



The Security Value of Small and Medium Sized Ports in a Supply Chain Service

by Pinelopi Kyranoudi^{1,2} & Nineta Polemi^{1,3}

Abstract

This study focuses on explaining key concepts about ports, their characteristics (e.g., size, operational field, infrastructure), potential threats (e.g., interception of sensitive information, illegal access, terrorism) and attacks (cyber, physical and/or combined), providing an overview of port risk analysis. It also focuses on recording the characteristics of port facilities to document the requirements in small and medium sized ports (SMPs), which act as Supply Chain Service (SCS) providers and/or business partners (BPs). Finally, three attack scenarios are described based on different types of threats, which could cause particularly problematic effects, even paralyzing an entire port and by extension the entire region that benefits from or depends on it.

Keywords

Supply Chain Service, Small and Medium Sized Ports, Cyber Security, Risk Analysis, Threats and Attacks Scenarios

1. Introduction

According to ISO 28000:2007 [1], a Supply Chain Service (SCS) “is considered the service that entails a linked set of resources and processes that begins with the sourcing of raw material and extends through the delivery of

products or services to the end user across the modes of transport.”

By extension, a maritime SCS is a dynamic system consisting of a set of interconnected organizations (e.g., port authorities, coast guards, customs services, shipyards, marine insurance companies), other critical infrastructures (e.g., energy, transportation, telecommunications), people, services and other elements aimed at providing a service or product to end users.

In recent years this complex chain has significantly increased its reliance on Information and Communications Technology (ICT) with the aim of providing innovative SCSs in the context of the highly competitive maritime trade [2],[3]. As a result, more and more cybersecurity incidents have been recorded in ports, due to the digitization related to the interconnection of Information Technology (IT), Operational Technology (OT) assets, as well as the introduction of new technologies, such as cloud computing, big data, Internet of Things (IoT), etc. Some of the most well-known events, due to their impact, are the cyber attack on port of Antwerp, the NotPetya ransomware on Maersk and the wave of ransomware attacks on the port of Barcelona and San Diego [3].

There are many ways to categorize ports; for the purposes of this study, the categorization of ports will be limited to two main axes: their size (i.e., small, medium, large)

¹ Department of Informatics, University of Piraeus, Karaoli & Dimitriou Str. 80, 18534 Piraeus, Greece

² MAGGIOLI SPA, Via Del Caprino 8, Santarcangelo Di Romagna 47822, Italy

³ Trustilio B.V., Vijzelstraat 68, 1017HL Amsterdam, The Netherlands

and the type of SCS they operate (i.e., cargo, passenger, fishing).

Small and medium sized port (SMP) facilities are often the mainstay of a variety of activities in remote areas, such as islands, riverside or peripheral areas. The SMPs play the most important economic role and have significant impact in the goods' distribution, people mobility and their well-being. SMPs in the small Greek islands, for example, are the main trading areas and economic local providers. Any negative impact on the operation of the SMPs have catastrophic impact to the small regions (e.g., loss of jobs, short-age of basic goods, loss of national safety, loss of lives).

So far, the area of cyber security in these types of ports has lacked attention in existing risk analysis methodologies. This study challenges the belief that SMPs are less important than the larger ones in SCS management and security.

2. Categories and Characteristics of SMPs

There are many ways to distinguish ports, especially the smaller ones, which may be the only communication of some remote areas with the rest of the world and because of this, probably provide more than one SCS. The most common approach to categorizing them is to use metrics based on annual cargo volume or the total volume of ships handled by them. Therefore, for the needs of this study, the categorization of ports will be focused on two main axes; their size and the type of SCS they manage. More specifically, for size the ESPO categorization will be followed, while regarding the type of SCS that can be managed by the ports their distinction will mainly be made according to that of ENISA. The two categorizations are analyzed below.

According to a European Sea Ports Organization (ESPO) report published in 2010 on the governance of European ports [4], port authorities are classified based on the annual volume of goods handled into small, medium and large.:

- small: 10 million tonnes maximum;
- medium: more than 10 million tonnes and 50 million tonnes maximum;
- large: more than 50 million tonnes.

