A conceptual framework that monitors port facility access through integrated Port Community Systems and improves port & terminal security performance

Ioannis Koliousis, MSc, MEng, PhD, CFILT
Associate Head of the School of Strategy & Leadership
Coventry University
Email: yannis.koliousis@coventry.ac.uk

Abstract

Ports and terminals are considered critical infrastructure with higher protection requirements for an effective and efficient operation. This research introduces a security enhancement architectural framework for the specific case of port and port terminal facilities' passenger traffic, combining two different attributes, the cyber and the physical, and operationally integrating the proposed subsystem to the Port Community System. More precisely, this paper identifies, introduces and analyses a system that supports risk management by developing and validating a security framework which is based on monitoring access through Automated Border Control (ABC) structures aimed at ports and terminals. Additionally, the modular prototype developed, enhances the information sharing capabilities of the Port Community Systems in a way that improves collaboration for security related procedures, based on existing and easy to develop software capabilities. The architectural framework is validated by domain experts through semi-structured interview workshop improving the robustness of the top-down model for the design and the implementation of a risk management approach based on improved communication sharing and utilizing advanced equipment.

Keywords: Port Community Systems, security, risk assessment, risk management, automation, threat analysis, information sharing, access control

Biographical Note:

Ioannis has academic and industrial experience in the fields of operations & supply chain management, transport management & finance, shipping, transport planning, cargo & freight logistics, public transport, urban logistics, project appraisal, transport policy and energy sources. He has consulting experience from the operational to the strategic level and has participated in different capacities in industry led projects as well as in cornerstone EU funded research projects and regularly advises senior leadership on these topics. He is currently the Associate Head of the School of Strategy & Leadership in Coventry University. Ioannis has a BSc in Maritime Studies (Uni Piraeus, GR), an MSc in Decision Sciences (AUEB, GR), an MEng in Supply Chain Management (Massachusetts Institute of Technology, USA) and a PhD in Transport Strategy and Regulation (Uni Piraeus, GR), for which he was awarded the highly competitive Herakletous-II Fellowship (GR).

1 Introduction

1.1 Overview

Ports and terminals represent an important element in maritime supply chains. Their criticality stems from economic, commercial and security aspects, not only for the local but also for the national economy. This criticality is especially important due to the current changes on the global economy as well as to the global security concerns. This environment pushes port operators to implement reliable and trustworthy e-maritime services in order to improve their efficiency, increase the quality of service and increase revenues.

The range of threats is massive and is increasing. The ports, the terminal facilities and the critical infrastructure in general are becoming an "affordable target". From economic crimes like tax avoidance and smuggling to carrying weapons of mass destruction, to attacking Liquefied Gas Carrier Vessels or to cyber-attacks that may put an entire regional government to its knees, the extent of consequences arising out of a security incident may be undesirably high. Burns (Burns, 2013) measured the economic losses from a hypothetical attack on the Port of Los Angeles/Long Beach at 0.5 billion USD only for the first week following the attack. To this extent, Ernst & Young's 2012 Global Information Security Survey (Ernst & Young, 2012) and PricewaterhouseCoopers' 2012 Information Security Breaches Survey (PriceWaterhouse Coopers, 2013) identified a significant increase in the number of cyber-threats, breaches of high-profile security systems and shut down of e-services all having a direct economic impact.

Current responses to improving the security of a port or a terminal facility include both governmental initiatives, for example the US DoHS (U.S. Department of Homeland Security, 2005) initiative to collect, analyse and fuse information to relevant stakeholders, EU's initiative to assign specific roles to certain authorities and stakeholders (European Commission, 2013), like the EU's definition of the Authorized Economic Operator (European Parliament, 2013) as well as industrial led initiatives like ISO 31000 and ISO 28000 among others. A number of cross governmental initiatives have also been set up, including the Customs Trade Partnership against Terrorism (C-TPAT), the World Customs Organization (WCO) Framework of Standards to Secure and Facilitate Global Trade, the Container Security Initiative (CSI) program led by U.S. Department of Homeland Security, the Global Container Control Program (CCP), a joint United Nations Office on Drugs and Crime (UNODC)/World Customs Organization (WCO) initiative, the Global Trade Exchange, the International Ship and Port Facility Security Code (ISPS Code), etc.

These attempts intend to enhance port security and to complement the already implemented strict monitoring guidelines, but at the same time to reduce both compliance costs and red tape. Strict rules, like 100% scanning in physical inspections, do not individually ensure improved security but are beneficial only as a part of an extended security framework. Due to the massiveness of the port area, unauthorized access becomes an even more imminent danger, which has to be sufficiently addressed.

This article complements existing academic and industrial literature by introducing a security enhancement framework for the specific case of port and port terminal facilities' passenger traffic. The proposed framework combines two different attributes that most commercial ports have, the cyber and the physical characteristic, by becoming an integrated subsystem of the Port Community System (PCS). By developing and validating a security framework based on Automated Border Control (ABC) systems as the main control of these physical threats and their interaction with the PCS, the cyber threats, the study goes a step further in identifying, introducing and analysing a systematic cyber-physical framework to support port access risk management. Additionally, the proposed framework sets up a methodology that enables real-time, multisource information capturing and sharing of potential threats and their respective vulnerabilities. Last but not least, this paper provides feedback captured through a validation workshop that was held with Port Facility Security Officers (PFSOs) from five ports acting as test beds.

1.2 Literature review

Port security is currently being revisited, not only due to the increasing significance of the role of the ports in global commerce but also due to the repercussions to the local, regional and national context of security incidents in lieu of an increasingly complex threat environment. Current approaches to risk management and to port security, based primarily on probabilistic assumptions, have resulted in isolated and inconsistent risk mitigation frameworks with certain but limited applicability.

Unauthorized access of a physical facility, including data centres, terminals, cruise terminal gateways and waiting areas has been recognized as one of the most significant threats. This threat may well exploit vulnerable sub-systems of the port damaging either the physical or the cyber assets or even putting the port's operation at risk. A port operator handles a very large number of persons and vehicles at any given time, transiting through or entering the port's respective catchment area. In order for this not to constitute a violation of access control, authentication and authorization of entrants should be performed on a regular basis and based on specific procedures.

Recent security incidents (the Cyprus Mari Port container blast, the Voltri Terminal Europa container emitting radiation, and numerous other post September 11, 2001 incidents) require stricter port security rules based not only on economic or financial aspects but equally importantly on security criteria, including strict security controls and implementation of safety and security procedures. Similarly, cyber-attack counter measures is also considered in this respect as a precaution of these incidents. US Navy Rear Admiral Thomas (Thomas, 2017) indicates that a certain number of ports still lag behind in technology adoption vis-à-vis these measures. Automated Border Control (ABC) Systems, is an appropriate security control for preventing the non-authorised access, controlling and authenticating related threats of passengers, vehicles and freight. This paper is devoted to developing a security framework based on ABC systems as the main control of these threats and their interaction with the Port Community Systems (PCS).

Relevant literature has identified a number of papers proposing and testing theoretical risk assessment frameworks. For example, Williams (Williams, 2015) introduces the “System-Theoretic Accident Model and Process” (STAMP) as a new model of causality, based on systems and on control theory which identifies specific technical or procedural security requirements by using a System Theoretic Process Analysis (STPA), thus developing port security design specifications that mitigate vulnerabilities. Similarly, analytical approaches to port security (Akhtar, Bjørnskau, & Veistein, 2010), (Ghafoori & Altiok, 2012), (Bakshi & Gans, 2010) seek to minimize the product of (a) the probability of a threat, (b) the probability of a vulnerability and/or (c) the expected value of losses / consequences. Furthermore, a stream of econometric models also analyse the optimal allocation (Burns, 2013) of security resources across supply chains composed of an ever widening disparity of socio-economically successful countries. Many researchers have focused on the physical security of the ports, including access control measures, risk management and vessel safety (Luiijf, Burger, & Klaver, 2003) or on Threat and Vulnerability Assessment methods (Alberts & Dorofee, 2001).

With respect to the PCSs, previous studies investigated PCSs with a particular attention on the relationships among private and public entities (Bagchi & Paik, 2001) or on the process of implementing a PCS (Rodon & Ramis-Pujol, 2006) or even on the architectural attributes of the underlying information systems (van Baalen, Zuidwijk, & van Nunen, 2009), (Koliousis, Koliousis, & Katsoulakos, 2015). Interoperability issues among PCSs at the EU level have also been researched, e.g. Baron (Baron & Mathieu, 2013) stressed that PCS operators are becoming key actors in the maritime supply chain. This literature review suggests that a PCS plays a pivotal role among different supply chain actors including customs and public agencies, business partners and ports, which necessitates the efficient information sharing to ensure improved collaboration. This paper will study this issue of information sharing at the specific level of sharing security related information.

