# Table of Contents

## Chapter 0 - Introduction

## Chapter 1 - ISPS Code and Legislation

- The International Maritime Organisation (IMO)
- Other legislation
- Abbreviations and definitions
- Summary of Chapter 1
- Questions and exercises
- Questions
- Exercise assignments

## Chapter 2 - (Electronic) Security Equipment

- Alarm/emergency centre
- Emergency centre (private emergency centre)
- Detection systems
- Warning and alarm systems
- Alarm receipt – processing systems
- Interior security systems
- Exterior security systems
- Closed circuit television (CCTV)
- Means of communication (means of connection)
- Metal detectors and scanners
- Access control systems
- Video transmission through telephone lines (Internet)
- Disadvantages of electronic means
- Summary of Chapter 2
- Questions and exercises
- Questions
- Exercise assignments

## Chapter 3 - Checking Persons and Goods - Inspections

- Checking persons
- Competencies of the port security officer
- Personnel with a permanent appointment
- Personnel for the ‘long term’
- Personnel of third parties
- Persons wishing to go aboard
- Visitors and suppliers
- Handling of announced and unannounced visitors
- Check and registration of identity
- Searching (inspection and body-searching) of persons
- Inspection and methods of checking
- Body-searching (ISPS Code, Part B, art. 9.15.)
- Inspection of movement of goods
- Routine check of the cargo
- Checking the company seals
- The ship’s provisions
- Gate of Access Control
- Tracking and tracing
- Scanning on the presence of radioactive material
- Summary of Chapter 3
- Questions and exercises
- Questions
- Exercise assignments

## Chapter 4 - Security Plan - PFSP - Corporate Policy

- Security Plan
- Inventory of risks induced by crime
- Drafting of a Security Plan
- Port Facility Security Plan (PFSP)
- Outline of vulnerable corporate assets and infrastructure
- Description of a terminal
- Organisation and execution of security tasks executed by the security organisation
- Organisation of communication between the Port Facility Security Officer, the Ship Security Officer (Company Security Officer) and the Competent Authority
- Policy on access control by the Port Facility
- No- or restricted areas
- Cargo handling
- Delivery of ship stores
- Handling unaccompanied luggage
- Check and revision of the Port Facility Security Plan
- Education and training of security personnel
- Corporate Policy
- Company regulations and rules
- Summary of Chapter 4
- Questions and exercises

## Chapter 5 - ID Documents

- Evasive actions and distractions
- Evasion of access control
- Unexplainable alarm (motion detection)
- Distraction of the attention
- Recognition of identity documents
- ID documents: from passports to ID cards
- Passport within the European Community
- Some examples
- Driving licenses
- Forgeries
- Original documents – fake credentials
- Authentication of identity documents
CHAPTER 6 - RECOGNITION OF WEAPONS AND AMMUNITION

Legislation on illicit trafficking of weapons or any other dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorised

ISPS Code

UN Firearms Protocol Definitions


Introduction


Introduction

Weapons other than firearms as defined in national legislation

Introduction

Hierarchy in law

Introduction

Weapons and Ammunition Act – weapon categories

Weapons and ammunition categories

Introduction

Some definitions

Category I – the Netherlands

Category II

Category III

Category IV

Various permits

Explosives

Note on the text provided

Questions and exercises

Questions

Exercise assignments

CHAPTER 7 - COMMUNICATION AND DEALING WITH AGGRESSION

Communication

What is communication? 83

Types of communication

Verbal communication

Written communication

The communication process

Noise

Active listening

Types of questions

CHAPTER 8 - DANGEROUS COMMODITIES

What are dangerous goods?

Introduction

Dangerous goods


Classification of dangerous goods (substances, materials or articles)

Identification

Labels (placards), signs and marks

Transport (shipping) document

ADR

International labelling of dangerous goods: IMDG Code labels, signs and marks

Questions

Exercise assignments
INTRODUCTION

Events in the recent past have proven that no country in the world is safe against terrorists. Terrorist attacks can, for whatever motives, occur at any time and at any place. Even the shipping industry cannot escape that fact.

Unfortunately, this problem is not new to the world, to the European Union. The U.S., the E.U. as well as many other countries have already taken numerous measures to protect their citizens and their means of transportation.

The E.U. Commission is of the opinion that the security of the entire logistical chain of sea transport, from supplier to end-user, is susceptible to improvement. As the chain of transport is as safe as the weakest link, the security of transport on all points could be improved by a parallel ‘multimodal approach’.

The International Maritime Organisation (IMO), the international organisation that is responsible for the safety of the shipping industry in general, has issued a number of obligatory regulations and recommendations that constitute a framework within which maritime safety can be improved considerably.

These obligatory regulations and recommendations are documented in an international agreement, the International Treaty for the Safety of Lives at Sea (SOLAS) and the accompanying code, the International Ship and Port Facility Security Code (ISPS Code). This International Ship and Port Facility Security Code (ISPS Code) contains detailed security-related requirements for governments, port authorities and shipping companies. It is intended to enable better monitoring of freight flows, to combat smuggling and to respond to the threat of terrorist attacks. Countries that fail to observe the ISPS Code, which took effect by 1 July 2004, risk being excluded from international trade.

By accentuating, among other aspects, the security measures on terminals that apply to international sailing ships of 500 GT\(^1\) or larger, certain requirements with regard to the professional skills of security personnel have been adjusted. To attain this level of knowledge, courses have been developed. The described knowledge level as documented in the ISPS Code is obligatory to be allowed to perform security activities on the terminals as described in the ISPS Code.

Part A and B cannot be discussed as separate parts of the ISPS Code. Part A contains the obligatory requirements, Par B clarifies them. Moreover, some of the recommendations worded in Part B are obligatory in many countries and possibly will be made obligatory in the future.

This course provides the specialist education ensuring the knowledge requirement of port facility security personnel as stated in the ISPS Code Part A: art. 18.1\(^2\).

As a result of the international character of the port facility security personnel activities, a basic knowledge of the English language is necessary.

---

1. Gross Ton is the measurement of the size/content of ships
2. “The port facility security officer 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”
1.1 THE INTERNATIONAL MARITIME ORGANISATION (IMO)

The United Nations is an organisation of sovereign states. The objective of the United Nations is to achieve world peace, maintain friendly relations between all nations and strive for economical and social progress. The United Nations was officially founded on October 24, 1945 and consisted at that time of 51 member states. Presently, 192 countries are member of the UN.

In 1948, the United Nations decided to set up a special department that should improve the security of the shipping industry. In 1958 the International Maritime Organisation (IMO) was founded, whose first objective was to safeguard the safety of the shipping industry and later on was charged with the prevention of marine pollution by ships as well. The IMO, an independent organisation with over 162 connected member states, still has close connections with the United Nations. The IMO is a technically-oriented organisation although people take up a central place as well.

Most of the work is performed by commissions and sub-commissions. The most well-known is the Maritime Security Commission (MSC) and, of a later date, the Maritime Environmental Protection Commission (MEPC). Under pressure of piracy, hostages and terrorist actions, the development of measures and the accompanying regulations regarding the maritime security were accelerated.

The final adaptation of SOLAS, chapter XI was adopted by the Diplomatic Conference of the on Maritime Security on December 12, 2002 and contains instruments whose objective it is to improve the safety of the shipping industry and to improve the interface between ship and shore (the terminal).

The resulting obligatory regulations and recommendations are recorded in an international agreement, the International Treaty for the Safety of Lives at Sea (SOLAS) and the accompanying code, the International Ship and Port facility Security Code (ISPS Code).

This agreement contains regulations and recommendations to which both international sailing ships as well as the receivers on the landward side (terminals) must comply with. The alteration of the SOLAS Treaty, inclusive of the corresponding ISPS Code, has been adopted by the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974, and has been in force as of July 1, 2004.

1.2 SAFETY OF LIVES AT SEA (SOLAS) TREATY AND THE ACCOMPANYING INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND PORT FACILITIES (ISPS)

The SOLAS/ISPS Code consists of the following parts:

- SOLAS Chapter XI-2: Special measures to improve the security on sea.
- Part B: Directives with regard to the regulations of chapter XI-2 of the enclosure of the International Treaty for the Safety of Lives at Sea (SOLAS) of 1974 as adapted and Part A of this Code.

The objective and functional demands of the ISPS Code

The Code has the following objectives:

1. Creation of an international framework for cooperation between states entering into a treaty, public bodies, local governments and the shipping and port industries to recognise the security threats and take preventive measures against security incidents relating to ships and port facilities in use during international trade;

2. Determination of the respective roles and responsibilities of the states entering into a treaty, public bodies, local governments and the shipping and port facilities on a national and international level to insure the maritime security;

1 Also part of the Regulations of the European Parliament and the Council with regard to improvements of the security of ships and port facilities.
3. Assurance for a timely and effective collection and exchange of information in the area of security;
4. Provision of a methodology to execute the security assessments in order to have plans and procedures available in order to be able to react on changing security levels;
5. To inspire confidence that adequate and appropriate maritime security measures have been taken.

To realise these objectives, the present Code dictates a number of functional demands. These are, among others:
1. To collect and assess information with regard to threats for the security and exchange of such information with the respective states entering into a treaty;
2. To demand that communication protocols are maintained for ships and port facilities;
3. To prevent that unauthorised people gain access to ships, port facilities and accompanying off-limit areas;
4. To prevent that forbidden weapons, fire bombs or explosives could be brought aboard ships or in port facilities;
5. To be equipped with means to sound the alarm in case of security threats or security incidents;
6. To make it compulsory to have security plans available based on security assessments for ships and port facilities;
7. To make it compulsory to have trainings and exercises available to ensure familiarity with security plans and – procedures.

**SUMMARISING:**

**IMO/SOLAS ISPS Code:**
- Worldwide legislation
- Effective as of July 1, 2004
- Requirements are formulated for governments, ships and port facilities
- Part A is obligatory and compulsory (binding)
- Part B consists of recommendations (US obligatory, EU partly obligatory)
- The EU has issued additional obligations and recommendations

**A survey of the most important regulations of the SOLAS Treaty part A and B of the ISPS Code (1)**

The regulations are valid for passenger ships, cargo ships with a load capacity of 500 GT, offshore drilling units and port facilities in charge with dealing with the above-mentioned international shipping traffic.

**SHIPS**

As observed from the SOLAS Chapter XI-1 and XI-2 the regulations require:
- An identification number, installed on the ship in the form of a durable identifying mark;
- An automatic identification system (AIS);
- A security alarm that should send an emergency call when the ship is being attacked;
- A continuous synopsis report, in other words: a curriculum vitae of the ship;

**SHIPS AND PORT FACILITIES**

- Active and passive security measures, classified in three levels:
  - Level 1: normal;
  - Level 2: high;
  - Level 3: exceptional.
- Obligation to appoint persons responsible for the execution of security measures (security guards of the ship, the company and the port facility);
• Formulation of security plans;
• Measures for the education and training of personnel;
• Port Facility Security Assessment (PFSA) - it is obligatory that a Port Facility Security Assessment (PFSA) is made on each port facility.
• Port Facility Security Plan (PFSP) - one of the measures taken after the PFSA, is the formulation of a Port Facility Security Plan (PFSP).
• Port Facility Security Officer (PFSO) - a Port Facility Security Officer (PFSO) should be appointed for each port facility. One person can be appointed PFSO for one or more port facilities.

Access to the Port Facility

The PFSP should take measures with regard to the access to the Port Facility via:

1. Waterways, inclusive of the entrances, rivers, canals and moor areas;
2. Traffic routes;
3. Footpaths;
4. Railways;
5. Piers, quays;
6. Adjacent works, locations from which people are able to observe (part of) the port or port facility;
7. Electronic information systems.

The combined articles from Part A and B of the ISPS Code

Access limitations at the different security levels (article 16.10)

The PFSP should indicate where access is restricted or prohibited for each location and for each security level.

For every security level the PFSP should indicate the type of restriction or prohibition as well as the way in which these limitations are maintained.

Identification – and pass system (article 16.11)

The PFSP should indicate the need for identification for each security level in order to gain access to the port facility or to remain on the port facility without identification. This could result in the design of an appropriate pass system for permanent or temporary passage of employees and visitors respectively.

Passengers could reveal their identity by showing their embarkation pass, tickets and so on. Entering restricted or prohibited areas without supervision should not be allowed.

The PSFP should contain regulations to guarantee that the pass system is revised regularly and that abuse of the system automatically leads to sanctions.
**Port Facility Identification System - No revelation of identity (article 16.12, 16.13)**

Persons who are asked to reveal their identity and refuse to do so or are unable to reveal their identity or state the purpose of their visit should be denied access to the port facilities. Their efforts to gain access should be reported to the PFSO or to local or national authorities with responsibilities with regard to security.

**Inspection of persons, their personal belongings and their vehicles (article 16.14)**

The PFSP should appoint locations where persons, their personal belongings and their vehicles can be inspected. These locations should be roofed areas in order to guarantee the continuity of the operations regardless of weather conditions in accordance with the content of the PFSP.

**Separate locations for persons who have already been searched/checked (article 16.15)**

The PFSP should appoint separate locations as waiting areas for persons who have already been checked and persons who should be checked/searched with all their personal belongings. If possible, separate areas should be created for passengers and crew going aboard and going ashore with their personal belongings to make sure that persons who are not searched/checked yet are not able to come into contact with persons that have already been searched/checked.

**Access Control**

**Description of the frequency of the access controls (article 16.16)**

The PFSP should describe the frequency of application of any access controls.

**Subjection to the Inspection (article 16.18)**

For security level 1, every person wanting access to the port facility should subject him or herself to inspection. The frequency of such inspections, inclusive random inspections, is described in the approved PFSP.

In the ISPS Code, three security levels are defined, namely:

- Level 1: normal;
- Level 2: high;
- Level 3: exceptional.

**Entrance Check (Article 16.17)**

**Security level 1 (normal)**

At security level 1, the PFSP should establish the control points where the following security measures may be applied:

1. Restricted areas which should be bound by fencing or other barriers to a standard which should be approved by the Contracting Government;
2. Checking identity of all persons seeking entry to the port facility in connection with a ship, including passengers, ship's personnel and visitors and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders, etc.;
3. Checking vehicles used by those seeking entry to the port facility in connection with a ship;
4. Verification of the identity of port facility personnel and those employed within the port facility and their vehicles;
5. Restricting access to exclude those not employed by the port facility or working within it, if they are unable to establish their identity;
6. Undertaking searches of persons, personal effects, vehicles and their contents;
7. Identification of any access points not in regular use which should be permanently closed and locked.

**Access Control (Article 16.19)**

**Security level 2 (high)**

At security level 2, the PFSP should establish the additional security measures to be applied, which may include:

1. Assigning additional personnel to guard access points and patrol perimeter barriers;
2. Limiting the number of access points to the port facility, and identify those to be closed and the means of adequately securing them;
3. Providing the means of impeding movement through the remaining access points, e.g. security barriers;
4. Increasing the frequency of searches of persons, personal effects, and vehicles;
5. Deny access to visitors who are unable to provide a verifiable justification for seeking access to the port facility;
6. Use of patrol vessels to enhance waterside security.

**Access Control (article 16.20)**

**Security level 3 (exceptional)**

At security level 3, the port facility should comply with instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close cooperation with those responding and the ships at the port facility, which may include:

1. Suspension of access to the entire or part of the port facility;
2. Granting access only to those responding to the security incident or threat thereof;
3. Suspension of pedestrian or vehicular movement within the entire or part of the port facility;
4. Increased security patrols within the port facility, if appropriate;
5. Suspension of port operations within the entire or part of the port facility;
6. Direction of vessel movements relating to the entire or part of the port facility;
7. Evacuation of the entire or part of the port facility.

**Monitoring the security of the port facility (article 16.49)**

The port facility security organisation should at all times be capable to monitor/ supervise:

- The ships on the port facility;
- The areas around the ships.

The above-mentioned aspects should be optimally guaranteed at all times including night time and periods of limited vision.

To do this, the following aids may be used:

1. Lighting;
2. Security guards, including foot, vehicle and waterborne patrols;
3. Automatic intrusion detection devices and surveillance equipment.

**Continuous occupation of the electronic security systems (article 16.50)**

When used, electronic security systems should activate an audible and visual alarm on a location that is continuously supervised 24 hours a day. From this location, the reactions on a security incident will be coordinated.

**Continuous functioning of the supervision equipment (article 16.51)**

The PFSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment (CCTV, electronic security systems etc.) will be able to perform continually, including consideration of the possible effects of weather conditions and power disruptions.

**1.3 OTHER LEGISLATION**


Security incidents resulting from terrorism are among the greatest threats to the ideals of democracy, freedom and peace, which are the very essence of the European Union. People, infrastructure and equipment in ports should be protected against security incidents and their
devastating effects. Such protection would benefit transport users, the economy and society as a whole.

On 31 March 2004, the European Parliament and the Council of the European Union adopted Regulation (EC) No 725/2004 (4) on enhancing ship and port facility security. The maritime security measures imposed by that Regulation constitute only part of the measures necessary to achieve an adequate level of security throughout maritime-linked transport chains. That Regulation is limited in scope to security measures on board vessels and the immediate ship/port interface.

In order to achieve the fullest protection possible for maritime and port industries, port security measures should be introduced, covering each port within the boundaries defined by the Member State concerned, and thereby ensuring that security measures taken pursuant to Regulation (EC) No 725/2004 benefit from enhanced security in the areas of port activity. These measures should apply to all those ports in which one or more port facilities covered by Regulation (EC) No 725/2004 are situated.

The security objective of this Directive should be achieved by adopting appropriate measures and should rely upon detailed security assessments to identify the exact boundaries of the security-relevant port area, as well as the different measures required to ensure appropriate port security. Such measures should differ according to the security level in place and reflect differences in the risk profile of different sub areas in the port.

Member States should approve port security plans which incorporate the findings of the port security assessment. The effectiveness of security measures also requires the clear division of tasks between all parties involved as well as regular exercises. This clear division of tasks and the recording of exercise procedures in the format of the port security plan is considered to contribute strongly to the effectiveness of both preventive and remedial port security measures.

Since this Directive concerns seaports, the obligations herein contained should not be applicable to Austria, the Czech Republic, Hungary, Luxembourg or Slovakia.

The Directive has been accepted on 26th of October 2005. The member states have 18 months to implement this Directive in their own national legislation.

The legislation will be in force as of June 15th, 2007.

1.4. ABBREVIATIONS AND DEFINITIONS

CSO (Company Security Officer)
Shipping Company Security Officer (CSO).
Maintains contacts with the SSO and PFSO and is responsible for the formulation of the SSA.

DoS (Declaration of Security)
Declaration of Security (DoS). A ship can issue a request for a declaration of security in a number of situations. This can be drawn up by the PFSO and the SSO.

PFSA (Port Facility Security Assessment)
It is obligatory that on each port facility a Port Facility Security Assessment (PFSA) is made. This is evaluated by the government, by an officer appointed by the government, or by a RSO (Recognised Security Organisation) on behalf of the Government. Governments approve!

PFSO (Port Facility Security Officer)
For each port facility a Port Facility Security Officer (PFSO) should be appointed. One person can be appointed as a PFSO for one or more port facilities.

PFSP (Port Facility Security Plan)
One of the measures taken after the PFSA is the formulation of a Port Facility Security Plan (PFSP).
This plan has been developed to apply the measures focused on the safeguarding of port facilities, ships, persons, cargo, cargo transport units and the ship’s provisions on the port terrain against the risks of a security incident.

**PSO - Competent Authority (Port Security Officer)**
Manager of a port area (PSO); a Security Manager of the entire port.

**RSO (Recognised Security Organisation)**
A security organisation recognised by the government (RSO).
The RSO is allowed to advise and give assistance to shipping companies, port facilities and ships with regard to security events.

**SSA (Ship Security Assessment)**
A Ship Security Assessment (SSA) should be drawn up for every ship.
The Company Security Officer (CSO), appointed by the shipping company, is responsible for making that inventory for all ships of that shipping company.

**SSO (Ship Security Officer)**
The Ship Security Officer (SSO) is a person appointed by the shipping company that is responsible for the security aboard the ship. He gives account to the captain and is contact person between the CSO and PFSOs. He is maintaining the SSP.

**SSP (Ship Security Plan)**
After the SSA is drawn up and evaluated, a Ship Security Plan (SSP) is formulated. This is the responsibility of the SSO (Ship Security Officer).
A plan has been developed to apply the measures focused on the safeguarding of persons aboard, cargo, cargo transport units and the ship’s provisions against the risks of a security incident.

### 1.5. SUMMARY OF CHAPTER 1

To combat terrorist attacks and other threats, the International Maritime Organisation (IMO) has proclaimed certain measures. These measures, SOLAS / ISPS Code, contain regulations and recommendations to which Ship Owners (international sailing ships as defined in the code) and the receiving port facilities (terminals) should comply with.

The European Parliament has adopted the alterations of the SOLAS Treaty 1974 with the accompanying ISPS Code integrally and has introduced additional measures where necessary. The Regulation has become effective as of July 1, 2004.

Moreover, as from June 15th 2007, European legislation addressing the security of Port Areas will be in force.

This will have a substantial impact on the security of Ports, Ships as well as the port facilities.

International maritime security works with three security levels (alertness levels)

- Security level 1 (normal),
- Security level 2 (high) and
- Security level 3 (exceptional).

When the security level increases, the amount of measures that have to be taken will be raised and intensified. Additional security personnel will be mobilised and, in case of an evacuation of the port facility, personnel of the company (for example the Emergency Respond Teams) will be mobilised as well. The government will raise its supervision when the security level is raised. The security levels on a ship and on the port facility should always be at the same level.

On ships and port facilities engaged in international trading, Security Assessments must be executed.
The Port Facility Security Assessment (PFSA) of the port facility will be audited and is the basis of a Port Facility Security Plan (PFSP) to be approved by the government.

The Ship Security Assessment (SSA) for a ship will be approved by its government as a basis to a Ship Security Plan (SSP), to be approved by the Government (Flag State).

When approved, the ship is issued an International Ship Security Certificate that will be valid for five years.

On these ships a Ship Security Officer (SSO) should be appointed.

On the port facility, a Port Facility Security Officer (PFSO) will be appointed by the company. The PFSO must be available / accessible 24 hours a day.

When the vessel arrives, the SSO and PFSO contact each other about security matters. During its stay, both PFSO and SSO consult regularly.

1.6. QUESTIONS AND EXERCISES

1.6.1 Questions

Question 1
For each port facility (if appointed for this purpose) a PFSO (Port Facility Security Officer) should be appointed. Who will appoint this person?

Question 2
What are the tasks of the PFSO?

