frontiers | Frontiers in Computer Science

TYPE Methods
PUBLISHED 27 June 2023
DOI 10.3389/fcomp.2023.1156726

OPEN ACCESS

EDITED BY
Stephen James McCombie,
NHL Stenden University of Applied Sciences, Netherlands

REVIEWED BY
Georgios Kavallieratos,
Norwegian University of Science and Technology, Norway
Adam Turner,
Macquarie University, Australia

*CORRESPONDENCE
Pinelopi Kyranoudi
✉ pkyranoudi@unipi.gr
Nineta Polemi
✉ dpolemi@unipi.gr

RECEIVED 01 February 2023
ACCEPTED 24 May 2023
PUBLISHED 27 June 2023

CITATION
Kyranoudi P and Polemi N (2023) Securing small and medium ports and their supply chain services. *Front. Comput. Sci.* 5:1156726. doi: 10.3389/fcomp.2023.1156726

Securing small and medium ports and their supply chain services

Pinelopi Kyranoudi[1,2]* and Nineta Polemi[1,3]*

[1]Department of Informatics, University of Piraeus, Piraeus, Greece, [2]MAGGIOLI SPA, Santarcangelo di Romagna, Italy, [3]trustilio B.V., Amsterdam, Netherlands

This paper argues that small and medium sized ports (SMPs) are as important as larger ones in terms of supply chain service (SCS) management and security, as they can become the weakest links for national and European Union (EU) resilience and security. It focuses on explaining key concepts about SMPs, their characteristics (e.g., size, operational field, infrastructure), potential threats (e.g., interception of sensitive information, illegal access, terrorism) and attacks (cyber, cyber-physical), as well as basic security concepts (e.g., attack path, attack vector, risk). Three SCS attack scenarios for SMPs are described based on different types of threats, which could cause catastrophic impacts, even paralyzing an SMP propagated in its SCS. Finally, a risk management methodology for SCSs that can be used by SMPs, named CYSMET, is presented considering their capabilities, needs and constraints.

KEYWORDS

maritime, small and medium sized ports (SMPs), supply chain service (SCS), cyber-physical security, attack scenarios, risk management methodology

1. Introduction

Small and medium sized port (SMP) facilities are often the mainstay of a variety of societal activities in remote areas (e.g., islands, riverside, small port villages), they are of geopolitical importance and the main economic drivers in these areas (Haase and Maier, 2021). SMPs are also supply chain service (SCS) providers and interconnecting with various entities (e.g., coast guards, customs, shipyards, insurance companies), other critical infrastructures (e.g., energy, transportation, telecommunications), people (e.g., port operators, crew, providers), aimed at providing maritime services [e.g., cruise services, container management, liquefied natural gas (LNG) transport]. So far, the cybersecurity field in these types of ports has lacked attention in existing risk analysis methodologies. This study challenges the belief that SMPs are less important than larger ones when it comes to SCS management and security. On the contrary, it claims that vulnerable SMPs may become the weakest links to national and European Union (EU) resilience and security.

In recent years, SCSs have significantly increased their reliance on Information and Communications Technology (ICT) with the aim of providing innovative services in the context of the highly competitive maritime trade (European Union Agency for Cybersecurity (ENISA), 2011). 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, 5G, Internet of Things (IoT), and satellite technologies, among others.

Some of the most well-known security events, due to their impact, are the NotPetya ransomware on Maersk, the cyber attack on the port of Antwerp, and the ransomware attacks on the ports of San Diego and Barcelona [European Union Agency for Cybersecurity (ENISA), 2019]. Such cyber attacks also put SMPs in the target zone, as they use similar systems but on a smaller scale. During July 2021–July 2022, vulnerability exploitation was reported to have increased by 33% compared to 2020 and was the most common cause of security incidents [European Union Agency for Cybersecurity (ENISA), 2022]. After the drop of COVID-19, IoT malware increased in the first half of 2022 by almost 100%, with the volume of attacks already higher than in the last 4 years [European Union Agency for Cybersecurity (ENISA), 2022]. Consequently, such events also affect the SCSs, whose cybersecurity incidents have also found fertile ground in the conflict between Russia and Ukraine (National Maritime Foundation, 2022).

This paper starts with an explanation of the port categories and the characteristics of SMPs. The potential threats and attacks on SMPs and SCSs are also analyzed as well as basic security concepts. Then, based on these, three port attack scenarios of SMPs are described to illustrate the likelihood of occurrence, as well as the significance and extent of potential cascading effects. Finally, a risk management methodology for SCSs in SMPs addressing their characteristics is proposed. This methodology is named CYSMET, and is based on the following existing SCS risk analysis methods:

- CYSM (Papastergiou et al., 2015),
- MEDUSA (Papastergiou et al., 2018),
- MITIGATE (Schauer et al., 2019), and
- eBIOS [Agence nationale de la Sécurité des Systèmes D'information (ANSSI), 2019].

A glossary of acronyms of this work is available in Table 1.

TABLE 1 Glossary of acronyms.

Acronym	Meaning
AI	Artificial Intelligence
AIS	Automatic Identification System
ANSSI	National Agency for the Security of Information Systems
AR	Availability Requirement
BP	Business Partner
CIA	Confidentiality, Integrity, Availability
CR	Confidentiality Requirement
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DB	Database
DDoS	Distributed Denial of Service
DoS	Denial of Service
ENISA	European Union Agency for Cybersecurity
ESD	Enhanced Security Declaration
ESPO	European Sea Ports Organization
EU	European Union
H	High
HSMS	Hull Stress Monitoring System
ICT	Information and Communications Technology
IoT	Internet of Things
IR	Integrity Requirement
IRL	Individual Risk Level
ISPS	International Ship and Port Facility Security
IT	Information Technology
IVSL	Individual Vulnerability Severity Level
L	Low
LNG	Liquefied Natural Gas
M	Medium
MA	Modified Availability
MAC	Modified Attack Complexity
MAV	Modified Attack Vector
MC	Modified Confidentiality
MI	Modified Integrity
MPR	Modified Privileges Required
MS	Modified Scope
MUI	Modified User Interaction
NVD	National Vulnerability Database
OT	Operational Technology
PoE	Ports of Entry

(Continued)

2. Port categories and characteristics of SMPs

To be able to understand the characteristics of SMPs, it is necessary to first study port classifications in general. 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 following are some port taxonomies found in the literature.

Based on the official guidelines of the Trans-European Networks (TENs), seaports are divided into three major categories (INTERREG IV A 2 Mers Seas Zeeën, 2014):

- Ports of international importance: minimum total annual transport volume of 1.5 million tons of cargo or 200,000 passengers;
- Ports of EU importance: minimum total annual transport volume of 0.5 million tons of cargo or 100,000 passengers;
- Ports of local importance: provide access to insular, regional or particularly remote areas.

TABLE 1 (Continued)

Acronym	Meaning
Ro-Ro	Roll-on/Roll-off
Satcom	Satellite Communication
SCADA	Supervisory Control and Data Acquisition
SCS	Supply Chain Service
SLA	Service Level Agreement
SMP	Small and Medium sized Ports
SQL	Structured Query Language
TENs	Trans-European Networks
VH	Very High
VL	Very Low
VSL	Vulnerability Severity Level

However, from examples such as the Danube or Black Sea ports, it is evident that even ports carrying a total annual volume of fewer than 0.5 million tons of cargo or 100,000 passengers or providing access to insular, regional, or particularly remote areas can be of EU or international significance. The categorization of the European Sea Ports Organization (ESPO) [European Sea Ports Organisation (ESPO), 2010] closes this gap, according to which port authorities are classified based on the annual volume of goods handled into:

- Small: 10 million tons maximum;
- Medium: more than 10 million tons and 50 million tons maximum;
- Large: more than 50 million tons.

