applied sciences

MDPI

Article

A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments

Eleni-Maria Kalogeraki [1,*], Spyridon Papastergiou [1], Haralambos Mouratidis [2] and Nineta Polemi [1]

[1] Department of Informatics, University of Piraeus, 80 Karaoli and Dimitriou Str., 18534 Piraeus, Greece; paps@unipi.gr (S.P.); dpolemi@gmail.com (N.P.)
[2] Centre for Secure, Intelligent and Usable Systems, University of Brighton, Brighton BN2 4GJ, UK; H.Mouratidis@brighton.ac.uk
* Correspondence: elmaklg1@gmail.com or elmaklg@unipi.gr

Received: 1 June 2018; Accepted: 24 August 2018; Published: 28 August 2018

Abstract: In recent years maritime logistics infrastructures are the global links among societies and economies. This challenges adversaries to intrude on the cyber-dependent ICTs by performing high-level intelligent techniques. A potential cyber-attack on such infrastructures can cause tremendous damages starting from supply chain service disruption ending up with threatening the whole human welfare. Current risk management policies embed significant limitations in terms of capturing the specific security requirements of ICTs and control/monitoring devices, such as IoT platforms, satellites and time installations, which are primary functioning for the provision of Maritime Logistics and Supply Chain (MLoSC) services. This work presents a novel risk assessment methodology capable of addressing the security particularities and specificities of the complex nature of SCADA infrastructures and Cyber-Physical Systems (CPSs) of the Maritime Logistics Industry. The methodology identifies asset vulnerabilities and threats to estimate the cyber-risks and their cascading effects within the supply chain, introducing a set of subsequent security assessment services. The utilization of these services is demonstrated via a critical, real-life SCADA scenario indicating how they can facilitate supply chain operators in comprehending the threat landscape of their infrastructures and guide them how to adopt optimal mitigation strategies to counter or eliminate their cyber-risks.

Keywords: maritime logistics services; SCADA infrastructures; cyber-physical systems; risk assessment; cyber-attacks; mitigation strategies; LNG transport

1. Introduction

In the modern era, Maritime Logistics and Supply Chains (MLoSCs) are the blood veins of global trade and economy where cross-border Critical Infrastructures (CI), such as ports, maritime authorities, airports, railways, energy providers, banks, maritime logistics and transport companies, collaborate in offering critical complex services, such as container management, vehicle transport, Liquefied Natural Gas (LNG) transport and cruising. The CIs that operate within their MLoSCs have physical and cyber multi-interdependencies, interacting with all sectors of the economy and therefore, their malfunctioning or disruption could have cascading effects on several other infrastructures or services depending on it throughout the global supply chain.

MLoSC services embed physical processes, such as vehicles and cargo stevedoring, ports Plant power supply procedures, pipeline management during LNG transport, which are monitored and controlled by composite and heterogeneous Industrial Control Systems (ICS) including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and

Programmable Logic Controllers (PLCs). Such installations play a vital role in the Maritime Industry as they analyze and display information aiming to promote a smooth and efficient performance of maritime logistics operations. SCADA systems, because of their high-level automation mechanisms and data interpretation capabilities, have managed to reduce waste of time and provide cost savings in logistics, maritime transport and control operations. In addition, they can gather environmental information, such as temperature, to protect both Port's plant and cargoes from physical disasters and potential industrial hazards [1].

Cargo ships are connected to ports and other MLoSCs operators via a plethora of communication and data links (e.g., through satellite network or conventional radio channel) and their navigation today is widely reliant on electronic solutions (e.g., satellite navigation with GPS, Galileo, Radar ARPA-Radio Direction and Ranging).

MLoSCs can be viewed as complex CPSs composed of heterogeneous, interconnected physical and cyber assets, owned by different national and foreign CIs, ensuring seamless and swift product/data exchange from the producer down to the end consumer.

MLoSCs' interconnected physical and cyber assets are highly valuable and thus lately they have become targets for attacks [2], attracting the attention of terrorism (e.g., Russian Business Network) [3], cyber-hacktivism organizations, militias (e.g., Anonymous, LulzSec) [3] and agencies (e.g., Stuxnet, Flame, Conficker, DuQu, APT1) [3]. In this context, the MLoSCs have garnered front-page attention as a victim of recent cyber-attacks: (i) A Chinese manufacturer stands accused of implanting malware in inventory scanners to steal supply chain intelligence [4]; (ii) hackers recently shut down a floating oil rig by tilting it [5]; (iii) engineering experiments have demonstrated that low-cost GPS jammers can be used to change a vessel's course by interfering with its navigation systems (GPS, ECDIS, AIS) causing a trackline-following autopilot to inaccurately interpret the ship's position and alter its course [3]; (iv) Somali pirates used hackers to gain access to shipping company's databases and vessel tracking systems to identify vessels with valuable cargoes, thus, many ships that transit the Gulf region are turning their Automatic Identification System (AIS) navigation tracking system off so that pirates cannot identify, locate and track them [3]; (v) in port of Antwerp, between 2011 and 2013, cyber-attacks were used to highjack, divert, or steal cargo [3]; (vi) a major maritime company, engaged in a deal to order a sea floor mining vessel, was the victim of a cyber-attack as it unknowingly pre-paid ($10 million of the $18 million charterer's guarantee) the deposit into a bank account that belonged to a cyber-criminal [6].

Attacks on the MLoSC may cause not only disruption of its services but also tremendous damage to the maritime operations and furthermore to the economies, societies, and environment, threatening the safety, security and stability within the EU and beyond. For example, an illegal intrusion on the ICS (e.g., supervisory control, SCADA installations) hosted in ports or maritime transport companies may lead to the disruption of loading/unloading services or harm critical mechanical devices (e.g., container cranes, safety and mechanical systems that operate locks and dams), or even worse, cause human casualties, loss of cargo and serious vessel damages. Another example is an attack on a container terminal management system causing malfunctions in the intermodal container services involving maritime, rail and truck transportation. Cyber-attacks (e.g., inserting a malware) in the ports' SCADA systems may generate fuel spills and affect water quality; attacks in the Port Community Systems (PCS) may turn LNG tankers into floating bombs; physical attacks (e.g., bombing) in a dry bulk storage area of coal products may create and carry dust by wind to tourist terminals or nearby residences.

Due to these threats, there is an urgent, pressing challenge for MLoSCs security officers and operators to protect their interconnected CIs', such as SCADA systems (i.e., telemetry systems, pipelines monitoring system, data collectors, lift stations and gantry crane crowbars) in the new digital maritime era. Existing risk management policies in EU Ports are using their own disparate methodologies which hurdles the comparison of risk assessment results among the Member States and greatens the appearance of cross-border multi-risks across the MLoSC [7]. In addition, the literature review [7,8] raises the challenge to update and combine security standards, such as NIST800-37 [9],

ISO27001 [10], ISO27005 [10] and ISO28001 [11]. Furthermore, there is a compelling need for more targeted Risk Assessment (RA) approaches dealing with the distributed and interconnected nature of the dynamic, ICT-based MLoSC environments.

The current study aims to present a novel evidence-based risk assessment methodology and illustrate the utilization of its generated sophisticated RA system, which has been developed under the EU H2020 Research Project "MITIGATE" [12]. The proposed methodology addresses the specificities and particularities of MLoSC cyber-assets, such as composite SCADA-based infrastructures and evaluates their evolving risk landscape by identifying assets interdependencies regarding the associated threats and cascading effects. To illustrate the level of disruption and damage that can cause a potential sophisticated cyber-attack to the MLoSC performance and underscore the necessity of protecting complex maritime logistics infrastructures, such as SCADA systems, we present three real-life SCADA cyber-attack scenarios on critical services of the MLoSC. Furthermore, to demonstrate how cybersecurity risks of SCADA installations pertaining the MLoSC can be captured, assessed and evaluated, we implement the MITIGATE effective, collaborative, standards-based security assessment services on a relevant SCADA supply chain scenario. To this purpose, all threats arising from the global supply chain will be considered, including those related to port CIs interdependencies and associated cascading effects.

Section 2 presents related works. In Section 3 security challenges on Industrial Control Systems (ICS) are addressed. Section 4 describes the MITIGATE evidence-driven risk assessment methodology and analyze its security assessment services. Section 5 presents SCADA real-life cyber-attack scenarios on maritime logistics critical services. Section 6 refers to the utilization of the MITIGATE system security assessment services on SCADA systems. Section 7 states the evaluation process and findings of the MITIGATE risk assessment methodology; it presents the limitations of existing RA methods, highlights corresponding MITIGATE advantages and reports the evaluation findings. Eventually, Section 8 integrates conclusion and discussion topics.

2. Risk Assessment Methodologies on Contemporary Maritime Logistics Infrastructures

A systemic review has been carried out to identify relevant existing literature on topics of supply chain security requirements engineering, risk management and supply chain security management standards of the Maritime Logistics Industry, to adumbrate cutting-edge issues and elicit important challenges.

Risk Assessment (RA) practices for CPSs have been developed over the past 40 years and they are still searching for methods to comprehend and facilitate the monitoring of risks [13]. The underlying principles of RA are captured in the National Academy of Science (Red Book) [14], where assessment and decision-making are distinguished [15].

With respect to SCADA systems, risk is assumed "a function of the likelihood of a given threat-source exploiting a potential vulnerability and the resulting impact of a successful exploitation of the vulnerability" (7). According to ISO/IEC 13335-1:2004 definitions [16], security goals are traditionally categorized into (i) Confidentiality (information is not made available or disclosed to unauthorized entities); (ii) Integrity (safeguarding the accuracy and completeness of assets) and (iii) Availability (being accessible and usable upon demand by an authorized entity).