Question 3
What are the objectives of the ISPS Code?

Question 4
What are the obligations of a port facility according the ISPS Code?

Question 5
What are the three security levels and describe in which cases these will be applied.

Question 6
What does the abbreviation PFSA stand for? Give a brief explanation.

Question 7
What does the abbreviation CSO stand for? Give a brief explanation.

Question 8
What is a PFSP?

Question 9
Is it possible that a PFSO assists a SSO on request?

Question 10
Can you mobilise any other personnel of the port facility next to the security personnel on that location? Motivate your answer.

1.6.2 Exercise Assignments

1. Describe the requirements of an international trading ship of 550 GT mooring on a Dutch port facility.

2. Describe your actions if a visitor to the port facility has the intention of visiting a ship that has already moored. He has reported to you but can not show you a valid identification document. At this moment, security level 1 is effective.
3. What are your actions toward visitors of the port facility from the moment that security level 3 is effective?

Also part of the Regulations of the European Parliament and the Council with regard to improvements of the security of ships and port facilities.
INTRODUCTION
As a security guard, you play an important role in the security of your (port facility) location. In particular as a result of the more stringent demands with regard to the legislation and instructions for port facilities in the ISPS code, modern security equipment will increasingly become a necessity.

In this chapter, the most commonly used security equipment will be explained. This way you will get a general impression of the possibilities and impossibilities of the various tools.

For a correct usage, you should read the directions for use carefully for all equipment your company deploys.

However, it is very important to know that all tools or security equipment produces or receives / detects signals or information only; it is an aid to help you perform your task.

The security guard, the user of the security equipment, determines the quality because a tool is of no use without a proper follow-up.

2.1 ALARM/EMERGENCY CENTRE
In the technical security branch (technicians) the term “alarm / emergency centre” signifies a signal box, as part of a burglar signalling system on a location.

This alarm / emergency receives all the data of all connected detectors and this data may be shown at the box.

Light bulbs (leds) are positioned in groups on the signal box. If a deviant situation occurs, the attention is drawn to this fact by lighting up of the bulbs, or by means of a LCD screen and an audible signal.

2.2 EMERGENCY CENTRE (PRIVATE EMERGENCY CENTRE)
At the private emergency centre, all kinds of (electronic) signals enter from different locations which must be assessed at its true value and than processed by the personnel.

2.3 DETECTION SYSTEMS
The purpose of a detection system is to trace, observe and expose unwanted situations that can occur at any given place.

1 light emitting diodes
Most modern systems record the information and keep track of the data. The systems are subdivided in several main groups that will be treated subsequently.

**FIRE DETECTION**
Heat, flames and smoke can be noticed and detected by automatic fire alarm systems. These alarm systems are detection instruments that run on electricity and are connected to a fire alarm centre.

If the fire alarm centre does not send the reports to the fire brigade immediately, these signals may be sent to a private alarm centre or a permanently manned post as well.

Under defined circumstances, these signals can be sent to the fire brigade with a delay (for example a two minutes delay). If that is the case, it must be recorded in a procedure. Personnel of that particular location will check their location and, in case of a false alarm, stop the report to the fire brigade.

Operating the fire alarm centre must be performed by authorised personnel only.
At the entrance (on a specific parking for the fire brigade) and sometimes at other strategic places, an additional panel has been positioned on which the most important signals of the fire alarm centre are displayed as well.

This additional panel is also known as the fire alarm panel. At the reception of a signal, personnel notice immediately where the report originated.

**BURGLAR ALARM**
When entering a building must be prevented and burglar alarms are installed to achieve this goal, then they are called interior security systems.

In case of burglar alarms, several kinds of detection methods are used.

**TECHNICAL- AND WATER DETECTION**
Power failure / loss of electricity, a low level alarm in machines, failure of the heating system, leakage, breakdowns, temperature, liquid and difference in pressure can be measured through means of detection equipment and will cause a technical alarm to go off.

**2.4 WARNING AND ALARM SYSTEMS**

**ALARM INDICATORS**
These indicators can consist of all kinds of equipment that will alarm the immediate vicinity if something goes wrong.

The alarm can consist of internal and external sirens, flashlights, horns, buzzers, alarm bells and the like.

**CONTROL PANEL**
It is possible to switch on or switch off an alarm reporting system or report an alarm with a predetermined personalised specific numeric code. This process functions with a sound signal (buzzer or bleep).

Some panels function by using a pass, a smart key or a swipe card and a card reader.

A door can be opened electronically as well by means of a control panel (numeric code).

**THE MOST FREQUENTLY OCCURRING RISKS**

1. Secretly “looking” while the code is entered in order to decipher it.
2. Loss of personal belongings as a result of which the code comes into possession of unauthorised persons.
3. People passing each other a code.
4. Not changing a numeric code on time. A general numeric code (intended to open a door) should be changed at regular intervals in order to avoid general use of that code.

5. The control panel will get dirty in time and if the same code is used frequently, the combination of figures can be “guessed”.

**Signal Box**

The technicians will call this the alarm centre. By this term, we do not refer to the private alarm/emergency centre.

This box, equipped with electronics, lamps and an automatic telephone dialler will immediately warn the pre-programmed telephone number and will pass on a code.

**Permanent and Dial-in Connections**

If the connection between the signal box on the location is directly linked to the private emergency centre, this is called a permanent connection. This is an effective, safe connection which can be monitored permanently by means of electronic signals. These reports will be sent on immediately to a private emergency centre or a permanently manned post. Sabotage and/or interruption of the connection will be noticed at once.

In case of a dial-in connection, the alarm signals are reported by a so-called automatic telephone dialler.

This dialler ensures that a connection (test report) is established with the security computer on the emergency centre at least once per 24 hours. This way, it is checked if the connection is still intact.

The telephone line is the weak link of a dial-in connection. If the connection is interrupted because the cable is being sabotaged, dug up or destroyed, then the alarm signal can not be reported anymore. That is the reason why the switch boxes of the PTT are especially secured.

**Alarm Verification**

Unnecessary involvement (asking for assistance) of the police can be prevented by the application of a small video camera or microphone next to a detector.

At the same time the alarm signal goes off, an image and/or sound will be transmitted to the private emergency centre. There personnel will then be able to observe directly what has caused the alarm to go off. It is also possible on the emergency centre to “listen in.”

This “listening in” is commonly used in case older people are involved (social alarming).

**Uploading and Downloading**

It is possible to upload or download (changed or new) information into the burglar alarm system. Altered closing times for instance can be passed on to the security computer with a code by the operator directly. The technician could, with a code of course, establish a connection from a distance quite easily. He is then able to observe the status of the system and can correct disturbances from a distance.

**2.5 Alarm Receipt – Processing Systems**

(Alarm) reports are received on a central location and should be supervised and processed. These reports can be received on several manners. Reports that are sent electronically are usually processed and automatically filed in a security computer.

“How to act” and “who to call” will automatically appear on the screen.

It is even possible to show drawings on which the location of the alarm is indicated.

**2.6 Interior Security Systems**

**Active Infrared Beam Detector**

An invisible infrared beam is transmitted across a specific distance from a sender to a receiver. If this beam is interrupted by something or someone, then contact is made in the receiver.
**Door- or window contact**
This device consists of two parts, one applied on or in the door and one on or in the groove. If a door or window is opened, contact between the two is broken and an alarm is then activated.

**Vibration contact**
This device can be placed on a window or a wall. If this connection is disrupted or if vibrations are detected, the burglar emergency centre will be activated.
In case these devices are applied on a window, they are also called broken glass detectors.

**Passive infrared detector**
This device can only detect movement or relocation of infrared energy through an infrared sensitive measuring head, radiated for instance by a human being.

The detector is called ‘passive’ because it can only receive information and does not transmit anything.

**Radar detector**
This detector has limitations in use because radar beams pass through certain materials, for instance glass and wood. In the detector, transmitter and receiver are assembled in one unit.

The transmitter transmits the signal and via floors and walls this is reflected towards the receiver in a specific pattern. If something moves within that space, the signal is disrupted and the contact will be switched on.

**Ultrasonic detector**
This detector functions the same as the radar detector, however on a lower frequency. These radar beams do not pass through certain materials.

**Dual detector**
Two detectors with different functions are assembled in one unit. One detector checks the other detector. An alarm signal is only passed on if both types of detectors notice an alarm. As a result of these detectors, the amount of unwanted alarms is reduced considerably.

If entering specific premises or approaching an object should be detected, then we refer to an exterior security systems.

**2.7 EXTERIOR SECURITY SYSTEMS**

**Active infrared beam detection**
Two or more poles of about two meters in height are placed at a certain distance from each other. In one pole several infrared transmitters are placed and in the other several infrared receivers. This way, a sort of invisible screen is created. In case two or more beams are interrupted, then an alarm will go off.

**Radar beam detection**
A transmitter and a receiver will be placed at a certain distance from each other. The sender transmits an invisible field in the shape of a cigar in the direction of the receiver.

**Fence detection**
Detectors will be placed at a short distance from each other against the fence that are sensitive to the vibrations of that fence and subsequently pass on an alarm signal.
Through, or in, the fence, wiring is placed or twined. An alarm signal will be passed on after disruption of the wiring or in case a certain mechanical tension is detected on the wire.

Seismic detection

Detectors are positioned closely together under the ground. A walking person can be recognised by these detectors by means of the produced vibrations.

Another system can also detect the difference in pressure on the ground. A pressure cable will then measure the difference in pressure.

An electromagnetic field can be created underground electronically. In case of disturbance of that field, an alarm will be set off.

Thin fibre optics cables that are incorporated in the wires of a fence prevent the fence from being cut through unnoticed. A ray of light running through the fibre optics cable is interrupted during the process of cutting through and an alarm signal will follow.

2.8. CLOSED CIRCUIT TELEVISION (CCTV)

CCTV is a system with (rotating / tilting) cameras and a monitor to enable a security guard to observe the access roads, the premises, the fencing, sheds, cranes, the waterside and ships from a distance.

The position of these cameras is very important:

- A camera will not function properly if the camera is pointed towards a source of light. (It is recommended to position the camera underneath a source of light).
- The vision of the camera should not be obstructed by trees, sheds or cargo.
- In case more cameras are placed, the overlapping of the range of vision should be taken into account.

Recording of data is usually performed by a computer. A back-up of this information should be performed at regular intervals.

2.9. MEANS OF COMMUNICATION (MEANS OF CONNECTION)

Telephone

The telephone is a commonly accepted and well-known means of connection.

GSM (Mobile phone)

The GSM is a commonly accepted and well-known means of communication.

Hotline

A hotline is a permanent connection. Connections to emergency services often are established through a permanent connection; a so-called hotline. Lifting up the receiver is enough to establish the connection.

Telephone dialler

A telephone dialler is activated for instance as soon as a burglar alarm goes off. The telephone dialler will dial a predetermined programmed number and will report a code to a computer or will reproduce a spoken text as soon as the receiver is picked up.

Sound system

On premises or in a building, a number of loudspeakers are positioned that are connected to a repeater and an operating point. Messages or announcements can then be broadcast. During the evacuations of large buildings, instructions (if necessary per floor) can be passed on.

Intercom

An intercom consists of a cable connection between two fixed mounted appliances (units). If a button is pressed, then a connection will be established. Through the loudspeaker, one can hear the other side (for instance security).
Disadvantage
This is no safe connection because everybody can listen in.

Megaphone
A megaphone is a device to reach large groups of people or someone at a big distance. The sound of a voice is being reinforced.

Radiotelephone
A radiotelephone is a fixed device in a means of transport that contains a sender as well as a receiver. Communication can take place wireless with a central post (permanent set-up). The distance across one can communicate with the central post is approximately 10 km, dependent on the area (degree of buildings, bridges etc.). The distance of a connection can amount to 25 km from the central post. Discipline is important during the process of communication with radiotelephones because you can not speak at the same time. You will have to wait until the other person is finished. A specific procedure with regard to communication is therefore followed.

Disadvantage
Confidential information can easily be overheard with a scanner.

Portable radio
A portable radio is practical device that can easily be transported. It works the same as a radiotelephone. The range is approximately one up to four kilometres.

Call up or Tracing system (system for searching persons)
A call-up or tracing system is a device with an operating post and a number of call-up receivers within a company.

The call-up receivers will be carried along during working hours within the company and will be handed in at the end of their working activities.

Alarm receiver
An alarm receiver is a handy-sized small device with which the carrier can receive alarm signals. It can receive certain spoken messages and/or light or led signals. It is not possible to talk back. The range of the central post to the alarm receiver amounts to four to seven kilometres. (In principle, these devices are only available for governmental services).

Pager
A pager is a portable device with which code signals can be received. Via the telephone one dials the pager number of the company, followed by a predetermined number. On the pager, the predetermined code appears accompanied by an attention signal.

The person carrying the pager knows what to do or what telephone number to call based on this predetermined code.

Computer
With a computer, it is possible to fax, receive messages and answer messages, send codes to pagers and establish connections with other people on the Internet with pictures and sound. The security computers and monitors receive alarms and file all kinds of information as well.

2.10 Metal Detectors and Scanners
Manual detector
A manual detector is a device that, if switched on, will produce an acoustic sound if metal is approached.

A manual detector can be used during the process of inspecting individuals, hand-luggage, etc.
 ters, packages, weapons, weapon components, ammunition and explosives that are hidden in a metal casing.

**Metal detector (permanent set-up)**
A metal detector is a kind of gate in a permanent set-up. Persons can only gain access if they pass that metal detector.

It is suitable for checking persons that could carry metal objects such as weapons, ammunition, tools or similar instruments along in their clothing or on their body.
The metal detector will transmit an acoustic sound if metal is detected.

**X-ray scans (hand) luggage**
The function of this device is based on performing an X-ray scan on luggage. These kinds of substances are made visible on the screen with a specific colour (for example organic substances will become orange).

**X-ray scan permanent set-up**
The X-ray scan with a permanent set-up is intended for containers, trucks, pallets etc. It functions based on the X-raying of goods and materials. People may be X-rayed for medical purposes only.

2.11 ACCESS CONTROL SYSTEMS

**Means of identification**
With ‘means of identification’ we refer to the various possibilities with which a person can prove that he is allowed to enter a port facility or a location. There is a large variety in means of identification.
Key-cards
The regular staff, or personnel that are hired on a regular basis, will be distributed with a key-card at the commencement of their employment on a port facility.

The key-card is the most frequently used means of identification. It looks like a little banker’s card. The backside of the card is equipped with a magnetic strip with a code. The magnetic strip can also file a photograph.

The card is swiped through a reader (see under reader equipment) at the entrance during which the code is checked by the system. Subsequently, the system will grant access. The entrance times can be programmed. A time registration can be linked to this system.

The regular staff, or personnel that are hired on a regular basis, will be distributed with a key-card at the commencement of their employment on a port facility.

The key-card is the most frequently used means of identification. It looks like a little banker’s card. The backside of the card is equipped with a magnetic strip with a code. The magnetic strip can also file a photograph.

The card is swiped through a reader (see under reader equipment) at the entrance during which the code is checked by the system. Subsequently, the system will grant access. The entrance times can be programmed. A time registration can be linked to this system.

Key with code
A key with a code is a sender with a code in the shape of a little stick on a key ring, a smart-key. The system is switched off and/or the door is opened if this key with code (sender) is held in the immediate vicinity of the receiver or the access panel.

Next to this type of access control, it is also possible to deploy the photo recognition through a reader- or computer systems, voice recognition, iris scan, fingerprint, palm print, signature etc.

In some cases, a visible colour code and/or a passport photo on a tag are used. This tag, which can contain an electronic code, is then called “badge” and is, in most cases, checked visually.

Reader equipment (readers)
Readers can understand the code, sometimes accompanied by a photo and extensive data that are programmed in the means of identification.

Some means of identification should be held against the reader and others have to be swiped through a slot or inserted into a slot. Certain means of identification already function at a distance of one meter.

2.12 VIDEO TRANSMISSION THROUGH TELEPHONE LINES (INTERNET)
At a large distance, it is possible to observe images taped by a video camera through a dial-in telephone line. The images will then enter as pictures one by one on the monitor. The sender is directly linked onto the telephone network.

Digidown look
By using cameras and a monitor, supervision can take place on locations directed from an emergency centre (central emergency room). A digital connection is established through a telephone line and a sender or a LAN connection through the Internet.

Cameras with movement detection are utilised as well. After detection of movement, an automatic connection is established with for instance the emergency centre. The security computer of the emergency centre will subsequently transmit an acoustic signal and the monitor will then produce images of the location where movement was detected.

A connection can also be established in the emergency centre and look at the location directly. The images are recorded and filed into a computer.

2.13 DISADVANTAGES OF ELECTRONIC MEANS
A. Limitation of examination, inspection and checking possibilities:
If the entrances and exits of a building, premises or environment are guarded by certain means (from a distance) by a port security officer, then he can only perform inspections or an examination in exceptional cases.

During the upgrade of the security level of a port facility (for instance from security level 1 to security level 2) an inspection or examination is not possible because of other priorities and additional security guards will then have to be employed.

2 Local Area Network
B. Broken down electronic means

If electronic means break down, this will affect the quality of the security.
As a result of broken down means (of security), the normal, at that moment valid security level, can not be reached.

In that case, the Port Facility Security Officer (PFSO) must be warned immediately. (Examples of situations in which the PFSO should be warned are defects in equipment that must detect burglary or fires, computers, communication equipment or CCTV’s and so on).

The first reaction on a disruption of electronic means must be executed by the security officer himself. He should have learned these procedures. In the regulations of the location, these procedures should be incorporated.

A rapid reaction is necessary if certain means are broken down. A 24-hour service of a fault-clearing organisation (internal or external service) is essential.

As a result of broken down electronic means, the current security levels on a port facility can not be maintained. In most cases, this can be compensated by the activation of additional personnel. Certain agreements will have to be formulated to have sufficient security personnel available should the above-mentioned situation occur. The defect must be repaired as soon as possible.

In case of explosions, calamities, fire or technical disturbances it is possible that the power supply will break down.

In case the power supply will break down, the emergency power supply will bring relief. It is then of the utmost importance that certain means of security keep functioning to be able to execute the alarm procedures. The reaction on a calamity will then be performed more rapidly, so that the calamity will be limited or solved sooner.

False alarms

It is quite common that fire- and burglar detector systems produce unnecessary alarms. There is nothing wrong with the quality of the equipment. Most of the time, other reasons are the cause of these false or unnecessary alarms. This could be caused by the improper application of detectors or the wrong choice of detectors.

If false or unnecessary alarms occur frequently, then this will affect the motivation of the security guard in a negative way. (“Again this same alarm, it is probably a false alarm again!”)
It should be determined in a procedure when and who will ask for technical support.

2.14. SUMMARY OF CHAPTER 2

Electronic security equipment is a device that mainly consists of an electronic circuit or electronic parts on the inside.
The term “alarm or emergency centre” can be explained in two ways. The technician will refer to the alarm or emergency centre as a “switchbox”. However, the security officer will refer to the alarm or emergency centre as the central post of his duty or a private emergency centre as mentioned in the Dutch Act on Private Security Companies and criminal investigation departments.

Detection systems are used for:
- Fire detection
- Burglar alarms
- Technical detection
- Water – or humidity detection

Here are systems to detect / signal and systems to report and file these signals electronically. These systems are interconnected. The signals are automatically conveyed to a permanently manned post.
If a system is installed that should prevent someone from entering a building, then we refer to this system as an interior security system. If entering premises or approaching an object should be detected, then we refer to the system as an exterior security system.

A (port) security officer will have to use/operate the means of security made available to him so that he can execute the first activities after a breakdown. He should be made familiar with the operation and user possibilities of the means and procedures his company is utilising. How these means should be used in his daily routines should be described in his regulations. It is therefore essential that the function, arrangement, range and limitations of those electronic means are familiar to him.

If electronic means of security break down, this will affect the quality of the security. The desirable security level can not be achieved. Immediate contact should be established with the Port Facility Security Officer (PFSO).

False or unnecessary alarms that occur quite frequently should be reported.

2.15. QUESTIONS AND EXERCISES

2.15.1. Questions

Question 1
Name four kinds of detection systems.

Question 2
What is the difference between an interior- and an exterior security system?

Question 3
Explain what a CCTV system is.

Question 4
What is the disadvantage of an intercom?

Question 5
Who is allowed to operate and/or restore the fire alarm centre in case of an automatic fire alarm?

Question 6
What are the disadvantages of a portable radio?

Question 7
For which purposes can a manual detector (metal detector) be used?

Question 8
Which means of identification are used on the port facility you are regularly employed at?

Question 9
What is a reader (reader equipment)?

Question 10
Describe why loss of power supply may only slightly influence the electronic means of security on the port facility according to the ISPS code.

2.15.2. Exercise Assignments

Exercise 1
During your working hours, the CCTV in the lodge of the port facility you are regularly employed at breaks down. Describe your actions according to the regulations.
Exercise 2
Explain why the security level can not remain on the desired level in case the electronic means of security break down.

Exercise 3
Describe which kinds of detectors are used on the port facility you are employed at.
3.1 CHECKING PERSONS

The purpose of the access control is to keep unauthorized people out.

One of the duties of the “port security officer” is (during the checking of persons) to inspect (existing and prescribed) security measures, visitors conditions and company regulations based on the ISPS code and other (European) legislation and instructions.

As already described in Chapter 1, security level 1, 2 or 3 is used.

The question is what a port security officer is allowed to do when he is searches persons. Or, in other words: what is the authority of the port security officer?

3.1.1 Competencies of the port security officer (with regard to checking / searching persons)

Certain competencies are attributed to the (port) security officer, for instance:

1. Asking questions to persons requesting access to the port facility (check if these persons are authorized to enter).
2. Checking the identity of the visitor based on identification documents, for example passports, driving licences, tickets, boarding passes, muster-books or checking by examining a crew list.
3. Verifying at certain departments if that person is expected.
4. Checking if people are allowed to be present on the port facility (or on certain areas or departments).
5. Paying attention to suspicious movements (both on the location as well as outside the fencing).
6. Watching suspicious goods during the process of granting access to the port facility.
7. Paying attention to suspicious goods during departure of the port facility.
8. Body-searching persons wishing to go aboard (which should be described in the PFSP and should also be explicitly approved by the government).
9. Inspections of persons on the port facility (both during entrance as well as during departure).
10. Checking transportation documents and supplies destined for ships.
11. Supervision on the maintenance of security measures.

The port security officer can only perform his task properly if he knows what to do on the working location and knows all procedures. On a port facility, multicoloured mixtures of persons are present. Below please find an enumeration of persons and possible ways of checking.

