Port Security Assessment
Casablanca port case

Presented by Mr Mustapha LOULID

MED PORT 2016

Tangier, 28th April 2016

Contact : loulid@marsamaroc.co.ma

Agenda

1. Introduction
2. The issue
3. Port Security organization
4. Potential Threat Scenarios for Port Facilities
5. Recommendations to Mitigate Facility Security Gaps
6. Technologies to Address Security Gaps
7. Recommendations to Achieve Complete Compliance with ISPS code
8. Conclusion

❶ Introduction : Casablanca Port

25.3 Million tons in 2015

Various types of traffics

CONTAINERS

853,000 TEU's

LIQUID BULK

386,000 tons

CARS

111,000 vehicles

DRY BULK

14.1 million tons

PASSENGERS

270,000 cruise passengers

GENERAL CARGOS

10.2 million tons

Casablanca Port – Eastern Container Terminal

IN BRIEF

Containers volume : 537 000 TEU

Main traffics : Container

Number of employees : 450

Main assets :

- A powerful information system for an automated management of the Eastern Containers' Terminal.
- Safety and security of goods : Electronic surveillance and securing port's areas.
- Real-time information services : Marsa conteneur.

Certification :

The Container Terminal is certified :

- ISO 9001, 2008 version.
- ISO 14001, 2004 version
- OHSAS 18001, 2007 version.
- Freight Forwarding activities are certified ISO 9001, 2008 version, ISO 14001 and OHSAS 18001.

MANAGED FACILITIES

Infrastructures :

- A 600 m long and 12 m deep quay
- 4 berths
- 60 ha of land for container storing

Equipement :

- 8 gantry cranes whose 2 are post-panamax
- 43 straddle carries of 40 t,
- 47 tractors
- 17 forklifts for empty containers,
- 4 forklifts for full containers,
- 60 high trailers of 40 t

Capacity : An annual processing capacity of 650.000 TEU

Casablanca Port – Cars Terminal

IN BRIEF

Traffic volume : 111 000 unit

Main traffics : Vehicles, Trailers

Main assets :

- Safety and security of goods : Electronic surveillance and securing port's areas.
- New vertical storage space for new vehicles.

Certification :

The cars Terminal is certified

- ISO 9001, 2008 version.
- ISO 14001, 2004 version
- OHSAS 18001, 2007 version

MANAGED FACILITIES

Infrastructures :

- 2 bridges of 100 t with a depth of 8 m
- Vertical storage space for vehicles with a storage capacity of 5000 units

Equipement :

- 13 RO-RO tractors of 60 t

Casablanca Port – Multi-purpose Terminal

IN BRIEF

Traffic volume Multipurpose (in tons) **:** 5 million

Main traffics :
Steel products, Sugar, wood and its derivatives, Oil seeds.

Main assets :
- Safety and security of goods : Electronic surveillance and securing port's areas.

Certification :
The RoRo Terminal is certified
- ISO 9001, 2008 version.
- ISO 14001, 2004 version
- OHSAS 18001, 2007 version

MANAGED FACILITIES

Infrastructures :
- A 1500 m long quay with a depth of 9 m to 10.5 m
- 12 berths
- 14.000 m² of covered storage areas
- 60.000 m² of land

Equipement :
- Cranes : 4 cranes of 38 t, 32 quay cranes with a capacity between 6 t and 25 t and 5 mobile cranes
- 106 forklifts,
- 20 tractors from 20 t to 40 t
- hydroelectric grapples,
- hoppers 7 weight bridges,

Port of Casablanca – Ore Terminal

IN BRIEF

Traffic volume (in tons) **:** 1 million

Main traffics : coal, scrap metal

Main assets :

- Safety and security of goods : Electronic surveillance and securing port's areas.

