THE INTERNATIONAL SHIP AND PORT FACILITY SECURITY AND PORT FACILITY SECURITY ASSESSMENT (ISPS) CODE

Dr. Jaime Rodrigo de Larrucea
Maritime Law Professor (UPC)

1.- INTRODUCTION

A new regime of security for international the maritime transport will take effect as of July 2004 following its adoption by the Diplomatic Conference developed in the month of December 2002, when the International Maritime Organization (IMO) established a series of measures destined to strengthen the maritime protection of ship and port facilities and to prevent and suppress acts of terrorism against the activity of the maritime transport. The 1st July 2004 is therefore the deadline for all port terminals with international traffics to implement a protection plan. These measures are added to other programs that already in place, such as the American CSI and C-PAT Programmes.

The Conference adopted several amendments to the SOLAS 1974 Agreement to cover port and the most important result was adoption of the International Ship and Port facility Security (ISPS) Code[1].

The new dispositions include the modification of chapter XI, that now is divided in two parts. The first part defines the changes in the SOLAS Convention[2], whereas the second one anticipates the mandatory nature

[1] *Conference of Contracting Governments to the International Convention for the Safety of Life at Sea*, 1974 ; Conference Resolutions 1-11 and Amendments to the SOLAS Convention and Resolutions 3 to 11 of the Conference on 17th December 2002.

[2] The most significant modifications to *Chapter V (Security of Navigation)* are the following ones:
New *Chapter XI-2* of the Agreement establishes that the ships other than ships of passage and oil tankers of 300Tns. And more, but smaller than 50,000 Tns. of TRB, will have to install an automatic identification system (AIS) that can determine the position of a boat with a precision of five meters, no later than the date of the first inspection of the security equipment of the ship, that it is made after July 1st 2004, or, December 31st 2004. Ships being equipped with AIS will at any moment maintain them operational, except when the international agreements, rules, or norms for protection of navigation information arrange for it.
Rule XI-1/3 was modified to require identification of the ship, with her number and the IMO prefix followed by a 7 numbered digit (in agreement with Resolution A. 600 (15)) and permanently marked in a visible place of the skull and the transverse bulkheads of the engine room. The ships of passengers must mark them on a horizontal surface and being visible from the air.
New Rule XI-1/5 introduces the *Synoptic Registry of Ships (RSS)* and establishes that the ships provided with a RSS have to contain her files reflecting information about her flag, names, owners, charterers,

of adopting the new ISPS Code, approved in that same meeting. From the very beginning of this process it was clear that the reference and main responsibilities for these new safety measures would be for the national Governments. Within the ISPS Code, functions and tasks of "the Contracting Governments" are directly and constantly referred to.

An detailed exam of the text and the dispositions of the Code, quoting duties and obligations of the Contracting Governments, emphasises that initiation and maintenance of the processes and procedures necessary to implement the applicable elements of the ISPS Code start and finish with the national Governments members of the International Maritime Organization and signatories of the Code and the corresponding conventions.

This Code recognizes terrorism as the greatest threat weighting on maritime transport. Part "A" contains mandatory dispositions, whereas part “B” refers to dispositions with guidance character.

2.- THE ROLE OF THE CONCESSIONARIES OF A PORT INSTALLATION.

The identification of a number of possible ship/port interfaces will take place in the areas and port facilities set within the located parts belonging to concessionary businesses related to their traffic and activity. Before the regulations of the Code, the concessionary companies had to maintain levels of security similar to those of the port where they were located, so that they themselves did not represent individual threats untied from the global security of the port.

With the entry into force by the ISPS Code, direct responsibility for the protection of the installation returns now to each single concessionary business, which will be forced to manage the corresponding Port Facility Security Plan (PFSP).