3.1.2 Personnel with a permanent appointment

Personnel with a permanent appointment on the port facility are, for the most part, in possession of a key-card. During working hours, they can quite easily gain access to the port facility or part of the port facility by using a key-card system with reader. Registration of time and presence...
can be kept up to date through the reader. They have an employment contract and are familiar with the company regulations of the port facility. During entrance and departure of the location, inspections / checks can take place in accordance with the company regulations and the ISPS.

3.1.3. Personnel for the ‘long term’
Some personnel are employed on a port facility for the “long-term.” Several companies have hired long-term personnel from other companies such as SHB etc. etc. In most cases, they are in possession of a key-card as well. We refer to “personnel with a permanent appointment” for further information.

3.1.4. Personnel of third parties
Examples of personnel of third parties who are employed by a port facility are security personnel, cleaners, service mechanics, maintenance personnel and personnel of a temporary employment agency. For most of these people, the regulations are not clear and with regard to security and safety, strict supervision should be maintained at all times. In order to gain access to the port facility, personnel of third parties must be known with security. Personnel must be announced in advance. There is no agreement between the port facility and the personnel of third parties. Third party personnel are usually not familiar with the valid regulations. The port facility should enter into a contract with the service organisation to ensure that the valid regulations are followed. The port security officer (hired security company) must have a contact person on the port facility he is employed at.

3.1.5. Persons wishing to go aboard
All persons wishing to go aboard will be checked by the port security officer on their identity and reasons for their visit (for instance assignment, passenger tickets, boarding passes and so on). Safe zones will be created in which examinations, inspections and body-searching of persons, searching their luggage, personal belongings, vehicles and their content can take place.

3.1.6. Visitors and suppliers
Visitors and suppliers of a port facility require special attention. Shippers, dispatch – and transport companies arrive in most cases with transport cars, trucks and so on at the gate of a company. It is essential that the activities of a company do not stagnate as a result of the check by security.

In the harbour area of Rotterdam, the CargoCard has been introduced. The driver of the dispatch company offers the CargoCard to a card reader on the port facility. The left palm of his hand will be scanned by a reader as well. The data of the palm of his hand have been filed on the CargoCard and will be compared electronically.

This system enables the truck driver to gain access to the location quite rapidly and without any delay. He then reports himself to the port facility at the cargo- or container counter.

The other visitors for instance: customs, the police, the pilots of the Pilotage Department, agents of the shipping industry, rowers of the Royal Rowing Club “Eendracht” (“Harmony”), the ship broker, the ship owner and provisioning companies with supplies, forklift trucks or laundry are all checked before they are allowed to enter the port facility. Governmental services can identify themselves with an appropriate pass.

1 Within the Rotterdam-Rijnmond region
Chapter 3 | Checking persons and goods/inspections

Port security officers and members of the personnel on a port facility are obliged to familiarize the visitors with the most elementary house regulations of the company. In the (petro) chemical industry, next to security, the issue of safety is emphasized. A visitor can not enter such a location without a security pass. First, he will have to watch a film about security and take a test.

Visitors can be accompanied and received in different ways.
- The port security officer will accompany the visitors on the facility or in a building (which will require additional manpower).
- The employee of the port facility expecting the visitor will pick this visitor up.
- Decoration of the reception room in the vicinity of the reception so that the visitor does not enter the port facility or the building.

The trend is that different kind of (port) facilities increasingly will have to deal with the care for safety and environment.

3.1.7. Handling of announced and unannounced visitors

Two kinds of visitors exist: announced and unannounced visitors. The “port security officer” must find out what the purpose of the visit is during a question and answer game that has to be executed in a most friendly manner.

If it is an unannounced visitor, then the port facility officer has to look at the admission most thoroughly.

If it is a curious person or if the port facility officer thinks this person wishes to explore the port facility, then he has to gather as much information as possible and report this to his PFSO.
- The port facility officer will pay attention to suspicious behaviour, suspicious goods and possibly the licence number and the description of that person.
- Access will be denied to that person at all times.

If the unannounced visitor is there for business and he may enter the premises of the port facility
with the permission of the management, then he will be checked. If the identity of that visitor and his vehicle correspond with the information provided, then he will then be treated as an unannounced visitor.

3.1.8. CHECK AND REGISTRATION OF IDENTITY

On a port facility, the port security officer will (in conformity with his regulations) verify and register the necessary information of the visitor in the current system used on that specific location.

It is a general rule that the visitor identifies himself with a general valid identification document (driving licence, passport or identity certificate).

In general, a computer programme is used for registration:

- Name and initial letters and possibly the address of the visitor
- Which company the visitor represents
- Purpose of the visit
- Parking place on the port facility
- Name of the person that is visited within the company
- Time of arrival
- Time of departure
- License number of the car which is parked on the premises

During this check one could consider:
- Check and registration of the passport (generally accepted)
- Check and registration of the driving licence (generally accepted)
- Checking passes distributed by the government (for instance police)
- Check and registration of the license number
- Check based on the muster-book and the list of crew members

Registration of presence is also important to check who is present (on which place) on the premises in case of a calamity. In case of an evacuation procedure, those persons can not be forgotten. A company is in possession of a company emergency plan / calamity plan in which the procedure of an evacuation is described.

3.2. SEARCHING (INSPECTION AND BODY-SEARCHING) OF PERSONS

Every company has to deal with a large flow of incoming and outgoing goods. Goods are purchased, repositioned, stored and transported elsewhere. The business interest will benefit from a strict supervision on the flows of incoming and outgoing goods. Different groups of people are importing and exporting these goods.

PERSONNEL IN GENERAL

All personnel are daily transporting all kinds of bags, rucksacks, suitcases and vehicles to work. In some companies, internal theft of company properties is a frequently recurring event. Employees have the disposal of so-called lockers in which the goods that are brought along to work can be stored. To prevent theft, persons can be inspected during entering and departure of the port facility as described in the ISPS code and the company regulations.

PERSONNEL OF THIRD PARTIES AND VISITORS

Employees of third parties, visitors, passengers and suppliers of the ship’s provisions, laundry, repair mechanics and maintenance companies etc., etc., should identify themselves and they should be announced in advance. Inspection before entering the port facility is necessary in order to maintain the standard security level.
Chapter 3 | Checking persons and goods/inspections

**Passengers, crew and persons wishing to go aboard**

The SSP should contain security measures that are supposed to guard the access to the ship (ISPS code, part B, art. 19.14).

The ship should take care of the following items in cooperation with the port facility:

- The identity of all persons wishing to go aboard and their reasons for wanting to go aboard will be checked (for instance assignment, passenger tickets, boarding pass and so on).
- Safe zones will be created in which examinations, inspections and body-searching of persons, searching through their luggage, personal belongings, trucks and their content, can take place.
- Vehicles, destined for roll-on/roll-off ships, ships for the transportation of cars and passenger ships should be inspected before embarkation.
- Persons with luggage, who have already been inspected, should be kept separated from persons with personal belongings who have not been checked yet.
- Embarking and disembarking passengers should be kept separated.
- Access roads to the ship will be guarded / secured in order to deny access to unauthorized people.

**3.2.1. Inspection and methods of checking (security level 1 – normal)**

Inspection / checking will take place in a special designated place if people, goods and their luggage enter the port facility and at random if people depart. Inspection is described in the company rules and regulations.

Special attention should be paid to:

- The cargo, in particular dangerous goods or dangerous substances
- The ship’s provisions
- Check of the cargo documents
- Check of seals
- Smuggling of weapons or equipment, including weapons of mass destruction
- Use of a ship to transport persons wishing to cause an incident
- Use of a ship as weapon or means to cause damage or destruction
- Unauthorized access to the ship
- Stowaways

**Inspection of persons (with luggage and vehicle) could take place in the following ways:**

- Inspection of a person (visually, with a scanner on a permanent set-up, manual scanner and/or with a dog)
- Examination of luggage (visually, physically, x-ray scanner and dogs)
- Inspection of the vehicle with cargo (visually and physically, with a scanner on a permanent set-up and with dogs).

**3.2.2. Body-searching (ISPS Code, Part B, art. 9.15.)**

Even on security level 1, all persons wishing to gain access to the ship could be exposed to body-searching or inspection.

The frequency of this body-searching or inspection should be described in an approved PFSP and should explicitly be approved by the government.

This should be a condition with regard to entering the facility and the ship.

If body-searching is not allowed, then access to the facility (and as a consequence the ship) will be denied. The PFSO should be informed about this immediately. The body-searching should preferably be executed by the port facility in close cooperation with the ship and in the immediate vicinity of the ship.

Unless specific security reasons exist, it can not be expected from the crew that they are body-searching their colleagues or their personal belongings.
3.3. INSPECTION OF MOVEMENT OF GOODS

3.3.1. ROUTINE CHECK OF THE CARGO (SECURITY LEVEL 1 – NORMAL)

In general, the cargo is not checked by the security of the port facility

- Check the cargo based on the cargo documents
- Check and register the license number of the truck and trailer
- Check and register the identity certificate of the driver
- Watch the driver and his substitute-driver (entrance check)

In case of a sealed container:

- Check the entire container visually
- Check the sealing of the containers based on the cargo documents
- Check and register the license number of the truck and trailer
- Check and register the identity certificate of the driver
- Watch the driver and his substitute-driver (entrance check)

3.3.2. CHECKING THE COMPANY SEALS (WHICH SHOULD AVOID TAMPERING WITH THE CARGO)

In order to open a container, this pinlock should be cut or the seal has to be broken. The number on the pin and the lock-up part are the same and should be similar to the number mentioned on the cargo documents.

Pay attention to the following aspects:

- Seals could be broken and sealed again.
- Numbering on the seal should be identical to the number on the cargo documents
- Seals should be positioned on the correct container door (right door)

Very advanced systems exist, for instance an electronic seal of Smart and Secure Tradelanes (SST).

This seal can be followed electronically world-wide and if this seal is broken, this will be reported immediately through a satellite to a connected emergency room.

If a familiar shipper will provide the container with an electronic seal after loading, then the container will receive preferential treatment in the United States of America.

Several seals exist, fabricated from different materials for instance plastic and metal.
3.3.3. The ship’s provisions

The amount of the ship’s provisions should be identical with the cargo documents (order).

- Never accept too much ship’s provisions
- Pay special attention to damaged packages and tampering with packages
- The ship’s provisions should be stowed aboard immediately.

Checking the ship’s provisions could take place in the following way:
1. By visual and physical inspection of the cargo and the vehicle
2. Use of scanners, detectors, mechanical equipment or with dogs

(Pay attention to the attitude and behaviour of the driver and possible substitute-driver)

3.3.4. Gate of Access Control

Another current system on port facilities is photographing the delivered combination. The truck and trailer, inclusive of container, are photographed from all sides. This photo will also include the license number of the truck and trailer (semitrailer). The driver is obliged to submit his driving licence or identification certificate and to let it be copied. Identification of container, truck and driver is part of the planning and operations of the terminal.

3.3.5. Tracking and tracing

Another new system that is used in the transportation industry is ‘tracking and tracing’. Planning of routes, transportation management, locations, two-way data communication and alarms can be attended to by a computer programme and relay stations or satellites.

With these tools, it is quite easy to follow a unit (container) that has been provided with a sender/receiver applied on a secret place. The unit can also be placed into a watch-box (fixed position). If that container is moved, the emergency centre will be alerted.

3.3.6. Scanning on the presence of radioactive material
On some port facilities, vehicles and their cargo are scanned on the presence of radioactive material. The permitted dose has been programmed in advance. In case the dose is too high, access to the premises will be denied. Regulations for the operation of the equipment and access to the facility are present on that specific location.

3.4. SUMMARY OF CHAPTER 3
The port security officer is working according his specific regulations. In these regulations, his authorities are clearly described. He is allowed to perform inspections and, if it is legally explicitly allowed, even execute body-searching.

He has to deal with different kinds of personnel, own (permanent) employees, “long-term” personnel, personnel of third parties, visitors, suppliers, passengers and crewmembers and governmental personnel.

In most cases, visitors arriving at the port facility are announced in advance. Occasionally, visitors arrive unannounced. This situation requires special attentiveness.

If the visitor is there for a ship that is moored at his facility, then the port security officer will exactly know what to do based on his regulations. In these regulations, it is described when and how he may allow this person to enter the facility. He also realises that he has to contact the PFSO if that person refuses to identify himself.

Entrance checks (including the check of the immediate vicinity) and registration of persons and goods with advanced means must be performed in a constant manner and very precise.

When the port security officer is checking the cargo, he will do so based on the cargo documents. He will note the numbers of the containers and seals and will copy the identity document of the driver. The license number of truck and trailer (semitrailer) will be recorded as well.

Checking the ship’s provision is a procedure that is described in his regulations. After a correct check of the supplies based on the order, paying attention to the correct amounts, shortages and/or damages, the information of the driver and the substitute driver are recorded. These provisions are stowed aboard directly in accordance with the procedure.

A port security officer has knowledge of the modern commonly used (cargo) means of security on the port facilities; has knowledge of the cargo checks and is able to take the appropriate measures during the procedure of admitting persons or movement of goods.

3.5. QUESTIONS AND EXERCISES

3.5.1. Questions

Question 1
A van with eight cleaners is requiring access to the port facility. It is a well-known company for you. What are the proceedings on your location? Is this in compliance with the valid ISPS code?

Question 2
How is an unannounced visitor treated on the port facility you are employed at?

Question 3
A driver is delivering supplies to the port facility. Describe your actions.

Question 4
What aspects do you pay attention to if you are checking a sealed container?
Question 5
A person is requesting access to the port facility in order to visit a ship operating on security level 1.
What are your actions?

Question 6
How are employees of third parties checked?

Question 7
How is an unannounced visitor accompanied?

Question 8
On the access road to the port facility you are employed at, a car has been parked suspiciously for a considerable amount of time. What are your actions?

Question 9
Which modern developments in the cargo security can you name?

Question 10
A driver is not in possession of a driving licence or identity card. He claims to have lost his wallet. Describe your actions.

3.5.2. Exercise Assignments

Exercise 1
Describe a modern security system that is used on the port facility you are employed at.

Exercise 2
Describe which information is present about inspections in your company rules and regulations.

Exercise 3
Fill in an entrance form for an unannounced visitor of the port facility where you are employed at. Make a copy of a visitor’s list.
Chapter 4 | Security plan / PFSP / Corporate policy

INTRODUCTION

Doing business means running risks.

We experience commercial risks (risks at procurements, production, stock control, money exchange, storage, distribution, etc.) and we act on their occurrence.

Moreover, every day an entrepreneur runs other risks as well, e.g. risks as a result of a criminal act.

It is very difficult to cope with these risks by abiding the law or by insurance.

Proper security management is an answer to those risks.

Adjusting corporate processes as well as the commercial process may be done in the progress of the process involved or at a later date.

However, in most cases the consequence of risks as a result of a criminal act will be noted to late and it will be difficult to correct it.

As a result of a risk analysis, the follow up by security measures and procedures will reduce the crime induced risks to an acceptable level.

Procedures required by the ISPS code will be documented in the Port Facility Security Plan, and complement already existing security procedures.

1. Procedure on Organization and execution of security tasks at the Port Facility
2. (Additional security measures when raising the security level)
3. Procedure for Communications and raising the alarm
4. (Communication between the Port Facility Security Officer – PFSo – and the Ship Security Officer / company Security Officer and the Competent Authority)
5. Procedure for Access to the port facility
6. Procedure for Areas with no or restricted access
7. (Execution and control of no or restricted areas)
8. Procedure for Monitoring the port facility
9. (Instructions and measures to protect effective supervision)
10. Procedure for Cargo handling
11. (Protecting cargo security)
12. Procedure for Delivery of ship’s stores
13. (Instructions and measures preventing tampering with ship’s stores)
14. Procedure for Unaccompanied baggage
15. (Preventing access of undesired luggage)
16. Procedure for Checking and modifying the Port Facility Security Plan
17. (Documenting the evaluation (and its corrective measures) of the Port Facility Security Plan – education and training of security personnel inclusive).

Each and every company has its own ‘house rules’.

These rules differ from company to company due to differences in nature (product) as well as culture. Often, house rules are a product of negotiations between management and union.

4.1. SECURITY PLAN

A security plan may be composed of various measures. Those measures may be grouped.

- Organizational measures covering:
  - All processes and security measures, responsibilities and authority of all employees, written procedures describing the handling of security equipment, interaction with personnel, key plan, access control, password and its protection, data and information security, the encouragement of the corporate culture with regard to criminality, etc.

- Physical measures covering:
  - Fastenings, fences, locks, lockers, glass (windows), climbing prevention measures, construction materials, openings in roofs, etc.

- Electronic devices
  - Burglar detection, failure and fire detection devices, hijack alarm, camera’s, connection to alarm centres, protecting of data, etc.
4.1.1 Inventory of risks induced by crime

A. Corporate processes and procedures

When loading, discharging and transport cargo may be stolen.

When transporting goods, you may be exposed to document fraud or falsifications or smuggling (with ferries: people!). When the commodities are in storage, risks may be theft, fire, burglary and explosions. When stuffing and stripping of containers theft is a risk.

Documents and its administration are liable to fraud, corruption and falsification.

Transport of passengers is sensitive to a terrorist threat.

B. Personnel

Fraud and criminal behaviour often originates from within the company.

When employees show criminal behaviour, colleagues may progressively join them (snowballing). It appears to them, that this behaviour is sanctioned by the management by the lack of response.

C. Finance

Authorisation of employees and management is an important issue. The policy on reimbursing expenses must be crystal clear. Control is a requirement.

D. Information and automation

Information circulates in varying degrees of confidentiality.

Procedures must be in place to document distribution.

Software to enable security on areas and workstations processing confidential data. The same applies to all information carriers like pc’s and laptops, containing confidential information.

Entry passwords must be changed regularly.

E-mail and internet connections must be protected.
E. Corporate assets

Corporate premises (plot), offices and other buildings.
Access control is governed by an active attitude on control and applying the documented standing orders and instructions. All employees and people requiring access must be informed on the access requirements.

To safeguard the corporate premises, it is advisable to install a fence with a safeguard to prevent climbing, with a height of 2.50 meters. Detection equipment to detect intruders is advisable as well.

Regular control of the complete fence is essential. Be sure that one inward- or exit gate is constructed as a sliding gate or chain link rolling gate.

Use cameras with movement detection coupled to a time laps recorder.

Utilize state of the art technology, like (smart) card readers coupled to barriers.

Visitors must report and comply with all access control requirements, escorting inclusive. Escort must be both ways!

To protect offices, it is important to have a key plan addressing locations and lock type and someone in charge on issue and reception of keys.

A proper administration is a requirement addressing the whereabouts of the keys: registration of persons possessing key, whether continuous or temporarily.

Check regularly, whether the administration is correct.

In this respect, card readers, cameras and time laps recorder can be used. It is extremely important to know who is on the premises and where he is at certain moments. Not just for security, for safety reasons as well.

Restricted and no access areas must be marked. These areas are prohibited to non authorized persons. The security lodge is such an area.

With most cases of internal fraud, there is a direct relation between function and perpetrator. A person, who is employed at a certain department, is aware of its vulnerabilities!

4.1.2. Drafting of a Security Plan

The security policy, as part of the corporate policy, is the responsibility of the board of directors, the management.

The first step is to assess all corporate security risks. The next step is to evaluate these risks on their priority and severity, their consequence.

The board of directors decide on the strategy to deal with the risks found.

Risks can be covered in several ways:

- Avoidance – if you avoid certain activities, you eliminate exposures to potential losses. However, in the real world, avoidance is rarely practical, which leads to the following:
- Loss Control – Loss Control or Loss Prevention is based on techniques to reduce the ‘probability’ or ‘frequency’ with which certain losses might occur.
- Retention – simply means that a business retains the financial consequences of a loss, whether intentionally or unintentionally.
- Contractual Risk Transfer – occurs when one business obtains a contractual promise from another entity to pay for any losses that might occur. The best example of this situation is ‘hold harmless agreement’ between a landlord and a tenant. The landlord contractually transfers any loss exposures to the tenant for use of the landlord’s premises.
- Insurance – ironically, the last risk management technique to be considered is insurance, in that it is the most expensive initiative in comparison to the previous four techniques, and therefore is the last consideration. It is important to note that many loss exposures identified are not economically possible to counter with the previous techniques, and therefore, insurance is quite necessary.
- Diminish risks – secure; a mixture of the above-mentioned risk-reducing measures.

Naturally, the basis of this should be a systematic approach which has been incorporated in the company’s vision / mission statement / business plan: policy.

After the management has decided on how to curb the risks, a security plan is drafted.
4.2. PORT FACILITY SECURITY PLAN (PFSP) (A POSSIBLE ENHANCEMENT OF THE EXISTING SECURITY PLAN)

4.2.1 OUTLINE OF VULNERABLE CORPORATE ASSETS AND INFRASTRUCTURE

The Port Facility incorporates in its security plan a topographical lay out of its premises. All vulnerable assets and infrastructure are marked.

Assets and infrastructure that should be considered important to protect may include:

- accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;
- cargo facilities, terminals, storage areas, and cargo handling equipment;
- systems such as electrical distribution systems, radio and telecommunication system and computer systems and networks;
- power plants, cargo transfer piping, and water supplies;
- security and surveillance equipment and systems; and
- the waters adjacent to the port facility.

A satellite picture of the premises provides a clear overall picture.

4.2.2. DESCRIPTION OF A TERMINAL

The security plan describes the type of terminal it concerns.

In Rotterdam, the Netherlands, 9 categories are defined:

- Container terminals
- Wet bulk terminals, food
- Wet bulk terminals, non food
- Dry bulk terminals, food
- Dry bulk terminals, non food
- Ro-Ro terminals and passengers terminals
- General cargo terminals, food
- General cargo terminals, non food
- Shipbuilding yards

4.2.3 ORGANISATION AND EXECUTION OF SECURITY TASKS EXECUTED BY THE SECURITY ORGANISATION

Government stipulate the requirements a security organization of a port facility must meet. To start with, adequate knowledge and expertise is a first and obvious requirement.

Secondly, there must be no misunderstanding on tasks and duties of the security organization: a clear and precise document outlining and defining the scope and depth of the tasks and duties; which must be properly communicated.

Lastly, the structure (organization) of the security organization and its interaction with local and regional / national authorities must be precise and documented.

The Port Facility has appointed a Port Facility Security Officer (PFSO).

The PFSO manages a qualified security organization (within its own organization or from an outside company) to execute all security tasks and duties as stipulated in the ISPS code level 1 to 3.

Handbook security (procedures and instructions)

The port facility must define and maintain a Handbook Security, or a coherent set of security procedures and instructions.