Certification :

The RoRo Terminal is certified

- ISO 9001, 2008 version.
- ISO 14001, 2004 version
- OHSAS 18001, 2007 version

MANAGED FACILITIES

Infrastructures :

- A 390 m long quay with a depth of 9,15 m to 10,5 m
- 2,5 ha of land

Equipement :

- 2 ore gantry cranes of 14 t and 16 t,
- 4 rail mounted cranes of 6 t

Container Terminal : TC 3

In a status of Project, this new terminal will start operations in the last trimester 2016

IN BRIEF :

Capacity volume (in TEU) : 650 000 TEU

Main traffics : Container

Main assets :

- A powerful information system for an automated management of the Eastern Containers' Terminal.
- Safety and security of goods : Electronic surveillance and securing port's areas.
- Real-time information : Marsa conteneur.

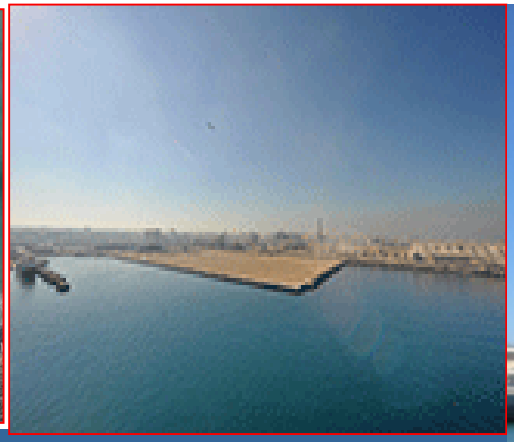
FACILITIES AND EQUIPEMENT:

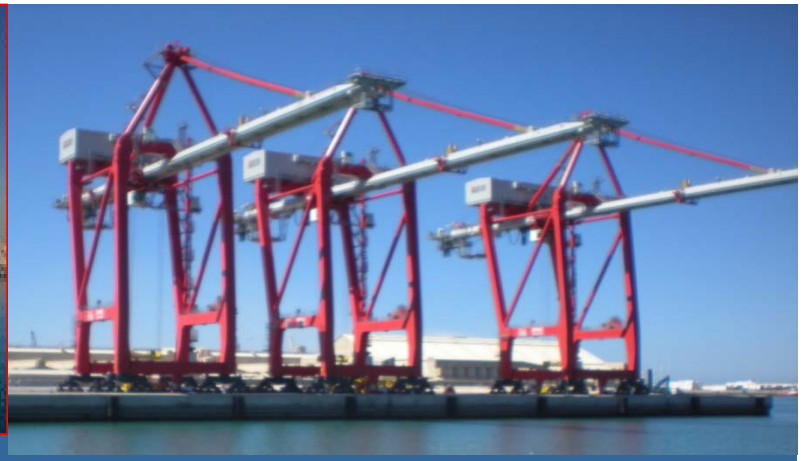
Infrastructures :

- A 530m long and 14 m deep quay
- 3 berths
- 30 ha of land for container storing

Equipement :

- 3 gantry cranes
- 7 RTG of 40 t,
- 15 tractors
- 02 forklifts for empty containers,
- 2 Reach stackers,
- 15 trailers of 40 t





Agenda

1. Introduction
2. The issue
3. Port Security organization
4. Potential Threat Scenarios for Port Facilities
5. Recommendations to Mitigate Facility Security Gaps
6. Technologies to Address Security Gaps
7. Recommendations to Achieve Complete Compliance with ISPS code
8. Conclusion

❷ The issue

How to avoid or mitigate risks of similar threats in our port environment? ?

Can we imagine the consequences of potential attacks to cruiser vessels?

