Port Security & Access Control
A systemic approach

Fivos Andritsos
European Commission, Joint Research Centre, Institute for the Protection & Security of the Citizen
fivos.andritsos@jrc.ec.europa.eu

Abstract— Ports constitute crucial intermodal nodes in the freight and passenger transport network as well as important border control points. Their security is therefore of paramount importance not only because of their critical transport functions but also because of their specific role, as control points, in the regional, national and European security. Port security is a cornerstone for the implementation of the new international maritime transport security regime. The aim of the present paper is to analyse the problem, highlight the issues faced in a systematic way towards a better port security without penalising excessively the trade or the port related activities, with a particular emphasis on access control and identity management. Finally, two practical measures for increasing the EU port security are highlighted.

Key words: port security, homeland security, border security, identity management, access control, critical infrastructure protection, ISPS, regulations, directives

I. INTRODUCTION

In 2006, European Commission proposed a European Programme for Critical Infrastructure Protection (EPCIP) implemented through a series of annual work programmes, parts of which are carried out by JRC. This report is based on work undertaken in the frame of the EPCIP-2011 activity on identity management framework for critical infrastructures. Efficient identity management is essential for critical infrastructure protection not only for access control but also for prevention and forensics. It also facilitates incident response, management of priority access during emergencies and restoration of services after emergencies. Ports were chosen as a suitable application area because:

- They are critical infrastructures but also important control points within the transport network and, consequently, for the EU and national borders.
- They provide a good mix of public and private spaces.
- They involve a good mix of trusted, announced or unknown flows of persons, including stowaways and illegal immigrants without any ID documents.
- They involve the access and control of pedestrians, drivers or passengers transiting through public or restricted spaces by a large variety of means.
- They involve a variety of stakeholders.
- Their security is subject to specific international (ISPS code) and European regulations (Regulation (EC) 725/2004 and Directive 2005/65/EC).

Ports are critical nodes in very complex economic intermodal subsystems that move people and goods around the world but are also important border control points. Ports are also shelter for maritime vessels of all kinds and, often, recreational areas. A comprehensive port security framework should consider all these aspects; it should integrate with the transport chain security, corporate local, regional and national level, extending well ashore and quite far out to the sea.

The scope of port security is to prevent any intentional unlawful acts that can threaten citizens’ safety (workers, passengers or crew) and affect economy (e.g., property damage, loss of revenue, trade disruption). It aims at a reasonable protection of the EU citizens interacting without penalizing excessively the trade or generating competition between the EU ports.

The aim of the present paper is to highlight in a systematic way the current issues related to the security of EU ports and give an insight as to the technologies that are best suited to secure EU ports, increasing rather than compromising their efficiency. It will focus of aspects relating to identity management and access control.

II. DEFINITIONS & CONCEPTS

A. Ports & Port Facilities

Ports are very complex and diverse entities. However, in their extreme diversity, ports have some fundamentally common functional characteristics. Their main functions are:

- Move freight and passengers across the sea to land interface and/or
- Service the maritime vessels, i.e. provide a refuge, supplies, maintenance, receive the ship wastes, etc.

Where the intermodal functionality prevails then we speak about commercial ports, otherwise we speak about servicing ports. Commercial ports can be seen as intermodal points of convergence between the sea and the land domain. Ports are maritime but also land terminals as well as important border control points for people and cargo. Some ports, due to their extent, also constitute borders that require surveillance. Ports, besides the above-cited functions, have a range of secondary, yet important functions related to their host cities, the local and the wider communities. They can be broadly classified as of private (like professional or industrial activities, property etc.) or of public nature (like leisure, transport, restaurants, sports).
Up until the September 11 events, security was not among the major criteria in their development, which have been driven mainly by economic efficiency. Building port security retroactively is not a simple matter at all, as it requires systemic intervention in all systems within and around the port, taking into account all the above stated functionalities.