From another perspective, according to a European Union Agency for Cybersecurity (ENISA) study [European Union Agency for Cybersecurity (ENISA), 2019], 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 fishing, through their special infrastructures, such as the reception of fishing vessels, loading and unloading, inspection, storage and cooling of catches, etc.

In addition, ports can also be categorized based on the type of water or land that encloses them (CYRENE EU H2020 Project, 2020–2023):

- Seaports: built on the coast of the sea or ocean;
- Inland ports: built near small water shorelines, such as lakes, rivers or their estuaries, which may end up in the sea or ocean, through a system of canals;
- Dry ports: types of inland ports, built in areas without water, which are connected to seaports by roads or railway facilities and usually act as multi modal transport hubs;
- Warm-water ports: built near waters that do not freeze during the winter, allowing their operation throughout the year.

This classification does not contradict the previous ones, as a port can belong to more than one category at the same time. The same applies to other types of ports such as the ones below (CYRENE EU H2020 Project, 2020–2023):

- Cruise home ports: usually consist of large terminals, from where services are provided for embarking and receiving cruise ship passengers, as well as loading and unloading supplies useful for the cruise, for example from drinking water and fuel to luxury food and beverages;
- Ports of call: ship station, which can be defined by charter, included in a predetermined itinerary of any type of ship for loading and unloading of goods, receiving and embarking passengers or traveling cruise ships or to be used in emergency cases of danger or need patrol boats, navy, denunciation, sabotage, inspection, control of violation of legislation, supply, etc.;
- Ports of entry (PoE): stations with a special customs presence, where services are provided to receive passengers and goods in a country, as well as border security services, passport control, baggage and goods inspection, etc.;
- Smart ports: those that use smart technologies in order to manage their SCS more efficiently, for example IoT, artificial intelligence (AI), blockchain, cloud-based software, automation, etc.

The most common approach to categorizing ports is to use metrics based on the annual volume of goods. However, to see the ports as holistically as possible, their categorization will be focused on two main axes; their size and the type of SCS they operate. Therefore, for the needs of this study, both the ESPO categorization will be adopted regarding the size of the ports, and the aforementioned ENISA approach regarding the type of SCS.

Nevertheless, an SMP may have additional roles due to its uniqueness in the area, such as serving Navy or Coast Guard vessels. By the same token, the SCSs that can be served by SMPs range from passengers on liners, private boats and yachts, fishing boats and trawlers to goods and materials, such as 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 in some cases it would be impossible for a ship carrying LNG or containers to dock and unload its cargo, due to the infrastructural

shortcomings, such as large terminals, special cranes, water depths, and skilled maritime operators.

Regarding the legal and regulatory framework applicable to SMPs, it applies to larger ones as well, except that compliance costs for SMPs can be disproportionately high (INTERREG IV A 2 Mers Seas Zeeën, 2014). The same applies to standards [e.g., International Ship and Port Facility Security Code (ISPS) (International Maritime Organization (IMO), 2004), ISO/IEC 2700x (International Organization for Standardization (ISO), 2018–2022], as they are designed to cover the full range of infrastructure and processes that may need to be secured.

3. Security fundamentals of SMPs and SCSs

SMPs are places through which people pass every day, goods are traded worldwide and, by extension, provide equally great economic, cultural, societal, 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 an SMP can suffer from maritime crime are not only financial, which are often immediate. Consequences may include potential loss of life, re-employment, re-training, re-designing 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 (U.S. Department of Transportation, 1997).

The most important physical threats that an SMP 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 [European Union Agency for Cybersecurity (ENISA), 2019].

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 [The Institution of Engineering Technology (IET), 2020]. 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, phishing, 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 [European Union Agency for Cybersecurity (ENISA), 2019].

SMPs play an important role in SCSs and their infrastructures have inter-dependencies at multiple levels, such as local, national or international. In this context, they closely interact with all the factors of an 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 [European Union Agency for Cybersecurity (ENISA), 2020].

It is also worth noting that some SCS cybersecurity challenges are related to the lack of cybersecurity certificates for port systems (e.g., Port Community System) and services, security risks related to remote vendor access to port networks/systems, long repair cycles for some system types, heterogeneity, large number of suppliers and difficulty in switching supplier services. In addition, external partners do not have sufficient control over the level of cyber security of their suppliers and consequently the risks created [European Union Agency for Cybersecurity (ENISA), 2019].

In an SMP, as in an 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 European Union Agency for Cybersecurity (ENISA) (2019) there are specific categories of effects that may occur due to threats and attacks in this 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 an SCS, even on a physical level, which, depending on the type of good being transported [e.g., classes of dangerous goods, according to the IMO (International Maritime Organization (IMO), 2022)], can be more or less devastating. If an SCS attack event occurs on an SMP, the results can be destructive, both for the SCS itself, as well as for the SMP and the region it serves. Such an impact may affect geopolitics, and lead to a new motivation for another potential attacker. This is something that has been noticed in the conflict between Russia and Ukraine, as hacktivist activity and cybercrime have increased significantly during July 2021–July 2022 [European Union Agency for Cybersecurity (ENISA), 2022].

In general, there are four different motivations that can lead an attacker to take related actions; (i) financial gain, geopolitics related to either (ii) espionage or (iii) disruptive actions, and (iv) ideological. Typically, the main threats fall under these motivations fairly evenly, with the exception of ransomware, which, while it can be a tool of destruction, is primarily aimed at financial gain [European Union Agency for Cybersecurity (ENISA), 2022]. It is very important for the organizations to find out the motives of their attackers in order to decide how their defense efforts should work [European Union Agency for Cybersecurity (ENISA), 2022]. In addition to motivation, it is also important to gauge the attacker's expertise and resources. According to International Organization for Standardization (ISO) (2012), these three components constitute a perceived possibility of the success of an attack, should it be launched, called attack

potential. In this paper, the concept of attack potential will be included in risk calculation in the form of an attacker profile (Section 5.3).

The attackers use a path or methods to penetrate an SCS asset or network in order to deliver a malicious outcome, which is defined as an attack vector (CYRENE EU H2020 Project, 2020–2023). Attack vectors can take many different forms, such as compromised credentials, weak and stolen credentials, ransomware, fishing, zero-day vulnerabilities, no or poor encryption, incorrect configuration, brute force attack, Distributed Denial of Service (DDoS) attack, etc.

All possible paths that a potential attacker can use to break into a target network are represented by specific data structures, called attack graphs (CYRENE EU H2020 Project, 2020–2023). In order to create an attack graph, it is necessary to analyze vulnerability information related to a specific component, network topology, and accessibility conditions between network hosts. They can be an extremely effective vulnerability analysis tool as they provide insight into potential attacker behavior before an attack occurs. They allow the detection and defense of potentially compromised nodes.

The implementation of one or more attack paths by attackers, starting with the exploitation of a vulnerability in a component used as an entry point, which allows a progressive security impact on specific components, and ends at a target point, is known as a vulnerability chain (CYRENE EU H2020 Project, 2020–2023). Figure 1 illustrates an example of different vulnerability chains that can be created among the vulnerabilities Vi of assets A1, A2, and A3, e.g., V1, A1 → V5, A2 → V7, A3.