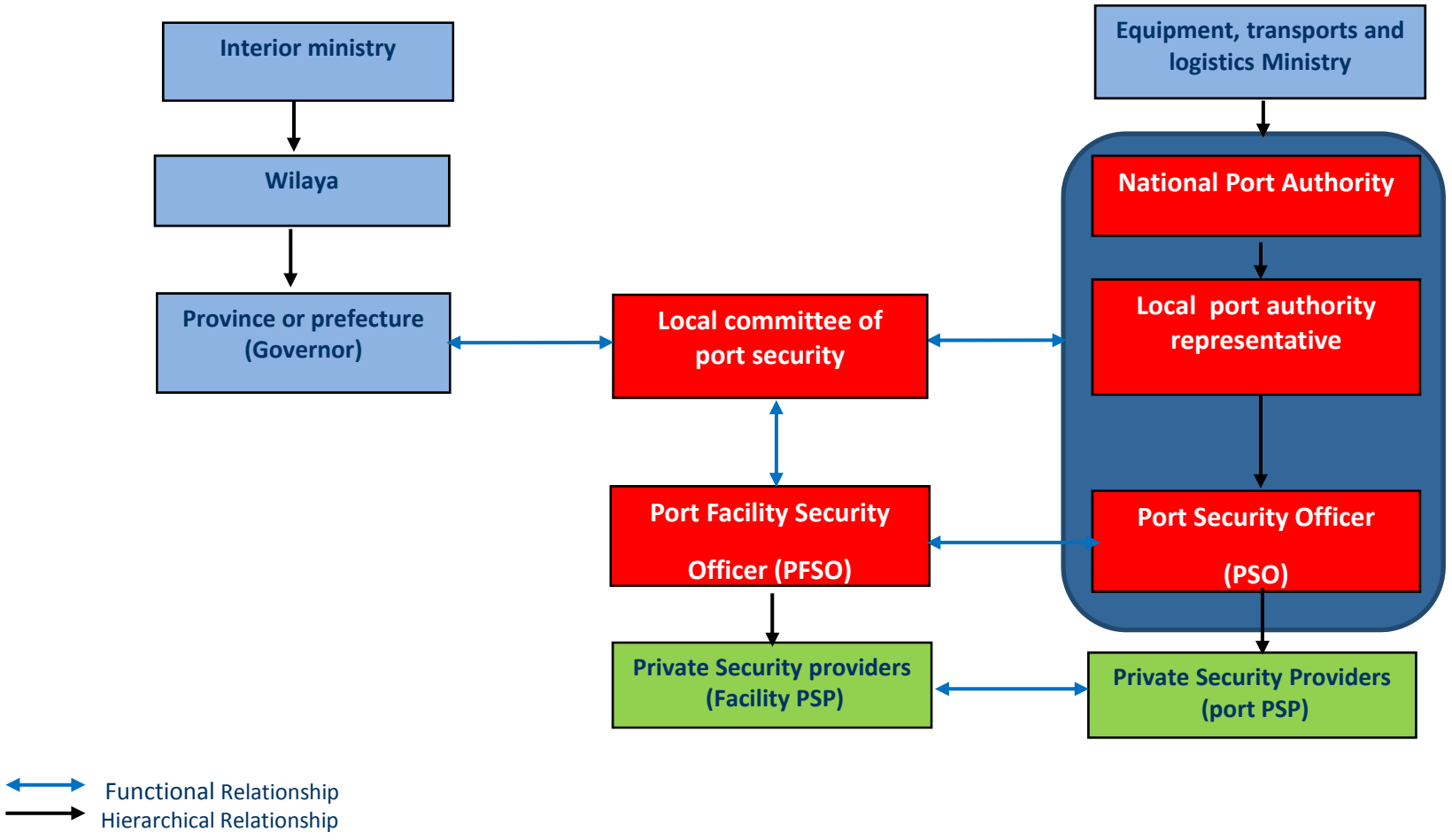
brussels attacks

Agenda

1. Introduction
2. The issue
3. Port Security organization
4. Potential Threat Scenarios for Port Facilities
5. Recommendations to Mitigate Facility Security Gaps
6. Technologies to Address Security Gaps
7. Recommendations to Achieve Complete Compliance with ISPS code
8. Conclusion

❸ Port security organization : Coordination - Subordination

In practice, The Port Security Officer (PSO), the Port Facility Security Officer (PFSO) and the local committee of port security who sustain the organization of security within the port



❸ Port security organization : Main responsibilities in terms of security

NATIONAL PORT AUTHORITY

- Implements the national port security policy
- approves projects of security improvement suggested by the ports
- centralizes and exploits security reports issued by ports
- empowers regional directions to implement national guidelines on security

PORT SECURITY OFFICER (PSO)

- Implements the port security plan
- Coordinates the various departments and entities responsible for port security
- oversees the implementation of the security measures in the port
- works with the PFSO to coordinate the implementation of the security plan