1.3 Knowledge management as the basis of PCSs

In order to effectively secure the transport chain, entities have to control their existing security related knowledge, use it and additionally create new knowledge that will enable them to successfully address potential threats. Knowledge Management (KM) is an approach that utilizes existing experiences and information in an attempt to utilize and create new knowledge. Polyani, (Polyani, 1966) differentiated knowledge between tacit and explicit whereas Duffy (Duffy, 2000) explained that explicit knowledge’s key characteristics include documentation, public status, structure, defined content and consciousness. Explicit knowledge may be captured and shared through information technology; to the contrary, tacit knowledge resides (Duffy, 2000) in the human mind, behaviour, and perception and evolves from human interactions. This paper adopts that explicit knowledge is more appropriate for addressing security related objectives.

KM is a process that identifies, collects, stores and disseminates tacit and explicit information to stakeholders. A wide spectrum of tools is used in this process to support and enable KM and several methods and applications have been proposed. The main categorization is between organizational, ecological, and technological KM. Organizational KM theory focuses on organizational structures and organizational design. Ecological KM theory focuses on people, relationships, and learning communities. Technological KM theory, which is the primary motivation of this paper, focuses on technology and the process of designing knowledge related flows.

Knowledge capturing techniques include content submission, regular training and personal development. This study follows Easterby – Smith and Lyles (Easterby-Smith & Lyles, 2003) who differentiate Organizational Learning, OL, from KM. The latter focuses strictly on the procedural aspects (being the ultimate goal of KM), whereas KM focuses on the content of knowledge and more precisely on its acquisition, creation and dissemination. This distinction helps firstly develop the port security management systems and as a second step, enhance the security related knowledge content. According to King (King, 2009) the knowledge process cycle includes certain activities starting from the KM initiation through to improving the organizational capabilities and performance (as depicted on Figure 1). Additionally, this paper builds on push KM strategies, as defined by Batini et.al (Batini, Lenzerini, & Navathe, 1986) and by Rishe et. al. (Rishe, Athauda, Yuan, & Chen, 2000), who disseminate knowledge through shared repositories. The two main theoretical premises for knowledge sharing repositories (Hansen, Mors, & LØVÅS, 2005) are (a) knowledge codification, the collecting and storing of accessible knowledge for both tacit and explicit items, and (b) personalization, the individually shared knowledge. Relevant tools that support KM and stimulate this research include storytelling, after-action reviews, practice communities, best practice transfer, knowledge fairs and collaborative software among others.

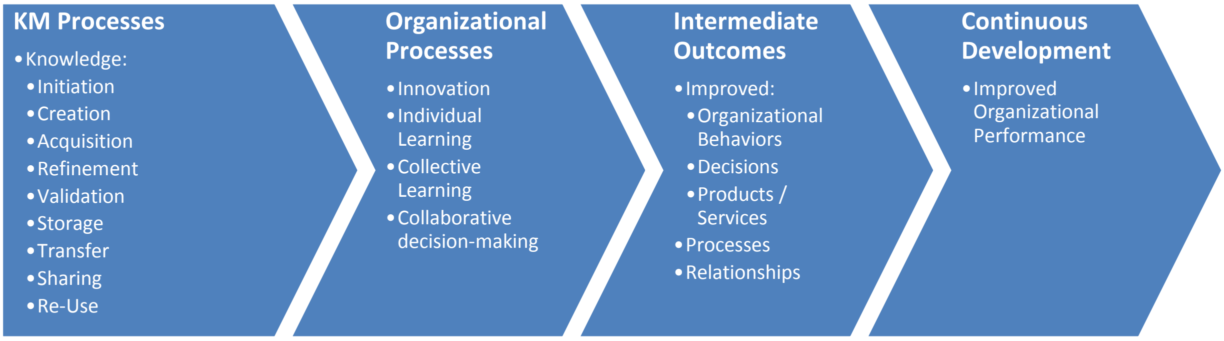


Figure 1 - KM in an organization (Source: adapted from (King, 2009) and (Bhatt, 2001))

1.4 Research objective and methodology

Based on this literature review, traditional port security approaches are predominantly focused on security regulations and compliance, instead of relying on system flexibility, on information sharing and on using advanced technologies and techniques. The frameworks reviewed in most of the cases work well but are isolated and thus, the exploiting of inherent vulnerabilities may prove easier. The proposed framework integrates a targeted risk management approach to an existing system, the Port Community System – PCS, and relying on advanced monitoring technologies, checks real time (unauthorized) access as well as shares this information across a multitude of stakeholders including both governmental agencies and commercial entities. The ports as basic components of critical infrastructure benefit from an improved system through a 3-Step Approach:

- Step I: Infrastructural Upgrade
- Step II: Procedural Upgrade
- Step III: Knowledge Upgrade

Each step is presented in Section 2 (Access control: Effectiveness upgrade through ABC systems), in Section 3 (Procedural Upgrade) and in Section 3.5 (Knowledge Upgrade). The ultimate goal is to improve the operational efficiency and at the same time improve the security effectiveness.

The methodology used is a case study approach validating a proposed framework in five ports whose security needs have significantly grown over the recent years. More specifically, through a semi-structured interview session with Port Facility Security Officers, PFSOs, (at the director's level or similar decision making authority) the applicability and the value of this framework are investigated. As a result, a top-down model for the design and the implementation of a risk management approach is presented based on improved communication sharing and utilizing advanced equipment.

2 Access control: Effectiveness upgrade through ABC systems

2.1 Overview

Unauthorized access in port and in container terminal facilities (whether physical or cyber) is a threat with a high impact causing significant security risks. The ABC systems are an acknowledged control that prevents such risks, especially in port related operational environments. An ABC System is intended for passenger traffic and is based on the biometric identification of the passenger using a biometric-enabled identification (e.g. a passport) enclosing a microchip. This microchip contains information which is checked by the automatic device's readers. In addition, the system compares the unique proportions of a real-time facial image to the image on the passport's chip.

The first ports in Europe that adopted such systems were the Finnish ones, with the Finnish Border Guard extending the use of automatic border control devices to the maritime border crossing point in the West Terminal of the Port of Helsinki. The Port Authority (PA) set up three automatic devices which are expected to increase efficiency by speeding up the border crossing times at the terminal. Following up the trend, the Spanish Ports Authority (Puertos del Estado) has been piloting since 2012 ABCs in certain Spanish ports.

The state of play in the Finnish Ports covers persons entering the Finnish sea borders, who possess a valid biometric passport. These entrants are eligible to use the ABC devices in Helsinki West Harbor (Port of Helsinki, 2016) for the border control both in- and outbound. It was planned that by September 2016, all Finns should be using biometric passports compared to 2017, when all EU citizens should be using only biometric passports. The citizens of the European Union (EU), of the European

Economic Area (EEA) and of Switzerland who possess a biometric passport can use the ABC Gateways. People travelling in a wheelchair or with an infant must still pass through the traditional border control. The Finnish Border Guard's goal is to be a pioneer in the use of automatic devices for border control. The Border Guard has been using automatic border control devices at the Helsinki-Vantaa Airport since 2008. For comparison purposes, 25 border control devices at the Helsinki-Vantaa Airport have an annual throughput of about 300,000.

Commercial insight (Future Travel Experience, 2011) complements experience and reveals that ports are not as advanced as anticipated, especially compared to airports. For example, the Malaysian ports have been piloting ABC systems in addition to Taiwan’s local government authorities who have begun (as early as 2011) trialling ABC systems (Taiwan’s Ministry of Foreign Affairs and the National Immigration Agency). In this context, ABCs were trialled at the Shuitou port in Kinmen, in Taiwan Taoyuan international airport, in Taipei Songshan airport and in Kaohsiung international airport.

The International Ship and Port Facility Security Code (ISPS) has provisions for border control and ports are heavily relying on manual inspections. However, the modern business and operational requirements call for upgrades and the new automated systems can increase value both for port operators and for users, who require efficient security controls. These ABC systems can be extended both for passenger and freight flows to include fast and flexible control tools for monitoring passenger and vehicle lane flows, docks and boarding areas, automation systems for speeding-up boarding flows, OCR cameras to control transit of passenger / vehicles through the boarding areas giving the real-time status of the boarding process and detecting unauthorized access. ABCs are essentially modular systems that are easily implemented and provide for operational efficiency increase. FRONTEX has released a practical handbook with generic requirements (FRONTEX, 2012) for the ABC systems which follows the requirements imposed by the “Schengen Handbook” (European Commission, 2006) and makes several technical recommendations regarding automation of border controls for passenger traffic.

Gate systems and automated access control systems ensure cost effective and quick boarding operations, however, on the other hand they are more prone to cyber related security risks.

2.2 ABCs within the PCSs

Ports around Europe and beyond have been redefining their position on the value chain. Ports are modernizing their service offerings, contributing to improved visibility and sharing various information across supply chain actors. The PCSs that are currently being built offer such visibility throughout the chain and act as Single Windows (United Nations, 2003). According to the International Port Community Systems Association (International Port Community Systems Association, 2012), PCSs “can, and will, play a major role as Europe moves towards the Single Window concept”.