As more information is added to a vulnerability chain system, new attack vectors can be created and exposed. In order to identify, communicate and understand threats and mitigation measures to protect an asset or an organization, all information collected that affects its security is represented in a structured way, the so-called threat model. In other words, threat modeling answers questions such as what people are working on, what can go wrong, what can be done to protect vulnerable assets from identified threats, and whether the measures taken were effective (The OWASP® Foundation, 2023).

The question of what can go wrong can otherwise be renamed risk. Risk represents the probability of occurrence of possible events or consequences or their combination under conditions that may change [International Organization for Standardization (ISO), 2018]. It is defined as the product of the probability of an event occurring times the impact it will cause (Risk = Probability * Impact) (Katsikas, 2013), or, in its extended version, Risk = Threat * Vulnerability * Impact, given that Probability = Threat * Vulnerability (Schauer et al., 2019).

Another concept, introduced by Common Vulnerability Scoring System (CVSS) [Forum of Incident Response and Security Teams (FIRST), 2019], which is part of the risk assessment and should not be used by itself, is the severity of a vulnerability. In this paper, this severity level will be used as part of the risk calculation (see Section 5.3).

From the above-mentioned formulas of risk, it follows that probability and impact are inversely proportional to each other, while they are proportional to the risk itself. In other words, the greater the probability of something happening or the impact it will cause, the greater the risk. Moreover, for a risk to manifest, a threat must be found that matches a vulnerability to have an impact. This means that an attacker must successfully exploit a vulnerability for a threat to appear.

4. SCS attack scenarios for SMPs

Essentially, any threat, cyber or physical, that can be exposed at a large port can also occur at a smaller one. The main difference is that in SMPs there are often limited resources, therefore insufficient expertise and security measures, leading to an increased degree of impact or an increased probability of occurrence, thus an increased risk. Next, three attack scenarios on different SCSs based on two types of threats (i.e., cyber, cyber-physical) are described, which could cause particularly problematic results, even paralyzing the entire SMP and by extension, the entire beneficiary or dependent region.

4.1. Attack scenario on SCS1—Transportation of passengers and/or patients

Assume that an adversary (e.g., competitor, spy) via Structured Query Language (SQL) injection [web application attack, in which the attacker manipulates data from database (DB) servers by inserting inputs into a system and executing malicious statements (Alghawazi et al., 2022)] gains access to the 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 passenger 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 synopsis of the SCS of the above-mentioned scenario is illustrated in Table 2.

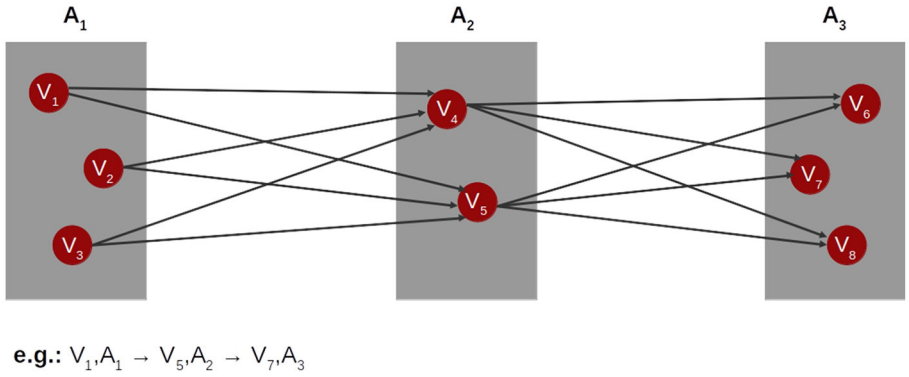

FIGURE 1
Graph example of vulnerability chains.

TABLE 2 Synopsis of SCS1: transportation of passengers and/or patients.

SCS1: Transportation of passengers and/or patients	
Provider	Small ferry company/ticket agent
BPs	Small ferry company/ticket agent, small island's medical center, SMP, large island's port authority, large island's hospital/clinic
SCS Assets	Cyber: ticket agent website (DB, server, etc), passenger data Physical: vessel, medical centers, people (passengers, employees, crew, port staff), SMP
Threats	Cyber: SQL injection, illegal access Physical: –
Impacts	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

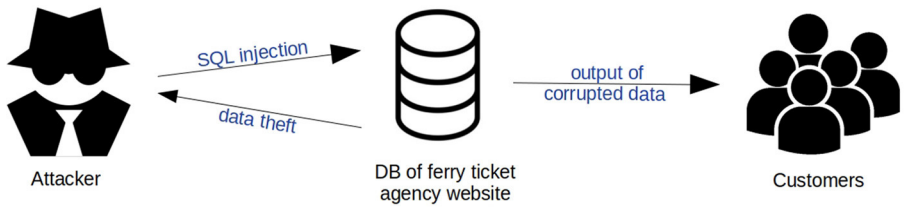

FIGURE 2
Attack graph of the SQL injection on a DB of a ferry ticket purchase website scenario on SCS1.

The attack graph of the SQL injection on a DB of a ferry ticket purchase website scenario is depicted in Figure 2.

SQL injection is a very common threat for DBs, which should make the BPs consider the wider implications of such an event not only to SMPs but on everyone who may depend on them.

4.2. Attack scenario on SCS2—Transportation of fuel

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), whose data are publicly available, 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 SMP 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 cover position for its ships, thus making its work on patrols more difficult.

The synopsis of the aforementioned scenario's SCS is presented in Table 3.

The attack graph of the terrorist act on a gas tanker truck inside a liner scenario is described as follows, in Figure 3.

The attackers' logic is to see opportunity where most people see schedule and convenience. The aforementioned scenario is an example of how everyday practices could act as a Trojan Horse and cause hard-to-recover consequences in SMPs and the surrounding area.

4.3. Attack scenario on SCS3—Transportation of oil

There are insular SMPs 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 conducted with care and the necessary 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 synopsis of the SCS of the scenario mentioned above is depicted in Table 4.

The flow of the attack on oil tanker's HSMS System scenario is described in the following attack graph, in Figure 4.

The open sea is not the only dangerous place to sink a ship. In fact, there are cases like this attack scenario where a port, especially an SMP, and the people involved can suffer greatly from a sinking ship.

The above attack scenarios were successful because the measures were not sufficient. Assessing and managing risks (implementing appropriate measures) is most important for the security of the entities. This is where CYSMET comes in, a proposed SCS risk management methodology designed to help SMPs assess and manage their risks.

5. CYSMET—A proposed SCS risk management methodology

The CYSMET risk management methodology is to assist SMPs in assessing and managing their SCS risks. It is designed to be user-friendly for SMPs, which lack expertise and resources, allowing them to even conduct self-assessments. This methodology provides the user with input scores [e.g., NIST National Vulnerability Database (NVD[1]), MITRE Common Vulnerabilities and Exposures (CVE) Details,[2] attacker profile, risk calculation formula] and semi-automated procedures (CVSS v3.1 calculator[3]). In this way, an SMP can make use of CYSMET without needing special equipment, a cybersecurity expert team, or spending a lot of time and money.