RAs are generally categorized into qualitative, quantitative and hybrid methods, which are a combination of the first two. Remarkable examples of semi-quantitative RA approaches for maritime logistics assets are found in the literature, such as the Fault Tree Events Analysis which estimates the frequency of event occurrence in an undesired (top/root) logical scale [17]. The OBEST object-based event scenario tree illustrates combined features of event tree analysis and Monte-Carlo discrete event simulation along with concepts of object-oriented analysis for RA [18]. Schneier [19] introduced the attack trees as a method to formalize the security of systems and subsystems regarding varying attacks. A probabilistic-based RA Tool provides a foundation for the estimation of risk reduction when applied to SCADA security [20]. Augmented vulnerability trees and two new indices for quantifying

risks were introduced by Graham, Patel, and Ralston [17]. Cheminod et al. [21] have presented the Quantitative modeling SCADA vulnerabilities CRA. A scenario-based approach to risk analysis in support of cybersecurity has been introduced [22]. In 2009, a cyber-terrorism SCADA risk framework has been presented [23].

The Institute for Information Infrastructure Protection (I3P), founded by the Department of Homeland Security (DHS) is a research SCADA project for "Unifying Stakeholders and Security Programs to Address SCADA Vulnerability and Infrastructure Interdependencies" [24], which aims to raise the security awareness of process control systems.

The key-concepts and impact measurement in SCADA systems, including system (asset), vulnerability, threat impact (consequence) and security control-countermeasure have been identified [8,24–27]. Cherdantseva et al. [8] have highlighted considerable risk assessment approaches on SCADA systems ranging from 2004 to 2014, stemming from the following countries: USA, Korea, France, Canada, China, Australia, Serbia, Ireland, and Italy. Cardenas et al. [28] cover the scope broader than RA and also describe modules for attack detection and automated response to an attack. Ten et al. [29] is a considerable research work introducing the four components of the security framework for SCADA systems: Real-time monitoring, anomaly detection, impact analysis and mitigation strategies. Byres et al. [30] illustrate the use of attack trees for assessing vulnerabilities in SCADA systems and control hardware. Significant research is carried out on assessing the Byres attack trees, to estimate vulnerabilities in SCADA systems based on MODBUS and MODBUS/TCP communication protocols and reckon the features of the topmost attack event investigating possible ways to achieve the final goal of the attack [8]. The literature shows that machine learning, Artificial Intelligence (AI) and data mining technologies are thoroughly utilized in SCADA Intrusion Detection Systems (IDS) to identify threats. In general, a strong reason is their ability to treat a variety of historical data sets, which improves the IDS performance [31]. Indicative research works on such SCADA IDS recognizing malicious traffic can be found in [31–33].

Haimes and Horowitz [34] describe the eight-phase process risk filtering, ranking, and management method (RFRM) which builds on an adaptive two-player Hierarchical Holographic Modeling (HHM) method to identify risks. The approach updates on the advances in probabilistic RA that can be applied to estimate the risk (exposure or expected loss) from SCADA and DCS installations.

To delineate risk assessment processes, there are various attempts to structure ontologies for general risk assessments, such as the AURUM system [35]. The OCTAVE method [36] is a priori distribution referring to subjectively estimated probabilities according to the Bayesian approach using UML modeling language. The CORAS [37] method allows the integration of several different risk assessment processes the recognition of the probability of an attack is done a priori to any risk assessment and not automatically. The MEDUSA's research method [38] sets a number of concepts, algorithms, and tools evolved from research, specially designed to protect the IT infrastructure and associated systems.

Standards and norms range from general considerations and guidelines for risk management processes, such as ISO 31000:2009 [39], ISO 31010 [39], ONR 49000:2004 [40], to specific guidelines for the IT sector; ISO 20000 [41], ISO 27000 [10], ISO/IEC 27005:2013 [10], ISO 27001:2005 [10], ISO/IEC 27005:2011 [10], NIST2002 [42], NIST800-37 [9], NIST800-30 [43], BSI: IT-Grundschutz catalogues [44] and to highly specific frameworks, such as EC725/2004 [45], CISSP/ICS 2015 [46], IMO04 [47], ISO 20858 [48] of the maritime sector. Most of these standards specify framework conditions for the risk management process but rarely go into detail on specific methods to analyze and assess cyber-risks, making it difficult to delineate a direct comparison of results among several and varied risk assessment applications. However, the CISSP/ICS 2015 certification provides some directions for risk calculation. The EU Directive (2015/C261/03) [49], "Risk Management Capability Assessment Guidelines" sets RA impact clarifications for CIs of the Energy and Transport sectors, which impedes the assessment of all vital services provided by CIs.

Summarizing, the literature shows that effective cost-benefit analysis and evaluation of SCADA cyber-risks are based on a straightforward approach combining a set of parameters and features, such as the likelihood of security events, the consequences of the event itself and the exploitation level of vulnerability [50]. The current work will present how the Mitigate security assurance services implementation justifies this approach using rational decision-making techniques.

3. Security Challenges in Industrial Control Systems

ICSs in the Maritime Logistics Industry encompass SCADA, DCSs, and PLCs. They are found in the dockside container cranes, straddle-carriers and autonomous vehicles supporting stevedoring procedures and transporting containers in a commercial port with GPS and optical recognition port operations [51]. In addition, they are used in the bulk liquid and dry cargo handling systems that load and unload grain, crude oil, diesel, toxic chemicals and LNG. ICSs are also found aboard the support vessels such as pilot boats, tugboats, fireboats and oil spill response vessels, which ensure the safe movement of vessels and their cargo while entering and leaving a commercial port and monitor their safety while berthed at passenger and cargo terminals. Most ICSs began as proprietary, stand-alone systems that were separated from the rest of the world and isolated from most external threats.

However, more recent SCADA systems have moved to more interoperability and open standards for cost efficiency and integration into management IT systems. For example, communication is now common over Ethernet TCP-IP including more standardized control protocols and applications. Open standards for SCADA systems are sources for adversaries to gain knowledge regarding the SCADA network topology [52]. Hence, SCADA systems are subject to external attacks and IT-based vulnerabilities.

Contemporary SCADA technologies used in the maritime logistics sector depend on position and monitoring (e.g., IoT devices like cameras sending information to IT assets, navigation given by satellite terminals) and timing [51]. Maritime logistics, as other industries, faces cybersecurity issues due to the lack of management awareness, incomplete knowledge of attacks and SCADA asset vulnerabilities, focusing more on physical security measures neglecting to arrange cybersecurity drills to train SCADA operators [53,54]. Summarizing, there is a strong need to enhance the cyber-threat awareness of SCADA systems within the MLoSC [53,54].

As SCADA control systems become increasingly complex, distributed and interdependent with other sectors [51] the number of potential attack vectors also increases, including via the internet, enterprise network, and direct connections to the control networks and field devices. Some of the most common types of attack vectors against SCADA are Backdoors and holes in the network perimeter; Attacks on field devices; Database attacks; Communications hijacking and man-in-the-middle attacks; Cinderella attack on time provision and synchronization. The types of attacks on SCADA systems fall into five main categories [54]: (i) On the Communication stack attacks can occur for example on the network layer via a diagnostic server); (ii) on the UDP port attacks can occur on the transport layer, such as a SYN flood attack saturating resources by sending TCP connection requests faster than the machine can process them; (iii) at application layer intrusions can happen as a lack of security control to many of the SCADA protocols (e.g., DNS forgery and packet replay are common); (iv) on the hardware attacks may occur, for example, when adversaries manage to obtain unauthenticated remote access to devices and change data set points that may cause the devices to fail at low threshold or an alarm not to go off. Lack of authentication for administrative tasks on the hardware means that an attacker can reprogram the logic or values and affect the functional behavior of the device; (v) on the software a cyber-attack can occur because SCADA systems use a variety of software to provide functionality from traditional IT applications to bespoke embedded device applications and more accumulated memory fragmentation, which can lead to programs stalling. Structured Query Language (SQL) is widely used to store sensor information in historians and other databases, thus, if not designed properly at the application level the systems are susceptible to SQL injection attacks.

Given the complexity of the SCADA systems infrastructure and how composite the cybersecurity assessment is, this may be an expensive outlay to deal with [51]. Another focal point is that Information Systems and SCADA operating infrastructures are directly linked and cyber-dependent. Thus, modern RAs methodologies must take into account this linkage when evaluating SCADA cyber-risks [51] and mind the cross-sector dependencies [7], which facilitate the entry points to access the SCADA network. Industrial Internet of things, because of its extending internet connectivity, is a new big challenge, requiring advanced security measures to be undertaken to protect it from cyber-threats, in which the latest communication protocols should be considered.

Social media communication capability in the operation of SCADA technical systems, with phenomena such as alerts or spurious news on hazards, dangers, opportunities, such as false fire alarm, may distort the level of response in operational and emergency situations [5]. Consequently, a successful RA approach for SCADA CIs may have the characteristics listed below:

- A structured body of cybersecurity knowledge using Knowledge Management practices to organize the knowledge [13,55].
- Adoption of business modeling and simulation techniques to carry out different real-life cyber-attack scenarios and experiment with the results [7,55].
- Taking into account rational decision-making techniques for probabilistic RAs of complex cyber-attack scenarios.
- Identify common or cross-border scenarios throughout national and regional limits [7].
- Involvement of all CI operators, including entities of both public and private sector participating, in order to have a clear and detailed view of SCADA cyber-risks at the asset-individual level and to identify the overall cyberdependencies across SCADA Networks and hence detecting the impact at the system level [55].
- Be compliant with regulations and directives or international standards applying to the supply chain (e.g., IMO practices and ISO standards).
- Introduce collaborative practices to facilitate the sharing and transfer of risk-related information across supply chain operators.

Moreover, there is the need for new risk and resilience assessment approaches that may assess and demonstrate the ability to develop and implement effective RA strategies and ensure SCADA systems resilience against aftermath cyber-incidents. The MITIGATE security assurance services are capable of responding to these requirements. The current work aims to raise MLoSCs operators' awareness of ICS security and assist them in learning how to recognize and react to an ICS cybersecurity SCADA incident.

4. The MITIGATE Supply Chain Risk Assessment Methodology

MITIGATE is the product of a research project [12], co-funded by the European Commission under its biggest Research and Innovation program Horizon 2020. The acronym "MITIGATE" stands for multidimensional, integrated, risk assessment framework and dynamic, collaborative Risk Management tools for critical information infrastructures.