LOCAL COMMITTEE OF PORT SECURITY

- Approves port and port facilities security assessments and plans
- Meets all port stakeholders responsible for security issues (police, gendarmerie, Customs, Local Authorities , Civil Protection, Merchant Navy , Royal Navy , Border Health , quality control)

PORT FACILITY SECURITY OFFICER (PFSO)

- Implements the port facility security plan
- Coordinates the various entities responsible for port facility security
- oversees the implementation of the security measures in the port facility
- Ensure the establishment and update of the assessment and security plan of the port facility
- Conducts regular security inspections of the port facility
- launches training, reminders and specific exercises related to security

❸ Port security organization : security levels

ISPS code defines three security levels:

Security Level 1 : Normal

The level at which the ship or port facility operates normally. Security level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.

Security Level 2 : heightened

The level applying for as long as there is a heightened risk of a security incident. Security level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

Security Level 3 : exceptional

The level applying for the period of time when there is the probable or imminent risk of a security incident. Security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target

❸ Port security organization : Coordination with ships (DOS)

DECLARATION OF SECURITY

Page 1

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.

Name of Ship:	**M.V. CrossTree**
Port of Registry:	**Port Name**
IMO Number:	**Assigned 7 digit number**
Name of Port Facility:	**Post of Call**

This Declaration of Security is Valid from _____ until _____
for the following activities:

Loading, Discharging, Bunkering, Husbandry or Repairs, Refuge, Dry Docking, etc

(List the activities with relevant details)

Under the following security levels

Security Level(s) for the Ship:	**Level 2 - Heightened Threat of Attack**
Security Level(s) for the port facility:	

The affixing of the initials of the SSO or PFSO under these columns indicates that the activity will be done, in accordance with the relevant approved plan, by:		
ACTIVITY	**THE PORT FACILITY**	**THE SHIP**
Ensuring the performance of all security duties.		
Monitoring restricted areas to ensure that only authorized personnel have access.		
Controlling access to the port facility.		
Controlling access to the ship.		
Monitoring of the port facility including berthing areas and areas surrounding the ship.		
Handling of Cargo.		
Delivery of Ship's Stores.		
Handling unaccompanied baggage.		
Controlling the embarkation of persons and their effects.		
Ensuring that security communication is readily available between the ship and port facility.		

DECLARATION OF SECURITY

Page 2

The signatories to this agreement certify that security measures and arrangements for both the port facility part A of the Code that will be implemented in accordance wit the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Dated at _____ on the _____

Signed for and on behalf of	
The Port Facility:	The Ship:
(Signature of port facility security officer)	*(Signature of master or ship security officer)*

Name and title of person who signed	
Name:	Name: Capt. Pawanexh Kohli
Title: Port Facility Security Officer	Title: Master/Chief Executive

Contact details *(to be completed as appropriate)* *(indicate the telephone numbers or the radio channels or frequencies to be used)*	
for the port facility:	for the ship:
Port facility	**Master** via Inmarsat: Ph- Fax- Tlx- Through Officer on Deck - Gangway watch
Port facility security officer	**Ship security officer** ----------
	Company ---------- ---------- ----------
	Company security officer ---------- ---------- ----------

Agenda

1. Introduction
2. The issue
3. Port Security organization
4. Potential Threat Scenarios for Port Facilities
5. Recommendations to Mitigate Facility Security Gaps
6. Technologies to Address Security Gaps
7. Recommendations to Achieve Complete Compliance with ISPS code
8. Conclusion

❹ Potential Threat Scenarios for Port Facilities – Risk Assessment Method

Security risk is assessed based on the **severity** of the consequences of potential crime and it **probability** of occurrence.

The security assessment is performed with a score of points from the assessment of severity and occurrence probability criteria.

