Annex 2. Guidelines for the definition of port boundaries under Directive 2005/65/EC on enhancing port security

Introduction

The first report assessing the implementation of Directive 2005/65/EC - adopted in 2009 by the Commission[5] - considered that a significant number of Member States faced difficulties to achieve the full practical implementation of the Directive, due by 15 June 2007. One of the main difficulties remained the definition of the boundaries of the port in terms of security. This difficulty was reflected in the variety of approaches adopted by Member States in determining the boundaries of the ports falling under the scope of the Directive.

Following the conclusions of this report, the Commission entrusted its Joint Research Centre[6] (JRC) to conduct a study with main focus on methodologies and technical means for efficient implementation of the Directive (Study on Technical Aspects of port Area Security – TAPS II). The definition of port boundaries is one of the core issues addressed in this study which identified the various relevant parameters (Section 2) and developed a methodology (Section 3) based on a systemic process for port boundaries definition.

The definition of port boundaries is naturally linked to port security assessments and plans. In accordance with Article 10 of the Directive, Member States shall ensure that the port security assessments and the port security plans are reviewed at least once every five years. In the conclusion of its second report[7] assessing the implementation of Directive 2005/65/EC, the Commission considers that the use of the methodology developed in the TAPS II study could be useful, where necessary, in order to redefine the perimeter of ports.

These guidelines for the definition of port boundaries have been agreed by the Member States delegates within the MARSEC Committee.

Parameters affecting port boundary definition (TAPS II study)

Port cohesion elements

As a real synergic system, the port cannot perform its functions without the contribution of a set of activities and/or services. The security of the port system depends on the vulnerability of each of its components, regardless their location.

In terms of planning and implementing security measures, a port, as any other system or organisation, has much more control on its internal components than on the external systems/ services.

Directive 2005/65/EC complements the security measures introduced by Regulation (EC) No 725/2004 on enhancing ship and port facility security by expanding a security regime to the entire port and goes beyond the ship/port facility interface. There are some basic elements that glue

[5] COM(2009)2 final
[6] DG JRC - Institute for the Protection and Security of the Citizen (IPSC) – Maritime Affairs Unit
[7] COM(2013)792 final

together various areas, activities, installations, infrastructures or organisations in one entity which is commonly understood as a port.

Before detailing any considerations on how and where to fix the port security boundaries, it is important to have a common approach as to when port or other facilities, terminals, installations, marinas etc. are part of a single port in terms of security requirements and when they are not. The factors that contribute to such a decision are common essential port element considered as ***cohesion elements***. A non-exhaustive prioritised generic list of such cohesion elements would be:

1. Common main port infrastructure like breakwaters, seawall etc.;
2. Common essential port services such as pilotage, towage, mooring, boatmen (commonly known as technical-nautical services);
3. Common water zones, seaward and inland waterways and anchorages;
4. Common inland access (road and railways) and networks;
5. Common general port services like bunkering, water supply, waste reception, ship chandlers, repair & maintenance services, ICT support;
6. Common emergency services and waterside traffic control systems (VTS), usually performed by a single entity for the entire port area;
7. Common supporting services as shipping agents, freight forwarders, banks, insurance companies, private security companies, railway and bus operators etc.
8. Other geographic, orographic, morphological aspects and port layout.

Port or other facilities, installations, entities or areas sharing such elements participate, as a matter of fact, the same systemic entity (the port) and should be considered in the same port security assessment and plan.

Such port cohesion elements can be identified and evaluated, for each specific case, at the very beginning of the Port Security Assessment - PSA[8].

Type of port facility, area or infrastructure

The classification of ports can depend on several factors: freight type (passenger, ferry, bulk, oil, gas, container, poly-functional), geographical location, sea and land access, urban aspect or administration model.

The definition of the port boundaries depends on the typology of the port as well as on the type of the terminals, infrastructure, and installations. Highly critical ports, terminals or port areas should imply:

- A more complex approach in terms of developing the risk assessment, taking in due consideration all port characteristics, vulnerabilities and potential impacts inside and outside the port;
- More effective security measures according to the three security levels;
- Eventual inclusion of additional adjacent areas under the port security regime in order to enhance the port global security according to the PSA.

[8] Directive 2005/65/EC on enhancing port security, Art. 6.

Port size

Regardless of their size, ports usually have the same structure and service typology. Small ports are not as complex as big ports; and even though the relations between the services, Public Authorities, stakeholders and hosting cities can be simpler, the port boundaries definition process does not differ significantly. Minor complexity can lead to easier solutions and can reduce the time necessary for the process of defining boundaries.

