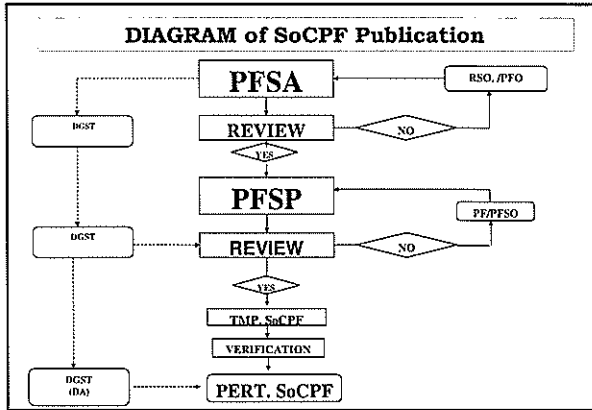
POLICY FOR RSO

1. Perform Security Assessment (SSA and PFSA).
2. Security planning Development (SSP and PFSP)
3. Assessment legalization and ship security planning (SSA and SSP)
4. Verification of Ship Security Planning Implementation (SSP)
5. Publication of International Ship Security Certificate (ISSC)
6. RSO is not allowed to approve an assessment result and ship security planning development (SSA and SSP), which performed or made by RSO itself.
7. RSO authority in Port Facility Security Planning development, only limited to assisting if needed.

PUBLICATION POLICY of ISSC & SoCPF

- 1) Assignment and training for capable officer and have experience in security aspect.
- 2) Perform the security assessment for ship or port facility (SSP/PFSA)
- 3) Review and approval SSA and PFSA
- 4) Making the security planning (SSP/PFSP)

- 5). Review and approval SSP and PFSP
- 6). SSP implementation on the ship and or PFSP in port facility
- 7). SSP implementation to ISPS Code implementation in the ship and port facility
- 8). Certification



B. PRE IMPLEMENTATION

- B.1. Problem
- B.2. Socialization
- B.3. Policy

C. REALIZATION

C.1. ACHIEVEMENT

C.2. PROBLEM

C.1. ACHIEVEMENT

1. Total of Recognized Security Organization (RSO), which has established: 25.
2. Total 196 port facilities have obtained SoCPF.
3. Total 378 ships have obtained ISSC.
4. Port Security Committee (PSC) in every port/ port facility.
5. Delivery Report to IMO.

EXPLANATION ABOUT RSO

With all consideration as explained at first, DGST can not limit RSO amount. Based on data in Directorate of Guard & Rescue, from total 25 RSO, which exist (have work activity) less than 50%. There are many people who interested to be RSO.

Explanation about Total of Port Facility

Details of total 196 ports:

- 25 Public Ports managed by PT. Pelindo
- 172 Special Ports; includes Single Buoy Mooring, Floating Storage Offshore.

Explanation about Total of Port Facility

Based on data in BKI, total of Indonesian ship that must compliance with ISPS Code is 350 ships.

Last position of ship amount, which has fulfilled ISSC neither from DGST or BKI is: 378 ships, so there are more 28 ships over target.

Rest of that number caused by market demand, which are, ships that according to Code is not required, but for safety reason from international ship, by the tenant/ carter, those ships mentioned above must fulfill ISPS Code.

Explanation about Port Security Committee

What is Port Security Committee



C.2. PROBLEM

- ✓ Less attention from related officer.
- ✓ There is mistake or error with application in the field.
- ✓ Less standard quality for security equipment, communication system, fund limitation, human resources.

A. Less Attention From Related Officer

Based on verification result and monitoring on the field, found that:

- ✓ There are still port/ port facility, which serve international ship but has not implemented or fulfill the requirement by ISPS Code.
- ✓ In some ports, Port Security Committee has not organized yet.

B. Mistake/ Error in Implementation

Problem which identified from First Verification (General)

- Misunderstanding
- misinterpretation

DOS, PSC, NON CONVENTION SHIP

- Comply only on the due day

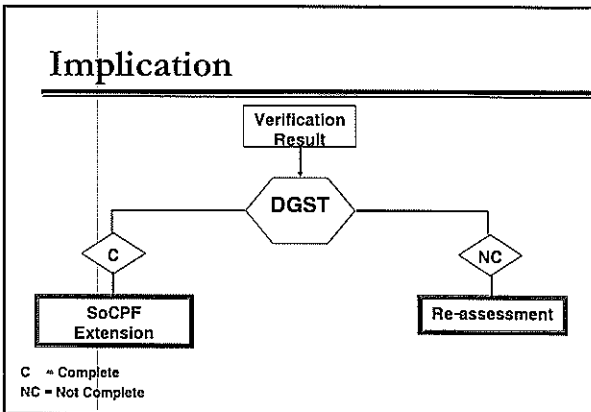
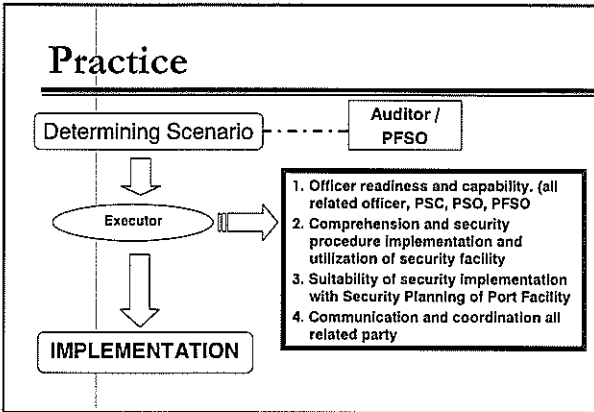
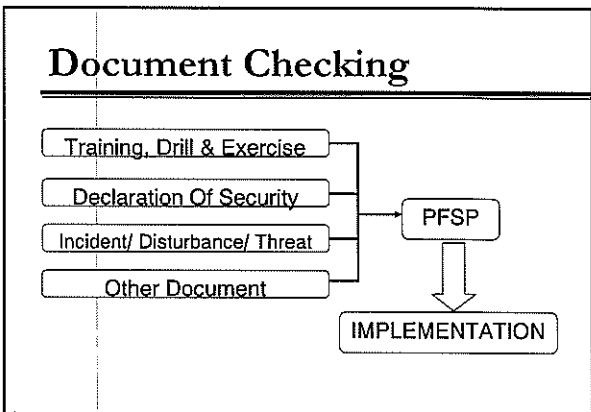
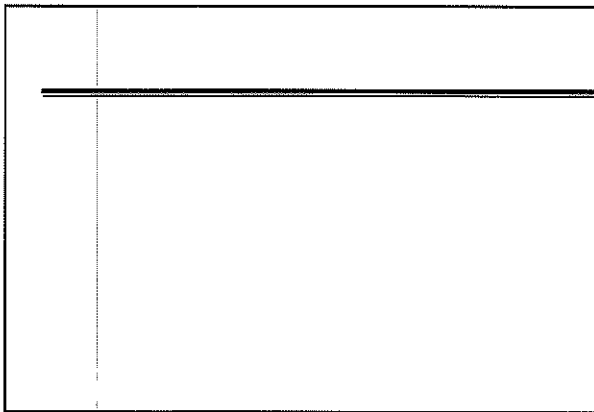
FUTURE PLAN

MECHANISM

- FIRST VERIFICATION
- SECOND VERIFICATION
- THIRD VERIFICATION
- FOURTH VERIFICATION

Result of Second Verification/ Intermediate and

- ### Material of Second Verification/Intermediate
- Re-examine about recent condition.
 - Physical condition and operational
 - PFSP / SSP and amendment (if available).
 - Comprehension about CSO, SSO, PFSP and other officer.
 - Document Checking
 - Implementation of Training, Drill and Exercises
 - DoS
 - Incident/ Disturbance/ Threat
 - Practice



Questions & Comments



**Permasalahan
dan
Rencana ke depan**
oleh
DIREKTORAT PENJAGAAN DAN PENYELAMATAN
DIREKTORAT JENDERAL PERHUBUNGAN LAUT

SISTIMATIKA

A. PENDAHULUAN

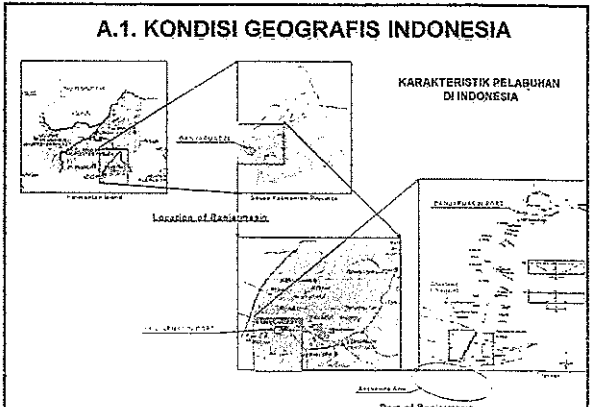
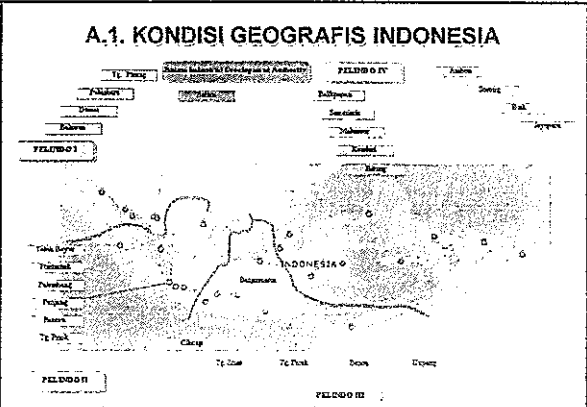
B. PRA IMPLEMENTASI

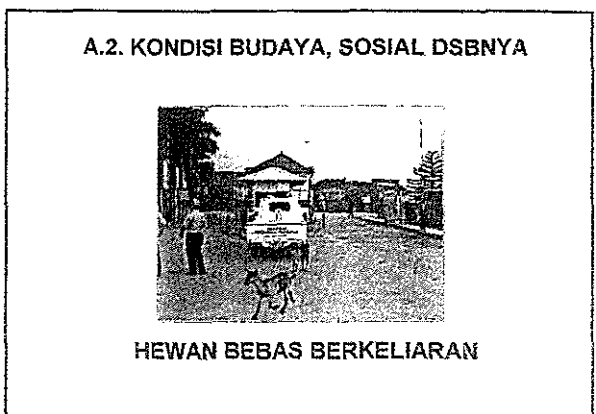
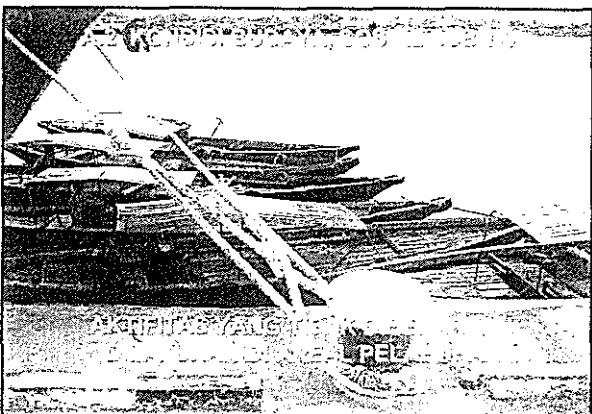
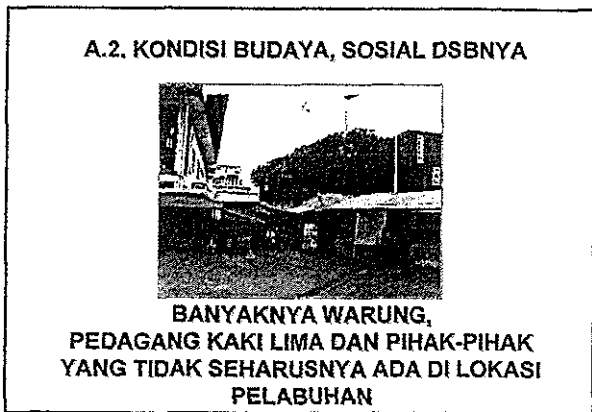
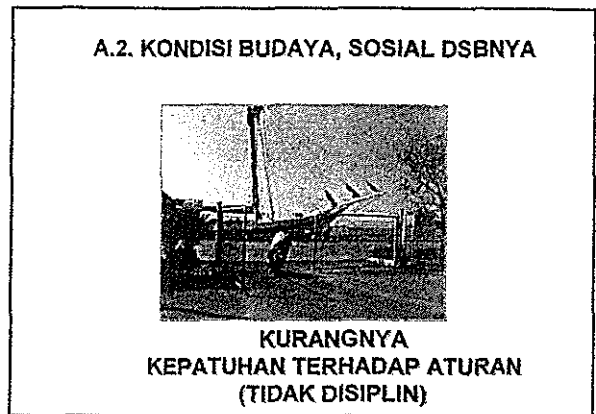
C. REALISASI

D. RENCANA KE DEPAN

A. PENDAHULUAN

A.1. Geografis Indonesia
A.2. Kondisi Sosial, Budaya, Ekonomis dan politik
A.3. Teknologi dan sistem yang digunakan
A.4. Sumber daya manusia
A.5. Dana
A.6. Lainnya





A.3. TEKNOLOGI DAN SISTEM ...

Sebagian besar pelabuhan (khususnya pelabuhan umum) masih menggunakan teknologi yang sudah ketinggalan, bahkan ada yang menggunakan sistem manual untuk operasionalnya

A.4. SUMBER DAYA MANUSIA

Masalah umum (klise)

A.5. DANA

Masalah umum (klise)

B.1. KENDALA

- TERDAPAT BEBERAPA INSTANSI YANG MENANGANI PENGAMANAN PELABUHAN.
- JUMLAH PELABUHAN YANG TERBUKA UNTUK PERDAGANGAN LUAR NEGERI CUKUP BANYAK.
- ANGGARAN UNTUK PENYEDIAAN FASILITA PENGAMANAN PELABUHAN TERBATAS.
- ORGANISASI YANG BERTANGGUNG JAWAB TERHADAP PENGAMAN DI PELABUHAN BELUM DIBENTUK.
- ALUR MASUK UNTUK KAPAL LUAR NEGERI DAN DALAM NEGERI TERBATAS (MENJADI SATU).

B.1. KENDALA

Instansi di Areal Pelabuhan

Pemerintahan :

KESELAMATAN PELAYARAN (SAFETY)
BEA DAN CUKAI (CUSTOM)
IMIGRASI (IMIGRATION)
KARANTINA (QUARANTINE)
KEAMANAN DAN KETERTIBAN (SECURITY)

Pengusahaan Jasa (Service)

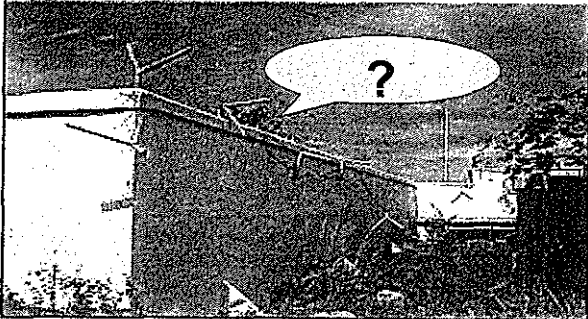
POKOK : PELAYANAN KAPAL, BARANG
DAN PENUMPANG
PENUNJANG : PERSEWAAN GUDANG, LAHAN
DAN LAIN-LAIN

B.1. KENDALA

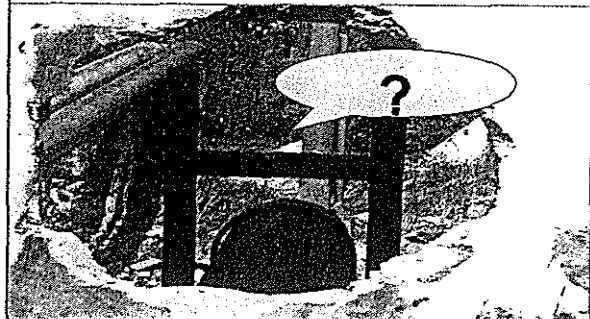
TOTAL JUMLAH PELABUHAN DI INDONESIA

JENIS PELABUHAN	TERBUKA PERDAG LUAR NEGERI	DALAM NEGERI	TOTAL
1. PELAB. UMUM			
a. UPT	10	513	523
b. PT PELINDO	85	58	111
2. PELB. KHUSUS			
TOTAL	48	1.386	1.412
	141	1.905	2.046

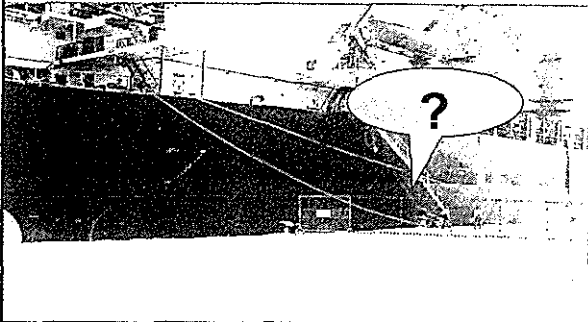
B.1. KENDALA
Masalah Dana



B.1. KENDALA
Masalah Dana



B.1. KENDALA
Masalah Dana



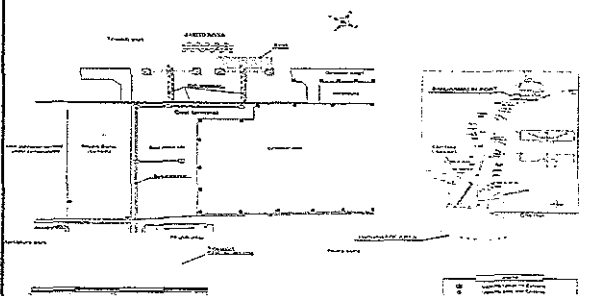
B.1. KENDALA

Belum Terbentuk Organisasi Pengamanan Pelabuhan



B.1. KENDALA

Satu Alur Masuk untuk Kapal Internasional dan Domestik



B.2. SOSIALISASI

DALAM RANGKA MEMPERKENALKAN ISPS CODE KEPADA APARAT DAN PIHAK-PIHAK TERKAIT, SEJUMLAH SOSIALISASI ISPS CODE TELAH DISELENGGARAKAN OLEH DITJEN HUBLA SENDIRI ATAU DENGAN PIHAK LAIN (LUAR DAN DALAM NEGERI), DIANTARANYA :

SOSIALISASI ISPS CODE

A. Dengan Pihak/Expert Luar Negeri

- Workshop ISPS Code - IMO (Jakarta & Surabaya)
Kerjasama Ditjen Hubla dan IMO
Peserta : Stake Holder, Adpel, Kanpel dan pihak terkait
- Workshop ISPS Code - Singapura
 - Kerjasama Ditjen Hubla dan MPA Singapore di Jakarta
Peserta : Stake Holder, Adpel, Kanpel dan pihak terkait
 - Kerjasama Ditjen Hubla dan BPMIGAS (3 angkatan) di Surabaya
Peserta : Pelsus dibawah kontrol BPMIGAS
- Workshop ISPS Code - Australia (Jakarta, Ktr Pusat)
Kerjasama Ditjen Hubla dan Dept. Transportasi Australia
Peserta : Ditjen Hubla, Bea Cukai dan pihak terkait
- Seminar sehari ISPS Code - Jepang (Jakarta)
Kerjasama Ditjen Hubla dan Japan Coast Guard (JCG)
Peserta : Stake Holder, Adpel, Kanpel dan pihak terkait

B. Dengan Pihak/Expert Dalam Negeri

- Seminar sehari ISPS Code - Jakarta (Juli 2004)
Kerjasama Ditjen Hubla dan INNI
Peserta : Stake Holder, Adpel, Kanpel dan pihak terkait
- Workshop PFSO ISPS Code - BATAM (Maret 2004)
Kerjasama Ditjen Hubla dan Adpel Batam
Peserta : Stake Holder, Adpel, Kanpel dan pihak terkait
- Workshop PFSO ISPS Code - BANTEN (Maret 2004)
Kerjasama Ditjen Hubla dan Adpel Banten
Peserta : Stake Holder, Adpel, Kanpel dan pihak terkait
- Seminar sehari ISPS Code - Jakarta (Maret 2004)
Kerjasama Ditjen Hubla dan LITBANG DEPHUB
Peserta : Stake Holder, Adpel, Kanpel, RSO dan pihak terkait

lanjutan ...

- Seminar sehari ISPS Code - Jakarta (Maret 2004)
Kerjasama Ditjen Hubla dan LITBANG DEPHUB
Peserta : Stake Holder, Adpel, Kanpel, RSO dan pihak terkait
- Workshop PFSO ISPS Code - BALIKPAPAN (April 2004)
Kerjasama Ditjen Hubla dan Adpel Balikpapan
Peserta : Stake Holder, Adpel, Kanpel dan pihak terkait
- Workshop PFSO ISPS Code - PALEMBANG (April 2004)
Kerjasama Ditjen Hubla dan Adpel Palembang
Peserta : Stake Holder, Adpel, Kanpel dan pihak terkait
- Workshop PFSO ISPS Code - Jakarta (Mei 2004)
Kerjasama Ditjen Hubla dan Armada PLP Tg. Priok
Peserta : UPT Ditjen Hubla dan pihak terkait

B.3. KEBIJAKAN

1. Keputusan Menteri Perhubungan KM. 33/2003 tanggal 14 Agustus 2003 tentang Pemberlakuan Amandemen SOLAS 1974 tentang ISPS Code di wilayah Indonesia.
2. Keputusan Menteri Perhubungan KM. 3/2004 Tahun 2004 tentang Penunjukan Direktur Jenderal Perhubungan Laut sebagai Designated Authority Pelaksanaan ISPS Code.

PETUNJUK PELAKSANAAN ISPS CODE

1. Keputusan Direktur Jenderal Perhubungan Laut Nomor KL. 93/II/3-04 tanggal 12 Februari 2004 tentang Pedoman Penetapan Organisasi yang diakui (RSO).
2. Keputusan Direktur Jenderal Perhubungan Laut Nomor KL. 93/2/1-04 tanggal 14 Mei 2004 tentang Penunjukan Direktur Penjagaan dan Penyelamatan Sebagai penanggung Jawab implementasi ISPS Code.

SURAT EDARAN : PEDOMAN IMPLEMENTASI

- a. SE - Nomor UM-48/16-04 tanggal 19 Maret 2004, perihal Pembentukan Port Security Committee.
- b. SE - Nomor KL.933/7/DV-04 tanggal 30 Juni 2004, perihal Tata Cara DoS dan penertiban masuk/keluar orang, kendaraan di pelabuhan.
- c. SE - Nomor UM-933/3/20/DV-04 tanggal 9 Juli 2004, perihal Penerapan Pre-Arrival Notification of Ship Security dan Tata Cara Port State Control.
- d. Mapel Dirjen Hubla no. 327/Phbl-04 tanggal 24 Desember 2004 tentang penggunaan freq.156.675 MHz (Channel 73)
- e. SE No. KL.933/7/8/DV-04 tanggal 27 September 2004 tentang Persiapan Verifikasi Pelabuhan/Fasilitas Pelabuhan dan Kapal.
- f. SE No. KL.933/1/12/DV-05 tanggal 4 Januari 2005 tentang Tindaklanjut Hasil Verifikasi Penerapan ISPS Code pada kapal.
- g. SE No. KL.933/2/1/DV-05 tanggal 7 April 2005 tentang Pemeliharaan dan Peningkatan Penerapan ISPS Code bagi Pelabuhan/Fasilitas Pelabuhan yang telah memperoleh SoC/PF

KEBIJAKAN : SYARAT MENJADI RSO

- ✦ Berbadan hukum Indonesia yang berbentuk Perseroan Terbatas (PT) dan/atau Koperasi yang didirikan khusus untuk usaha RSO.
- ✦ Memiliki Nomor Pokok Wajib Pajak (NPWP)
- ✦ Memiliki sekurang-kurangnya tenaga kerja sebagai berikut :
 - 1 orang tenaga ahli dibidang pengamanan/security
 - 1 orang tenaga ahli dibidang perkapalan dan kepelabuhanan
 - 1 orang ahli dibidang intelijen
 - 1 orang ahli dibidang manajemen resiko
- ✦ Tenaga ahli tersebut hanya dapat didaftarkan dalam 1 (satu) perusahaan RSO.

KEBIJAKAN UNTUK RSO

1. Melaksanakan penilaian keamanan (SSA dan PFSA).
2. Pengembangan perencanaan keamanan (SSP dan PFSP).
3. Pengesahan penilaian dan perencanaan keamanan kapal (SSA dan SSP).
4. Verifikasi penerapan perencanaan keamanan kapal (SSP)
5. Penerbitan Sertifikat Keamanan Kapal Internasional atau International Ship Security Certificate (ISSC).
6. RSO tidak dibenarkan untuk menyetujui suatu hasil penilaian dan pengembangan perencanaan keamanan kapal (SSA dan SSP) yang dilaksanakan atau dibuat oleh RSO bersangkutan.
7. Kewenangan RSO dalam pengembangan perencanaan keamanan fasilitas pelabuhan (PFSP) hanya sebatas memberikan asistensi jika diperlukan.

KEBIJAKAN PENERBITAN ISSC & SoCPF

- 1). Penunjukan dan pelatihan petugas yang dianggap cakap dan memiliki pengalaman dalam bidang keamanan : (CSO, SSO/PFSO)
- 2). Melakukan penilaian keamanan terhadap kapal dan atau fasilitas pelabuhan (SSA/PFSA)
- 3). Kaji ulang (review) dan persetujuan SSA dan PFSA
- 4). Pembuatan perencanaan keamanan (SSP/PFSP)
- 5). Kaji ulang (review) dan persetujuan (approval) SSP dan PFSP
- 6). Implementasi SSP di kapal dan atau PFSP di fasilitas pelabuhan
- 7). Pelaksanaan Verifikasi terhadap penerapan ISPS Code di kapal dan fasilitas pelabuhan.
- 8). Sertifikasi ;

DIAGRAM ALIR PENERBITAN SoCPF

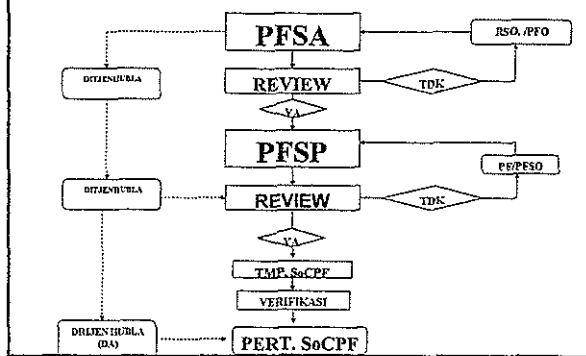
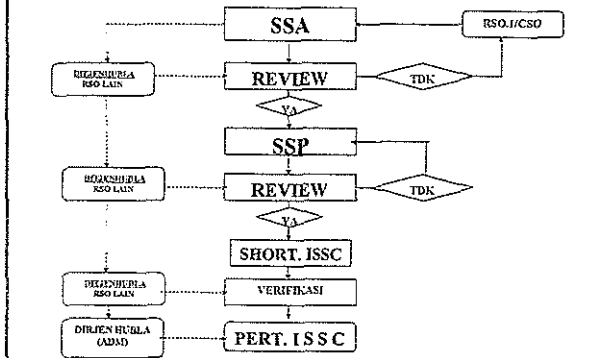


DIAGRAM ALIR PENERBITAN ISSC



B. PRA IMPLEMENTASI

- B.1. Kendala
- B.2. Sosialisasi
- B.3. Kebijakan

C. REALISASI

C.1. PENCAPAIAN PEMENUHAN

C.2. PERMASALAHAN YANG DITEMUI

C.1. PENCAPAIAN PEMENUHAN

1. Total jumlah Recognized Security Organization (RSO) yang telah ditetapkan : 25
2. Total 196 fasilitas pelabuhan telah memperoleh SoCPF
3. Total 378 Kapal telah memperoleh ISSC
4. Pembentukan Komite Keamanan Pelabuhan (Port Security Committee- PSC) pada setiap pelabuhan/fasilitas pelabuhan.
5. Penyampaian Laporan ke IMO

Penjelasan mengenai RSO

Dengan berbagai pertimbangan sebagaimana telah dijelaskan pada awalnya, maka Ditjen Hubla tidak dapat membatasi jumlah RSO.

Berdasarkan data pada Dit. GAMAT (HUBLA), dari total 25 RSO, yang eksis (memperoleh pekerjaan) tidak mencapai 50%-nya.

Peminat untuk menjadi RSO masih tetap ada

Penjelasan mengenai Jumlah Fasilitas Pelabuhan

Rincian dari total 196 fasilitas pelabuhan :

- 25 Pelabuhan Umum yang dikelola oleh PT. PELINDO
- 172 Pelabuhan Khusus; termasuk didalamnya Single Buoy Mooring, Floating Storage Offshore

Penjelasan mengenai Jumlah Fasilitas Pelabuhan

Berdasarkan data BKI, jumlah kapal berbendera Indonesia yang harus memenuhi ISPS Code adalah 350 kapal.

Posisi terakhir kapal yang telah memperoleh ISSC baik dari Ditjen Hubla atau BKI adalah : 378 kapal, dengan demikian ada kelebihan 28 kapal (melibiki target).

Kelebihan angka tersebut disebabkan karena permintaan pasar, dimana kapal-kapal yang menurut Code tidak dipersyaratkan namun karena alasan keamanan dari kapal asing maka oleh penyewa/carter kapal-kapal dimaksud harus memehuni ISPS Code.

Penjelasan mengenai Komite Keamanan Pelabuhan

What is Port Security Committee

21

C.2. PERMASALAHAN

- ✓ Kurangnya perhatian dari aparat terkait
- ✓ Adanya kesalahan atau kekeliruan dalam penerapan dilapangan
- ✓ Rendahnya standar peralatan keamanan, sistem komunikasi, keterbatasan dana, sumber daya manusia

A. Kurangnya Perhatian dari Aparat terkait

Berdasarkan hasil verifikasi dan pemantauan dilapangan ditemukan bahwa :

- ✦ Masih ada pelabuhan/fasilitas pelabuhan yang dalam operasionalnya melakukan pelayanan terhadap kapal-kapal pelayaran internasional tetapi belum menerapkan atau belum memenuhi ketentuan yang dipersyaratkan oleh ISPS Code
- ✦ Belum terbentuknya Komite Keamanan Pelabuhan (Port Security Committee) pada beberapa pelabuhan.

B. Kekurangan/Kekeliruan dalam Penerapan

Permasalahan yang teridentifikasi dari Verifikasi Pertama (Umum)

- Salah pengertian (mis-understanding)
- Salah penafsiran (mis-interpretation)
DOS, PSC, NON CONVENTION SHIP
 - Comply hanya pada hari "H"

RENCANA KE DEPAN

MEKANISME

- VERIFIKASI PERTAMA
(First Verification)
 - VERIFIKASI KEDUA
(Second Verification)
 - VERIFIKASI KETIGA
(Third Verification)
 - VERIFIKASI KEEMPAT
(Fourth Verification)

Hasil Verifikasi Pertama

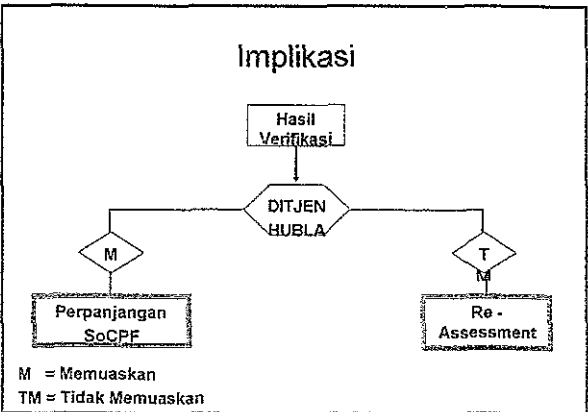
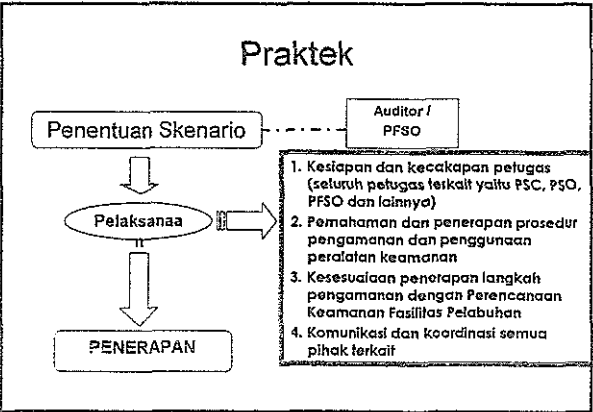
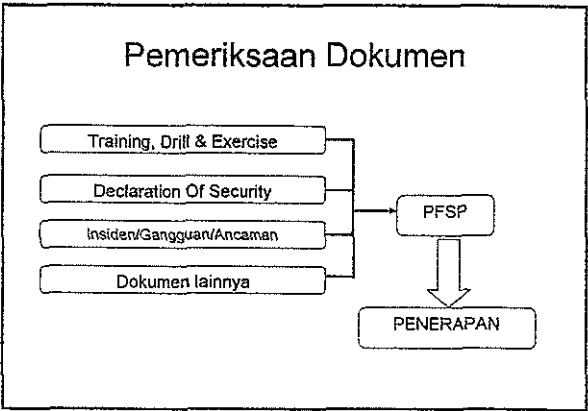
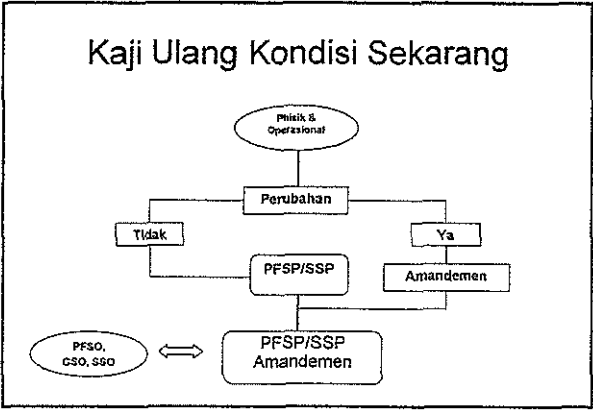
PELABUHAN / KAPAL

COMPLY

- Fisik
- Operasional
- Penerapan

Hasil Verifikasi Ke-Dua/Intermediate dan

- ### Materi Verifikasi ke-Dua/Intermediate
- Kaji ulang terhadap kondisi sekarang
 - PFSP/SSP dan amandemen (jika ada)
 - Pemahaman CSO, SSO, PFSO dan petugas lain
 - Pemeriksaan Dokumen (Arsip/Catatan)
 - Pelaksanaan Training, Drill dan Exercises
 - DoS
 - Insiden/Gangguan/Ancaman
 - Praktek
 - Kondisi Fisik dan Operasional



Questions & Comments

JICA - DGST Workshop ISPS Code

Outline of Port Security Improvement Strategy

JICA Study Team on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

1. Comprehensive Security Measures

In addition to security measures by ISPS Code

- Increasing awareness about port security
 - To have clear awareness about security
 - To carry out their duties surely and steadily
- Making clear the responsibility
 - Security Level 1: PFSO (PELINDO)
 - Security Level 2: PSC-PSO (KPLP)
 - Security Level 3: PSC
- Enlightening residents and stake holders

JICA - DGST Workshop ISPS Code

1. Comprehensive Security Measures

- Introduction of optimum transport security system
 - Container Seal
 - Reinforced hinges of container door
 - To open doors of an empty container & to check inside
 - X-ray device to scan containers
- Cooperation with other relevant organizations
 - As to containers : Customs
 - As to international passenger: Immigration & Police

JICA - DGST Workshop ISPS Code

1. Comprehensive Security Measures

- Appropriate education and training
 - Practical training: Drills & Exercises
- Sharing of latest security information
 - PFSO ⇒ PSO ⇒ PSC ⇒ DGST
 - Establishment of system for circulation of information obtained outside among relevant security officials
- Security of information on international cargo
 - Security regulation to handle the information
 - Regularly check of the handling of the information
- Formulation of Implementation Plan (Action Plan) on port security improvement strategy

JICA - DGST Workshop ISPS Code

2. Identification of International Public Ports where security measures are to be implemented

- Implementation of PFSA & PFSP
 - All port facilities receiving international ships in International Hub Ports and International Ports
 - Port facilities receiving international ships in National Ports which satisfies the following conditions:
 - +International cargo ship: more than 12 ships/year
 - +International passenger ship: more than 1 ship/year

For other facilities which do not satisfy the above conditions, quasi PFSP and DoSs are applied.

JICA - DGST Workshop ISPS Code

Port Hierarchy in Indonesia

Port Hierarchy	Number of Ports	26 Study Ports
International Hub Port	2	Tanjung Priok, Tanjung Perak
International Port	18	Belawan, Dumai, Teluk Bayur, Palembang, Panjang, Pontianak, Banten, Tg. Emas, Cilacap, Bena, Kupang, Banjarmasin, Balikpapan, Bitung, Makassar, Sorong (16)
National Port	245	Pekanbaru, Tg. Pinang, Batam, Kendari, Samarinda, Ambon, Biak, Jayapura (8)
Regional Port	139	
Local Port	321	

JICA - DGST Workshop ISPS Code

3. Prioritization on Implementation of Port Security Measures

- Grouping of port facilities
 - Group A: Strict security measures are needed. Container berths, liner passenger berths, exclusive hazardous material berths
 - Group B: Other facilities. Trampler passenger berths, hazardous material berths excluding above, bulk material berths, multi purpose berths

JICA - DGST Workshop ISPS Code

3. Prioritization on Implementation of Port Security Measures

Necessity of PFSP in Domestic Port

Group	No. of international ship calling per year	0	1 – 11	More than 12
A	Container berth	-	Quasi PFSP	PFSP
	Hazardous material berth	-	PFSP	PFSP
	Liner passenger berth	-	PFSP	PFSP
B	Tramper passenger berth	-	PFSP	PFSP
	Conventional cargo berth	-	Quasi PFSP	PFSP

JICA - DGST Workshop ISPS Code

3. Prioritization on Implementation of Port Security Measures

- Standard for Group A & B security facilities
 - Group A
 - Fence: Fixed type
 - Monitoring: Round-the-clock monitoring by CCTV except the time when no ship and no cargo are at berth
 - Patrolling: Check regularly in the restricted area by security guards
 - Others: X-ray inspection apparatus (for liner passenger berths)

JICA - DGST Workshop ISPS Code

3. Prioritization on Implementation of Port Security Measures

- Standard for Group A & B security facilities
 - Group B
 - Fence: Fixed or movable type
 - Monitoring: Conducted by security guards
 - Put security guards every 300m for fixed fence and every 40m for movable fence
 - Patrolling: Check in the restricted area by security guards
 - One security guard shall be provided for every 80,000 m2

JICA - DGST Workshop ISPS Code

3. Prioritization on Implementation of Port Security Measures

Intervals of patrolling at security level 1

International Ship	Group A	Group B
Berthing	Around 4 hr	Around 4 – 8 hr
Others	Around 4 – 8 hr	Around 8 hr

Intervals of patrolling at security level 2

International Ship	Group A	Group B
Berthing	Around 2 hr	Around 2– 4 hr
Others	Around 2 – 4 hr	Around 4 hr

JICA - DGST Workshop ISPS Code

3. Prioritization on Implementation of Port Security Measures

Intervals of patrolling at security level 3

International Ship	Group A	Group B
Berthing	Patrol in full time	Patrol in full time
Others	Patrol in full time	Patrol in full time

JICA - DGST Workshop ISPS Code

3. Prioritization on Implementation of Port Security Measures

Standard number of identity check at security level 1 - 3

Security Level	Contents
1	<ul style="list-style-type: none"> • Conformation of ID possession: all persons • Check ID photo and face for 5-10 out of every 100 persons • Conduct at least once in a day
2	<ul style="list-style-type: none"> • Conformation of ID possession: all persons • Check ID photo and face for 30-50 out of every 100 persons
3	<ul style="list-style-type: none"> • Check ID photo and face for all persons

JICA - DGST Workshop ISPS Code

3. Prioritization on Implementation of Port Security Measures

- Prioritization on port security measures
 - 1st priority: Group A
 - 2nd priority: Group B

Considering the number of int'l ship calls and situation of port use conditions

JICA - DGST Workshop ISPS Code

Group A – Container Terminal

JICA - DGST Workshop ISPS Code

Group A – Liner Passenger Terminal

JICA - DGST Workshop ISPS Code

Group B – Multi Purpose Berth with Fixed Fence

JICA - DGST Workshop ISPS Code


Group B – Multi Purpose Berth with Movable Fence

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

4. Port Security Facilities & Equipment Development Standards

- Restricted area
- Barriers (fence, gate and car stop bar)
- Security lighting facility
- Surveillance camera unit
- Intrusion detection sensor (fence sensor & gate sensor)
- Baggage inspection equipment
- Communication equipment (ship-port facilities, within port facilities and with police/super ordinate organizations)
- Power supply facilities
- Maintenance of port facilities & equipment

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

5. Basic Policy on Port Security System

- DGST
 - Organization buildup, management of security information, communication with PSC, distribution of latest security information
- PSC
 - Confirmation of each member's role and responsibility, effective communication system
- KPLP
 - A central role in port security using close relation with DGSC, water area security
- PELINDO
 - Support of PFSOs

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

6. Declaration of Security

- Declaration of Security is required in the following cases
 - When a ship is operating at a higher security level than the port facility or another ship with which it is going to interface
 - When a ship whose flag state is not a Contracting Government of SOLAS interfaces with a port facility
 - When an international ship interfaces with a port facility for which Port Facility Security Plan has not been formulated
 - When an international ship comes to a port facility through a port which is not compliant with the ISPS Code
 - When a PFSO obtains information on suspicious activity of a coming ship

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

6. Declaration of Security

- Valid duration of DoS (in Japan)
 - Security Level 1: 90 days
 - Security Level 2: 30 days
 - Security Level 3: only one time
- Minimum Retention Period
 - Three (3) years from the date of completion

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

6. Declaration of Security

- Procedure to complete DoS (Example)
 - Before ship's berthing at a port facility, a port facility requests to a ship to complete a DoS and vice versa
 - Both a port facility and a ship coordinate to specify security measures and responsibility each will implement and agree with the security measures during the ship stay at the port facility
 - The ship berths at the port facility
 - After ship's berthing at the port facility, a Port Facility Security Officer and a Master or a Ship Security Officer sign the DoS

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports





JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

7. Basic Policy for Enhancing Educational & Training Organization

- Role-Sharing of ISPS Code Training Organizations
 - BP3IP – Training and Education Agency, MOT
 - Authorized training centre for the conduct of IMO Model PFSO Courses
 - Pertamina Marine Training Center (PMTTC)
 - PMTTC can complement BP3IP for training such as PFSO courses to the private sectors
- RSO
 - RSOs have the resources and contacts to organize PFSO courses on an adhoc basis

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports






jica Japan International Cooperation Agency JICA - DGST Workshop ISPS Code 

8. Preparation of Supporting Tools

- Manual of DoS
- Manuals of PFSA and PFSP
- Commentaries on port security facilities & equipment development standards
- Standard specifications for port security facilities & equipment
- Port security measures examples book
- Port security regulations (draft)
- Procedures of Drills and Exercises
- Action plan on Port Security Improvement Strategy
- Port Security Development Plan

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports






jica Japan International Cooperation Agency JICA - DGST Workshop ISPS Code 

Thank you for your Attention

Terima Kasih

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

Outline of Port Security Facilities development Standard

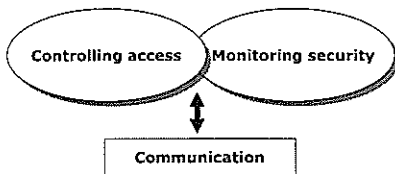
JICA Study-Team
Masaki ONO

Contents

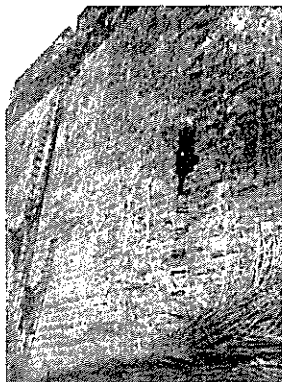
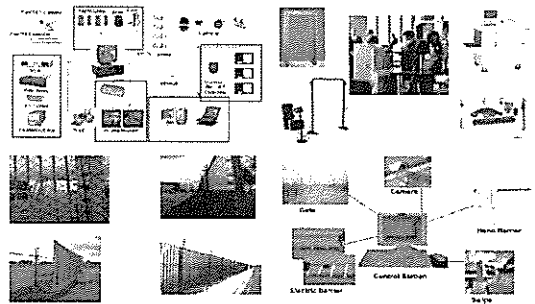
- 1 General
- 2 Port Security Facilities & equipment Technical Standards
 - (1) Barrier
 - (2) Lighting System
 - (3) CCTV Camera System
 - (4) Sensor System
 - (5) Inspection System of Belongings
 - (6) Telecommunication System
 - (7) Power Supply System
- 3 Maintenance of Port Security Facilities
- 4 Question

1 General Background

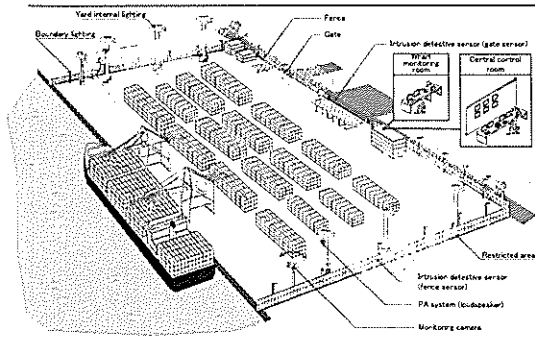
- Controlling access to port facility and monitoring security is a fundamental element of security for any organization.