The following matters must be addressed:

- Security tasks, assigned to other personnel
- Measures taken in case of a raise in security level to level 2 or 3
- Whether the security organization utilizes its own vehicles
- The procedure to log security incidents.

4.2.4 ORGANISATION OF COMMUNICATION BETWEEN THE PORT FACILITY SECURITY OFFICER, THE SHIP SECURITY OFFICER (COMPANY SECURITY OFFICER) AND THE COMPETENT AUTHORITY

The measures taken with regard to communication and alarm regulate:

- Agreements between port facility and vessel on cooperation on security, especially in case of a threat or crisis
Chapter 4 | Security plan / PFSP / Corporate policy

- The availability of an alarm- (emergency response) and security plan of the port facility in case of a threat or calamity
- Prevention of disruption of communication systems at the port facility premises and to guarantee the continuity of communication between port facility and vessel as well as to guarantee the accessibility to external and internal rescue or assistance units.

Procedure communication vessel – port facility
The port facility must have a procedure regulating the communication between vessel and port facility on cooperation regarding communication and alarm (emergency response).

Alarm / emergency response and evacuation scheme.
Every port facility as defined by the ISPS code must have a company emergency response plan to deal with emergencies. Interaction with other, existing plans, is allowed.

Means of communication
Whenever at times of emergency communication fails, internal and-or external emergency assistance will not be accessible with a possible disastrous result.

The port facility must describe in its rules/regulations:
- Which means of communication may be available at times of distress
- The (emergency) powersupply available at the various security levels
- An actual overview of relevant telephone numbers of management and emergency response services
- The responsible employee tasked to maintain and update this list.

4.2.5. Policy on access control by the Port Facility
The security measures taken by the port facility must prevent unauthorized access to the port facility.

Access may be possible through:
- Waterways
- Roads
- Pedestrian walkway
- Railroads
- Quay walls / piers
- sewers
- Adjacent premises

Procedure access to the Port Faculty
The PFSP should establish the security measures covering all means of access to the port facility identified in the PFSA.

Perimeter fence and access.
The Port Facility:
- must be fenced off adequately by means of a sound and clearly visible fence or other means of barrier.
- must be able to monitor all means of access: both by land and by water
- must be equipped with sufficient lockable gates; all road access gates are safeguarded adequately.
- must, when a railroad is present, protect adequately the railroad access.
- must protect the access via the waterside adequately.
- must control on a regular base all fences and its access gates.

Identification and Registration
When requesting access to the facility, the identity must be ascertained of:
- Personnel
- Employees
• Contractors
• Passengers
• Visitors
• Drivers (all vehicles)
• Train driver / motorman
• Others (agents, suppliers, officials, etc.)

Without proper identification persons are not allowed to enter the port facility. As soon as an attempt has been made to circumvent the identification and registration procedures, the security guard reports this incident to the PFSO and other authorities when so instructed.

The Port Facility must separate the searched and non searched persons by defining and preparing dedicated areas.

The cause for requesting access of vehicles, trains and vessels must be verified before access will be granted or vessels will be allowed to dock.

Number / license plates of vehicles must be registered. When docking, the vessel will be checked on identity of vessel and / or owner.

The name of the vessel and / or owner concerned will be written down.

The following will be searched and inspected on a random scheme:
• Drivers (all vehicles) and their personal belongings
• Vehicles and the content / carriage of vehicles
• Train wagons and their content / carriage
• Vessels

Procedure shore leave crews
Crews of vessels moored along the premises have the right on shore leave. A procedure must be in place. Security personnel is allowed (at the moment) to use a copy of a, by stamp validated, crewlist.

4.2.6. NO- OR RESTRICTED AREAS (RESTRICTED AREAS WITHIN THE PORT FACILITY)
The purposes of the no- or restricted areas are:
• To protect the Port Facility
• to protect passengers, crews, port facility personnel and visitors (visitors to the vessel incl.)
• to protect vessels, using and serving the port facility
• to protect all strategically sensitive locations and areas within the port facility
• to protect the security and surveillance / monitoring equipment and systems
• to protect cargoes, ship stores and unaccompanied luggage from tampering

An overview of measures, to be implemented by the PFSO in connection with monitoring the port facility and its nearby approaches, on land and water; at all times, including the night hours and periods of limited visibility, the restricted areas within the port facility, the ships at the port facility and areas surrounding ships, are:
• a procedure describing the monitoring of the port facility
• illumination at the perimeter fence and partition fence of the no or restricted access areas
• the maintenance of the lightning equipment
• disruption of the illumination at power failure
• surveillance of the port facility by foot, bicycle or vehicle
• locations to be patrolled on the port facility premises

Surveillance or patrolling the premises has to be conducted .... times/ day at irregular times.
Deviances and shortcomings noted whilst patrolling to be reported in writing.
The surveillance routing must be verified (registered at intervals during patrolling).
Chapter 4 | Security plan / PFSP / Corporate policy

4.2.7. Cargo handling

Security measures in relation to cargo handling must:
- prevent tampering with cargoes
- prevent cargo that is not meant for carriage from being accepted and stored within the port facility
- to prevent enclosure of undesired matters whilst in temporary storage.

In the port facility security regulations/rules a procedure cargo handling must be documented. Agreements on searches between the Ship Security Officer and the regular shipper/transporters must be communicated or accepted/acknowledged by the Port Facility Security Officer. The PFSO has an up to date list of all cargoes and their locations at the facility, or has immediate access to it.

Document searches

A check must be executed on:
- the date of loading and the location of delivery (loading)
- the conformity of data on cargo- and delivery documents or other relevant cargo documents.

Cargo searches

Prior to access to the port facility, the cargo seals must be checked. When inspecting, scan equipment may be used.

4.2.8 Delivery of ship stores

The security measures relating to the delivery of ship’s stores should:
- ensure checking of ship’s stores and package integrity;
- prevent ship’s stores from being accepted without inspection;
- prevent tampering;
- prevent ship’s stores from being accepted unless ordered;
- ensure searching the delivery vehicle; and
- ensure escorting delivery vehicles within the port facility.

In the port facility security regulations/rules a procedure ship’s stores delivery must be documented.

There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship. Prior to delivery, the SSO and PFSO have drawn up an agreement on stores, date and time.

Searches of ship stores

A procedure must be implemented regarding the conditions and requirements of ship’s stores deliveries. It concerns vehicle, driver(s), searches, documents, date/time/location at the various security levels.

The vehicle and its driver(s) must be escorted and monitored whilst being on the port facility’s premises.

4.2.9 Handling unaccompanied luggage

Security measures in relation to unaccompanied luggage must:
- prevent tampering with the luggage
- grant access to accepted luggage only
- to prevent enclosure of undesired matters whilst in temporary storage
Procedure unaccompanied luggage
Access of unaccompanied luggage to the port facility will be denied.

4.2.10 Check and revision of the Port Facility Security Plan
The objective of the measures addressing the checking and revision of the Port Facility Plan is:
• to execute periodical inspections regarding effectiveness of the port facility security plan
• to document a procedure addressing the revision and amendment of the port facility security plan.
• to protect the port facility security plan against unauthorised use.

Periodical inspection, revision and adjustment
The PFSO has at his disposal an inspection protocol to inspect, review and adjust the Port Facility Security Plan.

Safeguarding of the Port Facility Security Plan
The PFSO must implement measures to protect the content of the PFSP (both printed as well as digital versions) adequately against misuse by unauthorised persons.

4.2.11 Education and training of security personnel
Port facility personnel having specific security duties should have knowledge and receive training, in some or all of the following, as appropriate:
• knowledge of current security threats and patterns;
• recognition and detection of weapons, dangerous substances and devices;
• recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
• techniques used to circumvent security measures;
• crowd management and control techniques;
• security related communications;
• operations of security equipment and systems;
• testing, calibration and maintenance of security equipment and systems;
• inspection, control, and monitoring techniques; and
• methods of physical searches of persons, personal effects, baggage, cargo, and ship’s stores.

To ensure the effective implementation of the provisions of the port facility security plan, drills should be conducted at least every three months unless the specific circumstances dictate otherwise. These drills should test individual elements of the plan.

Exercises and training as ordained may include participation of port facility security officers, in conjunction with relevant authorities of Contracting Governments, company security officers, or ship security officers, if available. These exercises and training, enhancing the quality of the PFSP, must be conducted at least once a year, with a maximal interval of 18 months.

4.3. Corporate policy
4.3.1 Company regulations and rules
Port Facility Security guards must have a good knowledge of the company he is employed by as well as a general understanding of the functioning of related external services, organisations or institutions. He must know who is in charge, its products or services, its organisation scheme, legal registration (limited, etc.) and eventual related branches. The Port Security guard must be versed in the current procedures or specific instructions of either ISPS code origin and/or originating from other instructions like handling mail or the registration of employees not able to come to work due to illness.

The Port Facility Security guard maintains a good relationship with both his colleagues and personnel of the facility as well as with external services: government, others).
4.4. SUMMARY OF CHAPTER 4

A security plan consists of organizational, physical and electronic measures and procedures. The effectiveness is determined by the motivation/attitude, expertise and risk awareness of the entrepreneur, management and employees.

Risks induced by crime may be classified as follows:
- corporate processes and procedures
- personnel
- finance
- information and automation
- premises, offices – buildings and equipment

In addition to the assets and infrastructure that should be considered important to protect the ISPS code lists specifically:
- accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;
- cargo facilities, terminals, storage areas, and cargo handling equipment;
- systems such as electrical distribution systems, radio and telecommunication system and computer systems and networks;
- power plants, cargo transfer piping, and water supplies;
- security and surveillance equipment and systems; and
- the waters adjacent to the port facility.

The Port Facility must have a Handbook Security, or a coherent set of security procedures and instructions.

A Port Facility security organization must meet the requirements as put down by their Government. Sufficient knowledge and expertise will be verified. The tasks and duties of the security organisation must be clearly defined, documented and communicated to all involved.

4.5. QUESTIONS AND EXERCISES

Question 1
Name three types of measures implemented in a security plan
- job descriptions, procedures, instructions
- organizational, physical and electronic measures
- personnel, access control, passwords
- intruder detection, fence detection, ditches

Question 2
What is the effectiveness of technical and constructional measures in reality?
- 20
- 50
- 80
- 90

Question 3
Who executes the security policy of a company?
- Chief Security
- Port Security Guard
- PFSO
- Director
Question 4
the procedure (ISPS code) on cargo handling contains measures to:
- provide the port security guard knowledge on the cargo
- prevent unauthorized carriage of cargoes
- prevent tampering or enclosure of unwanted matters
- provide good and efficient performance of the scan equipment

Question 5
What port facility security organization requirements are asked for by the Government?
- the organization consists of a minimum of 7 persons
- sufficient knowledge and expertise, clearly defined tasks, duties, structure and communication
- satellite photo and topographical map
- an external service

Question 6
What is the purpose of access control at the port facility?
- prevent unauthorized access
- control of fences and access gates
- protect the access via the waterside
- protect the access by railroads

Question 7
In how many ways will it be possible to obtain access to a port facility?
- Waterways and roads
- Pedestrian walkways and railroads
- Quay walls, piers, adjacent companies or constructions
- All mentioned access ways are correct

Question 8
An employee of a contracting company request access to the port facility. He is not able to identify himself properly (forgot his ID card). What do you do?
- Call the police
- Refuse access
- Call his boss and grant access
- Grant access

Question 9
Vulnerable/sensitive corporate assets as mentioned in the ISPS are, a.o.:
- accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;
- cargo facilities, terminals, storage areas, and cargo handling equipment;
- systems such as electrical distribution systems, radio and telecommunication system and computer systems and networks;
- All abovementioned facilities / installations are correct
5.1. EVASIVE ACTIONS AND DISTRACTIONS

5.1.1 Evasion of access control
When using an electronic access control system, a key card must be presented to the card reader. The gate opens, and you enter... with someone following you through. Most employees are not as aware of this security risk and even let you pass, politely, sometimes...
A friendly face, and a certain determinedness – showing that he belongs, is mostly sufficient to enter.

5.1.2. Unexplainable alarm (motion detection)
A port facility security guard must be extremely alert when confronted, at a facility equipped with perimeter defence (a partition or fence around the property) by means of cameras with motion detection, or other security sensors, with repeatedly recurrent alarm signals.

Do not automatically assume that it must be a system or equipment failure. The port facility security guard must research this phenomenon very carefully, before putting it aside as a malfunction. A professional criminal, intruder or terrorist researches his intended intrusion very carefully by collecting all relevant information to misled, jam or disable the security equipment. Based on his findings he will develop a strategy to enter.
As an example, he might try to activate the alarm several times in succession to test the security reaction.
Immediately afterwards, a professional will make his move to enter.
Be aware, that professionals are equipped with the latest technology, communication, transport. And mostly, they operate as a team.

5.1.3. Distraction of the attention
Many times a port facility security guard was distracted by an event happening just in front of his eyes. Afterwards, it appeared the event was created to distract the attention of the security guard, away from his monitoring equipment.

5.2. RECOGNITION OF IDENTITY DOCUMENTS

5.2.1. ID documents: from passports to ID cards
An identity document (also known as I.D. or ID) is a piece of documentation designed to verify aspects of a person’s identity. If an identity document is in the form of a small standard-sized card, such as an ISO 7810 card, it is called an identity card.

Information present on the document - or in a supporting database - might include the bearer’s full name, a portrait photo, age or birth date, address, an identification number, profession or rank, restrictions, and citizenship status.
New technologies could allow identity cards to contain biometric information, such as photographs, face, hand or iris measurements, or fingerprints.

5.2.2. Passports within the European Community
A passport is an official travel document that:
• allows an individual to leave and return to his/her country of citizenship and to facilitate travel from one country to another
• is issued by official sources and clearly "evidences the officially accepted identity and nationality of the bearer"
• is dependent for validity on the issuing government vouching for the person named in the document

Citizens of EU countries have a passport with a uniform design. This facilitates free movement, enhances security features but also serves to “strengthen the feeling among nationals of the Member States that they belong to the same Community”, as the EU resolution on passports puts it.

This does not mean that there is one single EU passport or that citizens of EU countries have one single EU citizenship.
Each passport continues to reflect the nationality and citizenship of each respective country. However, in addition to national citizenship, the EU passport also gives rights and obligations that arise out of an added citizenship; EU citizenship.
EU citizenship exists over and above national citizenship. It does not replace it.
EU citizenship gives freer movement in and out of the EU territory.
Checks at EU borders marking entry into or exit from any EU country, distinguish between EU and non-EU citizens.
The “blue channel” (as against green and red channels) is used for EU citizens upon their entry into any EU territory.
The security checks are more stringent with respect to travellers holding a non-EU passport. Once in the EU territory, the distinction between EU and non-EU citizenship ceases for the purposes of movement; he or she has freedom of movement within the EU or rather within the EU countries that are part of the so-called Schengen system allowing complete free travel within their border even to non-EU citizens.
By way of exception, only the UK and Ireland still exercise controls on travellers entering from other EU countries.

5.2.3. Common features of EU passports
The common features of the passport issued to citizens of EU countries include its burgundy colour as well as the words on the front cover “European Union” in addition to the name and emblem of the country that is issuing the passport.
This information is to be provided in the official language or languages of the country issuing the passport.
Inside, in the first page, all this information is repeated, this time in all the official languages of the EU.
On the laminated page, the usual information, photo and details on the holder of the passport as well as the date of issue and expiry of the passport must be included.
As to security features in the passport, EU rules stipulate minimum security features that should be applied, but each country is free to go beyond.
EU rules on the format of passports have nothing to do with the criteria required for a person to obtain a passport.
Nor does the EU determine who can be a national or qualify for citizenship of a particular EU country.
These matters remain entirely up to each individual country to decide.

5.2.4. Some examples
In Germany as an example, it is compulsory at age 16 to possess either a “Personalausweis” or a passport, but not to carry it.
While police officers and some other officials have a right to demand to see one of those documents, the law does not state that one is obliged to submit the document at that very moment.
Fines may only be applied if an identity card or passport is not possessed at all, if the document is expired or if one explicitly refuses to show ID to the police.
If one is unable to produce an ID card or passport (or any other form of credible identification) during a police control, one can (in theory) be brought to the next police post and detained for max. 12 hours, or until positive identification is possible.
However, this measure is only applied if the police have reasonable grounds to believe the person detained has committed an offence.
In the Netherlands: Identification is compulsory as well as in many other countries.
On 1 October 1997, the Dutch Ministry of the Interior and Kingdom Relations introduced a new range of travel documents with extra authenticity features to counter misuse, fraud, and forgery. The new travel documents are structured and designed similarly to those issued since 1995.
Despite the extra features, the documents will be easy to check, guaranteeing their holders...
rapid processing at international borders. The extra features make it immediately obvious whether the document is authentic or fraudulent. The authenticity features come in two categories: first and second line.
First-line features are visible to the naked eye.
Second-line ones have to be checked with special instruments.

Since 2005, every person over 14 years of age must always carry a:
- Passport
  - National Passport (32 pages)
  - Business Passport (64 pages)
  - Diplomatic Passport
  - Official Passport
  - Aliens travel document
  - Refugee’s travel document
- Dutch driving licence
- Dutch/European identity card
- Dutch foreigner’s identification document
  - Residence permit document
  - W-document
  - Privileged person’s identity card
  - Inserts and stickers

No document?
If an alien is unable to produce a Dutch identity card for aliens, it does not necessarily imply that he is staying in the Netherlands illegally.
For example, it is possible that he has not yet collected this document from the municipal authorities or the aliens police. A note will usually have been made in his passport by means of a passport sticker to indicate that he has submitted an application.

EU or EEA?
Citizens from countries of the European Union or European Economic Area are not obliged for that matter to have an EU/EEA document. For EU/EEA citizens a valid passport is sufficient.

5.2.5. Driving licenses
Because a large number of countries, including Australia, Canada and the United States have no national identification cards and because of the widespread use of cars, driver’s licenses are often used as the standard form of identification. In such countries, driver’s license bureaus also issue identification cards for non-drivers. (However, a U.S. law requires Americans returning from Canada or Mexico to present a passport as proof of identity and citizenship.)

Many European countries require adults to carry an ID card at all times. Citizens of EU countries which have no national ID cards, have to carry their passports instead when travelling in these countries. In the People’s Republic of China, the driver’s license number is synonymous with the citizen’s ID number (and is up to 18 digits long).

5.2.6. Forgeries
Identity document forgery is the process by which identity documents issued by governing bodies are copied and/or modified by persons not authorized to create such documents or engage in such modifications, for the purpose of deceiving those who would view the documents about the identity or status of the bearer.

Identity documents differ from other credentials in that they are intended only to be usable by the person holding the card. Unlike other credentials, they may be used to restrict the activities of the holder as well as to expand them.
Falsified documents can be used for identity theft, age deception, illegal immigration, organized crime and terrorism.
Modern ID cards almost invariably carry a picture of the authorized user, a simple and effective form of biometric identification.

However, forgery of simple photographic ID cards has become simple in recent years with the availability of low-cost high-resolution printers and scanners and photo editing software. Simple fake ID cards are commonly made using an inkjet or laser printer to print a replica document which is then laminated to resemble a real ID card.

Most designs are made using computer programs, re-creating scanned copies of a license. Templates for many types of ID cards are available on the Internet.

More complex ID cards are now being created by printing on a material called Teslin, which is a paper-like material that is actually a micro-porous plastic sheet. When butterfly pouches and holograms are applied, the card is then run through a heat laminator which creates a professional-looking ID card.

Numerous security printing techniques have been used to attempt to enhance the security of ID cards. For example, many modern documents include holograms, which are difficult to replicate without expensive equipment which is not generally available. Though accurate recreation of these holograms is extremely difficult, using a mixture of pigments and base can create a similar shiny multi-coloured look which may pass cursory inspection.

Many modern credentials now contain some kind of barcode. For example, many U.S. driving licences include a 2-dimensional code in PDF417 format, which contains the same information as on the front of the license.

Barcodes allow rapid checking of credentials for low-security applications, and may potentially contain extra information which can be used to verify other information on the card.

In addition, some documents include a magnetic strip, which will also contain the same information, and may thus be checked against the machine-readable information on the barcode. Magnetic strips may also contain other secret identifying information.

Although magnetic strips can also be faked, they provide another barrier to entry for the amateur forger.

Other hidden security devices can also be added, including embedded secure crypto processor chips which are designed to be very difficult to forge, and RFID (radio frequency) tags: the two technologies may also be combined, in the case of contactless smart cards.

Another effective technique is the use of online verification of security information against a central database. In many cases, online verification can detect simple copying of a document, by detecting attempted use in multiple places at the same time, and it also allows revocation of lost or stolen documents.

5.2.7. ORIGINAL DOCUMENTS – FAKE CREDENTIALS

The combination of multiple high-security features, biometrics, and well-trained document inspectors with technical assistance can be very effective at preventing forgery.

However, all security techniques can be rendered ineffective if the ID document is a “genuine fake”, that is, a genuine document issued under false pretences.

One way of doing this is to present the document issuing authority with false credentials, which they will then endorse by issuing a new document. In this way, false identities and credentials can be “bootstrapped” over a period of time.

Another simpler way of generating false credentials is to suborn one of the officials involved the document issuing process.

Corruption in the document-issuing process is hard to counter, since as the value of a credential increases, the economic incentives for corruption also increase. This is particularly true in the case of ID cards which combine many functions in one document, and for documents which are issued in large numbers, thus requiring many thousands of people to have authorizing powers.
Another attack is to inject false information into the official database, in such a way that the database will recognize fake cards as being real.

5.3. AUTHENTICATION OF IDENTITY DOCUMENTS

5.3.1. European legislation on passports

An identity document (also known as I.D. or ID) is a piece of documentation designed to verify aspects of a person’s identity.

On 13 December 2004 the Council of the European Union has published a COUNCIL REGULATION (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

The annex: Minimum Security Standards of Passports and Travel Documents issued by the member states lays down the minimum level of security that the Member States’ passports and travel documents are required to provide.

The provisions in this Annex are concerned primarily with the biographical data page.

The generic security features also apply to the other parts of passports and travel documents.

The biographical data page may consist of various basic materials.

This Annex specifies the minimum level of security for the specific material that is used.

Some examples of specified requirements as follows:

Material: The paper used for those sections of the passport or travel document giving personal particulars or other data shall meet the specified minimum requirements. As an example: Stitching thread should be protected against substitution.

Biographical data page:

The passport or travel document shall contain a machine-readable biographical data page. The portrait of the holder shall also appear on this page and shall not be affixed but integrated into the material of the biographical data page.