Major ports have often a very complex layout where a variety of activities, industries, communications and urban areas coexist as a result of progressive development during decades or centuries. These are mostly multipurpose ports and can hardly be classified differently. This increases the complexity of the *harbour* layout and functions and of the interrelations between Authorities or other Entities.

Administrative port boundaries

The port, as an entity, is defined as the totality of elements and activities composing it, giving a complete description of its boundaries. A good starting point is to first consider the port's administrative limits and then evaluate if they are consistent with port security purposes for future planning. In most cases, the administrative limits define the ownership of the State or other Public entities, but have not been intended for security purposes. The definition of the port perimeter according to its main activities, services and purposes indicates an approach which is compatible with the port as a functional system.

Cross vulnerability

The vulnerability of port areas depends on their own security parameters as well as on the vulnerabilities of port areas and facilities they are adjacent or interacting with. Moreover, the vulnerability of the whole port is affected by the vulnerability of every single facility or port area. The presence of dangerous goods has to be carefully considered throughout the port and not only evaluated in a Port Facility Security Assessment - PFSA[9].

Port area permeability

Potential attackers could find an easy gap in the port security system in an adjacent area to their final real target. Port areas having a high rate of permeability to external agents, even if they have not a high rate of intrinsic criticality, are a challenge for the entire port security system.

Homogenous & continuous security measures

Security should be homogenous and continuous to be effective. When some areas are protected and others are totally open and unprotected, the latter are the weakest link and can affect the security of the entire port. Zones/ areas inside the port security boundaries may be included for the sake of continuity.

[9] Regulation (EC) No 725/2004 on enhancing ship and port facility security – Annex II (International Code for the security of ships and of port facility – ISPS code), Section A/15.

Port area clusters

According to Annex II of the Directive, not all port areas require the same preventive measures and have the same access requirements. Clusters of port areas can be defined in order to apply homogenous security measures.

Security levels [10]

The port security plan (PSP[11]) provides security measures to be enforced according to 3 security levels. For some areas access control or security requirements should enter into force only at security level 2 or 3. Many areas can be totally open according to their access requirements or port layout as being urban areas or public infrastructures and they do not need to be closed at security level 1. However, these areas should be included in the port security boundaries in order to be able to apply access restrictions when needed.

Additional remarks

Before tackling the main issue of this section, below are some remarks and observations.

Water port access / area

Article 3 (1) of Directive 2005/65/EC states that "port" means any specified area of land and water, with boundaries defined by the Member State in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations. The words "land" and "water" have to be carefully taken into consideration. If the Port Facility Security Plan - PFSP[12] primarily considers the land boundaries, then the PSP should equally consider the water area to be of an added value for the security of port facilities.

Water area provides common sea (river/canal) access to port facilities and other port areas contributing significantly in the integration of the entire port system. Water area is a very strong cohesive element which should be taken into high consideration when defining port boundaries.

Port security sectors

Port areas can be often divided in quite homogenous sectors. In some ports, the existence of a group of adjacent port facilities (PFs) allows the creation of a conveniently fenced and closed secure sector that includes more than one PF and can be entered through one or more gates.

It is possible to define homogenous areas where access control can be applied or, if not, where other homogenous security measures can be implemented. That is to say that it is possible to define clusters of similar areas as far as access requirements, risk assessment and other involved parameters are concerned.

---

[10] Directive 2005/65/EC on enhancing port security, Art. 8.
[11] Directive 2005/65/EC on enhancing port security, Art. 7.
[12] Regulation (EC) No 725/2004 on enhancing ship and port facility security – Annex II (International Code for the security of ships and of port facility – ISPS code), Section A/16.

TAPS II methodology

The proposed methodology is the result of a **systemic approach** where the port is considered as one complex entity whose security or vulnerability depends on all its components. It should be applied to all relevant ports under Directive 2005/65/EC[13].

The methodology consists of 2 fundamental checks/ controls described in the 2 loops in Figure 1. The first defines which port facilities and other elements are to be considered as a part of the same port, while the second defines the effective port security boundaries through security analysis.

The first step of the process is to check if the port, as defined initially, e.g. considering the port administrative boundaries, is effectively a stand-alone port or if it must include additional port facilities. The criterion is sharing one or more essential port elements (or port cohesion elements, as outlined in section 0) with one or more other port facilities. If two or more port facilities share water access, inland access and other essential services, they are likely to be part of the same port. On the contrary, if a port facility is isolated, with none of its essential elements being common to any other port facility, then this first loop can be avoided.