In 2019, the European Union Agency for Cybersecurity (ENISA) published a study on good practices for cyber security in shipping and in particular in ports [3]. According to this, ports can be distinguished into three main groups, depending on the categories of their maritime SCS infrastructure and services:

- cargo: those that have special infrastructures for the management of operations, such as loading, unloading and storage of goods, sanitary and customs control, etc., and related to any type of cargo, for example liquid, dry, container, etc.;
- passenger: those whose infrastructures are

specially designed for the transport of vehicles and passengers and provide reception services for them on ships with parking areas, passenger corridors, bars/restaurants, etc., e.g., serve ferries or Roll-on/Roll-off (Ro-Ro) ships, where the goods are transported in trucks and lorries;

- fishing: those which provide services related to fish-ing, through their special infrastructures, such as the reception of fishing vessels, loading and unloading, inspection, storage and cooling of catches, etc.

However, a small port facility may have additional roles due to its uniqueness in the area, such as serving Navy or Coast Guard vessels. By the same logic, the SCS that can be served by an SMP are from passengers on liners, private boats and yachts, boats and fishing trawlers, to goods and materials, such as for earthworks and construction works. The SCS that can be managed by an SMP is not limited in terms of its distance or the value of the goods transported, but only in terms of the volume of the goods, the infrastructures and the systems used. For example, a cargo of electronic devices could be transported from China or America, chocolates from Switzerland or diamonds from Africa, but it would be impossible for a ship carrying liquefied gas or containers to dock and unload its cargo, because of the shortcomings of its infrastructure, such as large terminals, special cranes or water depths. Regarding the legal and regulatory framework that applies to SMPs, "all the necessary regulations apply to both small and large ports and the cost of compliance can be disproportionately high," as Howard Holt, director of Sea-ports, reports [5]. The same applies to standards, as they are designed to cover the full range of infrastructure and processes that may need to be secured.

3. Potential Threats and Attacks

Port facilities are places through which countless crowds of people pass every day and a large volume of goods are traded worldwide and, by extension, provide equally great economic, political or even military benefits to the respective region. For this reason, they can become the target of a multitude of criminal actions. However, the losses a port can suffer from maritime crime are not only financial, which are often immediate. Costs may include potential loss of life, reemployment, retraining, redesigning functions, spending time with law enforcement such as the Coast Guard, lawyers, etc. or even the mass media. This means that the costs include port exposure and by extension exposure to liability, loss of goodwill and reputation, loss of business and/or increased insurance costs. So overall there is a big impact on productivity [6].

The most important physical threats that a port can face are fraud, for example, through false customs declarations for financial gain, sabotage for military, political or ideological reasons, vandalism, theft of property, unauthorized access to its premises, vehicles and equipment or even unauthorized port entry via vehicles. In addition, common

physical threats are terrorism for political, ideological or religious reasons, hacktivism, coercion, extortion or corruption, as well as piracy, any sort of illegal action or other crime. Finally, environmental or natural disasters are always potential physical threats [3].

As technology evolves, ports are becoming increasingly complex environments that include both onshore and offshore activities and systems, while combining the physical and digital worlds [7]. This results in them facing additional cyber threats. Such can be mediation and monitoring of communications and systems or espionage, interception or causing functional problems in systems through various cyber attacks, such as denial of service (DoS), entry of malicious software (malware), social engineering, etc. In addition, they pose intentional threats, such as the leakage or deletion of information by employees, system errors, etc., as well as failures or malfunctions. Finally, power or network outages, as well as staff shortages could paralyze the operations of the entire port [3]. Ports play an important role in SCSs and their infrastructures have interdependencies at multiple levels, such as local, national or international. In this context, they closely interact with all the factors of a SCS, i.e., SCS provider, SCS business partners (BPs), SCS physical and IT/OT/IoT assets, various authorities. This results in cyber-physical threats such as eavesdropping, piracy, interception, malicious activity and abuse, accidental damage, physical attacks as well as system failures and malfunctions, internally, externally and/or pervasively [8].