1- Severity Score : Minor (1) ; Serious enough (2) ; very serious (3)

2- Probability of occurrence Score (a, b, c):

– a) **physical security(*) :** Very dissuasive (1); dissuasive (2) ; Not dissuasive (3)

– b) **organic security(**) :** Very dissuasive (1) ; dissuasive (2) ; Not dissuasive (3)

– c) **Human factor (***) :** Very dissuasive (1) ; dissuasive (2) ; Not dissuasive (3)

(*) : accessibility of the port facility
(**) security facility organization : procedures, etc.
(***) : qualifications and skills

❹ Potential Threat Scenarios for Port Facilities – Risk Assessment Method

Severity / Probability	Minor	Serious enough	very serious
Unlikely			
Likely			
Inevitable			

Three levels of security risks :
1- Low risk (green) : no modifications to existing measures ; security sufficient
2- moderate risk (yellow) : Take where possible risk reduction measures
3- intolerable risk (red) : Required risk reduction measures

❹ Potential Threat Scenarios for Port Facilities

Potential threats are classified in the following order :

1. Presence of stowaways;
2. Drug trafficking
3. Smuggling weapons or equipment, including weapons of mass destruction;
4. Theft of goods
5. Intrusions
6. Unauthorized access
7. identity or access badge theft
8. Damage to, or destruction of, the port facility or of the ship, e.g. by explosive devices, *arson, sabotage or vandalism*
9. Blockage of port entrances, locks, approaches
10. Tampering with cargo, essential ship equipment or systems or ships stores;
11. Hijacking or seizure of the ship or of persons on board;
12. Use of the ship to carry those intending to cause a security incident *and their* equipment;
13. Use of the ship itself as a weapon or as a means to cause damage or destruction;
14. Nuclear, biological and chemical attack.

Agenda

1. Introduction
2. The issue
3. Port Security organization
4. Potential Threat Scenarios for Port Facilities
5. Recommendations to Mitigate Facility Security Gaps
6. Technologies to Address Security Gaps
7. Recommendations to Achieve Complete Compliance with ISPS code
8. Conclusion

❺ Recommendations to Mitigate Facility Security Gaps

Access to port and facilities

Monitoring requirements

Surveillance equipments

Cargo and baggage control

Communications requirements

Main messages

- ***Passengers Access to restricted Area***
  - – Use buses or vans for cruisers in general cargo terminal to ensure supervised access
  - – Establish clearly demarcated “Passengers pedestrian lanes” running from the berth to the facility restricted areas access control point
- ***Perimeter boundaries***
  - – Develop a systematic inspection and audit plan addressing all perimeter boundaries structures
- ***Access control system (ACS)***
  - – Use an integrated Access control system to improve incident assessment and response capabilities
- ***Signage***
  - – Improve signage at waterside perimeter to warn recreational boaters, commercial fishing vessels and others inauthorized vessels that they are approaching a restricted area.

❺ Recommendations to Mitigate Facility Security Gaps

- ***Access to port and facilities***
- ***Monitoring requirements***
- ***Surveillance equipments***
- ***Cargo and baggage control***
- ***Communications requirements***

Main messages

– Integrate a various subsystems with display and management capabilities on local workstation or display walls in order to enable the operators to better assess events and provide management with more accurate and timely notifications

❺ Recommendations to Mitigate Facility Security Gaps

- ***Access to port and facilities***
- ***Monitoring requirements***
- ***Surveillance equipments***
- ***Cargo and baggage control***
- ***Communications requirements***

Main messages

– Deploy perimeters intrusion detection sensors (laser and infrared technologies, microwave, etc.)

– Upgrade cameras to IP technology to provide improved assessment, video quality and control

– Deploy video analytics for intrusion detection

– Use License Plate Recognition (LPR) and optical character Recognition (OCR) at entry control point

– Automate call-up of cameras and review tasking of cameras

❺ Recommendations to Mitigate Facility Security Gaps

Access to port and facilities

Monitoring requirements

Surveillance equipments

Cargo and baggage control

Communications requirements

Main messages

– Deploy enhanced screening of baggage and ship's stores

– Use enhanced scanning technologies for chemical, biological, nuclear, radiation and explosive detection

– Use non intrusive inspection (NII) for stowaways and contraband (X-ray scanners)

❺ Recommendations to Mitigate Facility Security Gaps

Access to port and facilities

Monitoring requirements

Surveillance equipments

Cargo and baggage control

Communications requirements

Main messages

– Improve the access to trunked Radio system to develop the ability to communicate and coordinate with all security actors especially in the event of a major security incident