The biographical data shall be entered on the page following the title page in the passport or travel document. The layout of the biographical data page must be different from the other pages.

Numbering:

On all pages inside the passport or travel document a unique document number should be printed (where possible with a special style of figures or typeface and in UV-fluorescent ink), or perforated or, in passport cards, a unique document number should be integrated using the same technique as for the biographical data. It is recommended that in passport cards the unique document number is visible on both sides of the card.

If a sticker is used for biographical data the unique document number should be printed using fluorescent ink, and a special style of figures or typeface is obligatory.

Protection against copying:

An optically variable (OVD) or equivalent device, which provides for the same level of identification and security as currently used in the uniform format for visas, shall be used on the biographical data page and shall take the form of diffractive structures which vary when viewed from different angles (DOVID) incorporated into the hot-sealed or an equivalent laminate (as thin as possible) or applied as an OVD overlay, or, on stickers of a non-laminated paper inside page, as metallised or partially de-metallised OVD (with intaglio overprinting) or equivalent devices.

The OVD devices should be integrated into the document as an element of a layered structure, effectively protecting against forgery and falsification.

1 More information in: Working document– 28/06/2006 Eu-Passport-Specification, Biometrics Deployment of EU-Passports, EU – Passport Specification. The United Kingdom and Ireland have not taken part in the adoption of this measure,
Issuing technique

To ensure that passport or travel document data are properly secured against attempts at counterfeiting and falsification, biographical data including the holder’s portrait, the holder’s signature and main issue data shall be integrated into the basic material of the document. Conventional methods of attaching the photograph shall no longer be used.

To ensure that biographical and issue data are adequately protected against attempts at tampering, hot-seal or equivalent lamination (as thin as possible) with an anti-copying device is compulsory where laser printing, thermo-transfer or photographic techniques are used. Travel documents shall be issued in machine-readable form.

5.3.2. Dutch national passport and related ID documents

Exterior of passport

The Dutch passport comprises 32 numbered pages sewn into a cover.

- Page 1 contains a kinegram,
- page 2 is the passport holder page,
- page 3 contains the signature of the passport holder, and
- page 4 provides space for children to be included in the passport.

Pages 3 to 30 contain illustrations which together make up a chronological pictorial history of the Netherlands, each page having a different illustration. At the foot of these pages there is a text block explaining the story told by the picture. These text blocks are framed by micro texts.

Some of the special security measures to prevent forgery are described in the following text. However, for a complete overview see the official documentation on: http://www.bprbzk.nl/echtheidskenmerken/kenmerken_1997_2001/1997/gb/download/engels.pdf

The examples serve to show the complexity of the documents.

Line watermark:

- position: passport holder page
- description: repeating horizontal lines in the paper underneath the passport photo
- verification: the holder page is held up to the light or placed on a light source

Kinegram

- Position: page 1
- Description: an image on metallic foil that can change its shape and colour
- Verification: tilting the document to one side

Micro laser perforation

- Position: four places on the passport holder page
- description: various symbols perforated by laser
- verification: holding the passport holder page up to the light or placing it on a light source

Printed laminate

- Position: passport holder page, retro-reflecting laminate on the glued side
- description: repeating wavy blue text “KONINKRIJK DER NEDERLANDEN”
- verification: with the naked eye
Chapter 5 | ID documents

Uniquely numbered passport photo
Position: passport holder page
Description: the passport photo has a unique number and the letters “NL” punched into it
Verification: with the naked eye

Multi coloured binding thread
Position: between pages 16 and 17
description: burgundy, yellow ochre, and white thread intertwined to make a single binding thread
Verification: with the naked eye

Ultra violet inscription
Position: passport holder page
description: a circle of 12 stars and a propeller pattern fluoresce yellow, and a line drawing of a human figure fluoresces blue-green
Verification: holding the page under ultraviolet light

Extra small print
Position: page 1, partly over the hologram
Description: repeating pattern of the micro text “KONINKRIJK DER NEDERLANDEN”
Verification: with a magnifying glass

Retro-reflecting laminate
Position: passport holder page
Description: holding a retro viewer at a certain angle to the page will reveal a repeating propeller pattern
Verification: with a retro viewer

Diplomatic Passport and Service Passport. Authentication similar to the national passport.

5.3.3. IDENTITY CARD/PASSPORT GERMANY, OTHERS — AUTHENTICITY MARKINGS
Security features of the new provisional documents and children’s passports:

1. Latent image
A latent image printed in intaglio is visible in the upper part of the documents.
2. **OVI**
Optically variable ink is integrated in the upper part of the documents. Depending on the viewing angle, the colour will be red or green.

3. **Negative guilloche with micro lettering**
The negative guilloche lines under the fields where the data is entered are overprinted with intaglio printed micro lettering to make sure that any attempts to alter the entries can be detected.

4. **Integrated photo**
The inkjet printing process is used to integrate the photo into the document.

5. **Kinegram**
When tilting the document around the vertical axis, kinematic structures become visible. When tilted around the horizontal axis, the area where the eagle is depicted shows a reversal of contrast, i.e. the light eagle is now dark in a light hexagon.

6. **Fluorescent fibres in the paper**
The paper contains visible fibres which fluoresce under UV light as well as fluorescent planchets (i.e. disc-shaped inlays in the paper).

7. **UV overprinting**
The Federal Eagle surrounded by stars becomes visible under UV light.

8. **Numbering**
The documents have a 7-digit serial number with a preceding letter. The numbering is safeguarded by the guilloche lines and microlettering of the security background. The number fluoresces in red under UV light. The laser-perforated number of the passport booklet corresponds to the printed number of the sticker.

9. **Intaglio printing**
The captions, the border around the photo and the bar in the upper part of the document are tactile.

10. **Multi-coloured guilloche security printing**
Guilloches are security patterns consisting of fine, interwoven line structures that form a perfectly registered harmonic picture. The negative guilloche smoothly runs into a positive guil-
loche. When these patterns are reproduced (e.g. colour copy), the line structures appear as dotted screen structures.

11. Machine-readable zone (MRZ)
The documents are machine readable. The machine-readable zone (MRZ) features, among other things, the serial number, the holder’s name and date of birth, the expiry date as well as the check digit.

**England and Northern Ireland**

**ID Greece**

**ID Portugal**
5.3.4. Driving licenses

Current EU driving license, German version – front
1. Family name
2. Given name(s)
3. Date and place of birth
4a. Issuing date
4b. Expiry date
4c. Issuing authority
5. License number
7. Signature of bearer
9. Categories

German version reverse
9. License categories
10. Issue date of the category
11. Expiry date of the category
12. Restrictions (number coded)
5.4. CONTROL PROCEDURES

- Verify what kind of identification is required at each security level. Most Governmental organizations have their own identity document.
- Take the identity document out of its sleeve.
- Check the validity of the document.
- Check of all authentication marks and devices are present as required.
- Compare the photograph on the Identification document with the face of the person involved.
- Check whether a second layer of laminate has been applied.
- Check for irregularities or bumps on or around the photograph.
- Check whether the signature checks out with the signature required on the admittance registration form.
- Ask and verify the date of birth and place of the visitor.

This procedure must be documented in the companies' regulations and standing operating instructions.

5.5. SOME DEFINITIONS AND EXPLANATIONS

Refugee
A refugee is a person who, owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group, or political opinion, is outside the country of his nationality, and is unable to or, owing to such fear, is unwilling to avail himself of the protection of that country.

Asylum seeker or asylee
Political Asylum. A person seeking protection and sanctuary granted by the Government of the country concerned; within its territorial jurisdiction or on the high seas to a foreign national who applies for such protection because of persecution or fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion.

Hologram
A hologram is a three-dimensional image, created with photographic projection. Unlike 3-D or virtual reality on a two-dimensional computer display, a hologram is a truly three-dimensional and free-standing image that does not simulate spatial depth or require a special viewing device. Theoretically, holograms could someday be transmitted electronically to a special display device in your home and business.

Kinegram
The Kinegram security device is an optically variable device and has been used for over 20 years and is a unique, high-security, non-holographic authentication feature. Primarily the Kinegram was developed as a visual authentication feature to prevent people from copying and counterfeiting documents, banknotes and cards, yet the Kinegram can also contain machine-verifiable and machine-readable features.

Fluorescent fibres
A security paper that contains invisible fluorescent fibres (visible only under ultraviolet light).

Ultraviolet light
The invisible rays of the spectrum that are outside of the visible spectrum at its short-wavelength violet end. Ultraviolet rays are found in everyday sunlight and can cause fading of paint finishes, carpets, and fabrics.

Optically Variable Inks
Optically variable inks or OVI contain tiny flakes of special film which changes colour as the viewing angle is varied. The result is an ink which has this same optical property, changing
colours as the viewing angle is varied. They do offer excellent protection against all counterfeiting methods.

Micro printing
Micro printing is one of many anti-counterfeiting techniques. Micro printing involves printing very small text, usually too small to read with the naked eye. Microprint is frequently hidden in an inconspicuous, unnoticeable area on the note or item.

Guilloche lines
A pattern (as on metalwork) made by interlacing curved lines. Guilloches are security patterns consisting of fine, interwoven line structures that form a perfectly registered harmonic picture. The negative guilloche smoothly runs into a positive guilloche. When these patterns are reproduced (e.g. colour copy), the line structures appear as dotted screen structures.

Intaglio printing
Intaglio is a family of printmaking techniques in which the image is incised into a surface, known as the matrix or plate. Normally, copper or zinc plates are used as a surface, and the incisions are created by etching, engraving, drypoint, aquatint or mezzotint.

Machine-readable zone (MRZ)
The documents are machine readable. The machine-readable zone (MRZ) features, among other things, the serial number, the holder’s name and date of birth, the expiry date as well as the check digit.

5.6. SUMMARY OF CHAPTER 5
A port facility security guard must be very aware of his environment at all times. He must not be distracted and knows the possibilities and restrictions of each and every piece of equipment he uses. He has studied the data sheets and trained with it. He knows the vulnerable areas within the company as well as the physical environment and reports on it to his superior. Suspicious movements at, and as far as possible, with the areas adjacent to the facility, will be documented and reported. A healthy distrust is a second nature to him. When training, various case of breaking and entering (by professionals as well as by amateurs), action groups, terrorists and their modus operandi have been discussed. Within the Netherlands, any person over 14 years of age, must be able to identify himself.

Within the European Community, Passports are of a similar format. Security requirements are defined. More is possible, less not allowed.

Often the following security hallmarks are to be found:
- Latent image. A latent image printed in intaglio is visible in the documents.
- OVI. Optically variable ink may be integrated in the upper part of the documents. Depending on the viewing angle, the colour will be red or green.
- Negative guilloche with micro lettering.
- Integrated photo.
- Kinegram. When tilting the document around the vertical axis, kinematic structures become visible.
- Fluorescent fibres in the paper. The paper may contain visible fibres which fluoresce under UV light as well as fluorescent planchets (i.e. disc-shaped inlays in the paper).
- UV overprinting. Printing becomes visible under UV light.
- Numbering. The documents have a 7-digit serial number with a preceding letter. The numbering is safeguarded by the guilloche lines and micro lettering of the security background. The number fluoresces in red under UV light. The laser-perforated number of the passport booklet corresponds to the printed number of the sticker.
- Intaglio printing. The captions, the border around the photo and the bar in the upper part of the document are tactile.
5.7. QUESTIONS AND EXERCISES

5.7.1. QUESTIONS

Question 1
Which different kinds of methods are possible for checking ID?

Question 2
What is the youngest age when a person should identify him/herself in the Netherlands?

Question 3
What is an authenticating mark?

Question 4
Describe the control procedure or checking ID in your job.

Question 5
Can you read micro printing without aids?

Question 6
How does optical variable ink work?

Question 7
When is UV-light used?

5.7.2. EXERCISE ASSIGNMENTS

Give a short description of one of your experiences during work in case of the next subjects:

- Theft
- Burglary
- Robbery
- Misappropriate
- Unauthorized entrance
- Suspected persons
- Suspicious cargo
- Fire-raising
- Suspicious vehicles
- Visitation
- Control identity documents
- Control of passengers

Multi-coloured guilloche security printing
• Machine-readable zone (MRZ)
• The documents are machine readable. The machine-readable zone (MRZ) features, among other things, the serial number, the holder’s name and date of birth, the expiry date as well as the check digit.
INTRODUCTION

Worldwide, the manufacturing, sales, possession and use of arms is bound by a legal framework.
In the past, each country had and has its own laws and regulations.
Still, progress has been made.
Worldwide, legislation on combating crime and terrorism has been implemented.

The United Nations Convention against Transnational Organised Crime clearly states its purpose as to promote cooperation between Governments to prevent and combat transnational organised crime more effectively. Governments who have signed this convention are bound to cooperate on many areas like:
• How to interpret the various concepts: what is crime, what is a criminal organisation (definitions)
• Criminalisation of the laundering of proceeds of crime
• Criminalisation of corruption
• Liability of legal persons
• Prosecution, adjudication and sanctions
• Confiscation and seizure
• Etc.

Moreover, aware of the urgent need to prevent, combat and eradicate the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, owing to the harmful effects of those activities on the security of each State, region and the world as a whole, endangering the well-being of peoples, their social and economic development and their right to live in peace, a Protocol against the illicit manufacturing of and trafficking in Firearms, their parts and components and Ammunition (the Firearms Protocol), has been added to supplement the United Nations Convention against Transnational Organised Crime.

The Firearms Protocol is the first instrument of global application dealing with firearms. It sets out a comprehensive system to control the movement of firearms, their parts and components and ammunition, which includes provisions that require the criminalisation of offences relating to the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, as well as to the tampering with firearms markings.
This Protocol entered into force on 3 July 2005.


On July 1st 2004 legislation on terrorism combatment, applicable to ships engaged in international trade as well as the receiving Port Facilities came into force.

The International Maritime Organisation (IMO), the international organisation that is responsible for the safety of the shipping industry in general, has issued a number of obligatory regulations and recommendations that constitute a framework within which the maritime safety can be improved considerably.

The International Ship and Port facility Security Code (ISPS Code), which was adopted by more than 100 countries of the International Maritime Organisation, contains detailed security-related requirements for governments, port authorities and shipping companies. It is intended to enable better monitoring of freight flows, to combat smuggling and to respond to the threat of terrorist attacks. Countries that fail to observe the ISPS Code, which took effect 1 July 2004, risk being excluded from international trade. The fight against organised crime and terrorism makes the tracing of firearms particularly important.
6.1. LEGISLATION ON ILICIT TRAFFICKING OF WEAPONS OR ANY OTHER DANGEROUS SUBSTANCES AND DEVICES INTENDED FOR USE AGAINST PERSONS, SHIPS OR PORTS AND THE CARRIAGE OF WHICH IS NOT AUTHORIZED

6.1.1. ISPS Code

The ISPS Code is very clear on the subject. Part A art. 16.3 clearly states that the Port Facility Security Plan shall address, at least, the following:

- measures designed to prevent weapons or any other dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorised, from being introduced into the port facility or on board a ship;

It means, that we must be able to recognise weapons, dangerous substances and devices in order to detect and deter. Recognition is just one part of being able to recognise weapons, dangerous devices and substances. Understanding of the threats and dangers involved as well as a proven way of dealing with all possible events (scenarios) require instructions, procedures how to cope, proper equipment and maintenance as well as proper education and training of all personnel.

6.1.2. UN Firearms Protocol Definitions

Every country has its own ideas on how to define weapons and ammunition. It stands to reason to use definitions used in the United Nations Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition, Supplementing the United Nations Convention against Transnational Organised Crime. The articles listed are relevant to the topic discussed.

Article 2 – Statement of purpose

The purpose of this Protocol is to promote, facilitate and strengthen cooperation among States Parties in order to prevent, combat and eradicate the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition.

Article 3 – Use of terms

For the purposes of this Protocol:

- “Firearm” shall mean any portable barrelled weapon that expels, is designed to expel or may be readily converted to expel a shot, bullet or projectile by the action of an explosive, excluding antique firearms or their replicas. Antique firearms and their replicas shall be defined in accordance with domestic law. In no case, however, shall antique firearms include firearms manufactured after 1899;
- “Parts and components” shall mean any element or replacement element specifically designed for a firearm and essential to its operation, including a barrel, frame or receiver, slide or cylinder, bolt or breech block, and any device designed or adapted to diminish the sound caused by firing a firearm;
- “Ammunition” shall mean the complete round or its components, including cartridge cases, primers, propellant powder, bullets or projectiles, that are used in a firearm, provided that those components are themselves subject to authorisation in the respective State Party;
- “Illicit trafficking” shall mean the import, export, acquisition, sale, delivery, movement or transfer of firearms, their parts and components and ammunition from or across the territory of one State Party to that of another State Party if any one of the States Parties concerned does not authorise it in accordance with the terms of this Protocol or if the firearms are not marked in accordance with article 8 of this Protocol;
- “Tracing” shall mean the systematic tracking of firearms and, where possible, their parts and components and ammunition from manufacturer to purchaser for the purpose of assisting the competent authorities of States Parties in detecting, investigating and analysing illicit manufacturing and illicit trafficking.

Article 1 – General requirements for export, import and transit licensing or authorisation systems

- Each State Party shall establish or maintain an effective system of export and import licensing or authorisation, as well as of measures on international transit, for the transfer of firearms, their parts and components and ammunition.
The export and import licence or authorisation and accompanying documentation together shall contain information that, at a minimum, shall include the place and the date of issuance, the date of expiration, the country of export, the country of import, the final recipient, a description and the quantity of the firearms, their parts and components and ammunition and, whenever there is transit, the countries of transit. The information contained in the import licence must be provided in advance to the transit States.


6.1.3.1. Introduction

The name “Schengen” originates from a small town in Luxembourg. In June 1985, seven European Union countries signed a treaty to end internal border checkpoints and controls. More countries have joined the treaty over the past years. Visa Member Countries comprise 13 of the 25 European Union (EU) Member States and 2 European Economic Area (EEA) Member States. The 15 Schengen countries are: Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Italy, Greece, Luxembourg, Netherlands, Norway, Portugal, Spain and Sweden.

The Schengen Treaty lifts certain controls on EU member states by allowing for the free movement of people and goods across national borders; more specifically, it removes controls at internal land, sea and airport frontiers. Many EU Member States fully implemented the agreement since 1995; Ireland and the United Kingdom remain outside the agreement.

Member states who have signed the Schengen treaty have stepped up border controls and established the Schengen Information System, a multinational database containing over 10 million files regarding suspect persons, stolen vehicles, forged currency and firearms. In addition, the agreement contains provisions for police cooperation and mutual assistance “for the purposes of preventing and detecting criminal offences” and further outlines minimum standards for the marking and registering of weapons.

The Schengen agreement in its TITLE III Police and security Chapter 7, Article 39 - 91 translates the Firearm Protocol into greater detail. However, it restricts itself to firearms and ammunition (art. 77 – 91).

Other weapons than mentioned in Chapter 7 are left to the member states themselves; those weapons are regulated through the National Legislation of each member state.

For our goals, the main articles in the Schengen Agreement are articles 78 – 83.


The Schengen treaty describes firearms in a broad sense. There are many similarities with the directive of 18 June 1991. In this syllabus, we will highlight from both. A more precise understanding of these legal points of view may be read from the proper documents.

The directive is without prejudice to the application of national provisions concerning the carrying of weapons, hunting or target shooting.

Moreover, the directive shall not apply to the acquisition or possession of weapons and ammunition, in accordance with national law, by the armed forces, the police, the public authorities or by collectors and bodies concerned with the cultural and historical aspects of weapons and recognised as such by the Member State in whose territory they are established. Nor shall it apply to commercial transfers of weapons and ammunition of war.

Whereas the Directive does not affect the right of Member States to take measures to prevent illegal trade in weapons.

ANNEX I OF THE DIRECTIVE:

I. For the purposes of this Directive, ‘weapon’ means:
• any firearm as defined in section II of this Annex
• weapons other than firearms as defined in national legislation
II. For the purposes of this Directive, ‘firearm’ means:

A. Any object which falls into one of the following categories, unless it meets the definition but is excluded for one of the reasons listed in section III.

Category A - Prohibited firearms
1. Explosive military missiles and launchers.
2. Automatic firearms.
3. Firearms disguised as other objects.
4. Ammunition with penetrating, explosive or incendiary projectiles, and the projectiles for such ammunition.
5. Pistol and revolver ammunition with expanding projectiles and the projectiles for such ammunition, except in the case of weapons for hunting or for target shooting, for persons entitled to use them.

Category B - Firearms subject to authorisation
1. Semi-automatic or repeating short firearms.
3. Single-shot short firearms with rim fire percussion whose overall length is less than 28 cm.
4. Semi-automatic long firearms whose magazine and chamber can together hold more than three rounds.
5. Semi-automatic long firearms whose magazine and chamber cannot together hold more than three rounds, where the loading device is removable or where it is not certain that the weapon cannot be converted, with ordinary tools, into a weapon whose magazine and chamber can together hold more than three rounds.
6. Repeating and semi-automatic long firearms with smooth-bore barrels not exceeding 60 cm in length.
7. Semi-automatic firearms for civilian use which resemble weapons with automatic mechanisms.

Category C - Firearms subject to declaration
1. Repeating long firearms other than those listed in category B, point 6.
2. Long firearms with single-shot rifled barrels.
3. Semi-automatic long firearms other than those in category B, points 4 to 7.
4. Single-shot short firearms with rim fire percussion whose overall length is not less than 28 cm.

Category D - Other firearms

B. Any essential component of such firearms:

The breach-closing mechanism, the chamber and the barrel of a firearm which, being separate objects, are included in the category of the firearms on which they are or are intended to be mounted.

III. For the purposes of this Annex objects which correspond to the definition of a ‘firearm’ shall not be included in that definition if they:

- have been rendered permanently unfit for use by the application of technical procedures which are guaranteed by an official body or recognised by such a body
- are designed for alarm, signalling, life-saving, animal slaughter or harpoon fishing or for industrial or technical purposes provided that they can be used for the stated purpose only
- are regarded as antique weapons or reproductions of such where these have not been included in the previous categories and are subject to national laws

Pending coordination throughout the Community, Member States may apply their national laws to the firearms listed in this Section.