All previous plans have to be approved and admitted by the PFSP, and considered suitable and sufficient to guarantee the protection of those facilities, so that at any moment they are in line with the effectiveness foreseen in the Port Facility Security plan of the Port (PFSP).
The maintenance of the operative conditions of any of the plans of a port installation must be preformed on a day-to-day basis by the

classification societies, etc. Any change will be registered in the RBS, in order to provide updated information to the day, along with the history of the preformed changes.

concessionaire, independently whether the assessment plans were designed and developed by them or decided with the corresponding Port Authority.
The particular case of the PFSP can go through any of these two alternatives:

1. PFSP planned by own concession
2. PFSP decided in accordance with the Port Authority.

3.- CONSIDERATIONS ABOUT THE EXPRESSION "*SHIP/PORT INTERFACE*".

A fundamental aspect defining the application frame of the ISPS Code is given by the expression ship/port interface; The Code does not contribute to a definition allowing to clarify its reach and its limitations.

Knowing when and where exactly the application of the Code has to start is not of easy, comfortable and homogenous answer. Nevertheless, variations in this consideration can in reality mean a great dispersion in the decision making processes or the implementation of its measures.

The Communication COM/2003/0229 final from the Commission to the Council and defines in its article 2 the ship/port interface as follows:

> "the interaction that takes place when a ship is affected directly and immediately by activities that involve the movement of people or merchandise or provision of port services to the ship or from this one".

This definition comes to consider how and when we can talk about a ship/port interface, but it does not facilitate the determination of the moment or physical distance that in operational application of the security is always necessary to establish, and even more when the Code establishes, in point 5 of the introduction of the Annex, that "... the provisions relating to port facilities should relate solely to the ship/port interface".

The logical exposition would be to start from the figure of the ship as a primary target around which the whole Code is structured, and so being able to establish that the dividing line marking the limit is given by what represents the first line of protection control.

It has to be considered that the establishment of the limit from ashore towards the ship could correspond to the public port dominion of the port installation.
In the establishment of criteria for determining of the ship/port interface, is the real possibility to find a zone of dockage without interface, where the access is given directly from the gangway of the ship, without an existing preventive or restricted zone to perform controls.

Until now it has been considered that terrestrial transport was made using road networks supported by trucks and tractors that in reality can practically arrive at the flank of the ship so to embarked directly, but if modal railway transport is considered, a new distinctive necessity arises, since most of the present situations. The only control of these units consists of the access by a door without controls at the borders of the port public dominion, without at no later moment having any additional controls and being it therefore necessary in accordance with the principles applied until now- that the physical point where they are due to out, have to be decided and thus defining the ship/port interface.

A new uncertainty in the ship/port interface appears when the ship is in waters port public dominion, being it necessary to consider the different possible situations:

- Moored.
- Moored and operating.
- In manoeuvres.
- In navigation.

In principle, the maritime surface is of exclusive dependency of the corresponding Port Authority, nevertheless, different aspects can be determined:

- When does the bond of responsibilities begin?
- Under which conditions during the operations of the ship before dockage?

In analysing each block of possibilities while the ship is in port waters of public dominion, the following conclusions can be obtained:

A. Voluntary anchorage of the ship in port waters without her intention to accomplish operations, by any cause of navigation when the ship looks for refuge due to bad weather outside the sheltered zone, for

emergency repair, etc., in which case, either the Port Authority or Maritime Authority authorize the situation and assign an area of anchorage without benefiting from the service of pilotage, the ship depends on their Ship Security Assessment (SSA).

B. Forced anchorage of the ship in port waters in order to conduct operations, while awaiting dockage, tide, loading, bunkering while moored, taking of provisions and/or trough, etc., with benefit of the service of pilotage, being representatives of the Port Authority, the ship establishes an interface with the port.

C. Any operation conducted with other ships and boats while in anchorage, establishes a ship-to-ship interface and subsequently an interface between their respective SSAs.

D. Any situation in which the ship is in navigation and manoeuvres until reaching dockage and mooring, the port creates an interface with the ship through the indirect services that are being rendered.

Considering all these diverse alternatives, it is evident that each port installation and each partial or total zone related to the ship, must have previously determined a distance of applicable interface, and when it is not possible because of the port features, to consider the public dominion of the same one as the influence interface, although this treatment represents a strong complication by the scope it includes.