4.1. An Evidence-Driven Holistic Approach

The MITIGATE methodology is a dynamic, collaborative, standards-based risk management methodology for all maritime logistics actors of the global supply chain protecting CIs from cyber-criminal activities [56]. This RA approach deals with MLoSC infrastructures and can be respectively applied to SCADA systems to assess their cyber-risks. Its dynamic and collaborative notion derives from an evidence-driven Maritime Supply Chain Risk Assessment (MSCRA) holistic approach [56–58], which is implemented towards a step-by-step risk management methodology providing an holistic view of maritime logistics infrastructures and their supply chains, enabling cooperation and risk-handling transparency among supply chain stakeholders and

generating unique evidence about risk assessment and mitigation. This is achieved by an open simulation environment that allows the business partners to simulate risks and evaluate risk mitigation actions. To estimate the cascading and escalating effects of risks, threats and vulnerabilities of the ICT-based supply chains, the MITIGATE methodology uses specialized metrics and measurements. The identification and analysis of composite interdependencies between supply chain entities and their cyber-assets drive the process of assessing the propagation of incidents through multiple ICT networks. An application of game-theoretic algorithms yields the recognition of optimal mitigation actions, capturing a worst-case scenario damage for the defender, based on the game-theoretic risk management approach described in Reference [59], the mathematical module for uncertain payoffs described in Reference [60] and potential attack strategies presented in References [57,58,61]. In this context, the MITIGATE methodology focuses on the following objectives:

- To assess a given supply chain service at the asset individual level
- To promote a rigorous, rational approach that gathers, critically appraises and uses high-quality research information (produced either by well-defined simulation experiments or available online repositories and social media)
- To disclose new cyber-threats and thus enhance the risk assessment process
- To identify and measure all relevant cyber threats
- To evaluate the individual, cumulative and propagated vulnerabilities of IT infrastructures
- To estimate the existence of zero-day exploitable vulnerabilities
- To predict all possible attacks/threats paths
- To assess the possible impacts
- To derive and prioritize the corresponding risks and
- To formulate a proper mitigation strategy.

The methodology of design is compliant with a range of international standards (e.g., ISO27k and ISO28k families and ISPS code), capitalizing on them and other well-known and proven guidelines and good practices [15] and following standardized notations. Beyond the aforementioned standards and guidelines, the MITIGATE approach has taken into consideration, additionally, concepts coming from past projects and existing tools: The MEDUSA supply chain risk assessment methodology [38], Secure Tropos (e.g., the security modeling) [62] and AECID (e.g., informational interdependency types) [63].

4.2. A Novel Integrated Risk Management System and Services

Despite the importance of CIs and dynamic ICT-based assets for port operations, according to the literature, risk management methodologies for maritime logistics environments pay limited attention to the cyber-security nature of their infrastructures and do not adequately address the security requirements of the business processes associated with global supply chains. Motivated by these limitations, MITIGATE introduces, integrates, validates and commercializes a novel Risk Management (RM) system [64], which empowers stakeholders' collaboration for the identification, assessment and mitigation of risks associated with cybersecurity assets and supply chain processes. The MITIGATE RA approach can be utilized on SCADA infrastructures to assess their cyber-risks. This is demonstrated via an indicative example presented in Section 6. The MITIGATE system achieves its objectives through a bouquet of subsequent security assessment services, which integrate a number of activities ranging from asset identification, impact and threat analysis to the specification of the existing controls and the disclosure, evaluation and treatment of the inherent and interdependent risks. Thereby, the MITIGATE system supports the following flexible and configurable self-driven security assessment services:

- Security Assessment Service 1 (SAS-1): Supply Chain Service Modeling
- Security Assessment Service 2 (SAS-2): Vulnerabilities Management and Open Intelligence
- Security Assessment Service 3 (SAS-3): Threats/Controls Management and Open Intelligence

- Security Assessment Service 4 (SAS-4): Threat Scenarios Specification
- Security Assessment Service 5 (SAS-5): Supply Chain Risk Analysis
- Security Assessment Service 6 (SAS-6): Attack Paths Simulation
- Security Assessment Service 7 (SAS-7): Supply Chain Risk Management
- Security Assessment Service 8 (SAS-8): Social Engineering and Open Intelligence

4.2.1. Supply Chain Service Modelling (SAS-1)

The MITIGATE methodology addresses the cybersecurity requirements of the business processes encompassing the MLoSC performance through the modeling of the MLoSC services. This is achieved by adopting knowledge management practices, which analyze in-depth inter-organizational and cross-organizational key-concepts of MLoSC critical services: Key-management processes, participating business partners and operating CPSs. The aforementioned approach implements a combined technique of process-centric and asset-centric views analyzed in Reference [55]. The process-centric view, depicted in Figure 1, defines the business processes and business partners' participation and collaboration in the provision of the supply chain service whereas the cyber-asset view, shown in Figure 2, identifies the cyber-assets operation and their interrelation within the supply chain service.

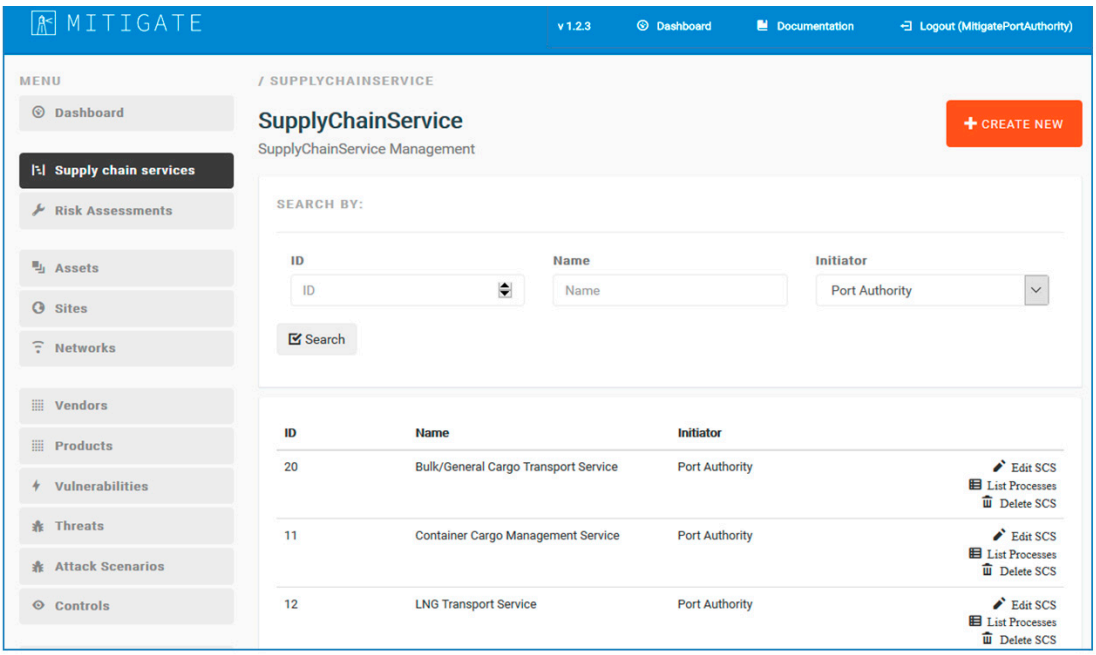

Figure 1. The Supply Chain Service Modelling (SAS-1) of the MITIGATE system enables business partners to create supply chain services and declare the corresponding processes and the list of business partners participating.

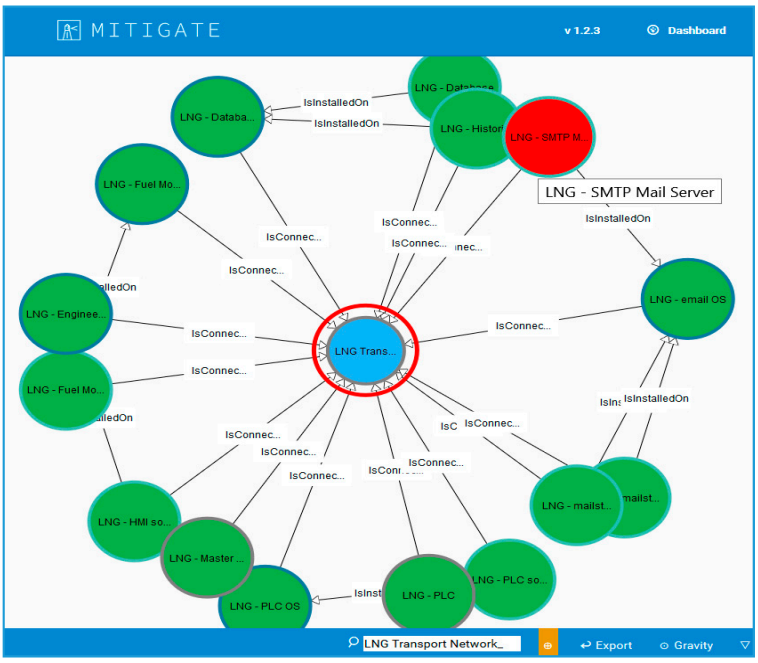

Figure 2. Visualization of Cyber-asset graphs using the Supply Chain Service Modeling (SAS-1) of the MITIGATE system.

Consequently, this security assessment service delivers a cyber-asset inventory including all computing (desktops, notebooks, servers) and networking related devices (switches, routers, etc.), printers, appliances (network attached storage, network capable cameras, etc.), applications and IT systems in general owned, managed, or otherwise used by the maritime logistics operators. Such devices are vessel traffic monitoring systems, intermodal maritime-based logistics, SCADA components, such as Human Machine Interface (HMI), Master Terminal Unit (MTU), Programming Logic Controllers (PLCs), Supervisory stations, Remote Terminal Units (RTUs), sensor systems for controlling stevedoring equipment, such as gantry cranes, trailers and forklifts [54].