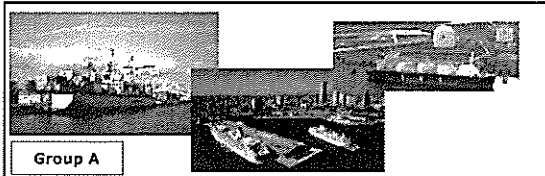
Port Security Facilities & equipment



1 An Overview of the Port Security System



Group A / Group B



Group A



Group B

Port Security Facilities & equipment of each Group

Port Security Facilities and Equipment	Group A		Group B	
	container / hazardous material (Special)	passenger (Line)	Others	passenger
1. Physical Barrier				
1-1 Fence (fixed)	○ (H: 2.4m and over)	○ (H: 2.4m and over)	○ (H: 1.8m and over)	○ (H: 1.8m and over)
1-2 Fence (mobile)				
1-3 Gate	○ (H: 2.4m and over)	○ (H: 2.4m and over)	○ (H: 1.8m and over)	○ (H: 1.8m and over)
1-4 Car-stop bar	○	○		
2. Lighting System (Emergency power source)	○	○	△ (Enhancing the patrol surveillance)	△ (Enhancing the patrol)
3. CCTV Camera System	○	○	△	△

Port Security Facilities and Equipment	Group A		Group B	
	container / hazardous material (Special)	passenger (Line)	Others	passenger
4. Sensor System (Fence Sensor / Gate Sensor)	△	△	△	△
5. Inspection System of Belongings (X-ray inspection device/Metal detector)	-	-	-	△
6. Telecommunications Equipment				
6-1 Ships / Port Facilities	○	○	○	○
6-2 Port Facilities (Public Address System)	○	○	△(CCTV)	△
6-3 Other Security Organizations	○	○	○	○
7. Power Supply System				
7-1 Uninterruptible power supply (UPS)	○	○	△(CCTV)	△(CCTV)
7-2 Emergency power generation facility	△	△	△	△

2 Port Security Facilities & equipment Technical Standards (1) Barrier (Fixed Fences)

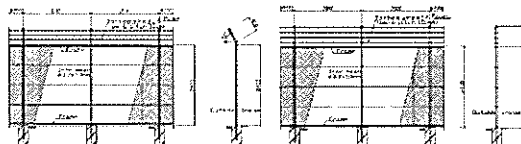
[Functional requirements]

- ① Sufficient height to prevent any person from easily intruding
- ② Sufficient strength and durability to withstand assumed loads
- ③ Wire mesh or grid rod diameter that will not be easily cut
- ④ Structure of a construction that will not allow detour for entry at water edge sections of borders with neighboring land
- ⑤ Signs posted to prohibit any trespassing
- ⑥ Clear zone provided on both sides of fences

[Standard Specifications]

- ① Effective height of 2400 mm or over for Group A facilities and 1800 mm or over for Group B facilities
- ② Spike added on top as overhung outward (length of 450 mm or over, angled 30 deg or over outward and barbed)
- ③ The assumed load is wind load (standard speed of 34 m/sec)
- ④ Mesh of a size (diamond side of 50 mm or less) or grid of a width (50 mm or less) that will not provide foothold
- ⑤ Mesh wire diameter of 3.2 mm or over (without cladding) and grid rod diameter of 6.0 mm or over
- ⑥ Prevention against any curling up, or construction against any crawling under the fence
- ⑦ Fences that are used at port must be highly resistant to corrosion in consideration of salt damage
- ⑧ Intrusion prevention fence must be provided as on large-sized drainage trench that passes across under the fence
- ⑨ Intrusion prevention fence must be provided on structures or communicating passage that pass across over the fence
- ⑩ Standard clear zone should be 3 meters inside the fence and some width on the outside as necessary for the early detection of any unauthorized intrusion.

Fence with correct-direction top guard / Fence with erect top guard



Effective height of fence

- The effective height of fence is calculated at the height except those of top guard and basement, because the basement can function as a step when somebody is going to come over the fence.



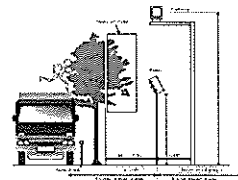
Top guard toward the outside

Effective height of fence
 (The height of fence looks like over 2.4 m. However, the effective height of fence should be calculated from the top of concrete base to the top of fence.)

The height of concrete base should be excluded, because it can be a step. (The thing in front of fence should be removed because this can also be a step.)

Outside the restricted area (road)

Clear Zone



- Both widths of inside and outside clear zone are set at 3 m as a standard. The width of outside clear zone should be over 1.5 m.
- if it is impossible to secure 3 m of clear zone. If it is impossible to secure outside clear zone anyhow, the effective height of fence has to be secured inevitably.

Grid Fence (Improvement)

- Grid fence is mainly applied in Indonesian ports and its interval is 100 mm without top guard.

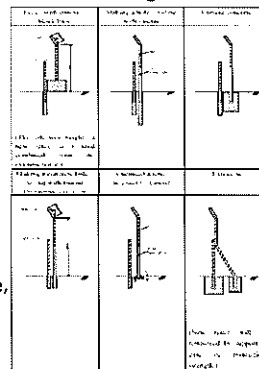
[Improvement plan of existing fence]

- Grid bar should be added between the existing grids to reduce its interval to below 50 mm.
- Correct-direction top guard should be installed on the existing fence.
- There is a wide space between the ground and the lowest edge of the fence. This space should be reduced to below 50 mm by installing the additional horizontal beam.

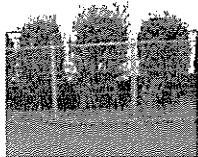


improvement plan of the existing fence

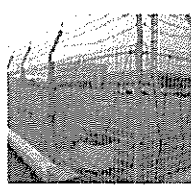
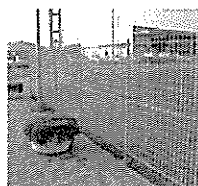
- Net or grid can be used in the whole surface of new fence though net or grid is not needed for its lower half. Barbed wire can be installed in the lower half instead of net or grid.
- The position of new fence is as near as possible from the existing fence not to invade from in-between.
- In case to put new fence apart from the existing fence, over 1.7 m should be away from each other.



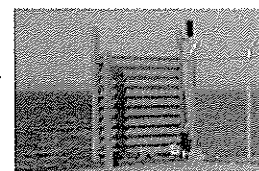
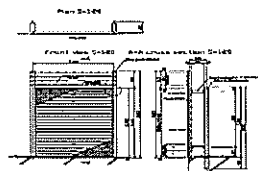
Before improvement



After improvement



Prevention wall from making a detour to avoid a fence



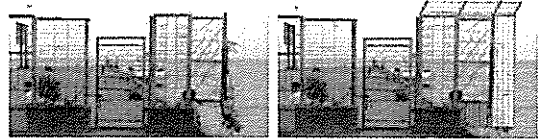
- To set a plat wall along a berth line prevents from making a detour to avoid a fence.
- This advantage is no projection into the sea.

Prevention fence from making a detour to avoid a fence①



- To set a projecting fence into the sea from the berth prevents from making a detour to avoid a fence.
- It will be more effective to install barbed wire on the prevention fence.

Prevention fence from making a detour to avoid a fence②

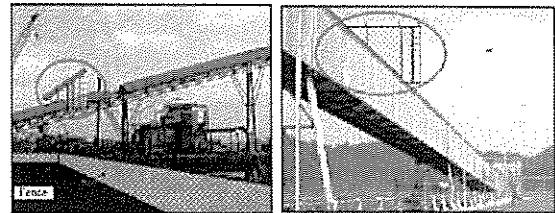


- The lower end of prevention fence should be down to the surface of apron.
- Top guard should be installed on the fence.
- Barbed wire should be installed on an extended projecting fence.
- Fence and gate should also be improved.

Prevention measures from invading through a drainage



Prevention measures from invading along a belt conveyor over the fence



Moving Fences

[Functional requirements]

- ① Ability to clearly indicate the boundaries to restricted areas to identify any intruder
- ② Signs posted to prohibit any trespassing
- ③ Clear zone provided

Moving Fences



Where the following conditions are met, moving fences may be used as substitute for part of the fencing.

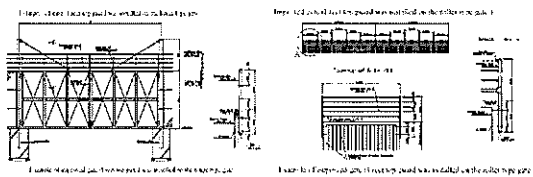
- ① The relevant pier facilities are used primarily for domestic navigating ships and rarely used by international ships.
- ② Sufficient clear zones can be secured as because the back of the pier facilities is unused land area.
- ③ Before demarking the restricted areas by moving fences, inspections are conducted with the cargoes and goods in the restricted areas.
- ④ Where moving fences fail to meet the standard specifications of fixed fences, additional guards are deployed to watch for any intrusion from outside while the restricted areas are being demarked by the moving fences.

Gates

[Functional requirements]

- ① Gates shall have the same height as fixed fences and shall be of a construction of strength and durability to withstand assumed loads.
- ② Car bump or cross bar shall be provided at the gate
- ③ Gate shall be of a construction that allows locking. When locked, the lock and key shall not allow any easy removal, replacement or replication.
- ④ The construction shall allow separate access control of humans and vehicles.

Gates



[Standard Specifications]

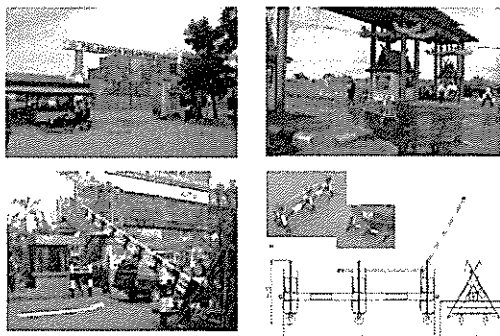
- The standard specifications shall be the same as with fixed fences.

Vehicle Stopping Equipment

[Functional requirements]

- ① Devices that clearly indicate the instruction to stop to the vehicle
- ② Devices that make a vehicle driver recognize the need to stop

Vehicle Stopping Equipment



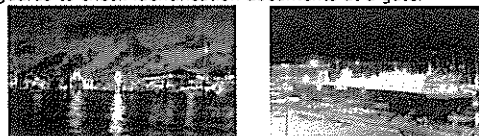
(2) Lighting System

[Interpretations]

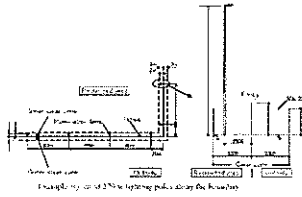
- A certain level of illuminance must be secured at the boundaries of restricted areas in order for psychological effects to deter any intrusion. For that reason, lighting needs to be provided separately from the yard lighting so the illumination can be maintained throughout the night.

[Policy on Lighting System]

- Lighting system has to provide enough brightness for security guards to monitor suspicious person by his own eyes or CCTV camera in harmony with site condition.
- Lighting system has to provide enough brightness for security guards to check identification documents at a gate.



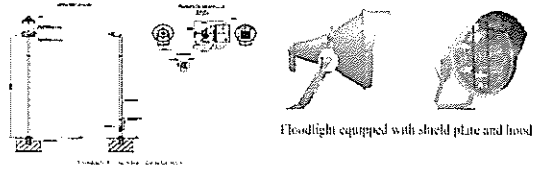
Lighting System (Boundary area)



[Standard Specifications]

- ① The illuminance should allow surveillance by cameras. The illuminance and lighting equipment are to be determined based on the capacity of the camera. The illuminance should basically be 3 lx that will allow surveillance by the naked eye.
- ② The equipment shall be of a construction that will easily prevent any vehicle from intrusion as by onrushing, running over or under.

Lighting System (Yard)



[Standard Specifications]

- Work lighting should be utilized and any deficiency be supplemented by providing additional lighting.

Lighting System (Gate)



[Standard Specifications]

- Spot lighting shall be provided at the position of the standing sentry. The standard illuminance should be 30-50 lx that will allow reading 10 point (approximately 3.5 mm) characters almost effortlessly.

Lighting System (Other)

[Standard Specifications]

- Backup measures shall be provided for any power outage to ensure the minimum level of surveillance functionality including the surveillance of boundary areas.
- Group A facilities shall be equipped with emergency power source. With Group B facilities, while having emergency power source is recommended, alternative measures may be used as enhancing the patrol surveillance upon any power outage.

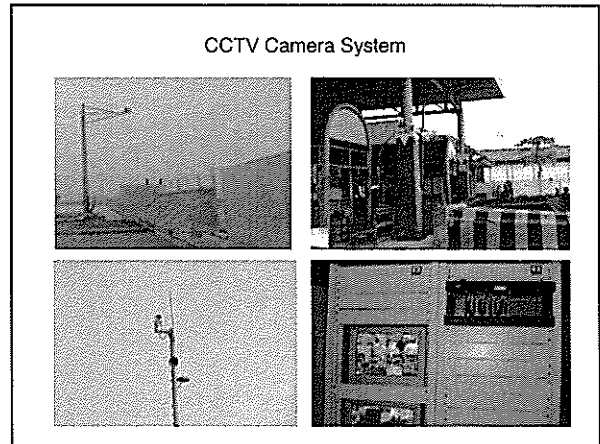
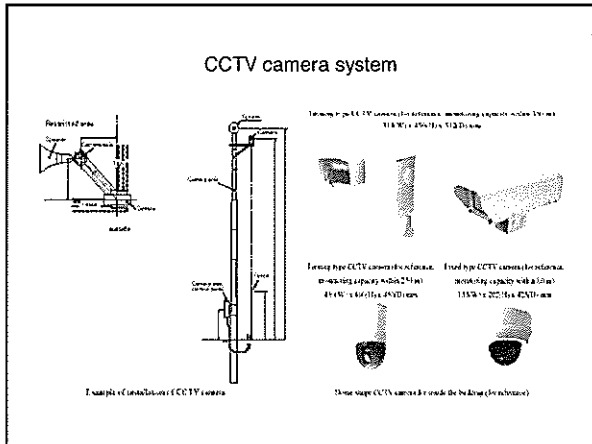
(3) CCTV Camera System

[Functional requirements]

- ① Must be able to cover all boundary areas of the restricted area for surveillance.
- ② Must be able to watch any particular area in the camera operating range within the restricted area.
- ③ With the combination of surveillance equipment and lighting equipment, it must be possible to identify specific actions of any suspicious person when such person's intrusion or tampering with the fence is underway.
- ④ Camera images must be recorded for a certain period of time.
- ⑤ The functionality of the surveillance equipment must be maintained for a certain period of time upon any power outage.

Installation policy on CCTV camera system

- ① CCTV cameras should be disposed with an interval in-between which CCTV cameras can monitor the motion of suspicious person under 3 lx during the night time. Considering the capacity, its number, monitoring area and the target (yard, passenger terminal, etc) of CCTV camera, the layout of CCTV camera should be determined.
- ② The layout should ensure that there is no blind spot by warehouses and stacking cargo to CCTV cameras and CCTV cameras can monitor the main route in the yard.
- ③ In the wharf, the layout should ensure that CCTV cameras do not obstruct cargo handling and there is no blind spot by cranes and handling cargo to CCTV cameras.
- ④ The setting level of CCTV camera should be determined to minimize the blind spot around the fence and by stacking cargo with considering the ease of the maintenance.



(4) Sensor System

Fence Sensor

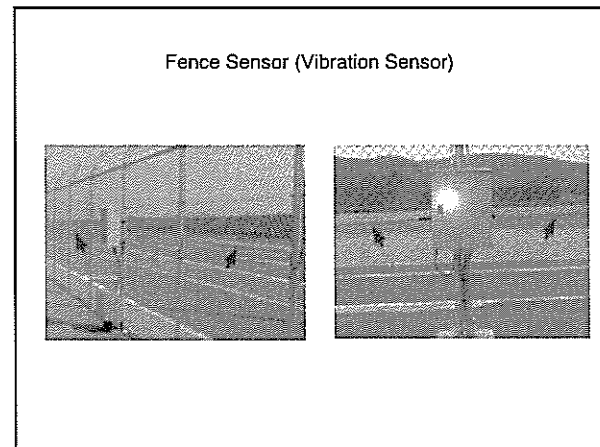
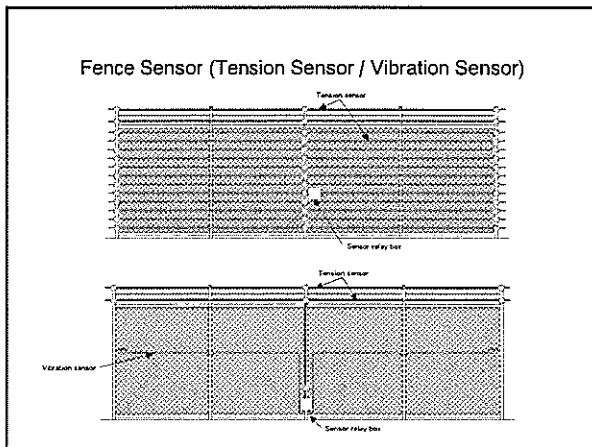
[Functional requirements]

- ① Must always be able to monitor any intrusion from the periphery of the restricted area and any tampering with the fence (by the provision of automatic detection functionality) and to notify the sentinel.
- ② The sensor shall detect any intrusion from the fence (as by climbing over, cutting or clash-breaking) and any tampering with the fence.
- ③ The fence intrusion sensor shall be designed to execute its predetermined functions in combination with the motions of the surveillance camera, after the sensor zone is determined from the preset position of the camera and the field of view of the camera at the moment.

Fence Sensor

[Standard Specifications]

- ① Fence sensors should be installed when they are necessary for any particular purpose. They are not essential conditions for the security facilities.
- ② Candidates shall be vibration sensor, optic fiber sensor, tension sensor, infrared ray sensor, electric field sensor, and image sensor, among which selection is to be made based on the criteria of adaptability, reliability, serviceability, and ease of installation.



Gate Sensor

[Functional requirements]

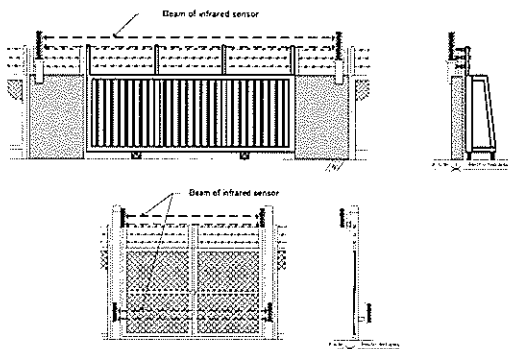
- ① Must have automatic detection functionality to detect any suspicious person and have the capability to report the detection to the sentinel.
- ② The sensor must detect any intrusion from the gate (as by climbing over, cutting and clash-breaking) or any tampering with the gate.
- ③ The gate sensor must be in alert mode while the gate is closed and non-alert mode while the gate is open. The system must be designed to preclude any possibility of non-alert mode while the gate is closed.

Gate Sensor

[Standard Specifications]

- ① Gate sensors should be installed when they are necessary for any particular purpose. They are not essential conditions for the security facilities.
- ② Candidates shall be tension sensor, infrared ray sensor, electric field sensor, and image sensor, among which selection is to be made based on the criteria of adaptability, reliability, serviceability, and ease of installation.

Gate Sensor (Beam of infrared sensor)



Gate Sensor (Beam of infrared sensor)



(5) Inspection System of Belongings

Hand Luggage Inspection Equipment

[Functional requirements]

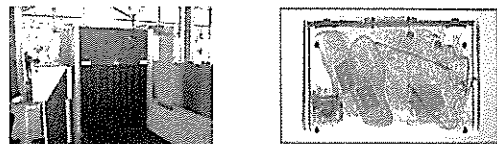
- Must be able to easily detect weapons, explosives and other objects that are prohibited to bring onto the ship.

[Standard Specifications]

- It is desired that international passenger facilities that international regular passenger liners routinely come and go and are visited by a lot of passengers be provided with X-ray inspection devices and portal-type metal detectors for the inspection as of hand luggage.



X-ray inspection device



[Standard Specifications]

- ① Must display the whole of an object being inspected
- ② Must have sufficient capacity to distinguish
- ③ Must have sufficient penetrating power
- ④ Must be able to obtain information on the material of any explosives or any other hazardous objects

Metal detector

[Standard Specifications]

- ① Must be able to detect metallic objects irrespective of their directions and positions
- ② Must be able to detect stainless steel and non-ferrous metals such as aluminum
- ③ Must be sensitivity adjustable
- ④ Portal type metal detector and handheld metal detector are used for the inspection of personal effects of the passengers



(6) Telecommunication System

[Telecommunications between Ships and Port Facilities]
[Functional requirements]

- Must provide capability for direct communication with ships

[Communications with Police Organizations and Other Security Organizations]
[Functional requirements]

- ① Shall be able to communicate immediately and securely with the relevant organizations (Maritime Security Agency, police, fire defense authority, port management etc.)
- ② Shall be able to make phone calls immediately and securely at times of emergency as by speed dialing.

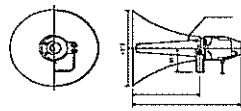
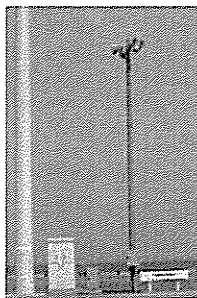
Telecommunication equipment



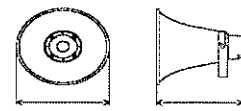
[Communications within Port Facilities]
[Functional requirements]

- ① Security personnel shall be able to make voice calls promptly at times of emergency.
- ② Upon any occurrence of harmful acts by unlawful intruder(s), the emergency reporting system shall be able to notify the security personnel immediately.
- ③ At times of emergency, the security personnel must be able to inform the workers within the restricted areas and give them instructions.
- ④ There shall be ability to simultaneously transmit the same broadcast to the entire restricted areas (including bridges of the ships).

Public Address System



Front view and side view of 50 W speaker
(for reference)

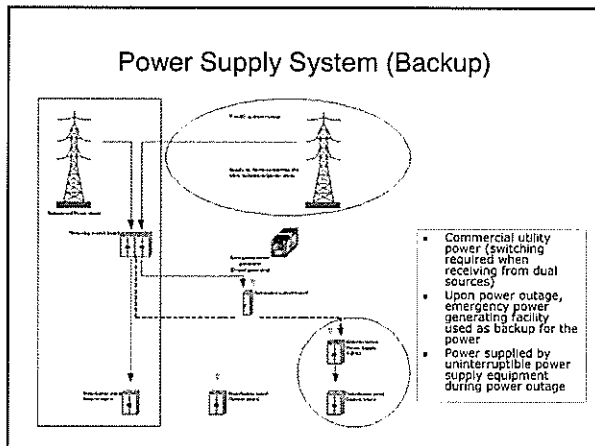


Front view and side view of 15 W speaker
(for reference)

(7) Power Supply System

[Functional requirements]

- ① Must supply consistent and sufficient amount of electric power to the security facilities.
- ② Even at times of power outage in the emergency situation, power must be supplied to keep the surveillance equipment functional in order to continuously capture the situation of the site while reporting to the police and other relevant organizations.



Uninterruptive Power Supply (UPS)

(Sample sizes of UPS are a guide to approximate dimensions)

Power	Capacity (kVA)	Capacity (kW)	Remarks
15A / 20k	10-15/10-15	10-15/10	Basic type
20 / 15	10-15/10-15	10-15/10	Basic type
15 / 12	10-15/10-15	10-15/10	Basic type
10 / 8	10-15/10-15	10-15/10	Basic type
7.5 / 6	10-15/10-15	10-15/10	Basic type
6.2 / 4.5	10-15/10-15	10-15/10	Basic type

3 Maintenance of Port Security Facilities

- In order to properly maintain the functions of port security facilities, inspections and services shall be conducted on a regular basis.

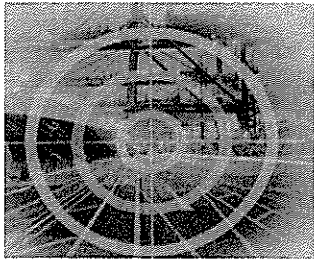
Outline of the maintenance work

Maintenance category	Purpose	Action
Routine inspection	Visually inspect the equipment for any unusual conditions. Or, check in the course of daily operations for any fault.	-Check the inspection items and follow the inspection procedures in accordance with the using instructions. -Actions by the operators
Scheduled inspection	Check the operating conditions of each piece of the equipment and at the same time conduct the maintenance with the sections that cannot be checked in routine inspections for early detection of any fault and for prevention of fault that may arise as a result of deterioration by ageing.	-To be conducted based on the scheduled inspection contract. -To be conducted by the maintenance service contractors or equipment manufacturers.
Maintenance	Take remedial actions upon any accidental malfunction or fault.	-To be conducted by on-call maintenance service contracts. -To be conducted by the maintenance service contractors or equipment manufacturers.

TERIMA KASIH !!

JICA - DGST Workshop ISPS Code

Outline of Enhancement Program on Exercises, Drills & Training




JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Introduction

It is important that ships/port facilities introduce and implement the policy for raising security awareness

Security Policy
 "It is the responsibility of every individual Onboard the ships and within the port facility to be vigilant against security threats and security-related activity"



JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Raising Security Awareness

- Contracting Government
- Port Authority
- Port Security Officer
- Security Services
- Employers
- Workers' Representatives
- Port Facility Security Officers
- People working in the port
- Port Security Advisory Committee

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports


JICA - DGST Workshop ISPS Code

Raising Security Awareness

Contracting Government

- Inform the public about:
 - Government's Security Policy
 - Threat levels
 - Measures that can be taken
- Request public vigilance

Homeland Security





JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES
 Usually large scale and comprehensive training events
 Involve two or more parties / organizations
 Tests issues on
 Command and Control
 Communications
 Coordination
 Resource availability and allocation
 Responses

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES

- More elaborate control organization
- Scenario-based
- Includes participation of two or more of :
 PSO, PFSO
 Relevant Authorities of Contracting Governments

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES

- Requires longer planning period
- Conducted as:
 - Practical with deployment of assets
 - Table-top discussions
 - Simulation-based activities




JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES

- Forming the Exercise Planning and Control Team (EPCT)
 - Plan the Exercise Programme
 - Control the Exercise

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

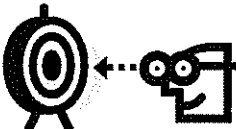


JICA International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES

Exercise Planning

- Determine the Aim of the Exercise
 - Provides focus for planning and conduct of the Exercise

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports



JICA International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES

Exercise Planning

- Set the Exercise Objectives
- Emphasize the Exercise Intent
- Resource availability, allocation & requirements
- Time available
- Types and Level of exercise play

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports



JICA International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES

Identify Required Attainments

- Consider performance outcome of the participants.
- Provide Checklists for evaluating required attainments.
- Include qualitative and quantitative measurements.

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports



JICA International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES

Selecting the Scenario

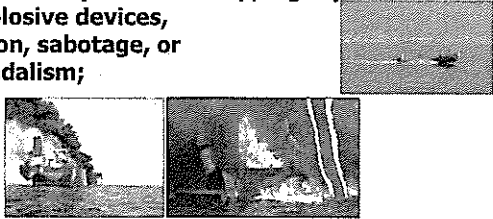
- Must meet stated objectives
- Realistic to overall environment setting
- Potential to escalate with added issues for players
- Refer to list of nine security threat scenario in Part B, Section 15.11 of the ISPS Code


JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

1. Damage to, or destruction of, the port facility or of the ship, e.g. by explosive devices, arson, sabotage, or vandalism;




JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

2. Hijacking or seizure of the ship or of persons on board;



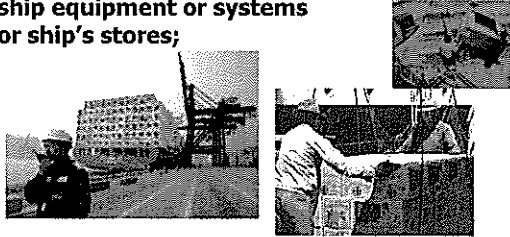
JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

3. Tampering with cargo, essential ship equipment or systems or ship's stores;




JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

4. Unauthorised access or use including presence of stowaways.



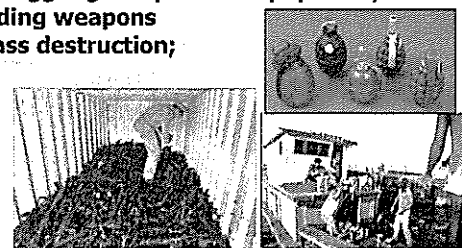
JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

5. Smuggling weapons or equipment, including weapons of mass destruction;



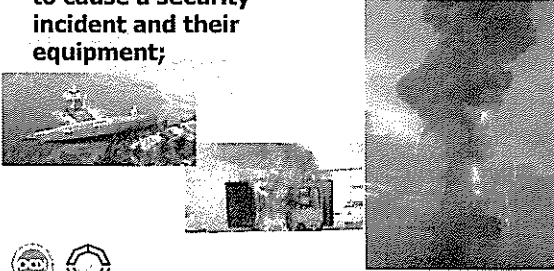
JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

6. Use of ship to carry those intending to cause a security incident and their equipment;




JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

7. Use of ship itself as a weapon or as a means to cause damage or destruction;




JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

8. Blockage; of port entrances, locks, approaches etc;



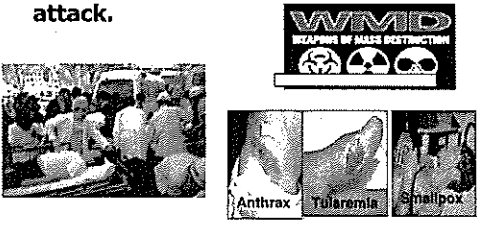
JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training

9. Nuclear, biological and chemical attack.



JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports



JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code


Exercises Drills and Training

EXERCISES

Developing the Exercise Narrative

- Opening Narrative with 1-2 phases of escalation
- Sets the Start State for the Exercise
- Do not describe response(s) to the event
- Subsequent narratives provided to:
 - Take stock of the existing situation
 - Shift the exercise play to jump to another level, time frame, or focus

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports



JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training


EXERCISES

Determine the Exercise Time-Table

Table-top exercise
within a few hours, or 1 or 2 days, if necessary

Deployment Exercise
may be within a few hours. Deployment exercises over several days involves extensive administrative and logistics planning and resources

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports



JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Exercises Drills and Training


EXERCISES

Develop Injects / Master Event List (MEL)
Injects to generate the required response


Example Scenario:
"Damage to, or destruction of, the ship or of a port facility"

injects to test the effectiveness of:

- Access Control Measures
- Command, control, co-ordination and communications of the responses



JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports



JICA - DGST Workshop ISPS Code

Develop Injects / Master Event List (MEL)

JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

MASTER EVENT LIST - TIMELINE

SERIAL	TIME	EVENT	EXPECTED RESPONSE/REMARKS	COORDINATED BY	RECOMMENDED PARTICIPANTS
AP01	0930	Brief to Senior Management on Indonesian Concept of ISPS Implementation	Discussion	STET	Management
AP02	1000 - 1200	Introduction and Briefing on the Aim, Objectives and Expected Attainments of the Ex (Drills)	Allow participants to understand the objectives of the Ex (Drills) and the requirements of them	STET and PFSO	STET, PFSO, Head of Security, security staff
AP03	1030 - (About 1.5 hrs)	Table top Exercise and Drills	Per the Start State and injects generated thereafter	STET Controllers	All participants
		Commencement of Access Control Drill	Personnel to meet their stations to execute Access Control as per their approved PFSO. Additional injects with personnel may double up to observe and provide critique on the drill	STET Controllers	STET, PFSO, Head of Security, Security Staff
		a. Attempt surveillance on Facility	Security staff to report, and challenge (even though the person conducting surveillance is outside the facility area).	STET supported by PFSO	Head of Security, Security Staff
		b. Store delivery from unauthorized source	Security staff to prevent ingress, check item, and if confirmed found, to take appropriate action	STET supported by PFSO	Head of Security, Security Staff
		c. Threat condition increases, Level 2 declared.	Security staff implement Level 2 measures	STET supported by PFSO	Head of Security, security staff

JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES

Inject Planning Considerations:

- Dynamics of exercise play
- Test the validity of existing (or lack of) plans and processes
- Not to cause complete destruction of, or overwhelm the responder's capabilities
- Draw participants through sequence of events to unfold during a response

JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES

Injects Planning Considerations:

- Be realistic – Controllers should not be seen as “playing-god”
- Avoid wasting exercise opportunities – Inform participants of the plans and processes to be evaluated

JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES

Set-up the Exercise Organization

- Exercise Director – Senior or Top Executive
- Chief Controller – Chairman of the EPCT
- Controllers / Players – EPCT Members / Department Managers/Key Appointment Holders

JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISE ORGANISATION

JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports



JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Exercises Drills and Training

Identify Participants / Organize Control Staff:
 Determine extent of the Participant List

- Internal and Invited Players
- Actual and "simulated" Players
- High and Low Controllers
- Observers

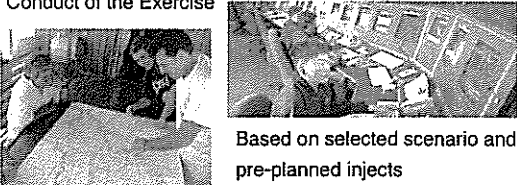



JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports



JICA - DGST Workshop ISPS Code

Exercises Drills and Training

Conduct of the Exercise



Based on selected scenario and pre-planned injects
 Players – Low Controller and High Controller interactions








JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES
 Exercise Players
 PSO, PFSO, CSO, SSO
 Personnel with security duties
 Live / Simulated port/port facility
 Operations, technical, logistics, marketing, and media representatives

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Exercises Drills and Training




Exercise Control and Safety Management

Where necessary and should the situation warrants, that safety issues might be compromised, the President Director may declare an **'Exercise Hold'**, pending the outcome of the state (example foul weather, shipboard accident, ambiguity arise).

When it is assessed that the issues have been clarified or status is correct, he will declare **'Exercise Resume'**.

However, should the situation regress beyond the control, and it is deem that the exercise can no longer continue, the President Director may declare an **'Exercise Abort'**.

Upon completion of the Maritime Security Exercise, the President Director will declare **'Exercise End'**.



JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXERCISES
 Post-Exercise Debrief and Reports

- Most important activity
- Involve as many participants as possible
- Draw comments, lessons learnt and recommendations on:
 - Exercise aim, objectives, scope and attainments
 - Exercise conduct
 - Deficiencies in the Plan
 - Participants' performance
- File the Report and pursue Follow-up Actions




JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Exercises Drills and Training

EXAMPLE OF AN ADVANCED EXERCISE
 A deployment exercise to test the PORT BUNGLE Security Plan, progressing from Level 2 to Level 3, involving the Police, Coast Guard Homeland Defense Force, and Hospital.

Scenario: A terrorist attack from the sea using a stolen harbour craft laden with with explosive against a container vessel loading chemicals at the facility. A simultaneous bomb truck attack on a storage facility.








JICA JICA – DGST Workshop ISPS Code

Exercises Drills and Training

Features of DRILLS

- Limited to specific procedures
- Conducted frequently to ensure proficiency
- Usually intra-Organisation/Agencies
- Uncomplicated management
- Live activities




JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA JICA – DGST Workshop ISPS Code

Exercises Drills and Training

DRILLS Objectives

- Maintain a high level of readiness
- Practice hands-on skills
- Test equipment
- Test procedures



JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA JICA – DGST Workshop ISPS Code

Exercises Drills and Training

Planning of a Drill

- Determine type of drill to be undertaken
- Determine objectives – procedures and/or elements of plan to be tested / practiced
- Develop drill with principal supervisors
- Identify & list the elements (e.g. bomb search, evacuation, mustering and headcount, reporting headcount)

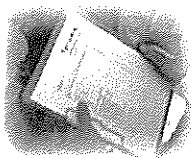


JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA JICA – DGST Workshop ISPS Code

Exercises Drills and Training

Planning

- Determine if evaluators are required
- Select date and time of drill
- Notify participants





JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA JICA – DGST Workshop ISPS Code

Exercises Drills and Training

Conduct of a Drill

- Brief all participants on drill parameters and special instructions (e.g. Bomb Search)
- Ensure participants have clear understanding of expectations
- Announce simulated events to facilitate the drill
- Safety and non-exercise conditions to be specified
- Determine end point of drill

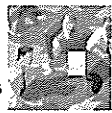


JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA JICA – DGST Workshop ISPS Code

Exercises Drills and Training

Drill Critique

- Collate notes
- Conduct debrief with all participants for feedback & lessons learnt
- Identify and correct personnel errors
- Record the conduct of the drill
- Follow-up on recommendations for improvements to procedures and/or equipment

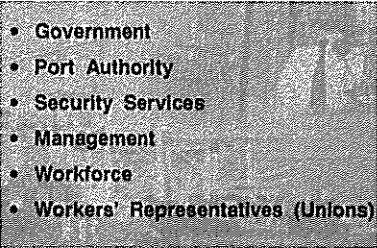


JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

Training needs to be provided for every level

- Government
- Port Authority
- Security Services
- Management
- Workforce
- Workers' Representatives (Unions)








JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

TRAINING PLAN

- The purpose of a training plan is to provide a structured guide for the trainer / instructor to:
 - Maintain focus on the lesson objectives and required attainments







JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

TRAINING PLAN

- The purpose of a training plan is to provide a structured guide for the trainer / instructor to:
 - Plan and prepare for his lesson / training
 - Directs the trainer to the right reference & resource
 - Make available the training aids needed
 - Conduct the lesson based on the scope, recommended delivery method and the time allocated



JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

TRAINING PLAN

Components

1. Topic Title
2. Objectives
3. Required Attainments
4. Method of Instruction
5. Resources / References
6. Training Aids / Means
7. Scope
8. Time Allocated
9. Execution

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports




TRAINING PLAN

Topic Title: Simply state the topic title.

Example : "Search Methods"

Objective(s): Statement (s) to indicate the objective (s) of the lesson, emphasizing the transfer of Knowledge, Skills and Attitudes (KSA).

Example: "To impart to stevedores the knowledge of the various search methods and their associated equipment."



JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

TRAINING PLAN

Required Attainments:

- Similar to the objective statement
- Emphasis is on the "recipient" of the KSA
- Specify recipients' required attainment(s) at the end of the lesson / training.
- Start off with "At the end of the lesson, participants will be able to ... (action verb)....."
- Use of action verbs to depict the learning level
- May include expected performance standards



JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

TRAINING PLAN



Required Attainments:

Example: At the end of the lesson, participants will be able to:

1. State the limitations of search.
2. Apply the techniques of personnel search.
3. Apply the techniques of a vehicle search.
4. Conduct a search.

JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports





JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code



TRAINING PLAN

Methods of Instruction:

- There are various modes of delivery.
- Select the most effective method for the subject.



JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports



JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Examples: Lecture, Demonstration, Discussions, Case studies, Project work, Role-play, Simulation games, Practical, Exercise

In the case of Search Methods, some effective methods to consider are:

1. Briefing / Discussion
2. Demonstration / Role play

JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code



TRAINING PLAN

Resources / References:

Material needed for the lesson – Books, Operating Manuals, Handouts, Professional articles, etc.

Example: Search SOP, Access Control SOP

JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code



TRAINING PLAN

Training Aids and Means:

Select the most effective training aids that can best support the lesson – e.g. computer / projector for PPT presentation, flip charts, videos and VCD player.

Example: For Search Methods, a video on a search being carried out.

JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

TRAINING PLAN



Scope:

To facilitate understanding, scope the lecture / training according to:

- Sub-topics / events
- Logical progression

Scope the training / lessons on established Standard Operating Procedures is usually not difficult as SOPs are generally well structured in logical sequence.


JICA Study on the Post Security Enhancement Program of the Major Indonesian Public Ports

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

TRAINING PLAN

Scope:
Example: For Search Methods,



1. Introduction
2. Right of search
3. Personnel search
4. Vehicle search

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

TRAINING PLAN

Time allocated:

Determine overall time required by summing up each of the sub-topics / sub-sections of the scope. Based on:

- Extent of contents to be imparted
- How simple or in-depth the contents are
- Participants' language proficiency

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

TRAINING PLAN

Execution:

- This section deals with the breakdown of the lesson sub-topics from the "Scope".
- It guides the trainer in apportioning the time allocation for each sub-topic.