A PCS is an extension of the traditional, oftentimes uni-dimensional, Enterprise Resource Planning System (Morrall, Rainbird, Katsoulakos, Koliousis, & Varelas, 2016), offering connectivity among multiple systems operated by different organizations and authorities. PCSs work on a distributed logic and are based on databases that belong to either private or public bodies. It can be easily understood that these systems contain sensitive information in terms of commercial data and public authorities' inspection results among others. Thus modern ports are not striving only to build these systems but more importantly to safeguard the information contained in these systems.

Based on feedback from the participating Port Facility Security Officers (PFSOs) (Port Facility Security Officer, 2016) Table 1 below was compiled. This table presents the needs for each terminal, based on the characteristics of the transportation flow. It is understood that although ABC systems are necessary for all types of port terminals where passengers need be transited in a seamless flow manner (i.e. cruise and ROPAX terminals), ports can take much more advantage of the ABC systems and use them for monitoring people access in general, including real-time background checks across a number of databases (e.g. Watch List, Schengen, FBI, Visa, Trusted Traveller and APIS). For example a cruise ship disembarking 3,000 passengers in less than an hour makes the existence and usage of an ABC System compulsory.

Table 1 – ABC needs based on the characteristics of the port terminal

Type	Passengers with seamless flows	Passengers	Workers	Seamen	Vehicles
Cargo Terminal			X	X	
Car Terminal			X	X	X
Container Terminal			X	X	X
Oil Terminal			X	X	
Ro-Pax Terminal	X	X	X	X	X
Cruise Terminal	X		X	X	

Source: Validation workshop (Port Facility Security Officer, 2016)

2.3 A model PCS architecture with ABC

Considering the functional and business requirements of modern ports, it is easily understood that the need for automation may be implemented from passenger control to cargo control as well. A small number of ports in the European Union (CONTAIN Consortium, 2011), (SUPPORT Consortium, 2010) have tested automated gates for cargo, in order to improve both the security of cargo transiting and/or transferring through their facilities and reduce the waiting time for trucks and cargo. These gates follow similar functional properties as ABC systems do for passengers.

The following Figure 2 presents a conceptual architecture for the PCS where the automated control systems including passenger (ABCs and wireless-ABCs) and cargo (automated cargo gates) are constituent modular elements.

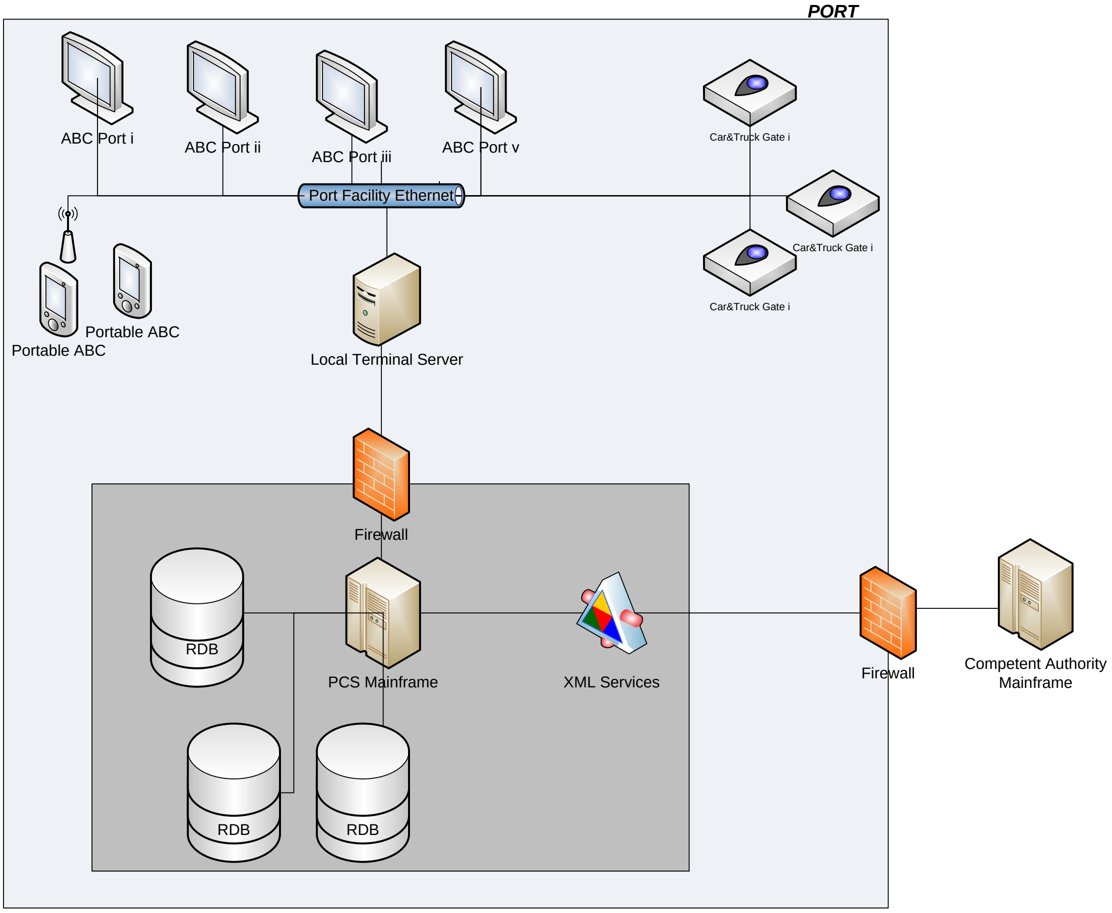


Figure 2 - A model PCS Architecture incorporating ABC

The PCS includes several Relational Databases (RDBs) that store and handle the relevant data. In terms of border control and/or access control automation, the PCS mainframe communicates with the local port terminal server that handles the automated systems (ABCs, Gates) through the PA's communications network. Additionally, the PCS communicates and shares data with the Competent Authority(ies), CAs. From the information flow point of view, once a ship announces a call (for example through sending a pre-arrival notice), it sends at the same time all relevant information to the PA and waits for instructions. For example, a cruise ship, submits the passenger list and the crew list. The PA communicates with the relevant CAs for entry approvals and/or rejections. Once this document is ready, the passengers are ready for disembarkation and when passing through the ABCs, they are granted access, rejected or wait for further inspections / instructions. This part of the process is the most risk prone, since compromised information may lead to unauthorized access to people/personnel.

The PCS plays a central role in this architecture, being the moderator of the information sharing as well as performing support services for both cyber & physical security inspections and control. The ABC component improves the inspections in terms of number, duration and effectiveness. This equipment may undertake a more inclusive monitoring role, not only for international movements which has been so far the main objective but also for domestic movements, similarly to other industries like the airline industry. It may also be extended to all stakeholders moving in and out of the port (especially in the ISPS designated secure area). PCS facilitates both preventive and reactive monitoring activities. Although the ABC component is an exposed system (in terms of risk management), nevertheless, the proposed framework considers such threats.

From Figure 2 above, it is well understood that although the systems have incorporated certain risk mitigation measures (for example firewalls and xml communications to reduce DB exposure, etc.) there are blackspots and weak links, since (a) infrastructure-wise, the distributed nature of the ABCs and Gate Controls expose part of the system to higher risks especially to outsiders and (b) process-wise, there is an increased need to implement and execute stricter and more robust security processes regarding the risk mitigation. It is self-explanatory that these systems are zero tolerance systems and additionally, unplanned / unforeseen downtime is an undesirable event.

2.4 ABCs for passenger terminals

Port facility security is important and should be done by specially trained personnel with the appropriate skills. The main challenges include the development of a viable port wide Security Plan (SP) that enforces access control at the different port areas and terminals and locks out undesired access and entrance (indicatively, illegal immigration, trespassing, etc). Additionally, the SP should also identify a port's critical infrastructural elements and also identify the current and the future traffic in and out of the port (in terms of passengers, crew, cargo and broadly defined stakeholders). The access control and the security, according to the ISPS Code, is rather critical and for many ports that handle international flows, this has to be effectively connected with border control systems.

Inefficient boarding systems, especially manual systems, leave passengers and ferry cruise operators dissatisfied. Port terminals need optimization of the boarding process (planning and execution) and the right mix of boarding systems, devices and procedures is essential. ISPS rules and regulations make mandatory the adoption of security and monitoring systems for both accessing the port facility and transiting through the boarding areas. Only passengers and vehicles with a valid boarding pass can access boarding areas, and their transit must be monitored real-time by using fast and flexible tools. The following provide an overview of essential security subsystems, based on the FRONTEX requirements (FRONTEX, 2012):

- **Gate Systems:** Gate systems and automated access control systems ensure cost effective and quick boarding operations for freight, cars and passengers. For Ports, the gate system can be implemented in the boarding area.
- **Self Service Systems:** Complete self-check-in solutions including full function kiosks as well as a wide range of high performance options and touch-screen applications. These are implemented in the check-in area of the port.
- **Ship Boarding Systems:** A solution that provides complete automation of vehicles check-in and check-out during the embarkation and disembarkation operations as well as passenger boarding automation.