The elementary block, starting point on which port security measures are built, is the port facility. It is important to distinguish between port facilities and ports:

- **Port facility**: a location where the ship/port interface takes place; this includes areas such as anchorages, awaiting berths and approaches from seaward, as appropriate, [Regulation (EC) No 725/2004];
- **Port**: a 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, [Directive 2005/65/EC].

Hence, the term port indicates the area encompassing a number of port facilities plus other public or private installations, infrastructure, spaces, sea access etc. The term port facility, unless otherwise stated, indicates a commercial port facility i.e. one of the following terminal types:

- Container terminals
- Cruise terminals, servicing passengers
Security aims at preventing (or minimizing the probability) that a security threat materialises into a security incident. Once a security incident has happened it becomes a safety concern. Consequently, any actions or measures dealing with the consequences of a security incident (i.e. crisis management, mitigation etc.) should not be classified under the term security. Strictly speaking, security should comprise only work aiming at identifying potential threats and preventing them from materialising. These notions are depicted graphically in Figure 3 above.

A security system can be seen as the control function of a system trying to minimize the effects of a security threat (perturbation), following the simple dynamic control model depicted in Figure 4 above. In such a model, the system’s security has the role of the control function. Anticipating a certain threat, the system takes preventive measures so as to minimize the possible consequences. Such a scheme is generally stable in case of perturbations that are independent of the control. In the case of security, the threat seeks to counter any security measures taken. This is, by definition, an unstable system, characterised, in the case of complex, nonlinear systems by a chaotic, unpredictable behaviour.

To date, security is primarily ensured by deterrence. However, in the modern context of the so-called emerging threats, the importance of deterrence is relative. On top of the existing criminal and antifraud framework, preventive measures are needed. Such measures usually aim at the segregation of potential threatening actors and their means of execution from their assumed targets through access control and screening activities.

Most practical security assessment methodologies start from identifying the assets to protect, proceed to identify some possible threats or attack scenarios and, finally, evaluate the vulnerability of the asset to a given threat and the consequences if it materialises.

III. PORT SECURITY

A. Legal framework and practices

In response to the tragic events of 11th September 2001 and the growing concern for the security, the International

---

1 Roll-On – Roll-Off
2 LNG: Liquid Natural Gas, LPG Liquid Petroleum Gas
Maritime Organization (IMO) agreed on a new security regime for maritime transport the cornerstone of which is the International Ship and Port facility Security (ISPS) code, amendment to the Safety of Life at Sea (SOLAS) convention, operative since 2004. It has been transposed to the EU legal framework by the Regulation (EC) 725/2004 [1].

The cornerstone of ISPS code is the Port Facility Security Plan (PFSP), an essential and integral part of the process of developing and updating the Port Facility Security Plan (PFSP). The assessment should be periodically reviewed and updated, taking into account changing threats and/or minor changes in the port facility and should, in any case, be reviewed and updated upon major changes to the port facility.

PFSA is carried out by the contracting government directly or by recognised security organisations and should include:

- Identification and evaluation of critical assets and infrastructure that it is important to protect.
- Identification of threats to assets and infrastructure in order to establish and prioritize security measures.
- Identification, selection and prioritization of measures and procedural changes and their level of acceptance in reducing vulnerability.
- Identification of weaknesses, including human factors, in the infrastructure, policies and procedures.
- Identification of perimeter protection, access control and personnel clearance requirements for access to restricted areas of the port.
- Identification of the port perimeter and, where appropriate, the measures for access control.
- Identification of the nature of the expected traffic.

A simplified risk-based method / tool is used for a PFSA or a PSA, is the Threat and Risk Analysis Matrix (TRAM). The object is to compare/evaluate security measures that will reduce, independently, the vulnerability or the impact and, collectively, will reduce the overall risk score, having in mind that a security measure for one threat may increase the risk of another. It usually includes 7 steps:

1. Identification of the potential targets
2. Identification of the threat scenarios and threat evaluation
3. Vulnerability assessment of the identified potential targets for each of the identified threats
4. Impact assessment of each potential security incident
5. Risk Score, calculated as the product of: threat x vulnerability x impact.
6. Action Prioritization: assessing the priority for protection measures against each potential incident
7. Finally, a master TRAM for the whole port facility is assembled from the individual vectors of each potential target, grouping similar threat scenarios and common security measures.