IV. For the purposes of this Annex:

- ‘short firearm’ means a firearm with a barrel not exceeding 30 centimetres or whose overall length does not exceed 60 centimetres
Chapter 6 | Recognition of weapons and ammunition

- ‘long firearm’ means any firearm other than a short firearm
- ‘automatic firearm’ means a firearm which reloads automatically each time a round is fired and can fire more than one round with one pull on the trigger
- ‘semi-automatic firearm’ means a firearm which reloads automatically each time a round is fired and can fire only one round with one pull on the trigger
- ‘repeating firearm’ means a firearm which after a round has been fired is designed to be reloaded from a magazine or cylinder by means of a manually-operated action
- ‘single-shot firearm’ means a firearm with no magazine which is loaded before each shot by the manual insertion of a round into the chamber or a loading recess at the breech of the barrel
- ‘ammunition with penetrating projectiles’ means ammunition for military use where the projectile is jacketed and has a penetrating hard core
- ‘ammunition with explosive projectiles’ means ammunition for military use where the projectile contains a charge which explodes on impact
- ‘ammunition with incendiary projectiles’ means ammunition for military use where the projectile contains a chemical mixture which bursts into flame on contact with the air or on impact

ANNEX II of the directive addresses the requirements to transport firearms.

European firearms pass

The ‘European firearms pass’ is a document which is issued on request by the authorities of a Member State to a person lawfully entering into possession of and using a firearm. It shall be valid for a maximum period of five years. The period of validity may be extended. Where only firearms classified in category D appear on the pass, the maximum period of validity thereof shall be ten years. It shall contain the information set out in Annex II.

The ‘European firearms pass’ is a non-transferable document, on which shall be entered the firearm or firearms possessed and used by the holder of the pass. The pass must always be in the possession of the person using the firearm. Changes in the possession or characteristics of the firearms shall be indicated on the pass, as well as the loss or theft of the firearm.

The pass must include the following sections:
- identity of the holder
- identification of the weapon or firearm, including a reference to the category within the meaning of the Directive
- period of validity of the pass
- section for use by the Member State issuing the pass (type and references of authorisations, etc.)
- section for entries by other Member States (authorisations to enter their territory, etc.)
- the statements:
  - ‘The right to travel to another Member State with one or more of the firearms in categories B, C or D mentioned in this pass shall be subject to one or more prior corresponding authorisations from the Member State visited. This or these authorisations may be recorded on the pass.’

The prior authorisation referred to above is not in principle necessary in order to travel with a firearm in categories C or D with a view to engaging in hunting or with a firearm in categories B, C or D for the purpose of taking part in target shooting, on condition that the traveller is in possession of the firearms pass and can establish the reason for the journey.

Where a Member State has informed the other Member States, in accordance with Article 8 (3), that the possession of certain firearms in categories B, C or D is prohibited or subject to authorisation, one of the following statements shall be added:
- ‘A journey to . . . (State(s) concerned) with the firearm . . . (identification) shall be prohibited.’
- ‘A journey to . . . (State(s) concerned) with the firearm . . . (identification) shall be subject to authorisation.’
**Purchasing and possession of a fire arm**

A permit to purchase and possess a firearm listed in Article 80 of the Schengen agreement may be issued only:

- if the person concerned is over 18 years of age, with the exception of dispensations for hunting and sport purposes
- if the person concerned is not unfit to purchase or possess a firearm as a result of mental illness or any other mental or physical disability
- if the person concerned has not been convicted of an offence or if there are no other indications that he might be a danger to public order and security
- if the reasons given by the person concerned for purchasing or possessing firearms can be considered legitimate

**6.2. WEAPONS OTHER THAN FIREARMS AS DEFINED IN NATIONAL LEGISLATION**

**6.2.1. INTRODUCTION**

The E.U. Member States have introduced the EU requirements into their legislation. Less is not allowed, as Article 3 stipulates:

‘Member States may adopt in their legislation provisions which are more stringent than those provided for in this Directive, subject to the rights conferred on residents of the Member States by Article 12 (2) CHAPTER 2 ‘Harmonisation of legislation concerning firearms’.

As it is impossible to discuss all country specific national legislation, this syllabus will present Dutch legislation as an example to a possible legal and operational framework on weapon recognition and deterrence. Generalisation is unavoidable.

In the Netherlands, the possession and use of firearms by members of the public is bound by strict statutory requirements in the Netherlands. Only licence holders, after an extensive check, are allowed to have a gun in their possession and use it in a gun club or for hunting purposes.

Possession of illegal firearms is punished severely and the severity of the sentences has recently been increased from nine months to four years.

**6.2.2. HIERARCHY IN LAW**

**6.2.2.1 Introduction**

Legislation is structured from top to bottom, that means that International Legislation, implemented into the National Legislation, is of the highest importance (provided ‘lower’ legislation covers the same subject).

From international legislation to national legislation to regional and / or municipal legislation.

We have seen the United Nations Firearm Protocol, signed by the European commission. The European legislation is the binding framework.

Furthermore the Schengen Agreement and the directive of 18 June 1991 on control of the acquisition and possession of weapons.

On a national level, weapon legislation in the Netherlands as follows:

- The law Weapons and Ammunition; this is the formal law
- The Regulation Weapons and Ammunition; clarifies and expands the law ( the Ministry of Justice)
- The Circular Weapons and Ammunition; further instruction by the Minister of Justice to the chiefs of police concerning the execution of the law and the policy to be followed.

This Weapons and Ammunition Act prohibits the unauthorised possession of firearms and provides for controls on authorised possession in the Netherlands.

As such, the Act prohibits a large number of activities involving weapons and ammunition.

Examples include:

- manufacturing
- trading
- importing
• exporting
• carrying in transit
• possessing
• carrying
• weapons and ammunition

The Weapons and Ammunition Act also sets out rules for the legal possession of weapons and ammunition.

Based on those rules, acts such as importing, exporting, transporting and possessing are in some instances permitted, subject to the condition that you possess a discretionary permit. Such a dispensation is referred to as a 'consent'.

Pursuant to the Weapons and Ammunition Act, Customs carries out inspections on the import, export and transit of weapons and ammunition to determine whether the party concerned possesses 'consent'.

The Weapons and Ammunition Act covers a wide range of weapons, i.e. not just firearms, but also knives, knuckle-dusters, nunchakus, catapults, tear gas and alarm pistols.

6.2.2.2. Weapons and Ammunition Act – weapon categories

In principle, in the Netherlands the possession of all fire weapons is prohibited, except for certain ancient fire weapons, defined by the exemption of Article 18.

Furthermore, to certain groups licenses are granted; such as people who execute shooting as a sport, collectors or hunters.

Moreover, weapons other than firearms have been prohibited. Weapons other than firearms like knives (for example stiletto's), reproductions / fake weapon, realistically looking toys and air guns, tasers and self-defence weapons (for example pepper spray and tear gas).

Weapons and ammunition have been classified according to the law Weapons and Ammunition in four categories. Ammunition has been classified in categories in accordance with the classification of weapons. That means that category II addresses the ammunition necessary for weapons from category II. For ammunition therefore no category I and IV exists, because the weapons from these categories do not use ammunition.

The law defines several Operations with weapons.

Six different operations are distinguished. As an example:
• To carry: The non-packaged and therefore ready-for-use availability at public places.
• To transport: On public roads transporting a weapon (and/or ammunition) that has been packaged in such a way that it is not available for immediate use.

The law Weapons and Ammunition defines for each category, which operations with weapons are prohibited. Also it has states, when then an exception can be made.

6.3. WEAPONS AND AMMUNITION CATEGORIES

6.3.1. INTRODUCTION

Weapons and ammunition have been classified according to the law Weapons and Ammunition in four categories.

Category I
• Undesirable weapons other than firearms such as stiletto’s, catapults and arrows
• Toy weapons which resemble strongly on real weapons and may be used for threat

Category II
• Military weapons, such as hand grenades
• Objects with toxic or substances rendering persons defenceless

Category III
• Guns, revolvers and guns
• Alarm guns and throwing knives

Category IV
• Weapons, such as knives, swords and cross bows
Weapons which as a weapon not meant to be a weapon but may be used as such; kitchen knives or baseball bats

Ammunition
Ammunition has been classified in categories in accordance with the classification of weapons. That means that category II addresses the ammunition necessary for weapons from category II. For ammunition therefore no category I and IV exists, because the weapons from these categories do not use ammunition.

6.3.2 Some definitions
The interpretation of ‘Definitions’ varies between counties. As an example, in Germany most switchblades are illegal to own or import into or out of Germany. However, if the blade is side-opening, max. 8.5 cm long, the breadth is max. 20% of length, and it’s not double-edged, they’re legal.

The English Section 141 of the Criminal Justice Act 1988 (offensive weapons) uses the following on ‘Undesirable weapons other than firearms’. Again, these definitions are given as an example. The National Legislation of the country the Port Facility Security Personnel Instruction is employed is binding. The Security Personnel must be instructed accordingly by education and Instructions.

• a knuckleduster, that is, a band of metal or other hard material worn on one or more fingers, and designed to cause injury, and any weapon incorporating a knuckleduster
• a swordstick, that is, a hollow walking-stick or cane containing a blade which may be used as a sword
• the weapon sometimes known as a “hand claw”, being a band of metal or other hard material from which a number of sharp spikes protrude, and worn around the hand
• the weapon sometimes known as a “belt buckle knife”, being a buckle which incorporates or conceals a knife
• the weapon sometimes known as a “push dagger”, being a knife the handle of which fits within a clenched fist and the blade of which protrudes from between two fingers
• the weapon sometimes known as a “hollow kubotan”, being a cylindrical container containing a number of sharp spikes
• the weapon sometimes known as a “foot claw”, being a bar of metal or other hard material from which a number of sharp spikes protrude, and worn strapped to the foot
• the weapon sometimes known as a “shuriken”, “shaken” or “death star”, being a hard non-flexible plate having three or more sharp radiating points and designed to be thrown
• the weapon sometimes known as a “balisong” or “butterfly knife”, being a blade enclosed by its handle, which is designed to split down the middle, without the operation of a spring or other mechanical means, to reveal the blade
• the weapon sometimes known as a “telescopic truncheon”, being a truncheon which extends automatically by hand pressure applied to a button, spring or other device in or attached to its handle
• the weapon sometimes known as a “blowpipe” or “blow gun”, being a hollow tube out of which hard pellets or darts are shot by the use of breath
• the weapon sometimes known as a “kusari gama”, being a length of rope, cord, wire or chain fastened at one end to a sickle
• the weapon sometimes known as a “kyoketsu shoge”, being a length of rope, cord, wire or chain fastened at one end to a hooked knife
• the weapon sometimes known as a “manrikigusari” or “kusari”, being a length of rope, cord, wire or chain fastened at each end to a hard weight or hand grip

6.3.3 Category I – the Netherlands
Category I
• Undesirable weapons other than firearms such as stiletto’s, catapults and arrows
• toy weapons which resemble strongly on real weapons and may be used for threat
1°. stiletto’s, fall knives and butterfly knives, provided that the blade:
• has more than one cutting edge
• is 7 cm or longer and 14 mm or smaller
• is 9 cm or longer or
• has been equipped with a guard

2°. other folding knifes if:
• the blade has more than one cutting edge or
• the length in open situation is longer than 28 cm

3°. knuckledusters, bludgeons, strangulation sticks, death stars, paring knives, ballistic knifes and sound silencing devices for fire weapons;
4°. weapons which resemble something not resembling a weapon – a stealth knife;

**Stealth knife (airport knife)**
cold steel's cat tanto is made from a single piece of high-impact resistant plastic. It looks like an ordinary knife, but features no metal components.

this cold steel spike is also manufactured from a high impact plastic. However, some knife makers also use other materials, for instance ceramics.

**Belt-buckle knife**
this belt buckle knife is a single piece buckle. Belt buckle knives are almost exclusively American in source, although many are manufactured in the far-east. They have a particular affiliation with motor-cycling groups in America.

this American made belt buckle includes a folding lock knife.
Belt buckle knives are often decorated.

the ink-pen knife pulls apart to reveal a sharp blade.
Typically of far-eastern origin, but sold around the world as novelty items.

from the outside this knife looks like a lipstick. Rotate the brass coloured barrel to extend the blade. Typically of far-eastern origin, but sold around the world as novelty items.

Common use names: hairbrush dagger, ink pen knife

Note:
knives commonly referred to as 'credit card' knives are not disguised knives, as although they are similar in shape to a credit card, this is simply to facilitate storage and no attempt is made to design the knife to appear to be a credit card - with or without the benefit of closer inspection.

5°. arrows and arrow points to be shot by a bow, provided with sharp edges and obviously meant to inflict bodily harm

6°. Slingshots / Catapults

**Slingshot or catapult**

7°. other objects designated by our minister which can be a serious threat of persons or who resembles as such on a weapon that they are arranged for threat or extortion
Chapter 6 | Recognition of weapons and ammunition

Advertisement:
‘Authentic full-size machined metal Blank-Firing Guns! Cannot fire real ammunition. Realistic working action, some gun models fire semi-automatically. Our Blank-firing Guns come fully assembled, but can be disassembled by a qualified gunsmith. These blank-firing guns weigh and feel just like the hard-to-get-origina1s’.

Replicas have become so convincing that even experts cannot tell the difference from two feet away. Increasingly these sorts of guns are being used by criminals. Scotland Yard says 75% of guns seized last year were de-activated or replica weapons.

6.3.4. Category II’

1º. Firearms not categorised in one of the other categories; Military equipment: missiles, tanks, mortars, launchers, etc.

Generally speaking it can be concluded that this category addresses military war equipment.

The weapons in this category are not meant to be handled or owned by civilians.

2º. Automatic firearms.

Heckler & Koch G41

3º. Firearms designed to be carried concealed or firearms with enhanced performance

A sawed-off shotgun (U.S.) or sawn-off shotgun (UK) is a type of shotgun with a shorter gun barrel and often a shorter or deleted stock, compared to a standard shotgun.

The sawed-off shotgun has a larger spread and a more limited range, but it has about the same destructive power.

Its reduced size makes it easier to conceal. Such a powerful and compact weapon is especially suitable for use in small spaces, such as by vehicle crews, and entry teams running through doorways. Think about what terrorists may do with it!

To make shotguns less concealable, many jurisdictions have a minimum legal length for shotgun barrels and most gun makers do not offer undersized shotguns to the public.

As its name implies, the sawed-off shotgun is usually produced by home-made modification of a standard shotgun.

1 see the EU Directive, Annex: Category A - Prohibited firearms
4°. Firearms disguised as other objects (ballpoint pistol, etc.).

5°. Devices rendering people defenceless or hurting them by administering an electrical shock, medical aids exempted.

An example is an electroshock gun, also referred to as a stun gun, is a weapon used for subduing a person by firing something which administers electric shock, disrupting superficial muscle functions.

A Taser is a well-known device of this type.

6°. Devices destined to harm people with poisonous or other harmful substances suffocating or rendering people defenceless or applying a gas that causes the eyes to sting and water but does not damage them; medical aid and firearms like guns, revolvers and pistols used for firing ammunition containing substances rendering people defenceless or teargas, exempted.

Tear gas is very effective in the hands of a trained person. Tear gas is considered “non-lethal” personal self-defence device. However, chemical sprays have caused death, under the certain conditions.

OC is short for oleoresin capsicum, which is extracted from chilli peppers and is commonly called Pepper Spray. This product is the most widely sold today and the spray of choice for police since 1977. Pepper spray is generally regarded to be the most distressing to experience, but it must be sprayed directly in the eyes or inhaled to be most effective.

7°. Devices destined to harm people or assets by fire or explosion. Explosives destined for civil use exempted provided a permit has been issued in accordance with the Law on Explosives, civil use.

C-4 can easily be moulded into any desired shape. C-4 is well known for its durability, reliability, and safety. It will not explode even if hit by a bullet, punched, cut, or thrown into a fire. The only reliable method for detonation is via a detonator or blasting cap. However, applying pressure in combination with heat can often cause detonation.
6.3.5. Category III

Category 3 addresses weapons, ammunition and other weapons requiring a permit. The legislator is of the opinion, that civilians may have access under certain conditions. Civilians must apply for a document of competency.

1e Firearms resembling guns, revolvers and pistols, not categorised under category II sub 2nd., 3rd. and 6th.

3°. Throwing knifes
- are equipped without barrel or with an obviously shortened or wholly filled barrel;
- not able to contain detonation caps of over 6 mm. calibre; and
- of which the chamber (of the shells) and the gas exhaust stand perpendicular to the barrel or to the longitudinal axis of the weapon.

6.3.6. Category IV

Relatively inoffensive hand weapons, in principle available to everyone. To the legislator these weapons are hardly of interest to the criminal. As such are considered to be ‘less offensive objects’. Less dangerous does not mean that carrying these weapons has been permitted.

Carrying these weapons at public places has been prohibited. To have these weapons available has been permitted, with a permit, to everyone of 18 years and older.

1e Unsheathed weapons, of which the blade has more than one cutting edge, as far as they are not categorised under category I; (A serrated saw edge will be considered a cutting edge)

The carriage of such weapons has been prohibited. However, it may be kept at home.
2e Foils, swords, sabers and bayonets

3e Batons
Not defined by law. Baton refers to several types of cylindrical or tapered instruments composed of a wide variety of materials (finished, not wood in the natural state).
Baton (also called a billy club, nightstick, or riot stick), a type of striking/parrying weapon typically used by police, military or security personnel

4e Air-, CO2- and spring loaded weapons, barring by our minister in accordance with category 1, under 7th, designated objects resembling a firearm suitable for threatening or extortion

5e Cross bow and harpoons
6th. By regulation of Our Minister designated objects capable of inflicting serious bodily harm to persons;

7th. Objects of which may assumed, by their nature or circumstances when found, to serve no other use than to inflict serious bodily harm to persons or to threaten and that are not listed in the other categories.

The provisions on weapons apply also on components and parts which are intended specifically for those weapons.

The provisions on ammunition apply also on components of that ammunition, provided ammunition can be made by it.

Exceptions have been made for:
- The armed forces regulated by the Minister of Defence,
- The police force regulated by the Minister of Justice and minister of Internal affairs
- Other public services and special fraud investigators.

The minister may grant exemption or dispensation to certain groups of weapons.
- Weapons, which cannot be made to use as such.
- Weapons, carrying the character of antiquities
- Other weapons, as far as these are intended for or are part of a collection or a wall decoration

6.4 VARIOUS PERMITS
The Dutch Act Weapons and Ammunition distinguishes 4 types of permits:
- Recognitions (Erkenningen) for commercial use of weapons
- Licences (Consenten) for import, export and transit of weapons
- Permits (Verloven) for weapons (and ammunition) of category III
- Dispensations (Ontheffingen) for weapons (and ammunition) of category I and II
6.5. EXPLOSIVES

Some examples:
- Semtex
- TNT
- Nitro Glycerine
- Tetryl
- Gunpowder (Blackpowder)

Explosives may be detected as follows:
- Visually, when checking, searching or frisking
- Dogs (smell)
- X-ray Scan of luggage (colour, organic material: orange)
- Chemical reaction kit (Expray).
- A recent development is the detection by means of a laser.

6.6. NOTE ON THE TEXT PROVIDED

We have discussed the Dutch Act Weapons and Ammunition (Wet Wapens en Munitie) as an example.


And the European Commission has signed the United Nations Protocol on the illicit manufacturing of and trafficking in firearms, their parts components and ammunition (the “Firearms Protocol”), annexed to the United Nations Convention against transnational organised crime.

Moreover, on July 1st. 2004 legislation on terrorism combatment, applicable to ships engaged in international trade as well as the receiving Port Facilities came into force.

All EU member states have implemented their own legislation, derived from the EU Directives, Protocols and Regulations. When education Security Officers, the National applicable legislation prevails (which follows EU legislation). Aside this textbook, the National Law of the country concerned, must be mirrored against the text provided. Instructions and procedures provided.

6.7. QUESTIONS AND EXERCISES

6.7.1. QUESTIONS

Question 1
Explain the composition of the ‘Act on Weapons and Ammunition’ in your country?

Question 2
At your Port Facility, a person carries a gun. Is that allowed? Why?

Question 3
When searching a car, you find a gun in a package. How do you react?

Question 4
A machine gun is categorised in Category………?

Question 5
How many category weapons are listed in your Act Weapons and Ammunition?

Question 6
Is it allowed to import- export weapons through your Port Facility?
If so, who supervises?
Chapter 6 | Recognition of weapons and ammunition

Question 7
When searching a crew member of a vessel at your Port Facility near your security lodge, appears to possess a death star. What do you do?

Question 8
When checking ship stores, you find in between two pallets a package not listed on the package list. What do you do?

Question 9
Is a special investigation officer allowed to carry a weapon? Why?

Question 10
What type of permits exist in your country, based on the Act Weapons and Ammunition?

6.7.2. Exercise assignments

Exercises

Exercise 1
Describe your actions when a suspected package is found against the outside wall of the office building of your Port Facility.

Exercise 2
A crew member of a vessel, moored at your Port Facility, brings you a dagger he found at the premises. What do you do?

Exercise 3
In your country, where do you apply for a permit concerning a weapon Category III?

In the Netherlands, see: http://www.minjust.nl/borgan/dbzwapens/procindex.htm
INTRODUCTION
Communication is a process at which verbal and non-verbal transfer of information takes place between people.

The communication may be either rationally or instinctive.

In our work, communication is important to:
- Getting general information regarding our work; status, what to expect, standing orders, etc.
- Exchange information with colleagues and superiors
- Getting information regarding security: access control / identity check, etc.
- Handling complaints
- Managing crowds

We will benefit by understanding on how we communicate.

Every organisation has its several networks of organised communication. This is called the formal communication-infrastructure. Receiving daily instructions as well as reporting are examples.

The flows of information crisscross the organisation. Important to know is that communication is not always at the same level of understanding or hierarchy. There is a difference in the way we communicate when we talk to our boss or to a colleague.

‘Formal information’ and ‘informal information’
- Informal information does not use the ‘official’ fixed channels
- Informal information may be the so-called ‘circulating rumours’, which are often incomplete and poison the atmosphere. Informal communication often exists of connection-networks where initiatives and/or interests are tested for feasibility.
- This type of communication is difficult to control.

Complaints occur both in our private lives and at work.
- When at work at the port facility, security personnel have to deal with complaints from clients, employees of the port facility, suppliers, visitors, colleagues and sometimes clients.
- A reaction that is against expectations is called a complaint; emotions will almost always be involved.
- Complaints influence other people in the environment.
- Complaints must be dealt with in the right way to prevent things getting worse. Complaints often arise as a result of the way in which people look upon (perceive) something.
- Arguing with the complainer will not solve the problem.

Conflicts may arise on the basis of individual problems or group problems. Each conflict has a history. The act of one person is experienced as unpleasant by another person. In a conflict situation one party will (often unconsciously) stand in the way of the other party. An aggressive attitude or sharp words and/or aggressive gestures indicate that a conflict arises and is growing.