- **Mobile Systems:** mobile applications that enable port operators to validate tickets, check-in passengers and print boarding cards directly on the dock, during the embarkation process.
- **Passenger Information Systems (PIS):** PIS provide passengers boarding information through different information channels and to different stakeholders (immigration, border police, customs, etc).
- **Document Authentication Systems (DAS):** Document authentication is the process by which Electronic Machine Readable Travel Documents (e-MRTD) presented by the traveller are checked and verified. Document Authentication Systems (DAS) determine whether the travel documents are genuine, whether the holder is the true and lawful owner and that s/he is not a threat to the state through optical document checks, e-Passport verification, etc.

3 Procedural Upgrade

3.1 Framework components

In this proposed framework, information security is defined by four components in terms of information compromise type, namely confidentiality, integrity, authenticity and availability. Risk management techniques ensure that none of these is violated, in order to use information as non-compromised. This work uses a simple definition for these components. More precisely, ***confidentiality*** is herein defined as the information that is not made available or disclosed to unauthorized individuals, entities or processes. ***Integrity*** is defined as the information accuracy and completeness including the ability to prove an action or event took place, so that it is repudiated again. ***Authenticity*** is the origin of the information which has been identified and validated. Last but not least, ***availability*** is defined as the accessibility of information and the usability upon demand by an authorized entity. Risk assessment is herein defined as the process to identify threats and assess the risks which can compromise any of the four abovementioned components.

In terms of physical security, similarly, four major components are identified and these include asset definition, threat assessment, vulnerability analysis and security measures selection. Asset definition includes not only the recognition of the asset but also the identification of the specificities and the prioritization compared to their organizational criticality. Threat assessment is the identification and the examination of potential risks and vulnerability analysis identifies the specific limitations / weaknesses each asset has compared to the identified threats which defines the compromise that could trigger the risk / threat. Finally, security measures are identified and selected based on the threat and vulnerability analysis. The main objective of physically securing a port facility is to develop a premise that has been specifically engineered with systems that either reduce the number of threats or minimize the impacts of the vulnerabilities.

3.2 High level overview of port related threats

Based on the previous analysis, four port main assets were identified and used. More precisely, this study covers the physical infrastructure, which includes all port facilities like terminal facilities, warehouses, parking areas, manufacturing areas. Additionally, it covers the ICT infrastructure, including networks, ICT related hardware systems/equipment, as well as systems and software, including servers, RDBs and subsystems like port services (e.g. cargo management, reservation, navigation) hosted by the PCS systems. Last but not least the framework covers, the information and the electronic data itself, including information, database content, log files and log books.

A matrix of possible threats has been developed. This matrix aims at capturing the four abovementioned categories of assets and their respective vulnerabilities. These threats may be used by the PFSOs to (a) improve security, (b) improve auditing of security processes and systems with an enterprise wide support and (c) fuse relevant knowledge to all involved stakeholders. Indicatively, the threat / vulnerability assessment includes malicious human activity related threats, physical attacks from outside the port perimeter, weather conditions (heavy winds, severe cold, heat waves, rain, etc) that may cause disruption of (ABC) systems' operation, physical disasters, unauthorized access in areas based on access rights permissions, inadequate equipment and materials as well as inadequate or incapable access control and authentications processes, cyber-attacks that affect the availability of information (DDOS attacks, Trojans, etc.) and last but not least improper execution and documentation of processes and procedures.

Table 2 below shows the number of threats that the matrix contains per type of asset. These threats were primarily based on ISPS standards as well as on the ISO 27000 standard and were validated during a workshop with five PFSOs (Port Facility Security Officer, 2016). Although the number may seem large, the number of the terminals, the essence of the infrastructure, the operational and the business rules necessitate this number. Additionally, it has to be noted that all these threats are pertinent to the ABC procedures proposed herein, however, they are non-exhaustive. An indicative list of these threats along with indicative vulnerabilities are both presented in Table 4 in Annex I as an explanatory breakdown per asset type.

Table 2 - Number of threats identified by Type of Asset

Type of Asset	Number of Threats Identified (Cyber & Physical)
ICT Infrastructure	165
Information and electronic data	283
Physical Infrastructure	1,482
Software	155
Grand Total	**2,085**

The analysis of a security risk depends upon the threats and the vulnerabilities that comprise each. For example, the risk level of a particular asset to a specific threat increases as the impact and the vulnerability levels are increased. For example the firewalls in the PCS architecture (see Figure 1) are not configured properly (vulnerability), non-authorized access (threat) of the PCS ABC (asset) is most likely to occur causing dangerous consequences (threat with high impact) to the whole PCS because there is no access monitoring device (vulnerability). In this case we conclude that the risk of the ABC, if the threat of non-authorized access occurs, is high.

3.3 Port security risk management methodology

The proposed framework addresses the ports' critical infrastructure security holistically by combining the ISPS Code with common ICT security management standards as stated above. This procedure meets established requirements like the ISO 9000 family of standards, (International Standardization Organization, 2009), (International Standardization Organization, 2008), the ISO 27000 family of standards, (International Standardization Organization, 2005), the ISO 31000 family of standards, (International Standardization Organization, 2009) as well as regulated standards like the ISPS Code (International Maritime Organization, 2012), the IMO Provisions (International Maritime Organization, 2002) and the SOLAS Convention (Lloyd's Register Rulefinder, 2005). This proposed methodology considers cultural, port industry practice and compliance aspects and involved a thorough analysis of risk templates and risk matrices for the five participating ports. The analysis was also compared to available risk consultants' Threat and Vulnerability Assessments (TVA) recommendations. The process to identify and validate the risks follows a taxonomy-based risk identification methodology which breaks down possible risk sources, selects the appropriate and adapts to the port industry.

Additionally, the framework has a multi-scope perspective in supporting risk analysis on the physical layer, on the cyber layer and on a combined layer. In this respect, it ensures collaboration among all ICT port stakeholders building up collective intelligence for the entire community and analyses sectoral, interconnected and interdependent threats by evaluating both direct and indirect risks. The proposed framework intends to improve security accuracy and implementation flexibility.

In this context, it is noted that compliance with ISPS requirements is obligatory. The company/ship/port develops, implements and maintains the SP which addresses, at the very least, the requirements laid down by ISPS. The SP is then approved by the CA. Indicatively, ISPS recognizes 3 Security Levels. Security level 1 is the normal level with minimum security measures maintained, for example the port facility only enforces "no access" areas. Security level 2 has higher security requirements compared to the normal level. Routine and cargo operations are carried out as in normal cases but with elevated security measures (controls, checks, monitoring, and surveillance). Security level 3 is enabled when an imminent danger is identified and specific protective measures are maintained. Operations are stopped and frequent security duties are carried out.

The first step of the risk management methodology was to develop a security awareness process. This comprises of a clear definition of an activities' framework, an agenda for robustly identifying the port security (awareness) level and finally of the development of an exhaustive list of all physical and cyber assets of the port and their interdependencies. The second step is the recognition and the establishment of a risk analysis framework which comprises of several interrelated sub-activities. The identification of the physical and the cyber threats that the port facilities face as well the cyber threats targeting the PCS systems themselves comes first. Then comes the identification of external threats (existing and potential) that arise from external interdependent entities (e.g. customs, maritime companies, logistics service providers) and finally comes the calculation of the impact levels of the identified threats. The development of a set of vulnerabilities based on the identified threats follows along with the calculation of the risks for each asset and each threat individually and collectively. The final step is the categorization of the risks into internal and external per port asset which concludes this methodology.

The initial validation was further evaluated at a second level through a peer review group that was set up, comprising of Port Security Officers (Port Facility Security Officer, 2016).

3.4 Procedural Flows

3.4.1 Threat and vulnerability assessment

Stakeholders carry out risk analysis of the events as required by the implemented risk management plan and based on a security threat assessment procedure which is set up to identify and quantify the potential threats. This study uses the Bow-Tie method (Gifford, Giltert, & Bernes, 2003) to conduct risk identification and risk analysis concurrently for a number of different events. This method effectively combines Fault Tree Analysis, Causal Factors Charting and Event Tree Analysis. The Bow-Tie methodology presents a central loss event, the threats that may cause that loss event, the consequences of that loss event occurring and the possible controls that may be used to reduce the probability of the loss event occurring.

Figure 3 below shows a practical example the validation workshop used in order to identify the threats and perform risk analysis for the specific event of “Passenger List content not matching the list submitted to the outgoing port”. The terminology is based on the CONTAIN project (CONTAIN Consortium, 2011). Specifically a ***Loss Event*** (LE) is defined as one of several identifications of related threats. A ***Threat*** (T) is a danger that once triggered produces harmful consequences. ***Proactive Control*** (PC) is an action that may lessen a threat from occurring. A ***Reactive Control*** (RC) is an action or a set of actions after a threat has actually occurred and ***Consequence*** (S) is defined as the extent of harm caused by a threat.