### B. Port facility security parameters

Systemic analysis of the main commercial port functions, under the perspective of a citizen-centric security model, resulted in a classification of the main port security parameters and costs. Four main classes of security parameters, further broken-down as in Figure 6 below, were identified:

- **Threat factors**: everything related to the motivation / intention to mount an attack
- **Physical access control**: control of the flow of persons (perimeter security and access control)
- **Material items flow control**: screening of cargo, luggage, personal items, equipment, consumables etc.
- **Information flow control**: efficient and secure management of information concerning the movement of vessels, vehicles and goods; communications.

Port security has a cost, which is not always evident or easy to quantify. Correct cost evaluation of any eventual security measures is crucial for a good planning and, ultimately, an effective implementation of whatever measures are deemed necessary. In Figure 7 below the main cost factors are given.

---

Figure 5: Schematic breakdown of the maritime security threats

In that regulation, *maritime security* is defined as the combination of preventive measures intended to protect shipping & port facilities against threats of intentional unlawful acts. Figure 5 above illustrates the main objectives of maritime security. It involves extremely varied and large inventories, installations and vessels, passengers, crew and port workers but also the general public.

The prime target of ISPS and the Regulation 725/2004 is the security of the maritime vessels and its land interfaces. Port facilities (or terminals) are the elementary vessel / land interfaces and, as such, are the building blocks of port security. It is prescribed that each port facility should have a Port Facility Security Officer (PFSO), a Port Facility Security Plan (PFSP) duly formulated after a dedicated risk analysis and approved by the National Authorities of the Member States. Regulation 725/2004 has been extended into the whole port area by the Directive 2005/65/CE [2].

The cornerstone of ISPS code is the Port Facility Security Assessment (PFSA), an essential and integral part of the process of developing and updating the Port Facility Security Plan (PFSP). The assessment should be periodically reviewed and updated, taking into account changing threats and/or minor changes in the port facility and should, in any case, be reviewed and updated upon major changes to the port facility.

PFSA is carried out by the contracting government directly or by recognised security organisations and should include:

- Identification and evaluation of critical assets and infrastructure that it is important to protect.
- Identification of threats to assets and infrastructure in order to establish and prioritize security measures.
- Identification, selection and prioritization of measures and procedural changes and their level of acceptance in reducing vulnerability.
- Identification of weaknesses, including human factors, in the infrastructure, policies and procedures.
- Identification of perimeter protection, access control and personnel clearance requirements for access to restricted areas of the port.
- Identification of the port perimeter and, where appropriate, the measures for access control.
- Identification of the nature of the expected traffic.

A simplified risk-based method / tool is used for a PFSA or a PSA, is the Threat and Risk Analysis Matrix (TRAM). The object is to compare/evaluate security measures that will reduce, independently, the vulnerability or the impact and, collectively, will reduce the overall risk score, having in mind that a security measure for one threat may increase the risk of another. It usually includes 7 steps:

1. Identification of the potential targets
2. Identification of the threat scenarios and threat evaluation
3. Vulnerability assessment of the identified potential targets for each of the identified threats
4. Impact assessment of each potential security incident
5. Risk Score, calculated as the product of: threat x vulnerability x impact.
6. Action Prioritization: assessing the priority for protection measures against each potential incident
7. Finally, a master TRAM for the whole port facility is assembled from the individual vectors of each potential target, grouping similar threat scenarios and common security measures.