5.1. Existing work and characteristics

This section refers to the existing SCS risk analysis methods that were reviewed, namely CYSM (Papastergiou et al., 2015), MEDUSA (Papastergiou et al., 2018), MITIGATE (Schauer et al., 2019) and eBIOS [Agence nationale de la Sécurité des Systèmes D'information (ANSSI), 2019], in order to create the CYSMET methodology.

The CYSM system is an innovative and scalable set of risk assessment tools, which facilitates a port's security team to identify, assess and effectively address security incidents affecting all port users and operators. Based on an innovative and dynamic risk management methodology, CYSM enables critical port infrastructure operators to assess physical and cyber risks against the requirements set out in the ISPS and ISO27001 security standards as well as the relevant legal and regulatory security framework.

MEDUSA is a risk assessment methodology that aims to systematically assess security risks affecting critical infrastructure operators in an SCS. MEDUSA's goal is two-fold. First, assessing the overall security risks of a SCS. The resulting aggregate risk values are used to define a baseline security policy, designating the least essential security controls required by each BP. In addition, MEDUSA allows the assessment of the cascading effects that a security event may have within the SCS.

MITIGATE is a system for assessing cyber risks in maritime SCSs. It is a dynamic software solution based on cloud computing that allows the involved stakeholders, such as ports and shipping companies, to monitor their IT environment, i.e., their software, hardware and networks for potential vulnerabilities. MITIGATE detects vulnerabilities, analyzes attack paths and considers the ripple effects of cyber threats within SCSs. In addition, it is based

1 https://nvd.nist.gov/

2 https://www.cvedetails.com/vulnerability-search.php

3 https://www.first.org/cvss/calculator/3.1

TABLE 3 Synopsis of SCS2: transportation of fuel SCS.

SCS2: Transportation of fuel	
Provider	Fuel trading company
BPs	Fuel trading company, large port authority, liner owning shipping company, SMP, gas stations
SCS assets	Cyber: fuel provider systems (SCADA, PLC, etc.), AIS Physical: fuel tanker vehicle, ship, people (passengers, employees, crew, port staff), SMP
Threats	Cyber: attacks on fuel provider systems (SCADA, etc.) Physical: trespass, explosion
Impacts	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

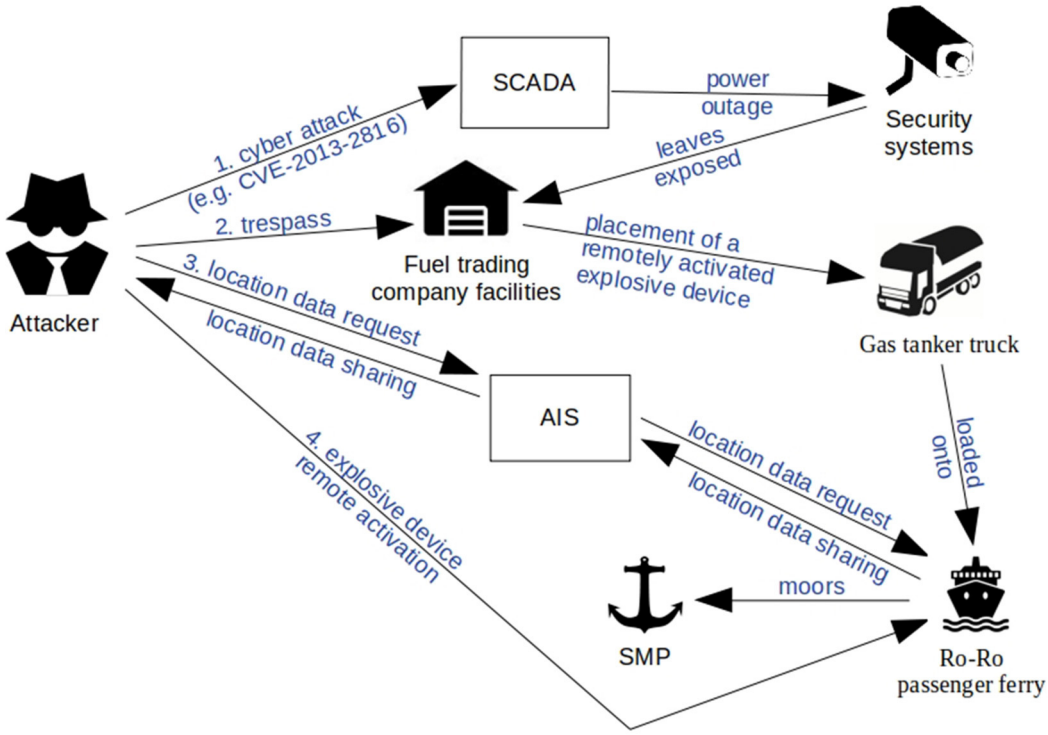

FIGURE 3
Attack graph of the terrorist act on a gas tanker truck inside a liner scenario on SCS2.

TABLE 4 Synopsis of SCS3: transportation of oil SCS.

SCS3: Transportation of oil	
Provider	Oil provider
BPs	Oil provider, loading port authority, shipping company, SMP, power plant
SCS assets	Cyber: HSMS, Satcom system Physical: oil, ship, port and area environment, people (passengers, employees, crew, port staff), SMP
Threats	Cyber: attack on the ship's HSMS/remote attack on the ship's Satcom system Physical: malicious crew, illegal access of natural port resources
Impacts	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

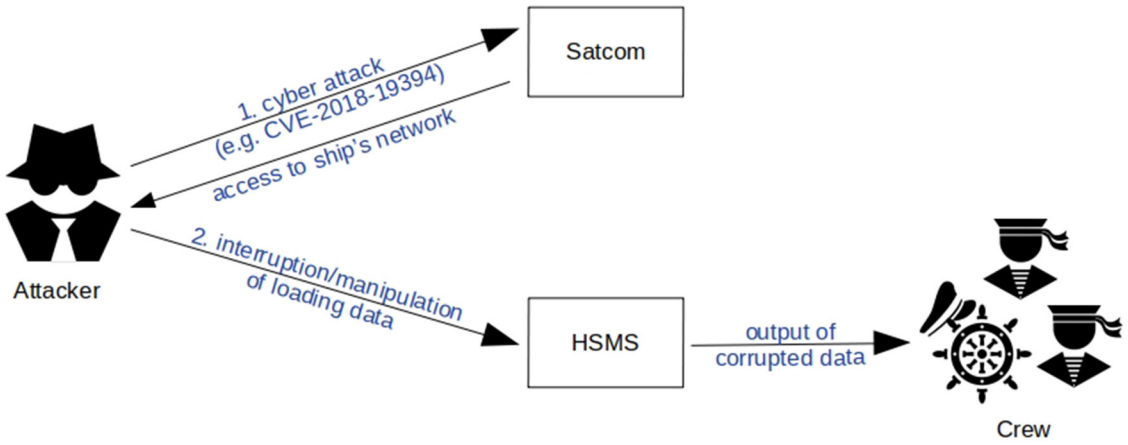

FIGURE 4
Attack graph of the attack on oil tanker's HSMS system scenario on SCS3.

on an in-depth analysis of user requirements and works with real-time threats, which are combined with identified vulnerabilities to recommend appropriate countermeasures.

EBIOS is a risk analysis method for information systems, created in 1995 by the French government. After more than 20 years of regular updates, the latest version intends to be more accessible and instructive than the previous ones, is named eBIOS Risk Manager and the French National Agency for the Security of Information Systems (ANSSI) is responsible for its maintenance. EBIOS is a high level, standardized approach, which supports decision-making by top management on both more general systems (e.g., electronic communications, mobile networks, or websites) and more specialized ones (e.g., business continuity plans, security master plans, or security policies).