– Deploy enhanced alert and warning capabilities

– Improve power conditioning, reliability, redundancy and resilience of security and network equipment

Agenda

1. Introduction
2. The issue
3. Port Security organization
4. Potential Threat Scenarios for Port Facilities
5. Recommendations to Mitigate Facility Security Gaps
6. Technologies to Address Security Gaps
7. Recommendations to Achieve Complete Compliance with ISPS code
8. Conclusion

❻ Technologies to Address Security Gaps

Technology	General description
Cameras	Thermal, infrared, long range, exterior motion detection and analytics
Perimeter intrusion detection sensors	Buried, fence mounted, Radar, infrared, laser, microwave
Video analytics and motion detection	Trip wire, speed, area penetration, behaviour recognition
Facial Recognition	Identity management of individuals in a crowd or at entry control point
License Plate and optical character recognition	Container, rail car and vehicle identification and tracking

⑥ Technologies to Address Security Gaps

Technology	General description
Cargo Screening and control	X-ray, Magnetometer, Pulsed Fast Neutron Analysis, Dual Ion Mobility Spectrometry
Detection of CBRNE products	Fixed, portable, Mobile Chemical Biological, Radiological, Nuclear and explosive detection
Physical Security Information Management	Security and Incident Management system integration
Network Management and monitoring	Network status information
Power conditioning, reliability Redundancy & resilience	Uninterruptible power supplies, surge suppression

Agenda

1. Introduction
2. The issue
3. Port Security organization
4. Potential Threat Scenarios for Port Facilities
5. Recommendations to Mitigate Facility Security Gaps
6. Technologies to Address Security Gaps
7. Recommendations to Achieve Complete Compliance with ISPS code
8. Conclusion

7 Recommendations to Achieve Complete Compliance with ISPS code

	Opportunity For Improvement
National security framework	*Adopt national legislation incorporating SOLAS, ISPS code and OMI recommendations*
Plans and procedures	*Align Port Facility Security Plans (PFSP) with Port Security Plan (PSP), port emergency plan, port operating rules, customs procedures and terminal Internal Organization plans (POIs)*
	Align Port Facility Security Plans (PFSP) with Port Facility Security Assessment (PFSA)
Port Security Committee	*Incorporate IMO guidelines related to development of National Maritime Security Committees and Port Security committee*

7 Recommendations to Achieve Complete Compliance with ISPS code

	Opportunity For Improvement
Port Security Levels	Explore targeted approach to use of elevated security levels
Record keeping	Work with all security stakeholders to advocate national standards for record keeping Develop and implement record keeping including national standards, a security incident log, transmission and distribution and training
Security Incident Logs	Implement a security incident log to record security related incidents, security breaches, improper use of credentials and suspicious behaviours

7 Recommendations to Achieve Complete Compliance with ISPS code

	Opportunity For Improvement
Threats scenarios	*Introduce threats scenarios and impact values reflecting differences in impact based on the types of vessels such as cruise vessels, or type cargo, such as hazardous cargo involved*
	Reassess the impact of Stowaway threat considering the international implications
Training	*Develop Quick Response Cards (QRC) to provide baseline direction for a range of actions and scenarios to ensure critical first steps are taken by responsible personnel*

7 Recommendations to Achieve Complete Compliance with ISPS code

	Opportunity For Improvement
Training	***Establish a systematic lifecycle of drills and exercises for security*** ***Develop an integrated training, drill and exercise program for PFSO, facility personnel having specific security duties and other facility personnel***

Agenda

1. Introduction
2. The issue
3. Port Security organization
4. Potential Threat Scenarios for Port Facilities
5. Recommendations to Mitigate Facility Security Gaps
6. Technologies to Address Security Gaps
7. Recommendations to Achieve Complete Compliance with ISPS code
8. Conclusion

⑧ Conclusion

Casablanca port has implemented significant measures to address risks in terms of security.

But, there are still areas for improvement to be explored especially in terms of procedures, training and capacity.