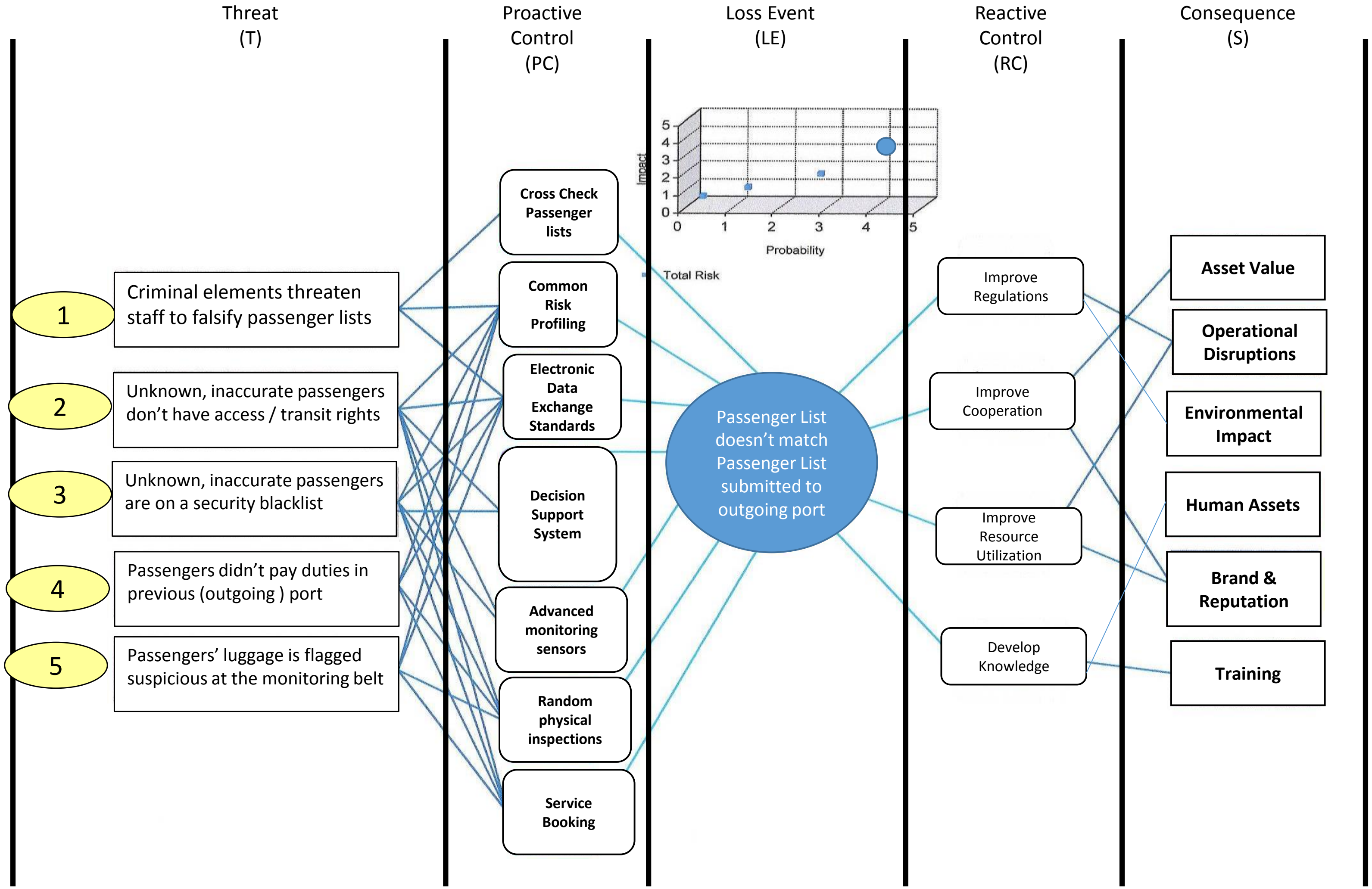
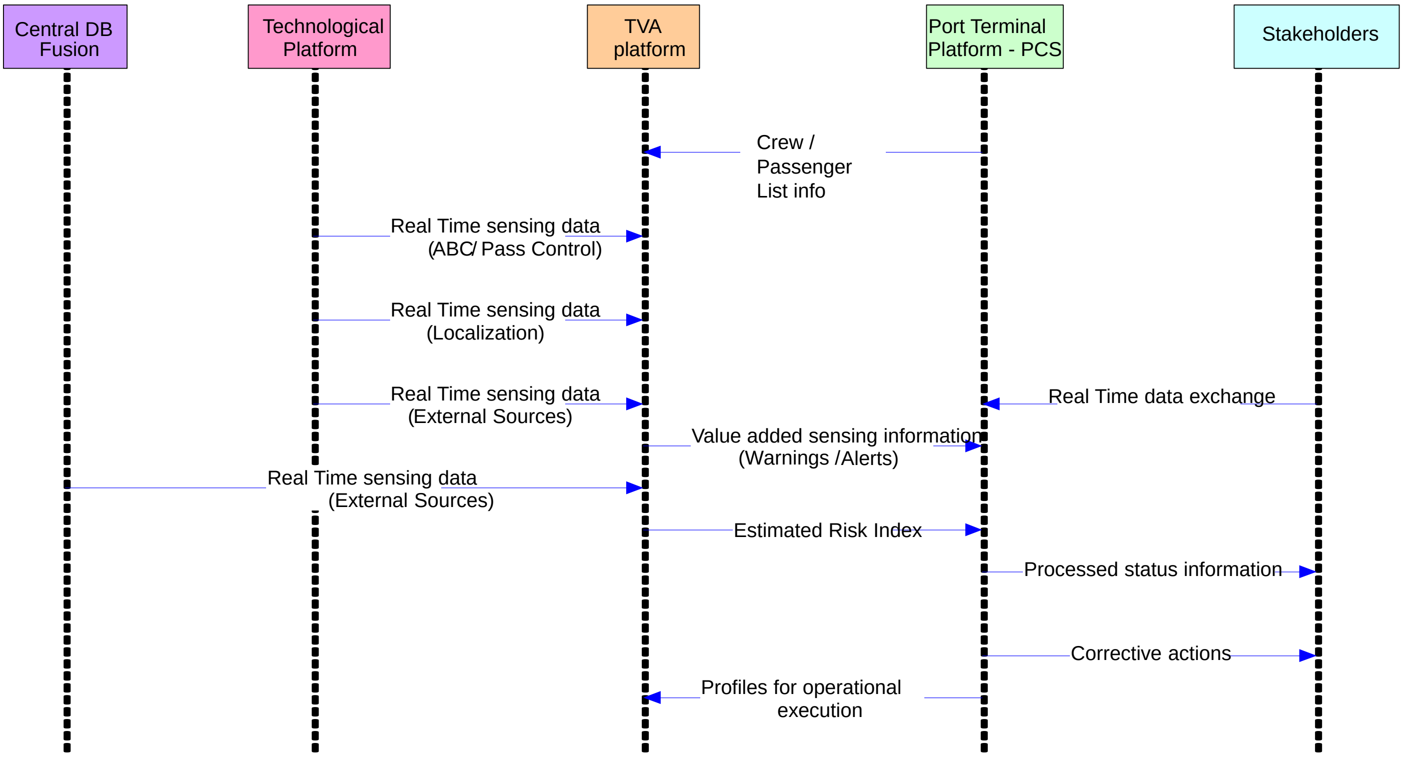

Threat
(T)
Proactive
Control
(PC)
Loss Event
(LE)
Reactive
Control
(RC)
Consequence
(S)
1
Criminal elements threaten staff to falsify passenger lists
2
Unknown, inaccurate passengers don't have access / transit rights
3
Unknown, inaccurate passengers are on a security blacklist
4
Passengers didn't pay duties in previous (outgoing) port
5
Passengers' luggage is flagged suspicious at the monitoring belt
Cross Check Passenger lists
Common Risk Profiling
Electronic Data Exchange Standards
Decision Support System
Advanced monitoring sensors
Random physical inspections
Service Booking
Impact
5
4
3
2
1
0
0
1
2
3
4
5
Probability
Total Risk
Passenger List doesn't match Passenger List submitted to outgoing port
Improve Regulations
Improve Cooperation
Improve Resource Utilization
Develop Knowledge
Asset Value
Operational Disruptions
Environmental Impact
Human Assets
Brand & Reputation
Training

Figure 3 - Bow tie based TVA for passenger lists with matching errors

3.4.2 Indicative information flow plan and data fusion

Figure 4 below represents the exchange of messages among the stakeholders when sharing the passenger list. This diagram shares the basic principles described in Figure 3 above and includes all related authorities, agents, companies, etc.