In a port, as in a SCS, there are different services that have been developed for the smooth running of business activity. All services are affected by threats that have various consequences if a malicious user exploits them. According to [3] there are specific categories of effects that may occur due to threats and attacks in such a space and environment. Such may be the shutdown/paralysis of the port operations, human injury or death, theft of cargo/goods, theft of sensitive/critical data, financial loss, illegal trafficking, theft of money/fraud, system failures/disaster, loss of competitiveness/tarnished reputation and/or environmental disaster. A further category of impact is added to this work; that of social/commercial/political disruption. The impact of cyber-attacks can extend to a SCS, even on a physical level, which, depending on the type of good being transported, can be more or less devastating. Examples of dangerous goods are classified by International Maritime Organization (IMO), according to the main risks they pose during transport (e.g., explosive substances and articles, gases, radioactive material, etc.) [9].

4. Attack Scenarios

According to the formula, risk is equal to the product of the probability of an event occurring times the impact it will have ($\text{Risk} = \text{Probability} \times \text{Impact}$). This means that probability and impact are inversely proportional to each

other, while both are proportional to the risk itself. In other words, the greater the probability of something happening or the impact it will have, the greater the risk. Essentially, any threat, cyber or physical, that can happen to a large port can be adapted to the goods of a smaller one. The main difference is that in SMPs there is often a resource constraint, which increases the degree of impact, or a reduced budget, therefore insufficient security measures, which increases the probability and consequently leads to increased risk.

For a risk to manifest, a threat must be found to match a vulnerability in order to have an impact. In other words, a malicious user must successfully exploit a vulnerability. Next, three attack scenarios are described based on different types of threats, which could cause particularly problematic effects, even paralyzing the entire port and by extension the entire region that benefits from or depends on it.

4.1. SQL injection attack on a database of a ferry ticket purchase website (cyber threat)

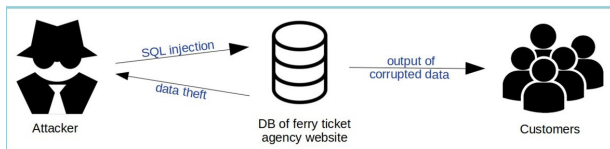
Assume that someone malicious (e.g., competitor, spy) via SQL injection gains access to the database (DB) of the ferry ticketing website of a small company that owns a limited number of passenger cruise ships that operate from the port of a small island to that of a larger one and vice versa, three times a week. The attacker compromises the confidentiality, integrity and/or availability (CIA) of passen-

Table 1: Elements of scenario 4.1

1.	Maritime SCS	Transportation of passengers and/or patients
2.	SCS Provider	Small ferry company/ticket agent
3.	SCS BPs	i. Small island medical center ii. Large island hospital/clinic iii. Port authority
4.	SCS Assets	a. Digital: ticket agent website (DB, server, etc), passenger data b. Physical: vessel, medical centers, people (passengers, employees, crew, port staff), SMP
5.	Threats	a. Cyber: SQL injection, illegal access b. Physical: -
6.	Impacts	<ul style="list-style-type: none"> • Patient health burden / loss of life • Interception of personal data and payment details • Damage to company reputation • Financial loss of the company • Social, commercial and political disruption

ger data by gaining access to their personal information and their debit/credit card or other means of payment. The attacker can additionally create dummy passenger bookings in the DB with the aim of disrupting their transport and disorienting the Coast Guards. This tourist ship is also used by the junior doctor or the general practitioner of the small island's medical center for transfers of patients to the hospital of the larger island, patient referrals to the Emergency Department or to specialist doctors in general. Thus, it could either delay a transfer, as it would eventually have to be done in a different way (e.g., a special Coast Guard vessel or helicopter) or delay a referral, which could not be done in a different way, resulting in the health burden of the person needing medical care or even death. Such an incident would cause loss of human life, heavy damage to the company's reputation, financial damage, political unrest.