The modeling of supply chain services elicits information about the main cyberdependencies that exist among assets. A cyberdependency of assets is considered a pair cyber-asset (node) interrelation and/or interconnection (edge) aiming to fulfil an electronic service/operation across communication networks [55,59]. The MITIGATE methodology assumes a twofold dependency concept: (i) The dependency type and (ii) the dependency access vector. The dependency type identifies the manner in which a cyber-asset pair is interdependent in a supply chain service: 1. Hosting; 2. Exchange data/information; 3. Storing; 4. Controlling; 5. Processing; 6. Accessing; 7. Installing; 8. Trusted; 9. Connecting. The cyber-asset pair consists of a source cyber-asset and a destination cyber-asset. The dependency access vector defines the location the two cyber-assets are able to interact through a communication network within the supply chain: Adjacent Network (A), Local (L), Network (N) [34,55,56]. This allows the MLoSC operators to understand how these assets are used and cooperate. Additionally, the MITIGATE service provides a visualization of the entire infrastructure, which expands the cyber-assets knowledge and improves the data sharing of the spectrum [55].

4.2.2. Vulnerabilities Management and Open Intelligence (SAS-2)

Organizations involved in the MLoSC should be aware of the vulnerabilities associated with the cyber-assets of their IT infrastructures. This service acts as a central repository for all known and unknown/undisclosed vulnerabilities. It makes use of open data sources, such as the CVE Details portal [65] where these vulnerabilities have been disclosed, replicating all the confirmed and known

vulnerabilities and associating them with the affected assets via synchronization and knowledge management mechanisms. Unknown/undisclosed vulnerabilities can be, additionally, declared and treated by business partners. To quantify vulnerabilities, a set of metrics is taken into account as listed below [65]:

- The access vector showing how vulnerability can be exploited.
- The attack complexity illustrating how easy or difficult is to exploit the discovered vulnerability.
- The authentication describing the number of times that an attacker must authenticate to a target to exploit it.
- The confidentiality outlining the impact on the confidentiality of data processed by the asset.
- The availability describing the impact on the availability of the target asset.
- The integrity describes the impact on the integrity of the exploited asset.

4.2.3. Threats/Controls Management and Open Intelligence (SAS-3)

The digital era presses supply chain operators and organizations involved in the MLoSC to be highly knowledgeable about the threat landscape their IT infrastructure is exposed to. Hence, they should be armed with the appropriate tools and solutions that could help them familiarize themselves with the threats that may affect their organizations and the security controls that can be either deployed or applied in order to mitigate the risks and confront the defined threats and weaknesses. In this context, the MITIGATE system acts as a knowledge base of identified threats indicating corresponding mitigation controls that can be used to counter such cybersecurity issues.

This service adopts the CAPEC classification of MITRE [66], which synchronizes the MITRE attack identifiers and associates the identified vulnerabilities with one or more weakness identifiers. Custom threats can be declared by supply chain business partners. Furthermore, the service supports the creation and customization of security controls, which are categorized into two types: "Mitigates Threats" and "Mitigates Vulnerabilities".

4.2.4. Threat Scenarios Specification (SAS-4)

The interconnectivity and heterogeneity of ICT systems foster the frequent emergence of new, complex threats and vulnerabilities. As cybercriminals continue to do the unexpected by discovering new ways to break into ICT processes and SCADA operations, the nature of cyber-attacks within the MLoSC is becoming even more targeted, sophisticated and ingenious. Against this background, the MITIGATE system serves threat scenario specification to help MLoSC operators realize the consequences deriving from the identified threats and vulnerabilities on their cyber-assets. Threat scenario is assumed a use-case in which a threat can compromise an asset by exploiting vulnerabilities and weaknesses as well as taking advantage of the lack of adequate security controls. The MITIGATE service provides the capability to declare statically the mapping of threats and vulnerabilities with assets to increase the cybersecurity awareness of MLoSC operators. Figure 3 illustrates the threat scenarios declaration in the MITIGATE system.

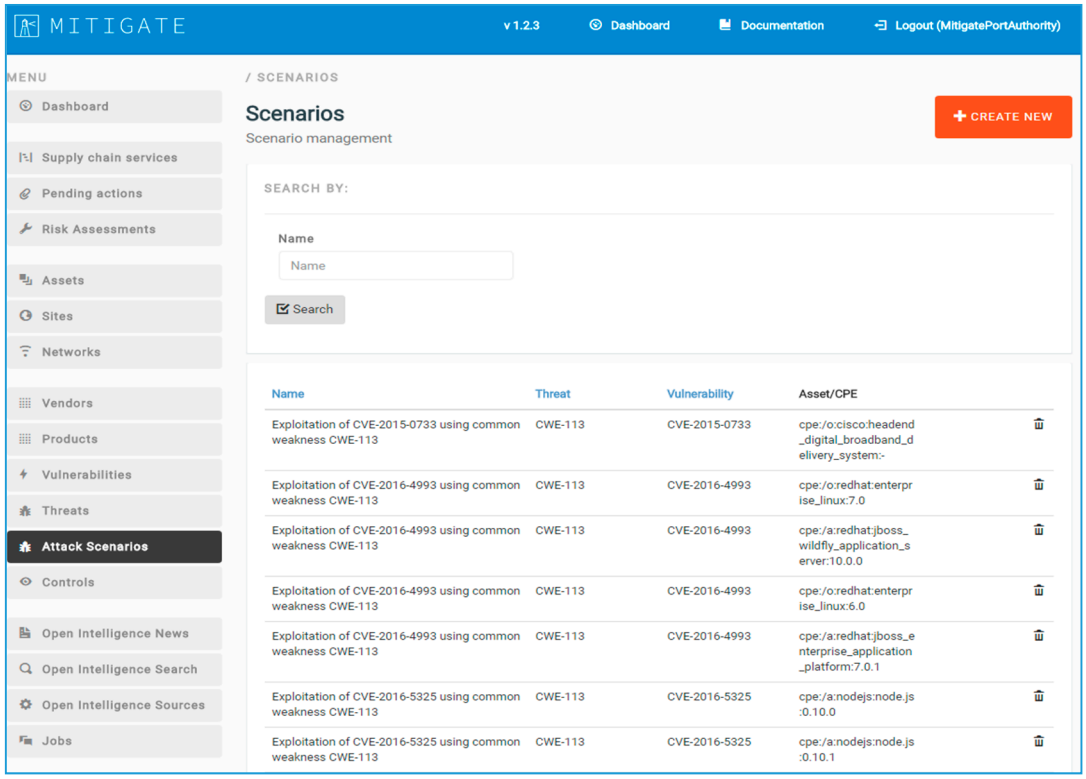

Figure 3. Threat scenarios specification illustrates the mapping between assets, vulnerabilities and threats as a result of the corresponding MITIGATE system services.

4.2.5. Supply Chain Risk Analysis (SAS-5)

This MITIGATE service provides guidance to the MLoSC operators to assess and organize the cybersecurity issues associated with the supply chain services in which they are involved. Moreover, the MITIGATE system encompasses and executes an evaluation process that implements the main steps of the proposed MSCRA approach [56–58,61]. Furthermore, MLoSC operators, such as Port employees, SCADA operators, forwarders, Port Authorities, shipping and carrier agencies, can use this service to identify and measure all relevant cyber threats, vulnerabilities, assess the possible impacts and derive and prioritize the corresponding risks. In particular, the MITIGATE MSCRA approach estimates the cyber-assets' risk exposure concerning the following three main types of risks: (i) The individual risk, which represents how dangerous a threat is to a specific cyber-asset within a supply chain service; (ii) the cumulative risk, which estimates the risk exposure of the successful exploitation of multiple vulnerabilities, in order to reach a specific cyber-asset within the supply chain service starting from different entry points and (iii) the propagated risk, which shows how deep into the supply chain service an attacker may penetrate in case he successfully exploits vulnerabilities found in asset entry points dealing with threats.

Risk Assessment is initiated on the cyber-assets declared on the supply chain processes pertaining to the MLoSC services, identified during the execution of the supply chain service modeling. MLoSC operators are able to assess the risks on their cyber-assets operating in supply chain processes, which are either directly defined from them or realized by other business partners in which they have been invited and accepted to participate via the MITIGATE system collaborative environment.

The Supply Chain Risk Analysis service supports two types of risk assessment: "Real" and "Simulation". The key difference is that simulation allows MLoSC operators to further customize their cyber-assets by changing the security information on them; disregard certain vulnerabilities and threats, amend the threat probability indicators and add more or replace security controls while the "Real" risk assessment type does not permit such alterations. Furthermore, the simulation mode offers

a virtual playground where asset cartography has been cloned and thus it permits to run dynamically different mitigation strategies without affecting the status of the real asset inventory.

The security assessment service delivers a detailed summary of the calculated risks at asset individual level, as presented in Figure 4. Cyber-assets operating in the selected supply chain process are presented in a lexicographical order. For each asset, the operator can see the individual risk level, defined previously, which is calculated per vulnerability along with the associated threat category. Moreover, the mapping of attacker's capability with respect to the asset-vulnerability combination provides the likelihood that an attacker may be able to exploit a specific vulnerability. This estimation relies on a qualitative nature of a five-tier nominal scale, which is thoroughly analyzed in References [56–58]: (i) "Very High" (VH) risk is expected to occur within the assets of the business partner with very high probability and an incident has been realized more than once in the last year (12 month period); (ii) "High" (H) risk is expected to occur within the assets of the business partner with high probability and an incident has been realized once in the last 1 year (12 month period); (iii) "Moderate" (M) risk is expected to occur within the assets of the business partner with moderate probability, where more than one incident has been realized over the last 2 years; (iv) "Low" (L) risk is expected to occur within the assets of the business partner with low probability, where at most one incident has been realized over the last 2 years; (v) "Very Low" (VL) risk is expected to occur within the assets of the business partner with very low probability, where at most one incident or no incident has been realized over the last 3 years.

Figure 4. Results from the Supply Chain Risk Analysis service (SAS-5) of the MITIGATE system.

To classify the asset's risk, the worst-case scenario of the vulnerability risks per asset is used to introduce the "Dominant Individual Risk Level", which is additionally visualized by a Risk Analysis Diagram.

Besides, the operator can see for each asset the threat's dominant risk level, which is the maximum risk of all vulnerabilities under a particular threat. The "Threat Analysis" diagram illustrates a count of different threats that contribute to the asset's risk level classification.