After deciding which port facilities are to be included in the port, the process continues with the second loop to define the port security boundaries. To fulfill the role of port security boundaries, the port reference boundaries (in most cases, administrative) are considered and then - if necessary – they are modified as required. An iterative process is used to consider the port layout and area clustering, along with the vulnerabilities, cross vulnerabilities and impacts analysis. Following the process, additional areas can be included or not within the port security boundaries. It must be noted that the inclusion of certain areas within the port security boundaries does not imply their protection or the application of access restrictions. This can be part of the port security plan and can vary according to the security level considered.

[13] Ports in which one or more port facilities are covered by an approved port facility security plan pursuant to Regulation (EC) No 725/2004 – see Directive 2005/65/EC - Article 2(2).

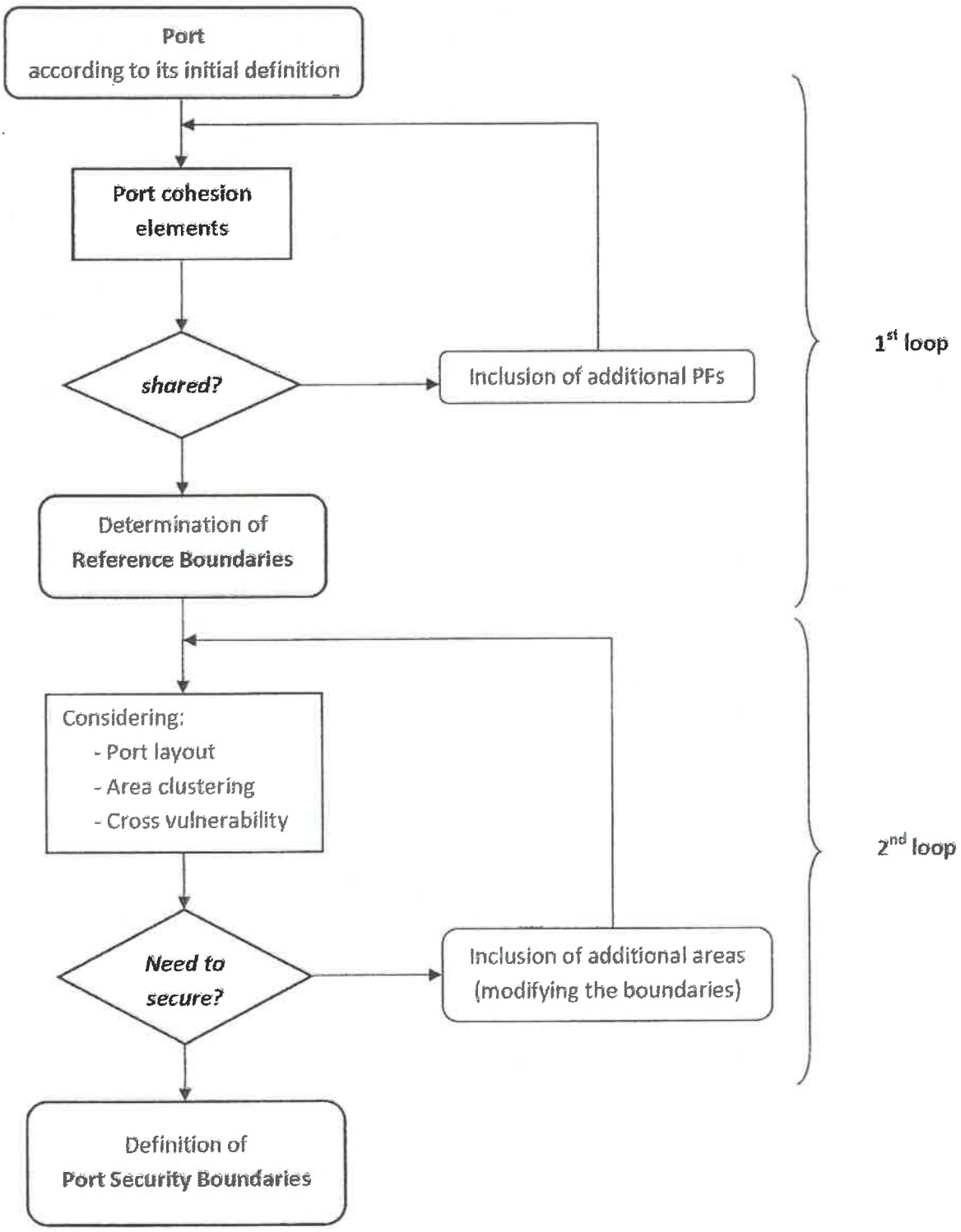

Figure 1: Port security boundary definition process flow-chart

Each of the above steps is further explained in the following subsections:

Port constitutive elements & reference boundaries

The first step consists of the identification of all the essential elements of the port by listing all port facilities including marinas, fishing ports and any other facility, coast/location with port functionality within a region where interactions could be expected.