Central DB Fusion
Technological Platform
TVA platform
Port Terminal Platform - PCS
Stakeholders
Crew / Passenger List info
Real Time sensing data (ABC/ Pass Control)
Real Time sensing data (Localization)
Real Time sensing data (External Sources)
Real Time data exchange
Value added sensing information (Warnings /Alerts)
Real Time sensing data (External Sources)
Estimated Risk Index
Processed status information
Corrective actions
Profiles for operational execution

Figure 4 - Information flow overview, port TVA subsystem viewpoint

The system presented herein exchanges short messages on a Machine-to-Machine basis and each sub-system stores the data for analysis and risk management / analytics. Furthermore, depending on the content, the proposed system is scalable to accommodate longer messages.

3.5 Knowledge Upgrade

One of the most important feedback that emerged from the validation workshop (Port Facility Security Officer, 2016) is the need for a knowledge management system. This system should capture the essential information regarding threats, vulnerabilities, risks and risk management approaches and store it. The proposed platform contained a simple web-based, open-source KM system in the form of Content Management System. The reason for adopting such a system was mainly as a proof of concept. In a real life case, more advanced systems add value by improving the entire knowledge management process. The proposed system offered a number of critical services like capturing knowledge at the individual level (experiences, known faults, known issues, threat descriptions, etc), distributing knowledge on-demand at the organizational level as well as across similar access rights offices. Additionally, the proposed system executed peer reviews and assessed information to improve accuracy and consistency and set up hotline services, to answer questions as soon as possible and also comment individually per message. In addition, an enterprise wide portal was set up to aggregate security content and share information across the organizations which was also coupled with an eLearning module accommodating simple explainer and situational videos. This is a top-down approach in regulating information sharing offering robust KM usage.

The proposed KM system couldn't support, by default, real time interactions, however, by using open-source off-the-shelf systems, it increased satisfaction among workshop participants and improved insight. Feedback from the validation workshop included utilizing more advanced systems, including semantic KM systems as well as further exploring the utility of Serious Games and gamification based training.

4 Port Security Officers' Validation and Feedback

As discussed above, during a one day workshop, a validation of the proposed framework was performed based on structured discussions and feedback from the participants representing five ports.

Table 3 below describes the general characteristics of the ports participating in the validation workshop as well as the respective validation workshop participants' characteristics and background / experience. It has to be mentioned that the selected ports are indicative and not representative, for the initial validation purposes. The participation on behalf of the ports included either the PFSO or the Deputy PFSO. A significant part of the TVA matrices were co-developed with the participating ports, thus anonymity for security reasons is preserved. The questionnaire appears on ANNEX II and was based on the usability test proposed by Lin, Choong and Salvendy's (Lin, Choong, & Salvendy, 1997) and on the usefulness test developed by Lund (Lund, 2001).

Table 3 - Validation workshop participants' characteristics including port characteristics

#	Port Size	Main Trade	Traffic (Passengers, 2015)	Traffic (Cars, 2015)	Traffic (Cargo, 2015)	Throughput (Containers: TEUs/2015)	Ownership	Participating Officer	Background
1	Small	Cruise, ROPAX	200,000	20,000	N/A	N/A	Public	PFSO	• Ex Police Enforcement, • 25 years of security experience, 5 or more in this position • Qualified PFSO
2	Large	Cruise, ROPAX, Container, General Cargo, Liquid	2,000,000 (transit) 300, 000 (cruise, home porting) 9,000, 000 (ferry traffic) 7, 000, 000 (pure ROPAX)	300,000	400,000	4,000,000	Mixed	Deputy PFSO	• Managerial background (within the port) • Qualified PFSO • 5 years or more in position
3	Large	Cruise, ROPAX, Container, General Cargo, Liquid	800,000	700,000	100,000	4,000,000	Mixed	Deputy PFSO	• Ex Police Enforcement, • 30 years of security experience, 5 years or more in this position • Qualified PFSO
4	Medium	RORO, ROPAX, General	600,000	300,000	200,000	-	Public	PFSO	• Ex Military, • 25 years of security experience, 5 years or more in this position • Qualified PFSO
5	Medium	RORO, ROPAX, Container	2,000,000	500,000	400,000	800,000	Public	PFSO	• Managerial Background (within the port), • 6 years of security experience (position related) • Qualified PFSO

N.B.: Numbers rounded by author to preserve anonymity

The analysis of the validation workshop resulted in some interesting conclusions. A broad range of definitions and security concepts was observed, however, PFSOs seem to give particular attention to physical security (safety), oftentimes tacitly ignoring the four components of cyber security, i.e. confidentiality, integrity, authenticity and availability. Although all participating ports were ISPS compliant, covering effectively the safety component within the ports, it was understood that the security standard approach is not holistic in terms of risks identified, assessed, and mitigated. The absence of a comprehensive security culture favoured a focus on physical inspections which draws on from the enforcement background of most security officers.

None of the ports presented an exhaustive TVA, although sporadic measures and best practices were identified by all PFSOs. Similarly, the ports surveyed have only recently started coping with cyber threats (e.g. attacks, masquerading identities, network traffic monitoring, theft /modification of personal data), however, they identified the lack of a comprehensive and exhaustive risk matrix, where they could include and utilize best practices and "how-to" solutions. It is evident that the value of information security is not entirely realized as a core constituent of the business model and of the business offering, thus it is overlooked.

Another interesting observation is that Critical Infrastructure Protection (CIP) planning standards or methodologies are not sufficiently implemented. Most importantly, there is no effective classification methodology to categorize the criticality of the port assets nor of the port facilities. This is attributed partly to the lack of an appropriate legislation framework and partly to limited standardization initiatives. The reporting framework put in place from the CAs seems weak compared to the value of the asset and doesn't provide adequate knowledge sharing between authorities. This issue was also raised as part of the reporting and/or feedback procedures on security incidents to the CAs. The reporting focuses only on aggregate statistics mainly of physical incidents and doesn't cover in sufficient detail cyber incidents. Furthermore, the existing procedures don't effectively report lessons learned nor develop (or store) any other knowledge content. Procedurally, the collaboration among ports, stakeholders and authorities is based only on individual relations and initiatives and don't utilize robust, explicit KM creation mechanisms. Interestingly, the interviewees also considered useful the practice of insurance coverage other industries adopt, particularly the information security losses insurance contracts as part of a holistic mitigation plan.

With respect to the technology element, the participants claimed that plans to install diverse technologies, from access control systems (e.g. smart cards, ABC, RFIDs) to access awareness (e.g. firewalls, intrusion detection systems, etc) are put in place. Additionally, the ports are also planning to improve the training for cyber security threats for ports and critical infrastructure. All of these systems will be greatly supported by a more extensive use of ABCs. ABC's parallel background procedures and their capabilities to more effectively share information is an interesting option that will be further explored in the near future.

Based on the discussions, the proposed system has the flexibility to become a centralized security database containing knowledge on the threats, the vulnerabilities and the risk management approaches used by all stakeholders. The use will be based on access rights permissions. It is self-evident that this knowledge has to be appropriately shared across all relevant stakeholders. The use of the PCS as the backbone KM system, either centralized or decentralized, was well received by all interviewees. The horizontal deployment and the inclusive character of both internal and external stakeholders offers significant value to more effectively manage the port risks.

With regards to the ABC proof of concept validation some interesting conclusions were drawn. Notably, ABCs should be placed in various locations of the port, including on the ship, in arrival/departure areas, in warehouses, in ports' entry/exit points. The number and the deployment of the ABCs should ensure that controls are carried out quickly and efficiently, minimizing turnaround duration. The operational attributes should also be adjusted to the local elements and restrictions, for example indoor ABC gates, mobile ABC gates, portable devices to act as ABCs and to be administered by enforcement / patrol officers as well as large Automated Cargo Gates (ACGs) for vehicles, wagons and containers. All participating PFSOs agreed that ABC may improve both the efficiency and the effectiveness of the inspections for all incoming persons, as it has the flexibility to perform 100% monitoring and inspections. This gives a unique opportunity to ports to secure the ISPS designated port area.

A robust cross certification procedure and mechanisms between Country Verifiers Certification Authorities (CVCA) should ensure ABC's interoperability, which should be followed by a thorough harmonization of ABCs in all entry points (i.e. railways, roads, airports) in order to accelerate the check-in process but most importantly improve the information sharing among the stakeholders. This harmonization should also ensure the integration of ABCs in the PCS so as to increase the value of information and share it appropriately to all stakeholders.

Conclusively, the most important insight drawn was the lack of a comprehensive security management plan, since most of the PFSOs draw on their enforcement background, giving attention primarily to physical security management without cross referencing of the background of each security item. However, modern ports are also information hubs, where security management has to effectively implement, establish, assess, monitor, improve and audit both the physical and the cyber security elements of the ports' facilities (assets). Additionally, security management is a continuous and systematic process of identifying, analysing, mitigating, reporting and monitoring technical, operational and other types of security risks (both physical and cyber risks) as well as implementing appropriate security measures and controls.