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

TRAINING PLAN

Example:

Introduction: (10 minutes)
 State why Searches are required (Slide 1)
 State the importance of a physical search (Slide 2)

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

TRAINING PLAN

Main topic: (30 minutes)

Describe the rights of a search team	(Slides 3 - 9)
Explain the methods of conducting a personnel search	(Slide 10 - 15)
Explain the methods of conducting a vehicle search	(Slides 16 - 25)
Show training video "Vehicle search"	(VHS tape no 1)
Discuss how to conduct a ship search	(Discussion and Presentation)

Conclusion: (5 minutes)

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

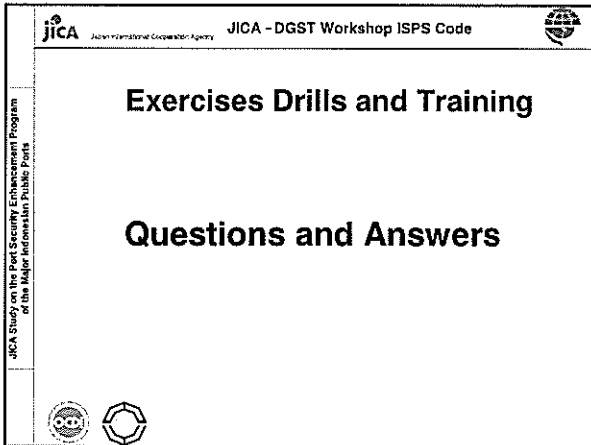
Exercises Drills and Training

Summary

This module has covered the requirements and techniques for the planning and conduct of:

- Security Exercises
- Security Drills
- Security Training

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports



JICA - DGST Workshop ISPS Code

Outline of Port Facility Security Assessment Manual

JICA Study Team on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

1. Objective of PFSA

- The Port Facility Security Assessment (PFSA) is an essential and integral part of the process of developing and updating the Port Facility Security Plan (PFSP)
- To identify the vulnerability of port facilities, to conduct the risk evaluation of PFSA and to recommend the countermeasures in order to appropriately formulate the PFSP

JICA - DGST Workshop ISPS Code

2. Formulation Flow of PFSA

```

graph TD
    A[General Provisions] --> B[Identification of Present Situation of the Port  
(Outline of the Port, Layout of Port Facilities and Port Utilization)]
    B --> C[Identification of the Existing Port Facilities]
    C --> D[Risk Evaluation]
    D --> E[Concept of Countermeasures]
    E --> F[Recommendations on port security measures]
    F --> G[Revised Risk Evaluation after mitigation]
  
```

JICA - DGST Workshop ISPS Code

3. General Provisions

- At the introduction of the PFSA, following general matters shall be described
 - Feature of the PFSA
 - Name of the port administrator
 - Port facilities to be compliant with ISPS Code
 - Definitions of words

JICA - DGST Workshop ISPS Code

4. Identification of Present Situation of the Port

- Outline of the port
 - Location of the port, history of the port, situation of circumstances and outline of port activities
- Layout of facilities and equipment
 - Figure of layout of facilities and equipment, dimensions of the main facilities such as international wharves
- Port utilization
 - Number of ship calls, volume of cargo and passenger

JICA - DGST Workshop ISPS Code

5. Identification of the Existing Port Facilities

- Situation of all existing facilities, equipment and neighboring area shall be identified and described

Channel	Cargo handling equipment	Power plant	Electricity, city gas & water supply
Anchorage area	Passenger terminal	Bunker point (Fuel)	Pipeline
Wharf	Control center	Storage tank	Service boat
Storage & handling area	Port office	Fresh water supply point	Road, railway & bridge
Warehouse & shed	Substation (Distributor)	Fresh water supply tank	Neighboring Area

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Risk evaluation is conducted according to the following procedures

```

graph TD
    A[Selection of Port Facilities Relevant to International Vessel Calls] --> B[Evaluation of the Likelihood of Threat Scenario Occurrence]
    B --> C[Impact Evaluation In Occurrence of Threats]
    C --> D[Vulnerability Evaluation]
    D --> E[Risk Evaluation]
  
```

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Generally, Risk can be represented as the product of the probability and impact of a given security breach as follows

$$R = P \times I$$

Where

- R** = risk score for a given security breach
- P** = probability – probability of a security breach. The probability of a security breach can further be defined as the product of threat occurrence (T) and vulnerability (V).
- I** = impact – the sum of possible impacts associated with a successful security breach. Impact may be based on impacts to life, economic security, symbolic value, and national defense

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Facilities and equipment that are relevant to international vessel calls shall be identified
- The following nine scenarios which are defined in ISPS Code, B 15.11 shall be considered as envisaged threat scenarios

Scenario	
1	Attack by explosive devices, arson or sabotage
2	Hijacking or seizure
3	Tampering with cargo or ship's store and unauthorized remodeling of important equipment, machinery or systems
4	Interference with port activities by unauthorized access of stowaways or unauthorized use of port facilities
5	Smuggling weapons or equipment
6	Use of the ship to carry terrorists and their weapons
7	Use of the ship itself as a weapon
8	Blockage of port entrances, channels etc.
9	Nuclear, biological and chemical attack

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Evaluation of the Likelihood of Threat Scenario Occurrence

- Considering the threat motive such as politics, symbolic, economic and fear, the likelihood of occurrence of each scenario shall be evaluated using the following table and three steps: A (high), B (Middle) and C (Low).
- Likelihood value is a quantified numeric of the likelihood of occurrence, A: 3, B: 2 and C: 1.

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

No	Scenario (ISPS Code, B 15.11)	Assessment	Likelihood of Occurrence	Likelihood Value
1	Attack by explosive devices, arson or sabotage	Some bomb incidents occurred in Indonesia, and likelihood of occurrence of this scenario is high.	A	3
2	Hijacking or seizure			
3	Tampering with cargo, essential ship equipment or systems or ship's stores	Scenario of illegal act in the port such as tampering is possible.	B	2
4	Unauthorized access of stowaways or unauthorized use of port facilities			
5	Smuggling weapons or equipment			
6	Use of the ship to carry terrorists and their weapons	There have been few cases where a ship itself has been used as a weapon. Likelihood of occurrence of terror by small ship with bomb is low.	C	1
7	Use of the ship itself as a weapon			
8	Blockage of port channels etc.			
9	Nuclear, biological and chemical attack			

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Impact Evaluation in Occurrence of Threats

- Evaluation items of impact consist of "social", "economic", "environment" and "symbolic" points. Impact value is obtained from the following formula using the total of these four items.

$$\text{Total score} = (\text{Social point}) + (\text{Economic point}) + (\text{Environment point}) + (\text{Symbolic point})$$

Maximum; 12, Minimum; 4

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Impact Evaluation in Occurrence of Threats
Social point ; degree of effects on casualty toll in case that a port (facility) is destroyed by terrorist attack (Three scoring steps: 1-3)

3	Numerous deaths
2	Some loss of life
1	Little loss of life or injury

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Impact Evaluation in Occurrence of Threats
Economic point ; degree of economic loss in case that a port (facility) is destroyed and damaged (Three scoring steps: 1-3)

3	National or long term economic loss due to interference with port activities
2	Local or short term economic loss due to interference with port activities
1	Little economic loss due to interference with port activities

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Impact Evaluation in Occurrence of Threats
Environment point ; degree of natural and social environment impact incase that facilities and equipment is influenced by threat scenarios (Three scoring steps: 1-3)

3	Complete destruction of a natural environment and social environment over a large area
2	Long term damage to part of a natural environment and social environment
1	Very limited or small scale damage to part of a natural environment and social environment

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Impact Evaluation in Occurrence of Threats
Symbolic point ; degree of symbolic loss in case that facilities and equipment is influenced by threat scenarios (Three scoring steps: 1-3)

3	High symbolic effect
2	Middle symbolic effect
1	Low symbolic effect

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Impact Evaluation in Occurrence of Threats
Impact value = 3 (Total score: 12 – 10)
2 (Total score: 9 – 7)
1 (Total score: 6 – 4)

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Impact Evaluation in Occurrence of Threats

Port facilities	Impact items				Total score	Impact value
	Social	Economic	Environment	Symbolic		
(1) Channel (River; a few number of international ship sailings)	1	2	1	1	5	1
(2) Anchorage and basin	1	1	1	1	4	1
(3) Wharf	2	2	1	2	7	2
(4) Storage and handling area	2	2	1	2	7	2
(5) Warehouse	1	1	1	1	4	1
(6) Cargo handling equipment	2	2	1	2	7	2
(7) Control center	2	3	2	2	9	2
(8) Port office	3	2	2	2	9	2
(9) Substation (Distributor)	2	2	1	1	6	1
(10) Fresh water supply point	1	1	1	1	4	1
(11) Fresh water supply tank	1	1	1	1	4	1
(12) Electricity and city gas	1	1	1	1	4	1
(13) International ship (Dangerous goods)	3	2	3	3	11	3
(14) Tugboat, Pilot boat	1	2	1	2	6	1
(15) Road	1	1	1	2	5	1
(16) Neighboring Area	3	1	1	1	6	1

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Vulnerability Evaluation
 - In advance of vulnerability evaluation, the issues related to the current security measures at port facilities shall be identified and resolved here

Accessibility issues (Example)

Gate: Main gate near the international berth is not equipped with a pole to stop cars nor is there a lock.

Fence: Some part of the fence is broken and no outrigger is installed.

Lighting facilities: Half of the lighting facilities are out of order.

Clear zone: Cargo is stored an inch away from the fence. etc

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Vulnerability Evaluation
 - Organic security issues (Example)
 - Access control: No access control is conducted for vendors.
 - When persons pay fees and receive receipts, no checking of the individual's identity is conducted.
 - Only external appearances of incoming vehicles are inspected.
 - ID/pass check: Entry pass is not issued for vehicles that pass through the gates.
 - Patrol in port facility: Access channel is not patrolled.

etc

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Vulnerability Evaluation
 - Based on the issues on current security measures, the vulnerability against threat is evaluated using 5 scoring steps (2-6).
 - Evaluation items of vulnerability consist of "Accessibility" and "Organic security" points.
 - Vulnerability value is the total of these two items.

Vulnerability value = (Accessibility point)
+ (Organic security point)
Maximum; 6, Minimum; 2

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Vulnerability Evaluation
 - Accessibility point ; degree of accessibility of the facilities and equipment to the threat incidents (This relates to physical and geographic barriers that deter the threat independently of organic security.) (Three scoring steps: 1-3)

3	No deterrence (ex. unrestricted access to vessel, unrestricted internal movement and facilities and equipment not to withstand specific attack)
2	Good deterrence (ex. single substantial barrier, unrestricted access to within some short distance from vessel and facilities and equipment to withstand specific attack)
1	Excellent deterrence (expected to deter attack, access restricted within some long distance from vessel, multiple physical/geographical barriers and facilities and equipment to withstand specific attack well)

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Vulnerability Evaluation
 - Organic security point ; degree of the ability of the security personnel to deter the threat incidents, which includes having in place security capability, guard force, intrusion detection systems, and timeliness of outside law enforcement to prevent threat incidents (Three scoring steps: 1-3)

3	No deterrence capability (ex. no security plan, no guard force, no emergency communication, outside law enforcement not available for timely prevention, no detection capability)
2	Good deterrence capability (ex. minimal security plan, some communications, armed guard force of limited size relative to the vessel, outside law enforcement not available for timely prevention, limited detection systems)
1	Excellent deterrence capability (expected to deter attack, covert security elements that represent additional elements not visible or apparent)

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Vulnerability Evaluation

Vulnerability Value

Port facilities	Vulnerability items		Vulnerability value
	Accessibility	Organic security	
(1) Channel (River; a few number of international ship sailings)	3	3	6
(2) Anchorage and basin	2	3	5
(3) Wharf	2	2	4
(4) Storage and handling area (hazardous)	2	2	4
(5) Warehouse	2	2	4
(6) Cargo handling equipment	2	2	4
(7) Control center	3	3	6
(8) Port office	2	3	5
(9) Substation (Distributor)	2	2	4
(10) Fresh water supply point	2	2	4
(11) Fresh water supply tank	2	2	4
(12) Electricity and city gas	1	2	3
(13) International ship (Dangerous goods)	2	2	4
(14) Tugboat, Pilot boat	2	2	4
(15) Road	2	2	4
(16) Neighboring Area	3	2	5

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Risk Evaluation

• Risk for each threat scenario is evaluated as the product of the likelihood value, impact value and vulnerability value using the following formula.

$$\text{Risk value} = (\text{Likelihood value}) \times (\text{Impact value}) \times (\text{Vulnerability value})$$

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Risk Evaluation

• Risk ranks consist of 3 categories for grouping of risk values

M: Mitigate (protective measures and/or procedures to reduce risk for that scenario are needed)
(Risk values: 54-30)

C: Consider (Scenario should be considered and protective measures should be developed on a case-by-case basis)
(Risk values: 29-15)

D: Document (Scenario may not need a protective measure at this time and therefore needs only to be documented)
(Risk values: 14-2)

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Risk Evaluation

• Risk evaluation for each scenario shall be conducted as in the following table

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Risk Evaluation

• Scenario 1: Attack by Explosive Devices, Arson or Sabotage on Ships or Port Facilities

Port facilities	Likelihood value	Impact value	Vulnerability value	Risk value	Risk rank
(1) Channel (River; a few number of international ship sailings)	3	1	6	18	C
(2) Anchorage and basin	3	1	5	15	C
(3) Wharf	3	2	4	24	C
(4) Storage and handling area	3	2	4	24	C
(5) Warehouse	3	1	4	12	D
(6) Cargo handling equipment	3	2	4	24	C
(7) Control center	3	2	6	36	M
(8) Port office	3	2	5	30	M
(9) Substation (Distributor)	3	1	4	12	D
(10) Fresh water supply point	3	1	4	12	D
(11) Fresh water supply tank	3	1	4	12	D
(12) Electricity and city gas	3	1	3	9	D
(13) International ship (Dangerous goods)	3	3	4	36	M
(14) Tugboat, Pilot boat	3	1	4	12	D
(15) Road	3	1	4	12	D
(16) Neighboring area	3	1	5	15	C

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Risk Evaluation

• Scenario 3: Tampering with Cargo or Ship's Store and Unauthorized Remodeling of Important Equipment, Machinery or Systems

Port facilities	Likelihood value	Impact value	Vulnerability value	Risk value	Risk rank
(1) Channel (River; a few number of international ship sailings)	2	1	6	12	D
(2) Anchorage and basin	2	1	5	10	D
(3) Wharf	2	2	4	16	C
(4) Storage and handling area	2	2	4	16	C
(5) Warehouse	2	1	4	8	D
(6) Cargo handling equipment	2	2	4	16	C
(7) Control center	2	2	6	24	C
(8) Port office	2	2	5	20	C
(9) Substation (Distributor)	2	1	4	8	D
(10) Fresh water supply point	2	1	4	8	D
(11) Fresh water supply tank	2	1	4	8	D
(12) Electricity and city gas	2	1	3	6	D
(13) International ship (Dangerous goods)	2	3	4	24	C
(14) Tugboat, Pilot boat	2	1	4	8	D

JICA - DGST Workshop ISPS Code

6. Risk Evaluation

- Risk Evaluation

Summary of risk evaluation (it easy to identify the weakness of facilities and equipment)

Port Facilities	Threat Scenario No.									Max	
	1	2	3	4	5	6	7	8	9		
(1) Channel (River; a few number of international ship sailings)	C		D	C				D	D	D	C
(2) Anchorage and basin	C		D	C				D	D	D	C
(3) Wharf	C		C	C	C	C		D	D	D	C
(4) Storage and handling area	C		C	C	C	C		D	D	D	C
(5) Warehouse	D		D	D	D	D		D	D	D	C
(6) Cargo handling equipment	C		C	C	C			D	D	D	C
(7) Control center	M		C	M							M
(8) Port office	M		C	M							M
(9) Substation (Distributor)	D		D	D							D
(10) Fresh water supply point	D		D	D							D
(11) Fresh water supply tank	D		D	D							D
(12) Electricity and city gas	D		D	D							D
(13) International ship (Dangerous goods)	M	M	C	M	M	M		D	D	D	M
(14) Tugboat, Pilot boat	D	C	D	D	D	D		D	D	D	C
(15) Road	D		D								D
(16) Neighboring area	C		C								C
Max	M	M	C	M	M	M		D	D	D	M

JICA - DGST Workshop ISPS Code

7. Concept of Countermeasures

- The concepts of countermeasures for each scenario are described in the following table. Countermeasures may be recommended referring to the following table.

No	Scenario	Max Risk Rank	Concept of Countermeasures
1	Attack by explosive devices, arson or sabotage		-To implement intensive access control to prohibit terrorists with weapons and vehicles and cargoes concealing weapons from passing gates -To monitor along fence to prevent intrusions -To implement monitoring and patrol of water area to prevent attack from seawide
2	Hijacking or seizure		-To implement intensive access control and monitor fence and its surrounding area to prohibit boarding of potential hijackers -To intensively implement patrol in water area and near wharves and monitor in water area for a ship not to be seized from water area

JICA - DGST Workshop ISPS Code

7. Concept of Countermeasures

No	Scenario	Max Risk Rank	Concept of Countermeasures
3	Tampering with cargo or ship's store and unauthorized remodeling of important equipment, machinery or systems		-To implement intensive access control and monitor cargo storing area to prevent tampering and unauthorized remodeling in the terminal area -To implement intensive access control to prevent weapons from entering into ship's store and equipment
4	Interference with port activities by unauthorized access of stairways or unauthorized use of port facilities		-To implement intensive access control at gates and monitor fence area and storage area against stairways -To intensively monitor cargo storing area against unauthorized use
5	Smuggling weapons or equipment		-To implement intensive access control at gates and intensively monitor cargo storing area against smuggling in the restricted area Customs are basically responsible for smuggling check.
6	Use of the ship to carry terrorists and their weapons		-To implement intensive access control at gates -To intensively monitor cargo storing area

JICA - DGST Workshop ISPS Code

7. Concept of Countermeasures

No	Scenario	Max Risk Rank	Concept of Countermeasures
7	Use of the ship itself as a weapon		-To implement offshore patrol to prevent sea hijacking and seizure as well as attack by small boats including hijacked tugboats, pilot boats or traffic boats -Patrol boats are required to furnish communication equipment
8	Blockage of port entrances, channels etc.		-To take measures mentioned in scenario No. 2 and 7 to prevent a ship colliding with and sinking a large ship in port entrances and channels -To take measures mentioned in scenario No. 1 and 3 to prevent sinking of a ship by blowup of explosives that is illegally loaded into it
9	Nuclear, biological and chemical attack		-To take measures mentioned in scenario No. 1 (To replace "explosives" with "nuclear, biological and chemical weapon")

JICA - DGST Workshop ISPS Code

8. Recommendations on Port Security Measures

- Based on the risk evaluation, security measures shall be recommended along the following lines at least in order to improve "M (Mitigate)" to "C (Consider)"

- Installation of fence or barrier
- Access control
- Monitoring terminal area
- Monitoring water area
- Communication with related organizations
- Response to emergency
- Training
- Others

JICA - DGST Workshop ISPS Code

9. Revised Risk Evaluation after Mitigation

- Based on the above recommended security measures, risk for each scenario is reevaluated in this section.
- Basically, vulnerability can be improved by the implementation of the recommended security measures.
- In principle, accessibility point or organic security point can be reduced one point response to the contents of security measures.

JICA - DGST Workshop ISPS Code

9. Revised Risk Evaluation after Mitigation

Revised Vulnerability Value


Port facilities	Revised vulnerability items		Revised vulnerability value
	Revised accessibility	Revised organic security	
(1) Channel (River; a few number of international ship sailings)	3	2	5
(2) Anchorage and basin	2	2	4
(3) Wharf	1	2	3
(4) Storage and handling area (hazardous)	1	2	3
(5) Warehouse	2	2	4
(6) Cargo handling equipment	1	2	3
(7) Control center	2	2	4
(8) Port office	2	2	4
(9) Substation (Distributor)	2	2	4
(10) Fresh water supply point	1	2	3
(11) Fresh water supply tank	2	2	4
(12) Electricity and city gas	1	2	3
(13) International ship (Dangerous goods)	1	2	3
(14) Tugboat, Pilot boat	2	2	4
(15) Road	2	2	4
(16) Neighboring Area	3	2	5

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

9. Revised Risk Evaluation after Mitigation

- Using the revised vulnerability value, the risk reevaluation for each scenario shall be conducted as in the following table



JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

9. Revised Risk Evaluation after Mitigation

Scenario 1: Attack by Explosive Devices, Arson or Sabotage on Ships or Port Facilities

Port facilities	Likelihood value	Impact value	Vulnerability value	Risk value	Risk rank
(1) Channel (River; a few number of international ship sailings)	3	1	5	15	C
(2) Anchorage and basin	3	1	4	12	D
(3) Wharf	3	2	3	18	C
(4) Storage and handling area	3	2	3	18	C
(5) Warehouse	3	1	4	12	D
(6) Cargo handling equipment	3	2	3	18	C
(7) Control center	3	2	4	24	C
(8) Port office	3	2	4	24	C
(9) Substation (Distributor)	3	1	4	12	D
(10) Fresh water supply point	3	1	3	9	D
(11) Fresh water supply tank	3	1	4	12	D
(12) Electricity and city gas	3	1	3	9	D
(13) International ship (Dangerous goods)	3	3	3	27	C
(14) Tugboat, Pilot boat	3	1	4	12	D
(15) Road	3	1	4	12	D
(16) Neighboring area	3	1	5	15	C

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

9. Revised Risk Evaluation after Mitigation

Scenario 3: Tampering with Cargo or Ship's Store and Unauthorized Remodeling of Important Equipment, Machinery or Systems

Port facilities	Likelihood value	Impact value	Vulnerability value	Risk value	Risk rank
(1) Channel (River; a few number of international ship sailings)	2	1	5	10	D
(2) Anchorage and basin	2	1	4	8	D
(3) Wharf	2	2	3	12	D
(4) Storage and handling area	2	2	3	12	D
(5) Warehouse	2	1	4	8	D
(6) Cargo handling equipment	2	2	3	12	D
(7) Control center	2	2	4	16	C
(8) Port office	2	2	4	16	C
(9) Substation (Distributor)	2	1	4	8	D
(10) Fresh water supply point	2	1	3	6	D
(11) Fresh water supply tank	2	1	4	8	D
(12) Electricity and city gas	2	1	3	6	D
(13) International ship (Dangerous goods)	2	3	3	18	C
(14) Tugboat, Pilot boat	2	1	4	8	D

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

9. Revised Risk Evaluation after Mitigation

Summary of risk evaluation


Port Facilities	Threat Scenario No.									
	1	2	3	4	5	6	7	8	9	Max
(1) Channel (River; a few number of international ship sailings)	C	D	C				D	D	D	C
(2) Anchorage and basin	D	D	D				D	D	D	D
(3) Wharf	C	D	C	C	C		D	D	D	C
(4) Storage and handling area	C	D	C	C	C				D	C
(5) Warehouse	D	D	D	D	D				D	D
(6) Cargo handling equipment	C	D	C				D		D	C
(7) Control center	C	C	C						D	C
(8) Port office	C	C	C						D	C
(9) Substation (Distributor)	D	D	D						D	D
(10) Fresh water supply point	D	D	D						D	D
(11) Fresh water supply tank	D	D	D						D	D
(12) Electricity and city gas	D	D	D						D	D
(13) International ship (Dangerous goods)	C	C	C	C	C	C	D	D	D	C
(14) Tugboat, Pilot boat	D	C	D	D	D	D	D	D	D	C
(15) Road	D		D						D	D
(16) Neighboring area	C		C						D	C
Max	C	C	C	C	C	C	D	D	D	C

JICA Study on the Port Security Enhancement Program of the Major Indonesian Public Ports

JICA - DGST Workshop ISPS Code

Thank you for your Attention

Terima Kasih



Outline of Port Facility Security Plan Manual

JICA Study Team on the Port Security
Enhancement Program of Major
Indonesian Public Ports

Port Facility Security Plan

ISPS Code Part A

A PFSP shall be developed and maintained,
on the basis of PFSA, for the each port
facility, adequate for the ship/port interface

based on a PFSA

↓
different port → different PFSP

↓ **HOWEVER**

min. requirement in ISPS Code

↓ **MOREOVER**

security measure → limited

- fencing
- access control
- patrol

↓
Standard Form

Characteristic of PFSP Form

1. Avoid omissions

- easy to make by RSO
- easy to check by DGST

2. Customizable

- forms for { Container
Passenger ship
General cargo (multipurpose)

3. Practical

- Procedures for { Access control
Monitoring
Maintenance Work
DoS etc.

Outline of PFSP Form

- Main Body
- Supplementary Figures
- Appendices
- Annexes

Main Body

- General Provision
- Security Measures Pegged to Security Level
- Installation and Maintenance of Facilities
- Designation of PFSO
- Training, Drills and Exercises
- Audit
- Information Management Method
- Response to Occurrence of Security Hazard
- Amendment of PFSP

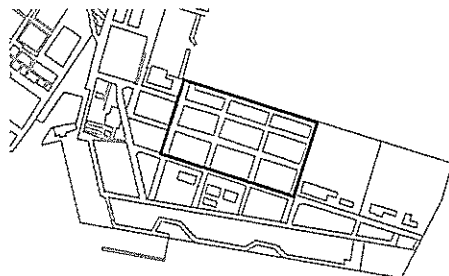
Supplementary Figures

- Location of the Facility
- Location of the Restricted Area
- Layout Plan of the Facility
- Security Organization

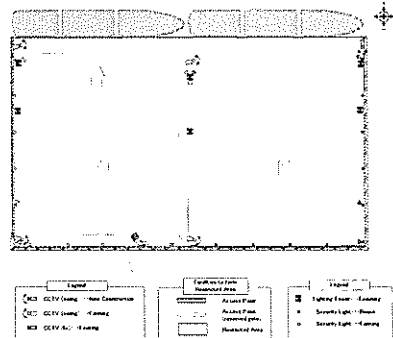
Location of the Facility

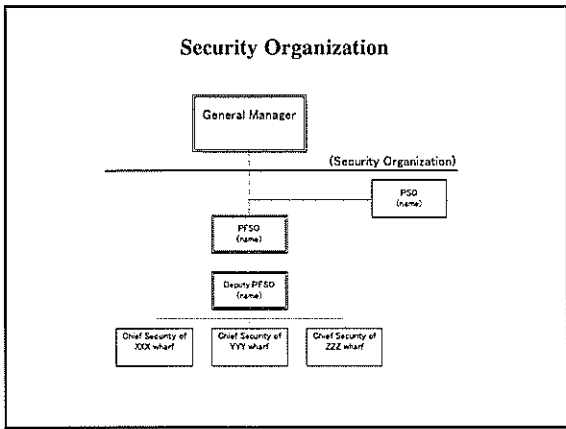


Location of the Restricted Area



Layout Plan of the Facility





- ## Appendixes
- Security Measures during Interim Period
 - Access Control
 - Monitoring Security
 - Maintenance Works
 - Document Management Rules
 - Emergency Management Plan
 - Declaration of Security
 - Evacuation Route

Security Measures during Interim Period

Security Control Level		Level 1	Level 2	Level 3
Monitoring Method	Monitoring	Dynamical hours		
	Frequency	Every 4 hours		
	Procedure	By car or on foot		
	Route	Random		
Monitoring Items	Along the Restricted Area	Suspicious persons and goods	Strengthen the measure of Level 1 Patrol every 3 hours	Address and security guards shall be posted
	at Gate	Suspicious persons and goods		
	Inside of the Restricted Area	Storage tank, antic. warehouse, etc		
	Alongside the quay	Introducer used in a ship from a ladder or a mooring rope		
	Water area	Suspicious boat, goods		

- ### Access Control
- #### Category of Entrance
- Port User (by foot or otherwise)
 - Container Truck
 - Cargo truck
 - Construction/Maintenance Vehicle
 - Ships Stores/Equipment
 - Ships Crew's exit and return entry
 - Taxi
 - Emergency Service Vehicle

Port User (by foot or otherwise)

Security Level	Level 1	Level 2	Level 3
Foot or Vehicle Entry	<ul style="list-style-type: none"> •Request to stop •Ask all entering persons to show ID card 	<ul style="list-style-type: none"> •Same as the left column •Check ID photo and the face for 10 out of every 100 	Port shall be closed
Baggage	<ul style="list-style-type: none"> •Check appearance of baggage 	<ul style="list-style-type: none"> •Confirm contents of baggage for 10 out of 100 	

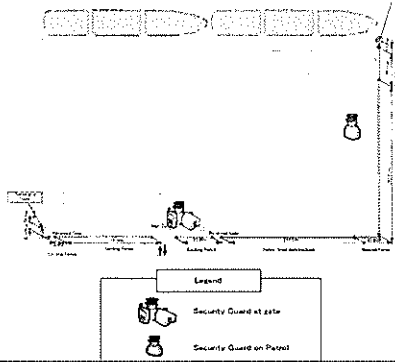
If the level is reached to Level 3, port users shall immediately be evacuated from the restricted area following the instruction of PFSO.

Container Truck

Security Level	Level 1	Level 2	Level 3
Vehicle	<ul style="list-style-type: none"> •Request to stop •Confirm documents 	•Same as the left column	Port shall be closed
Driver	<ul style="list-style-type: none"> •Ask to show ID card for 10 out of every 100 	•Ask all drivers to show ID card	
Helper	<ul style="list-style-type: none"> •Admit entrance on guarantee of driver 	•Same as the left column	
Full Container	<ul style="list-style-type: none"> •Check documents and appearance 	•Same as the left column	
Empty Container	<ul style="list-style-type: none"> •Check documents and confirm inside 	•Same as the left column	

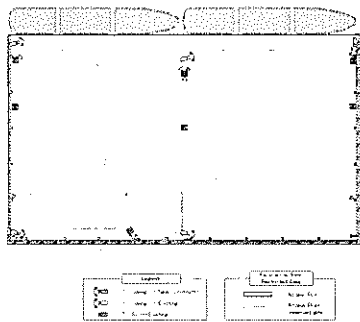
In the event of level 3, drivers in the restricted area shall stop operation, leave the car and immediately evacuate the area following the instruction of PFSO.

Monitoring Security



Security Level	Level 1	Level 2	Level 3
by manpower: mutual monitoring (security guard and workers in the restricted area)	(method) • monitoring hours: • monitoring location: (items) • fence and boundary: • gate: • within the yard: • alongside the quay:	• i • j	• c • g
by equipment (CCTV system)	(method) • monitoring hours: • monitoring location: (items) • set up for equipment: • fence and boundary: • gate: • within the yard: • alongside the quay:		

Maintenance Works



Description	Items to be Checked	Daily Inspection	Periodical Inspection
Fence and Gate		• j	• C • C
Security Light	Lighting Condition	• E	• C • C • C
Monitoring System	CCTV Camera CCTV Monitor	• m • s	• Cr • C
Communication System	VHF Radio Telephone Fax	• C	• C • C

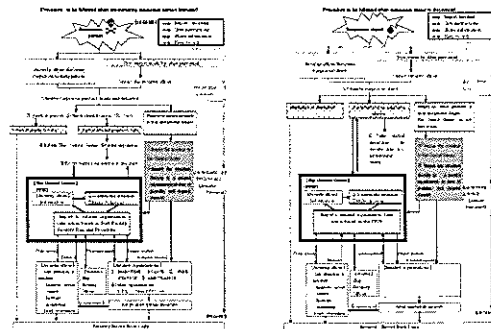
Document Management Rules

PFSA } Confidential Documents
PFSP }

need to establish management rules

- Custody of the documents
- organization

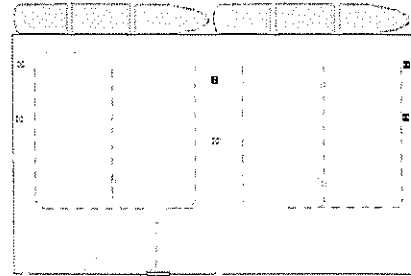
Emergency Management Plan



Declaration of Security (DoS)

- Requirement of DoS from a ship from a port
- Who request completion of DoS?
- Procedure for completion of DoS requested by a port requested by a ship

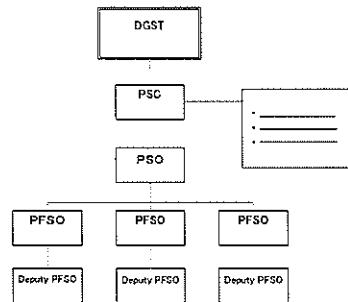
Evacuation Route



Annexes

- Composition of the Port Security Committee
- Emergency Contact List
- Format of DoS
- Format of Security Log
- Contrast Chart for ISPS Code and PFSP

Composition of the Port Security Committee



Emergency Contact List

Security Officer

Organization/Title	Name	Tel.	Remarks
PFSO			
Deputy PFSO			

Port of XXXXX

Organization/Title	Name	Tel.	Remarks
ADPEL			
KPLP/PSO			
KPPP			
PORT HEALTH			
IMMIGRATION			
CUSTOMS			

Form of DoS (partial)

Form of a Declaration of Security between a ship and a port facility¹

DECLARATION OF SECURITY

Name of Ship: _____
 Port of Registry: _____
 IMO Number: _____
 Name of Port Facility: _____

This Declaration of Security is valid from _____ until _____, for the following activities

(list the activities with relevant details)

under the following security levels

Security level(s) for the ship: _____
 Security level(s) for the port facility: _____

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of Part A of the International Code for the Security of Ships and of Port Facilities

Form of the Security Log

- Test, Maintenance & Breakdown Record for Security Equipment and Devices
- Security Threats and Security Incidents
- Training Drills and Exercises
- Change in Security Level
- Completion of DoS
- ISPS Inapplicable Ship Calling at the Port and Security Measures Conducted
- Enforcement of Audit

No.1 Test, Maintenance & Breakdown Record for Security Equipment and Devices

Date	Classification	Outline of Occurrence (details to be attached)	Countermeasure (details to be attached)	Recorded by (PFSSO)
	1.Test 2.Maintenance 3.Breakdown			
	1.Test 2.Maintenance 3.Breakdown			
	1.Test 2.Maintenance 3.Breakdown			
	1.Test 2.Maintenance 3.Breakdown			

No.2 Security Threats and Security Incidents

Date	Classification	Outline of Occurrence	Countermeasure	Recorded by (PFSSO)
	1.Threats 2.Incidents			
	1.Threats 2.Incidents			
	1.Threats 2.Incidents			
	1.Threats 2.Incidents			

No.3 Training, drills and Exercises

Date	Classification	Outline (details to be attached)	Recorded by (PFSSO)
	1.Training 2.Drills 3.Exercises		
	1.Training 2.Drills 3.Exercises		
	1.Training 2.Drills 3.Exercises		
	1.Training 2.Drills 3.Exercises		

Contrast Chart for ISPS Code and PFSP

ISPS Code No.	ISPS Code	PFSP
Part A		
16.1	General	1.1 Feature of the Plan
16.2	Approval of the Plan	(duty of the Contracting Government)
16.4	Combined with port security plan	not applicable
16.6	Format and protection of the Plan	7 Information management method *
16.7	Protection from unauthorized access	same as above
16.8	PFSP for more than one port facility	1.2 Application
17.1	Designation of PFSSO	4.1 Designation of PFSSO
17.2	Duties and responsibilities of PFSSO	same as above
17.3	PFSSO support	same as above
18	Training Drills & Exercises	5 Training, drills and exercises on port *
Part B		
16.1	PFSSO's responsibility to prepare PFSP	4.2 Duties of the PFSSO
16.2	PFSA and PFSP	1.1 Feature of the Plan

Thank You

JICA - DGST Workshop ISPS Code

Outline of Action Plan on Port Security

1

JICA - DGST Workshop ISPS Code

Action Plan Timeline

- ★ Communication to IMO
- ★ Joint seminar
- ← Jica Study on Port Security
- ← Capacity Building
- ← Dual Plan Do See Action Cycle
- ← Security equipment Installation
- ← Port Security Training in Japan
- * Internal Audit
- # External Audit

Minister Meeting

Up Date

2

JICA - DGST Workshop ISPS Code

Min-Do-Sec of Ministry of Communications

Plan-Do-See of Port Measurement Body

3

JICA - DGST Workshop ISPS Code

Phase I

The Study on the Port Security Enhancement Program Major Indonesia Public Ports by Jica Study Team

April 2005 to June 2006 (PLAN Do SEE)

4

JICA - DGST Workshop ISPS Code

Out Put Image:

- * Recommendation for Security Equipments and training, drill and exercise
- * Preparation for PFSA and PFSP
- * Manual for PFSA and PFSP

5

JICA - DGST Workshop ISPS Code

Phase II

July 2006 to 2007 (DO and SEE)

- * Enforce PFSA by DEA with the manual
- * Enforce Self Assessment or Internal Audit by PELINDO
- * REVIEW PFSA and PLAN
- * Training, Drill and Exercise and Capacity Building

6

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code


Self Assessment

* MSC Circulation 1131

**APPENDIX 1:
VOLUNTARY SELF-ASSESSMENT
QUESTIONNAIRE FOR CONTRACTING
GOVERNMENTS**

**APPENDIX 2:
VOLUNTARY SELF-ASSESSMENT TOOL FOR
PORT FACILITY**

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports



7

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

APPENDIX 1

**QUESTIONNAIRE FOR CONTRACTING
GOVERNMENTS**

1 Implementation Process

2 Port Facility Security Assessment (PFSA)


3 Port Facility Security Plans (PFSPs)

4 Security Levels

5 Declaration of Security

6 Delegation of Tasks and Duties

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports



8

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code


Appendix 2

(i) Port Facility Overview:

(ii) Particular characteristics of the port facility, if any, including the vessel traffic, which may increase the likelihood of being the target of a security incident.

1. Ensuring the performance of port facility security duties (ISPS Code sections A/14.2.1 and A/14.3)

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports



9

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code


Appendix 2 continue

2. Controlling access to the port facility (ISPS Code sections A/14.2.2, A/14.2.1 and A/14.3)

3. Monitoring of the port facility, including anchoring and berthing area(s) (ISPS Code sections A/14.2.3 and A/14.3)

4. Monitoring of restricted areas (ISPS Code sections A/14.2.4 and A/14.3)

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports



10

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code


Appendix 2 continue

5. Supervising the handling of cargo (ISPS Code sections A/14.2.5 and A/14.3)

6. Supervising the handling of ship's stores (ISPS Code sections A/14.2.6 and A/14.3)

7. Ensuring security communication is readily available (ISPS Code sections A/14.2.7 and A/14.3)

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports



11


JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Appendix 2 continue

8. Training, Drills and Exercises (ISPS Code section A/18)

9. Miscellaneous

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports



12

JICA - DGST Workshop ISPS Code

Phase III

2008 to 2009 (Action and Rolling Plan)

- * Action and Rolling Plan (Update)
- * External Audit by DEA with the Manual
- * Training, Drill and Exercise

13

JICA - DGST Workshop ISPS Code

Contentes of Action Plan

- * Communication to IMO
- * Jica Study on port security
- * Capacity building
- * Security equipment installation
- * Port security training in Japan
- * Self Assessment
- * Audit
- * Revise
- * Upgrade (new plan)
- * Verification
- * SoCPF

14

JICA - DGST Workshop ISPS Code

Audit

15

JICA - DGST Workshop ISPS Code

Internal Audit or External Audit

- * **Internal Audit** : conducted by auditors from the organization who are responsible for PFSP, but not PFSO.
- * **External Audit** : conducted by auditors from outside the organization.

16

JICA - DGST Workshop ISPS Code

Audit Planning

- * **Plan** What you are going to do
- * **Do** what you have planned to do
- * **See** whether what you have done has been according to the plan
- * **Action** on the difference to improve the plan (Rolling Plan)

17

JICA - DGST Workshop ISPS Code

Clasification

- * **Audit 1** audit security activity in the port facility by internal audit team including compliance of PFSP with ISPS Code
- * **Audit 2** audit security activity in the port facility by external audit team including compliance of PFSP with ISPS Code
- * **Audit 3** audit compliance of security assessment with ISPS Code
- * **Audit 4** audit compatibility between PFSP and PFSA
- * **Audit 5** audit compliance of PFSP with ISPS Code
- * **Audit 6** audit compliance of legislation and regulation with ISPS Code
- * **Audit 7** audit central government duty

18

JICA - DGST Workshop ISPS Code

Audit 1	Internal audit	Security activity
Audit 2	External audit	Security activity
Audit 3	External audit	PFSA should be compliant with ISPS Code
Audit 4	External audit	PFSP should be compatible with PFSA
Audit 5	External audit	PFSP should be compliant with ISPS Code
Audit 6	External audit	Legislation or regulation should be compliant with ISPS Code
Audit 7	External audit	Central government duty

19

JICA - DGST Workshop ISPS Code

Audit 1/2

- * Almost same as Security Test
- * Countermeasures
- * Training, drill and exercise
- * Document [Dos, Communication chart, Evidence of approval, Record form, Security Confidential Information and so on]
- * Port Security Committee
- * Security Organization

20

JICA - DGST Workshop ISPS Code

Audit 3

- * PFSA should be compliant with ISPS Code
- * Code A 15.2 RSO
- * Code A 15.2.1 Approved for compliance with section 15 by government
- * Evidence of the approval
- * Code B 15.2 Another RSO is allowed verifying compliance

21

JICA - DGST Workshop ISPS Code

Audit 3 continue

- * Code A 15.4 Periodical Review and update
- * Code A15.5
- * Identification and evaluation of important assets and infrastructure
- * Identification of possible threats and likelihood of occurrence
- * Identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability
- * Identification of weakness

22

JICA - DGST Workshop ISPS Code

Audit 3 continue

- * Code A 15.7 A report on completion of the PFSA
- * Summary of how the PFSA conducted
- * Vulnerability Finding
- * Counter measures

23

JICA - DGST Workshop ISPS Code

Audit 4

- * PFSP should be compatible with PFSA
- * Counter measures which were recommend in the PFSA should be described in the PFSP


24

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Audit 5

- * PFSP should be compliant with ISPS Code
- * Code A 16.2 PFSP should be in the working language of the port facility
- * Code A 16.3 .1 to .15

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports




25

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Audit 5 continue

- * Code A 16.6, A 16.7
The PFSP should be protected from unauthorized access or disclosure

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports




26

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Audit 5 continue

- * Code 17.2 Port Facility security officer

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports




27

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Audit 5 Continue

- * Code A 18 Training, drill and exercise
- * PFSO and security personnel should have received training
- * PFSO should participate in exercises

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports




28

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Audit 6/7

- * Legislation and regulation should be compliant with ISPS Code
- * Central government's obligation
- * Chapter X1-2 Regulation 3 government should set security level and inform to port facility
- * Chapter X1-2 Regulation 2 Government should decide extent of application of this chapter and of the relevant section of Part A to the port facility which are occasionally required to serve international vessel
- * Chapter X1-2 Regulation
- * Government communicated to IMO a list

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports











29

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code


ASEAN – Japan Joint Seminar

Japan leads implementation of Port Security in ASEAN countries

- * Joint Seminar in Indonesia 
- * Joint Seminar in Philippines 
- * Joint Seminar in Indonesia 
- * Joint Seminar in Cambodia 
- * Joint Seminar in Myanmar 
- * Joint Seminar in Thailand 
- * Joint Seminar in Myanmar 
- * Joint Seminar in Vietnam 

Meeting for minister of Transportation and Security(G8, China, Korea, Singapore) in Jan, 2006

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports




30

JICA JICA International Cooperation Agency JICA - DGST Workshop ISPS Code

APEC ISPS IMPLEMENTATION ASSISTANCE PROGRAM

- * The Philippines in March 2005
- * APEC- Jica Joint Seminar in Indonesia in December 2005
- * Review in 2006

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports




31

JICA JICA International Cooperation Agency JICA - DGST Workshop ISPS Code

Jica training course in Japan

- *For a month in fall yokohama
- *Awareness training by MLIT or OCDI
- *Site survey
- *Introduction of port security in Japan
- *Asean- Japan Workshop
- *Exercise and drill

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports



32

JICA JICA International Cooperation Agency JICA - DGST Workshop ISPS Code

Terima Kasih

ARIGATOU

GOZAIMASITA

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports



33

Port of Tanjung Intan, Cilacap

Port Facility Security

JICA Study Team on the Port Security
Enhancement Program of Major
Indonesian Public Ports

Acknowledgement

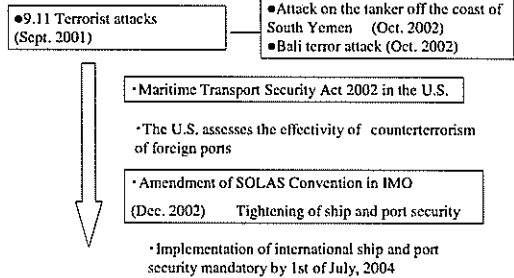
- This study was based on the survey conducted on 17May ~ 19 May, 2005.
- We apologize in the areas of ignorance and/or misunderstanding with regards to your operations and procedures.

Table of Contents

1. Background of Tightening Port Security
2. PFSA for Port of Tanjung Intan, Cilacap
3. PFSP for Port of Tanjung Intan, Cilacap
 - (1) Restricted Area for Each Pier
 - (2) Port Security Facilities to be Provided
 - (3) Access Control to be Conducted at Gates
 - (4) Maintenance Work
 - (5) Procedure of Emergency Management Plan
 - (6) Evacuation Route
 - (7) Emergency Contact List
 - (8) Contrast Chart for ISPS Code and PFSP

I. Background of Tightening Port Security

(1) Background of the Amendment of SOLAS Convention



(2) What is SOLAS Convention?