Despite the aforementioned, the successive controls starting from the first and not yet being the objectives of Code ISPS of application, they will have to be closely coordinated amongst each other in order to create the necessary sealing of the protection system.

4. - JURIDICAL ASPECTS OF THE PORT PROTECTION

4.1. INTRODUCITON

Europe insists in finding protection solutions with a worldwide impact as the EU operated in a global economic context. But at the same time, Europeans point out that maritime protection should not turn into a unfair competence issue in particular within the EC boundaries. It is worth noting that the measures adopted by the diplomatic Conference it is limited to ships and port infrastructures, integrated by the ship/port

interface, but not to the harbours themselves, for which the Commission is already working on a legislative initiative to regulate their protection.

The main object of this regulation[3] is to settle and apply communitarian measures to improve vessel protection used both in international and national traffic, together with the port infrastructures related to them in front of illicit deliberate actions. Additionally, the Regulation pretends to establish a platform for the harmonised interpretation and application, and the communitarian control, of special measures to increase the maritime protection approved by the Diplomatic Conference of the IMO.

In this sense, the Spanish regulation goes further than the IMO measures, as it makes compulsory some ISPS Code sections which are only contemplated as recommendations in their original text (for example it broadens the measures to the passenger ships in national trips and it also increases the security analysis for certain national voyages).

4.2. - NATIONAL PORT SECURITY AUTHORITIES.

The ISPS Code states that the Contracting Governments and or their respective authorities shall adopt a series of measures to comply with its requisites and sections.

Given the fact that certain countries have many port installations and huge geographical extensions in need of security analysis, certain sections assign several tasks and responsibilities at the local level of that country. It will be the responsibility of the designated Authority to determine what measures are necessary at national level to comply with the ISPS Code and to establish a cooperation field between the several governmental organisations, local administrations and port and maritime transport sector.

It also establishes that such an Authority shall limit the functions and duties of those entities to guarantee the maritime security at national and international level.[4]
Despite the establishment of a cooperation field between governmental organisms with specified duties, the maritime commerce dynamics and

[3] *Proposal for a Regulation of the European Parliament and of the Council on Enhancing Ship and Port Facility Security* (presented by the Commission) COM (2003) 229 final 2003/0089 (COD).

[4] Ibíd. Part A, Section 1.2.

the port installations will most probably require the assistance of non-governmental organisations and that of the private sector. The ISPS Code also states that the Designated Authority can allow that Recognised Security Organisations (RSO) undertake certain functions related to the security of port installations and services.

4.3. - RECOGNISED SECURITY ORGANISATIONS.

In its article 4.3 of its Part A, the ISPS Code states the Designated Authority can allow certain Recognised Security Organisations (RSO)5 undertake certain functions related to the security of port installations and services. It is necessary to consider the type of functions that could be performed by these organisations recognised to evaluate their competence to perform the assigned tasks. A Port Authority could be designated or even a port service or installation provider as Recognised Security Organisations, provided it has the certificate contemplated in the ISPS Code. 6

A Recognised Security Organisations is defined as '… the organisation that has been recognised by the Spanish Maritime Administration or any other Member State of the European Union7…', being a classification society8 or another private entity which evaluates the maritime security in the name of a Member State of the European Union and that has been recognised to take such activities under the Regulation. As soon as the

[5] See also: Resolution IMO A. 739 (18), Annex, Appendix 1*)-(" Directions relative to the authorisation of the organisations that act in the name of the Administration*"), Resolution OMI A. 789 (19)-("*Specifications related to the functions of recognising and certification of the recognised organisations acting in the name of the Administration) and* Circular MSC.

[6] Ibíd. Part B, Sections 4.3 and ff.

[7] Ibíd. Art. 2.g).