The above methodologies are undoubtedly a solid foundation on which the CYSMET methodology can be based, as they introduce good practices and clearly defined risk analysis procedures. However, these methodologies also have limitations. In particular, the first three risk calculation methods are based on older versions of metric systems, such as the CVSS v2.0, while exploiting only a subset of their capabilities to calculate the impact on information systems. In addition, they do not consider the interactions between goods of the physical and digital world that may exist within a SCS. In practice, a physical threat can lead to a digital one, and vice versa. For example, a vulnerability in the loading and unloading system of a ship can lead to a physical threat, such as the destabilization of the ship, with the possible consequence of creating a fault, threatening the integrity of workers, contaminating the environment, etc. Such chains of cascading effects of cyber-physical threats remain a research challenge in the field of risk analysis in SCSs. Finally, the existing methodologies have been designed taking into account the operational and security requirements of large port facilities. The extent to which these methodologies can be adapted and adopted in smaller port organizations with different operational characteristics (e.g., limited computational and human resources) is a critical question. Although eBIOS is basically a self-assessment technique, which is more user friendly for SMPs, it remains a vague approach, based on a subjective and unquantified assessment that does not make any specific calculations in the corresponding vulnerability analysis phase and is not subject to external evaluation.

The CYSMET methodology aims to combine cyber and physical threats through a holistic solution while using the most up-to-date metric systems to quantify risk in SCSs. The entire CYSMET platform will support and integrate tools that will facilitate risk management through a user-friendly environment. Finally, CYSMET is harmonized with the operational and security requirements that exist in smaller port facilities, complies with all relevant standards and frameworks (Kyranoudi et al., 2021) and enhances the existing methodologies by:

- Including additional assets in the perimeter of the assessment (i.e., OT, IoT)—not only ICT;
- Using additional vulnerability database records related to OT and IoT;
- Calculating risk and attack paths originated by both cyber and cyber-physical threats;
- Applying the updated v3.1 of the CVSS;
- Utilizing all CVSS v3.1 metric fields: Base, Temporal and Environmental Scores to increase accuracy of the measurements;
- Using the vulnerability and impact assessments as a combined process, as the CVSS v3.1 takes into account the impact that a vulnerability exploitation could have on the environment under consideration.

5.2. Use and general assumptions

CYSMET methodology can be used by SCS providers and BPs, as well as any third-party (e.g., risk assessor, auditor), guiding them to manage cyber risks with a better control and management approach for the physical ones as well, in the best possible way.

TABLE 5 Description of the threat scale.

Threat scale values			Description		
Qualitative	Range (%)	Quantitative (%)	Incident history	Intuition and knowledge (probability)	Social information (probability)
VH	(80–100]	100	1 in the last 12 months	VH (>80%)	VH (>80%)
H	(60–80]	80	1 in the last 12 months	H (61%−80%)	H (61%−80%)
M	(40–60]	60	>1 in the last 2 years	M (41%−60%)	M (41%−60%)
L	(20–40]	40	≤1 in the last 2 years	L (21%−40%)	L (21%−40%)
VL	[1–20]	20	≤1 in the last 3 years	VL (≤20%)	VL (≤20%)

For the design of this methodology the following assumptions have been made:

- It is adapted to be used for SCSs by SMPs and their BPs.
- A Service Level Agreement (SLA) needs to be assigned among SCS provider and BPs for each SCS they are involved in, which includes its standard aspects, such as scope, quality assurance, responsibilities, etc.
- Since the specific methodology is at the level of assets, which concern the entire extent of an SCS, it is necessary for the SCS provider and BPs to generate an Enhanced Security Declaration (ESD), in order to ensure the protection and confidentiality of the data that will be processed. This statement is a prerequisite for process compliance in terms of ISO27001 [International Organization for Standardization (ISO), 2022], ISO27002 [International Organization for Standardization (ISO), 2022], ISO27005 [International Organization for Standardization (ISO), 2018], ISO28001 [International Organization for Standardization (ISO), 2007] and ISPS (IT) [International Maritime Organization (IMO), 2004] as it is a confidential and legally binding document included in the SLA and helps BPs identify all of their necessary assets for the SCS provision and the controls they have undertaken.
- SCS assets are isolated from the internal operations of BPs and dedicated to the provision of SCS processes.
- Cyber threats related to IT, OT and IoT are examined.
- It is assumed that the SCS can be modeled as a one-way graph, thus the cyber assets of the BPs are interconnected in one-way directed, linear paths.
- Only independent, linear attacks and not circular attacks are considered, since the SCS under consideration is represented by unidirectional graphs. Using game theory, existing methodologies such as MITIGATE have found this to be the silver lining of accurately calculating a multitude of possible attack paths while sacrificing the dubious outcomes of more complex types of attacks, therefore less likely to occur.
- The main threat categories (loss of CIA) correspond to specific vulnerability categories.
- It considers security controls, if and how they are implemented, and their implementation levels, as included in CVSS v3.1.
- The SCS is treated as the environment under consideration, which may be modified after a successful attack (CVSS v3.1 Environmental Score).
- NVD, CVE details, or other online open repositories can also be used.

5.3. Scales and measurements

To calculate the severity of vulnerabilities, the CYSMET methodology utilizes the CVSS v3.1, which consists of three metric groups: Basic Score, Temporal Score, and Environmental Score, providing a more accurate estimation of the vulnerability severity. The severity level is used as part of the risk calculation as the product of the vulnerability times the impact (Severity = Vulnerability * Impact).

The threat scale of Table 5 is used for the definition of a qualitative entry threat value and its conversion to a quantitative default value for the risk calculation. There are five threat categories [very low (VL), low (L), medium (M), high (H), and very high (VH)], and the assessment is based on the following criteria:

- The expected frequency of occurrence based on the history of previous events;
- The assessor's intuition and knowledge;
- The information to be extracted from the data retrieved from social media and existing repositories.

For the calculation of the risk, it is also needed to give a quantitative value to the attacker profile with the help of Table 6. Similar to the previous table, there are five qualitative values, from VL to VH, and they are identified according to:

- Their ICT skills: novice, narrow, skilled, expert, sophisticated;
- The resources it has: minimum, limited, medium, significant, sufficient; and
- The opportunities it may have or create for a successful attack: minimum, limited, medium, significant, sufficient.

By the same logic, Table 7 helps to convert the quantitative value of the final calculated Risk into a qualitative value in order to make it better understood by the user. Qualitative values also consist of five levels, from VL to VH.

TABLE 6 Description of the attacker profile levels.

Attacker profile measurements			
Qualitative	Range (%)	Quantitative (%)	Description
VH	85–100	93	Sophisticated, sufficient, sufficient
H	65–84	75	Expert, significant, significant
M	35–64	50	Skilled, medium, medium
L	15–34	25	Narrow, limited, limited
VL	0–14	7	Novice, minimum, minimum

TABLE 7 Description of the probability scale.

Probability scale values		
Qualitative	Range	Quantitative
VH	0.85–1.00	0.93
H	0.65–0.84	0.75
M	0.35–0.64	0.50
L	0.15–0.34	0.25
VL	0.00–0.14	0.07

Having explained these core components, an analysis of the CYSMET methodology's steps follows.