➤ Formally each shipping nation had its own maritime laws. However in response to the Titanic disaster, which resulted in death of 1,500 passengers and crew out of over 2,000, treaty for international maritime safety was concluded in 1914

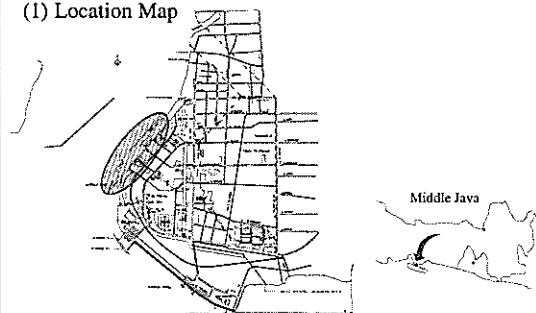
(3) Outline of Amendment of SOLAS Convention

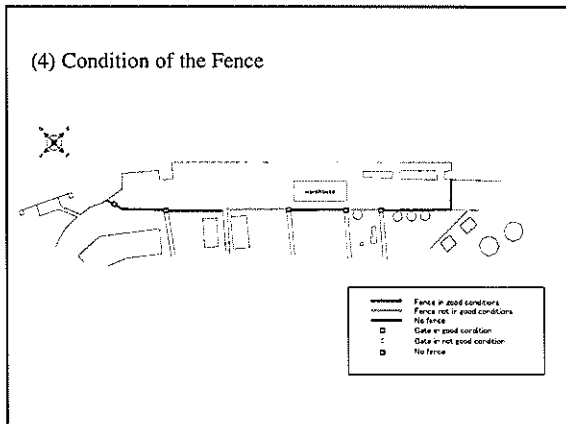
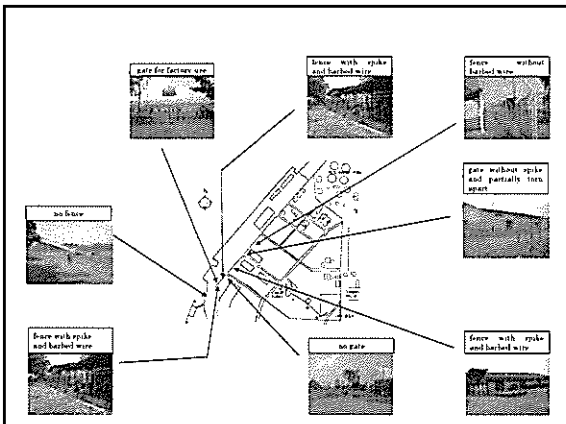
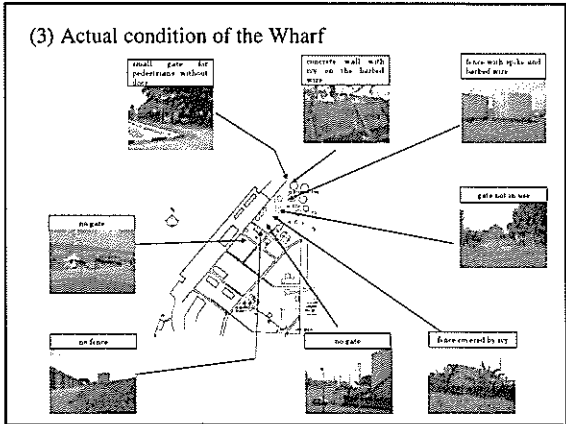
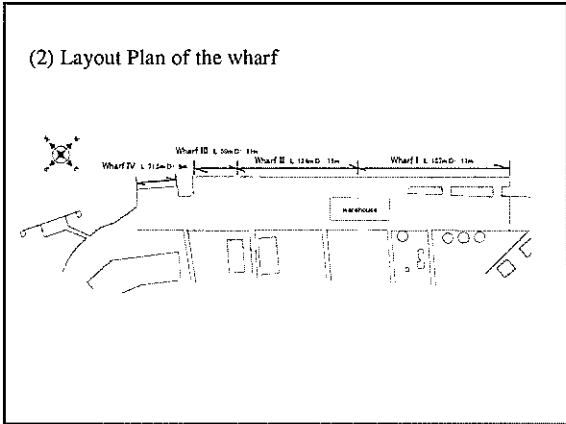
➤ To improve the reliability of international sea transportation system by having the ship owners, the port operator and the port administrator take security measures

➤ To prevent an unlawful act related to international sea transportation by not admitting a ship identified to be a threat to enter the port

2. PFSA for Port of Tanjung Intan, Cilacap

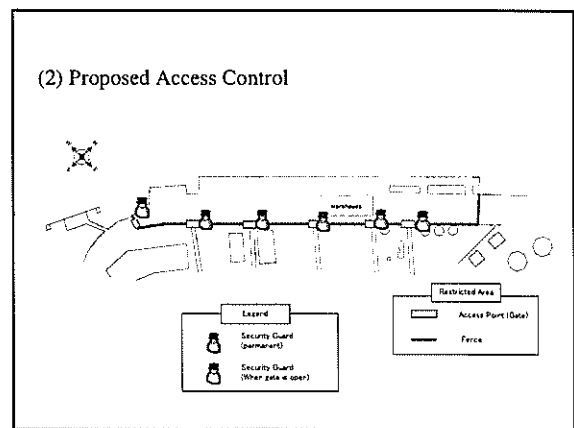
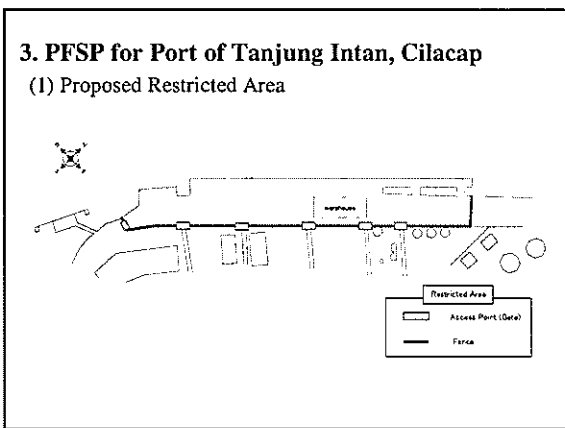
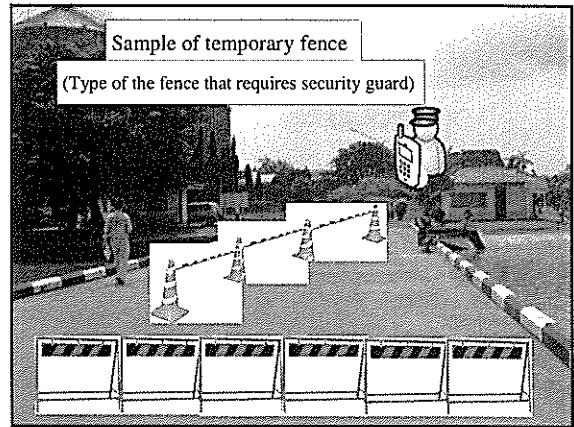
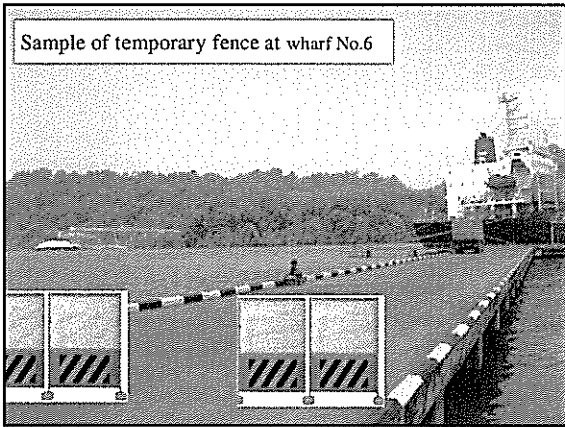
(1) Location Map





- ### (5) Current Situation of Tanjung Intan Port
- No access control conducted
 - Fence and Gates were very old and have tears
 - Many people were fishing on the wharf
 - No container handling
 - Residence and cornfield inside the port area

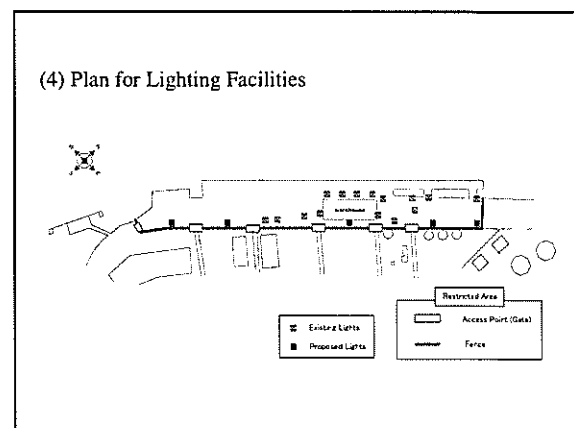
- ### (6) Recommendation
- Install new fence and gates with outrigger and barbed wire
 - Install additional security lights
 - Establish a procedure for access control
 - temporary fence



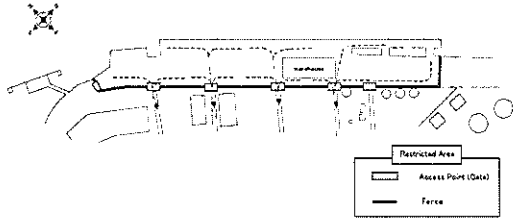
(3) Access Control to be conducted at gates

Access Control for Customs and ISPS Code

- Different Purpose
 - Customs
 - Avoid smuggling
 - Avoid goods taking out illegally
 - EXIT CONTROL
 - ISPS
 - Avoid Suspicious Person/Goods inside the Restricted Area
 - Protect from Terrorism
 - ENTRY CONTROL



(5) Evacuation Procedure



JICA - DGST Workshop ISPS Code

Port Facility Security Assessment and Port Facility Security Plan for Tenau Port

1

JICA - DGST Workshop ISPS Code

2

JICA - DGST Workshop ISPS Code

About Berth

- Total length of the wharf is 610m and water depth is -3m to -8.0m.
- Berth length for international vessels (Multi-purpose wharf) is 237m.
- Berth length for domestic cargo vessels (Inter-islands wharf and Pelra wharf for sail boat) is 273m
- Berth length for domestic passenger is 100m.

3

JICA - DGST Workshop ISPS Code

Tenau Port

4

JICA - DGST Workshop ISPS Code

Port facility

- Warehouse
- Storage area
- Cargo handling equipment
- Port office and control center
- Power plant
- Bunkering point
- Water supply point
- Water storage tank Storage capacity: 870 tons
- Max. supply: 40 tons/hour
- Well pump: 276ton/day
- Adjacent area: Fishery wharf

5

JICA - DGST Workshop ISPS Code

Risk evaluation

```

graph TD
    A[Selection of Port Facilities Relevant to International Vessel Calls] --> B[Evaluation of the Likelihood of Threat Scenario Occurrence]
    B --> C[Impact Evaluation in Occurrence of Threats]
    C --> D[Vulnerability Evaluation]
    D --> E[Risk Evaluation]
  
```

6

JICA - DGST Workshop ISPS Code

Important Facility to be protected

- Wharf, handling yard and container storage yard
- Cargo handling equipment
- Ship
- Lightning system
- Distributor
- Water point
- Bunker point

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

7

JICA - DGST Workshop ISPS Code

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

8

JICA - DGST Workshop ISPS Code

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

9

JICA - DGST Workshop ISPS Code

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

10

JICA - DGST Workshop ISPS Code

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

11

JICA - DGST Workshop ISPS Code

Recommendations

General

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports


12

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

(1) Restricted area and important facilities to be protected

- Multi-Purpose Wharf should be strictly fenced off by a fence with outrigger and a new gate
- Important facilities to be fenced off by the fence and to be protected should be as follows.
- Wharf, handling yard and container storage yard
- Cargo handling equipment
- Ship
- Lightning system
- Distributor

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports




13

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

(2) Access control

- To introduce a procedure to implement intensive access control concerning personnel, vehicle and cargo at the new gate
- To take measures such as the issuance of visitor card/ID card to prevent unauthorized person's access
- To ensure that the external appearance of cargo is checked
- To inspect suspicious goods such as explosives of a vehicle using mirrors and metal detectors

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports




14

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

(3) Lighting

- To installed new lighting along the boundary

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports




15

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

(4) CCTV Camera

- To installed CCTV camera to monitor restricted area.

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports




16

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

(5) Monitoring of terminal area

- To introduce a procedure to implement intensive inspection of personnel and vehicles, cargo appearance check and suspicious goods check inside restricted area
- To intensively patrol boundary

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports




17

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

(6) Monitoring of water area

- Patrol of the water area including the channel and anchorage area should be enhanced.

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports



18

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

(7) Communication with related organizations

- A procedure to ensure communication between security personnel and relevant organization should be introduced.

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

19

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

(8) Response to emergency

- An emergency communication system and emergency response plan including initial action order should be established and they should be included in the PFSP

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

20

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

(9) Training

- Training, drills and exercises should be conducted as necessary

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

21

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

(10) Others

- Domestic passenger terminal should be fenced off strictly for safety and security reasons.
- The pilot office apart from Tenau Port should be fenced off and subject to access control
- Port office including ADPEL and KPLP office should be subject to access control

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

22

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

The Plan

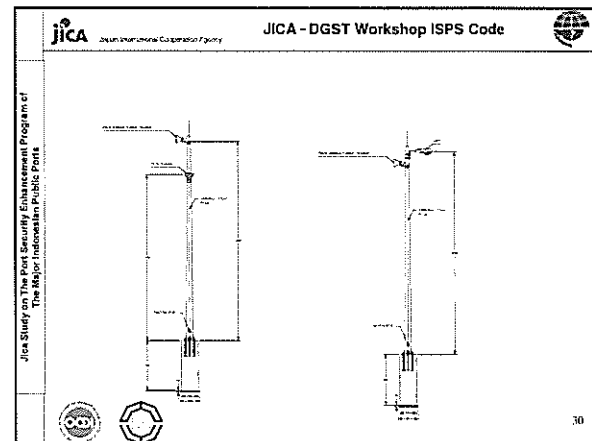
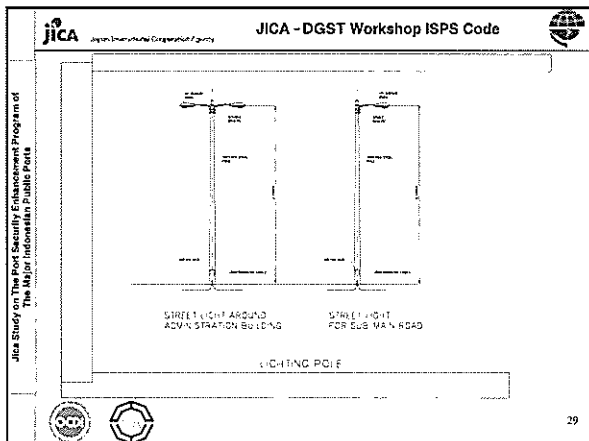
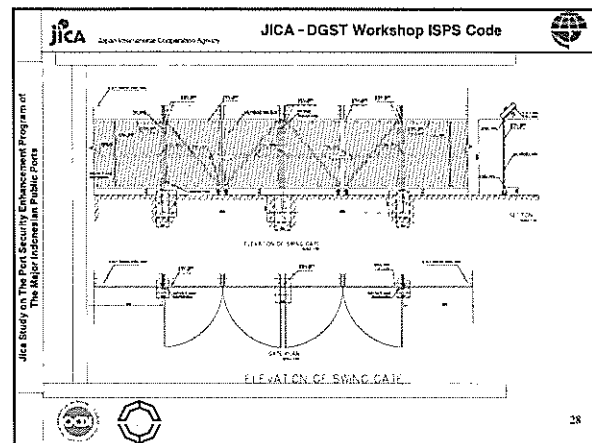
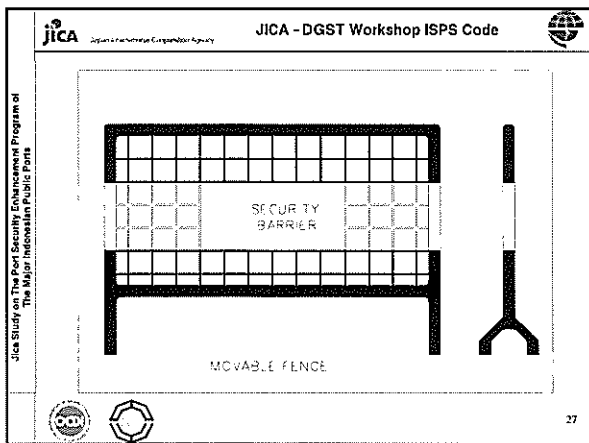
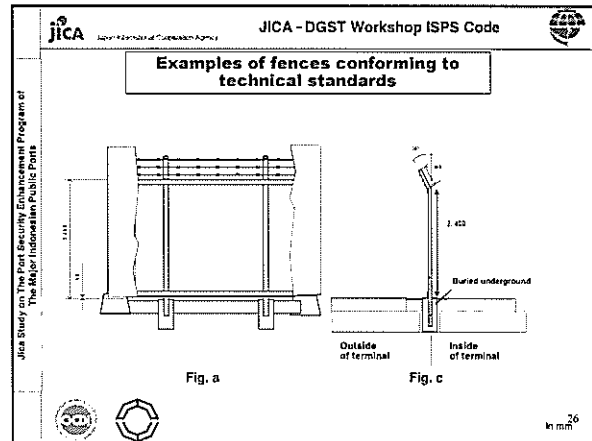
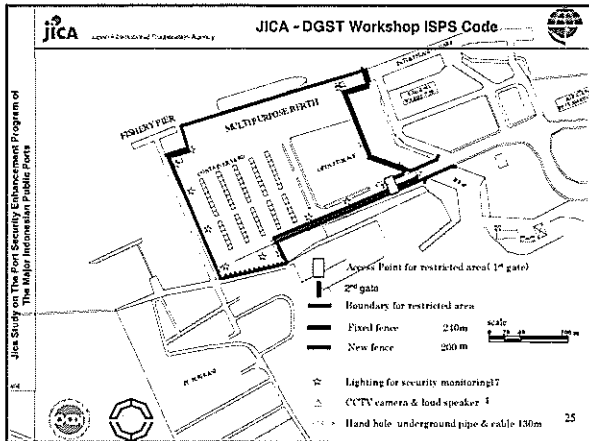
JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

23

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

JICA Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

24



JICA - DGST Workshop ISPS Code

Access Control

*Port User (by foot or otherwise)

Security Level	Level 1	Level 2	Level 3
Foot or	• Request to stop	• Same as on the left	
Vehicle Entry	• Ask for ID card all those wishing to enter	• Check ID photo and the face for 10 out of every 100	Port shall be closed
Baggage	• Check appearance of baggage	• Confirm contents of baggage for 10 out of 100	

31

JICA - DGST Workshop ISPS Code

*Container Truck

Security Level	Level 1	Level 2	Level 3
Vehicle	• Request to stop • Confirm documents	• Same as on the left	Port shall be closed
Driver	• Ask for ID card for 10 out of every 100	• Ask all drivers for ID card	
Helper	• Admit entrance on guarantee of driver	• Same as on the left	
Full Container	• Check documents and appearance	• Same as on the left	
Empty Container	• Check documents and confirm inside	• Same as on the left	

32

JICA - DGST Workshop ISPS Code

*Cargo Truck

Security Level	Level 1	Level 2	Level 3
Vehicle	• Request to stop • Confirm documents	• Same as on the left	Port shall be closed
Driver	• Ask for ID card for 10 out of every 100	• Ask all drivers for ID card	
Helper	• Admit entrance on guarantee of driver	• Same as on the left	
Freight	• Check Documents & appearance of cargo	• Inspect and confirm cargo against documents	

33

JICA - DGST Workshop ISPS Code

*Maintenance Vehicle

Security Level	Level 1	Level 2	Level 3
Vehicle	• Request to stop • Confirm approval with PFSO	• Same as on the left	Port shall be closed
Driver	• Ask all drivers for ID card	• Ask all drivers for ID card • Check ID photo and the face for 10 out of every 100 • Request to fill in form and issue temporary pass when there is no ID card	
Passenger/ Workmen Cargo	• Admit entrance on guarantee of driver/foreman • Check appearance	• Same as above • Inspect contents	

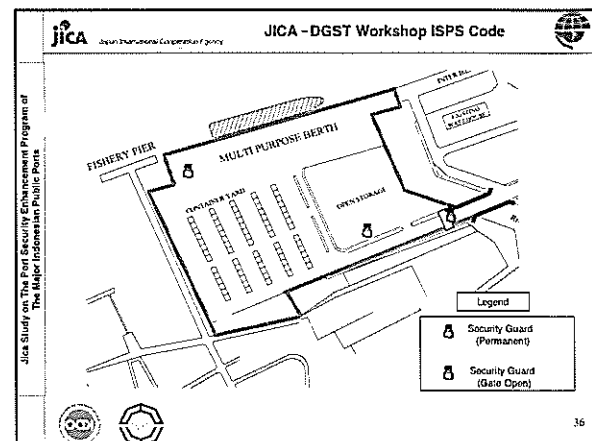
34

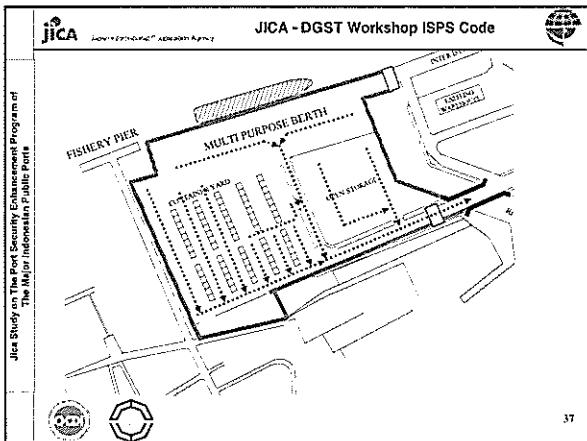
JICA - DGST Workshop ISPS Code

Ship's Stores/Equipment

Security Level	Level 1	Level 2	Level 3
Vehicle	• Request to stop • Check documents	• Request to stop • Confirm documents	Port shall be closed
Driver & Passenger	• Ask all drivers/Passengers for ID card • Check ID photo and face for 50 out of every 100	• Ask all drivers/Passengers for ID card • Check ID photo and the face for all those wishing to enter	
Cargo	• Not necessary to check when under escort • Confirm customs report or work order when there is no escort	• Confirm contents of cargo for 50 out of every 100	

35





- JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code
- ## Evacuation Procedures
1. Evacuate following the instruction of PFSO.
 2. Direct the gate number when evacuating from the restricted area.
 3. Direct the name of facility when evacuating to the building.
 4. PFSO may direct, navigate and confirm that no one fail to escape.
- Jica Study on The Port Security Enhancement Program of The Major Indonesian Public Ports
- 38

JICA Japan International Cooperation Agency JICA - DGST Workshop ISPS Code

Jica Study on The Port Security Enhancement Program of The Major Indonesian Public Ports

Terimakasih
Arigatou
Gozaimashita

39

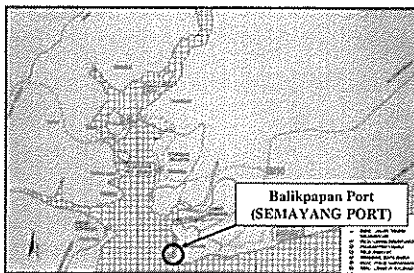
Port Facility Security Assessment & Port Facility Security Plan for Balikpapan (SEMAYANG PORT)

JICA Study-Team
Masaki ONO

Contents

- 1. PFSA for Balikpapan Port (SEMAYANG PORT)**
 - (1) Outline of Balikpapan port
 - (2) Layout Plan of the Port
 - (3) Present Situation of the Port Facility Security Measures
 - (4) Issues of Implementation Port Facility Security Measures
 - (5) Risk Evaluation
 - (6) Recommendation on Port Security
- 2. PFSP for Balikpapan Port (SEMAYANG PORT)**
 - (1) Restricted Area
 - (2) Port Security Facilities to be provided
 - (3) Access Control to be conducted at Gates
 - (4) Maintenance Work
 - (5) Procedure of Emergency Management Plan
 - (6) Emergency Contact List
- 3. Question**

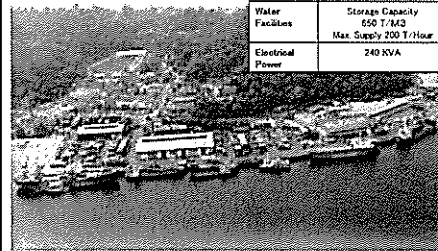
1. PFSA for Balikpapan Port (1) Outline of Balikpapan port



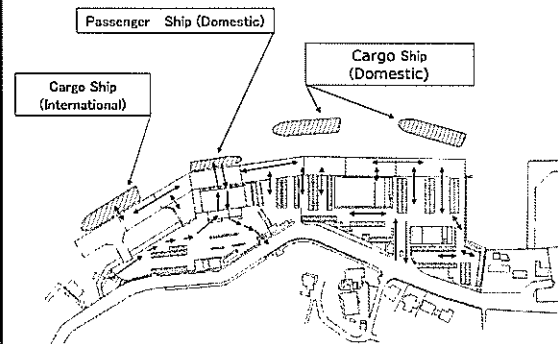
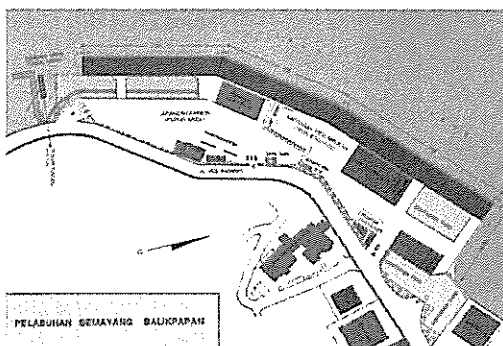
Balikpapan port (SEMAYANG PORT)

Summary of Main Port Facilities

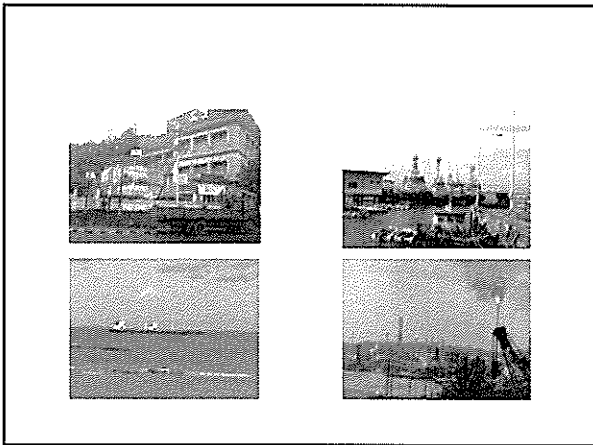
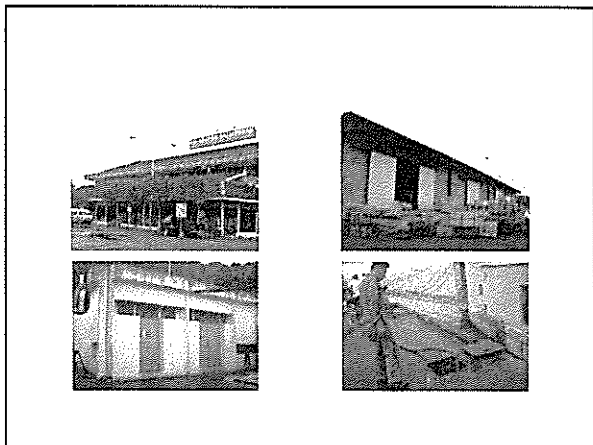
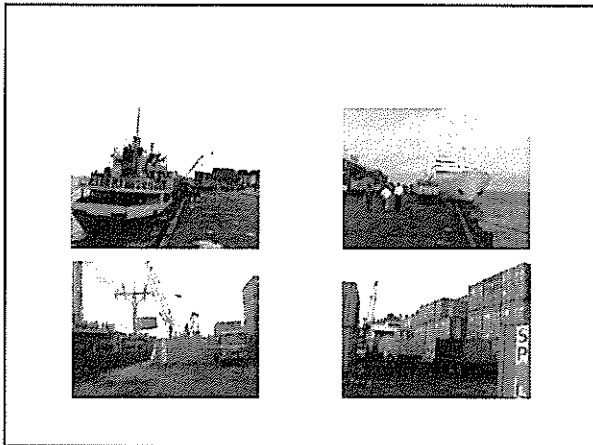
Item	Scale Length or Area	Remarks
Wharf	Length 489 m	Structure: Concrete
Transit Sheds	No.1 Area 2,450 m ²	Structure: Steel
	No.2 Area 1,170 m ²	
Open Storage	Container 11,840 m ²	Structure: Concrete
	Break bulk 815 m ²	
Water Facilities	Storage Capacity 550 T/483	Structure: Concrete
	Max. Supply 200 T/Hour	
Electrical Power	240 KVA	



(2) Layout Plan of the Port

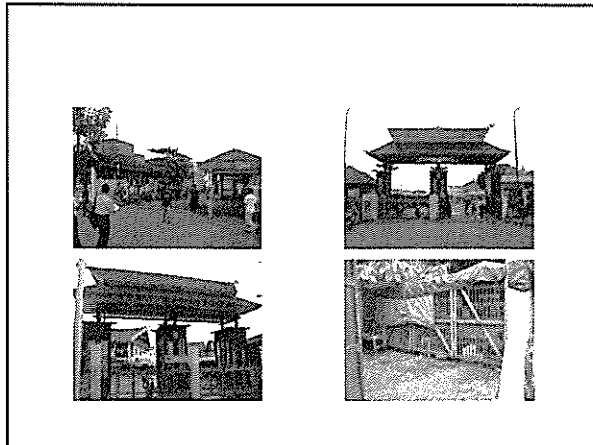
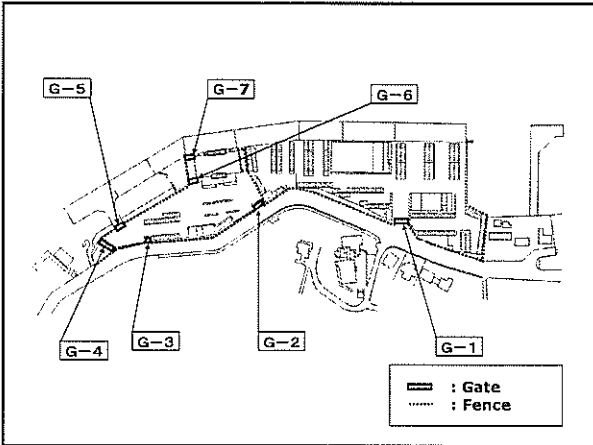


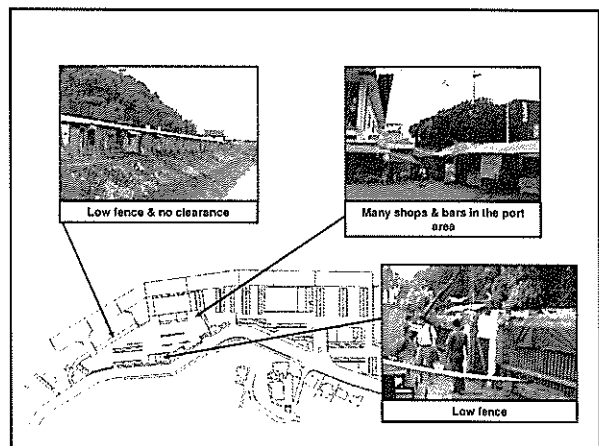
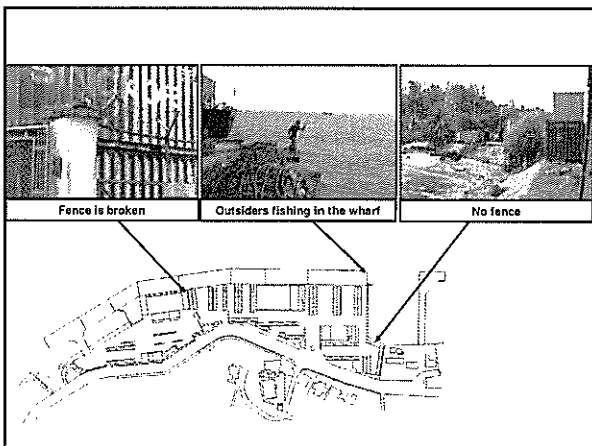
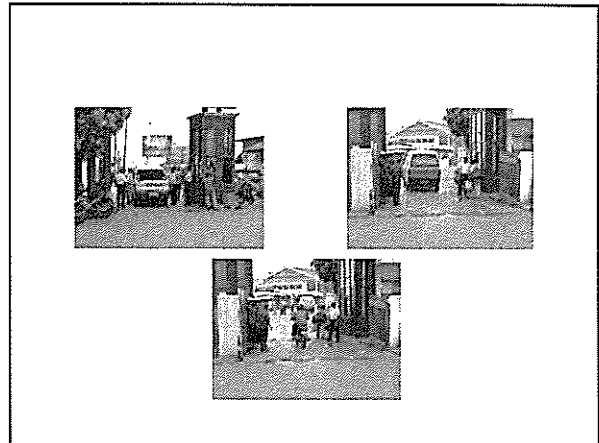
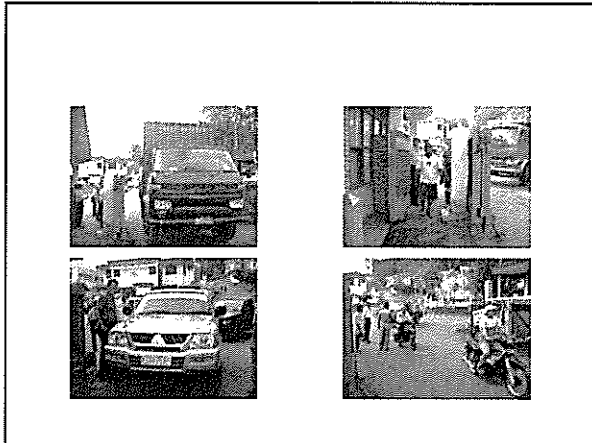
International ship calls are very few, and the main commodity is live stock (cattle) in 2005.



(3) Present Situation of the Port Facility Security Measures

- PELINDO, KPLP and KPPP conduct access control at the main gate of the port and in passenger wharf for safety.
- Neighboring area of the wharf is a commercial area.





**(4) Issues of Implementation
Port Facility Security Measures**

- It is very difficult to separate domestic area from international area and also to separate wharf area from related area including shops and bars by fixed

(5) Risk Evaluation

- Access control is conducted by PELINDO, KPLP, and KPPP at the Main Gate of the port. They check the ID card and ID sticker of persons and vehicles. However, a stricter inspection is necessary.
- No security equipment at the main entrance/gate.
- No unauthorized persons and vehicles can access the cargo berth and passenger berth as security procedures are in place.
- The passenger terminal and cargo handling area are not separated, resulting in dangerous and unsecured conditions.

- ⑤ Since the cargo terminal handles domestic passengers and cargoes mainly, it is not designated as a restricted area.
- ⑥ The terminal area is equipped with a fence and gate. However some part of the fence does not meet standards.
- ⑦ There are many non-secure places, such as small shops and bars for seamen, in the port area. They should be excluded from the restricted area.

(6) Recommendations on the Port Security

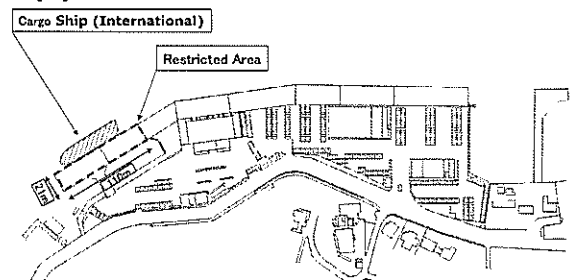
- ① The restricted area should be designated and be enclosed by physical barriers such as fence and gates in order to conduct access control at the gates. In case that a fixed fence would interface with cargo handling the mobile fence should be replaced.
Before international passenger ship berths, the wharf, the mobile fence should be set up and the patrol should be conducted to make sure no suspicious persons or no unusual objects are present in and around the restricted area.

- ② Access control for persons, vehicles and cargo should be conducted strictly to prevent suspicious person and things from entering port facilities.
- ③ Random patrols (intervals and routes) should be executed to ensure the security of facilities and cargo.
- ④ The water area including a channel and an anchorage should be monitored and patrolled periodically. Patrol by a patrol boat is preferable.
- ⑤ In a part of the terminal, the lighting is not sufficient for monitoring during the night. The lighting system should be repaired and improved.

- ⑥ The inspection of person's belongings should be done by using hand-held metal detector at the gate.
- ⑦ In an emergency, a warning against suspicious persons and evacuation directions for ships, passengers, etc. should be given immediately by using a public address (PA) system.
- ⑧ Measures should be taken quickly whenever trouble arises.

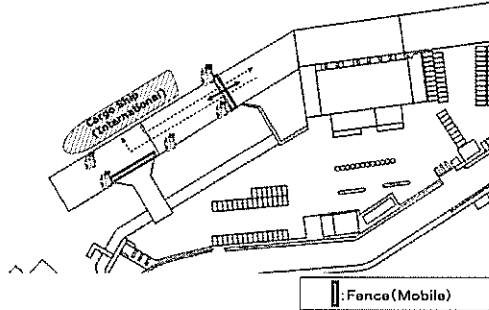
- ⑨ Emergency plan including communication network and instructions in case of emergency should be prepared and put in the PFSP.
- ⑩ To ensure communication between security personnel and a PFSO.
- ⑪ To conduct training, drills and exercises periodically.

2. PFSP for Balikpapan
(1) Restricted Area

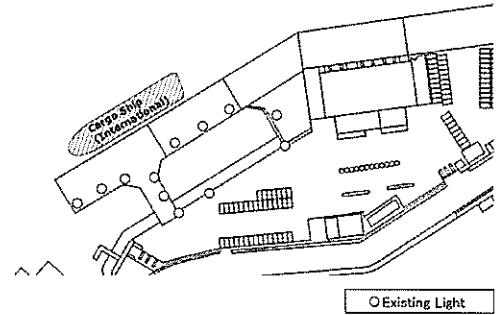


(2) Port Security Facilities to be Provided

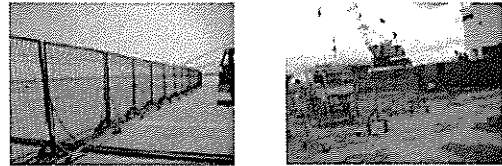
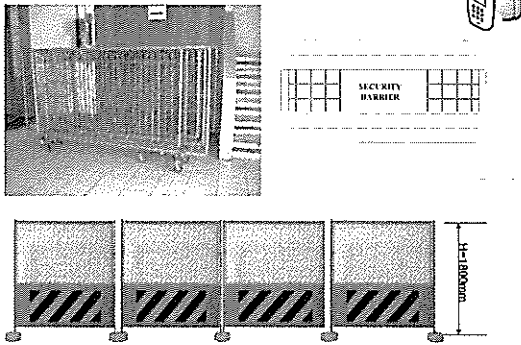
① Fence



② Lighting System



**Temporary Fence
(Type of the fence that requires security guard)**



(3) Access Control to be Conducted at Gates

Category of Entrance

- ① Port User (by foot or otherwise)
 - Container Truck
- ② Cargo Truck
- ③ Construction/Maintenance Vehicle
- ④ Ships Stores/Equipment
- ⑤ Ships Crew
 - Taxi
- ⑥ Emergency Service Vehicle

① Port User (by foot or otherwise)

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Foot or Vehicle Entry	.Request to stop .Ask for ID card all those wishing to enter	.Same as on the left .Check ID photo and the face for 10 out of every 100	.Do not admit entry
Baggage	.Check appearance of baggage	.Confirm contents of baggage for 10 out of 100	.Do not admit entry

② Cargo Truck

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	.Request to stop .Confirm documents	.Same as on the left	.Do not admit entry
Driver	.Ask for ID card for 10 out of every 100	.Ask all drivers for ID card	.Do not admit entry
Helper	.Admit entrance on guarantee of driver	.Same as on the left	.Do not admit entry
Freight	.Check Documents & appearance of cargo	.Inspect and confirm cargo against documents	.Do not admit entry

③ Construction/Maintenance Vehicle

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	.Request to stop .Confirm approval with PFSO	.Same as on the left	.Do not admit entry
Driver	.Ask all drivers for ID card	.Ask all drivers for ID card .Check ID photo and the face for 10 out of every 100 .Request to fill in form and issue temporary pass when there is no ID card	.Do not admit entry
Passenger/ Workmen	.Admit entrance on guarantee of driver/foreman	.Same as above	.Do not admit entry
Cargo	.Check appearance	.Inspect contents	.Do not admit entry

④ Ship's Stores/Equipment

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	.Request to stop .Check documents	.Request to stop .Confirm documents	.Do not admit entry
Driver & Passenger	.Ask all drivers/Passengers for ID card .Check ID photo and face for 50 out of every 100	.Ask all drivers/Passengers for ID card .Check ID photo and the face for all those wishing to enter	.Do not admit entry
Cargo	.Not necessary to check when under escort .Confirm customs report or work order when there is no escort	.Confirm contents of cargo for 50 out of every 100	.Do not admit entry

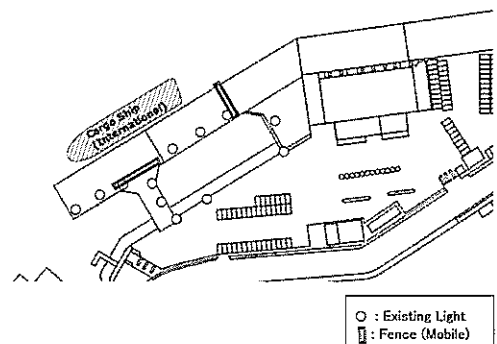
⑤ Ships Crew's Exit and Return Entry

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Ships Crew exit	.Confirm shore pass or ID issued by the ship	.Same as on the left	.Do not admit entry
Ships Crew entry/go on board	.Same as above .Confirm an embarkation order, seamen's book or passport or confirm with the ship	.Same as on the left	.Do not admit entry
Baggage	.Check appearance of baggage	.Confirm contents of baggage for 10 out of 100	.Do not admit entry

⑥ Emergency Service Vehicle

Security level	Security level 1,2 and 3 (Emergency Service personnel not required to have ID)
Vehicle	.Confirm the type of vehicle .Record time of entry into record book
Driver	.Confirm by the type of vehicle
Vehicle Crew	.Same as above

(4) Maintenance Work Layout Plan for Security Facilities

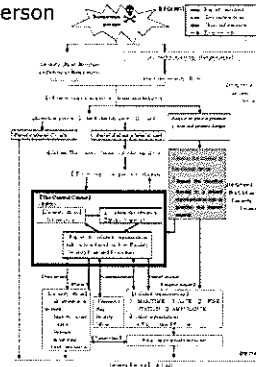


Inspection Procedure

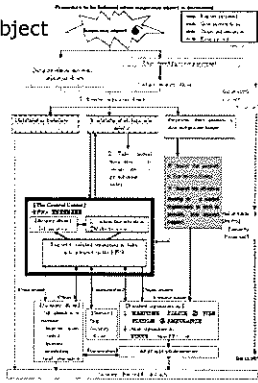
Description	Items to be Checked	Daily Inspection	Periodical Inspection
Fence and Gate		*Visual inspection during patrol (repair, reinforce, or replace if necessary)	*Conduct monthly *Sway and confirm net is not loose
Security Light	Road Light	*Ensure that all security lights are illuminated by visual inspection during patrol	*Conduct annually *Check mounting of lamp fitting *Clean the cover *check cables and switch box
Monitoring System			
Communication System	VHF Radio Telephone Fax	*Check in daily usage	*Conduct annually by the supplier *Cleaning adjustment, and change consumables

(5) Procedure of Emergency Management Plan

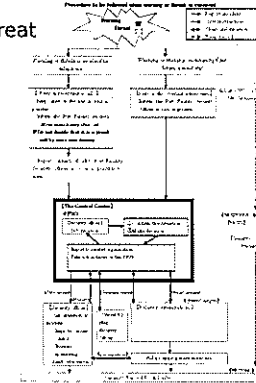
Suspicious Person



Suspicious Object



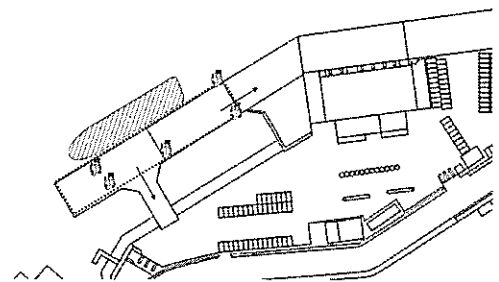
Warning Threat



Evacuation Procedure

- Evacuate following the instruction of PFSO
- Direct the gate number when evacuating from the restricted area
- Direct the name of facility when evacuating to the building
- PFSO may direct, navigate and confirm that no one fail to escape

Evacuate Route



(6) Emergency Contact List

Security Officer

Organization/Title	Tel.	Name	Remarks
PFSO			
Deputy PFSO			

Port of Benoa

Organization/Title	Tel.	Name	Remarks
ADPEL			
KPLP/PSO			
KPPP			
PORT HEALTH			
Fire Department			



Port of Kendari Nusantara Wharf

Port Facility Security

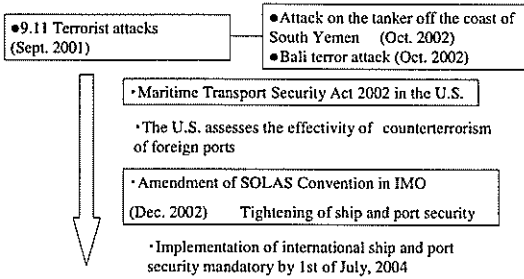
JICA Study Team on the Port Security
Enhancement Program of
Major Indonesian Public Ports

Table of Contents

1. Background of Tightening Port Security
2. PFSA for Kendari Port, Nusantara Wharf
3. PFSP for Kendari Port, Nusantara Wharf
 - (1) Proposed Restricted Area for Nusantara Wharf
 - (2) Port Security Facilities to be provided
 - (3) Access Control to be conducted at Gates
 - (4) Maintenance Work
 - (5) Procedure of Emergency Management Plan
 - (6) Evacuation Route
 - (7) Emergency Contact List
 - (8) Contrast Chart for ISPS Code and PFSP

1. Background of Tightening Port Security

(1) Background of the Amendment of SOLAS Convention



(2) What is SOLAS Convention?