[8] The EU has recognised the following Classification Societies:

- American Bureau of Shipping (ABS)
- Bureau Veritas (BV)
- China Classification Society (CSS)
- Det Norske Veritas (DNV)
- Germanischer Lloyd (GL)
- Hellenic Register of Shipping (HRS)
- Korean Register of Shipping (KR)
- Lloyd's Register of Shipping (LR)
- Nippon Kaiji Kyokai (NK)
- Registro Italiano Navale (Rina)
- Registro Internacional Naval (Rinave)
- Russian Maritime Registry of Shipping (RS)

Public Infrastructures Ministry had authorised an RSO to undertake those inspections and controls stated in the Regulation through authorisations, this will convert into an authorised Organisation.

According to the Code, a port, a Port Authority or those trading with port installations could be designated as an RSO as long as they posses the relevant know how in protection issues9, including the approbation of vessel security plans, or modification of them, in the name of the Administration; verification and certification that the vessel complies with provisions contained in chapter XI-2 and in part A of the ISPS Code, to take evaluations of the protection of the port installations required by the contracting government and the assistance of the companies or port installations regarding the protection of the port infrastructures. In case an RSO had already evaluated the vessel, that same RSO will not be able to be authorised to approve the vessel protection plan.

4.4. - THE PORT AND THE PORT AUTHORITY AS RSOs.

The ISPS Code states in Part B (art. 4.7) that it is possible to designate as RSO a port, a Port Authority or the owner of a port installation if they are in possession of the necessary know-how of the protection issues, including:

1. Specialised knowledge of the relevant protection issues
2. Relevant knowledge of the operation of the vessels and the harbours, including detailed knowledge of the project and port construction
3. Capacity to evaluate the common risks in relation to protection of the port operations and the port installations including the ship-port interface and way to reduce such risks.
4. Capacity to update and improve the specialised knowledge of its personnel
5. Capacity to control that its personnel are confident
6. Capacity to maintain the appropriate measures to avoid its non authorised divulgation
7. Knowledge of chapter XI-2 and part A of the Code and the national and international legislation relevant to the subject of protection and security
8. Knowledge of the tendencies and threats to protection
9. Knowledge of detection of weapons and dangerous goods
10. Knowledge of recognition of dangerous people
11. Knowledge of the techniques used to avoid protection measures

9 Consideration of the *ISPS Code*, Annex 1, Part B, Sections 4.7 and ff.

12. Knowledge of equipments and systems of protection and watching and of its operational limitation.

4.5. - OPERATIVE FIGURES

In the concept of the several types of interface created according to the operational characteristics of the port installations, certain aspects can be identified that need to be précised:

A) Port Facility Security Officer (PFSO)

Paragraphs n 17 refer to the profiles committed to the Port Facility Security Officer (PFSO) that will be designated to each and every port installation. His responsibilities will focus on evaluate a complete initial evaluation of the port installation, guarantying and implementing the elaboration and maintenance of the protection plan of the port installation and taking periodical inspections of protection of the installation to make sure that the measures of protection are still covering gaps and upgrading the plan according to the changes in the installation.

B) SHIP SECURITY OFFICER (SSO) AND COMPANY SECURITY OFFICER (CSO)

The figures of the SSO and CSO do not precise additional interpretations, for its presence is a policy of relation with the human resources established either by the carrier or by the port in question.

The Flag State Implementation (FSI) subcommittee of the IMO has decided to recommend to the Maritime Safety Committee (MSC) to establish that the Master of a vessel could be designated as Ship Security Officer[10]. However, with the CSO figure doubts can be raised to consider the interface located in the vessel.

1. When the vessel has its own port terminal, the company is present at all times and its disposal is immediate, covering the necessary protection needs in a large number of probabilities in the interface.
2. when the vessel is in a service terminal of another owner, if the company has representation at the harbour, it is also easy to designate a person of their staff to assume CSO functions.

[10] See Briefing 11/2004 of the Subcommittee (FSI).

3. the problem arises frequently, when the vessel arrives at port in which the ship owner has no branch, two solutions can be adopted:

    a. the consignee will be the CSO
    b. the port installation will designate a person.