5.4. Methodology steps

In this section, the CYSMET methodology is described in detail in steps and sub-steps, as follows from what was mentioned above.

This enhanced Risk Management methodology is SMP-oriented and applies to any SCS, following the six main axes of risk analysis as outlined in Table 8.

The CYSMET methodology flows as shown in the following steps. Additionally, one of the aforementioned attack scenarios serves as an example to demonstrate how the CYSMET methodology is used in the transportation of fuel SCS (see SCS2 in Section 4.2). For the purposes of this use case, only the data mentioned in the respective scenario is used, without further detailed analysis or additional information. The aim is to better understand the flow of the methodology with an emphasis on calculations.

5.4.1. Step 0: Scope of SCS risk assessment

The assessor selects the SCS for which the risk assessment will be carried out, as well as its limits, i.e., the scope, the objective and the expected result. An SLA is created and signed by the SCS provider and all BPs.

Example: The risk assessment is going to be implemented on the maritime SCS of transportation of fuel and the unloading SMP. The assets concerned are those that directly participate in the operation of the SCS2.

TABLE 8 CYSMET methodology at a glance.

Main axes of risk analysis	CYSMET methodology
1. Perimeter/boundaries setting	Step 0: Scope of SCS risk assessment Step 1: Analysis of SCS *1.1 Scope and objectives of SCS* *1.2 Identification of SCS-BPs* *1.3 SCS modeling*
2. Threat analysis	Step 2: SCS threat analysis *2.1 Identification of cyber and/or physical individual threats linked to an SCS asset* *2.2 SCS threat assessment*
3. Vulnerability analysis	Step 3: SCS vulnerability and impact analysis *3.1 Determination of attacker profile* *3.2 Identification of confirmed individual vulnerabilities* *3.3 Identification of confirmed/zero-day vulnerabilities* *3.4 Creation of vulnerability chains in SCS* *3.5 Identification of attack methods and graphs* *3.6 Assessment of individual vulnerability severity level*
4. Impact analysis	
5. Risk assessment	Step 4: Risk assessment *4.1 Assessment of risk level of individual assets* *4.2 Vulnerability chain risk level assessment*
6. Risk mitigation strategy	Step 5: Risk mitigation—Selection of security controls

5.4.2. Step 1: Analysis of SCS

The SCS under consideration is selected and decomposed, as defined in step 0 by the assessor and the agreement of the BPs.

5.4.2.1. Step 1.1: Scope of SCS risk assessment

The assessor defines the under consideration SCS scope and provides its objective and expected outcome.

Example: The SCS2, to which the specific attack is applied, concerns the distribution of fuel to gas stations using tanker vehicles (described in Section 4.2).

5.4.2.2. Step 1.2: Identification of SCS-BPs

The assessor identifies the SCS-BPs, in agreement with them. Each of them declares all participants from their organization for the current risk assessment.

Example: See the SCS2-BPs in Table 3.

TABLE 9 Threat assessment of SCS2.

Threats	Threat scale values		
	Qualitative	Range (%)	Quantitative (%)
1. Disruption of surveillance systems	M	(40–60]	60
2. Violation of biometric systems	H	(60–80]	80

TABLE 10 Attacker profile level.

Attacker profile measurements			
Qualitative	Range (%)	Quantitative (%)	Description
H	65–84	75	Expert, significant, significant

5.4.2.3. Step 1.3: SCS modeling

The main objective is to identify and model the main processes involved in the SCS under consideration. In addition, the following actions shall be performed:

- Identify the SCS business processes: All cyber and/or physical processes are defined and recorded.
- BPs links: The already identified BPs are linked to the defined SCS business processes.
- Identify SCS assets: All assets required to provide the under consideration SCS and its corresponding business processes are identified and reported.
- *Example*: See the cyber and physical assets in Table 3.
- Asset interdependencies modeling: The specifications are recorded and the interconnections that exist between the entities and SCS assets are depicted. The assets recorded are only those that directly participate in the operation of the SCS.
- Enhanced Security Declaration (ESD): Identify and report the security controls applied to each asset identified in the previous steps.

5.4.3. Step 2: SCS threat analysis

All those threats related to the SCS under consideration are identified and evaluated for their probability of occurrence. This step consists of the following:

5.4.3.1. Step 2.1: Identification of cyber and/or physical individual threats linked to an SCS asset

In this sub-step, all physical individual threats and/or those that exist in cyberspace for a specific SCS asset will be identified using online repositories, social media, crowdsourcing, threat data recorded by BPs (intrusion incidents, detection system logs, reported exploits, firewall logs, malware reverse engineering, internal policies and procedures, system configuration information, etc.)

Example: See the cyber and physical threats of SCS2 in Table 3.

5.4.3.2. Step 2.2: SCS threat assessment

In this sub-step, the probability of occurrence of each threat is assessed for each SCS asset. A five-level scale is used (see Table 6).

Example: In Table 9 the threats of SCS2 are assessed to take a quantitative value, according to the threat scale values of Table 6.

5.4.4. Step 3: SCS vulnerability and impact analysis

The vulnerability analysis aims to identify, quantify and prioritize the vulnerabilities of the assets of the SCS under consideration and consists of the following steps:

5.4.4.1. Step 3.1: Determination of attacker profile

Based on Table 6, the assessor decides the level of the attacker profile, which is given a quantitative value to be used in step 4, in order to calculate the individual risk.

Example: In Table 10 the level of the attacker profile takes a quantitative value, according to the levels described in Table 6.

5.4.4.2. Step 3.2: Identification of confirmed individual vulnerabilities

Online and various DBs are searched to find confirmed vulnerabilities, which have not been addressed by BPs and are accompanied by specific characteristics and indicators that aid in subsequent analysis and inference.

Confirmed vulnerabilities that have not been addressed by BPs can be found through NVD, CVE Details, other online DBs, commercial or open-source vulnerability scanners (e.g., OpenVas[4]), or the list of applied security controls identified in the ESD of step 1.3.

Example: The vulnerabilities Vi that match a threat Ti from step 2.2 are the following.

V1 (T1): CVE-2022-44153[5]

CVSS 3.x severity and metrics:

- DB: NVD.
- Base Score: 6.1 MEDIUM.
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N.[6]

V2 (T2): CVE-2019-18618[7]

CVSS 3.x Severity and Metrics:

- DB: NVD.
- Base Score: 6.0 MEDIUM.
- Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N.[8]

4 https://openvas.org

5 https://nvd.nist.gov/vuln/detail/CVE-2022-44153

6 https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

7 https://nvd.nist.gov/vuln/detail/CVE-2019-18618

8 https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

5.4.4.3. Step 3.3: Identification of confirmed/zero-day vulnerabilities

The purpose of this sub-step is to investigate the possibility of additional vulnerabilities, particularly zero-day, that can be used against SCS assets before they are noticed by their suppliers, in order to gain a realistic picture of the risk they may be exposed to.

Estimation of these vulnerabilities can be done at all time scales in the available data, defined either empirically or by determining the number of publicly announced vulnerabilities for a specific time period. In addition, social media can be particularly useful to the assessor, providing information about possible unconfirmed vulnerabilities, as well as various tools such as Snort.[9]

Zero-day vulnerabilities are modeled in the same way as confirmed ones, and each SCS-BP is to provide the Base Score manually, based on their findings and experience. A common DB can be used for internal information sharing by the BPs.