➤ Formally each shipping nation had its own maritime laws. However in response to the Titanic disaster, which resulted in death of 1,500 passengers and crew out of over 2,000, treaty for international maritime safety was concluded in 1914

(3) Outline of Amendment of SOLAS Convention

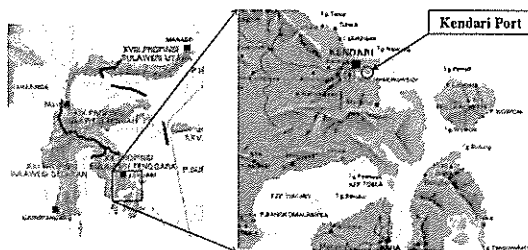
➤ To improve the reliability of international sea transportation system by having the ship owner, the port operator and port administrator take security measures

➤ To prevent an unlawful act related to international sea transportation by not admitting a ship identified to be a threat to enter the port

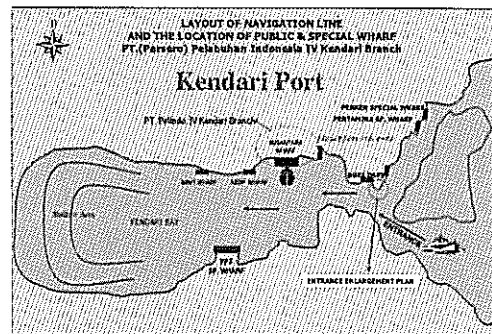
2. PFSA for Kendari Port, Nusantara Wharf

(1) Location of Kendari Port

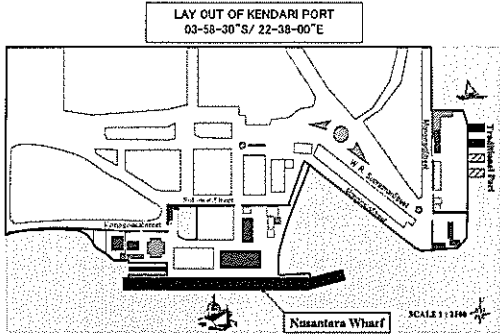
Location of Kendari



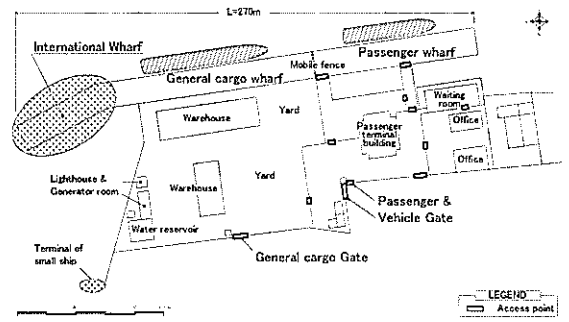
Location of Kendari Port



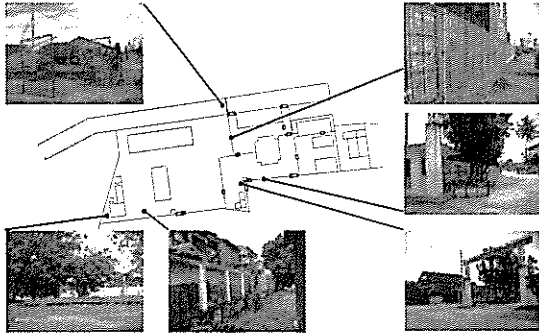
(2) Layout of Kendari Port, Nusantara Wharf



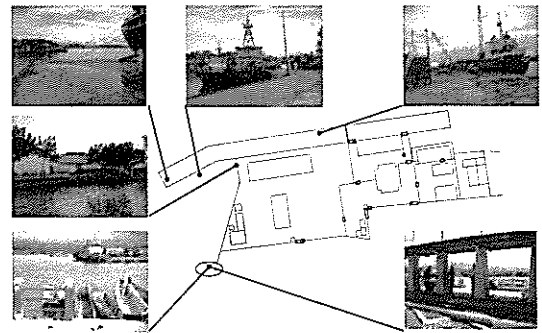
Layout of Nusantara Wharf



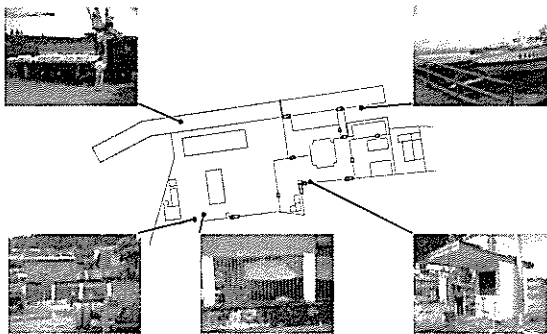
(3) Actual condition of the Nusantara wharf (1/3)



Actual condition of the Nusantara wharf (2/3)



Actual condition of the Nusantara wharf (3/3)



(4) Current situation of Kendari Port, Nusantara Wharf

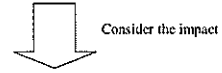
- No access control conducted
- Various ships are using the same wharf
 - International Ships
 - Domestic Ships
 - Domestic Passenger Ships
- Difficult to set restricted area for international ships
 - There is little entering port of the freighter of a foreign trade. (About once every several years international calls / year)
 - Setting of fence will interfere the activities of cargo handling and so on

(5) Important Assets and Infrastructures

- Passenger Terminal (domestic)
- Wharf

(6) Risk Evaluation

- The biggest port in southeast Sulawesi



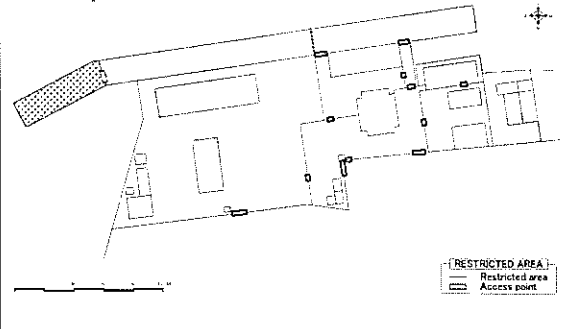
- “Social” and “Economic Activities”
- “Symbolic” and “Port Activities”

(7) Recommendations

- Access control system(Gate) of the restricted area
- Fence surrounding the restricted area
- Lighting system within the restricted area
- Communication system
- Use temporary fence and minimize the interference of port service
- Establish a procedure of international ship's calling
 - Type of temporary fence
 - Decide the number of security guards
 - Deployment of security guards
 - Area of temporary restricted area

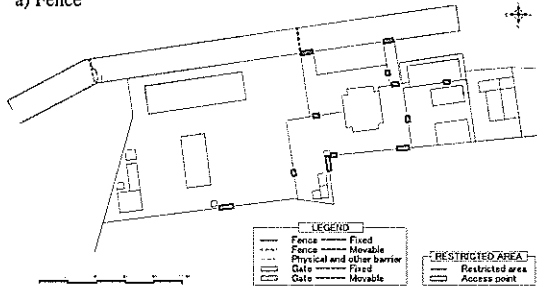
3. PFSP for Kendari Port, Nusantara Wharf

(1) Proposed Restricted Area

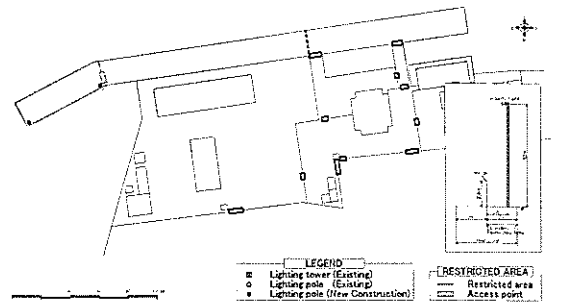


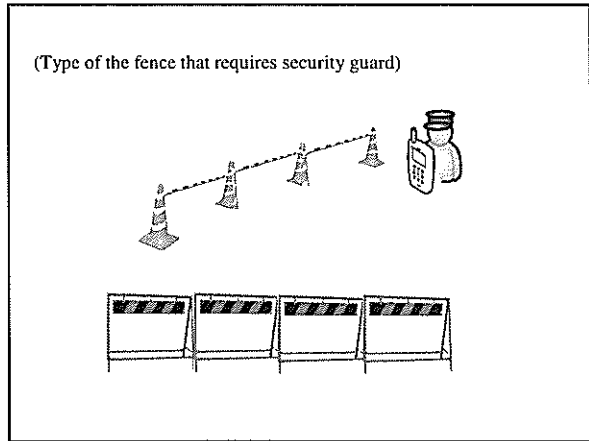
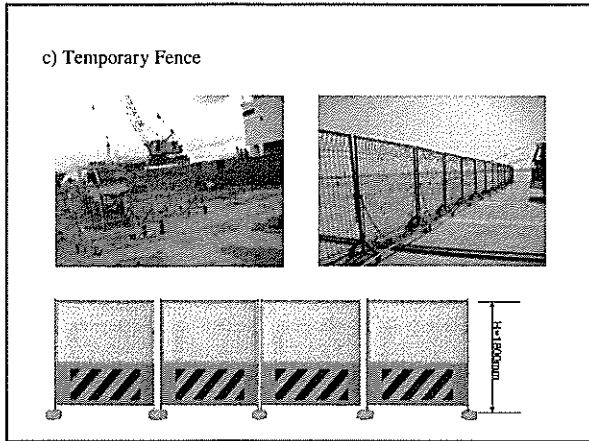
(2) Port Security Facilities to be Provided at Nusantara Wharf

a) Fence



b) Lighting System





(3) Access Control to be Conducted at Gates

a) Access Control for Customs and ISPS Code

- Different Purpose
 - Customs
 - Avoid smuggling
 - Avoid goods BEING TAKEN out illegally
 - EXIT CONTROL
 - ISPS
 - Avoid Suspicious Person/Goods inside the Restricted Area
 - Protect from Terrorism
 - ENTRY CONTROL

b) Category of Entrance

- Port User (by foot or otherwise)
- Container Truck
- Construction/Maintenance Vehicle
- Ships Stores/Equipment
- Ships Crew
- Taxi
- Emergency Service Vehicle

Port User (by foot or otherwise)

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Foot or Vehicle Entry	•Request to stop •Ask for ID card all those wishing to enter	•Same as on the left •Check ID photo and the face for 10 out of every 100	•Do not admit entry
Baggage	•Check appearance of baggage	•Confirm contents of baggage for 10 out of 100	•Do not admit entry

Container Truck

Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Confirm documents	•Same as on the left	•Do not admit entry
Driver	•Ask for ID card for 10 out of every 100	•Ask all drivers for ID card	•Do not admit entry
Helper	•Admit entrance on guarantee of driver	•Same as on the left	•Do not admit entry
Full Container	•Check documents and appearance	•Same as on the left	•Do not admit entry
Empty Container	•Check documents and confirm inside	•Same as on the left	•Do not admit entry

Cargo Truck			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Confirm documents	•Same as on the left	•Do not admit entry
Driver	•Ask for ID card for 10 out of every 100	•Ask all drivers for ID card	•Do not admit entry
Helper	•Admit entrance on guarantee of driver	•Same as on the left	•Do not admit entry
Freight	•Check Documents & appearance of cargo	•Inspect and confirm cargo against documents	•Do not admit entry

Construction/Maintenance Vehicle			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Confirm approval with PFSO	•Same as on the left	•Do not admit entry
Driver	•Ask all drivers for ID card	•Ask all drivers for ID card •Check ID photo and the face for 10 out of every 100 •Request to fill in form and issue temporary pass when there is no ID card	•Do not admit entry
Passenger/Workmen	•Admit entrance on guarantee of driver/foreman	•Same as above	•Do not admit entry
Cargo	•Check appearance	•Inspect contents	•Do not admit entry

Ship's Stores/Equipment			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop •Check documents	•Request to stop •Confirm documents	•Do not admit entry
Driver & Passenger	•Ask all drivers/Passengers for ID card •Check ID photo and face for 50 out of every 100	•Ask all drivers/Passengers for ID card •Check ID photo and the face for all those wishing to enter	•Do not admit entry
Cargo	•Not necessary to check when under escort •Confirm customs report or work order when there is no escort	•Confirm contents of cargo for 50 out of every 100	•Do not admit entry

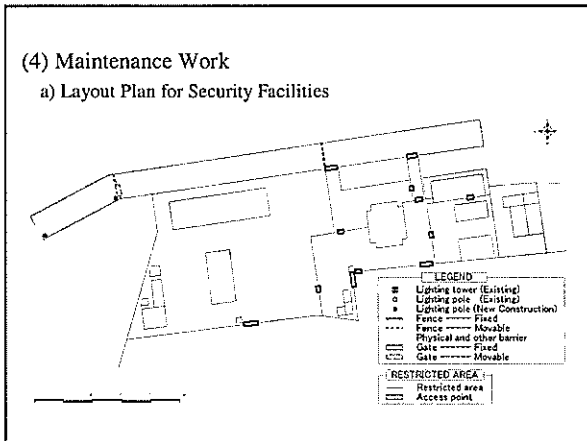
Ships Crew's Exit and Return Entry			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Ships Crew exit	•Confirm shore pass or ID issued by the ship	•Same as on the left	•Do not admit entry
Ships Crew entry/go on board	•Same as above •Confirm an embarkation order, seamen's bunk or passport or confirm with the ship	•Same as on the left	•Do not admit entry
Baggage	•Check appearance of baggage	•Confirm contents of baggage for 10 out of 100	•Do not admit entry

Taxi			
Security Level	Level 1 Conducted by PFSO	Level 2 Conducted by PSO	Level 3 Conducted by PSO
Vehicle	•Request to stop	•Request to stop •Inspect trunk	•Do not admit entry
Driver	•Ask all drivers for ID card	•Ask all drivers for ID card •Check ID photo and the face for 10 out of every 100	•Do not admit entry
Passenger	•Same as above	•Same as above •Ask destination	•Do not admit entry
Baggage	•Check appearance of baggage	•Confirm contents of baggage for 10 out of 100	•Do not admit entry

Emergency Service Vehicle	
Security level	Security level 1,2 and 3 (Emergency Service personnel not required to have ID)
Vehicle	•Confirm the type of vehicle •Record time of entry into record book
Driver	•Confirm by the type of vehicle
Vehicle Crew	•Same as above

(4) Maintenance Work

a) Layout Plan for Security Facilities

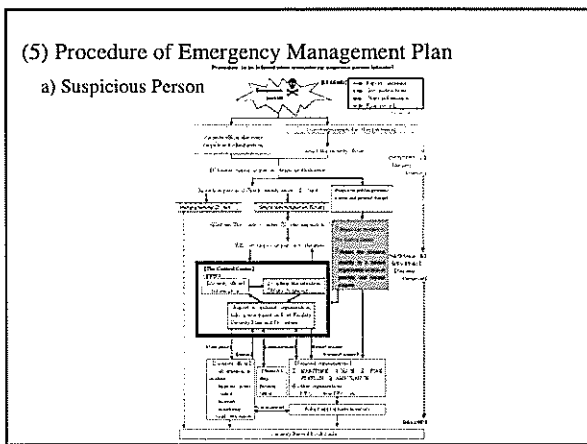


b) Inspection Procedure

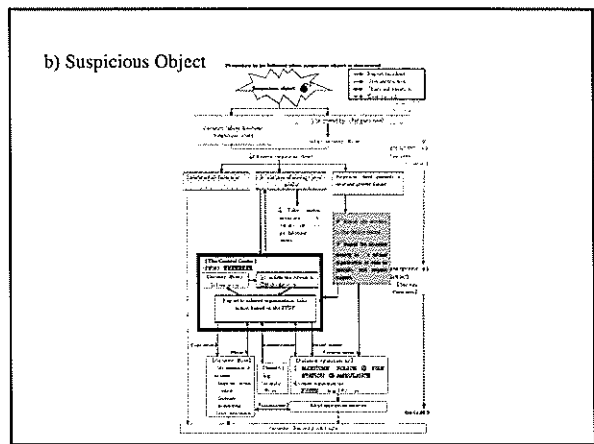
Description	Items to be Checked	Daily Inspection	Periodical Inspection
Fence and Gate		*Visual inspection during patrol (repair, reinforce, or replace if necessary)	*Conduct monthly *Sway and confirm net is not loose
Security Light	Road Light	*Ensure that all security lights are illuminated during patrol	*Conduct annually *Check mounting of lamp fitting *Clean the cover *Check cables and switch box
Communication System	VHF Radio Telephone Fax	*Check in daily usage	*Conduct annually by the supplier *Cleaning adjustment, and change consumables

(5) Procedure of Emergency Management Plan

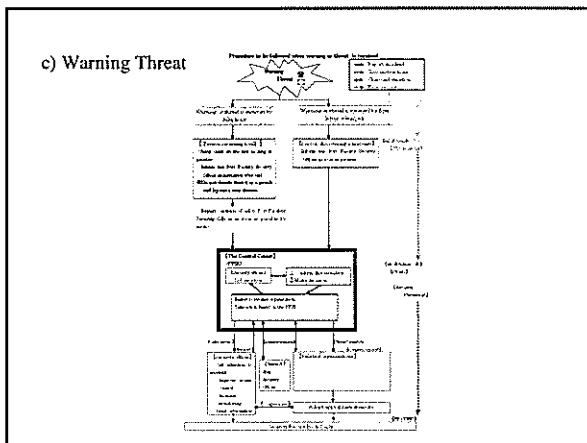
a) Suspicious Person



b) Suspicious Object



c) Warning Threat



(6) Evacuation Procedure

- Evacuate following the instruction of PFSO
- Direct the gate number when evacuating from the restricted area
- Direct the name of facility when evacuating to the building
- PFSO may direct, navigate and confirm that no one fail to escape

APPENDIX-IV URGENT SECURITY DEVELOPMENT PLAN

I-1 SELECTION OF PORTS FOR URGENT SECURITY MEASURES

1. The DGSC puts priority on reinforcement of security measures based on ISPS Code for 25 strategic ports in Indonesia. Since last year port security equipment such as CCTV camera has been installed in the ports of Tg.Priok, Tg.Perak and Batam and the first development stage of security measures on land for these three ports will be completed soon.
2. One year has already passed since July 1, 2004 when the ISPS Code became effective. The DGSC is now accelerating port security measures and installation of security equipment with PELINDO and other related organizations including private companies in ports. However installation of security measures at public ports is stalled because of budget constraints.
3. The DGSC strongly and urgently requests enhancement of security facilities and equipment for the following seven ports. These ports need the establishment of port security soon after the above three ports from the viewpoint of cargo handling volume and the impact to the region and geographic distribution. The main characteristics of these ports are as follows:
 - 1) Belawan Belawan port is one of the four major ports in Indonesia and plays an important role in Sumatra. Its container handling volume is large. It also has close relations with Singapore and Malaysia. Security measures enhancement is strongly requested.
 - 2) Dumai Dumai port is one of the gateways to Malaysia. Its role in social economic activities in the region is very big. Urgent enhancement of security facilities and equipment is requested.
 - 3) Palembang Palembang port is one of the big ports in south Sumatra. It plays an important role in social economic activities. Security facilities and equipment are insufficient and improvement is urgently requested.
 - 4) Banjarmasin Banjarmasin port is the gateway port to Kalimantan. It plays an important role in the export of raw materials. It ranks first in export volume in Indonesia (as of 2003). Establishment of security measures is urgently requested.
 - 5) Samarinda Samarinda is one of the big ports in Kalimantan. It plays an important role in transportation of raw materials especially plywood. International cargo is ammonia imported from China, Malaysia and Australia. Security measures of PELINDO IV have been delayed and establishment of security measures is urgently requested.
 - 6) Bitung Bitung port plays an important role in social economic activities in north Sulawesi. New container terminal was completed this January by Japanese loan. Security measures of PELINDO IV have been delayed and port security enhancement is strongly requested.

- 7) Makassar Belawan port is one of the four major ports in Indonesia and plays an important role not only in Sulawesi but also in the eastern part of Indonesia. Its container handling volume is also large. Security measures of PELINDO IV have been delayed and enhancement of security facilities and equipment is urgently requested.

I-2 PRESENT SITUATION OF PORTS

I-2-1 Belawan Port

1) Outline of port facilities and handling cargo (Type and Volume)

4. Port of Belawan belonging to PELINDO I is located about 30km north of Medan and faces the Malacca straight. Conventional, container and passenger vessels call the port.

- Conventional terminal (UjungBaru terminal)
 - Total length 1,195m (Liquid bulk; 650m, Dry bulk; 380m, General cargo; 165m)
 - Water depth -9m
 - Cargo handling volume: Export 4,530,070 tons (CPO, fertilizer (oil cake))
Import 1,197,823 tons (fertilizer, steel, corn)
- Container terminal (Belawan container terminal)
 - Total length 500m (connects domestic container terminal in a row; 350m)
 - Water depth -10m
 - Cargo handling volume: Export 40,000TEU
 - Cargo handling equipment: Gantry crane;4, Mounted crane;7, Super stacker;2
- International passenger terminal
 - Total length 350m
 - Passenger barking and embarking: 304,659 in 2004
 - Facilities and equipment: No gangway, X-ray scanner owned by Customs

2) Present situation and issues of port security measures

5. Present situation and issues of port security measures on Belawan port are as follows:

- Conventional terminal
 - External fence has enough height and outrigger. No boom for stopping vehicles is installed at gates and persons can enter the port area without any check.
 - Some security guards who conduct access control and patrol the port area have no radio communication device.
 - ID with photo is issued but confirmation of ID has not been conducted.
- Container terminal
 - Net fence with overhang is installed inside and along concrete wall which is built between the container terminal and neighboring marina. The problem is that there is no clearance between net fence and concrete wall and it is easy for a person to climb the concrete wall and enter the port.
 - Domestic container terminal abuts on international container terminal and they are separated by movable fence. However, access control is insufficient due to fence damage.

- International passenger terminal
 - Access gate of international passenger terminal is closed except during terminal operation time. There is no area for passengers to stay.
 - No check by metal detector and X-ray scanner including baggage inspection and explosive check is conducted.
 - Clearance between ground surface and movable fence which is placed on the boundary with general cargo berth and small vessel berth is more than 30cm. Junctions of fence are loose. Any one can easily enter the terminal area and therefore the terminal security is vulnerable.
 - Movable fence placed on the border with general cargo berth and small vessel berth has clearance gap of more than 30cm from ground surface and has loose connection. In addition, there is room between the movable fence edge and berth face line where persons can enter the terminal area easily. Therefore security of the terminal area is vulnerable.

3) *Proposal on port security measures*

6. Proposals on port security measures in Belawan port are as follows:

- Repair of fence and gates
- Implementation of check by X-ray scanner, portal metal detector and handy metal detector
- Implementation of strict access control
- Installation of CCTV cameras and lighting
- Installation of Public Address System

I-2-2 Dumai Port

1) *Outline of port facilities and handling cargo (Type and Volume)*

7. Dumai port which is located in central Sumatra and faces the Malacca strait is a good natural harbor. Public facilities which handle international cargo are the multi-purpose wharf and general cargo wharf. Crude palm oil and its by-product account for most of the international cargo. Both facilities handle international and domestic cargo. Projects to increase port capacity including the extension project of the multi-purpose wharf are being carried out since both facilities are approaching their capacity limits.

8. In addition, Dumai port has a passenger terminal for international and domestic passengers. International passenger ships enter service between Dumai port and Malaka, Port Dikson and Port Klang 4 times a day. Moreover private wharves operated by petroleum and gas companies exist in Dumai port.

Table I-2-2-1 International Cargo Volume (Unit: ton)

	Trade Type	2000	2001	2002	2003	2004
Non Oil & Gas Commodity	Export	2,393,399	2,756,918	3,144,644	3,858,016	4,130,476
	Import	329,957	278,678	365,133	387,907	387,398
	Sub-total	2,723,356	3,035,596	3,509,777	4,245,923	4,517,874
Oil & Gas Commodity	Export	16,868,385	17,168,144	14,916,352	13,163,728	12,500,980
	Import	0	44,038	10,939	33,795	99,339
	Sub-total	16,868,385	17,212,182	14,927,291	13,197,523	12,600,319
Total		19,591,741	20,247,778	18,437,068	17,443,446	17,118,193

Source: PELINDO I

Table I-2-2-2 International Passenger

		2000	2001	2002	2003	2004
International Passenger	Embarkation	141,178	177,368	188,928	180,337	148,373
	Disembarkation	151,370	143,392	209,604	125,054	147,003
	Total	292,548	320,760	398,532	305,391	295,376

Source: PELINDO I

2) *Present situation and issues of port security measures*

9. At the general cargo wharf, some part of the fence is not installed or overhang of the fence inclines in the wrong direction of inclination (slopes to inside). Double gate system which is composed of entrance gate of the port (outer gate) and one of the restricted area (inner gate) is adopted for access control in both wharves. At the outer gate, gate check is conducted. However at the inner gates of both wharves gate check is not conducted. General public can enter the restricted without any inhibition.

10. At the passenger wharf, fence surrounding the restricted area is under construction. New passenger terminal has been built but no X-ray scanner for baggage, walk-through type metal detector, cameras for monitoring inside of the terminal, etc. are installed there.

3) *Proposal on port security measures*

11. It is proposed that fence surrounding the restricted area and emergency gate be installed at the general cargo wharf. It is also proposed that X-ray scanner for baggage, walk-through type metal detector, and cameras for monitoring inside of the terminal be installed in the new passenger terminal.

I-2-3 Palembang Port

1) *Outline of port facilities and handling cargo (Type and Volume)*

12. Palembang port, which is located in Musi River, the largest river in south Sumatra, is a public port owned by PELINDO II. It has conventional, container and (domestic) passenger terminals.

➤ Conventional terminal

- Total length: 370m
- Water depth: -6 to -7m

➤ Container terminal

- Total length: 366m
- Water depth: -9m
- Cargo handling equipment: Gantry crane;1, Forklift;9, Self-propelled crane;2
- The number of calling vessel: 4,030 in 2004
- Cargo handling volume: 11,008,936 tons, 58,612TEU
- Major cargo items: Rubber; 481,504 tons, CPO; 319,021 tons

2) *Present situation and issues of port security measures*

13. Present situation and issues of port security measures at Palembang port are as follows:

- Fence near the gate is low and aged.
- Clearance gap between the gate/fence and ground surface is about 20cm.

- Although two gates have a pole for stopping vehicles, the poles are always raised (not used).
- Some security guards who conduct access control and patrol the port area have no radio communication device.
- IDs have not been checked at gates.
- Many unauthorized vehicles park in the port area.

3) *Proposal on port security measures*

14. Proposals on port security measures in Palembang port are as follows:

- Repair of fence and gates
- Implementation of strict access control
- Installation of CCTV cameras and lighting
- Installation of Public Address System

I-2-4 Banjarmasin Port

1) *Outline of port facilities and handling cargo (Type and Volume)*

15. Banjarmasin port has a conventional terminal composed of continuous berths for container, general cargo and passenger, a coal terminal as well as a new container terminal at the far end of the port that is separated from the former berths by a cement company. Passenger berth is used for domestic passenger but it is also used for general cargo when a passenger ship is not berthing.

16. Large vessels for coal transport cannot enter the port because Banjarmasin port is a river port and its water depth is shallow. Therefore coal is transshipped from a large vessel to barges at an anchorage which is set out offshore of the river mouth. (About 750 vessels calls the port in a year.) Major cargos are coal and plywood. Plywood is handled at private ports. International container ships and general cargo ships call the port once or twice a month.

Table I-2-4-1 Cargo Handling Volume through Banjarmasin Port

Description	Unit	Year 2001	Year 2002	Year 2003	Year 2004
General Cargo					
- Export	ton or m ³	8,041,954	9,951,347	12,729,859	16,016,393
- Import	ton or m ³	61,125	53,499	53,338	17,121
- In-coming (domestic)	ton or m ³	3,327,169	3,272,347	3,304,719	2,177,352
- Out-going (domestic)	ton or m ³	2,681,287	2,961,015	4,106,811	5,240,905
Total	ton or m ³	14,111,535	16,238,208	20,194,727	23,451,771
Container					
- Export/Import	TEU	13,163	15,448	16,634	14,643
- Domestic	TEU	125,677	133,854	142,664	168,972
Total	TEU	138,840	149,302	159,298	183,615

Source: PELINDO III Banjarmasin Port

2) *Present situation and issues of port security measures*

17. Security guards are deployed at gates but do not implement ID check and cargo inspection. At some gates no security guard is deployed in the night time. Moreover some gates are shared with several areas because the restricted area has not been designated. Some part of fence is insufficient or broken. Some broken lighting ramp remains untouched. In general maintenance of equipment is insufficient.

3) *Proposal on port security measures*

18. Proposals on port security measures in Banjarmasin port are as follows:

- Establishment of restricted area
- Access control at gates
- Installation of security equipment (fence, gate, lighting, public address system)

I-2-5 Samarinda Port

1) *Outline of port facilities and handling cargo (Type and Volume)*

19. Samarinda public port is located in East Kalimantan Province and is about 2 to 3 hours by car from Balikpapan Airport. (South latitude 0° 30'25'', East longitude 117° 24'16'') Mahakam river flows from west to east in Samarinda city and Samarinda port is a river port on the Mahakam river. Forty-five ports including private berths are scattered along the river. Samarinda public berth is a slender terminal along the river with a width of about 80m and a length of about 935m. The port faces the trunk road and opposite of the trunk road is the downtown area.

20. International cargoes in Samarinda public port are mainly plywood and coal. These cargoes are transported to Tg.Perak and Tg.Priok as domestic cargo and then exported after transshipment. Cargo vessels which transport these cargoes and their calling wharves fall under domestic ones. Therefore these vessels and wharves do not need to comply with the ISPS Code. However, chemical cargo vessels call the port and berth at a particular place several times a year. PFSA is conducted for the place given it is surrounded by movable fence and is set as a restricted area.

21. Terminal dimensions are as follows:

- Total length of the wharf is 935m and water depth is -5.5m.
- No of terminal operators: 8
- Berth length for international vessels is 60m.
- Berth length for domestic passenger is 80m.

22. International ship calls at the port were quite limited in 2004. There were no container vessel or RORO vessel call. Chemical vessels which carried ammonium nitrate call the port about ten times a year.

23. Major export cargoes are plywood, coal and moulding (manufactured wood). The total export volume amounted to 43,578 tons in 2004. Plywood is put into containers in a factory and transported from Samarinda public wharf to an anchorage by barge. Containers are transhipped to the domestic vessel at the anchorage, and transhipped to an international vessel at Tanjung Priok port or Tanjung Perak Port. Major container cargo in Samarinda port is plywood. Coal is also transported from private ports to anchorage by barge and is transhipped

at anchorage like plywood. Coal exports reached 10,367,561 tons in 2004. Coal is transported by domestic vessels to T.Priok and Tg.Perak and exported from these two ports. Moulding is directly exported from Samarinda public port to Middle East and Korea. Several times a year.

24. Import cargo volume at Samarinda port amounted to 25,803 tons in 2004 and its major commodity is ammonium nitrate which is a dangerous cargo used in explosive materials. It is not unloaded at anchorage but loaded directly unloaded at the wharf..

2) *Present situation and issues of port security measures*

25. At present, installation of external fence, access control and patrol of the port area is conducted as security measures by KPLP. KPLP implements periodical patrols on water area by a patrol boat.

26. Cargoes for export such as plywood and coal are transshipped at anchorage but these cargoes are deemed to be domestic cargoes between Samarinda and Tg.Priok and Tg.Perak. Therefore, the anchorage is not forced to comply with the ISPS Code.

3) *Proposal on port security measures*

27. Proposals on port security measures in Samarinda port are as follows:

- Separate the wharf and cargo handling area for international vessels from the whole port area by movable fence, conduct control and patrols of the restricted port area only when an international vessel berths at a wharf and unloads cargo.
- Monitor water area adjacent to a wharf

I-2-6 Bitung Port

1) *Outline of port facilities and handling cargo (Type and Volume)*

28. Bitung port is the largest port in north Sulawesi. New container terminal started operation this January and it is now used for domestic containers. International cargoes are handled at the neighboring old berths. Major export cargoes are Copra, dry coconut cake, coconut powder, nutmeg seed, rattan, vanilla, seaweed, tuna and canned fish and they are exported to USA, European countries, Korea, North Korea, India, Japan, China, Philippines, Singapore, Malaysia, Australia and New Zealand. Cargo handling volume and calling vessels are as follows:

Table I-2-6-1 Cargo handling volume (ton)

	2000	2001	2002	2003
Export	72,727	51,796	144,722	92,491
Import	394,911	232,936	531,420	388,676

Source: PELINDO IV

Table I-2-6-2 Container (Box)

	2000	2001	2002	2003
Export	45	36	590	200
Import	1,589	928	1,739	645

Source: PELINDO IV

Table I-2-6-3 Calling vessels

Year	2000	2001	2002	2003
Calling vessels	354	293	334	334

Source: PELINDO IV

2) Present situation and issues of port security measures

29. Three continuous berths are used for international cargo (container, bulk), domestic cargo and domestic passengers. International cargo volume accounts for only a small portion (8%) of the total cargo. Therefore, if the restricted area is designated only for international cargo, it would pose a serious problem for domestic cargo handling. In future, international containers will be handled at the new container terminal.

3) Proposal on port security measures

30. Considering the above situation, it is unrealistic to install a permanent fence. International vessels call very few times a year and different vessels use different berths. Therefore it is proposed that a temporary fence be installed, security guards be appropriately deployed, and port security procedures during international vessel calling be established. It is also necessary to increase lighting because some part of the area is dark.

I-2-7 Makassar Port

1) Outline of port facilities and handling cargo (Type and Volume)

31. Makassar port which is located in the west of south Sulawesi is the largest port in eastern part of Indonesia. Public facilities which handle international cargo are Hatta container terminal and Cargo terminal. Major international cargos are clinker, cacao, cement (export), gurisuto (cereal), sugar and automobile (import). Domestic containers account for 95% of the total container handling volume in the port.

Table I-2-7-1 International Cargo Volume (Unit: ton)

	1999	2000	2001	2002	2003	2004
Export	669,431	923,687	1,510,363	1,028,516	1,138,219	1,241,077
Import	488,691	628,688	451,746	620,797	637,017	708,689
Total	1,158,122	1,552,375	1,962,109	1,649,313	1,775,236	1,949,766

Source: PELINDO IV

Table I-2-7-2 Container Volume (Unit: TEU)

	1999	2000	2001	2002	2003	2004
Export	8,792	10,682	10,167	7,671	8,604	9,783
Import	178	41	1,035	2,318	1,536	1,957
Int'l Total	8,970	10,723	11,202	9,989	10,140	11,740
Domestic	119,917	154,228	166,214	197,496	222,014	238,104
Total	128,887	164,951	177,416	207,485	232,154	249,844

Source: PELINDO IV

2) Present situation and issues of port security measures

32. In Hatta container terminal, the entire terminal area is designated as a restricted area, and access gate and fence (height: 2.7m) have already installed. Access control and patrol in the terminal area is properly implemented. However, intrusion to the restricted area does not

seem to be so difficult because fence gage is coarse and no overhang is attached. Although security guards patrol the container yard, it is difficult for them to grasp conditions behind piled containers. Lighting in the terminal is adequate.

33. At Cargo terminal, wharf, apron and warehouse are set out as the restricted area and access gate and fence have been installed. Movable fence is used on the border abutting with domestic passenger terminal when a domestic passenger ship berths at a domestic passenger terminal. Ordinarily, however, movable fence is removed because vehicles carrying domestic cargo from the domestic wharf which is situated next to the north side of the passenger terminal pass the border. Security can be ensured by security guard's patrol because Cargo terminal area is not so large.

3) *Proposal on port security measures*

34. It is proposed that overhang of fence and CCTV cameras be installed to prevent unauthorized personnel from entering the restricted area and to monitor the container yard.

I-3 FACILITIES AND EQUIPMENT FOR URGENT SECURITY MEASURES

I-3-1 Basic Policy

35. Container terminal, dangerous goods terminal and passenger terminal belong to Group-A and remaining ones Group-B. As for Group-A, high-standard security facilities and equipment including CCTV camera are installed.

I-3-2 Required Facilities and Equipment

36. Required facilities and equipment of the urgent development plan are shown in Table I-3-2-1.

Table I-3-2-1 Required Facilities and Equipment

Name of Port	Province	Item	Quantity
Belawan	North Sumatra	Access control system (Gate) of the restricted area (new)	5 units
		Fence surrounding the restricted area (new)	500 m
		Fence removal	500 m
		CCTV camera system within the restricted area	6 units
		CCTV monitoring system	1 unit
		Sensor	500 m
		X-ray inspection system in the passenger terminals	1 unit
		Lighting system within the restricted area	11 units
		Hand hole, under ground pipe and cable	6,300 m
		Gate typer metal detector	1 unit
		Communication system (P.A. system)	9 units
		Sub Total	
Dumai	Riau	Access control system (Gate) of the restricted area (new)	1 unit
		CCTV camera system within the restricted area	6 units
		CCTV monitoring system	1 unit
		X-ray inspection system in the passenger terminals	1 unit
		Lighting system within the restricted area	15 units
		Hand hole, under ground pipe and cable	1,200 m
		Gate-type metal detector	1 unit
		Communication system (P.A. system)	7 units
		Fence surrounding the restricted area (new)	260m
		Fence removal	225 m
		Sub Total	
Palembang	South Sumatra	Access control system (Gate) of the restricted area (repair)	3 units
		Fence surrounding the restricted area (new)	200 m
		Fence removal	100 m
		CCTV camera system within the restricted area	6 units
		CCTV monitoring system	1 units
		Sensor	200 m
		Lighting system within the restricted area	21 units
		Hand hole, under ground pipe and cable	2,000 m
		Communication system (P.A.system)	4 units
		Sub Total	
Banjarmasin	Kalimantan	Access control system (Gate) of the restricted area	1 unit
		Fence surrounding the restricted area	300 m
		Lighting system within the restricted area	14 units
		Hand hole and under ground pipe	1,000 m
		Communication system (P.A. system)	2 units
		Sub Total	
Samarinda	East Kalimantan	Fence surrounding the restricted area (mobile)	180 m
		Sub Total	
Bitung	North Sulawesi	Lighting system within the restricted area	6 units
		Hand hole and under ground pipe and cable	600 m
		Communication system (P.A. system)	6 units
		Sub Total	
Makassar	South Sulawesi	Access control system (Gate) of the restricted area (new)	1 unit
		CCTV camera system within the restricted area	6 units
		CCTV monitoring system	1 unit
		Hand hole, under ground pipe and cable	3,000 m
		Sensor	1,550 m
		Fence improvement	1,550m
Communication system (P.A. system)	7 units		
		Sub Total	

I-4 OPERATION AND MAINTENANCE OF FACILITIES AND EQUIPMENT

37. The DGSC is directly responsible for the project. After procuring the facilities and equipment, DGSC turns them over to each PELINDO or KPLP. Each PELINDO is responsible for operation and maintenance of the facilities and equipment except for patrol boats. KPLP is responsible for operation and maintenance of the patrol boats.

I-5 CONSULTING SERVICE AND PROCUREMENT WORKS

I-5-1 Consulting Services:

38. Consulting services are as follows:

- Review the feasibility study and detail design
- Conduct the procurement supervisory services
- Advise and train PELINDO I, II, III and IV on operation and management of security facilities and equipment, KPLP on operation and management of patrol boats.

I-5-2 Procurement Works

39. The following facilities are installed/procured:

- Access control system of the restricted area
- Fence surrounding the restricted area
- CCTV camera system within the restricted area
- X-ray inspection system in the passenger terminals
- Lighting system within the restricted area
- Security equipments such as a gate type metal detector
- Communication system
- Security infrastructure

I-6 COST ESTIMATE ON URGENT SECURITY DEVELOPMENT PLAN

I-6-1 Objective Ports of Urgent Security Development Plan

40. The security equipment and facilities required for 26 strategic Indonesian public ports are proposed by the study team upon review, analysis and the site survey in the first works in Indonesia as summarized in Appendix 1.

41. In these 26 strategic ports, the following seven (7) public ports have been selected to enhance the security facilities and equipment as the urgent security development plan to be complied the ISPS Code upon review, analysis and the site survey the existing ports and under strong request of the DGSC.

Table I-6-1-1 The Ports Required for Urgent Security Enhancement

No.	PELINDO	Port Name	State	Remarks*
1	I	Belawan	North Sumatra	International port (Secondary trunk port)
2	I	Dumai	Riau	International port (Secondary trunk port)
3	II	Palembang	South Sumatra	International port (Secondary trunk port)
4	III	Banjarmasin	South Kalimantan	International port (Secondary trunk port)
5	IV	Samarinda	East Kalimantan	National port (Tertiary trunk port)
6	IV	Bitung	North Sulawesi	International port (Secondary trunk port)
7	IV	Makassar	South Sulawesi	International port (Secondary trunk port)

* Categorization under the Port Affairs by PP No. 69/2001 in August 2002

I-6-2 Cost Estimate for Urgent Security Development Plan

1) Scope of Works

42. The project scope is defined to 2 categories of hard component for procurement and installation of the required facilities and equipment for urgent security measures as the structural measures, and soft components for educational, training and other capacity building as the non-structural measures for urgent security measures of 7 ports on the urgent security development plan.