All ports are compliant with the regulations required by CAs however, the workshop session made clear that the CA's framework doesn't require a comprehensive analysis of security measures in order to protect Critical Port Infrastructure. The current regulatory context of the ISPS maintains a generic consideration on cyber security elements and remains with the PA to adopt a stricter security plan. Towards this direction EU (European Commission, 2010) adopted a more information targeted policy framework, in the context of Action 94 (eMaritime) of the Digital Agenda for EU.

5 Synthesis of results, conclusions and further research

Conclusively, although PAs and operators are compliant with the regulations required by CAs (e.g. IMO, EU), nevertheless, our analysis revealed that there are opportunities for improvement. For example, in order to improve security efficiency and effectiveness, ABC systems may be implemented. This system will greatly benefit from sharing information through the PCSs, which could improve both the front-end quality perception (e.g. reduce waiting times) and also improve the security level as well as significantly reduce unauthorized access. Compared to the currently available frameworks, the proposed system introduces a more exhaustive analysis of security threats and risks to the Ports' Infrastructure, including the Critical Information Infrastructure and additionally utilizes advanced equipment to monitor unauthorized access, share information and introduce analytics to increase situational awareness for the security operators.

Furthermore, the state-of-play analysis showed that cyber security threats are not adequately covered and remain at the PA's discretion to adopt a stricter and more inclusive security plan. Port facility security awareness needs to be improved also through provision of appropriate cyber security training to relevant actors (e.g. internal and external users), awareness campaigns and training initiatives, while their provision could be coordinated by relevant cyber security organizations (e.g. PFSOs, maritime authorities, national certification authorities, public-private partnerships, etc).

Nevertheless, in order for a proper ABC system to be installed, not only the physical features, but most importantly the soft characteristics of the ports have to be assessed and modified accordingly. Compared to the state-of-play, the proposed framework is capable of handling security information and fusing this information to the proper handler (including public and private entities) in a timely manner so as to execute more efficiently and more effectively the inspections. Additionally, the proposed framework supports effectively a risk management system not only by combining different information sources but also by supporting different security philosophies.

This study in not exhaustive, but intends to become a basis of discussions on how to further improve the security level in ports, terminals and generally critical infrastructure. More importantly, in recognizing the limitations of this paper, additional research has to be carried out in terms of (a) measuring the impact of introducing this framework, including cost benefit analysis, economic impacts, security impacts, (b) understanding the value of semantic technologies in improving the inspections and (c) improving the information sharing standards.

6 Acknowledgements

The author would like to thank the anonymous reviewers for the invaluable reviews, comments and suggestions which have greatly improved the paper.

7 Nomenclature

ABC	Automated Border Control

ACG	Automated Cargo Gate
BoL	Bill of Lading
B2A	Business to Authority
B2B	Business to Business
CA	Competent Authority
CVCA	Country Verifiers Certification Authorities
ICT	Information and Communication Technologies
ISPS Code	International Ship and Port Facility Security Code
KM	Knowledge Management
PA	Port Authority
RDB	Relational Database
ROPAX	Roll On – Passenger Ship
RORO	Roll On – Roll off Ship
PCS	Port Community System
PFSO	Port Facility Security Officer
SSO	Ship Security Officer
TVA	Threat and Vulnerability Assessments

8 References

1. Akhtar, J., Bjørnskau, T., & Veistein, K. (2010). Assessing security measures reducing terrorist risk: inverse ex post cost-benefit and cost-effectiveness analyses of Norwegian airports and seaports. Journal of Transportation Security, 3(3), pp. 179-195. doi:https://doi.org/10.1007/s12198-010-0046-z

2. Alberts, C., & Dorofee, A. (2001). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCT A VE) Method Implementation Guide, v2.0. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

3. Bagchi, P. K., & Paik, S.-K. (2001). The role of public-private partnership in port information systems development. International Journal of Public Sector Management, 14(6), pp. 482-499. doi:https://doi.org/10.1108/EUM0000000005965

4. Bakshi, N., & Gans, N. (2010). Securing the Containerized Supply Chain: Analysis of Government Incentives for Private Investment. Management Science, 56(2), pp. 219-233.

5. Balmata, J.-F., Lafonta, F., Maifretb, R., & Pessel, N. (2009, November). MAritime RISk Assessment (MARISA), a fuzzy approach to define an individual ship risk factor. Ocean Engineering, pp. 1278–1286.

6. Baron, M.-L., & Mathieu, H. (2013). PCS interoperability in Europe: a market for PCS operators? The International Journal of Logistics Management, pp. 117-129.

7. Batini, C., Lenzerini, M., & Navathe, S. (1986). A Comparative Analysis of Methodologies for Database Schema Integration. ACM COMPUTING SURVEYS.
8. Bhatt, G. (2001). Knowledge management in organizations: examining the interaction between technologies, techniques and people". Journal of Knowledge Management, pp. 68-75.
9. Burns, M. G. (2013). Estimating the impact of maritime security: financial tradeoffs between security and and efficiency. Journal of Transportation Security, 6(4), pp. 329-338. doi:https://doi.org/10.1007/s12198-013-0119-x
10. CONTAIN Consortium. (2011). Container Security Advanced Information Networking; GA No: 261679 / Funded under: FP7-SECURITY. Brussels, BE.
11. CYSM Consortium. (2013). Collaborative Cyber/Physical Security Management System (Grant Agreement No 4000003750 (Co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union). Brussels, BE.
12. Duffy, J. (2000). Knowledge management: to be or not to be? Information Management Journal, 34(1).
13. Easterby-Smith, M., & Lyles, M. (2003). The Blackwell handbook of organizational learning and knowledge management. Oxford: Blackwell.
14. ENISA. (2011). First annual report of cyber incidents in the EU: 51 severe outages reported over 2011.
15. Ernst & Young. (2012). 2012 Global Information Security Survey: Fighting to close the Gap. London, UK: EYGM.
16. European Commission. (2006). Commission Recommendation establishing a common "Practical Handbook for Border Guards (Schengen Handbook)". Brussels, BE.
17. EUROPEAN COMMISSION. (2010). A Digital Agenda for Europe COM(2010) 245 final/2. Brussels, BE.
18. European Commission. (2013, 12 18). COMMISSION REGULATION (EC) No 2286/2003. Brussels, BE.
19. European Parliament. (2013, 10 9). Union Customs Code (UCC): Regulation (EU) No 952/2013. Brussels, BE.
20. FRONTEX. (2012). Best Practice Operational Guidelines for Automated Border Control (ABC) Systems. Brussels: EU Publication Office.
21. FRONTEX. (2012). Best Practice Technical Guidelines for Automated Border Control Systems. Brussels, BE: EU Publication Office.

22. Ghafoori, A., & Altiok, T. (2012). A mixed integer programming framework for sonar placement to mitigate maritime security risk. Journal of Transportation Security, pp. 253-276. doi:https://doi.org/10.1007/s12198-012-0095-6
23. Gifford, M., Giltert, S., & Bernes, I. (2003). Bow-Tie Analysis. Equipment Safety Assurance Symposium (ESAS).
24. Hansen, M., Mors, M. L., & LØVÅS, B. (2005). Knowledge sharing in organizations: Multiple networks, Multiple phases. Academy of Management Journal, pp. 776-793.
25. International Maritime Organization. (2002). IMO adopts comprehensive maritime security measures. Retrieved from http://www.imo.org/blast/mainframe.asp?topic_id=583&doc_id=2689
26. International Maritime Organization. (2010). ISM Code and Guidelines on Implementation of the ISM Code 2010. London: IMO Publications Office.
27. International Maritime Organization. (2012). GUIDE TO MARITIME SECURITY AND THE ISPS CODE. London: IMO Publications Office.
28. International Port Community Systems Association. (2012). Port Community Systems. Retrieved from http://www.epcsa.eu/port-community-systems
29. International Standardization Organization. (2005). ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management. Geneva, CH: ISO.
30. International Standardization Organization. (2008). ISO 9001:2008: Quality management systems -- Requirements. Geneva, CH: ISO.
31. International Standardization Organization. (2009). ISO 9004:2009: Managing for the sustained success of an organization - A quality management approach. Geneva, CH: ISO.
32. International Standardization Organization. (2009). ISO/DIS 31000: Risk management — Principles and guidelines on implementation. Geneva, CH: ISO.
33. King, W. (2009). Knowledge Management and Organizational Learning. Annals of Information Systems.
34. Koliousis, I., Koliousis, P., & Katsoulakos, T. (2015). Maritime Single Windows: Lessons Learned From The Emar Project. In E. Sören, B. E. Asbjornslett, O. Jan Rodseth, & B. T. E., Maritime-Port Technology and Development (pp. 27-34).
35. Lin, H., Choong, Y.-Y., & Salvendy, G. (1997). A Proposed Index of Usability: A Method for Comparing the Relative Usability of Different Software Systems. Behaviour & Information Technology, pp. 267-278.