Example: There are no confirmed/zero-day vulnerabilities in SCS2 assets.

5.4.4.4. Step 3.4: Creation of vulnerability chains in SCS

It is an analyst responsibility scoring a chain of vulnerabilities to determine which ones combined could form the chained score. Also, during vulnerability scoring, the analyst can define other types of related vulnerabilities that are often interconnected and can be linked to the vulnerabilities being scored. In order to score the vulnerability chain, the analyst should consider the Exploitability, Scope, and Impact metrics of each vulnerability included in the chain. It is recommended by CVSS v3.1 that less restrictive exploitability score metrics and the most impactful subscore metrics be taken.

Example:

The vulnerability chain for SCS2 created from the vulnerabilities found in steps 3.2 and 3.3 is:

V1 → V2

5.4.4.5. Step 3.5: Identification of attack methods and graphs

The attack vectors shall be identified, and the vulnerabilities information shall be analyzed in order to create the attack graphs (see Figure 1 in Section 3).

Example: See Figure 3 in Section 4.2.

5.4.4.6. Step 3.6: Assessment of individual vulnerability severity level

The vulnerability severity level (VSL) of each vulnerability found in the previous sub-steps is assessed, in order to consider whether it can be successfully exploited when all the required conditions are met.

In this sub-step the individual VSL (IVSL) is estimated, which measures the ability of an attacker to successfully approach and exploit a specific vulnerability (either confirmed or zero-day) taking into account the vulnerability's temporal characteristics and impact according to user's environment on a particular asset.

The environmental metric of CVSS v3.1 calculates the vulnerability severity of an asset vulnerability exploitation in the business (organizational) environment, which essentially includes the impact that the exploitation of an asset vulnerability can have on the entire SCS.

In order to calculate the IVSL, the CVSS v3.1 Base Score metrics retrieved from the online vulnerability DBs are used and then the Temporal and Environmental Scores metrics are parameterized by the security officer of the corresponding BP, resulting in a value from 1 to 10.

A vulnerability profile is created using the vulnerability inventory, according to the following CVSS v3.1 scores:

- Base score: default by CVE (derived from step 3.2) or manually put by each SCS-BP (derived from step 3.3).
- Temporal Score: all at "Not Defined" by default, unless another value has been agreed by the SCS-BPs that is more realistic.
- Environmental score:
  - Confidentiality Requirement (CR), Integrity Requirement (IR), Availability Requirement (AR), Modified Attack Complexity (MAC), Modified Confidentiality (MC), Modified Integrity (MI), Modified Availability (MA): manually put by each SCS-BP.
  - Modified Attack Vector (MAV): "Network" by default (since the environment is a SCS, modifications to the attack vector could only be possible over a network).
  - Modified Privileges Required (MPR), Modified User Interaction (MUI): "Not Defined" by default (they are going to be changed by the multiplication with AP later).
  - Modified Scope (MS): "Changed" by default.

Example:

CVSS v3.1 output of V1:

- Total score: 9.7 CRITICAL (9.7/10 = 97%)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/CR:H/IR:H/AR:H/MAV:N/MAC:L/MS:C/MC:H/MI:H/MA:H.[10]

CVSS v3.1 output of V2:

- Total Score: 8.3 HIGH (8.3/10 = 83%).
- Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N/CR:H/IR:H/AR:H/MAV:L/MAC:L/MS:C/MC:H/MI:H/MA:H.[11]

5.4.5. Step 4: Risk assessment

In this step the following risk assessments are carried out.

9 https://www.snort.org/

10 https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/CR:H/IR:H/AR:H/MAV:N/MAC:L/MS:C/MC:H/MI:H/MA:H

11 https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N/CR:H/IR:H/AR:H/MAV:L/MAC:L/MS:C/MC:H/MI:H/MA:H

5.4.5.1. Step 4.1: Assessment of risk level of individual assets

After collecting all threat values (step 2), IVSL (step 3) and Attacker Profile (step 3) for a specific vulnerability of an asset, the Individual Risk Level (IRL) value is calculated as follows:

$$\begin{aligned} &\textit{Individual Risk Level} \\ &= (\textit{Threat Level}^{*}\textit{Vulnerability Level}^{*}\textit{Impact Level}) \\ &^{*}\textit{Attacker Profile}, \textit{where Vulnerability Level}^{*}\textit{Impact Level} \\ &= \textit{IVSL} \end{aligned}$$

Example:
For vulnerability V1 (from step 3.2):

$$\begin{aligned} &\textit{Individual Risk Level} \\ &= (\textit{Threat Level}^{*}\textit{Vulnerability Level}^{*}\textit{Impact Level}) \\ &^{*}\textit{Attacker Profile} = 60\%^{*}97\%^{*}75\% = 0.6^{*}0.97^{*}0.75 \\ &= 0.4365 \end{aligned}$$

For vulnerability V2 (from step 3.2):

$$\begin{aligned} &\textit{Individual Risk Level} \\ &= (\textit{Threat Level}^{*}\textit{Vulnerability Level}^{*}\textit{Impact Level}) \\ &^{*}\textit{Attacker Profile} = 80\%^{*}83\%^{*}75\% = 0.8^{*}0.83^{*}0.75 \\ &= 0.498 \end{aligned}$$

5.4.5.2. Step 4.2: Vulnerability chain risk level assessment

The objective of this sub-step is to illustrate the risk that characterizes vulnerability chains in the SCS. It is calculated as follows:

$$\begin{aligned} &\textit{Risk}(\textit{Vulnerability Chain}) \\ &= \textit{Risk}(\textit{Node}1)^{*}\textit{Risk}(\textit{Node}2)^{*}\textit{Risk}(\textit{Node}3) \\ &^{*}\ldots^{*}\textit{Risk}(\textit{NodeN}) \end{aligned}$$

To better understand the effect of vulnerability chain risk, it can be transformed into a qualitative one, following five-level scale, as shown in the probability scale of Table 7.

Example:

$$\begin{aligned} &\textit{Risk}(\textit{Vulnerability Chain}) \\ &= \textit{Risk}(\textit{Node}1)^{*}\textit{Risk}(\textit{Node}2)^{*}\textit{Risk}(\textit{Node}3) \\ &^{*}\ldots^{*}\textit{Risk}(\textit{NodeN}) = 0.4365^{*}0.498 = 0.217377 \end{aligned}$$

After moderating probability of occurrence according to the Probability Scale (Table 7), the result is "L".

5.4.6. Step 5: Risk mitigation—Selection of security controls

The risk assessment values are compared to predetermined criteria, which are determined by all BPs. The BPs jointly along with the SCS provider decide what risks they are willing to accept and to what extent and/or carry out additional security controls, which meet the thresholds set by the assessor, the provider and the BPs as a whole and pre-agreed in their ESD. As CYSMET is an ISO/IEC 27002 compliant risk management methodology, they can use this standard, among others, for guidance.

Example: Physical security for facilities should be designed and applied.

6. Conclusions and future work

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

All ports are 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 and work under the same laws and regulations as major ports challenges their day-to-day safe and secure operation, due to the limitation of financial resources. Risk analysis is a process that usually requires deep knowledge of the infrastructure and factors that can affect the operation of an organization, so cybersecurity experts are needed to model and calculate risk.