According to 3.a. the consignee will represent another dimension of the ship owner, compatible with the existing one, that make possible the final objective of commercial maritime transport.

According to 3b many negative aspect will arise, for the person will not be hundred per cent independent and the port installation can see its duties and protection affected.

4.6. - PORT FACILITY SECURITY ASSESSMENT (PFSA).

The PFSA establishes the relative importance of the different structures and facilities for the functioning of a port installation. This process of identification and evaluation is crucial, since it is the base for determining strategies of risks attenuation related to goods and structures and to protect them against an upcoming negative event. This process will take into consideration possible loss of lives, economic importance of the port, its symbolic value and the presence of governmental facilities.

The correct assessment of protection, carried out by professionals with deep knowledge in harbour security, is a process that has to identify goods and infrastructures that are important to protect; to select and to classify by precedence measures to resist threats to the detected soft spots. The PFSA must consider aspects of the harbour installation, its physical protection and structural integrity, the systems of personnel protection, norms and procedures, radio electric and telecommunications systems, including computer science systems and networks; transport infrastructure; services public; and other zones that, when suffering damages, or used as observation point for illicit aims, could put in danger people, goods or operations that are performed within the harbour installation.

4.7. - ARTICLE 132 OF THE SPANISH PORT LAW.

In its article 132, the Spanish Port Law (Law 48/2003 of November 26th: *Ley de régimen económico y de prestación de servicios de los puertos de interés general")* establishes an ample and exhaustive control by the Port Authority related to the following areas, not withstanding the competences that correspond to other branches of the Public Administrations and the responsibilities of other users and concessionaires of the port:

- Compliance of rules relating to admission, manipulation and storage of dangerous goods.
- Compliance of regulations referring to coordination of activities for labour risk prevention11.
- Regulations regarding security systems, including protection against antisocial and terrorist acts.

In agreement with current legislation on prevention and emergency control, each Port Authority will issue a so-called "Plan of Interior Emergency" for each port they manage and it will be part of the port decrees. "Plan of Interior Emergency" consists of equipping to the Port with their own resources and personnel, able to carry out actions of risks prevention, as well as of alarm, evacuation and aid, fire extinguishing, rescue, salvage and rehabilitation of essential services. With such aim, the aforementioned plan establishes training activities, not only for all the personnel being directly involved, but also for people of the port surroundings.

4.8. - FORMAL BINDING AND COHERENCE OF THE PROTECTION IN THE SPANISH PORT SYSTEM.

On the basis of article 16.4 of ISPS Code, the Port Facility Security Plan will have to be combined with the Port Facility Security Plan or any other plan of the Port for emergency situations, or be part of them. Unlike loading ports, cruises ports and terminals must take measures that correspond to the civil defence, given the number of passengers they transport and interact with ship/port interface, the commercial and administrative areas that are part of the terminals and the areas visited within the tourist site.

5. - CONCLUSIONS

[11] Refer to rules established in article 24 of the *Spanish Law 31/1995,* of November 8th.

The Code the International of Protection of Ships and Port Facilities represents a complete programme to improve the general profile of security in the international maritime commerce. It give Contracting Governments a direction endorsed by a methodology that is centred in the identification of assets and the vital infrastructure for an uninterrupted and safe flow of commercial maritime operations, recognizing, at the same time, that there can be vulnerabilities that put those critical elements at risk.

Having identified those vulnerabilities, the ISPS Code offers a direction for elaborating, approving and implementing suitable security plans that will eliminate or attenuate the exhibition of those vulnerabilities to well-known or perceived threats.

The ISPS Code does not have to be considered a unique and absolute source with regard to international port security, but has to be seen like a document containing a series of norms and optimal practices that offer Contracting Governments or Designated Authorities a matrix for formulating their programmes and national plans of port security, granting them space to carry out amendments and modifications, as conditions or threats vary with time. The ISPS Code has to be considered a dynamic document that will adapt to the changing nature of ports, their operations and infrastructure, and to the nature of threats they are exposed to.