Table 1 in its first column shows all essential port elements considered as port cohesion elements, mapped against each of the port facilities listed. Typically, such elements include water zones, sea access, land access, essential infrastructure and services. The scope is to identify the relation and the interdependencies in order to verify if those port facilities are part or the same port.

Table 1 provides an example, Port A, for which the security boundaries are to be established could potentially have common elements with port facilities PF 1, PF 2, PF 3 and PF 4. All these entities are placed in the column headers, while the port cohesion elements are in the line headers. All essential / cohesion elements of Port A are identified in the 2nd column. For each of the port facilities listed in the remaining column headers it is considered if they share the Port A's essential / cohesion elements. Accordingly, each of the cells of the table is filled with one of the following marks:

FS → Share fully, if the element of cohesion is, at a great extent, shared with Port A
PS → Share partially, if the element of cohesion is only marginally shared with Port A
-- → No sharing, if the element of cohesion is not shared at all with Port A

The color of the PF xx column should be an indication as to if PF xx should be considered or not within the Port A. For example, according to Table 1, PF 1 should clearly be part of Port A, PF 2 should also be included, whereas PF 3 and PF 4 are not.

If Port A includes PF 1 and PF 2 the boundaries[14] of PF 1 + PF 2 + relevant areas of essential/cohesion port elements constitute the port reference boundaries--starting point for the subsequent analysis.

Table 1: Example of mapping of the essential port constitutive elements between the target port and neighbouring port facilities[15]

Cohesion Elements	Port A : Identification	PF 1	PF 2	PF 3	PF 4
Main infrastructure	Breakwater, dockside	FS	PS	PS	--
Essential services	Pilotage, towage, mooring, boatmen	PS	PS	PS	PS
Water zones	Corridor as per map, anchorages	FS	PS	--	--
Inland access	Access to national highway	PS	PS	--	--
General services	Bunkering, supplies, waste reception	PS	PS	--	--
Emergency services	.....	FS	FS	FS	FS
Supporting services	....	PS	PS	PS	PS

[14] Usually the administrative or the property and boundaries and the boundaries of the associated water zones.

[15] For the purposes of this table, port facilities include also marinas, fishing ports and other facilities with port functionality.

Other	.....	PS	PS	PS	PS

Identification of port assets and infrastructures

In order to define the final port security boundaries, after considering the reference boundaries, common port essential elements and port facilities including marinas, fishing pears and shipyards, other elements (areas, assets and infrastructure) should be identified for security reasons. These elements are not necessarily port areas.

Areas to be protected can be also outside the reference port boundaries (e.g. power supply or water, physical and cyber-based essential systems, emergency services, etc.). Areas hosting such important elements have to be included in the PSP even if they are disconnected, i.e. physically outside the port.

All these areas/ elements have to be identified and marked on the port plan or map in order to proceed with the third step which concerns the port layout.

Verifying the port layout

After defining essential port assets and infrastructure, the evaluation of the port layout is an important stage to verify the resulting port security boundaries. Port security limits should, ideally, contain all port facilities, all essential port elements, assets and infrastructure. However, in order to fulfill their security role, they must also be practical and manageable[16].

As a logical consequence of the port layout evaluation and depending on the location of facilities and relevant areas, it is possible to verify potential crossed vulnerability relations between port portions. In this case, an appropriate evaluation should verify the opportunity to include additional areas which could affect the security of the port. A relevant example is that of connected water zones: sometimes it is impossible to reach a very well confined port facility from the landside, while it could be simple to do so from the water. The inclusion of port water areas has to be carefully considered not only according to the specific facilities they are related to, but also following another logical procedure: waters inside the same seaside protective structures have a strong cohesion. The same concept applies to anchorages or waterways. It is also important to stress that marine **traffic monitoring systems,** useful and used not only for safety reasons but also **for security purposes**, are managed by the Authorities for the entire port area. This can be considered as an additional cohesion element.