4.2.6. Attack Paths Simulation (SAS-6)

MLoSC interdependent assets can be increasingly affected by multi-stage targeted cyber-attacks (such as Stuxnet, Duqu, and Flame) using this cross-organizational dependency as a stepping stone to reach the actual target. MITIGATE implements an attack-path discovery method [57,58,61] that relies on unique characteristics, such as the attacker's location, the attacker's capability, assets interdependencies and which the entry and target points are in order to return all attack paths that exist in the

examined supply chains. The service supports the calculation and rendering of all the relevant attack graphs representing the different paths a cyber-attacker can follow to reach and harm a target asset. The operator can see all the potentially affected assets and their individual relationships.

This attack path generation and visualization (Figure 5) is carried out by the execution of rule-based reasoning mechanisms that develop all alternative chains of sequential vulnerabilities on the examined cyber-assets following an attack-path discovery method. It is a logic rule-based reasoning approach, which basically consists of the attacker profile, the attacker location and each association rules that are executed to build the attack graph and generate the paths. In addition, it relies on two components; (i) the knowledge base component and (ii) the path construction component. A further description of the approach is presented in References [57,58,61].

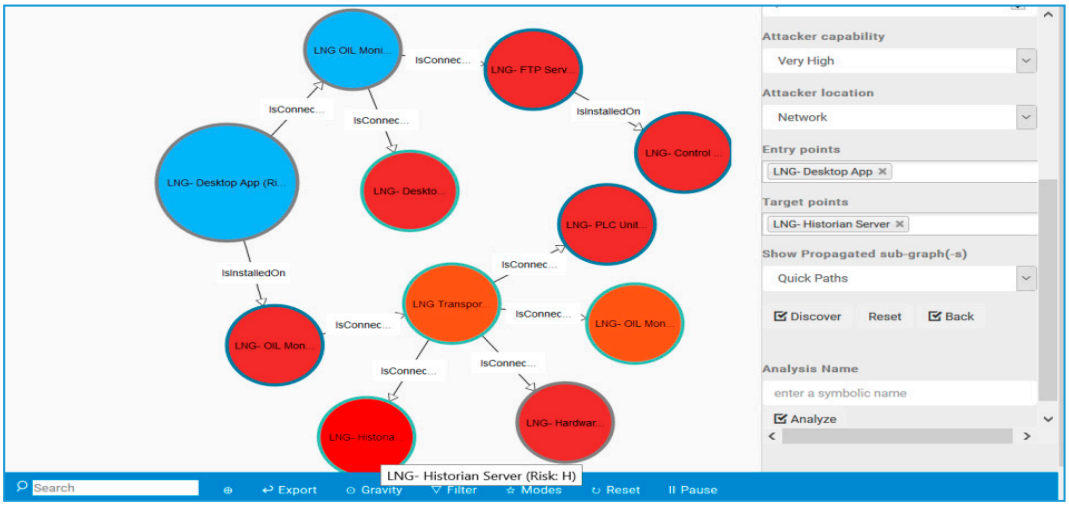

Figure 5. Attack-path simulation service (SAS-6) implementation over the MITIGATE system.

4.2.7. Supply Chain Risk Management (SAS-7)

The vulnerabilities trees, produced during the Attack Path Simulation Service, expose the risks embedded in the individual cyber-assets and in the entire supply chain. Thereupon, the MLoSC business partners require guidelines recommending the selection of the most appropriate security controls and indicating optimization practices, to minimize the expected damage. In this vein, the MITIGATE assures an acceptable risk level for the collaborative business partners and the overall MLoSC. In particular, the proposed system provides the necessary defensive capabilities and supports a rational decision-making to determine which security controls must be implemented and which partners need to implement them to encounter the identified security issues and cyber-risks. Since all defence strategies and the corresponding payoffs have been determined, the game-theoretic algorithm implementation, which is analytically presented in References [59,60], delivers an optimal way of selecting actions both of the attacker and defender. This equilibrium has a twofold notion: (i) To protect the assets by adopting the proper proposed security measures that eliminate the damage; (ii) to identify the highest damage an adversary may cause to the business partner and indicate the defense strategy that deviates the attacker from this optimal solution providing the minimum business partner's loss. To this end, the worst case scenario of damage within the supply chain service is described. Summarizing, MITIGATE recommends to maritime logistics organizations the performance of the following activities, in order to manage the MLoSC's cyber-risks:

- Review the risk assessment results and focus on assets with high individual risk; highlight the responsible vulnerabilities and the applicable security controls.
- Run attack path analysis scenarios setting (i) high-risk assets as entry points (e.g., GIS web services, malware SCADA supervisory workstations, etc.) (ii) cyberdependencies as targets.

Then, explore the paths and the vulnerabilities that contribute more to the cumulative risk on the cyberdependencies. Mitigating these will limit the potential impact imposed on the collaborating business partners. In addition, attack path analysis can be carried out setting cyberdependencies as entry points and study the propagated sub-graph.

- Mitigation Strategy Selection. Select the security controls of choice and build different defensive strategies. The game theoretic module will evaluate them and return the optimal results.

4.2.8. Social Engineering and Open Intelligence (SAS-8)

World Wide Web is full of cybersecurity-related content. Social media like Twitter and Reddit, as well as security blogs, RSS feeds and general-purpose websites, contain invaluable information about disclosed vulnerabilities, cyber-threats, exploitation methods and security controls. The Open Intelligence service captures information from various sources and repositories, analyzes and correlates their content with cybersecurity concepts and stores the results for further browsing and processing.

This Social Engineering and Open Intelligence procedures can be managed by adding, editing or deleting sources, specifying the media source and search-keyword. The MITIGATE system consults the inherent list in further data gathering job executions and provides an enhanced result set. A remarkable example of the open intelligence service is shown in Figure 6.

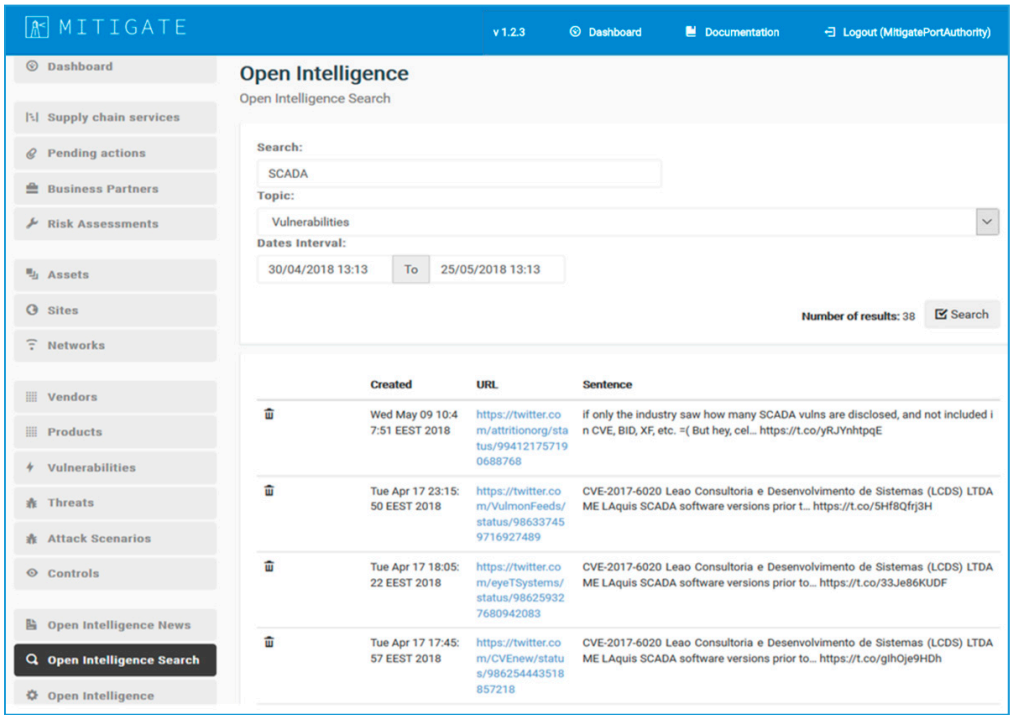

Figure 6. The Open Intelligence Mitigate Service (SAS-8) depicts current vulnerability statements for SCADA infrastructures.

Hence, the service provides the "Open Intelligence News", where MLoSC operators can view cybersecurity news relevant to their assets. The Assets' CPE identifier is used in particular to define the relevance of a new entry with the business partner's asset inventory. Further, searching is allowed via the available filters (time-range, free-text) and the "Search" button. "Open Intelligence Search" allows operators to explore content without applying the asset inventory relevance filter described previously.

5. Attack Scenarios on Real-life Maritime Logistics and Supply Chain Services

This section aims to illustrate how the performance of MLoSCs can be threatened and disrupted by cybercriminals. It stresses the need for providing security assessment methods that can increase the cybersecurity awareness of MLoSC operators' for supply chain's SCADA Infrastructures and can advise them how to protect their assets against potential cyber-attacks or eliminate the security damage in case an attack occurs. This is presented by exploring cyber-attack scenarios that have been either reported or known or assumed or suspected against real-life MLoSC services: The Container Cargo Management, the Vehicle Transport and the Liquefied Natural Gas (LNG) Transport.

The selected services have been identified as critical to the Maritime Logistics Industry due to security and economic reasons. The criteria for selecting these Critical Services satisfy the hereunder prerequisites:

- European level nature: Implemented on large, European commercial ports.
- Economic enablers: Address high economic impact across the EU Maritime Logistics Industry and the whole European economy.
- Environmental value: Meet the EU environmental requirements and standards.

The selected MLoSC Services can be subject to a number of possible threat scenarios that can be realized by conducting a combination/series of specific cyber-attacks in various MLoSCs' SCADA CPSs. Hence, malicious users/adversaries are able to realize complex threat scenarios for the purpose of disrupting MLoSCs' operations or facilitating illegal activities aimed at obtaining financial, political/military or even ideological gain and benefits. For example, adversaries may manage to smuggle illegal material of any kind (e.g., drugs, weapons) or illegal immigrants, or destroy a CI of the MLoSC by interrupting and modifying its services, gaining access to it either locally or remotely to take advantage of the system's security-sensitive operations. To this end, three credible cyber-attack scenarios against the aforementioned critical MLoSC services are described sequentially.