43. The cost for structural measures is the cost for procurement and installation of the facilities and equipment for urgent security measures as presented in Clause 10.6.3 including the cost for the consultant for engineering design and supervision for the security systems.

44. The cost for soft components is assumed mainly the cost for the human resources input from donor/s, Indonesia and other source on the following major scope and activities.

- Personnel training necessary for security and ISPS Code
- Capacity building for the agencies concerned
- O&M training for security facilities and equipment
- Other non-structural measures

2) Project Cost

45. The project cost, structural measures and non-structural measures, is estimated at equivalent US\$ 9.7 million in total as summarized in Table I-6-4-1 below and as broken down in Table I-6-4-2, Table I-6-4-3 and Table I-6-4-4 for the structural measures and in Table I-6-4-5 for the non-structural measures under the conditions and assumptions described in Clause I-6-5.

Table I-6-2-1 Project Cost (Preliminary)

Project Cost Items	Project Cost (US\$ 1,000)
Structural Measures	9,137
Non-structural Measures	518
Total	9,655

Table I-6-2-2 Cost for Structural Measures for 7 Ports (Preliminary)

No.	Cost Items	Amount (US\$1,000)
1	Procurement and Installation Cost of Facilities and Equipment *1	6,110
2	Training Cost of Operators for Facilities and Equipment by Experts from Manufacturer or Agents *2	180
3	VAT (10% of 1)	611
4	Sub Total (1+2+3)	6,901
5	Land Acquisition and Compensation Cost (1% of 1)	61
6	Administration Expenses (2% of 1)	122
7	Engineering Service Cost (20% of 1) *3	1,222
8	Sub total (4+5+6+7)	8,036
9	Contingency (10% of 8)	831
10	Grand Total (8+9)	9,137

Notes:

- *1: Including spare parts cost of 5 % of the cost of facilities and equipment for 2-year operation approximately
- *2: Assumed 3 men-months by 2 experts for 7 ports
- *3: Consulting services to review the feasibility study, execute detailed design including tender document preparation, conduct and coordinate the procurement, supervisory services, advising and training PELINDO, KPLP on management, and other incidental engineering services.

Table I-6-2-3 Procurement and Installation Cost of Facilities and Equipment (Preliminary)

PELINDO	Port Name	Amount (US\$1,000)
I	Belawan	1,898
	Dumai	1,000
II	Palembang	1,092
III	Banjarmasin	338
IV	Samarinda	9
	Bitung	185
	Makassar	1,297
Sub Total		5,819
Spare Parts (5% of Sub Total)		291
Total		6,110

Table I-6-2-4 Breakdown of Project Cost

Name of Port	Province	Facility/Equipment	Unit	Q'ty	Unit Price (US\$)	Amount (US\$)
Belawan	North Sumatra	Access control system (5-Gate) of the restricted area (new)	unit	30	2,800	84,000
		Fence surrounding the restricted area (new)	m	500	190	95,000
		Fence removal	m	500	47	23,500
		CCTV camera system within the restricted area	unit	6	37,383	224,298
		CCTV monitoring system	unit	1	280,000	280,000
		Sensor	m	500	140	70,000
		X-ray inspection system in the passenger terminals	unit	1	65,420	65,420
		Lighting system within the restricted area	unit	11	7,477	82,247
		Hand hole, under ground pipe and cable	m	6,300	140	882,000
		Gate type metal detector	unit	1	7,480	7,480
		Communication system (P.A. system)	unit	9	9,346	84,114
		Sub total				1,898,059
Dumai	Riau	Access control system (1-Gate) of the restricted area (new)	unit	6	2,800	16,800
		CCTV camera system within the restricted area	unit	6	37,383	224,298
		CCTV monitoring system	unit	1	280,000	280,000
		X-ray inspection system in the passenger terminals	unit	1	65,420	65,420
		Lighting system within the restricted area	unit	15	7,477	112,155
		Hand hole, under ground pipe and cable	m	1,200	140	168,000
		Gate type metal detector	unit	1	7,480	7,480
		Communication system (P.A. system)	unit	7	9,346	65,422
		Fence surrounding the restricted area (new)	m	260	190	49,400
		Fence removal	m	225	47	10,575
		Sub total				999,550
Palembang	South Sumatra	Access control system (3-Gate) of the restricted area (repair)	unit	30	1,400	42,000
		Fence surrounding the restricted area (new)	m	200	190	38,000
		Fence removal	m	100	47	4,700
		CCTV camera system within the restricted area	unit	6	37,383	224,298
		CCTV monitoring system	unit	1	280,000	280,000
		Sensor	m	200	140	28,000
		Lighting system within the restricted area	unit	21	7,477	157,017
		Hand hole, under ground pipe and cable	m	2,000	140	280,000
		Communication system (P.A. system)	unit	4	9,346	37,384
				Sub total		
Banjarmasin	Kalimantan	Access control system (1-Gate) of the restricted area	unit	6	2,800	16,800
		Fence surrounding the restricted area (new)	m	300	190	57,000
		Lighting system within the restricted area	unit	14	7,477	104,678
		Hand hole, under ground pipe and cable	m	1,000	140	140,000
		Communication system (P.A. system)	unit	2	9,346	18,692
		Sub total				337,170
Samarinda	East Kalimantan	Fence surrounding the restricted area (mobile)	m	180	47	8,460
		Sub total				8,460
Bitung	North Sulawesi	Lighting system within the restricted area	unit	6	7,477	44,862
		Hand hole, under ground pipe and cable	m	600	140	84,000
		Communication system (P.A. system)	unit	6	9,346	56,076
				Sub total		
Makassar	South Sulawesi	Access control system (1-Gate) of the restricted area (new)	unit	6	2,800	16,800
		CCTV camera system within the restricted area	unit	6	37,383	224,298
		CCTV monitoring system	unit	1	280,000	280,000
		Hand hole, under ground pipe and cable	m	3,000	140	420,000
		Sensor	m	1,550	140	217,000
		Fence improvement	m	1,550	47	72,850
		Communication system (P.A. system)	unit	7	9,346	65,422
		Sub total				1,296,370
Total (Procurement and Installation Cost)						5,815,946

Table I-6-2-5 Cost for Non-structural Measures

No.	Cost Item	Unit	Q'ty	Amount (US\$1,000)*1
1	Personal training necessary for security and ISPS Code *1	M/M	6.0	164
2	Capacity building for the agencies concerned	M/M	6.0	164
3	Q & A training for security facilities and equipment	M/M	4.0	109
4	Other non-structural measures	M/M	3.0	82
Total			19.0	519

Notes:

*1: JY 3,000,000 per month for foreign expert and JY 500,000 for local expert included fee, per diem and all other costs

*2: 2 foreign experts x 3 months

*3: 3 foreign experts x 2 months

*4: 2 foreign experts x 2 months

*5: 1 local expert x 3 months

3) Operation and Maintenance Cost

46. Annual operation and maintenance cost for the structural measures is estimated at 5% of the procurement and installation cost on the said facilities and equipment as tabulated in Table I-6-4-6 below.

Table I-6-2-6 Annual Operation and Maintenance Cost

PELINDO	Port Name	O&M Cost (US\$)	Equivalent Rp. mil. (US\$ 1.0=Rp.9,770)
I	Belawan	94,903	927
I	Dumai	49,978	488
II	Palembang	54,570	533
III	Banjarmasin	16,859	164
IV	Samarinda	423	4
IV	Bitung	9,247	90
IV	Makassar	64,819	633
Total		290,799	2,839

I-6-3 Conditions and Assumptions for Cost Estimate

47. The project cost estimates under the following estimate approaches, conditions and assumptions:

1) Implementation Schedule

48. An implementation schedule for the structural measures is planned to be 18 months started from July 2006 immediately after the completion of the feasibility study among the detailed design of 6 months and 12 months for the tender, procurement, installation and training.

49. Non-structural measures will be implemented in 24 months duration started from the year 2006.

2) Method of Procurement and Installation of Facilities and Equipment

50. Method of procurement and installation of facilities and equipment are as follows:

- The facilities and equipment which are not available in Indonesia has to be procured from Japan or the third countries. Miscellaneous materials for installation are to be procured from locally such as cables and cement.
- International competitive bid will be applied for the procurement and installation.

- One contract package will be adopted among the procurement and installation.
- The eligible tenderer will be Japanese trading companies and they will make up the necessary components from several manufacturers since the equipment to be procured in this project are produced by different specialized manufacturers in the Europe, USA, Canada, and Japan.
- The power required for the facilities and equipment will be supplied from existing public power source. As for CCTV cameras, electric power will be supplied directly from the monitoring rooms in principle in order to secure uninterrupted power supply.
- Facilities and equipment are to be installed under the supervision of the consulting engineers.
- Since specialized techniques are necessary for installation and adjustment of equipment such as X-ray inspection system and explosives detection system, manufacturers or agents are necessary to dispatch technicians when equipment is installed. Electrician will be locally employed as the assistants for installation and adjustment. General workers are also locally hired for installation works.
- Many electrical contractors are available in Indonesia. Their capability and manpower are to be utilized for the installation works as much as possible.
- Staff education and improvement of security control system are required in order to improve these defects. In this project, guidance and advice for improvement of security measures are required in addition to supply of necessary equipment under the urgent security development plan.

3) *Cost Estimate*

51. Cost estimate conditions are as follows:

- The cost estimated in this stage is preliminary level.
- The exchange rate applied for the cost estimate is referred to the rate of PT Bank Mandiri (PERSERO) Tbk Cabang Jakarta Menara Thamrin dated 1st August 2005 as: US\$ 1.0 = Rp. 9,770 JY 1.0 = Rp. 86.79
- The cost of security facilities and equipment estimates referred to current market prices in Japan, quotations collected at Jakarta in this study stage and tendered prices of similar projects.
- The following materials are referred to in this cost estimate stage.
 - Analysis of unit construction cost, construction materials unit prices and labor charges, issued by PELINDO IV Cabang Bitung-Manado, for year 2006
 - Analysis of unit construction cost, construction materials unit prices, labor charges and rental cost of equipment, issued by PELINDO IV Cabang Makassar, for year 2005
 - Analysis of unit construction cost, construction materials unit prices, labor charges and rental cost of equipment, issued by PELINDO III Cabang Tanjung Emas-Semarang, for year 2005
 - Analysis of unit construction cost, construction materials unit prices, labor charges and rental cost of equipment, issued by PELINDO III Cabang Tanjung Perak-Surabaya, for January to June 2005
 - Journal of building construction and interior material prices, Edition XXIII Year XII 2005

4) Basic Prices

52. Table I-6-5-1 to Table I-6-5-4 below presents unit construction cost, unit price of construction materials, equipment rental cost and labor charges for major items for installation works for the facilities and equipment which collected a quotation from contractors in Jakarta during the first works in Indonesia.

Table I-6-3-1 Unit Construction Cost

No	Cost Items	Unit	Unit Cost (US\$)
1	Excavation, common	m ³	4.6
2	Excavation, rock	m ³	11.0
3	Removal of concrete	m ³	88.0
4	Concrete, K-200	m ³	58.0
5	Asphalt pavement	m ²	14.0
6	Backfill with compaction	m ³	6.0
7	RC building	m ²	380.0

Table I-6-3-2 Unit Prices of Construction Materials (Site delivery basis)

No	Cost Items	Unit	Unit Cost (US\$)
1	Cement	ton	95.0
2	Reinforcement steel bar	ton	930.0
3	Ready mixed concrete, K-200	m ³	72.5
4	Sand	m ³	17.5
5	Aggregate	m ³	19.0
6	Wooden material for formwork	m ³	530.0
7	Fuel	liter	0.23
8	Gasoline	liter	0.27

Table I-6-3-3 Rental Cost for Construction Equipment

No	Cost Items	Unit	Unit Cost (US\$)
1	Backhoe w/breaker, 100 kg	day	226
2	Backhoe w/bucket, 0.9 m ³	day	200
3	Bulldozer, 6 ton	day	200
4	Dump truck, 6 ton	day	84
5	Ordinary truck, 4 ton	day	75
6	Truck crane, 10 ton	day	267
7	Air hand breaker, 7.5 kg	day	7
8	Portable air compressor, 3.7 m ³ /min.	day	6
9	Portable diesel generator, 10 kVA	day	33
10	Boring machine	day	25

Table I-6-3-4 Labor Charge (8 hours/day)

No	Cost Items	Unit	Unit Cost (US\$)
1	Foreman, civil	day	8.33
2	Mechanic	day	8.33
3	Electrician	day	8.33
4	Equipment operator	day	8.33
5	Vehicle driver	day	5.56
6	Rigger	day	8.33
7	Common labor	day	3.33

5) Availability of Equipment and Materials

53. With regard security facilities and equipment, its availability will be as follows following the hearing survey and quotation from contractors in first works in Indonesia.

Table I-6-3-5 Availability of Equipment and Materials

No.	Security Facility/Equipment	Availability
1	Access control gate	Import
2	Crossing gate	Import
3	Metal detector	Import
4	Fence, barbed wire, h=1,900	Local
5	Fence, barbed wire, h=900	Local
6	Fence, barbed wire (special), single helical, loop unclipped	Import
7	Intrusion sensor for fence	Import
8	Lighting system, SON lamp 270 W	Local
9	Galvanized pole, h=12 m	Local
10	Surveillance camera	Import
11	Hand held metal detector	Import
12	CCTV camera	Import
13	X-ray inspection system, middle size	Import
14	X-ray inspection system, small size	Import
15	Electric cable	Local
16	Metal pole for CCTV camera	Local
17	Electric distribution board	Local
18	Patrol boat, L=6.2 m (1-engine x 75 HP)	Local
19	Patrol boat, L=7.2 m (2-engine x 100 HP)	Local
20	Speaker (mixer 60 W)	Local
21	UPS, 15 kVA, 220 V, 3-phase, 3-wire	Import
22	UPS, 20 kVA, 220 V, 3-phase, 3-wire	Import
23	Lighting protection, EF type	Import

I-6-4 Urgent Security Equipment Package

54. View from its urgency, one (1) contract package will be applied for the procurement and installation of the security facilities and equipment on this urgent security development plan, upon international competitive bid.

I-6-5 Funding Plan

55. The DGSC stated that international assistance should be fully utilized. Donor may be fund for supply and install for the security equipment including the consulting and engineering services expenses. In principle, non-structural measures should have to be self-support of Indonesia side that a donor/s may support it in some extents within his capacity. The following scenarios may be envisaged.

56. Firstly, at the central government level, DGSC will explain and report to BAPPENAS for the projects' urgency and necessity with satisfaction data regarding sustainability of the project. Then, BAPPENAS will request to foreign donor/s to support the implementation of the project for the structural measures and non-structural measures. Secondary, at the central and state level, DGSC will coordinate well for training, organization structures, and necessary budget arrangement for non-structural measures.

57. There are two (2) kinds of financial mechanism. One is the Indonesian government plans, including budgetary arrangements for training, technology guidance and investments costs for the project. Other one is by grant aid or loan funds from foreign countries based on the request by Indonesia government. The followings are considerable financial source for the implementation of the project.

- Loan of Indonesia national budget
- Grant of Indonesia national budget
- Donor` grant aid
- Foreign countries` project type loan
- Combination of donors` grant aid and Indonesia national budget

Note: This “Urgent Security Development Plan” was prepared on August 2005 and then the present DGST is described as “DGSC”.

APPENDIX-V STANDARD SPECIFICATION FOR PORT SECURITY FACILITY & EQUIPMENT

I. Coverage

This standard issue covers technical requirement for the installation plan of the ports security facilities and equipment.

This specification issue is just basic, therefore it is necessary to examine it individually in consideration of the situation etc. in which facilities concerned are used when applying to actual facilities and equipment.

II. Environmental condition

(1) Give the anti-damage measures from salt water enough because facilities and equipment are set up outdoors in the coast part of the port area.

(2) Ambient conditions

1) Outdoor equipment

The equipment that is set up in outdoor, and operated must satisfy the following environmental conditions.

Temperature : -10°C - +40°C (45°C)

Relative humidity : 10% - 99%RH

Resistance to wind velocity: Endure the maximum instantaneous wind speed 60m/s.

2) The indoor equipment

The equipment that is indoors set up, and operated must satisfy the following environmental conditions.

Temperature : 0°C - +40°C

Relative humidity : 30% - 90%RH (Dew must not attach)

III. Power-supply voltage

(1) It is expected that the power-supply voltage supplied to this equipment is different according to circumstances of an individual port facilities.

Thus, it makes it to the standard voltage by setting up the transformer of which it inputs the power supply supplied if necessary by the port facilities in this equipment. The standard voltage for facilities is the following.

Standard voltage : AC200/220V, 50/60Hz

(2) Power-supply voltage of equipment

The power-supply voltage of the equipment is as showing in clause above-mentioned (1).

However, have the power-supply unit to make it to the power supply specification that is necessary in equipment including an equipment or them individual when the power supply specification is different according to an individual equipment. The input of the power-supply

unit in this case is assumed to be a standard voltage.

IV. System configuration

Because the system configuration and the equipment arrangement are the secret information, it is not opened to the public.

【However, because the system configuration and the equipment arrangement are things that are basic to planning equipment, it is made as internally.】

The example of the surveillance equipment system is shown as follows. This example of the surveillance equipment system is just basic, and it is necessary to examine it individually in consideration of the situation etc. in which facilities concerned are used.

(1) Example 1: Key switch operation method.

There is no online database retrieval of the accumulation image.

Analog method

(2) Example 2: CRT operation method.

There is no online database retrieval of the accumulation image.

Digital method

(3) Example 3: There is no online database retrieval of the accumulation image.

There is an intrusion detection sensor.

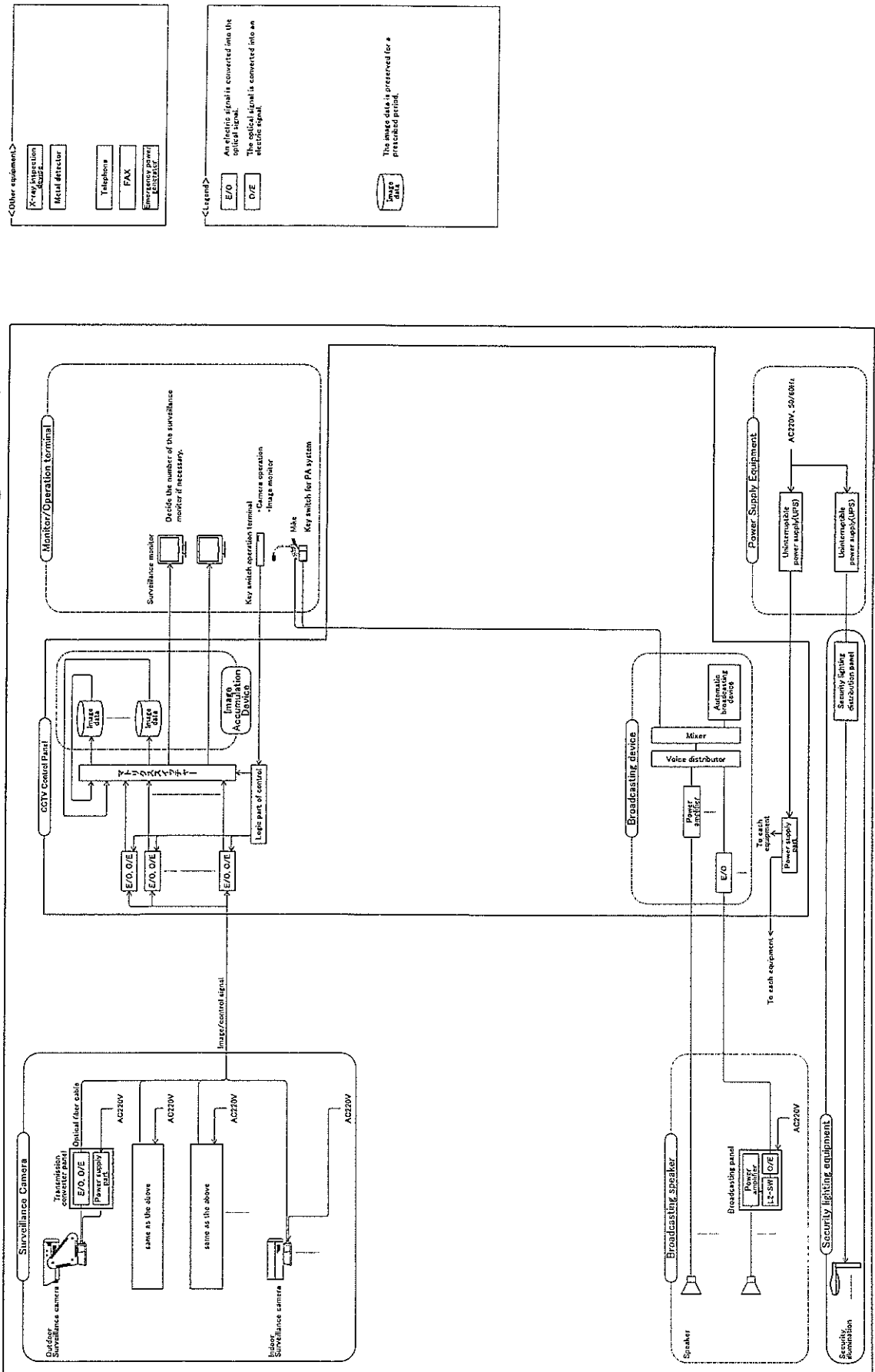
(4) Example 4: There is an online database retrieval of the accumulation image.

Digital method

(5) Example 5: There is an online database retrieval of the accumulation image.

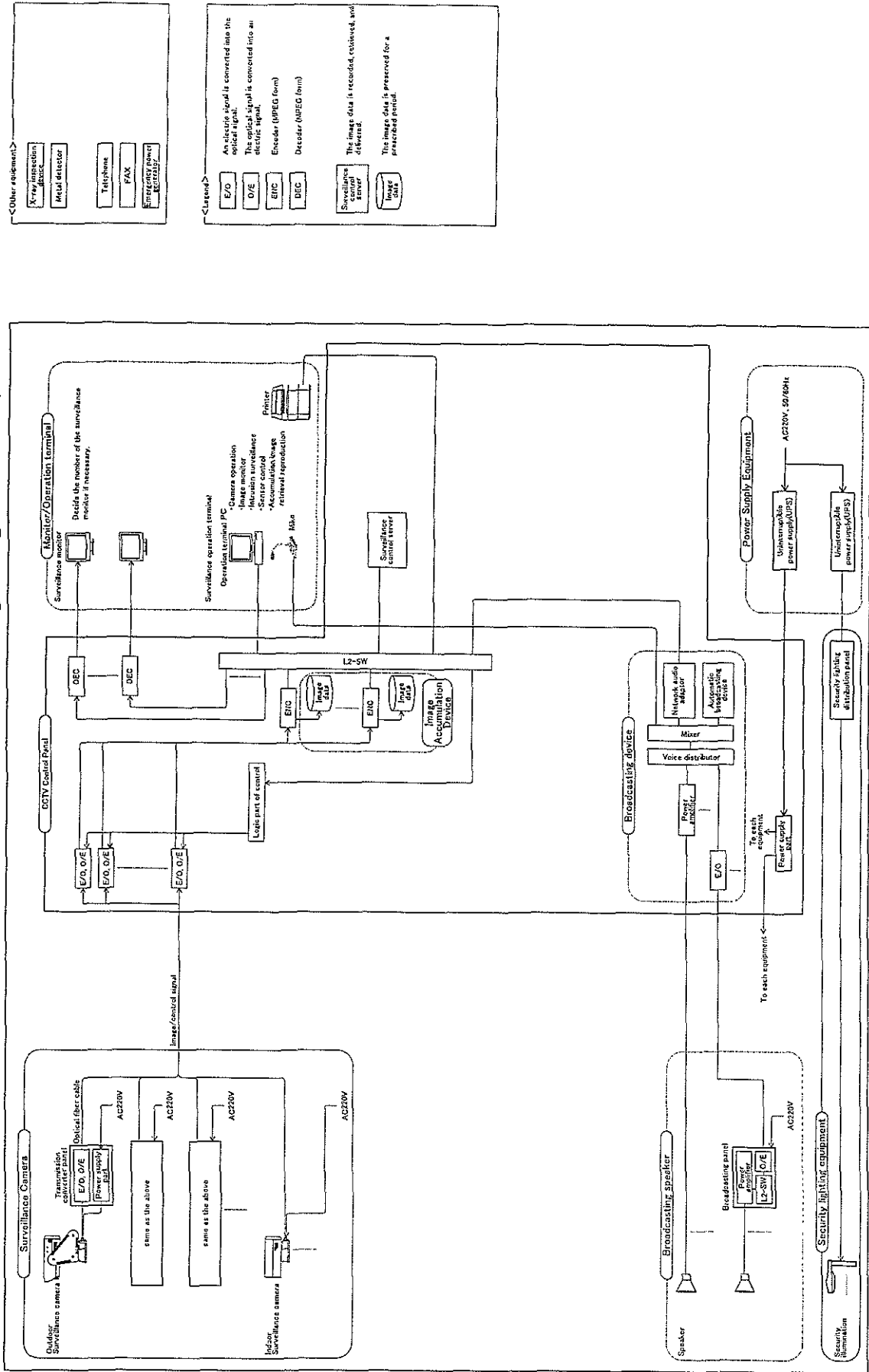
Analog, digital division method

(1) Example of monitoring system configuration - 1 : Key switch operation method
 There is no online database retrieval of the accumulation image. (Analog method)



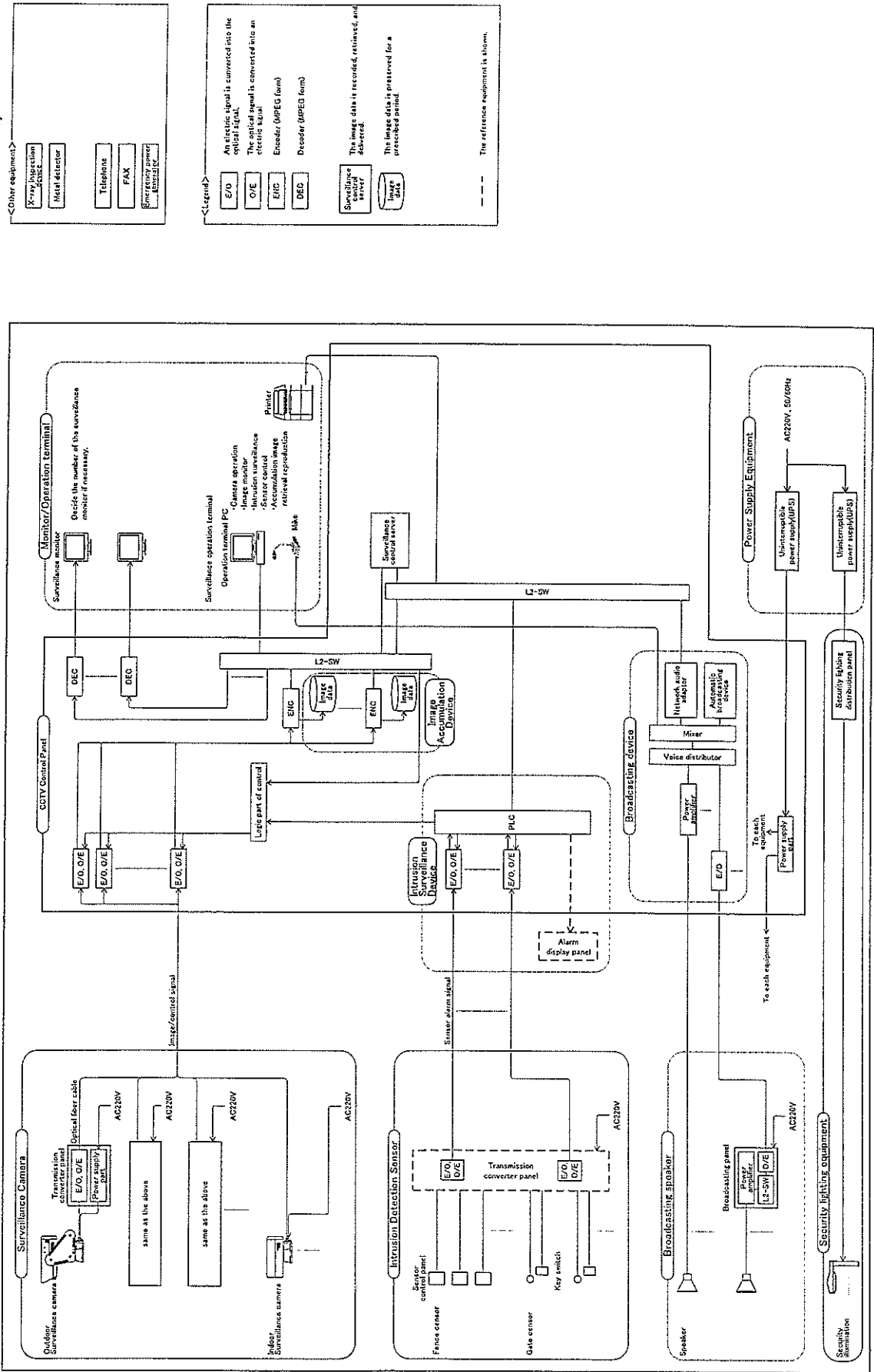
(2) Example of monitoring system configuration - 2 : CRT operation method

There is no online database retrieval of the accumulation image. (Digital method)



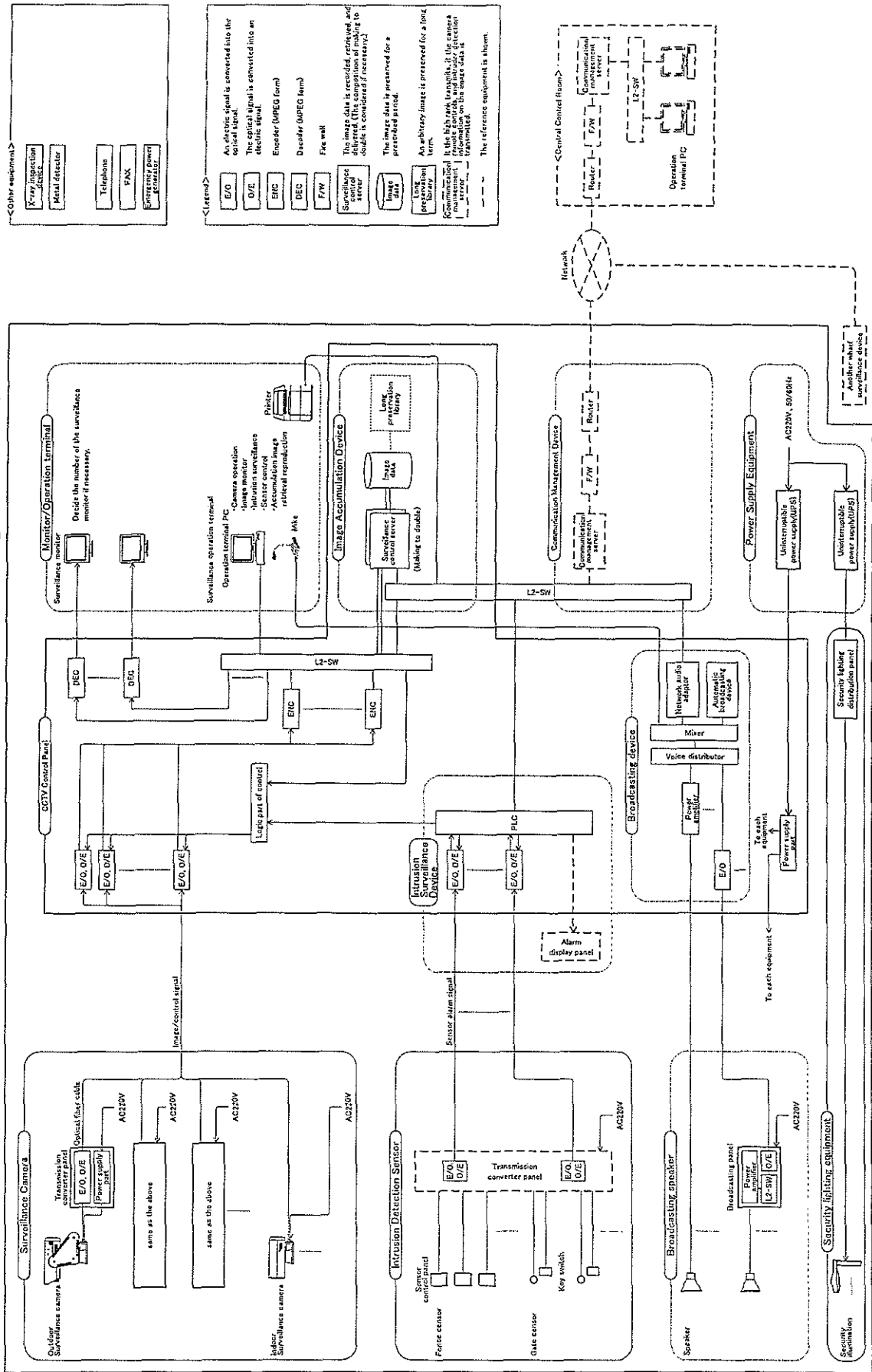
(3) Example of monitoring system configuration - 3

There is no online database retrieval of the accumulation image. (There is an invasion detection sensor.)



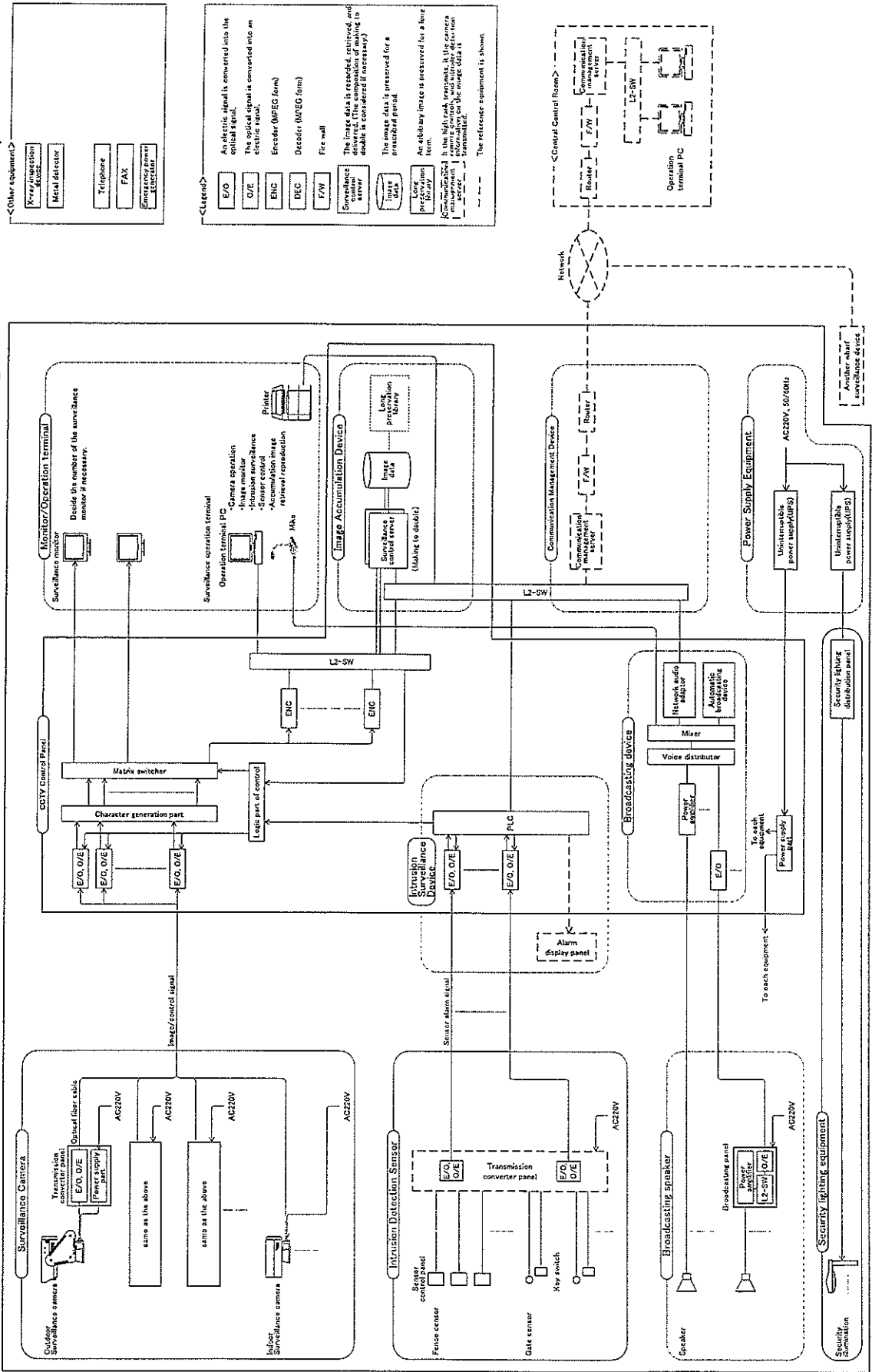
(4) Example of monitoring system configuration - 4

There is an online database retrieval of the accumulation image. (Digital method)



(5) Example of monitoring system configuration - 5

There is an online database retrieval of the accumulation image. (Analogue and digital division method)



V. Requirement for port security equipment

It is assumed for the port boundary and the yard, the equipment to observe the intruder from the fence, the person in the yard, the movement of the vehicle and moreover can acquire be a necessary image by the turn and the zoom of the surveillance camera.

A. Equipment selection

The standard of the selection of the port security equipment is shown as follows.

Port security equipment table

Equipment		Equipment(specification)	Selection requirement	Remarks
Security lighting equipment	Boundary lighting	Road light <ul style="list-style-type: none"> • High-pressure sodium light • 270W 1 light type • Install on 12mh pole. 	The road illuminator is suitable to illuminate the vicinity of the fence efficiently continuously. In this, the purpose of the distribution light of the road illuminator is to be able to illuminate it efficiently by using this along the fence of the road it is controlled linear along.	The use of the fluorescent lamp is examined in the small place.
	Gate lighting	Road light <ul style="list-style-type: none"> • High-pressure sodium light • 270W 1 light type • Install on 10mh pole. 	<ul style="list-style-type: none"> • It uses it combinedly with the boundary illumination. • When a special light is set up by the usage condition, the range of distribution of a necessary luminance can be widened more than 12m, if the height of pole of the road light is adjusted to 10m. 	The use of the fluorescent lamp is examined when depending on the place in front of the guard place etc.

	Apron lighting	<p>Floodlight</p> <ul style="list-style-type: none"> High-pressure sodium light 940 W x n light Install on 15mh lighting tower. <p>Road light</p> <ul style="list-style-type: none"> 270W 1 light type Bracket installation <p>Wall-hanging type</p>	<ul style="list-style-type: none"> The floodlight method is suitable to illuminate the wide range in the yard of the port equipment. The purpose of this is to be able to install the illuminator in the position where on pole who is higher than 12m of the sports lighting and the structure are high, and to illuminate the wide range. When lighting is done to the existing lighting tower, strength of the existing lighting tower is considered. <p>When the front side of the warehouse continuously illuminated along the wall, the road light is illuminated to the warehouse front wall by setting it up.</p> <ul style="list-style-type: none"> It supplies power in each lighting system. The on-off control of the illumination is done with the sunlight switch or the timer. 	The lighting of existing is used. When the lighting short, add new lighting.
	Lighting distribution panel			
Surveillance camera device	Outdoor turn type	<p>For medium distance</p> <ul style="list-style-type: none"> Range of turn: The horizontal 0-360° Vertical +20--70° 	<p>It is used to see of about 0-350m within the range.</p> <ul style="list-style-type: none"> The wharf extension uses it to observe port of 150m or more in the boundary part and the yard. 	
	Outdoor turn type	<p>Dome type</p> <ul style="list-style-type: none"> Range of turn: The horizontal 0-360° Vertical 0--90°(180°) 	<p>It is used to see of about 0-80m within the range.</p> <ul style="list-style-type: none"> The wharf extension uses it to observe port of 150m or less in the boundary part and the yard. 	It is secured to see of the wharf extension about 150m by setting up the camera at both ends of the apron.
	Outdoor fixation type	For short distance	<p>It is used to see of about 0-80m within the range.</p> <ul style="list-style-type: none"> Surveillance for the gate, the person, the traffic line in the vehicle, and the fixed point surveillance of a specific part. 	

The indoor turn type	Dome type •Range of turn: The horizontal 0-360° Vertical 0--90°(180°)	Surveillance for the indoor whole area in the passenger terminal building etc.	
The indoor, fixed type	Color camera	Surveillance for the gateway such as in the passenger terminal buildings, person's traffic line, and the fixed point surveillance of a specific part.	
Transmission converter panel	Outdoor wall hanging type (coaxial cable transmission method)	It supplies power to the transmission signal conversion, the relay, and the camera device of the image and the control signal. •The lightning resistance transformer and the arrester are set up. •When the distance from the camera to the CCTV control panel becomes 500m or more, transmission with the optical signal is recommended. •The transmission converter panel of the adjoining intrusion detection sensor is stored if possible.	The optical transmission method that the inducement obstruction by the electromagnetic radiation is not received is preferable in the transmission of the image and the control signal. However, the price rises compared with transmission with the coaxial cable.
	Outdoor wall hanging type (optical transmission method)	It supplies power to the optical transmission signal conversion, the relay, and the camera device of the image and the control signal. •The optical signal converter is set up. •The lightning resistance transformer and the arrester are set up. •The transmission converter panel of the adjoining intrusion detection sensor is stored if possible.	

Intrusion detection sensor				
Fence Sensor	Vibration sensor Sensor control panel •Outdoor wall hanging type	If the adaptability to the fence is good, it is a top priority method of the fence sensor. •Use for a net type fence. •In case using of grid type fence, it is necessary to confirm transmitting condition for the vibration. •The sensor control panel is set up on the machine side. •The signal relay and the power supply of the infrared sensor that is are done to be near.	The vibration by the strong wind might be mis-detected.	
	Tension sensor • Line type • Encoder pulse type sensor control panel • Outdoor wall hanging type	It applies to the place where the vibration sensor cannot be used. • It uses it for the top guard part. • It uses it for the type that the vibration sensor of the grid type fence cannot be used. The sensor control panel is set up on the machine side. • The signal relay and the power supply of the infrared sensor that is are done to be near.	The encoder pulse type can output the multistep of alarm.	
	Infrared sensor	It uses it for the place where the vibration sensor and the tension sensor cannot be used. • It uses it for the top guard part. • Because degree of freedom to installation features is higher than other methods, it becomes the object of the application sensor to a special place.	The heavy rain and the fog might not do the detection function.	
Gate Sensor	Infrared sensor	Top priority method of gate sensor • It installs it upper (top guard part) and down side of the net type gate. • It installs it upper (top guard part) side only in the gate that cannot do the cut or clash-broken of the grid type etc.	The heavy rain and the fog might not do the detection function.	