The sooner a conflict is recognised, the more likely is the chance that this conflict does not end in an overt conflict. An overt conflict is e.g. an argument, a gossip war, right and false accusations etc.

7.1. COMMUNICATION
7.1.1 What is communication?
Communication is the process of verbal and non-verbal transfer of selected information and relations between people. When we get into contact with people, we always communicate, by voice and by using words: (spoken language) verbal communication. Instead of words, or besides using words, non-spoken language or non-verbal communication is frequently used. This includes attitude and movement, place in the room, use of time and intonation when speaking. Non-verbal communication is better known as body language.
7.1.2. Types of communication

Non-verbal communication

Facial expressions, gestures and/or posture, voice intonation, are called non-verbal communication or body language. Looking someone in the eye is different from not looking at someone. Even our mere presence is a message in itself. In contact with other people it is therefore not possible not to communicate.

Several investigations have shown that at least 70% of all communication between people takes place by means of sound and body language.

The American psychologist Mehrabian has a theory that when feelings are involved:

- 55% of the communication consists of body language
- 38% is expressed by sound and only
- 7% is communicated by means of words.

If this is right, our feelings are expressed non-verbally for 93%.

Verbal communication

Verbal communication is taken to mean: communicating with the use of words (language). This can be verbal as well as written communication.

7.1.3. Verbal communication

Advantages of verbal communication are:

- the possibility of getting/giving feedback
- it is possible to give a more detailed explanation of difficult points
- it is possible to clarify certain intentions or ideas by means of gestures, stress and intonation
- a good possibility to check whether the information has got across and has been understood

Disadvantages of verbal communication are:

- miscommunication
- distortion of information

7.1.4 Written communication

Advantages of written communication are:

- the same information for everybody (no distortion)
- recorded for later (proof)
- the information does not change (is not coloured)

Disadvantages of written communication are:

- information is never complete
- further information not immediately available
- information is not further explained
- feedback not immediately possible

7.1.5. The communication process

When two or more people communicate, information is passed on. In communication this is called the message.

- The person who delivers the message to another person is called the sender.
- The person who receives the delivered message is called the receiver.

Communication is a matter of two-way traffic.

This means that the receiver, in turn, is also the sender.

Communication can be disturbed by all kinds of causes. This is called noise.

The receiver always reacts to the receiver. Even by saying nothing, body language speaks for itself. There is a big difference between looking at a person and not looking at a person.
Keeping a big or a small distance, your absence, your silence or not answering are all messages to the other person.

When two people are in a living room together, and one of them is reading a book, while the other is watching TV, there will still be communication between them. This is known as unconscious communication.

When professionally communicating, conscious transfer of information is meant. The sender intends to deliver the message (consciously) to the receiver, who will understand the message.

Channel
There are several manners that you can choose for delivering a message. This can be done by means of writing, words and/or gestures. The medium used for delivering a message is called the channel.

There are all kinds of channels, such as:
- Sensory channels: sight, hearing, feeling, smelling and tasting
- Mechanical channels: pen, typewriter
- Electronic channels: computer, radio and telephone

Frame of reference
Whether or not a message gets across depends on several factors. It is very helpful when you know some things about the background of the receiver. Cultural differences account for a lot of misunderstandings.

Distance and touch
As an example, Dutch people who for the first time get into contact with people in countries with vivid bodily expressions, experience the short physical distance that these people keep during their conversations sometimes as too close and they even call these people obtrusive. These people for their part find the Dutch cold and aloof because they keep such a distance.

Eye contact
It is self-evident that we look at each other during a conversation, it is evidence of credibility. However, in some countries eye contact during a conversation is not so self-evident at all.

7.1.6. Noise
External and internal noise
External factors that distract the receiver and thus disturb communication are regarded as external noise. When someone is telling something in a noisy room, it is very likely that you will miss parts of the story. Internal noise is when something is wrong with one of the senses, or a creaky telephone line or the illegible handwriting of the sender. The receiver may have false expectations regarding the message; he can be emotional or not have enough prior knowledge of the subject. He may even be distracted by his own thoughts.
7.1.7. Active listening
Listening is an important part of communication between people. Listening carefully not only means a better understanding, it will also give the speaker the feeling of being understood. The person who is an active listener takes the initiatives to understand the speaker well.

Example active listening:
Speaker: “I don’t understand part of that new contract”.
Listener: “What part is it you don’t understand”?

7.1.8. Types of questions
Miscommunication can be avoided by asking the right question at the right moment. Procedures describe when and what to ask, you decide on ‘how’ you ask it.

Leading questions
You want some coffee, don’t you?
The answer is already in the question. This is not an objective question.

Closed questions
To a closed question only a few answers are possible.
Do you work here? Answer: Yes or no.
Would you like some coffee? Answer: Yes or no
Have you come for loading or discharging? Answer: Loading or discharging.

Reflecting questions
Have I understood it right that you work here?

Open questions
The answer to this type of question is not simply yes or no. It asks for an explanation.

How was your holiday? Where must I discharge? What has happened?

Choice questions
The person spoken to has a choice.
Would you like a soft drink, coffee or tea?

7.1.9. Assertive communication - examples of assertive communication
During a conversation, be:

Direct
Don’t beat around the bush, tell it straight out.

Self-confident
Your thought must be “I can handle the situation”. Think positive.

Positive
In what you say and how you say it.

Clarity
First, work on behaviour; work comes later.
Make sure you know what you want to say and say it.
Do not make any ambiguous remarks.

Specific
Use normal words, no high-flown style.

Exact
Short sentences.
Repeat if necessary.
Do not be too sensitive (Keep feelings under control)
Talk with a colleague about your feelings before you start a difficult conversation.
Remember during a conversation to keep your breathing steady. In this way you can keep your self-control. Take some time after the conversation to recover yourself; take a short walk, take a break. Discuss your emotions with a colleague.

7.1.10. Tips to encourage communication
- The most important means of encouraging communication is to take an active part in it. The sender must be prepared for the receiver.
- Avoid vagueness in communication. Use your own ideas and statements.
- The information must be complete and further information must be given if the receiver requires so by making signals.
- The information must be understandable to the way of thinking of the communication partner.
- Ask closed or reflecting questions to check whether the message has got across.
- Make sure that verbal and non-verbal signals are in conformity with one another.
- Try as much as possible to use more than one way to get the message across. Show things, so that the message will be understood better.
- Repeat the message, preferably by adding something new, so that the interest is aroused again.
- Use your senses as much as possible.
- The preparation of a conversation is important both to the sender and to the receiver.
- Deal with the main points and establish them beforehand (the connecting thread).
- Allow feedback.

7.2. Dealing with conflicts/aggression
7.2.1. Complaints and causes
Both in our work and in our private lives, port facility security personnel have to deal with complaints. Complaints may come from colleagues and from third parties, clients, suppliers, visitors etc. In most cases emotions are involved. Complaints have influence on what you do and influence others as well. Work is not carried out so well or so quickly. Complaints must be dealt with in the right way to prevent things getting worse.

Let us assume that you get a complaint. There are three types of complaints:

The objective complaint:
You consider the complaint appropriate. Deal with the complaint, take your time; listen carefully and ask specifically chosen questions.
Appreciate that the complainer has come to you with that complaint. Bring the non-verbal communication into line with the verbal communication and treat the complainer fairly.

The subjective complaint:
The complainer thinks that his complaint is appropriate, but you do not. Take the complainer seriously. Ask further information. Do not defend yourself and do not argue. Do not interrupt the complainer and let him tell the whole story. Do not get emotional, but deal with it in a climate allowing of consultation.

A camouflage complaint:
These are complaints that have been invented or that are only partly true, because the complainer does not dare to tell the real complaint. This is often caused by shame, distrust or a taboo. There is more going on than it would seem at first.

Complaints often arise because people look at things in a certain way; different people may have different perceptions.

Complaints are not always expressed immediately and are bottled up sometimes. At a later stage this may either lead to an outburst of anger or aggression, or to conflicts.
7.2.2. Dealing with complaints

Dealing with complaints requires a positive attitude of the person to whom complaints are made. Placing yourself in the complainer’s position and trying to sympathise is also called empathy.

Tips for dealing with complaints:

- **LISTEN!** Analyse the complaint. This prevents endless discussions.
- **THANK** the complainer. It takes a lot of courage to come with a problem. See it as a token of faith.
- **USE BODY LANGUAGE.** Do not act like a complainer. Do not cross your arms, otherwise the complainer will find you conceited and obnoxious.
- **LOOK AT THE COMPLAINER:** By doing so, the receiver shows interest in the complainer and his problem.
- **ASK POSITIVE QUESTIONS.** Think of body language.
- **CLARITY:** Be clear and direct when asking questions.

7.2.3. Perception

Perception is a sensory registration of what is happening. However, do we register everything that happens around us, and do we take action on what we register? That depends on how people’s characters are.

The perception process is as follows:

- **Becoming conscious**
- **Attentiveness**
- With our senses – sight, feeling, tasting, smelling and hearing – we perceive stimuli from our environment. We do not generally perceive all stimuli. The level of consciousness determines how we react to these stimuli. When you are sleepy, you will not (be able to) react to certain stimuli. When you are unconscious, you will not react when somebody speaks to you.
- **Interpretation**
- On the basis of our backgrounds (values, standards, emotions and experience) stimuli will subsequently be interpreted.

7.3. Conflicts and aggression: individuals and crowds

7.3.1. Conflicts

Conflicts arise:

- On the basis of individual problems or group problems
- On the basis of organisational problems or systematic (work-related) problems.

7.3.2. How conflicts arise

Conflicts arise when people have completely different wishes, aims, feelings, needs, values and opinions, and communicate or do not communicate and/or do not wish to submit to or go along with those of the other.

When this happens, the opinions differ so much that this is even called polarisation.

The will of one person is incompatible with the will of another person. Who is right is not the point. Both feel that they are intimidated.

Therefore each conflict has a history. It commences with an act or with an omission, which is experienced as unpleasant by somebody else.

7.3.2 Observing a conflict situation

In a conflict situation a person or party may really want something, but something or somebody stops them.

Then the conflict will grow.
**Chapter 7 | Communication and dealing with aggression**

**Fundamental phase**
Signals of agitation, an aggressive attitude, sharp words, irritated behaviour and aggressive gestures will at that moment indicate the beginning of a conflict situation.

**Explicit phase**
Feelings and facts are discussed; the information passed on is biased and exaggerated; supporters are found; a plan is made; breaking down into a smaller group opposed to others.

**Polarisation**
Groups start fighting, literally or figuratively.
Sabotage may take place.
People gossip and scold.

**7.3.4 Conflict management styles**
All people can benefit, both personally and professionally, from learning conflict management skills.

Typically we respond to conflict by using one of five modes:
- Competing
- Avoiding
- Accommodating
- Compromising
- Collaborating

Each of these modes can be characterised by two scales: assertiveness and cooperation. None of these modes is wrong to use, but there are right and wrong times to use each.

The following sections describe the five modes. The information may help each team member to characterise her/his model for conflict management.

**Competing**
Being very assertive without taking the relation into account.

**Avoiding**
Neither being assertive, nor taking the relation into account.

**Compromising**
Taking the relation into account, but also being assertive.

**Accommodating**
Do everything you can to maintain good relations without being assertive.

**Collaborating**
Being very assertive, but also trying to maintain good relations.

**7.3.5 Identifying and approaching conflicts**
It is of course of great importance to identify a conflict at an early stage.

You should always be attentive to the symptoms. This may apply in the home situation, in the own organisation or workplace, but as port facility security personnel you may suddenly be confronted with people who, by one reason or other, get angry or are emotional when they walk in.

Some examples are:
- A truck driver who has to wait long before he can load or discharge.
- A person who, under protest, gives permission to be searched before he is allowed to enter the location.
- Permanent staff who forgot their pass and have to wait for a temporary replacement pass.
• Refusing visitors when safety regulations have been tightened on the location.
• Etc.

7.3.6. Conflict Management Plan

Question: How can this be solved?

Answer: By creating an Individual Conflict Management Plan

A conflict management plan is a thought and behavior process one can follow when in conflict. You create a list of steps you can follow when a conflict comes up so that you can productively manage/solve the conflict. These steps have to be thoughts or behaviors that can be realistically done. The literature shows that, if we can identify we are in conflict and can then implement a conflict management plan, our opportunity for resolution of the conflict increases significantly.

We identify we are in conflict by identifying our physiological responses when in conflict and by identifying thoughts and feelings we are having that trigger us to realize that we are experiencing a conflict.

There are three steps to making a conflict plan.

• First, write down what physiological responses you have when you know you are in conflict (e.g., my palms are sweaty, my heart is racing).
• Second, write down what thoughts you typically have when in a conflict (e.g., “I want to hurt him”; “I want to just get away from her”).
• Finally, list 4–8 steps you can follow to help you manage your thoughts and emotions in a productive way to manage/solve your conflict (e.g., 1. I will take a deep breath; 2. I will think about how I want to respond, etc.).

Some advice:

• Stay calm
• Take a deep breath (breathe out) and wait a minute

• Speak calmly (do not raise your voice)
• Never get emotional
• Do not act like the complainer (do not adopt the same attitude as that person)
• Let that person tell his story
• Do not interrupt him
• Look straight into this person’s eyes
• Do not cross your arms
• Show understanding and try to empathise
• You may say what you do not like about his personal remarks
• Take time to explain the situation on the location
• Try to find a solution
• Stay calm when you show him the way

7.4. Crowd Management and Control

The management of crowds even in times of a non-emergency is a difficult task. It takes extra effort to maintain some sort of control during a crisis. What is said and the actions you take can determine to a large extent the chance of a successful result.

Very often, people in a crowd do not react rationally but are governed by emotions. It is useful to understand how a group of people will react to an announcement.

The following figures are only guidelines as the responses by persons can to a large extent depend on the situation or emergency.

From the initial announcement:

• 10% accept the situation
• 30% investigate
• 60% ignore the situation
After people accept the danger:

- 10% flee thus, will take care of themselves
- 5% will stand and address the event
- 10% help others
- 60% await initiative from others
- 12 to 14% freeze and do nothing
- 1 to 3% panic

Without going into great detail you can see that a large percentage of persons still need help. You can see how the “help group” can aid the “frozen group” and how the “stand and fight group” can be helpful but will still need guidance.

When giving direction in person or by public address system here are some key points:

- think carefully or write down exactly want you want to say, before you pick up the microphone
- try and keep you voice clear and calm
- remember the communication module which stresses simple clear messages
- avoid use of negative messages “At this time we are not going to evacuate the facility”. The personnel will only hear: At this time .. evacuate.
- avoid negative words if possible: bomb, fire, emergency
- people will look for guidance, if possible and warranted, try to use word “I” instead of “We”. “I have decided at this time that security will conduct a full search of the facility ...”.
- at the end of the announcement give an indication of when you will speak to them again and update them on the situation. Mark the time and don’t be late!

In an organisation there is an informal communication infrastructure next to a formal communication infrastructure. The formal communication is laid down in regulations, whereas the informal communication mostly consists of incomplete circulating rumours, which are difficult to control.

A reaction to a deviating expectation pattern is called a complaint. Something is disapproved of, or people disagree with procedures. This is usually expressed in disappointment, anger or dissatisfaction.

Conflicts arise on the basis of individual problems or group problems. The escalating of conflicts can mostly be avoided if signals of a conflict are recognised at an early stage. These signals can be:

- An aggressive attitude
- Sharp words and/or
- Abrupt and aggressive gestures

An overt conflict consists of arguments, gossip war, right and false accusations.

The styles of conflict management, forcing, avoiding, compromising, accommodating and collaborating, are used by anyone (mixed up if necessary). Aggression cannot always be stopped or solved.

If possible, use in actual practice the tips mentioned in ‘identifying and approaching conflicts’

7.6. QUESTIONS AND EXERCISES

Question 1

What is communication?
Question 2
Why is non-verbal communication important when communicating?

Question 3
What does verbal communication mean?

Question 4
What are the advantages of verbal communication?

Question 5
Give a short description of the communication process.

Question 6
What is meant by noise during communication?

Question 7
Mention 3 causes of a conflict.

Question 8
What phases does a conflict situation consist of?

Question 9
One style of conflict management is being very assertive, while you do not take your relation into account. What is this style called?

Question 10
A truck driver is angry and scolding when he enters the security lodge of the port facility. How do you react and what are the tips that prevent this situation from escalating?

Question 11
What is a Conflict Management Plan?

Question 12
How to approach angry crowds?
Chapter 8 | Dangerous Commodities

8.1. WHAT ARE DANGEROUS GOODS?

8.1.1. INTRODUCTION

Dangerous goods are not only found in an industrial context but are part of everyday life. You only have to look in the bathroom at antiperspirant or hairspray aerosols which contain propellants that are flammable, or in the garage at tins of paint, turpentine, a can of petrol and gardening items such as weed killer or pesticides. They may have flammable or toxic symbols on them and instructions for their safe use but no mention is made of any transportation requirements to suit the nature of the transportation mode.

All modes, that is land (road, rail), inland waterway, air and sea have regulations in place governing their safe transport and although their classification criteria may be harmonised, each may have specific carriage requirements. At the Port Facility, mostly we will see the markings as used in the IMDG code.

At sea the particular considerations include time to evacuate, availability of emergency services, proximity to land, sea conditions and associated vessel motion and so on.

Or, put simply, on land you can walk away from a situation whilst at sea you cannot.

The carriage of dangerous goods has increased substantially since 1945 owing to the enormously increased use of many of these goods.

Transport of dangerous goods is regulated in order reasonably to prevent injury to persons, or damage to property.

Transport of environmentally hazardous goods is regulated to prevent harm to the environment.

8.1.2. DANGEROUS GOODS

Definition. Goods possessing inherent hazardous properties, the transport of which is regulated in order to prevent accidents to persons or property, damage to the environment, the means of transport employed or to other goods, and their misuse for malevolent acts.


These instruments address classification of dangerous goods, their listing, packing requirements (including standards for construction, testing and approval of all kinds of packaging, containers and tanks), marking, labelling, documentation, loading, stowage, segregation, emergency response, training, supervision, construction and approval of means of transport and their operation.

The main international legal instrument, harmonised on the basis of the UN Model Regulations, are the International Maritime Dangerous Goods (IMDG) Code; the ICAO Technical Instructions for the Safe Transport of Dangerous Goods by Air; the European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR); the European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways (ADN); the Regulations concerning the International Carriage of Dangerous Goods by Rail (RID).

Dangerous goods can be defined as substances, articles or materials which are capable of posing a significant risk to health, safety, property or the environment when transported by air, inland waterways, rail, road or sea.

Dangerous goods can be carried safely providing certain principles are adopted. They have been used in developing international and national regulations for the safe transport of dangerous goods by air, inland waterways, rail, road or sea.

In spite of the preventive regulations accidents or incidents with dangerous goods during transport will happen eventually.
An accident is an occurrence associated with and related to the transport of dangerous goods which results in:
- fatal or serious injury to a person or
- major damage to property of the environment

An incident is an occurrence other than an accident associated with and related to the transport of dangerous goods which results in:
- injury to a person
- damage to property of the environment
- fire
- breakage
- spillage
- leakage of fluid or radiation or
- other evidence that the integrity of the packaging has not been maintained

In order to prevent or minimise the possibility of an accident or incident, proper measures must be taken. The execution of these measures will be successful only, when all personnel involved are properly trained with the right amount of knowledge and expertise.

All equipment to be used must be available in the required capacity and maintenance status.

At last, the organisational approach of incidents and accidents determines the efficiency of measures taken: from education to repression and aftercare, from all involved.

In this respect, the security guard has an important task.

When an incident or accident happens, and safety is involved, the emergency response crews must be able to attack as soon as possible to minimise the consequences to people, assets and environment.

Instructions are in place on how to grant access to fire brigade, police and other services required.

Traffic regulation will be ordered.
Evacuation scheme, when needed, put into force.
Security and assistance are two major drives at such an occurrence.

8.2. INTERNATIONAL CODES AND GUIDELINES RELATING TO THE CARRIAGE OF DANGEROUS GOODS - INTERNATIONAL MARITIME DANGEROUS GOODS (IMDG) CODE AND THE EUROPEAN AGREEMENT CONCERNING THE INTERNATIONAL CARRIAGE OF DANGEROUS GOODS BY ROAD (ADR)

8.2.1. INTRODUCTION

The International Conference on Safety of Life at Sea, held in 1960, laid down a general framework of provisions in chapter VII of the Convention and invited the International Maritime Organisation (IMO) to undertake a study with a view to establishing a unified international code for the carriage of dangerous goods by sea. This study should be pursued in co-operation with the UN Committee of Experts and should take account of existing maritime practices and procedures.

Such an international code should cover at least the following subjects:
- classification
- identification (description)
- a list of dangerous goods
- labelling
- the shipping documents
- packing;
- container traffic; and
- stowage, with particular reference to the segregation of incompatible substances

IMO’s Maritime Safety Committee appointed a working group drawn from those countries having considerable experience in the carriage of dangerous goods by sea.
In 1965 the first edition of this Code has been completed by the working group, approved by the Maritime Safety Committee and adopted by the Assembly of IMO. The Assembly has recommended the IMDG Code to Governments for adoption or for use as the basis for national regulations. The IMDG code has been amended several times since.

In discussing aspects of international codes and guidelines for vessels carrying chemicals, under IMO rules and recommendations a distinction is made between dangerous goods in:

- packaged form,
- solid form in bulk and
- liquid form in bulk.

The latter category is divided into:

- oil,
- noxious liquid substances and
- liquefied gases.

8.2.2. The IMDG Code (International Maritime Dangerous Goods Code)

The International Maritime Dangerous Goods (IMDG) Code was developed as a uniform international code for the transport of dangerous goods by sea covering such matters as packing, container traffic and stowage, with particular reference to the segregation of incompatible substances.

Development of the IMDG Code

The development of the IMDG Code dates back to the 1960 Safety of Life at Sea Conference, which recommended that Governments should adopt a uniform international code for the transport of dangerous goods by sea to supplement the regulations contained in the 1960 International Convention for the Safety of Life at Sea (SOLAS).

A resolution adopted by the 1960 Conference said the proposed code should cover such matters as packing, container traffic and stowage, with particular reference to the segregation of incompatible substances.


Since its adoption by the fourth IMO Assembly in 1965, the IMDG Code has undergone many changes, both in appearance and content to keep pace with the ever-changing needs of industry. Amendments which do not affect the principles upon which the Code is based may be adopted by the MSC, allowing IMO to respond to transport developments in reasonable time.

Amendments to the IMDG Code originate from two sources; proposals submitted directly to IMO by Member States and amendments required to take account of changes to the United Nations Recommendations on the Transport of Dangerous Goods which sets the basic requirements for all the transport modes.