5.1. Cyber-Attack on SCADA Systems of the Container Cargo Management Service

According to Eurostat 184/2016 statistics, the containerized freight represents almost the third part of total trade exchanges measured in monetary value. On the other hand, the percentage of maritime transport in relation to total transported is even higher when kilometres or tonne-kilometres are measured. Consequently, these references are pointing out the important role of container terminals in the international carriage of goods. Containers-uniform boxes that can be easily moved between a lorry, a train and a ship have reshaped global trade over the past few decades.

A terrorist group wants to carry out a terrorist attack at a port in order to inflict wide-scale death and destruction by placing a bomb in a container, shipping it to the target port and detonating it before it could be inspected. The terrorist group is aware that a name-brand company ships containers of products and other cargoes to this port. The containers on any given ship are packed at the factories of the company; the container doors are shut and a mechanical seal is put into the door pad-eyes. A transportation company has undertaken the responsibility to pick up the container and transfer it to a container vessel. However, the containers are not delivered directly from the name-brand company's premises to the port terminal; rather, they go through a third party, a container packing warehouse.

The terrorists are aware of that the deliveries are managed through an IT system at the container packing warehouse; thus they cooperated with skilled hackers who can infiltrate the IT environment of the third party and gain access to the container management system. The terrorists change the information of the shipping container in order to replace it with another one carrying a bomb, which has been already placed by the terrorist group in the container packing warehouse.

Alternatively, the hackers could target any RFID tags and sensors attached to the container to monitor the goods. Such RFID kits are usually used to monitor various: (i) safety-oriented features such as whether the container door is opened or closed, the temperature inside the container, etc. or (ii) national security concerns like the illegal transportation of radioactive material and/or chemicals

used in bomb construction. Each container's RFID tag transmits its ID number and sensor data to an RFID reader, which then forwards that information (e.g., via a GSM base station) to an onboard control system and finally to the system administrator. The hackers could remotely exploit these RFID tags and sensors by injecting their own malware so that they transmit falsified information for the cargo of the targeted container. Even worse, they can manipulate the tags of other legitimate containers to make them look as if they hold suspicious cargo instead of the actual malevolent container.

At the target port, the security authorities inspect containers that the screening identifies as suspicious, based on ports of call, manifest data, shipping company, etc. In order for the terrorists to circumvent the authorities and bypass the inspection process, they compromise the IT infrastructure of the port and gain access to the container shipping system that keeps the routing or scheduling of the containers. Hence, they can change the container's details in the system and place the container in the desired location so that the detonation of the bomb could cause the maximum number of injuries and deaths.

5.2. Cybercriminals Attack OBUs during Vehicle Transport

The Vehicle Transport is a relatively long and complex service supported by numerous players, such as shippers and port authorities, involving the shipment and receipt of various types of vehicles and equipment, such as container terminals, trucks, gantry cranes and providers of Dockers. The service involves domestic and international transportation, such as warehouse management, order and inventory control, materials handling, import/export facilitation, and information technology. In this vein, the Vehicle Transport affects multiple sectors across the global supply chain.

A criminal gang aims to steal vehicles from the vehicle terminal of a port. To achieve this, hired hackers engage malicious activities spanning from simple phishing attacks, targeting port authorities and key employees, to the exploitation of more sophisticated, remote malware targeting the onboard communication interfaces and units of the pointed vehicles.

By launching a series of cyber-attacks, the adversaries manage to compromise few computers and critical elements based on software-related vulnerabilities and dynamic memory errors criteria. Thus, they manage to get access to the vehicle's vast network of interconnected On-Board Units (OBUs) and eventually spoof their geolocation. Examining the in-port vehicle scheduling processes followed, the criminals can then change the route and the location of the vehicles, to their preferred points of interest, without the port system administrator detecting any of these changes. In addition, the hackers could exploit vulnerabilities in the surveillance system of the port that controls the CCTV video cameras in order to gain access and delete video streams that show their malicious activities. Such a synergy of various attack paths against the CPSs reflects the investigation that will be performed following the MITIGATE methodology to exam the different types of vulnerabilities that may lead to the proposition of appropriate mitigation strategies.

5.3. Intrusion Scenario on the Oil Monitoring System of the LNG Transport Service

Liquefied natural gas (LNG) is natural gas, predominantly methane, CH4 that has been converted to liquid form for ease of storage or transport. It is odorless, colorless, non-toxic and non-corrosive. Hazards include flammability after vaporization into a gaseous state, freezing and asphyxia. Considering that a tanker contains more than one hundred thousand cubic meters of LNG, it represents a potential explosive hazard comparable to a nuclear bomb.

A terrorist group seeks to cause significant human casualties, economic losses and environmental damages by attacking the LNG land-based facilities of a port or an LNG tanker. For example, a possible cyber-attack to LNG land-based infrastructure may cause catastrophic fires either inside the port or even nearby populated areas and an LNG tanker attack may result in a major spill that could pose a hazard to coastal communities along the tanker's route. Furthermore, a physical attack on the LNG storage facilities, either in the form of bombing or by impacting a vehicle in the facility, may cause an explosion that leads to a widespread fire jeopardizing people's lives within the port.

Therefore, we assume that a terrorist group commits a cyber-attack during LNG shipping as follows. A shipping company receives an e-mail purportedly coming from the IT company that supports and maintains its ICT infrastructure asking them to download and install a software that improves the performance of their systems. In this way, the terrorists successfully download and execute arbitrary code on the victims' systems to gain access to them.

Accordingly, the terrorists can leverage their access to go deep into the network by exploiting vulnerabilities in the oil company's monitoring software that provides remote tank monitoring, asset tracking, and data reporting services to break into the system. Therefore, they can empty the oil tank without being detected.

6. How to Utilize the MITIGATE Security Assessment Services

The security assessment services of the MITIGATE system can be utilized to support SCADA CPSs of MLoSC services and protect them against malicious activities, such as those described previously. Hereunder, is presented how MLoSC business partners can utilize the MITIGATE services to estimate cyber-risks on maritime logistics SCADA infrastructures and discover mitigation strategies to encounter cybersecurity issues. This is illustrated by applying the MITIGATE security assessment services in an indicative scenario of SCADA cyber-assets considered to operate within the critical service of the LNG Transport, mentioned previously. The demonstration is given in a sequential report, aiming to provide a thorough and comprehensive perspective of the MITIGATE utilities towards a supply chain service. According to the scenario, a number of business partners, such as a Local Agent of a maritime logistics company, a Greek Port Authority, a Spanish Port Authority and a Gas Shipping Company, collaborate for the provision of the LNG Transport Service and they are highly dependent on the combined use of the port's physical (i.e., facilities, buildings, cranes, pipelines, rail track, roads, data centers) and cyber infrastructure (i.e., networks, ICT hardware equipment, communication systems, access control/authentication of users and containers). These four MLoSC business partners have signed a Security Declaration Statement, which is a documented commitment of each partner to exchange any security-related information and data concerning the LNG Transport Service and report any security risks or information related to the provision of this service. This information includes the security measures implemented on their infrastructures, how CPSs of LNG Transport are safeguarded and how their accompanying information is protected. The security measures are demonstrated and verified.

In particular, the business partners use the security assessment services of the MITIGATE system to assess their SCADA components, identify individual cyber-risks and evaluate the corresponding propagated and cascading effects with respect to the entire LNG Transport Service. The goal is to have a holistic treatment of threats, offering an enhanced understanding of the cyber interfaces for unidentified vulnerabilities, providing decision-making with an improved assessment of the integrated risks containing the propagating and cascading effects of the entire supply chain.

6.1. Utilization of SAS-1: LNG Transport Service Modeling

All partners, representing their business entities, use the MITIGATE system to model their interconnected SCADA cyber-assets, operating in the processes supporting the LNG Transport Service, such as the LNG Monitoring Service process. The LNG Monitoring Service process refers to the LNG handling functions of the LNG port terminal and the LNG carrier vessel operating during the LNG Transport (i.e., pipeline monitoring and fuel monitoring) The MITIGATE system's invitation/acceptance functionality facilitates collaboration among business partners to declare their assets as participating in each specific process (i.e., Figure 7 shows that regarding the LNG Transport Service, Port Authority has invited the Local Agent to participate and the latter has accepted the invitation). This refined CI representation of the various cyber-assets and their interconnections is fundamental towards measuring and assessing their threats and vulnerabilities and the investigation of scenarios with combined cyber-attacks. The current example presents indicative SCADA components

of the LNG Transport Monitoring Service process: (i) FUEL monitoring service assets (i.e., software installed on an operating system) that deliver fuel consumption information for the LNG carrier vessel; (ii) PLCs that handle the LNG tank capacity; (iii) a MTU, which controls the PLCs using the Modbus TCP/IP communication protocol; (iv) a Historian Data Server, which records historical data upon LNG tank capacity and stores in the LNG database center; (v) a HMI, which is considered an input-output device with a panel view for depicting graphically the process data to human operators of the engineering workstations; (vi) a SMTP mail server with each mail operating system for the e-mail communication across the LNG Transport network.