### B. Port facility security parameters

Systemic analysis of the main commercial port functions, under the perspective of a citizen-centric security model, resulted in a classification of the main port security parameters and costs. Four main classes of security parameters, further broken-down as in Figure 6 below, were identified:

- **Threat factors**: everything related to the motivation / intention to mount an attack
- **Physical access control**: control of the flow of persons (perimeter security and access control)
- **Material items flow control**: screening of cargo, luggage, personal items, equipment, consumables etc.
- **Information flow control**: efficient and secure management of information concerning the movement of vessels, vehicles and goods; communications.

Port security has a cost, which is not always evident or easy to quantify. Correct cost evaluation of any eventual security measures is crucial for a good planning and, ultimately, an effective implementation of whatever measures are deemed necessary. In Figure 7 below the main cost factors are given.
C. EU standard instructions for PFSA

These parameters, elaborated for each of the main port facility types, should be taken into account, together with any specific factors, during the port facility security assessment (PFSA). Indeed, such a uniform PFSA methodology is a pre-requisite for establishing in a fair level playing manner, acceptable levels of protection of the EU port facilities.

It is evident that not all port facility types can be assessed in the same way. Security essentially deals with the control of the flows of persons and material items. Thus, the main criteria for the classification of port facilities in terms of their security assessment requirements is the quantity and nature of persons accessing the facility and the volume and nature of the material items handled. Coherently with our analysis, it is proposed to introduce five distinct classes of port facilities, as in Table 1. For each of the above five classes of port facilities there should be a standard set of instructions, preferably in the form of a PFSA report template.

D. EU port facility security relevant events reporting

Another important consideration regarding the PFSA has to do with the availability of security data. Security measures are implemented following assessments and plans based primarily on expert judgment. In order for port security to depend on collective rather than individual knowledge, it must be supported by a stable base for the collection and dispatching of homogeneous security incident data.

Availability of statistically significant data concerning security related events could improve significantly the quality and effectiveness of PFSP. An efficient mechanism for exchanging security related information, perhaps through a central depository / database, will result in better security risk assessment during everyday port operations. Establishing such a security incident reporting system has numerous difficulties, mainly of administrative and political nature, requiring
consensus among member states, technical development and legislation at EU and MS level. The technical issues that should be tackled regard primarily:

- A common taxonomy: a structured set of parameters covering all important aspects of envisaged security incidents and taking into account all stages of process data integration, dissemination and analysis;
- The network topology: an adequate architecture based on the user needs and constraints taking into account issues like data security, ownership and integrity but also confidentiality and privacy; Figure 8 below depicts a such a possible network configuration.

![Figure 8: Possible network topology: in each Member State port facilities/authorities report to a national entity (MS); national entities exchange information mutually; European Central Repository (ECR) integrates information.](image)

An important issue relates to the different authorities under which fall the various port facility security functions:

- Protection of the vessel → captain
- Protection of the port facility → port security officer
- Security of the transport chain → customs
- Protection of the borders → border police

Information fusion/sharing between these entities and, possibly, the commercial and port operators, is one of the prime factors that can enhance both the security and the efficiency of EU port systems.

IV. ID MANAGEMENT & ACCESS CONTROL

Access control is fundamental for the security of any critical infrastructure. Indeed, in order to ensure the security of an infrastructure one should prevent that a security threat manifests itself. This, among other things, implies:

- Prevent physical (or digital) access
- Prevent the ingress of any necessary means of execution (explosives, guns, software) of a threat

In case of physical infrastructures this is typically achieved through a combination of perimeter protection and access control and screening measures, which are typically taken after a security risk assessment study and, consequently, an area / zone planning.

It is very important to stress that security is achieved by a properly balanced combination of various measures, technical systems and procedures applied / supervised by humans, who must be properly trained and motivated. Even the best access control system is of little use without any proper perimeter security while even the most sophisticated technical systems are useless unless they are properly manned and unless the proper procedures are in place.

A. Access control

The aim of access control measures is that of controlling the flow of persons through the designated area access points (i.e. the entrance and exits) ensuring that only authorized / allowed persons and material items can enter or transit through. Security is only one of the reasons for access control, others being safety, efficiency, commercial etc., according to the specific facility, corporate policies etc. Indeed, most of the times, access control equipment and procedures serve other functions as well.