	Tension sensor Sensor control panel	<ul style="list-style-type: none"> In case the sensor wire is woven into the net, use as a cutting sensor. It uses it for the top guard part. <p>The sensor control panel is set up on the machine side.</p> <ul style="list-style-type: none"> The signal relay and the power supply of the infrared sensor that is are done to be near. 	There are a lot of number of parts and sensor wiring in the front side. Therefore undesirable to use as a tension sensor.
	Key switch panel	It uses it to set "Use-No use" of the infrared sensor signal at the gate.	
Transmission converter panel	Outdoor wall hanging type	<ul style="list-style-type: none"> Two or more adjoining sensor signals are gathered and transmitted to the surveillance control panel. Storing it on the transmission converter panel of the adjoining surveillance camera is economical if possible. The cable can be connected from an individual sensor control panel to the surveillance control panel without setting up this panel. However, the number of the cable and the number of wicks increase, and the construction of construction is bad. 	It has the signal transmission unit on an individual sensor control panel or if the cable is connected without using the transmission unit, this panel is unnecessary.
Surveillance control panel 1 (CCTV control panel)	Image and control signal converter Character generation part *1. Matrix switcher *2. Logic control part (PLC) Encoder/decoder *3. Network equipment *4. Timeserver Power supply unit	<ul style="list-style-type: none"> The control of the surveillance camera and the image from the surveillance camera are selecting displayed. It supplies power to each equipment. <p>*1 :If the character generation function is provided in the camera, and it meets the specification, it is unnecessary. When the image signal is digitalized, it is unnecessary because the character can add at this point.</p> <p>*2 :It is necessary and it is unnecessary in case of not being, select the analog image signal from the camera directly, switch, and display it (It converts digitally and process it.)</p> <p>*3-4: When the image signal is digitalized, it is necessary.</p>	A necessary function and the equipment are decided based on the surveillance equipment system.
Monitor and control			

Intrusion surveillance device	PLC Alarm display panel	<ul style="list-style-type: none"> •The signal from the intrusion detection sensor is displayed on the alarm display panel. •The Alarm signal of the sensor is sent to the image record device for making the index of the image data. •PLC is stored on the surveillance control panel. Moreover, using with logic part (PLC) of the control of the surveillance control panel combinedly is also possible. 	The alarm display panel is unnecessary if it is not necessary to display alarm in the PC operation table, and to display it in other places.
Monitor and control	Surveillance control server	<ul style="list-style-type: none"> •The image data is recorded, retrieved, and delivered. •The surveillance control server is stored on the surveillance control panel. 	
Image record device	Video recorder	<ul style="list-style-type: none"> •Online database retrieval none. (basic method) •The image data is preserved for a prescribed period. •The image of each camera is in real time recorded. •Backup function none. 	<ul style="list-style-type: none"> •The video recorder is assumed to be a basic method. •However, the video recorder or the hard disk is selected if necessary.
	Hard disk	<ul style="list-style-type: none"> •There is online database retrieval. •The image data is preserved for a prescribed period. •The image of each camera is real time and digital recorded. •Even if the trouble occurs by recording in the disk array of the RAID5 composition on one disk, it is possible to back up. 	It sets it up if necessary.
Surveillance and operation terminal	Hard disk (for long preservation record)	<ul style="list-style-type: none"> •There is online database retrieval. •An arbitrary image is preserved for a long term. •It is assumed the RAID5 composition. 	
	Key switch controller	<ul style="list-style-type: none"> •Switch panel type. CRT operation type is compared, and it is cheap and maintenance is easy. •When the online database retrieval and the intrusion detection sensor of the accumulation image are maintained because only the camera operation can be done, the device is separately necessary. 	<ul style="list-style-type: none"> •The key controller is assumed to be a basic method. •However, the key

		<p>PC operation table</p> <ul style="list-style-type: none"> • PC • Display part(20 types TFT) • Printer 	<ul style="list-style-type: none"> • CRT operation type. Operativeness improves compared with the switch panel type. • The online database retrieval of the accumulation image, and the intrusion detection sensor is observed and it is possible to operate it. • The display device of the attachment recommends two for the surveillance operation screen and for the camera image display. 	<p>controller or the PC operation table is selected if necessary.</p>
		<p>Surveillance monitor</p> <ul style="list-style-type: none"> • 20 types TFT 	<ul style="list-style-type: none"> • The image of the surveillance camera is displayed by dividing in one screen or the screen. • The number is decided if necessary. • The collective setting is recommended to the monitor panel when there are a lot of numbers. 	<p>It is possible to set it up on the wall hanging, the ceiling hanging, and the desk when the number is few.</p>
	<p>Communication management device</p>	<p>Communication management server</p> <p>Networking gear</p>	<ul style="list-style-type: none"> • The trouble watch and the history of networking equipment are managed. • If the high rank transmits, it the camera remote controls, and intruder detection information on the image data is transmitted. 	<p>It is unnecessary if there is no communication with a high-ranking organization.</p>
	<p>X-ray inspection device</p>	<p>Medium</p> <ul style="list-style-type: none"> • Size of tunnel: 650mm-800mm or more • Height of conveyor: About 230mm-350mm <p>Small size</p> <ul style="list-style-type: none"> • Size of tunnel: 600mm-400mm or more • Height of conveyor: About 600mm-800mm 	<p>Traveler's depositing luggage is inspected.</p> <ul style="list-style-type: none"> • The material identification function and the outline emphasis function are provided. <p>Traveler's carrying luggage is inspected.</p> <ul style="list-style-type: none"> • The material identification function and the outline emphasis function are provided. ; 	<p>It is attached uninterrupted power supply system (UPS) as back up and fixed voltage device during power failure.</p> <p>The back-up time is assumed to be ten minutes.</p>
	<p>Luggage inspection device</p>			

	<p>Metal detector</p> <p>Gate type</p> <ul style="list-style-type: none"> • Gate size: 700mm W-2000mmH or more <p>Portable type</p> <ul style="list-style-type: none"> • Weight: 400g or less 	<p>Inspect the possession goods of the traveler who passes in the gate by non-contact.</p> <ul style="list-style-type: none"> • The metal and nonferrous metals are detected. • Back-up battery is built into the system for power failure. <p>The traveler's possession goods inspection and the inspection of luggage are arbitrarily done by non-contact.</p> <ul style="list-style-type: none"> • The metal and nonferrous metals are detected. • There must be an enough detection sensitivity. • It is possible to use it by adopting dry battery or rechargeable battery. 	<p>The necessary detection sensitivity is decided in consideration of the detection object and the usage condition.</p>
	<p>Speaker</p> <p>Speaker</p> <ul style="list-style-type: none"> • 50W, 110dB(basic ratings) • 15W, 108dB <p>Broadcasting panel</p> <ul style="list-style-type: none"> • Power amplifier: 15, 30, 60, 120W • Panel case: Outdoor wall hanging type 	<p>Outdoor installation: Horn speaker (Possible set up is 50 W x 2 parallel instead of 100Wx1 installation)</p> <p>The indoor installation: Box speaker or horn speaker (15W or less)</p> <p>When the power amplifier is put on the speaker side, it stores it on the broadcasting panel.</p> <ul style="list-style-type: none"> • Ratings of the power amplifier are decided from the capacity of the connected speaker. 	<p>The speaker ratings for the ship are decided for the vicinity of the bridge to reach a necessary sound pressure.</p> <p>When doing, concentrated installation is unnecessary in the cabinet rack type broadcasting device it.</p>
Public address system			

Cabinet rack type broadcasting device	Power amplifier • 30, 60, 120, 240W	Concentrated installation is done to the cabinet rack type broadcasting device the power amplifier. • Ratings of the power amplifier are decided from the capacity of the connected speaker.	When the broadcasting panel is put, it doesn't store the power amplifier on each broadcasting panel.
	Voice distribution machine	The speaker line is selected, and the audio signal is output. • Number of lines: More than six(6) lines • Broadcasting can be selected individual or together.	
	Microphone mixer	The input line such as microphones is selected, the signal is amplified, and it outputs it. • Number of lines: More than three(3) lines	
	Digital announcement machine	The voice registered beforehand is arbitrarily reproduced. • Number of reproduction programs: Eight programs	
	Network audio adapter	A remote broadcasting and the line selection control by way of the network are done.	It is unnecessary if there is not broadcasting from remoteness by way of the network.
	Power supply unit	The power supply to each equipment is done. When blacking out, the battery for Baccap is built into. • It is internal organs as for the battery for the backup to power failure.	
Mike	Mike	The voice is converted into an electric signal, and it inputs it to the microphone mixer. • The line selection switch selects the speaker output system of the voice distributor with the selection of the microphone mixer input system.	If it substitutes it with the PC operation table, the line selection switch is unnecessary.

Communication equipment	Telephone	Power supply unnecessary	The speed dialing can register.	Even when power failure, it is necessary to be able to use it.
	FAX	Record paper size: A3	The broadcast can transmit to two or more places.	
	Uninterrupted power supply system (UPS)	Ratings output capacity: 5.2, 7.5, 10, 15, and 20kVA Power force: 80% AC input: AC220V and 50/60Hz AC output: AC220V and 50/60Hz Power failure back-up time: 10 minutes or more	It is always assumed the inverter feeding power supply method. It functions as a result as the fixed voltage device; moreover, ten minutes of the power failure as emergency power supply equipment. The declared power is decided from the capacity of the use load. The automatic change over function is required for shutdown or recover of commercial power supply line. The power supply backup object is assumed to be security surveillance equipment, security lighting equipment (for boundary), and well informed man report equipment.	It sets it up in facilities where the surveillance camera is used. When the declared power becomes 20kVA or more, it divides for the security surveillance equipment and for the security lighting.
	Power-supply unit	Power input/output panel	The commercial power is sent directly to the load side separating UPS from the power supply system when breaking down adding the Power input/output panel to UPS for the security surveillance equipment.	It sets it up if necessary for the lighting.

Generator for emergency	Ratings output capacity: 25/30kVA Power force: 80% Rated voltage: AC220V and 50/60Hz Start time: Within 40 seconds Automatic change panel	The place with the generator for the emergency for the port equipment examines the use. •The declared power is decided from the capacity of the use load. •It starts automatically by the power failure signal from the automatic change panel with the commercial power, and it stops again automatically by the telegraphic communication title. •The fuel tank recommends the capacity that can continuous be driven about 12 hours or more. The commercial power supply system is switched to the power supply system of the generator for the emergency. •The commercial power is power failure or recovered the signal issue to start or stop of the generator for the emergency.	It sets it up if necessary.
Electrical panel for receiving transformer (remodeling)	The primary voltage: - The secondary voltage: AC220V, 50/60Hz Voltage: AC220V, 50/60Hz	When the receiving voltage is different from the standard voltage, transformer makes it to the standard voltage. The power supply to the security equipment is supplied. •May use it combined with the Electrical panel for receiving transformer and the UPS Power input/output panel. •Power supplies of the security surveillance equipment except the security lighting power supply may provide the function of the distribution panel for the surveillance control panel. •May use it combined with the lighting distribution panel for the security lighting.	It newly establishes or it remodels it, if necessary. It sets it up if necessary.
Distribution panel			

B. Requirement for port security surveillance equipment

(1) Camera

The standard issue with the outdoor surveillance camera that sees the medium range applies as follows.

- | | |
|------------------------------|--|
| 1) Type | : Outdoor camera-platform integrated slewing-type camera |
| 2) Optical system (lens) | |
| Structure | : Electric zoom lens |
| Focal length | : Short 10 mm or less, longest 120 mm or more (However, the zoom ratio is 15 times or more.) |
| Effective aperture | : About 75 mm, Maximum focal ratios: F 1.6 or less, T no. 2.0 or less. |
| Squeezing | : Equipped with auto iris, auto focusing function |
| The preset function | : The zoom and focus can be set. |
| 3) Image part (camera) | |
| Image pickup device | : 1/2 inches high sensitivity CCD single plate color |
| The valid pixel | : About 380,000 pixels |
| Image signal output | : PAL or NTSC conforming |
| Lowest object illuminance | : 0.4 lx (F1.6) at color mode (light storage nullified) |
| Light storage function | : The principle is not used.
(Only the light storage function up to four frames or less is used to catch quick movement of the intruder etc. even when using it.) |
| Resolution | : Horizontal 480 TV lines or more, vertical 350 TV lines or more |
| S/N ratio | : 50db or more |
| Backlighting compensation | : Auto |
| 4) Machine (Camera platform) | |
| Structure | : Electric rotorplatform for outdoor |
| Turn angle | : Horizontal 0-360° slewing, vertical +20- -70° slewing
(To assume the sight of one's feet to be minimum, vertical is brought close to -90° as much as possible.) |
| Maximum slewing speed | |
| •Preset operates | : Horizontal 180°/second or more, Vertical 60°/second or more
(It is necessary to be able to turn to the preset position instantaneously.) |
| •Manual operation operates | : Horizontal 15°/second , Vertical 15°/second
(The turn operation that pursues the person who runs while seeing the surveillance monitor should be able to be done.) |

Stop accuracy : Within $\pm 0.3^\circ$
Number of presets : 32 points or more (The horizontal, vertical, and the zoom and focus of each point can be set.)

5) Camera case

Structure : Outdoor jet-proof type (IP65 conforming)
Attached mechanism : Defrosta, heater, and wiper equipment

6) Others

- Resistance to wind velocity : 60m/second or more (non-operating nondestructive),
40m/second or more (manual operation)
- Protection against lightning : It equips it with arrestor and the lightning resistance transformer.
- Salt resistance : The salt resistance processing of the anti-corrosion material and the salt resistant painting is given.
- Suit it separately with the equipped image record device.

(2) System

The function of the monitoring instrument applies to the following specifications.

1) Image management

- The surveillance image and the camera signal from the surveillance camera are digitalized, and it is transmitted to the network.
- The image received from the specified surveillance camera is in real time output to the image indicator.
- The display of the image arbitrarily selected with the surveillance terminal is enabled.
- It is enabled that it is arbitrarily a setting of the surveillance condition of the camera (direction and magnification, etc.) with the surveillance terminal.
- The image is recorded.
- The index is put on the surveillance footage, and it is possible to preserve it in real time.
- The image delivery to the terminal the image search from each surveillance terminal is possible, and with the demand enables it.

The image retrieval by the index from each surveillance terminal and the image retrieval by the space that uses the map of the retrieval at the time of the camera image and the wharf and the image charts are enabled.

- The image record and the reproduction are assumed to be executable at the same time.

2) Image delivery function

- The image to a high-ranking bureau is delivered.

3) Sensor control

- When detect abnormality with the sensor, can preserve the detected image of about time.

- It synchronizes with the sensor Alarm signal, and the direction of view of the camera is moved.
- The synchronization setting of the sensor and the camera is enabled.

(3) Security

It is a thing when communicating via the public circuit to do the security measures.

VI. The specification of main equipment (Example)

A. Security lighting equipment

(1) Road light

1) Function

An intentional alarm is sent to the intruder by setting up the security lighting in the port facilities boundary part (The gate is included). And, to secure a necessary luminance of the surveillance camera, the security lighting is arranged. Moreover, to secure the luminance of the front side of the warehouse, the security lighting is set up on the wall of the warehouse.

2) Specification and standard

Lamp name	: High-pressure sodium lamp corresponding
Size of lamp	: 270W×1(light)
Lamp voltage	: AC200/220V 50/60Hz
Height of installation	: The installation is assumed to lighting Pole of 10m or 12m. The installation is assumed to the wall of the warehouse with the bracket.
Waterproof performance	: Spray-proof type's corresponding
Others	: Give the per-device the salt damage measures enough.

(2) Floodlight (beam type)

1) Function

To secure the illuminance needed to guard the ship in the port with the surveillance camera, the floodlight is set up in the apron part.

2) Specification and standard

Lamp name	: High-pressure sodium lamp corresponding
Size of lamp	: 940W×3 (light) assumption 【Decide it according to individual facilities and installation features】
Lamp voltage	: AC200/220V 50/60Hz
Height of installation	: The installation is assumed to the lighting tower of 15m. 【Decide it according to individual facilities and installation features】
Waterproof performance	: Spray-proof type's corresponding
Others	: Give the per-device the salt damage measures enough.

(3) Lighting Pole

1) Function

Set up the lighting. Moreover, contain the anchor bolt.

2) Specification and standard

a) Lighting Pole (for road light)

Structure	: Base plate type
Material	: Steel pipe (STK-400)
Processing	: Melted zinc plating processing (HDZ35 or more)
Length	: The height of 10m or 12m on the ground should be able to be equipped with the lighting.
Others	: Give the per-device the salt damage measures enough.

b) Bracket (for road light)

Structure	: 【 Decide it according to individual facilities and installation features 】
Material	: Steel pipe (STK-400)
Processing	: Melted zinc plating processing (HDZ35 or more)
Installation	: The structure wall should be able to be equipped with the lighting.
Others	: Give the per-device the salt damage measures enough.

c) Lighting tower (for floodlight)

Structure	: 【 Decide it according to individual facilities and installation features 】
Others	: Give the per-device the salt damage measures enough.

3) Notes

Decide the prop and the base according to the strength calculation.

(4) Lighting distribution panel

1) Function

The lighting power supply system is divided into the plural, and the power supply is supplied. Moreover, an automatic blinking the illumination is controlled with the sunlight switch set up in outdoor or the timer.

2) Specification and standard

Structure	: Indoor, dustproof, wall-hanging type, with a door key
Power supply	: AC200/220V, 50/Hz
Main circuit	: 1 x MCCB

Divergence circuit	: n x ELCB 【The number of circuits is decided in individual facilities】
The control circuit	: In the signal of the sunlight switch (outdoor installation) or the timer, MC (electromagnetic contactor) is on and off.
Operating switch	: "Automatic operation - manual operation" selection switch, "On", "Off" push button switch
Panel material	: Steel plate
Painting	: Melamine resin printing painting (Half gloss is erased) or corresponding after rust prevention is processed
Others	: Give the per-device the salt damage measures enough.

B. Surveillance camera device

(1) Medium distance of vision of outdoor slewing type camera (1)

1) Function

It is required in the yard of the port boundary that the equipment will observe the movement of the intruder from the fence and the person and the vehicle in the yard. Moreover, can acquire necessary images by the turn and the zoom.

2) Specification and standard

- a) Type : Outdoor camera-platform integrated, slewing-type camera
- b) Lens : Electric zoom lens
 - Distance of vision : 350m or more
 - Focal length : 10-250mm, 25 time zoom lenses
 - Effective aperture : 107.5mm, Maximum focal ratios: F1.5 (W) and T no. 1.79 (W)
 - Squeezing : Equipped with auto iris, auto focusing function
 - Preset function : The zoom and focus can be set.
- c) Main body of camera
 - Image pickup device : 1/2 inches high sensitivity CCD single plate color and 410,000 pixels
 - Image signal output : PAL or NTSC conforming
 - Lowest object Illuminance : 0.31 lx (F1.5) at color mode (light storage nullified)
 - Light storage function : 2 - 128 times
 - Resolution : Horizontal 480 TV lines or more, vertical 350 TV lines or more
 - S/N ratio : 50dB or more
 - Backlighting compensation : Auto
- d) Camera platform
 - Structure : Electric rotorplatform for outdoor
 - Turn angle : Horizontal 0-360° slewing, vertical +20- -70° slewing
 - Maximum slewing speed
 - Preset operates : Horizontal 180°/second or more, Vertical 60°/second or more
 - Manual operation operates : Horizontal 15°/second , Vertical 15°/second
 - Stop accuracy : Within horizontal, vertical $\pm 0.3^\circ$
 - Number of preset positions : 256
(The horizontal, vertical, and the zoom and focus of each point can be set.)
- e) Camera case
 - Structure : Outdoor jet-proof type (IP65 conforming)
 - Material : Aluminum alloy

Cooling : Built-in fan
Attached mechanism : Defrosta and heater, Wiper

f) Others

Power supply : Ac200/220V or AC100V, 50/60Hz
Environmental condition : Temperature -20°C - +40°C, relative humidity 10% - 90%RH

Wind pressure (Camera platform operation)

- Normal performance : 20m / second or less
- Manual operation possible : 40m / second or less
- Nondestructive : 60m / second or more

Salt damage measures : The painting of the part that has been exposed outside is finished up by fluoroplastics painting.
The screw that does processing (Cr-3) that endures salt resistance is used for the screws that have been exposed outside.

(2) Medium distance of vision of outdoor slewing type camera (2)

1) Function

It is required in the yard of the port boundary that the equipment will observe the movement of the intruder from the fence and the person and the vehicle in the yard. Moreover, can acquire necessary images by the turn and the zoom.

2) Specification and standard

a) Type : Outdoor camera-platform integrated slewing-type camera

b) Lens : Electric zoom lens

Distance of vision : 350m

Focal length : 7.5-120mm, 16 time zoom lenses

Effective aperture : 68mm, Maximum focal ratios: F1.6 (W) and T no. 2 (W)

Squeezing : Equipped with auto iris, auto focusing function

The preset function : The zoom and focus can be set.

c) Main body of camera

Image pickup device : 1/2 inches high sensitivity CCD single plate color and 380,000 pixels

Image signal output : PAL or NTSC conforming

Lowest object Illuminance : 0.4 lx (F1.6) at color mode (light storage nullified)

Light storage function : 2 - 64 times

Resolution : Horizontal 480 TV lines or more, vertical 350 TV lines or more

S/N ratio : 50dB or more

- Backlighting compensation : Auto
- d) Camera platform
- Structure : Electric rotorplatform for outdoor
- Turn angle : Horizontal 0-360° slewing, vertical +20- -90° slewing
- Maximum slewing speed
- Preset operates : Horizontal 180°/second or more, Vertical 90°/second or more
 - Manual operation operates : Horizontal 0.05 - 30°/second , Vertical 0.05 - 30°/second
- Stop accuracy : Within horizontal, vertical $\pm 0.05^\circ$
- Number of preset positions : 256
- (The horizontal, vertical, and the zoom and focus of each point can be set.)
- e) Camera case
- Structure : Outdoor jet-proof type
- Material : Aluminum alloy
- Cooling : (Built-in fan)
- Attached mechanism : Defrosta and heater, Wiper
- f) Others
- Power supply : Ac200/220V or AC100V, 50/60Hz
- Environmental condition : Temperature -20°C - +40°C, relative humidity 10% - 90%RH
- Wind pressure (Camera platform operation)
- Normal performance : 20m / second or less
 - Manual operation possible : 40m / second or less
 - Nondestructive : 60m / second or more
- The salt damage measures : Give the per-device the salt damage measures enough.

(3) Outdoor slewing-type dome camera

1) Function

It is required in the yard of the Port boundary the equipment will observe the movement of the intruder from the fence and the person and the vehicle in the yard. Moreover, can acquire necessary images by the turn and the zoom.

2) Specification and standard

- a) Type : Outdoor slewing-type dome camera
- b) Lens : Electric zoom lens
- Distance of vision : m
- Focal length : 3.79 - 83.4mm, 22 time zoom lenses
- Effective aperture : 68mm, Maximum focal ratios: F1.6 (W) and T no. 3 (W)
- Squeezing : Equipped with auto iris, auto focusing function

- The preset function : The zoom and focus can be set.
- c) Main body of camera
- Image pickup device : 1/4 inches CCD single plate color and 380,000 pixels
- Image signal output : PAL or NTSC conforming
- Lowest object Illuminance : 1 lx (F1.6) at color mode (light storage nullified)
- Light storage function : 2 - 64 times
- Resolution : Horizontal 480 TV lines or more, vertical 350 TV lines or more
- S/N ratio : 50dB or more
- Backlighting compensation : Auto
- d) Camera platform
- Structure : Electric rotorplatform for outdoor
- Turn angle : Horizontal 0-360° slewing, vertical 0- -90° siewing
- Maximum slewing speed
- Preset operates : Horizontal 300°/second or more, Vertical 300°/second or more
 - Manual operation operates : Horizontal 0.1 - 20°/second , Vertical 0.1 - 20°/second
- Stop accuracy : Within horizontal, vertical $\pm 0.05^\circ$
- Number of preset positions : 64
- (The horizontal, vertical, and the zoom and focus of each point can be set.)
- e) Camera case
- Structure : Outdoor jet-proof type
- Material : Aluminum die cast and others
- Cooling : (Built-in fan)
- Attached mechanism : Defrosta and heater
- f) Others
- Power supply : Ac200/220V or AC100V, 50/60Hz
- Environmental condition : Temperature -20°C - +40°C, relative humidity 10% - 90%RH
- Wind pressure (Camera platform operation)
- Nondestructive : 60m / second or more
- The salt damage measures : Give the per-device the salt damage measures enough.

(4) Short distance of vision of outdoor fixed type camera

1) Function

It is required to the Port boundary the equipment will observe the intruder from the fence.

2) Specification and standard

- a) Type : Outdoor camera-platform integrated fixed-type camera

- b) Lens : Manual zoom lens
 - Distance of vision : 80m
 - Focal length : 8 - 48mm, 6 time manual zoom lenses
 - Effective aperture : mm, Maximum focal ratios: F1.4 (W) and T no. (W)
 - Squeezing : Manual operation
- c) Main body of camera
 - Image pickup device : 1/2 inches high sensitivity CCD single plate color and 380,000 pixels
 - Image signal output : PAL or NTSC conforming
 - Lowest object Illuminance : 1 lx (F1.4) at color mode (light storage nullified)
 - Light storage function : 2 - 32 times
 - Resolution : Horizontal 480 TV lines or more, vertical 350 TV lines or more
 - S/N ratio : 50dB or more
 - Backlighting compensation : Auto
- d) Camera platform
 - Structure : Outdoor, Manual adjustment type
 - Adjustment angle : Horizontal ± 30 , vertical ± 30
- e) Camera case
 - Structure : Outdoor jet-proof type
 - Material : Aluminum alloy
 - Cooling : (Built-in fan)
 - Attached mechanism : Defrosta and heater, Wiper
- f) Others
 - Power supply : Ac200/220V or AC100V, 50/60Hz
 - Environmental condition : Temperature -20°C - $+40^{\circ}\text{C}$, relative humidity 10% - 90%RH
 - Wind pressure (Camera platform operation)
 - Nondestructive : 60m / second or less
 - The salt damage measures : Give the per-device the salt damage measures enough.

(5) Indoor slewing-type dome camera

1) Function

It is assumed the equipment to observe person's movement in the Port passenger terminal building. Moreover, can acquire be a necessary image by the turn and the zoom.

2) Specification and standard

- a) Type : Indoor slewing-type dome camera
- b) Lens : Electric zoom lens

Distance of vision : m
 Focal length : 3.79 – 83.4mm, 22 time zoom lenses
 Effective aperture : 27mm, Maximum focal ratios: F1.6 (W) and T no. 3 (W)
 Squeezing : Equipped with auto iris, auto focusing function
 The preset function : The zoom and focus can be set.

c) Main body of camera

Image pickup device : 1/4 inches CCD single plate color and 380,000 pixels
 Image signal output : PAL or NTSC conforming
 Lowest object Illuminance : 1 lx (F1.6) at color mode (light storage nullified)
 Light storage function : 2 - 64 times
 Resolution : Horizontal 480 TV lines or more, vertical 350 TV lines or more
 S/N ratio : 50dB or more
 Backlighting compensation : Auto

d) Camera platform

Structure : Electric rotorplatform for outdoor
 Turn angle : Horizontal 0-360° slewing, vertical 0- -90° slewing
 Maximum slewing speed
 ·Preset operates : Horizontal 300°/second or more, Vertical 300°/second or more
 ·Manual operation operates : Horizontal 0.1 - 20°/second , Vertical 0.1 - 20°/second
 Stop accuracy : Within horizontal, vertical $\pm 0.05^\circ$
 Number of preset positions : 64
 (The horizontal, vertical, and the zoom and focus of each point can be set.)

e) Camera case

Structure : Indoor dust-proof type
 Material : Aluminum die cast and others
 Cooling : (Built-in fan)
 Attached mechanism : (Defrosta and heater)

f) Others

Power supply : Ac200/220V or AC100V, 50/60Hz
 Environmental condition : Temperature -20°C - +50°C, relative humidity 10% - 90%RH

(6) Indoor, fixed camera

1) Function

It is assumed the equipment to observe person's movement in the Port passenger terminal building.

2) Specification and standard

- a) Type : Indoor fixed-type camera
- b) Lens : Manual zoom lens
 - Distance of vision : 80m
 - Focal length : 8 - 48mm, 6 time manual zoom lenses
 - Effective aperture : mm, Maximum focal ratios: F1.4 (W) and T no. (W)
 - Squeezing : Manual operation
- c) Main body of camera
 - Image pickup device : 1/2 inches CCD single plate color and 380,000 pixels
 - Image signal output : PAL or NTSC conforming
 - Lowest object Illuminance : 1 lx (F1.4) at color mode (light storage nullified)
 - Light storage function : 2 - 32 times
 - Resolution : Horizontal 480 TV lines or more, vertical 350 TV lines or more
 - S/N ratio : 50dB or more
 - Backlighting compensation : Auto
- d) Camera platform
- e) Camera case
- f) Others
 - Power supply : AC200/220V or AC100V, 50/60Hz
 - Environmental condition : Temperature -10°C - +50°C, relative humidity 10% - 90%RH

(7) Camera signal transmission converter panel

1) Function

The supply of the function of the video protector and AC power from the outside that protects the equipment from a dielectric lightning and the noise is assumed to be the one to have the function of the lightning resistance transformer that supplies a necessary voltage and current for the receiving equipment.

2) Specification and standard

a) Video protector

- Input impedance : 75Ω no equilibrium
- Output impedance : 75Ω equilibrium

b) Lightning resistant transformer

- Input voltage : 1φ2W AC200/220V
- Output voltage : 1φ2W AC100V, (AC200/220V)
(Match it to the power supply specification of the equipment)

Capacity : 500VA
used in the camera and the panel.)
(Match it to the power supply capacity of the equipment used in the camera and the panel.)

c) Camera operation switch

The switch for the camera adjustment is set up if necessary.

d) Optical signal converter

i) Function

The image and the control signal of the camera are converted into the optical signal, it restores, and it transmits with the optical fiber cable.

It is unnecessary when transmitting with the coaxial cable without converting it into the optical signal.

ii) Specification and standard

Image signal : PAL or NTSC
Control signal : RS-232C and RS-485, etc.
I/O connector : BNC
Transmission method : Optical signal

e) Panel case

Structure : Outdoor, Waterproof, wall-hanging type, shading board installation, with a door key
Detection of door open : With door switch
Panel material : Stainless steel
Painting : Salt resistant painting

f) Others : Give the per-device the salt damage measures enough.

(8) Camera pole

1) Function

Set up the surveillance camera. Assume the structure equipped with the check stand, and contain the anchor bolt if necessary.

2) Specification and standard

a) Steel pole

Structure : Base plate type

Material : Steel pipe (STK-400)
Processing : Melted zinc plating processing (HDZ35 or more)
Length : 5-10m on the ground should be able to be equipped with the surveillance camera.
Others : Give the per-device the salt damage measures enough.

b) Concrete Pole

Standard : Precast presto concrete pole
Structure : Conic body with taper
Material : Ferroconcrete
Processing : Centrifugal force well-set hardening formation
Length : 10m on the ground should be able to be equipped with the surveillance camera.
Others : Give the salt damage measures enough to metal fittings put up to the pillar. (melted zinc plating processing)

3) Notes

Decide the prop and the base according to the strength calculation.

C. Intrusion detection sensor

1. Fence sensor

(1) Vibration sensor

1) Function

It is a method of the precaution on the side to observe the vibration of the entire fence (net part) for the intrusion detection from the fence. If the main body of the fence is 2.4m or less, the sensor cable Article 1 is horizontally put on the position between iron wires put on height at the middle level of the main body of the fence total height and the vicinity that almost becomes middle and it passes it.

2) Specification and standard

a) Vibration sensor cable

Sensor cable : Ferroelectric plastic coaxial cable

Sensor cable length : 300m/controller or less

The detection division length : 50m or 100m or less is assumed to be a standard.

The fence is delimited to an arbitrary division, and the vibration is detected at each division.

【An individual detection division is suited to the fence and ambient conditions and decided 】

The detection requirement : The person climbs the fence.

The fence is cut.

Accessory : Cable of no perception, terminator, Inshurocctai, and silicon

Others : Give the per-device the salt damage measures enough.

b) Vibration sensor controller

Number of input circuits : 1 circuit, or 2 circuits

Detection condition : The judgment algorithm corresponding to the vibration type : in the controller. It is enabled that it is a setting.

(The vibration by the traffic of a strong wind and a large-scale vehicle etc. must have the regulating function excluded so as not to mis-detect it as much as possible.)

Cutting is detected : Cutting the sensor cable is detected.

Detection sensitivity : The adjustment must be possible.

Alarm output : Two step output of advisory signal and alarm signal

Dry contact relay output (1b) × 2

Power-supply voltage : 12-24V DC

c) Vibration sensor control panel

i) Function

The controller for the vibration sensor is stored. Moreover, the supply of AC power from the outside is supplied and a necessary voltage and current for the receiving equipment are supplied. Moreover, the signal relay and the power supply of the infrared sensor and the key switch that is are done to be near.

ii) Specification and standard

Structure	: Outdoor, Waterproof, wall-hanging type, with a door key
Detection of door open	: With door switch
Number of controller	: 1 fence sensor circuit
Power supply unit	: AC200/220V /DC24V
Power-supply voltage	: AC200/220V、1φ、2W
Panel material	: Stainless steel
Painting	: Salt resistant painting
Protection against lightning	: It equips it with arrestor and the lightning resistance transformer.
Salt damage measures	: Give the per-device the salt damage measures enough.

(2) Tension sensor

1) Function

In order to detect the intrusion from the fence a few lines are installed in all aspects of the fence and top guard part. And the sensor detects the loud, pull, and cutting which occur when the intruder hangs those lines. The sensor line is horizontally put by the pitch of 220mm or less and passed in front of the net part of the fence. The top guard part also similarly horizontally puts and passes Article or more than 2 in the pitch of 220mm or less.

2) Specification and standard

a) Tension sensor (The display mechanism of operation is none.)

Method	: The wire is pulled, or Cutting of wire (loop energizing method)
Sensor wire	: SUS304 and polyethylene double sheath (Outside diameter 2.8mm, wick wire 0.3mm x 7)
Sensor line length	: 500m/circuit or less
Detection division length	: 50m or 100m or less is assumed to be a standard. 【An individual detection division and the number of circuits are suited to the fence and ambient conditions and decided.】
Sensor installation span	: 20m (installation of one every 20m)
Detection condition	
• Operation load	: 4.0kg(horizontal direction)
• Cutting load of wire	: 80kg (sensor wire) and whole load 40kg

·Cutting is detected : The cutting of the sensor wire should be able to be detected.
 Operation sensitivity : The adjustment must be possible.
 Alarm output : Lead switch
 The sensor automatic operation return : The sensor after it warns must return automatically. (However, the destruction of the sensor and cutting the sensor wire are excluded.)
 Sensor operation display : None
 Power-supply voltage : 12/24V DC
 Accessory : Holder (support of sensor wire), sensor cushion rubber, Installation band
 Others : Give the per-device the salt damage measures enough.

b) Tension sensor (There is an operation display mechanism.)

Method : The wire is pulled, or Cutting of wire (loop energizing method)
 Sensor wire : SUS304 and polyethylene double sheath
 (Outside diameter 2.8mm, wick wire 0.3mm x 7)
 Sensor line length : 500m/ circuit or less
 Detection division length : 50m or 100m or less is assumed to be a standard.
 【An individual detection division and the number of circuits are suited to the fence and ambient conditions and decided.】
 Sensor installation span : 20m (installation of one every 20m)
 Detection condition
 ·Operation load : 2.5kg or more (vertical direction), 11kg or more (horizontal direction)
 ·Operating distance : 110mm or more (vertical direction), When expanding by 6.5mm or more
 ·Cutting is detected : The cutting of the sensor wire should be able to be detected.
 Operation sensitivity : The adjustment must be possible.
 Alarm output : Dry contact relay output (1b)
 The sensor automatic operation return : The sensor after it warns must return automatically. (However, the destruction of the sensor and cutting the sensor wire are excluded.)
 Sensor operation display : (Even if the sensor returns automatically, the display remains until the manual operation returns.)
 Power-supply voltage : 12~24V DC
 Accessory : Holder (support of sensor wire), adjuster (The sensor wire from the sensor is fixed, and the tension is adjusted.)

Others : Give the per-device the salt damage measures enough.

c) Tension sensor (encoder pulse count type)

i) Main body of sensor

Method : Encoder wire detection pulse count type
Sensor line : SUS304 and polyethylene double sheath
(Outside diameter 2.8mm, wick wire 0.3mm x 7)
Sensor line length : 100m/circuit or less
The detection division length : 50m or 100m or less is assumed to be a standard.
【An individual detection division and the number of circuits are suited to the fence and ambient conditions and decided.】
Sensor installation : 1/circuit
Detection condition
· Operation load : 0.5-10kg (vertical direction), maximum load 70kg
· Operating distance : 100mm or less
· Cutting is detected : The cutting of the sensor wire should be able to be detected.
(However, the case where the sensor wire is fixed is excluded.)
Sensor automatic operation return : Sensor automatic operation return after it warns (However, the destruction of the sensor and cutting the sensor wire are excluded.)
The sensor operation display : None
Accessory : Holder (support of sensor wire), collaboration box (The sensor wire from the sensor is fixed, and the tension is adjusted.)
Others : Give the per-device the salt damage measures enough.

ii) Tension sensor controller

Number of input circuits : The number of circuits is selected if necessary.
Set sensitivity : The adjustment must be possible.
Alarm output : Dry contact relay output (1b) x n
Power-supply voltage : 12~24V DC

d) Tension sensor control panel

i) Function

The supply of AC power from the outside is supplied and a necessary voltage and current for the receiving equipment are supplied. When the encoder pulse count type tension sensor is used, the controller is stored. Moreover, the signal relay and the power supply of the infrared sensor and the key switch that is are done to be near.

ii) Specification and standard

Structure	: Outdoor, Waterproof, wall-hanging type, with a door key
Detection of door open	: With door switch
Number of the controller	: It is necessary number to one fence sensor division.
Power supply unit	: AC200/220V /DC24V
Power-supply voltage	: AC200/220V, 1φ, 2W
Panel material	: Stainless steel
Painting	: Salt resistant painting
Protection against lightning	: It equips it with arrestor and the lightning resistance transformer.
The salt damage measures	: Give the per-device the salt damage measures enough.

(3) Infrared sensor for boundary (land)

1) Function

It is assumed to the person the equipment to confirm the presence of the intrusion in the boundary part.

Getting over with on the wall in the boundary part and a superior roof is chiefly detected.

2) Specification and standard

Detection system	: Near-infrared beam interruption system (4 beams simultaneous interruption)
Infrared beam	: Double modulation pulsed beams by LED
Protection distance	: Outdoor 200m
Response time	: 50ms to 700ms variable
Alarm output	: Dry contact relay output (1b) Reset : Interruption time + off-delay (approx. 1.5 sec)
Environmental output	: Dry contact relay output (1b) Contact operation : Output when weather condition gets worse
Tamper output	: Dry contact relay output (1b) Contact operation : Output when receiver cover is detached
Alarm LED	: Red LED (receiver) lights when an alarm is initiated
Sensitivity attenuation LED	: Red LED (receiver) lights when beam reception is attenuated
Beam adjustment	: Horizontal : $\pm 90^\circ$, vertical : $\pm 10^\circ$
Power supply voltage	: 12V to 30V DC
Attached mechanism	: Housing case and space heater
Pole	: 2.5m The installation of the back match of 2 pieces must be possible in the upper part of Pole.

Others : Give the per-device the salt damage measures enough.

2. Gate sensor

(1) Infrared sensor for gate

1) Function

It is assumed to the vehicle and the person the equipment to confirm the presence of the intrusion at the port gate.

2) Specification and standard

Detection system	: Near-infrared beam interruption system (4 beams simultaneous interruption)
Infrared beam	: Double modulation pulsed beams by LED
Protection distance	: Outdoor 50m
Response time	: 50ms to 700ms variable
Alarm output	: Dry contact relay output (1b) Reset : Interruption time + off-delay (approx. 1.5 sec)
Environmental output	: Dry contact relay output (1b) Contact operation : Output when weather condition gets worse
Tamper output	: Dry contact relay output (1b) Contact operation : Output when receiver cover is detached
Alarm LED	: Red LED (receiver) lights when an alarm is initiated
Sensitivity attenuation LED	: Red LED (receiver) lights when beam reception is attenuated
Beam adjustment	: Horizontal : $\pm 90^\circ$, vertical : $\pm 10^\circ$
Power supply voltage	: 12V to 30V DC
Attached mechanism	: Housing case and space heater
Others	: Give the per-device the salt damage measures enough.

(2) Key switch panel for gate sensor

1) Function

When the infrared sensor is used, "Use - the nonuse" of the sensor alarm signal when the gate opens and shuts is set. The signal is transmitted by way of the sensor control panel. The key switch panel is set up in the vicinity of the gate, and when the gate opens and shuts on the site, operated by maintenance personnel. Assume the system from which the surveillance room can do a similar operation.

2) Specification and standard

Structure	: Outdoor, Waterproof, wall-hanging type, with a door key
Detection of door open	: With door switch
Installation features	: 1/gate
Installation apparatus in panel	(To understand neither the operation nor the setting from the

	outside, install it in the door.)
·Key switch	: 1 piece It is recommended that the key to a gate concerned, the door key to the key switch panel, and this three key switches be made the same thing.
·Display light	: 1 piece "Use - No use" of the infrared sensor is displayed.
Panel material	: Stainless steel
Painting	: Salt resistant painting
Others	: Give the per-device the salt damage measures enough.

(3) Cutting detection sensor

1) Function

It is a method to detect cutting this line when the line is woven to all aspects of the fence (net part) for the breakthrough intrusion detection from the fence and the gate, and the intruder breaks through the fence. The sensor line is horizontally woven to the net part of the fence by the pitch of 220mm or less.

2) Specification and standard

a) Sensor wire

Method	: Cutting detection method(loop energizing method)
Sensor wire	: SUS304 and polyethylene double sheath (Outside diameter 2.8mm, wick wire 0.3mm x 7)
Sensor wire length	: 500m/circuit or less
Detection condition	: The cutting of the sensor wire is detected.
·Cutting load	: 80kg(sensor line) As for the cutting load of the sensor wire, small one is desirable.
Power-supply voltage	: 12/24V DC
Accessory	: Connection box
Others	: Give the per-device the salt damage measures enough.

3. Intrusion detection sensor signal transmission converter panel

1) Function

The signal of each area of the intrusion detection sensor is consolidated and the transmission between the surveillance control panel is done.

This panel becomes unnecessary as follows.

a) With the transmission device with an individual intrusion detection sensor control panel.

- b) When wiring for the cable without transmitting converting the signal.
- c) The device of the camera signal transmission converter panel is used combined by camera signal transmission converter panel's passing.

2) Specification and standard

a) Transmission converter

- Input/output signal : RS-232C, RS-485, and RS-422, etc.
- I/O connector : BNC
- Transmission method : Optical, current or voltage method

b) Power supply unit : AC200/220V/DC24V

c) Panel case

- Structure : Outdoor, Waterproof, wall-hanging type, shading board installation, with a door key
- Detection of door open : With door switch
- Power-supply voltage : AC200/220V, 1φ, 2W
- Panel material : Stainless steel
- Painting : Salt resistant painting
- Protection against lightning : It equips it with arrestor and the lightning resistance transformer.
- Salt damage measures : Give the per-device the salt damage measures enough.

4. Intrusion surveillance device

1) Function

When information on the key switch for Alarm information and the gate from the intrusion detection sensor is collected, and Alarm is detected, the information is displayed on the alarm display panel. Moreover, sensor Alarm information can be offered to the image record device, and information for making the index of the image data be output.

2) Specification and standard

a) Intrusion monitoring part

If this function is added by using PLC (Programmable Logic Controller) in the logic part of the control of the surveillance control panel (CCTV control panel) combined, this PLC becomes unnecessary.

Programmable logic controller (PLC)

- Program preservation : Nonvolatile memory

·Restart	: Auto restart
Network interface	
·Protocol	: TCP/IP
·Interface	: 100Base-TX/10Base-T (RJ-45)
I/O module	: Dry contact relay input, dry contact relay output, Current (DC4-20mA), voltage analog input if necessary
I/O number	: 【A necessary point is decided by a detailed design】
Power-supply voltage	: AC200/220V、1φ、2W
The installation	: The DIN rail installation must be possible.

b) Alarm display panel

If sensor information is displayed on the surveillance operation terminal, this panel becomes unnecessary.

However, sensor Alarm information need not be displayed in the place without the operation terminal of a guard place etc. left from the surveillance room.