Another circumstance is the existence of urban or other totally open areas, very close to port facilities or to other sensitive inland or water areas. Port areas, especially **obsolete or abandoned facilities**, converted to recreational centers, museums, cinemas, recreational activities, shops or supermarkets, which are not intended to perform a "port function" anymore, could be excluded from port security boundaries.

[16] For example, fragmented boundaries are difficult to manage and should, in general, be avoided.

If an area is completely or partially excluded from the port security boundaries, this cannot affect its safety or security. Member States have to guarantee that **equivalent controls and security measures** are applied in such areas to ensure that they are at least as effective as those prescribed for similar areas outside the port.

In the end of the process, due to identified crossed vulnerabilities or the port layout, extra areas have to be included inside port borders even if they are not directly related to the port activities. This can also be due to the need to take into account the orography, road network or port infrastructure.

Those additional areas are listed in Table 2. The first and second columns identify and organize the elements, while the third prioritize their inclusion within the port security boundaries. Accordingly, each of the cells of the 3rd column is filled with one of the following marks:

1 → Priority 1: to be included
2 → Priority 2: to be considered
3 → Not to be included

Areas not considered in this process will be out of the application of any security measures and will not contribute to the security of the port at all.

Table 2: Additional areas / assets / infrastructure, potentially included within the port security boundaries

Area classification	Additional elements	Priority
A 1 (non-operational)	Power supply, sector 1	1
A 2 (non-operational)	Industrial area, sector 2	2
A 3 (public)	Restaurants, shops and pubs, sector 3	3
A 4 (public)	Parking, sector 4	1
A 4 (public)	Railways station, sector 3	2
A 5	....	....

Port typology, size and area clustering

The port typology, PF type, categories of traffic and activities performed within the port borders, are other parameters to be considered when assigning the priorities. Railways and rail accesses will necessarily have an impact on a container port, while pipelines and other similar devices will characterise an oil port.

A careful consideration should be given to the presence (permanent or occasional) of dangerous goods or hazardous materials, not only for maintaining an acceptable security level, but also for evaluating and containing the potential negative effects of a security incident. In case of high-risk facilities, the necessity to have a more effective "double barrier" can result in the inclusion of additional inland or water zones in the port area

according to PSA.

The systemic approach calls for the inclusion within the security port boundaries of all the areas that have a significant role in the economy of the port or where important assets are located. Different areas may have different access requirements. Many of them can be totally open to the public, at least at security level 1.

Permeability to external agents has to be considered under a more complex point of view and be compared with access needs and access restrictions[17]. Interaction of non-homogenous activities inside an area or a system could amplify risks. Inside the port area, as far as access control is concerned, clusters of homogenous areas need to be identified.

Clustering similar areas (with analogous security requirements) has obvious scale effects. Table 3 shows an example of possible homogenous areas and applied security measures.

Table 3: Port security area clustering

Port Security Clusters	Areas	Access requirements	Access control Level #1	Access control Level #2	Access control Level #3	Other security measures
CL #1	PF1, PF2 PF3	Access reserved to authorised personnel (permanent, trusted, occasional)	Access control: Procedures; Technical means On car, trucks & pedestrians; Etc.	Access control: Procedures; Technical means On car, trucks & pedestrians; Etc.	Procedures; Technical means On car, trucks & pedestrians; Etc.	Video surveillance SL 1-3); Patrolling (SL 2-3)
CL #2	Public area sector 1	Open for public use (unlimited, non-identified)	No access control;	No access control;	Access control: Procedures; Technical means On car, trucks & pedestrians; etc.	Signage; Public awareness; Other security measures patrolling (SL 3)
CL #3	....	....	....	....	....	....

In addition, the relevant port security objects can be classified in clusters according to the expected effects of a potential incident, thus the following categories can be identified:

Cat. A: objects whose intentional disturbance would cause many victims, disturbance of national economy, considerable damage to the environment and a shock to the society;

Cat. B: objects whose intentional disturbance would cause some victims, disturbance of regional economy, substantial damage to the environment;

Cat. C: objects whose intentional disturbance would cause no such damage as specified for cat. A-B.

Such clusters can be useful while deciding which security measures have to be applied to port areas. They will be the result of a complex assessment which has to include, among

[17] TAPS II study, section 4.8 – table 4.

other factors, a crossed evaluation of access requirements and of the most probable consequences of potential incidents.