36. Lloyd’s Register Rulefinder. (2005). SOLAS - International Convention for the Safety of Life at Sea. London: Lloyd’s Register Groour.

37. Luiijf, H., Burger, H., & Klaver, M. (2003). Critical infrastructure protection in the Netherlands: A Quick-scan. EICAR Conference Best Paper Proceedings 2003.

38. Lund, A. (2001). Measuring Usability with the USE Questionnaire. Usability Interface, pp. 3-6.

39. Morrall, A., Rainbird, J., Katsoulakos, T., Koliousis, I., & Varelas, T. (2016). e-Maritime for automating legacy shipping practices. Transportation Research Procedia, pp. 143-152.

40. Polyani, M. (1966). The tacit dimension. London: Routledge & Kegan Paul.

41. Port Facility Security Officer. (2016, 11 5). Workshop with Port Facility Security Officers from 5 EU Ports Port Authority Names Unidisclosed for security purposes.

42. Port of Helsinki. (2016). Port of Helsinki West Terminal. Retrieved 2016, from http://www.portofhelsinki.fi/passengers/west_terminal

43. PriceWaterhouse Coopers. (2013). The Global State of Information Security Survey 2013.

44. Rishe, N., Athauda, R., Yuan, J., & Chen, S.-C. (2000). Knowledge Management for Database Interoperability. Proceedings of the 2nd International Conference on Information Reuse and Integration (pp. 23-26). Honolulu: ISCA.

45. Rodon, J., & Ramis-Pujol, J. (2006). Exploring the Intricacies of Integrating with a Port Community System. BLED 2006 Proceedings.

46. SUPPORT Consortium. (2010). SUPPORT - Security UPgrade for PORTs. Brussels, BE.

47. Thomas, R. A. (2017, 08). More port cyber security is needed. (www.portstrategy.com, Editor)

48. U.S. Department of Homeland Security. (2005). The national strategy for maritime security. Washington, D.C.: USDoHS; Bureau of Political - Military Affairs.

49. United Nations. (2003). The Single Window Concept. Geneva, CH: UNECE.

50. US Coast Guard. (2010). Maritime Security Risk Analysis Model: Overview for USCG-CREATE Maritime .

51. van Baalen, P., Zuidwijk, R., & van Nunen, J. (2009). Port Inter-Organizational Information Systems: Capabilities to Service Global Supply Chains. Foundations and Trends® in Technology, Information and Operations Management, pp. 81-241. doi:http://dx.doi.org/10.1561/0200000008

52. Williams, A. (2015). Beyond a series of security nets: applying STAMP & STPA to port security. Journal of Transportation Security, pp. 139-157. doi:DOI 10.1007/s12198-015-0161-y

ANNEX I – Indicative Threats & Vulnerabilities

Table 4 – Indicative Threats & Vulnerabilities by type of asset

Asset Type	Threats	Vulnerabilities
ICT Infrastructure	Technical failures	Dusty equipment
ICT Infrastructure	Electronic Interference & Cyber Interference	Electromagnetic radiation
ICT Infrastructure	Hurricane	No business continuity plans or procedures for recovery of information and information assets
ICT Infrastructure	Electric surge	Backup files and systems not available
ICT Infrastructure	Equipment Failure	Inadequate change control settings
ICT Infrastructure	Theft and Fraud	Uncontrolled copy of software
ICT Infrastructure	Fire	Inadequate Physical and Environmental Security Policy and Procedures
ICT Infrastructure	Storm	Location is in an area highly susceptible to natural disasters
ICT Infrastructure	Power Fluctuations	Improper or inappropriate maintenance of technical facilities
ICT Infrastructure	Cyber security failure	Worm threats
Information and electronic data	Equipment Failure	Not adequate policy for critical equipment
Information and electronic data	Communications Failure	Communication lines without protection
Information and electronic data	Files incidents	Uncontrolled copies of sensitive files
Information and electronic data	Procedural Failures	Lack of usage policies (Cyber Attacks)
Information and electronic data	Fire	Lack of fire detection devices
Information and electronic data	Storm	Location is in an area susceptible to natural disasters
Information and electronic data	Transmission errors	Inadequate incident handling
Information and electronic data	Unauthorized Software Changes	Inadequate engineering and quality processes for design and code review
Information and electronic data	Sabotage	Lack of Physical Security
Information and electronic data	Cyber security failure	Lack of audit logs to detect unauthorized use of application
Information and electronic data	Masquerade	Inadequate identity and password policy
Information and electronic data	Eavesdropping	Unencrypted communications
Physical Infrastructure	Fire	Fire detection devices malfunction
Physical Infrastructure	Storm	No business continuity plans or procedures for recovery of information and information assets
Physical Infrastructure	Terrorist attacks	Lack of Logical Access security

Physical Infrastructure	Port Facility Incidents	The port's surroundings are not clearly communicated to personnel
Physical Infrastructure	Inspections at the gates – searches failures	There is no equipment for inspecting passengers
Physical Infrastructure	Berthing area failures	There are no procedures to search waterfront areas for explosives or other dangerous devices prior to a ship arrival at PF or waterfronts that have been unmanned or unmonitored
Physical Infrastructure	Cyber security failure	The facility doesn't have a clear information security procedure
Physical Infrastructure	Training, control and supervision failures	There is no training on body searching
Physical Infrastructure	Training, control and supervision failures	There is no training on luggage inspection
Physical Infrastructure	Training, control and supervision failures	There is no training on vehicle inspection
Software	Fire	Inadequate monitoring of environmental conditions
Software	Storm	Back-up files and systems are kept at the same place / premises also prone to storms
Software	Power Fluctuations	Location is in an area susceptible to power fluctuations
Software	Cyber security failure	Easily accessible devices (servers, mainframes, etc).
Software	Malicious Code	Lack of policy for opening email attachments
Software	Denial of Service	Lack of a Firewall / No regular updates

n.b.: Vulnerabilities are generic to preserve port anonymity and commercially sensitive information. Sampled elements; not exhaustive, representative. Realistic vulnerabilities.

ANNEX II – Workshop Questionnaire

PART I – INTERVIEW

(To be completed by interviewer)

I. Background questions

1. What is the name of your company?

2. What is the title of your position

3. What is your position's level in the firm?

□ Senior Management

□ Middle Management

□ Operational staff

□ Other, please specify: ____

4. How would you describe your role within your organization?

5. Please indicate the number of employees in your firm:

□ 0- 49	□ 250 to 499
□ 50 to 249	□ 500 and more

6. How many employees in your firm are related to security activities?

□ 0- 09	□ 75 to 99
□ 10 to 24	□ 100 to 249
□ 25 to 49	□ 250 to 499
□ 50 to 74	□ 500 and more

7. How would you describe your mode of operation and day-by-day work within your organization?

8. Do you regard that the role of security officer has changed over recent years?

II. Description of the Port / Port Facility Security Plan and definitions

1. Please give a working definition for “security” and for “risk”.

2. Does this definition differ from the security definition that you are using for your facility? How?

3. What security elements are you focusing on?

4. What are the risks that you identified, assessed, and mitigated?

5. What are the assets that you identified, assessed, and mitigated?

6. Please describe the physical inspections process.

7. Please describe the Threat & Vulnerability Analysis you are performing.

8. Please describe the security team, their backgrounds and their selection process.

9. Are you also managing cyber related risks?

Yes □ No □

10. What are the main cyber threats you are defending your organization against (Please tick all that apply)

□ Attacks □ Masquerading identities □ Network traffic monitoring □ Theft /modification of personal data

□ Other, please specify: ____

11. Please describe briefly the major problems you are facing with you current security plan.

12. How do you define a Critical Infrastructure Protection (CIP) Plan?

13. What are the main elements for a CIP Plan?

14. What are the standards you adopt for the CIP Plan?

III. Reporting requirements and formalities

1. How do you report to the Competent Authority?

   i. Periodicity

   ii. Communications means

   iii. Responsible Officer / Executive

   iv. Liaison Means

2. Please indicate briefly the contents of this reporting.

3. How do you report lessons learned and knowledge creation?

4. How do you include (feedback loop) your lessons learned to your organization?

i. Training Methodology / Learning Loop

ii. Organizational Development

iii. Procedural Development

IV. Monitoring Technologies.

1. What technologies do you currently use to monitor physical access?

2. Are you planning to use new technologies to monitor physical access?

3. What technologies do you currently use to monitor cyber access?

4. Are you planning to use new technologies to monitor cyber access?

5. What personnel capacity upgrade plans you have adopted?

PART II - CONSENSUS MEETING

Now, lets discuss the systems you experienced.

1. Please comment on the proposed system overall.

2. Please comment on the use and integration of ABC Gates overall throughout the proposed system.

3. Please comment about the current security frameworks overall.

4. How do you perceive “knowledge exchange” and “security policy” regarding security enhancement?

5. How do you perceive the holistic and interdisciplinary approach of knowledge organizations regarding security challenges and for the planning of security frameworks?