The elements characterizing the above scenario are summarized in Table I and it is depicted in Graph I.



Graph I: Depiction of scenario 4.14

2. Terrorist act on a gas tanker truck inside a liner (cyber-physical threat)

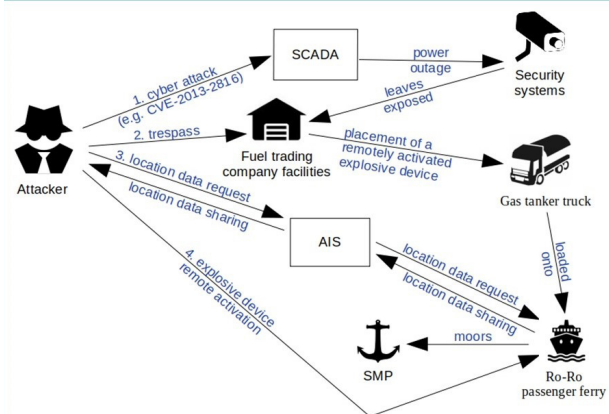
An SMP located within a natural bay, when free from scheduled coastal shipping routes, is often used by naval vessels when they are required to anchor temporarily to hide from the radar of enemy ships while patrolling the surrounding area. The enemy, unable to approach the port with its own warship, attacks the Supervisory Control And Data Acquisition (SCADA) system related to the supply of power to the gas warehouse and tanker trucks refueling facilities of a fuel trading company. This causes a power outage paralyzing all security systems in the area. Members of the terrorist group enter the site and place a remotely activated explosive device on a gas tanker truck. The tanker truck then follows its established route, for which it must be loaded onto a Ro-Ro passenger ferry. The ship, in turn, temporarily moors at the specific SMP for boarding and disembarking passengers, as it is an intermediate destination of its itinerary. Then, knowing the precise location of the ship through the Automatic Identification System (AIS), which shares the data publicly, the terrorist group remotely activates the explosive device, with the risk that the initial explosion could cause a larger explosion if extended and in the ship's fuel tanks. This results in injuries and loss of human life, as well as the destruction of the port or even part of the residential area around it with all this implies for the functionality, economy and tourism of the area, while at the same time alerting the national security and the navy loses an important cov-

er position for its ships, thus making its work on patrols more difficult.

The elements characterizing the above scenario are summarized in Table II and it is depicted in Graph II.

Table II: Elements of scenario 4.2

1.	Maritime SCS	Transportation of fuel
2.	SCS Provider	Fuel trading company
3.	SCS BPs	i. Shipping company that owns the large ship of the line ii. Shipping company to which the oil tanker vehicle belongs iii. Port authority
4.	SCS Assets	a. Digital: fuel provider systems (SCADA, PLC, etc.), AIS b. Physical: fuel tanker vehicle, ship, people (passengers, employees, crew, port staff), SMP
5.	Threats	a. Cyber: attacks on fuel provider systems (SCADA, etc.) b. Physical: trespass, explosion
6.	Impacts	<ul style="list-style-type: none"> • Injuries/loss of life • Destruction of the port and potentially part of the surrounding residential area/damage to the functionality, tourism and economy of the area • Jeopardizing national security, reputation of the country • Patient health burden/loss of life



Graph II: Depiction of scenario 4.2

4.3. Attack on oil tanker's HSMS System (cyber-physical threat)

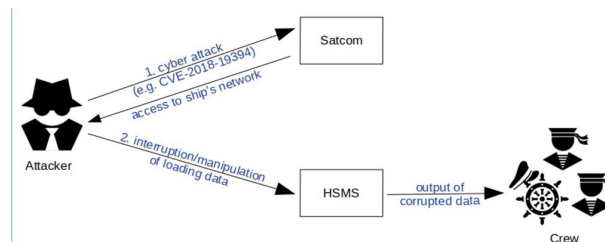
There are ports of small island regions that serve tankers carrying oil, which is vital for residents as it is used to generate energy. The transport of this good, of course, is also common in larger ports, in order to supply factories, gas stations, etc. If the process of loading and unloading these ships is not done carefully enough and the neces-