For these reasons, CYSMET, an enhanced, user-friendly risk management methodology is presented, which correlates cyber and physical threats. Its aim is to help SMPs conduct risk assessments in SCSs without requiring a team of cybersecurity experts, or a large financial budget, but even performing a self-assessment and manage their own risks.

Our future research work leans toward creating a tool that can provide a highly automated holistic solution of the CYSMET risk management methodology; a key governance tool which will also aid in the selection and implementation of security controls.

Data availability statement

The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding authors.

Author contributions

The paper was primarily written by PK. All authors listed participated in discussions and in editing drafts of the sections, have

made substantial, direct, and intellectual contributions to the work and have approved it for publication.

Funding

This research has been co-financed by the European Regional Development Fund of the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship and Innovation, under the call RESEARCH – CREATE – INNOVATE (project code: T2EDK-03488).

Acknowledgments

The authors would like to thank all partners of CYSMET project as well as the University of Piraeus, Research Centre (UPRC) for its continuous support.

Conflict of interest

PK is employed by Maggioli SpA. NP is employed by trustilio B.V. and University of Piraeus. Both authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Agence nationale de la Sécurité des Systèmes D'information (ANSSI) (2019). *EBIOS Risk Manager – The Method*. Available online at: https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/ (accessed February 1, 2023).

Alghawazi, M., Alghazzawi, D., Alarifi, S. (2022). Detection of SQL injection attack using machine learning techniques: a systematic literature review. *J. Cybersecur. Privacy* 2, 764–777. doi: 10.3390/jcp2040039

CYRENE EU H2020 Project (2020–2023). *Glossary*. Available online at: https://www.cyrene.eu/glossary (accessed February 1, 2023).

European Sea Ports Organisation (ESPO) (2010). *European Port Governance Report of an Enquiry into the Current Governance of European Seaports. The ESPO Fact-Finding Report*. Available online at: https://www.espo.be/media/espopublications/espofactfindingreport2010.pdf (accessed February 1, 2023).

European Union Agency for Cybersecurity (ENISA) (2011). *Cyber Security Aspects in the Maritime Sector*. Available online at: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1 (accessed February 1, 2023).

European Union Agency for Cybersecurity (ENISA) (2019). *Port Cybersecurity – Good Practices for Cybersecurity in the Maritime Sector*. Available online at: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector (accessed February 1, 2023).

European Union Agency for Cybersecurity (ENISA) (2020). *Guidelines – Cyber Risk Management for Ports*. Available online at: https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports (accessed February 1, 2023).

European Union Agency for Cybersecurity (ENISA) (2022). *ENISA Threat Landscape 2022*. Available online at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (Accessed February 1, 2023).

Forum of Incident Response and Security Teams (FIRST) (2019). *Common Vulnerability Scoring System v3.1: User Guide*. Available online at: https://www.first.org/cvss/v3.1/user-guide (accessed February 1, 2023).

Haase, D., and Maier, A. (2021). *Research for REGI Committee – Islands of the European Union: State of Play and Future Challenges*. Brussels: European Parliament, Policy Department for Structural and Cohesion Policies. doi: 10.2861/138835

International Maritime Organization (IMO) (2004). *International Ship and Port Facility Security Code (ISPS Code)*. Available online at: https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx (accessed February 1, 2023).

International Maritime Organization (IMO) (2022). *International Maritime Dangerous Goods (IMDG) Code – Corrigenda*. Available online at: https://wwwcdn.imo.org/localresources/en/publications/Documents/Supplements/English/QM200E_180522.pdf (accessed February 1, 2023).

International Organization for Standardization (ISO) (2007). *ISO 28001:2007 Security Management Systems for the Supply Chain – Best Practices for Implementing Supply Chain Security, Assessments and Plans Requirements and Guidance*. Available online at: https://www.iso.org/standard/45654.html (accessed February 1, 2023).

International Organization for Standardization (ISO) (2012). *ISO/IEC 27032:2012 Information Technology – Security Techniques Guidelines for Cybersecurity*. Available online at: https://www.iso.org/standard/44375.html (accessed February 1, 2023).

International Organization for Standardization (ISO) (2018). *ISO/IEC 27005:2018 Information Technology – Security Techniques – Information Security Risk Management*. Available online at: https://www.iso.org/standard/75281.html (accessed February 1, 2023).

International Organization for Standardization (ISO) (2018–2022). *ISO/IEC 27001 and Related Standards - Information Security Management*. Available online at: https://www.iso.org/isoiec-27001-information-security.html (accessed February 1, 2023).

International Organization for Standardization (ISO) (2022). *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*. Available online at: https://www.iso.org/standard/82875.html (accessed February 1, 2023).

International Organization for Standardization (ISO) (2022). *ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Controls*. Available online at: https://www.iso.org/standard/75652.html (accessed February 1, 2023).

International Organization for Standardization (ISO) (2018). *ISO/IEC 27000:2018 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary*. Available online at: https://www.iso.org/standard/73906.html (accessed February 1, 2023).

INTERREG IV A 2 Mers Seas Zeeën (2014). A cluster initiative: Small and Medium Sized Ports as Hubs for Smart Growth and Sustainable Connectivity. *2 Seas Magazine*. Available online at: http://archive.interreg4a-2mers.eu/2seas-files/page_ext_attachments/1602/PAC2_2SEAS_MAGAZINE_EN.pdf (accessed February 1, 2023).

Katsikas, S. (2013). "Risk management," in *Computer and Information Security Handbook*, 2nd ed., ed. J. R. Vacca (Amsterdam: ELSEVIER Inc.), 905–927.

Kyranoudi, P., Kalogeraki, E., Michota, A., Polemi, N. (2021). "Cybersecurity certification requirements for supply chain services," in *IEEE Symposium on Computers and Communications (ISCC)* (Athens, Greece: IEEE), 1–7. doi: 10.1109/ISCC53001.2021.9631467

National Maritime Foundation (2022). Available online at: https://maritimeindia.org/cyber-operations-associated-with-the-ukraine-russia-conflict-an-open-source-assessment/ (accessed February 1, 2023).

Papastergiou, S., Polemi, N., Karantjias, A. (2015). "CYSM: an innovative physical/cyber security management system for ports," in *Human Aspects of Information Security, Privacy, and Trust. HAS 2015. Lecture Notes in Computer Science*, Vol. 9190, eds T. Tryfonas, and I. Askoxylakis (Cham: Springer), 219–230. doi: 10.1007/978-3-319-20376-8_20

Papastergiou, S., Polemi, N., and Kotzanikolaou, P. (2018). Design and validation of the Medusa supply chain risk assessment methodology and system. *Int. J. Crit. Infrastruct.* 14, 1. doi: 10.1504/ijcis.2018.090647

Schauer, S., Polemi, N., Mouratidis, H. (2019). MITIGATE: a dynamic supply chain cyber risk assessment methodology. *J. Transp. Secur.* 12, 1–35. doi: 10.1007/s12198-018-0195-z

The Institution of Engineering and Technology (IET), Department for Transport (2020). *Good Practice Guide – Cyber Security for Ports and Port Systems*. Available online at: https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice (accessed February 1, 2023).

The OWASP® Foundation (2023). *Threat Modeling*. Available online at: https://owasp.org/www-community/Threat_Modeling (accessed February 1, 2023).

U.S. Department of Transportation (1997). *Port Security: A National Planning Guide*. Available online at: https://rosap.ntl.bts.gov/view/dot/13693 (accessed February 1, 2023).