Structure	: Indoor, dustproof, wall-hanging type, with a door key
Installation features	: -
Surface of the panel installation apparatus	
·alarm display lamp	: It installs it on a set display lamp or a graphic panel the display lamp.
·Alarm buzzer	: 1 piece
·Push button switch	: 2 pieces (lamp check, buzzer stop)
Panel material	: Stainless steel
Power-supply voltage	: AC200/220V、1φ、2W
Painting	: Melamine resin printing painting (Half gloss is erased) or corresponding
Others	: Give the per-device the salt damage measures enough.

D. Monitor and control

1. surveillance control panel 1 (CCTV control panel)

1) Function

Surveillance image from surveillance camera is displayed selecting, and control of camera and image of surveillance camera are switched and displayed. Moreover, the camera image is digitalized.

2) Camera control specification

Control item:

- Camera power : On/off
- Wiper : On/off
- Camera pan/Tilt : Upper/lower, right/left
- Lens : Zoom/focus
- Preset : Selection function

3) Specification and standard

a) Signal transmission converter

Select a necessary function and the equipment.

- Image signal : PAL or NTSC
- Audio signal : PWM or equal
- Control signal input : RS-232C or equal
- Control signal output : RS-485 control or coaxial, multiple control

Image / control signal optical converter

: Conversion into optical signal, it restores it

Voice signal optical converter: Conversion into optical signal, it restores it

RS232C/485 conversions : The surveillance camera control signal is converted between RS232C and RS485.

RS232C/IP conversion : The surveillance camera control signal is converted between RS232C and IP.

· Network interface : 100Base-TX/10Base-T (RJ-45)

· Serial interface : RS-232C, RS-485

· Serial communications speed : 9,600bps

b) Character generator

The camera number etc. of which it takes a picture to the camera image are inserted.

If the character generation function is provided in the camera, and it meets ..becoming it.. specification for, this equipment is unnecessary.

Moreover, if an epenthesis of the camera number etc. of which it took a picture when processing it digitally can be done, this equipment is unnecessary when only the digitalized image signal is treated.

Display letter types : Alphabet, figure, and sign

Total characters on screen : 14 characters

Number of image signal I/O : 4 or 8

c) Matrix switcher

Can select be a necessary image from two or more images.

This equipment is unnecessary if there is no processing of the switch of the treatment only of the digitalized image signal, and the two or more, analog image signal, and the selection and the displays in the surveillance monitor, etc.

Image signal I/O : 1.0Vp-p(VBS)

Number of input : 8 or 16

Number of outputs : 8 or 16

d) Image distribution machine

Can output two or more input images at the same time.

If it is not necessary to distribute the analog image signal to the plural at the same time, this equipment is unnecessary.

e) Camera controller

It controls the camera, and the image switch is controlled.

If this function is included in Matoricssitcha, this equipment is unnecessary when Matoricssitcha is used.

Moreover, the controller only for the camera control is used for. Or, necessary function processing is done by using general-purpose PLC.

Control input : Sensor input, LAN control input

Control output : Matrix switcher, camera control part

Control I/O signal : LAN, RS-232C, and contact, etc.

f) IP encoder

The digital ..analog image signal.. compression processing is done.

When the analog image signal is not digitalized, this equipment is unnecessary.
Moreover, a digital recorder has this function and when the analog image signal is not digitalized, this equipment is unnecessary in another even when a digital recorder is used.

Image input : PAL or NTSC, 1ch
Voice input/output : It doesn't use it.
Resolution : 640×480 dots
Image compression method : MPEG-4 compression method (simultaneous delivery method)
Audio compression method : It doesn't use it.
Processing speed : 30fps (maximum)
Camera control method : It doesn't use it.
Network interface : 100Base-TX/10Base-T (RJ-45)
Necessary transmission band : 2Mbps (at 640×480 30fps)
Point of contact I/O : It doesn't use it.
Protocol : TCP/IP, multicast

g) IP decoder

The image signal compressed digitally is restored to the analog signal.

When the digital compression image signal is not used, this equipment is unnecessary.
Moreover, a digital recorder has this function and when the digital compression image signal is not restored to the analog signal, this equipment is unnecessary in another even when a digital recorder is used.
Softdecoding by the server etc. of the display monitor who displays the image without using this equipment is enabled.

Image output : PAL or NTSC, 1ch
Voice input/output : It doesn't use it.
Resolution : 640×480 dots
Image compression method : MPEG-4 compression method
Audio compression method : It doesn't use it.
Processing speed : 30fps (maximum)
Camera control method : It doesn't use it.
Network interface : 100Base-TX/10Base-T (RJ-45)
Necessary transmission band : 2Mbps (at 640×480 30fps)

Contact I/O : It doesn't use it.
Protocol : TCP/IP, multicast

h) L2-SW

Network interface

It is unnecessary when there are neither digital processing nor a network communication.

Network interface : 100Base-TX/10Base-T (RJ-45)
Number of ports : [It is assumed more than a necessary number of connected lines]
Network management : SNMP
Protocol : IGMP Snooping, QoS

i) Power supply part

Power supply input : 1φ2W AC200/220V
Power supply output : Power-supply voltage that is necessary in this device
Accessory : Lightning resistance transformer, breaker, and service outlet

j) Panel case

Function : It is assumed the structure that the door is installed forward and the maintenance check is easy.
Structure : Indoor, dustproof, independence type, with a door key
Detection of door open : With door switch
Panel material : Steel plate
Painting : Melamine resin printing painting (Half gloss is erased) or corresponding
Others : The panel air conditioner is set up if necessary.

2. Monitor control panel 2

(1) Surveillance control server

1) Function

Information from surveillance camera and intrusion detection sensor is managed, and controlled

2) Accumulation control and retrieval operation function of image

- Function that importance degree of accumulation image can be set and be managed
- Image retrieval function by index
- Retrieval function of time of camera image
- Image retrieval function by space that uses map and image chart of wharf

3) Hard specification and standard

a) Main body of server

Type	: Rack mount or mini tower type
CPU	: Intel Xeon 3.60GHz or more
Memory	: 1GB or more
HDD	: 146GB or more
FDD drive	: 3.5-inch 1.44MB (two modes) × 1 drive
CD drive	: 16 times speed, DVD+RW/+R × 1 drive
Network interface	: 100Base-TX/10Base-T
Power-supply voltage	: AC200/220V 50/60Hz

b) Display

Size	: 15-inch color liquid crystal monitor device
Resolution	: More than 1024×768 dots

(2) Time server

It is an equipment because it synchronizes accurately according to the client software with which OS has been equipped normally as for connected PC, the workstation, and the clock of the server.

Type	: FM radio time signal correction method
Time of correction accuracy	: ±100m/s
Network interface	: 10Base-T or 100Base-TX
Antenna	: Special indoor antenna

(3) Image record device(with online database retrieval function)

1) Function

So that image from surveillance camera is connected with surveillance control server and it accumulates

Moreover, it uses it also for the long preservation library of the image.

2) Image record function and retrieval function

- The camera image can be in real time recorded by digital.
- An online arbitrary image from the surveillance control server can be retrieved.

3) Specification and standard

a) Recording management server

Image record specification :

- Format : Motion JPEG, MPEG-4
- Frame rate : 4 fps or more
- Resolution : 640×480 dots

Hard specification

- Type : Rack mount type
- CPU : Intel Xeon 3.40GHz or more
- Memory : 1GB or more
- HDD : 146GB or more
- FDD drive : 3.5-inch 1.44MB (two modes) × 1 drive
- CD drive : 24 times speed, CD-RW/DVD-ROM ×1 drive
- Network interface : 100Base-TX/10Base-T
- Power-supply voltage : AC200/220V 50/60Hz

b) Storage device

Image record time : Have the capacity of the disk at a necessary period in which the image can record.

【 When the image is recorded, each individual wharf is decided 】

- Type : Rack mount type
- Capacity of disk : Possible equipped with 146GB x 14
- Composition of making to tedium : SCSI RAID5
- Rotational speed : 10,000rpm
- Voltage : AC200/220V 50/60Hz

(4) Image record device(online database retrieval function none)

1) Function

Image from surveillance camera is accumulated directly

2) Specification and standard

Image record function	: The camera image should be able to be recorded in real time.
Image record time	: 【Each individual wharf is decided】
Image record specification	:
- Format	: motion JPEG, MPEG-4
- Frame rate	: 4 fps or more
- Resolution	: 640×480 dots
The image quality setting	: By about ten (10) stages
Capacity of disk	: 250GB or more
Network interface	: 100Base-TX/10Base-X
Protocol	: TCP/IP
Voltage	: AC100V or AC200/220V±10% 50/60Hz

(5) Power supply part

It is possible to use it combinedly with the power supply part of surveillance control panel 1(CCTV control panel).

Power supply input	: 1φ2W AC200/220V
Power supply output	: Power-supply voltage that is necessary in this device
Accessory	: Lightning resistance transformer, breaker, and service outlet

j) Panel case

Function	: It is assumed the structure that the door is installed forward and the maintenance check is easy.
Structure	: Indoor, dustproof, independence type, with a door key
Detection of door open	: With door switch
Panel material	: Steel plate
Painting	: Melamine resin printing painting (Half gloss is erased) or corresponding
Others	: The panel air conditioner is set up if necessary.

3. surveillance and operation terminals

(1) PC operation table

1) Function

So that information from surveillance camera and infrared sensor is displayed, and control is operated. Moreover, it is the one to call the image recorded in the image record device when it is necessary and for the function to operate to have.

2) Control function

The table shows the required control function.

Control function list (reference)

Camera operation function	The surveillance camera should be able to be operated. (Facilities outside the wharf are included.) It is enabled that it is an operation of the following equipment and functions. · Camera power supply · Wiper · Camera platform · Lens · Preset function
	The camera individually observed should be able to be selected.
	The zoom in, the zoom out, and the turn operation should be able to be done.
	It automatically turns to the registered preset position when the automatic turn beginning is directed. An automatic turn must operate continuously until the turn stop is selected.
Display function	The image of the specified surveillance camera should be able to be displayed in real time.
	The image of the specified surveillance camera should be able to be displayed and to display two or more camera images to the display monitor switching.
	Gate sensor use information from the key switch set up by the gate Should be able it to acquire, and to display the state of the gate sensor by the color.
	The sensor should be able to be displayed the state and to set it.
	The simplified wharf arrangement chart is displayed, and the camera position, the sensor division, and the gate should be able to display it.
	Registration and the order of the display of the camera displayed at the camera image cycle should be able to be registered.
	The interval displayed at the camera image cycle should be able to be set.
Preset function	The surveillance condition of the specified camera (direction and magnification, etc.) should be able to be set.
Image accumulation and reproduction function	The reproduction should be able to be displayed by the retrieval function the accumulating image.
Hard copy function	The hard copy of the screen should be able to be output to the printer.
Sensor detection function	Display the camera image of the object district to the display monitor automatically when the sensor detects abnormality. At same time, display the wharf arrangement chart and display the division that detects abnormality emphatically.
	Display the wharf arrangement chart and display the division that detects abnormality emphatically when the sensor abnormally detects two places or more.

3) Specification and standard

a) Operation terminal PC

Type

: Mini tower type

CPU	: 2xCPU - Intel Xeon 3.60GHz or more
Memory	: 1GB or more
HDD	: 146GB or more
FDD drive	: 3.5-inch 1.44MB (two modes) × 1 drive
CD drive	: 16 times speed, DVD+RW/+R ×1 drive
Network interface	: 100Base-TX/10Base-T
Power-supply voltage	: AC200/220V 50/60Hz
Accessory	: Keyboard and mouse

b) Display part

Amount	: 2 (for 1x operation and for 1x camera image monitor)
Method	: TFT liquid crystal display
Size	: 20-inches corresponding
Resolution	: More than 1600×1200 dots
The structure	: It leaves untouched in operating desk-top, and one of can the angle adjustment in the display part.

c) Main body of table

Structure	: OA desk type Structure that shelf can be installed under desk and operation terminal PC main body be stored
Voltage	: AC200/220V±10% 50/60Hz

d) Printer

Size of form	: A4 and A3
--------------	-------------

(2) Key switch operation bord

1) Function

Control of surveillance camera is operated

2) Control item

a) Camera control

• Camera selection	: 「No.1」～「No. n.」
• Camera power supply	: "On", "Off"
• Wiper	: "On", "Off"
• Camera pan/Tilt	: " Upper", " Lower " and "Right", "Left"
• Lens zoom/focus	: " Tel", "Wide" and "Long ", "Short"
• Preset function	: 「No.1」～「No. n.」 and "Setting"

b) Surveillance monitor display

- Surveillance monitor selection : 「No.1」～「No. n.」
- Display method selection : "All screens" and "Division"

3) Specification and standard

- Method : Push-button operation method
- Structure : The push button switch of each function is arranged on the panel.
- Shape : Plane type

(3) Surveillance monitor

1) Function

Surveillance image from surveillance camera is displayed monitoring

2) Specification and standard

a) Display monitor

- Method : TFT liquid crystal display
- Image signal input : 1.0Vp-p(VBS)×1
- Size : 20-inch corresponding
- Resolution : More than 1600×1200 dots
- Power-supply voltage : AC100V or AC200/220V±10% 50/60Hz
- Accessory : Ceiling hanging metal fittings or wall installation metal fittings

b) Multiplexer

Two or more screen separation ..image input.. display outputs are done.

If the screen separation display output is done with no screen separation display and other equipment, this equipment is unnecessary.

- Image input : 4 or more"
- Image output : One point
- Number of image displays: One screen and screen and division into four screen of division into nine
- Character representation : Alphanumeric character eight characters or more
- I/O connector : BNC connector

c) Surveillance monitor panel

The surveillance monitor is stored. Concentrated arrangement is done to the surveillance

monitor surface of the panel a lot of monitors.

When the surveillance monitor is set up by ① ceiling hanging method, ② wall hanging method, and ③ desktop method, this panel is unnecessary.

Structure	: The indoor, independence type
Panel material	Steel plate
Power-supply voltage	: AC200/220V±10% 50/60Hz
Painting	: Melamine resin printing painting (Half gloss is erased) or corresponding
Others	: With ventilation fan

E. Hand luggage inspection device

1. X-ray inspection device

(1) X-ray inspection device (medium)

1) Function

It uses for traveler's depositing baggage inspection. To do an inspection inboard besides arms and the explosive adequate though it brings in and is prohibited, it sets it up.

2) Specification and standard

a) Main body of X-ray inspection device

Structure	: Indoor, steel plate, independence type, and roller casters addition
Tunnel size	: 650mm x 800mm or more
Conveyer height	: 230mm~350mm
Conveyer maximum load	: 100kg or more (overall capitation cloth)
Conveyer speed	: 10m/minute or more (A reversible running must be possible.)
Conveyer control	: It is necessary to be able forward / reversed / stop with the monitor desk.
Running time	: 24hr is continuous.
Radiation area of X rays	: The entire inspection thing must reflect.
Resolution (cupper wire detection ability)	: 36AWG (0.13mmΦ) or more
Penetration (steel plate)	: 25mm or more The adjustment of the penetrating power must be possible.
Image zoom function	: 4 times or more
Image contrast	: 22 gray level or more
Image processing function	: Have the material identification function and the outline emphasis function. (The explosive, the drug, and other material division should be able to be facilitated. Have the operator assistance function of the image to emphasize the outline.) Provide the previous X-ray image call function. The image accumulation function (hard disk of 40GB or more) with possession Equip with the CD R/W driver.
Emergency stop switch	: It puts it on the place where the main body can be operated at once. The emergency stop function is put on the monitor desk.
Self protection function	: Have the protection function from the over voltage, over current and /or over heating.

Radiation leakage	: 5 μ Sv/h (0.5mR/h) or less
Film safe.	: Guarantee ISO1600. There must not be danger of radiation exposure for the operator, the traveler, and the freight.
Power supply	: Single phase 200/220V \pm 10% and 50/60Hz
Environmental condition	: Ambient temperature 0-40 $^{\circ}$ C, Humidity 10-90%
b) Monitor desk	(It is separated, and make it to an independent monitor desk with the main body.)
Size	: The monitor desk is assumed to be an enough size to put the keyboard for monitor (CRT) of two and the operation. The angle adjustment of the drip must be possible of height and the back of the seat of the chair.
Monitor	: Full-color CRT x 2 expression in 24 bits or more of 17 inches (CRT should be able to be used by mending in Indonesia.)
c) Extension conveyer	
Entrance side	: The total length is assumed to be 1.5m or more including the conveyer of the main body from the tunnel entrance.
Exit side	: The total length is assumed to be 2.0m or more including the conveyer of the main body from the tunnel exit.
Structure, etc.	: Height, width, and shape are made the same thing as the conveyer of the main body. The height of the leg of the extension conveyer should be able to be adjusted. The roller is made a thing covered with the resin or rubber so as not to damage the inspection thing.
d) Power-supply unit	: Provide with uninterrupt power supply (UPS). It always has the function of the voltage stabilizer as an inverter feeding power method. The battery backup time when blacking out is assumed to be ten minutes.
e) Others	
Standards of manufacturing	: standard (CFR) of the United States and relating global standard for the influence and the safety to the human body.
Test piece	: Supply a standard test piece.

(2) X-ray inspection device (small size)

1) Function

It uses for the traveler's carrying luggage inspection. To do an inspection inboard besides arms and the explosive adequate though it brings in and is prohibited, it sets it up.

2) Specification and standard

a) Main body of X-ray inspection device

Structure	: Indoor, steel plate, independence type, and roller casters addition
Tunnel size	: 600mm x 400mm or more
Conveyer height	: 600mm~800mm
Conveyer maximum load	: 100kg or more (overall capitation cloth)
Conveyer speed	: 10m/minute or more (A reversible running must be possible.)
Conveyer control	: It is necessary to be able forward / reversed / stop with the monitor desk.
Running time	: 24hr is continuous.
Radiation area of X rays	: The entire inspection thing must reflect.
Resolution (cupper wire detection ability)	: 36AWG (0.13mmΦ) or more
Penetration (steel plate)	: 25mm or more The adjustment of the penetrating power must be possible.
Image zoom function	: 4 times or more
Image contrast	: 22 gray level or more
Image processing function	: Have the material identification function and the outline emphasis function. (The explosive, the drug, and other material division should be able to be facilitated. Have the operator assistance function of the image image to emphasize the outline.) Provide the previous X-ray image call function. The image accumulation function (hard disk of 40GB or more) with possession Equip with the CD R/W driver.
Emergency stop switch	: It puts it on the place where the main body can be operated at once. The emergency stop function is put on the monitor desk.
Self protection function	: Have the protection function from the over voltage, over current and /or over heating.
Radiation leakage	: 5μSv/h (0.5mR/h) or less
Film safe.	: Guarantee ISO1600.

	There must not be danger of radiation exposure for the operator, the traveler, and the freight.
Power supply	: Single phase 200/220V±10% and 50/60Hz
Environmental condition	: Ambient temperature 0-40°C, Humidity 10-90%
b) Monitor desk	(It is separated, and make it to an independent monitor desk with the main body.)
Size	: The monitor desk is assumed to be an enough size to put the keyboard for monitor (CRT) of two and the operation. The angle adjustment of the drip must be possible of height and the back of the seat of the chair.
Monitor	: Full-color CRT x 2 expression in 24 bits or more of 17 inches (CRT should be able to be used by mending in Indonesia.)
c) Extension conveyer	
Entrance side	: The total length is assumed to be 1.5m or more including the conveyer of the main body from the tunnel entrance.
Exit side	: The total length is assumed to be 2.0m or more including the conveyer of the main body from the tunnel exit.
Structure, etc.	: Height, width, and shape are made the same thing as the conveyer of the main body. The height of the leg of the extension conveyer should be able to be adjusted. The roller is made a thing covered with the resin or rubber so as not to damage the inspection thing.
d) Power-supply unit	: Provide with uninterruptible power supply (UPS). It always has the function of the voltage stabilizer as an inverter feeding power method. The battery backup time when blacking out is assumed to be ten minutes.
e) Others	
Standards of manufacturing	: standard (CFR) of the United States and relating global standard for the influence and the safety to the human body.
Test piece	: Supply a standard test piece.

2. Metal detector

(1) Walk-through metal detector

1) Function

It uses for the traveler's possession goods inspection. To do an inspection arms and inboard additionally adequate though it brings in and is prohibited, it sets it up.

2) Specification and standard

Structure	: It is necessary to be able to fix to the gate type independence and the floor. (It is assumed the standard or the waterproof construction by the system requirements.)
Gate size	: 700mmW x2000mmH or more
Zone composition	: Multi (8 zones or more)
Object of detection	: Ferrous and nonferrous metals
Sensitivity	: The threat level adjustment must be possible. Those who operate it should be able to set sensitivity. Conform to 3- Gun-Test standard of FAA. The electromagnetic field as possible in a walk-through metal detector must be as constant.
Alarm display	: The sight display and the signal display proportional to the size of a metallic thing should be able to be done.
Alarm sound	: Inform me because of the alarm sound. (The volume and the tone should be able to be adjusted.)
Alarm output	: Dry contact relay output
Interface	: RS-232C
Magnetic intensity	: According to standard of NILECJ-0601
Safety	: Do not give to the person and the pregnant woman who acquired the pacer or other life-support systems and do not give the detrimental effect to electricity, the electron device, and the magnetic storage media, etc. to say nothing of a harmless thing.
Removal of interference	: There must be a high defense for an electric, mechanical trouble.
Power-supply voltage	: Single phase 220V±10% and 50/60Hz. (Shall be backed-up by emergency battery.)
Environmental condition	: Ambient temperature 0-40°C, Humidity 10-90%
Others	
Other standard	: According to the latest international standard of EMC/EMI, IEC, and IATA in addition to the above-mentioned specification Suit the international safety standard.

Test piece : Supply the test piece to set the best detection sensitivity.

(2) Handheld metal detector

1) Function

It uses it for the traveler's possession goods inspection. To do an inspection arms and inboard additionally adequate though it brings in and is prohibited, it equips it.

2) Specification and standard

Weight : 400g or less

Object of detection : Ferrous and nonferrous metals

Sensitivity : The adjustment must be possible.

Detection performance (highest sensitivity)

: Next, the Cab material of the shown size should be able to be detected.

Select the model of the best detection sensitivity from use conditions by the model so that there is an opening in the detection sensitivity as shown in Table 1 and Table 2.

(The reference value of Table 1 and Table 2 made of the manufacturer separate.)

Table 1 detection performance(A company)

Cab material	Detection distance
Revolver 22cal of mini-	12cm
Pistol 25cal	14cm
Magnum cartridge. 357	7cm
Cable 2x1.5mm ² (2x14AWG)	3cm
Copper pipe 12mm diameter	8cm
Ball of 10mm diameter of carbon steel	5cm

Table 2 detection performance(B company)

Cab material	Detection distance
Pistol: Glock 17	40Cm
M4 Magnum	38Cm
P7 Heckler & Koch	35Cm
Bullet: Caliber 9mm bullet	17Cm
357 Magnum	17Cm
38 Special	16Cm
Coin: 10φ aluminum disc	11Cm

Alarm	: It informs because of the sight and the alarm sound. (The volume and the tone should be able to be adjusted.)
Magnetic intensity	: According to standard of NILECJ-0602
Safety	: Do not give to the person and the pregnant woman who acquired the pacer or other life-support systems and do not give the detrimental effect to electricity, the electron device, and the magnetic storage media, etc. to say nothing of a harmless thing.
Power supply	: It is necessary to be able to use it with a dry battery and rechargeable.
Environmental condition	: Ambient temperature: 0-40°C, Humidity 10-90%
Others	
Other standards	: According to the latest international standard of EMC/EMI, IEC, and IATA in addition to the above-mentioned specification Suit the international safety standard.

F. Public address system

(1) Horn speaker

1) Function

It is an emergency contact by the voice, and the one to the person engaged in work in port set up to broadcast at the regular time.

2) Specification and standard

a) 50W reflex horn speaker

Ratings input	: 50W
Ratings impedance	: 200Ω
Output sound pressure level	: 110dB (1W, 1m)
Frequency characteristic	: 180~7,700Hz
Wind pressure	: Maximum wind speed about 60m/s at moment (15m in height from the ground)
Salt damage measures	: Salt resisting coating

b) 5W horn speaker

Ratings input	: 15W
Ratings impedance	: 670Ω
Output sound pressure level	: 108dB (1W, 1m)
Frequency characteristic	: 250~7,700Hz
Salt damage measures	: Salt resisting coating

c) Box speaker (indoor use)

Ratings input	: 5W
Ratings impedance	: 2kΩ
Output sound pressure level	: 94dB (1W, 1m)
Frequency characteristic	: 150~12,000Hz
Attached mechanism	: Adjustment unit of volume

(2) Broadcasting panel

1) Function

The power amplifier is set up on the speaker side, the power amplifier and transmitting unit are stored, and then the audio signal is amplified, and it outputs to the speaker.

This panel is unnecessary when doing concentrated installation of the power amplifier in the cabinet rack type public address system.

2) Specification and standard

Structure	: Outdoor, Waterproof, wall-hanging type, shading board installation, with a door key
Detection of door open	: With door switch
Installation features	: Near speaker
Installation apparatus in panel	
·Power amplifier	: 【The number and capacity are decided by the specification of the connected speaker】
·Power supply unit	: AC100V or AC200/220V±10% 50/60Hz
Panel material	: Stainless steel
Painting	: Salt resistant painting
Others	: Give the per-device the salt damage measures enough.

(3) Cabinet rack type public address system

1) Function

It is the one that work is set up in port to broadcast the emergency contact by the voice and the regular time broadcasting, etc. from the station to the employed person in port.

2) Specification and standard

a) Preamp

Input	mike input	: Two system -2/-62dB 600Ω equilibrium horn Jack
	Line input	: Two system -2dB 600Ω equilibrium horn Jack
	Mike input	: No two system -2/-22dB 600Ω equilibrium horn Jack
	Line input	: No two system -2dB 600Ω equilibrium horn Jack
Output	line output	: One system and no 0dB 600Ω equilibrium all input
	Line output	: One system and no 0dB 600Ω equilibrium all input
	Recording output	: No -10dB 5kΩ equilibrium
Frequency characteristic		: Within 50-15000Hz ±3dB
Rate of distortion		: 1% or less

b) Digital announce machine

i) Function

It is the one to reproduce the voice registered beforehand arbitrarily.

ii) Specification

Number of reproduction programs	: 8 programs or more
Urgent sentence reproduction	: 1 sentence or more
Control input	: Dry contact relay input

c) Network audio adaptor

i) Function

It is a voice-data communication equipment set up to transmit the voice from the remote place to the public address system of the port equipment through the communication network. One is set up at the remote place and each public address system. The line band should be able to be selected if necessary.

ii) Specification and standard

Voice input	: 1 circuit
Voice output	: 1 circuit
Frequency characteristic	: 50-14,000Hz (sampling frequency 32KHz time)
Distortion rate	: 0.3% or less (1KHz and sampling frequency 32KHz time)
Control input	: 8 circuits, dry contact relay input
Control output	: 8 circuits, open collector outputs
Network interface	: 100Base-TX/10Base-T automatic operation change
Network protocol	: TCP/IP、UDP、HTTP、RTP
Voice packet transmission method	: Unicast (4 maximum, simultaneous places) Multicast (64 maximum, simultaneous places)

d) Microphone mixer

i) Function

It is the one to input, to amplify the signal of the microphone, and to output the line.

ii) Specification and standard

Mike input	: 6 line -62dB 600Ω equilibrium horn Jack
Line output	: 1 line 0dB 600Ω equilibrium horn Jack
Recording output	: 1 line 0dB 1KΩ equilibrium pin Jack

e) Speaker line selector

The speaker output control is done to ten individual lines. Moreover, the speaker output is controlled all together.

f) Power amplifier

Declared power	: 15、30、60、120、240W
----------------	---------------------

Input	: 0dB equilibrium horn Jack
Output impedance	: High impedance 42Ω, 21Ω, and 10Ω corresponding
Frequency response	: 70-100-10000Hz(+1---2dB) 1kHz standard
Distortion rate	: Within 1%(Ratings are output the AC100V operation 1kHz.)

g) Monitor panel

The movement of the entire cabinet rack is observed with the monitor speaker and the meter.

Input	: Ten systems
Monitor speaker	: Adhering
Meter	: LED meter seven point corresponding

h) Power supply unit

Power supply input	: 1φ2W AC200/220V
Power supply output	: Power-supply voltage that is necessary in this device
Accessory	: Lightning resistance transformer, breaker, and service outlet

i) Cabinet rack

Rack standard	: Suit the EIA standard.
---------------	--------------------------

(4) Microphone

1) Function

The voice is input.

2) Specification and standard

Input	:
Output	: 0dBV 600Ω

(5) Monitor speaker

1) Function

It is the one to monitor the voice output situation. (A microphone and an integral thing of shape are acceptable.)

2) Specification and standard

Declared power	: 10W
Output sound pressure level	: 89dB(1W, 1m)
Frequency response	: 100-15,000Hz
Cable microphone input	: Road impedance once 600Ω
Line input	: 1 line -14dB 2kΩ equilibrium

G. Security communication equipment

(1) Telephone

1) Function

It is telecommunications equipment that sets up contacting by phone with a port office and a related organization to take it.

2) Specification and standard

- Dialing system : Dial-up network DP signal (10PPS/20PPS)
Push line PB signal
- Dial function : The speed dialing should be able to register.
- Power supply specification : For power supply unnecessary type or power failure measures

(2) Fax

1) Function

It is telecommunications equipment that sets up the report by the character and the figure with a port office and a related organization to take it.

2) Specification and standard

- Sending and receiving manuscript size
- Transmission : A4 or A3
 - Reception : A4 or A3
- Record paper size : (A4) 210mm × 297mm or A3
- Recording mode : Heat transcript record method or plain paper record method
- Use line : Household phone line
- Power supply specification : AC100V or AC200/220V 50/60Hz

H. Power supply equipment

1. Uninterrupted power supply system (UPS)

1) Function

Electricity can be supplied to the surveillance equipment and lighting equipment at the stop of a sudden electric supply.

2) Specification and standard

a) Main body of UPS

Ratings output capacity	: 5.2, 7.5, 10, 15, 20kVA 【Decide it by the installed capacity of the connected load】
Feeding power method	: Inverter feeding power method always
AC input	: Single phase 3 wire, AC200/220V±20%
Input frequency	: 50-60Hz±5%
AC output	: Single phase 3 wire, AC200/220V±3%
Output frequency	: 50-60Hz, It changes according to the input automatically.
Backup time	: 10 minutes or more
Overload of endurance	: 120% 60 second
Transition voltage fluctuation	: ±5% or less (The load changes suddenly 0-100%). (under power failure and recovery)
Distortion ratio of voltage wave form	: 4% or less (declared power and linear load)
Auto return function	: It changes to the by-pass in 300% excess at the load current peak automatically. It returns to the inverter feeding power automatically after the fixed time.
Battery type	: Small seal lead storage battery
Others	: With automatic shutdown function at power supply trouble And, with automatic shutdown instruction signal output function to load side Give the per-device the salt damage measures enough.

b) Input / Output panel for UPS

i) Function

Maintenance (maintenance check and component replacement, etc.) is enabled without the stop of the load equipment. Moreover, the function of power distribution is provided.

ii) Specification and standard

Structure : Indoor, dustproof, wall-hanging type, with a door key

Power supply	: AC200/220V, 50/60Hz
Main circuit	: 4 x MCCB (2 x input and 2 x load side) One load side is made a turning on mechanism with the key.
Divergence circuit	: n x MCCB 【The number of circuits is decided in individual facilities】
Panel material	: Steel plate
Painting	: Melamine resin printing painting (Half gloss is erased) or corresponding
Others	: Give the per-device the salt damage measures enough.

2. Emergency power generator

1) Function

Electricity can be supplied to surveillance equipment and a part of important lighting equipment before the limit of the supply of the no power failure power supply when a sudden electric supply is stopped.

2) Specification and standard

a) Generator for emergency

Generator

- Output : 25/30 KVA and 20/24 KW corresponding
- Rated Voltage : Single phase 3 wire, AC200/220 V
- Frequency : 50/60 Hz

Diesel engine

- Type : Series vertical type, water-cooled, 4 cycle corresponding
- Fuel to be used : Light oil

Fuel tank

- Running time : It is necessary to be able to drive continuously for one hour or more.

Characteristic

- Momentary speed variation : 5% or less corresponding (After completing the start)
- Voltage regulation : $\pm 2.5\%$ or less corresponding (After completing the start)
- Start time : 40 seconds or less

Others

- It starts automatically by the power failure signal from the automatic change unit, and it stops with power supply again automatically.
- Give the per-device the salt damage measures enough.

b) Automatic change unit

The function of the automatic change machine is shown below.

- The commercial power is blacked out, and TEL is detected again.
- The automatic start signal is sent to the generator for the emergency when the power failure is detected, and it is started automatically.
- When the output voltage of the generator for the emergency reaches a regulated value, and the start completion is done, the power supply circuit is switched from the commercial power to the generator for the emergency use.
- The automatic stop signal is sent to the generator for the emergency after it switches to the commercial power, and it is stopped again automatically after the power supply.

3. Transformer panel

1) Function

Electricity from the electric power company is received, and a necessary power supply for a predetermined wiring system is supplied.

A necessary power supply is supplied from the power supply panel of the port equipment, and or, it diverges, and a necessary power supply for a predetermined wiring system is supplied.

2) Specification and standard

Wiring system : 1 × system for UPS (**KVA)
1 × system for security lighting (**KVA)

4. Distribution panels

It supplies power in each equipment and/or facilities.

APPENDIX-VI RELEVANT SECURITY MEASURES

III-1 CONTAINER SEAL

1. The original definition of freight security was to carry cargo to a destination safely and in good condition. These days in addition to this, the prevention of any unauthorized use or misuse of cargo and vessels are included. The original seal was used to detect whether a door of a container was opened by breaking the seal. It was affixed to a door edge of a container. However it was easily broken because it was made of a thin and slender metal.

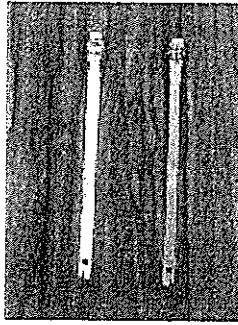


Figure III-1-1 Thin and Slender Seals

2. Many cases of theft by breaking a seal put more durable seals into place. Many kinds of seals came onto the market, which were called mechanical seals. ISO/PAS 17712 which provided definitions, types and requirements and testing of mechanical seals was released in October 2003. Use of a mechanical seal is becoming common. Now an electronic seal is proposed and being developed. Expanded use of electronic seals is expected in the years to come.

III-1-1 Mechanical Seal

3. Prior to ISO/PAS 17712, there was no comprehensive standard for mechanical seals. Therefore container owners and shippers were unsure on how to choose the most suitable seals for their containers and what strengths are needed for a seal. Since its publication in October 2003, ISO/PAS 17712 has played a fundamental role in improving security measures taken against terrorism, theft and smuggling.

4. Ten different types of mechanical seals are prescribed in ISO/PAS 17712; wire seals, padlock seals, strap seals, cable seals, bolt seals, cinch or pull-up seals, twist seals, scored seals, label seals and barrier seals.

Table III-1-1 Types and General Outline of Mechanical Seal

Type	General outline
Wire seals	a loop wire with seizing device
Padlock seals	a locking body with a bail
Strap seals	a loop metal or plastic strap with a locking mechanism
Cable seals	a cable and a locking mechanism
Bolt seals	a metal rod with a formed head and a separate locking mechanism
Cinch or pull-up seals	a thin strip of material with a locking mechanism
Twist seals	steel rod or heavy-gauge wire, which is inserted through the locking fixture and twisted
Scored seals	a metal strip which is scored perpendicular to the length of the strip
Label seals	a paper or plastic backing adhesive
Barrier seals	a significant barrier to container entry

Source: ISO/PAS 17712

5. Security and high security seals in mechanical seals are requested to have some strength and durability to prevent accidental breakage, early deterioration or undetectable tampering under normal usage. This performance gain contributes to a reduction in cargo theft and a more secure transportation chain from a shipper to a consignee. Mechanical seals also have to be able to be affixed easily and quickly, be easily identified by marks and numbers and be as difficult as possible to copy. Moreover, mechanical seals do not permit removal or undoing without breaking, or tampering without leaving readily apparent traces, and using more than one.

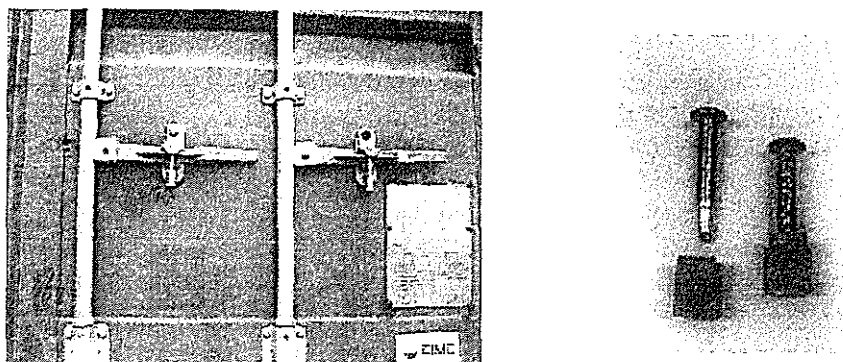


Figure III-1-2 Mechanical Seal (Security Seal)

6. It is said that the US Department of Homeland Security will introduce a new regulation which will require all containers arriving and departing ports in the United States to be affixed with a mechanical seal approved by Customs-Trade Partnership Against Terrorism and conforming to the ISO. Moreover, shippers/consignees, shipping companies, terminal operators, insurers and governments of leading countries have become more enthusiastic in the fight against cargo theft and smuggling. Therefore it is expected that mechanical seals will be widely used in container transportation.

7. Prices of mechanical seals are getting lower and the cheapest one is now under half a US dollar. This will also accelerate the spread of mechanical seals.

III-1-2 Electronic Seal

1) *Difference between Mechanical Seal and Electronic Seal*

8. A mechanical seal was used originally to confirm whether a container door was opened or not during transportation but recently a function which makes doors of a container difficult to open has been added. On the other hand, electronic seals can record histories of locking and unlocking, and can raise an alarm in case of opening in the wrong manner. However, a locking device must be attached to the electric seal, because an electronic seal itself does not have locking function. When these functions of an electronic seal are combined with radio communication systems and data management devices, the status of a container can be confirmed in real-time including whether an unlawful opening has occurred.

9. Electronic seals can be used repeatedly. However, in maritime container transport, reuse rate of materials (material for preventing collapse of cargo and hooks for dressed carcass) generally remains very low (10 to 20% reuse rate). An electronic seal has the same problem in addition to its high cost.

2) *Performance and Composition*

10. There are two kinds of electronic seals: IC tag and Radio Frequency ID (RFID). An IC tag is used for cargo itself because its radio wave reaches only about 10cm and its memory capacity is small. On the other hand, RFID has good prospects for the future for containers due to long reach of its radio waves and large memory capacity. An electronic seal is composed of IC chip, antenna, reader and writer, and main control computer.

3) *Characteristics of RFID*

11. Characteristics of RFID are as follows:

- Information recorded on IC chips can be read and written without any contact with a RFID itself.
- Information can be read and written from multiple RFIDs in block and simultaneously.
- Information can be read and written from a RFID attached to a moving container without stopping it.
- Information can be read and written even in the case that a RFID is covered by material other than metal.
- Information on a RFID can be updated including adding and erasing although that on bar code cannot.
- Compared to a bar code, memory capacity of a RFID is large. Information of thousands of kilo-bytes can be saved. Electronic Product Code is that to control products electronically in which micro chip is substituted for functions of a bar code. In micro chip, serial numbers are allocated to all individual bodies and they are linked to data bases. It can save more information than bar code.
- Compared to a bar code, it is difficult to make illegal copies.
- A RFID has resistance to dust and rust, and can be used in high temperature and humidity.

4) *Price and Status of Development*

12. Prices of electronic seals vary widely. Price of an electronic tag is 500 yen a piece. Price of a set of RFID is about 2,500 yen and its reader costs 3 million yen (about 27 thousand US dollars).

13. Various kinds of electronic seal have been developed. The seals have made sufficient technological advancements. Standardization remains an issue. The following table shows model units.

Table III-2-1 Electronic Seal Model Units

	e-Logicity	Hi-G-Tek	SAVI	All Set Tracking	CGM
Electronic seal	e-Seal	Data Seal	ST-605-DL1 Start	All Seal	Navalock+ Mac Seal
Data transmission	Active RF	Active RF	Active RF	Active RF	Contact Memory
Frequency	433.92MHz	916MHz	433.92MHz & 123 KHz	2.44GHz	(Contact type memory)

5) *Application and Merit*

14. Applications of electronic seal for every transportation process are shown in the following Table.

Table III-2-2 Application of electronic seal

	Transportation process	Application of electronic seal
1	Production factory or designated warehouse	Attach an electronic tag on an article(carton/pallet)
2	Loading to a truck	Set an electronic seal on container door
3	During transportation by truck	Real-time grip of container transport
4	Arriving at terminal gate	Automatic confirmation at a gate
5	Loading to a ship	Confirmation of loading/automatic transmission of information
6	During transportation by ship	Automated positioning of a moving ship
7	Unloading from a ship	Confirmation of unloading/automatic transmission of information
8	Carrying out from a terminal	Automatic confirmation at a gate
9	During transportation by truck	Real-time grip of container transport
10	Door open at destination (factory or warehouse)	Check of records in an electric seal
11	Transportation to final destination	Real-time grip of an article's transport

15. Merits of electronic seal for each work item are shown in Table III-2-3.

Table III-2-3 Merit of electronic seal

	Work items	Merits
1	Packing in a container at a factory/warehouse	Effective cargo management/Automated inspection/ Simplification of data input/Rapid paper work/ Easy in-advance declaration
2	Cargo handling at an export terminal	Obtaining correct information from a truck/ Monitoring of transportation by truck/ Effective packing in a container/ Effective inspection/ Automated documentation/ Check of illicit breaking of a seal/ Effective gate management
3	Sea transportation	Monitoring of transportation by ship/ Check of illicit breaking of a seal
4	Cargo handling at an import terminal	Effective cargo handling at a terminal/ Automated information handling/ Check of illicit breaking of a seal/ Accurate information for customs clearance/ Possibility of in-advance customs clearance/ Effective import inspection/ Automated check at a gate
5	Taking out from a container	Monitoring of transportation by truck/ Sharing of sales information/ Feedback of sales information to a producer

III-2 CONTAINER TRACKING SYSTEM

16. Container tracking system is based on the combined technologies of RFID (Radio Frequency Identification) and artificial satellite system. This system has the following functions.

- ◆ To monitor and report on access to a container
- ◆ To report the position of a container during transportation
- ◆ To carry manifest data and other data related to a container

17. This system can provide the information on whether an unauthorized breach is being made to a sealed container or not, and the position of a container in real time. Therefore this system can contribute to enhancing security of container transportation on the sea as well as on land.

18. As to RFID, a transponder stores information and sends it through radio frequencies when requested. RFID fitted with other sensors such as a laser sensor can detect a breach on a container after it is sealed. RFID technology can be built into a device which is mechanically rigid and has tolerance to temperature changes (from -50 to 70 degree centigrade) Data processing capacity of some RFID is up to 64 kilobytes.

19. There are two kinds of GPS satellite systems. One is a geostationary or high orbit satellite which is about 36,000 km above the earth and rotates along the earth. Another is a low earth orbit (LEO) satellite system which is about 800 km above the earth and does not rotate around the earth. An LEO satellite system can provide an inexpensive narrow-band data transmission and send voice and visual signals. LEO also has advantages to have fewer dead spots and to use non-protruding antennas. Therefore an LEO satellite system is used for container tracking system.

20. Even in the container tracking system which is regarded as integrating the latest technologies, humans play an important role in making the system perfect. A person or persons must confirm cargo on the manifest, attest the accuracy of the manifest and contents of a container, activate the system and lock the doors. These works also must be done at the destination. Once the system is activated, data contained in the RFID device can be read at almost any time and the condition of a container (including an authorized breach) is reported to a supervisor.