sary safety measures are not taken, then oscillations are created capable of splitting the ship in half and consequently sinking. For this reason, the Hull Stress Monitoring System (HSMS) is used to help the crew ensure that design specifications are not exceeded, hogging and sagging are avoided and the ship balances more correctly by sending audible signals to the bridge if excessive stress is detected on the ship's reefs. Suppose a malicious crew member gains access to the ship's network and then to the HSMS in order to intercept or manipulate the cargo data fed to and from the monitoring system. As the crew fully trusts the system during the unloading process, they believe that everything is going well, until the ship from the significant deformations in its hull caused by the excessive pressures breaks in two and finally sinks in the harbor. Alternatively, a malicious person could gain access to the ship's network remotely, by hacking the Satellite Communication (Satcom) system. The sinking of the ship can cause injuries or even loss of human life, loss of energy and all that this entails due to the loss of oil, environmental disaster, port malfunction until cleared, as well as damage to the reputation and, by extension, financial loss of the shipping company, but also of the area itself, due to the reduction/loss of tourism.

The elements characterizing the above scenario are summarized in Table III and it is depicted in Graph III.

Table III: Elements of scenario 4.3

1.	Maritime SCS	Transportation of oil
2.	SCS Provider	Oil provider
3.	SCS BPs	i. Shipping company ii. Transport company iii. Port authority
4.	SCS Assets	a. Digital: HSMS, Satcom system b. Physical: oil, ship, port and area environment, people (passengers, employees, crew, port staff), SMP
5.	Threats	a. Cyber: attack on the ship's HSMS/remote attack on the ship's Satcom system b. Physical: malicious crew, illegal access of natural port resources
6.	Impacts	<ul style="list-style-type: none"> • Injuries/loss of human life • Environmental disaster • Loss of energy due to the loss of oil • Port malfunction until cleared • Damage to the reputation of the shipping company • Financial damage to the company and also to the island due to reduction/loss of tourism



Graph III: Depiction of scenario 4.3

5. Conclusions and Future Work

In this study, basic concepts related to ports are analyzed, such as the categories used to be distinguished and their characteristics, such as their size, operational scope, infra-structure, focusing on small and medium-sized ports (SMPs). An overview of a brief port risk analysis is provided citing potential threats such as interception of sensitive information, illegal access, terrorism, as well as cyber, physical and/or combined (cyber-physical) attacks and the impacts they can cause. Based on different types of threats, three attack scenarios are presented, which show how particularly problematic effects can be caused to SMPs by exploiting vulnerabilities in maritime supply chain services (SCSs) capable of crippling an entire port and by extension the entire region benefiting from it.

All ports are economically and strategically valuable to surrounding areas, especially SMPs, as there are areas that are completely dependent on them. All of the above leads to SMPs acting as hubs of an SCS like major ports, since the delivery of goods has no borders. The fact that SMPs have the same types of needs, work under the same laws and regulations as major ports and can be exposed to similar threats and attacks challenges their day-to-day safe and secure operation, due to the limitation of financial resources and the expenses of security management. Risk analysis is a process that usually requires deep knowledge of the infra-structure and factors that can affect the operation of an organization, so cybersecurity experts are needed to model and calculate risk.

There is a need for a methodology and a corresponding tool that can provide a holistic solution of highly automated cyber risk assessment and enable the correlation of cyber and physical threats. Our future research work leans towards this direction and aims to create a methodology and a tool that can be easily used by SMPs as well.

Acknowledgment

This work is supported by Partnership Agreement for the Development Framework 2014-2020, Operational program "Competitiveness, Entrepreneurship & Innovation" (EPA-nEK), in the context of the project CYSMET: Integrated, Dynamic & Collaborative Risk Management System for Maritime Transport & Supply Chains, with project number: T2EAK – 03488. The authors also thank all partners of this project as well as the University of Piraeus, Research Centre (UPRC) for its continuous support.