Here, the term access control will refer to the practice of restricting entrance (and exit?) to/from a given area only to authorized persons3, usually by controlling specific access points. An access control system has 3 essential functions:

a. **Entitlement**: provide, based on specific corporate criteria, the access rights, i.e. who can enter where, for how long, for what purpose, how frequently etc.;

b. **Identification**: ensure that the person entering the area is indeed the entitled person;

c. **Documentation**: document all accesses.

These functions are usually achieved by a combination of human (a guard, bouncer, or receptionist), mechanical means (locks and keys) and IT systems (card access system, video surveillance or biometric identification), according to the specific operational requirements.

Access control systems serve to fulfil one or more of the functions above through a combination of procedures and technical means (see Figure 9). Usually, access procedures are outlined in the corporate safety and/or security regulations, which should be in line with any national, EU, or international regulations (SEVESO directive, ISPS code etc.). They determine who, when and through what access control point somebody is allowed to transit and, sometimes, define some follow-up actions.

In general, access procedures are closely linked to the technical access control means and should not be examined apart. On terminals that deal with important fluxes of people, they must not cause significant operational overheads but should integrate as seamlessly as possible with normal operations4.

---

3 Instead, the control of the material items flow through the access points will be referred to as screening

4 For example: integrate security driven functionalities with ticket or customs controls
The most common means of access control is the mechanical key-lock system, which is obviously limited only to the entitlement functionality (possession of the right key). In modern electronic access control systems, a wide range of credentials can be used to replace mechanical keys. Such systems also monitor the accesses and send alarms if a door is forced or held open too long after being unlocked.

Credentials, much like keys, can be passed around, thus subverting the access control list. To prevent this and identify if the credential bearer is the one who is supposed to be, a two-factor authentication can be used. In a two-factor transaction, a second factor is needed along the presented credential for access to be granted. That second factor can be a PIN, a second credential, an operator intervention, or a biometric input.

B. Identity management

Identification is an essential part of access control and, hence, security. As identification we understand all functions aiming at ensuring a positive (or negative) evidence of one’s identity. There exist several identification methods based in one or a combination of the following categories:

- Card based methods, based on something you have,
- PIN based method, based on something you know, e.g. a PIN, an important date etc.
- Biometric methods, based on a physical characteristic, typically a biometric input like a fingerprint

It is important to note that identity management is a notion much broader than identification. It refers to the management of individual identifiers, their authentication, authorization and privileges across the port system with the goal of increasing security and productivity.

In Figure 1 we can note the complexity of the port system, involving a variety of functions, like cargo and passenger transport, maritime vessel support, immigration, customs etc., each with different requirements, under different regulations and supervised by different authorities.

In addition, ports constitute important logistic nodes in a very complex information system, without which the physical flow of goods cannot be ensured. Hence, the identity management in the cyber domain is as important as the access identity management (AIM). Cyber security and port IT security issues have been tackled in numerous publications, among which in [6] and [7] Here, we focus on the management of the identity of physical persons. We must note that, since most port operational and security systems are IT based, the physical and the cyber security are tightly related.

Small insular cruise ports and RO-RO (car ferry) terminals are by far the most challenging cases, due to the big numbers of passengers and crew fluxes. The tendency is to shift the AIM procedures and responsibilities (even border controls) to the operator. This is particularly true in the cruise sector, where most checks are done either by the operator or at the first embarkation.

C. Port actors

A first step for an effective identity management in ports is to identify and classify correctly all the port actors, that is all the physical persons or group of persons that interface in any way with the port.