Amendments to the provisions of the United Nations Recommendations are made on a two-yearly cycle and approximately two years after their adoption, they are adopted by the authorities responsible for regulating the various transport modes. In that way a basic set of requirements applicable to all modes of transport is established and implemented, thus ensuring that difficulties are not encountered at inter-modal interfaces.

What’s in it

The Code lays down basic principles; detailed recommendations for individual substances, materials and articles, and a number of recommendations for good operational practice including advice on terminology, packing, labelling, stowage, segregation and handling, and emergency response action.

This code lays down certain basic standards concerning the transport, handling and storage of packaged goods by sea.
It deals with the:

- classification
- documentation
- storage/stowage
- segregation
- packing
- marking and labelling
- placarding of packaged dangerous goods

Other sections of the IMDG code of interest to responders are:

- requirements for written statements in the form of declarations or certificates that packages, freight containers and/or vehicles are properly packed
- requirements for proper shipping name, durable markings that include the UN number and in the case of marine pollutants, the addition of “Marine Pollutant” on the label
- requirements that each package offered for transport be clearly identified with distinctive labels or stencil marking
- specific requirements for segregation of incompatible cargoes and
- special list/manifests of dangerous goods on the vessel and location details

The two-volume Code is divided into seven parts:

Volume 1 (parts 1, 2 and 4-7 of the Code) contains sections on:

- general provisions, definitions, training
- classification
- packing and tank provisions
- consignment procedures
- construction and testing of packaging, IBCs, large packaging, portable tanks and road tank vehicles
- transport operations

Volume 2 contains:

- the Dangerous Goods List (equivalent to the schedules in previous editions of the Code), presented in tabular format
- limited quantities exceptions
- the Index
- appendices

Supplements to the IMDG Code contain the:

- Emergency Schedules for Ships Carrying Dangerous Goods (EmS);
- Medical First Aid Guide for Use in Accidents Involving Dangerous Goods (MFAG);
- Code of Safe Practice for Solid Bulk Cargoes (BC Code);
- Reporting Procedures under SOLAS 74 and MARPOL 73/78;
- IMO/ILO Guidelines for Packing Cargo in Freight Containers or Vehicles;
- Recommendations on the Safe Use of Pesticides in Ships; and
- International Nuclear Fuels Code (INF Code).

IMDG Code amendments

Amendments to SOLAS chapter VII (Carriage of Dangerous Goods) adopted in May 2002 make the IMDG Code mandatory from 1 January 2004.

Amendments adopted in December 2004 to the International Maritime Dangerous Goods (IMDG) Code update several sections of the Code relating to the carriage of dangerous goods and also include a new chapter 1.4 on Security Provisions intended to address the security of dangerous goods being transported by sea.

The amendments are expected to enter into force on 1 July 2006, but may be applied on a voluntary basis from 1 January 2005.
8.2.3. Emergency procedures for ships carrying dangerous goods

These procedures outline emergency actions to be used in conjunction with the IMO Medical First Aid Guide (MFAG) during chemical incidents. Each schedule lists:

- special emergency equipment to be carried;
- emergency procedures;
- emergency actions; and
- special remarks for specific substances.

8.2.4. IMDG procedures in the UK – an example

Competent Authority Approvals

The IMDG Code allows and requires competent authorities to issue approvals; relaxations to the Code, in certain circumstances to carry goods where the transport is not specifically set down in the Code. Examples are the use of non-standard packaging or in some circumstances for Intermediate Bulk Containers (IBC).

As an example, in the UK, there are three types of approvals:

- Packages (Including large packages and IBC’s) MSF 3014(r3)
- Portable Tanks MSF 3015(r3)
- Balloon Request Form MSF 3016(r3)

To enable the UK Authorities to process an approval the following information is required:

- completion of the appropriate form given above;
- a safety data sheet giving details of the material being carried.
- Approvals are granted on a case by case basis with safe carriage being the primary and over-riding factor.

Competent Authority Exemptions

In certain circumstances an exemption may be given to a shipping line allowing them to carry agreed dangerous goods on a specific ship where its normal conditions of carriage would not allow it. They generally only apply to domestic ferries. The shipping line should be contacted for details of such exemptions.

8.2.5. Classification of dangerous goods (substances, materials or articles)

For maritime transport goods are considered as dangerous if a substance, material or article has been classified or can be classified in accordance with the definitions and criteria of one of the classes of the IMDG Code. Moreover, in accordance with the criteria for the selection of marine pollutants for the purposes of Annex III of MARPOL 73/78, a number of dangerous substances in the various classes have also been identified as substances harmful to the marine environment (MARINE POLLUTANTS).

Classes and divisions

The IMDG Code comprises the following classes and divisions:

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Explosives</td>
</tr>
<tr>
<td>1.1</td>
<td>Substances and articles which have a mass explosion hazard</td>
</tr>
<tr>
<td>1.2</td>
<td>Substances and articles which have a projection hazard but not a mass explosion hazard</td>
</tr>
<tr>
<td>1.3</td>
<td>Substances and articles which have a fire hazard and either a minor blast hazard or a minor projection hazard or both, but not a mass explosion hazard</td>
</tr>
<tr>
<td>1.4</td>
<td>Substances and articles which present no significant hazard</td>
</tr>
<tr>
<td>1.5</td>
<td>Very insensitive substances which have a mass explosion hazard</td>
</tr>
<tr>
<td>1.6</td>
<td>Extremely insensitive articles which do not have a mass explosion hazard</td>
</tr>
<tr>
<td>2</td>
<td>Gases; compressed, liquefied or dissolved under pressure</td>
</tr>
<tr>
<td>2.1</td>
<td>Flammable gases</td>
</tr>
<tr>
<td>2.2</td>
<td>Non-flammable, non-toxic gases</td>
</tr>
<tr>
<td>2.3</td>
<td>Toxic gases</td>
</tr>
</tbody>
</table>
Class 3    Flammable liquids
Class 4.1  Flammable solids
Class 4.2  Substances liable to spontaneous combustion
Class 4.2  Substances which, in contact with water, emit flammable gases
Class 5.1  Oxidising substances (agents)
Class 5.2  Organic peroxides
Class 6.1  Toxic substances
Class 6.2  Infectious substances
Class 7    Radioactive materials
Class 8    Corrosives
Class 9    Miscellaneous dangerous substances and articles

8.2.6. IDENTIFICATION
When dangerous goods are offered for transport by sea it is essential that they can be identified as such in order to allow those in any way involved to take the necessary care and precautions.

Dangerous goods can be identified by the:
- proper shipping name;
- class;
- UN Number and;
- hazard labels (placards), signs and marks

To ensure that the substance, material or article can be readily identified during transport the proper shipping name, class and the UN Number of a substance, material or article offered for transport and, in the case of a marine pollutant, the addition of MARINE POLLUTANT should be indicated on documentation accompanying the consignment.

For the same reason packages, Intermediate Bulk Containers (IBC’s), and if applicable cargo transport units (containers, freight vehicles, portable tanks (tank containers) and tank vehicles) and bulk packaging containing the goods should be durably marked or affixed with the relevant proper shipping name, UN Number, hazard label(s) or placard(s), signs and marks.

The names of dangerous goods vary greatly, because there are so many different synonyms, initials and abbreviations used for the same substance, material or article throughout the world. To prevent confusion the UN has recommended the use of only one name, which is called the “proper shipping name”. This recommendation has been implemented in the IMDG Code.

**UN number**
In order to facilitate the identification of dangerous goods the UN has assigned a specific number to each substance, material or article and generic or not otherwise specified entry which has been classified as dangerous during transport.

These identification numbers which are called UN Numbers are four-digit figures. Only the UN Numbers below 1000 can be related to substances or articles of a particular class being class 1 (explosives).

The IMDG Code comprises a UN numerical Dangerous Goods List in volume 2, chapter 3.2
### Chapter 8 | Dangerous commodities

#### Dangerous goods list

<table>
<thead>
<tr>
<th>UN No.</th>
<th>Proper Shipping Name (PSN)</th>
<th>Class or Division (1)</th>
<th>Subs. risk(s) (2)</th>
<th>Packing Group (3)</th>
<th>Limited quantities (4)</th>
<th>Instr. (5)</th>
<th>Prov. (6)</th>
<th>Instr. (7)</th>
<th>Provisions (8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2360</td>
<td>DIALLYL ETHER</td>
<td>3</td>
<td>6.1</td>
<td>II</td>
<td>1 litre</td>
<td>P001</td>
<td>-</td>
<td>IBC02</td>
<td>-</td>
</tr>
</tbody>
</table>

Identification number assigned to Diallyl Ether. When the UN number is not given, than check the alphabetical index.

#### IMDG / ADR and UN number

The ADR Hazard Identification Number HIN, also known as the Kemler Code, is carried on placards on tank cars and tank containers running by road under international ADR regulations. Identification numbers are shown in such a way, that the upper number is indicating the danger and the lower number identifies the substances with the UN-number given in the UN Recommendations on the Transport of Dangerous Goods.

An orange blank placard without any numbers indicates vehicle carrying dangerous load (drums, packages, etc.) or multi-load tanker.

**X338 1717** The ADR Hazard Identification Number HIN The substance’s UN Number

Doubling of a figure indicates an intensification of that particular hazard. Where the hazard associated with a substance can be adequately indicated by a single figure, this is followed by a zero.

If a hazard identification number is prefixed by letter ‘X’, this indicates that the substance will react dangerously with water.

<table>
<thead>
<tr>
<th>The first figure of the Kempler Code indicates the primary hazard</th>
<th>The second and third figure generally indicate secondary hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>the hazard is adequately described by the first figure</td>
</tr>
<tr>
<td>2</td>
<td>(flammable) gas may be given off</td>
</tr>
<tr>
<td>3</td>
<td>fire risk</td>
</tr>
<tr>
<td>4</td>
<td>fire risk</td>
</tr>
<tr>
<td>5</td>
<td>oxidising risk</td>
</tr>
<tr>
<td>6</td>
<td>toxic risk</td>
</tr>
<tr>
<td>7</td>
<td>radio-active substance</td>
</tr>
<tr>
<td>8</td>
<td>corrosive risk</td>
</tr>
<tr>
<td>9</td>
<td>risk of spontaneous, violent reaction</td>
</tr>
<tr>
<td>X</td>
<td>reacts dangerously with water</td>
</tr>
</tbody>
</table>

The hazard identification number combinations have following meanings:

<p>| 20 | inert gas                                      |
| 22 | refrigerated gas                              |
| 223| refrigerated flammable gas                    |
| 225| refrigerated oxidising (fire-intensifying) gas|
| 23 | flammable gas                                 |
| 236| flammable gas, toxic                          |
| 239| flammable gas, which can spontaneously lead to violent reaction|
| 25 | oxidising (fire-intensifying) gas             |
| 26 | toxic gas                                     |</p>
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>265</td>
<td>toxic gas, oxidising (fire-intensifying)</td>
</tr>
<tr>
<td>266</td>
<td>highly toxic gas</td>
</tr>
<tr>
<td>268</td>
<td>toxic gas, corrosive</td>
</tr>
<tr>
<td>286</td>
<td>corrosive gas, toxic</td>
</tr>
<tr>
<td>30</td>
<td>flammable liquid or self-heating liquid</td>
</tr>
<tr>
<td>323</td>
<td>flammable liquid which reacts with water emitting flammable gases</td>
</tr>
<tr>
<td>33</td>
<td>highly flammable liquid (flash point below 21°C)</td>
</tr>
<tr>
<td>333</td>
<td>pyrophoric liquid</td>
</tr>
<tr>
<td>338</td>
<td>highly flammable liquid, corrosive</td>
</tr>
<tr>
<td>339</td>
<td>highly flammable liquid, which can spontaneously lead to violent reaction</td>
</tr>
<tr>
<td>36</td>
<td>self-heating liquid, toxic</td>
</tr>
<tr>
<td>362</td>
<td>flammable liquid, toxic</td>
</tr>
<tr>
<td>38</td>
<td>self-heating liquid, corrosive</td>
</tr>
<tr>
<td>382</td>
<td>flammable liquid, corrosive, which reacts with water emitting flammable gases</td>
</tr>
<tr>
<td>3982</td>
<td>flammable liquid, corrosive, which reacts dangerously with water emitting flammable gases</td>
</tr>
<tr>
<td>39</td>
<td>flammable liquid, which can spontaneously lead to violent reaction</td>
</tr>
<tr>
<td>40</td>
<td>flammable self-heating solid</td>
</tr>
<tr>
<td>423</td>
<td>solid, which reacts with water emitting flammable gases</td>
</tr>
<tr>
<td>44</td>
<td>flammable solid, in molten state, at elevated temperature</td>
</tr>
<tr>
<td>446</td>
<td>flammable solid, toxic, in molten state, at elevated temperature</td>
</tr>
<tr>
<td>46</td>
<td>flammable or self-heating solid, toxic</td>
</tr>
<tr>
<td>462</td>
<td>toxic solid, which reacts with water emitting flammable gases</td>
</tr>
<tr>
<td>48</td>
<td>flammable or self-heating solid, corrosive</td>
</tr>
<tr>
<td>482</td>
<td>corrosive solid, which reacts with water emitting flammable gases</td>
</tr>
<tr>
<td>50</td>
<td>oxidising (fire-intensifying) substance</td>
</tr>
<tr>
<td>539</td>
<td>flammable organic peroxide</td>
</tr>
<tr>
<td>55</td>
<td>strongly oxidising substance</td>
</tr>
<tr>
<td>556</td>
<td>strongly oxidising substance, toxic</td>
</tr>
<tr>
<td>558</td>
<td>strongly oxidising substance, corrosive</td>
</tr>
<tr>
<td>559</td>
<td>strongly oxidising substance, which can spontaneously lead to violent reaction</td>
</tr>
<tr>
<td>56</td>
<td>oxidising substance, toxic</td>
</tr>
<tr>
<td>568</td>
<td>oxidising substance, toxic, corrosive</td>
</tr>
<tr>
<td>58</td>
<td>oxidising substance, corrosive</td>
</tr>
<tr>
<td>59</td>
<td>oxidising substance which can spontaneously lead to violent reaction</td>
</tr>
<tr>
<td>60</td>
<td>toxic or harmful substance</td>
</tr>
<tr>
<td>63</td>
<td>toxic or harmful substance, flammable (flash point between 21°C and 55°C)</td>
</tr>
<tr>
<td>638</td>
<td>toxic or harmful substance, flammable (flash point between 21°C and 55°C), corrosive</td>
</tr>
<tr>
<td>639</td>
<td>toxic or harmful substance, flammable (flash point between 21°C and 55°C), which can spontaneously lead to violent reaction</td>
</tr>
<tr>
<td>66</td>
<td>highly toxic substance</td>
</tr>
<tr>
<td>663</td>
<td>highly toxic substance (flash point not above 55°C)</td>
</tr>
<tr>
<td>68</td>
<td>toxic or harmful substance, corrosive</td>
</tr>
<tr>
<td>69</td>
<td>toxic or harmful substance, which can spontaneously lead to violent reaction</td>
</tr>
<tr>
<td>70</td>
<td>radioactive material</td>
</tr>
<tr>
<td>72</td>
<td>radioactive gas</td>
</tr>
<tr>
<td>723</td>
<td>radioactive gas, flammable</td>
</tr>
<tr>
<td>73</td>
<td>radioactive liquid, flammable (flash point not above 55°C)</td>
</tr>
</tbody>
</table>
### Chapter 8 | Dangerous commodities

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>74</td>
<td>radioactive solid, flammable</td>
</tr>
<tr>
<td>75</td>
<td>radioactive material, oxidising</td>
</tr>
<tr>
<td>76</td>
<td>radioactive material, toxic</td>
</tr>
<tr>
<td>78</td>
<td>radioactive material, corrosive</td>
</tr>
<tr>
<td>80</td>
<td>corrosive or slightly corrosive substance</td>
</tr>
<tr>
<td>X80</td>
<td>corrosive or slightly corrosive substance, which reacts dangerously with water</td>
</tr>
<tr>
<td>83</td>
<td>corrosive or slightly corrosive substance, flammable (flash point between 21°C and 55°C)</td>
</tr>
<tr>
<td>X83</td>
<td>corrosive or slightly corrosive substance, flammable (flash point between 21°C and 55°C), which reacts dangerously with water</td>
</tr>
<tr>
<td>839</td>
<td>corrosive or slightly corrosive substance, flammable (flash point between 21°C and 55°C), which can spontaneously lead to violent reaction</td>
</tr>
<tr>
<td>X839</td>
<td>corrosive or slightly corrosive substance, flammable (flash point between 21°C and 55°C), which can spontaneously lead to violent reaction and which reacts dangerously with water</td>
</tr>
<tr>
<td>85</td>
<td>corrosive or slightly corrosive substance, oxidising (fire-intensifying)</td>
</tr>
<tr>
<td>856</td>
<td>corrosive or slightly corrosive substance, oxidising (fire-intensifying) and toxic</td>
</tr>
<tr>
<td>86</td>
<td>corrosive or slightly corrosive substance, toxic</td>
</tr>
<tr>
<td>88</td>
<td>highly corrosive substance</td>
</tr>
<tr>
<td>X88</td>
<td>highly corrosive substance, which reacts dangerously with water</td>
</tr>
<tr>
<td>883</td>
<td>highly corrosive substance, flammable (flash point between 21°C and 55°C)</td>
</tr>
<tr>
<td>885</td>
<td>highly corrosive substance, oxidising (fire-intensifying)</td>
</tr>
<tr>
<td>886</td>
<td>highly corrosive substance, toxic</td>
</tr>
<tr>
<td>X886</td>
<td>highly corrosive substance, toxic, which reacts dangerously with water</td>
</tr>
<tr>
<td>89</td>
<td>corrosive or slightly corrosive substance, which can spontaneously lead to violent reaction</td>
</tr>
<tr>
<td>90</td>
<td>miscellaneous dangerous substance</td>
</tr>
</tbody>
</table>

### 8.2.7. Labels (placards), signs and marks

A method of identification of the specific hazard(s) of a dangerous substance, material or article is the use of specific labels (placards), signs and marks on packages, Intermediate Bulk Containers (IBC’s), cargo transport units (containers, freight vehicles, portable tanks (tank containers) and tank vehicles) and bulk packaging which indicate the hazard(s) by means of colours and symbols of the enclosed substances, materials or articles.

Hazard labels and placards (enlarged labels) indicating the primary or subsidiary hazard should bear the class number in the bottom corner. Descriptive text on the labels is optional with exception of the labels for class 7 (radioactive materials).

Hazard labels should be used on packages and IBC’s and hazard placards on cargo transport units.

### Freight containers

In the IMDG Code freight containers and freight vehicles are often indicated as “Cargo transport units (CTUs). According to the definition a CTU means:

- a road freight vehicle
- a railway freight wagon
• a freight container
• a road tank vehicle
• a railway tank wagon
• a portable tank

The regulations for the transport of cargo transport units on board ships can be found in volume 1, part 7, chapter 7.4 and for packing of cargo transport units in volume 1, part 7, chapter 7.5 of the IMDG Code

8.2.8. TRANSPORT (SHIPPING) DOCUMENT

When dangerous goods are offered for shipment, similar transport (shipping) documents to those required for other categories of goods have to be prepared.

The form of these documents, the particulars to be entered on them and the obligations they entail may be fixed by international conventions applying to certain modes of transport and by national legislation.

One of the primary requirements of a transport (shipping) document for dangerous goods is to convey the fundamental information relative to the hazards of the goods. It is, therefore, necessary to include certain basic information on the document for a consignment of a (the) dangerous good(s) unless otherwise exempted or regulated in the IMDG Code.

When an existing transport or shipping document, or cargo handling form, cannot be used for multimodal transport the Multimodal Dangerous Goods Form as specified in section 5.4.5 of the IMDG Code may be used.

Fig.: Multiple element gas container
The transport document shall contain the following information for each dangerous substance, material or article offered for transport:

- the UN number preceded by the letters “UN”
- the Proper Shipping Name
- the class or, when assigned, the division of the goods, which may be preceded by the words “Class” or “Division”
- for substances and articles of class 1, the division should be followed immediately by the compatibility group letter
- any assigned subsidiary hazard class or division number(s) enclosed in parenthesis
- the packing group, where assigned, which may be preceded by “PG”

8.2.9. ADR

The European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR) was done at Geneva on 30 September 1957 under the auspices of the United Nations Economic Commission for Europe, and it entered into force on 29 January 1968.

The Agreement itself was amended by the Protocol amending article 14 (3) done at New York on 21 August 1975, which entered into force on 19 April 1985.

The Agreement itself is short and simple. The key article is the second, which say that apart from some excessively dangerous goods, other dangerous goods may be carried internationally in road vehicles subject to compliance with:

- the conditions laid down in Annex A for the goods in question, in particular as regards their packaging and labelling and
- the conditions laid down in Annex B, in particular as regards the construction, equipment and operation of the vehicle carrying the goods in question

Annexes A and B have been regularly amended and updated since the entry into force of ADR.

These annexes were entirely revised and restructured between 1992 and 2000, and a first version of the restructured annexes entered into force on 1 July 2001.

A set of new Amendments entered into force on 1 January 2005, and consequently, a third consolidated “restructured” version was published as document ECE/TRANS/175, Vol. I and II (“ADR 2005”).


Annex A: General provisions and provisions concerning dangerous articles and substances
- Part 1 General provisions
- Part 2 Classification
- Part 3 Dangerous goods list, special provisions and exemptions related to dangerous goods packed in limited quantities
- Part 4 Packing and tank provisions
- Part 5 Consignment procedures
- Part 6 Requirements for the construction and testing of packaging, intermediate bulk containers (IBCs), large packaging and tanks
- Part 7 Provisions concerning the conditions of carriage, loading, unloading and handling

Annex B: Provisions concerning transport equipment and transport operations
- Part 8 Requirements for vehicle crews, equipment, operation and documentation
- Part 9 Requirements concerning the construction and approval of vehicles
8.2.10. International labelling of dangerous goods; IMDG Code labels, signs and marks

8.3. QUESTIONS

Question 1
What is a dangerous commodity?

Question 2
What do we mean when referring to the ‘transport of dangerous goods’?

Question 3
What is required to handle dangerous goods properly?

Question 4
What is the meaning of this symbol?

Question 5
What is a HIN?

Question 6
What does the numbers of a HIN mean?

Question 7
What documents do you need to see as a port facility security guard at access control?

Question 8
What do you do when you notice something incorrect on the freight documents?

Question 9
Who do you inform, what do you do, in case of missing placards?