References

- [1] ISO 28000:2007 international standard, "Specification for security management systems for the supply chain", 1st Edition 2007-09. Online available: <https://www.iso.org/standard/44641.html>, accessed on September 14 2022.
- [2] ENISA, "Cyber security aspects in the maritime sector", December 19, 2011. Online available: <https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1>, accessed on September 14 2022.
- [3] ENISA, "Port Cybersecurity - Good practices for cybersecurity in the maritime sector", November 26, 2019. Online available: <https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector>, accessed on September 14 2022.
- [4] ESPO, "The ESPO Fact-Finding Report", 2010. Online available: <https://www.espo.be/media/espopublications/espofactfindingreport2010.pdf>, accessed on September 14 2022.
- [5] "A cluster initiative: Small and Medium Sized Ports as Hubs for Smart Growth and Sustainable Connectivity", 2 Seas Magazine, November 2014. Online available: http://archive.interreg4a-2mers.eu/2seas-files/page_ext_attachments/1602/PAC2_2SEAS_MAGAZINE_EN.pdf, accessed on September 14 2022.
- [6] U.S. Department of Transportation, "Port Security: A National Planning Guide", May 21, 1997. Online available: <https://rosap.ntl.bts.gov/view/dot/13693>, accessed on September 14 2022.
- [7] The Institution of Engineering and Technology, "Good Practice Guide – Cyber Security for Ports and Port Systems", January 27, 2020. Online available: <https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice>, accessed on September 14 2022.
- [8] ENISA, "Guidelines - Cyber Risk Management for Ports", December 17, 2020. Online available: <https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports>, accessed on September 14 2022.
- [9] IMO, "International Maritime Dangerous Goods (IMDG) Code", 2020, Corrigenda May 2022. Online available: https://wwwcdn.imo.org/localresources/en/publications/Documents/Supplements/English/QM200E_180522.



Pinelopi Kyranoudi has obtained her master's degree in Security of Information and Communication Systems from the School of Engineering of the University of the Aegean (Dept. of Information and Communication Systems Engineering). She served as Network and Information Security Officer at the European Union Agency for Cybersecurity (ENISA) contributing: to five publications in the areas of Cybersecurity in Maritime, e-Health, and National Cybersecurity Strategies; to the creation of web tools, and to the organization of EU Cybersecurity events. She worked as a Web and Application Developer at Express Publishing S.A. and as IT Security Engineer at Cosmote S.A., among others. She is currently conducting her Ph.D studies in the Cybersecurity field at the University of Piraeus (Dept. of Informatics). She holds a position as Cybersecurity researcher at Maggioli SpA. Her research interests are in the field of Cyber Security, especially in Maritime, IoT, and Threat Intelligence



Professor Nineta Polemi has obtained her Ph.D. in Applied Mathematics (Coding Theory) from The City University of New York (Graduate Center). She is an Associate Professor in the University of Piraeus (Dept. of Informatics) teaching cryptography, security of ICT systems, port security and e-business & innovation. She is a member in the European Network of Information Security Agency (ENISA) high level expert groups on Artificial Intelligence and working group on Risk Assessment. She has served as Programme Manager and Policy Officer in the European Commission, DG CONNECT, Unit H1: Cybersecurity Technologies & Capabilities. She held teaching and research positions in Queens College, Baruch College of City University of New York, the State University of New York and Université Libre de Bruxelles (ULB)- Solvay Brussels School. She has acted as President of the BoD in the security consultancy company, Expertnet. Her research interests are in the fields of security and cyber defense. She has over one hundred publications in the above areas and

has organised numerous security scientific international events. She has received many research grants from various organizations such as the Danish Research Foundation, MSI Army Research Office/Cornell University, IEEE, State University of New York (SUNY), and The Graduate School of City University of New York (CUNY). She has been project manager (PM) / technical manager (TM) in security projects of various programmes such as National Security Agency (NSA), NATO, Dr. Nuala McGann Drescher Foundation, Greek Ministry of Defence the last three (5th, 6th, 7th) Framework Programmes of the European Commission (E.C.)