There are many ways to classify port actors. In what follows, we attempt an as complete classification as possible, pertinent for the AIM of physical persons, related to the port facility and the port area security (see port security parameters in Figure 6) and to the port border functionality:

- Actors who are involved in direct ship/port activities:
  - Essential services pertaining to the ship, such as pilotage, towage, mooring, boatmen;
  - Port operations concerning transhipment, handling and storage (terminal operators and stevedores);
- Actors who are involved in indirect ship/port activities:
  - General services as bunkering, water supply, waste reception, repair & maintenance services;
  - Supporting services as shipping agents, freight forwarders, banks, insurance companies, private security companies, railway and bus operators etc.
- Passengers (cruise-ship, ferry, cargo-ship passengers)
  - Schengen area passengers;
  - Extra-Schengen area passengers;
  - Returning stowaways
- Ship Crews
- Public Authorities as police, customs, port authorities, emergency health services, fire brigades etc.
- Actors involved in the typical activities of marinas:
  - Yachtsmen, crews and their guests;
  - Nautical and sailing schools, recreational activities
- Actors not involved in core-port activities but have a regular access to port areas:
  - Personnel of facilities like restaurants, pubs or shops, which for any reasons are located in port areas, and their suppliers;
– Non-professional fishermen, taxi drivers, etc.
• Other actors who occasionally enter port areas like:
  – Customers of restaurants, pubs or shops located in the port area;
  – Others
• Trespassers:
  – Stowaways;
  – Illegal immigrants;
  – Others
• Security personnel:
  – Police, coast guards, border guards, customs
  – Private security operators

In terms of identity management, independently of their access rights, we could distinguish the following broad classes of actors:

  Trusted: known persons, who have undergone background checks, like employees, authorities, green-lane passengers, regular ship crews etc.

  Identified: positively identified persons, usually through some kind of ID bearing controllable biometric features; passengers, occasional ship crews, occasional workers and suppliers etc.

  Unidentified: persons who cannot be identified either because they, legally, do not have ID documents or because they cannot be checked.

  Trespassers: persons who should but do not have ID documents; i.e. illegal immigrants, stowaways etc.

V. CONCLUSIONS

The starting point for any port facility security plan (PFSP) is a security risk assessment, for which there is no scientifically established methodology. The practical methods currently in use are based on expert judgement rather than statistical or other objective data. However, even these practical methods are not standard across EU, sometimes even across the same national administration.

Even if big security incidents are unpredictable, availability of statistically significant data on past security events/incidents is very important for the further elaboration and improvement of the port facility security methodologies and plans.

Hence, two priority items are judged necessary in the basis of any follow-up measures for the efficient implementation of the ISPS code throughout the applicable EU port facilities:

1. A standard methodology, in the form of unified templates, toolkit, guidelines or instructions for the security risk assessment of port facilities;
2. Setting-up an efficient mechanism for exchanging security incident related information perhaps through a central depository / database that would permit some statistical backing / verification of the various threat scenarios considered.

Port facility protection is necessary but not enough to ensure port security. Directive 2005/65/EC extended Regulation (EC) No 725/2004 security measures to the whole port area, the boundaries of each port (land and sea) being defined by the Member State concerned.

Access identity management in ports is an essential component for the port security (seen as critical infrastructure) but also for the efficient port operations. The diversity of ports, port functions, port actors, regulations and authorities involved is a key issue that has to be overcome. Small, intermediate cruise and, primarily, RO-RO ferry terminals are the most critical in terms of security and access control.

Proper area planning, identification and classification of the expected physical actors according each port / area type and managing the access identities accordingly, with dedicated procedures and technical means (i.e. through green lanes or additional controls, badges etc.) is a first element for an efficient port security. Pushing the access control to the operator and integrating access identity management for all required access functions (border, port and vessel) appear to be other key elements for simpler, more efficient and secure port operations.

ACKNOWLEDGMENT

This paper is, to a large extent, based on work done at the Joint Research Centre of the European Commission in support of the Directorate General for Mobility & Transport (DG MOVE) on technical and scientific aspects of port and port area security. It includes also analysis done in the frame of the EPCIP-2011 study [8] done at JRC on behalf of DG HOME on the Identity Management in Ports, as part of a larger program on Critical Infrastructure Protection (CIP).

REFERENCES