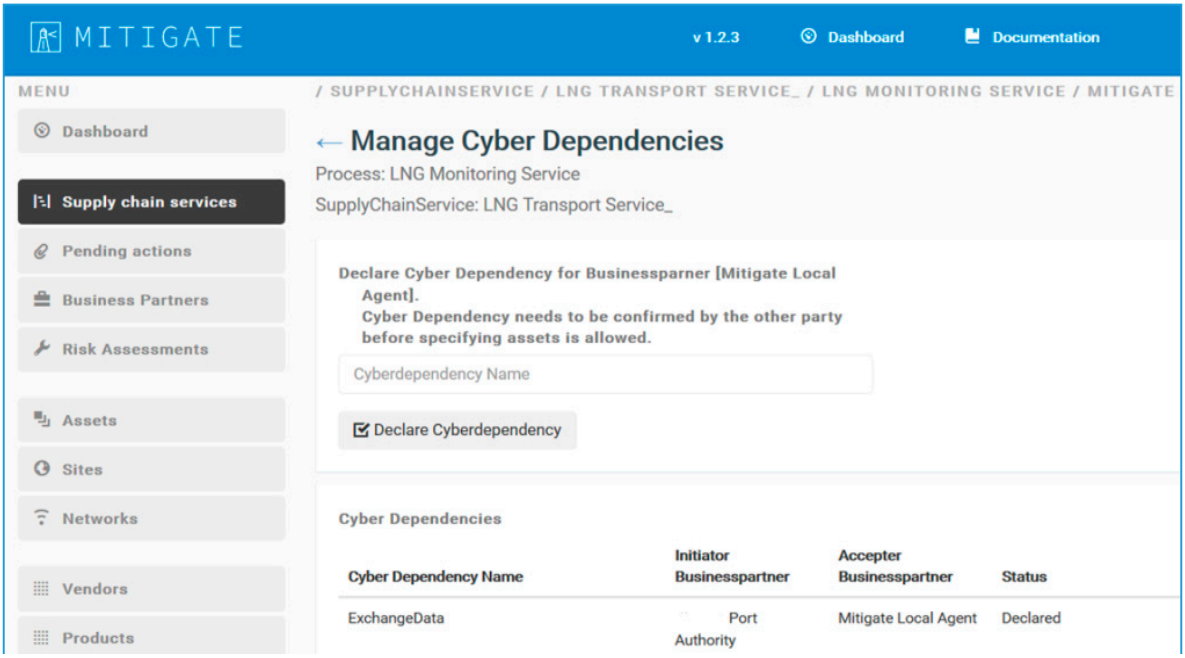

Figure 7. The "Exchange Data" cyberdependency is declared between the Port Authority and the Local Agent accepter business partner as a result of an e-mail exchange.

To this purpose, the Supply Chain Service Modelling (SAS-1) provides asset mapping (assets are characterized based on its cyber-nature; Application, Operating System or Hardware) and asset cyberdependency identification (Figure 7), where a set of logical rules are followed that guarantee the valid creation of a graph of assets and their cyberdependencies according to the twofold dependency concept analyzed in Section 4; an indicative example is presented in Table 1. This allows the business partners of the LNG Transport Service to understand assets interrelations within the LNG Transport Network. The asset-graph of the LNG Transport Network example is depicted previously in Figure 2.

Table 1. Example of SCADA assets cyberdependencies within the LNG Transport Network.

Asset Source	Asset Destination	Dependency Type: 1. Hosting, 2. Exchange, Data, 3. Storing, 4. Controlling, 5. Processing, 6. Accessing, 7. Installing, 8. Trusted 9. Connecting	Dependency Access Vector: Adjacent Network (A), Local (L), Network (N)
LNG—PLC software	LNG—PLC OS	installing	L
SMTP Mail Server	Local Agent Mail Server	Exchange data	N
LNG—PLC	LNG—Master Terminal Unit	Connecting	A

6.2. Utilization of SAS-2: SCADA Assets Vulnerabilities Management of the LNG Transport Service

A set of metrics is defined to present the vulnerabilities found in the declared assets from online repositories [65] using open intelligence techniques. The Vulnerability Management Menu of the MITIGATE system (SAS-2 service) delivers the confirmed vulnerability attributes and it is capable of creating zero-day exploitable vulnerabilities. Figure 8 shows an example of vulnerability attributes of confirmed and a created zero-day vulnerability via the Vulnerability Management service of the MITIGATE system. The presented vulnerabilities are both concern heap-based buffer overflow weaknesses in the Graphic Device Interface (GDI).

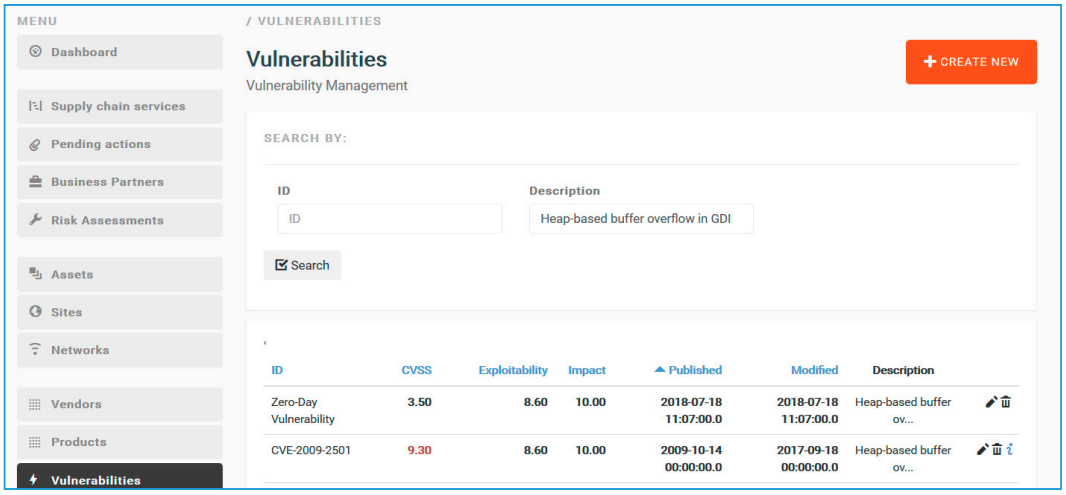

Figure 8. Confirmed and zero-day vulnerabilities attributes found on the "LNG Fuel Monitoring Software" asset operating in the LNG Monitoring Service process.

6.3. Utilization of SAS-3: Threats/Controls Management within the LNG Transport Service

The MITRE CAPEC, synchronization services [66] have associated the vulnerabilities identified on SCADA assets of the LNG Monitoring service process with one or more weakness identifiers. This is depicted from the Threat Management menu of the MITIGATE system (Figure 9).

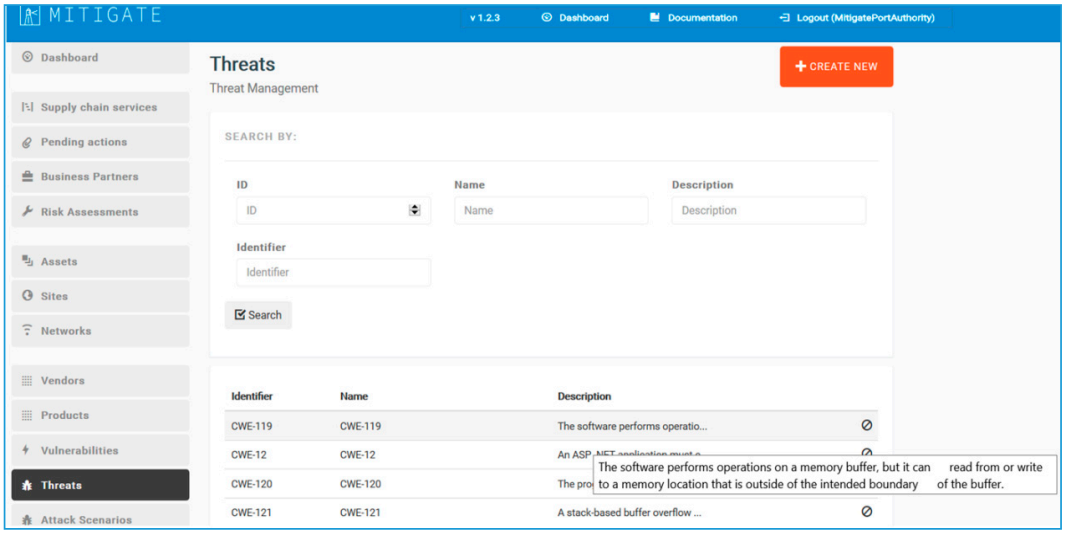

Figure 9. Threats Management service of the MITIGATE system showing the threat "Buffer Errors" (threat ID: CWE-119), which is the corresponding threat of the CVE-2009-2501 vulnerability found on the LNG Fuel Monitoring Software declared asset.

6.4. Utilization of SAS-4 Threat Scenarios Specification for LNG SCADA Assets

The "Attack Scenarios Management" environment of the MITIGATE system implements the mapping of threats and vulnerabilities with assets service. An example of this mapping is illustrated in Figure 10. The visualized attack scenario concerns the exploitation of vulnerability "CVE-2016-7960" found on the PLC software declared asset, which corresponds to the "information exposure" threat (CWE-200).

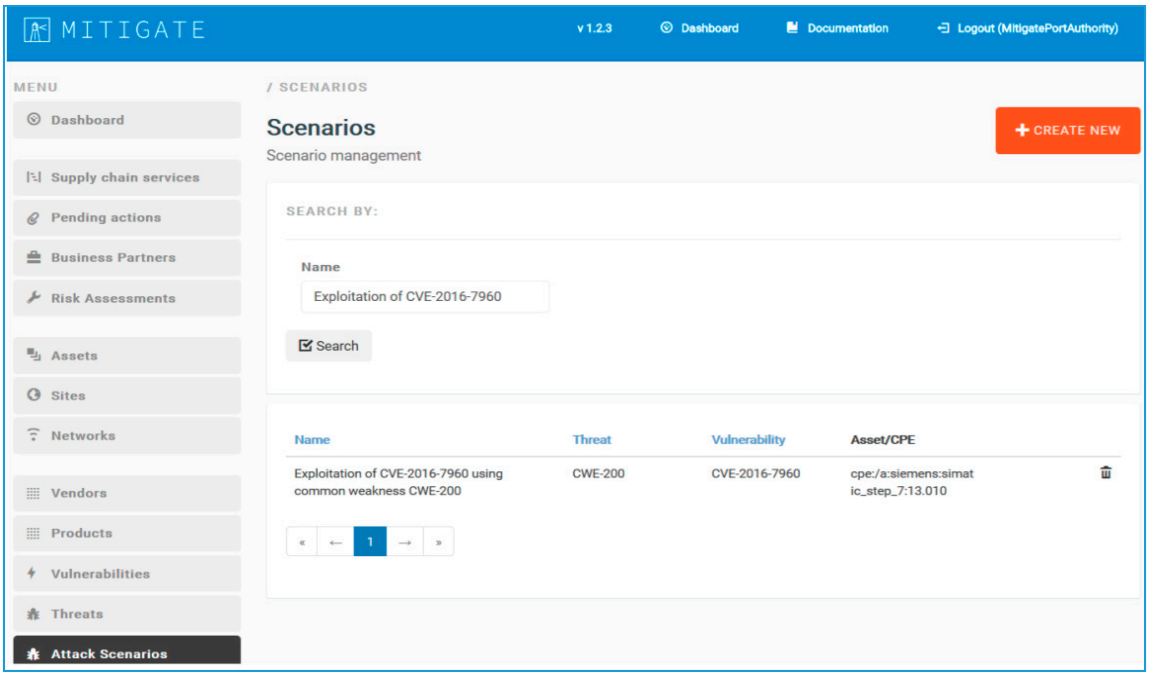

Figure 10. The Threat Scenarios Specification service shows a possible threat scenario for the "PLC software" declared asset of the LNG Transport Service.

The graphic representations of SAS-3 and SAS-4 accordingly have been implemented via business logic rules on top of a Neo4J database. The formal/normative concepts of Asset, Vulnerability, Threat, Control element, Vendor, Attack scenario, Impact Level are unified and uniquely represented in the supportive database schema.

6.5. Utilization of SAS-5: Supply Chain Risk Analysis of the LNG Monitoring Service process

To estimate the cyber-risks of the LNG Monitoring Service supply chain process, we have executed a simulation type risk assessment on the declared assets. The Supply Chain Risk Analysis service is capable of estimating cyber-risks for zero-day exploitable vulnerabilities. This is illustrated in Figure 11.

Figure 12 presents the Risk Analysis diagram of SCADA assets participating in the LNG Monitoring Service process, whereas Figure 13 shows the Threat Analysis diagram of the aforementioned assets, providing an indication of how crucial the protection is of an asset-based not only on the possibility of being attacked but also on the impact of the potential attack. The graphs depict individual cyber-risk level reports following the qualitative scale described in Section 4.2.5.

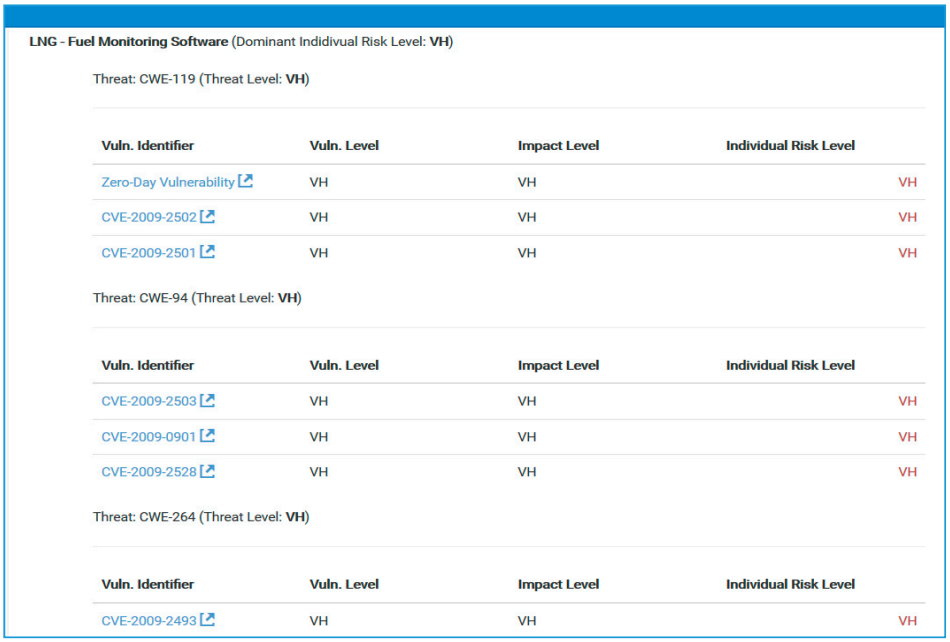

Figure 11. The Supply Chain Risk Analysis service has estimated the individual cyber-risk (VH) of the Fuel Monitoring software asset due to a zero-day exploitable vulnerability, which has been respectively counted in all types of cyber-risk estimation.

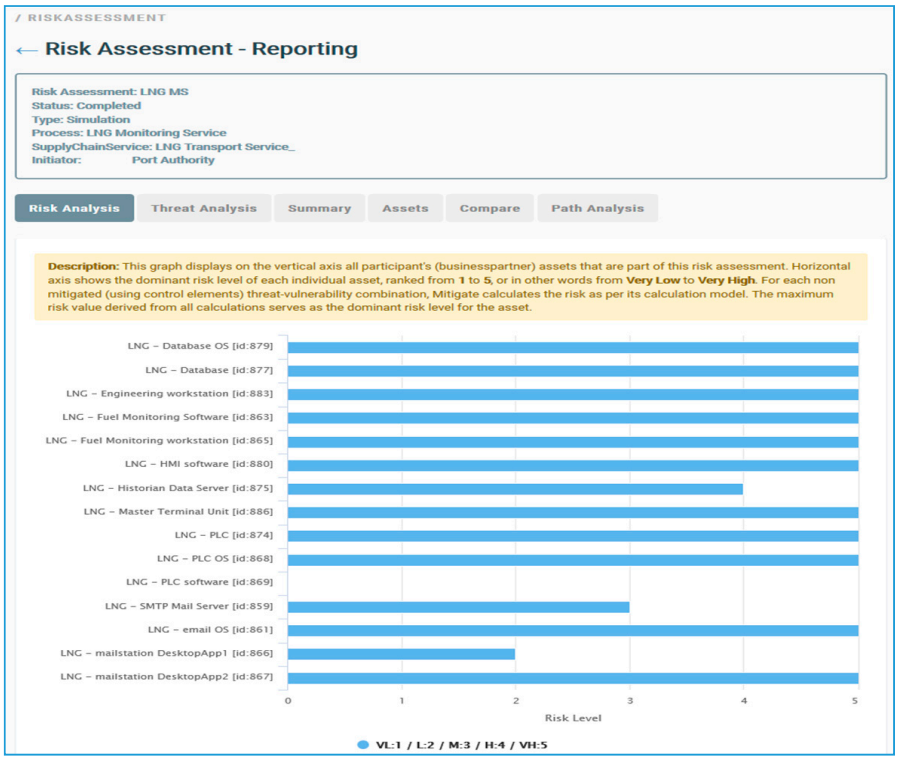

Figure 12. The Risk Analysis report diagram supports the Supply Chain Risk Analysis service presenting the dominant risk level per SCADA asset declared in the LNG Monitoring Service process.

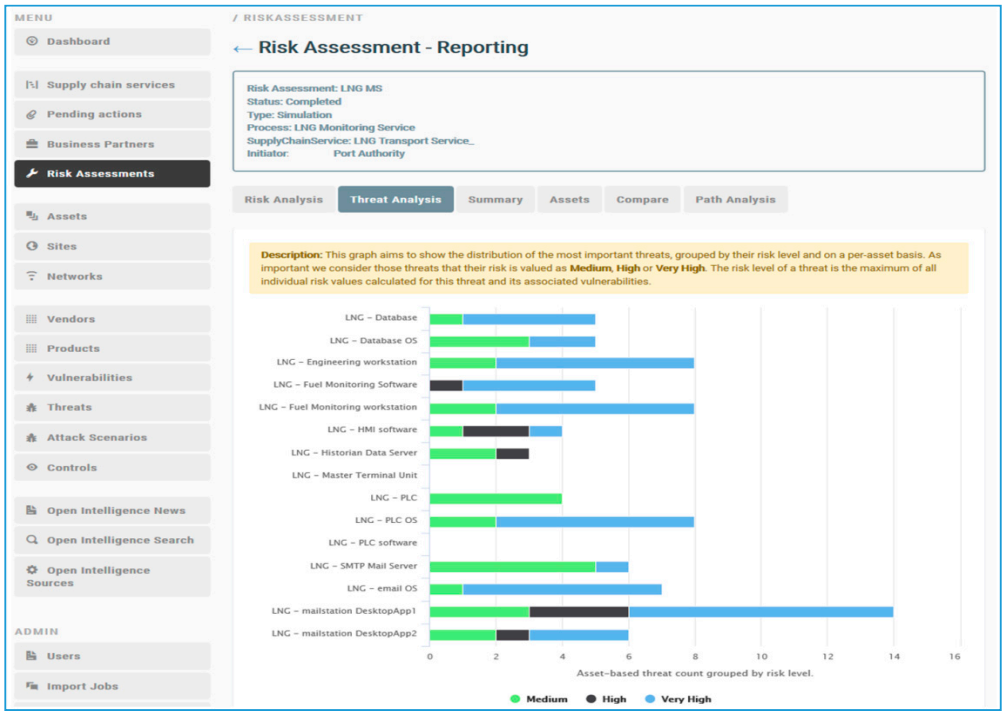

Figure 13. The Threat Analysis report diagram supports the Supply Chain Risk Analysis service presenting threats distribution of the most important threats grouped by their risk level per SCADA asset declared in the LNG Monitoring Service process.

6.6. Utilization of SAS-6: Attack Paths Simulation Scenarios of the LNG Transport Service SCADA Assets

Once the risk assessment has been performed, additional schemas are created that are inherited from the unified ones, such as the Attack Paths, simulating the different paths that a hacker can follow to harm a specific asset. This is supported by the Attack Path Simulation Service in the MITIGATE system (SAS-6). Figure 14 shows the attack path analysis query results according to different attack path parameters (i.e., attacker's profile, attacker's location, attacker's capability). For example, the "Local Attack" path analysis includes the query results for the given entry/target points, assuming that the attacker is an insider intruding into the Fuel Monitoring system using the local LNG network.

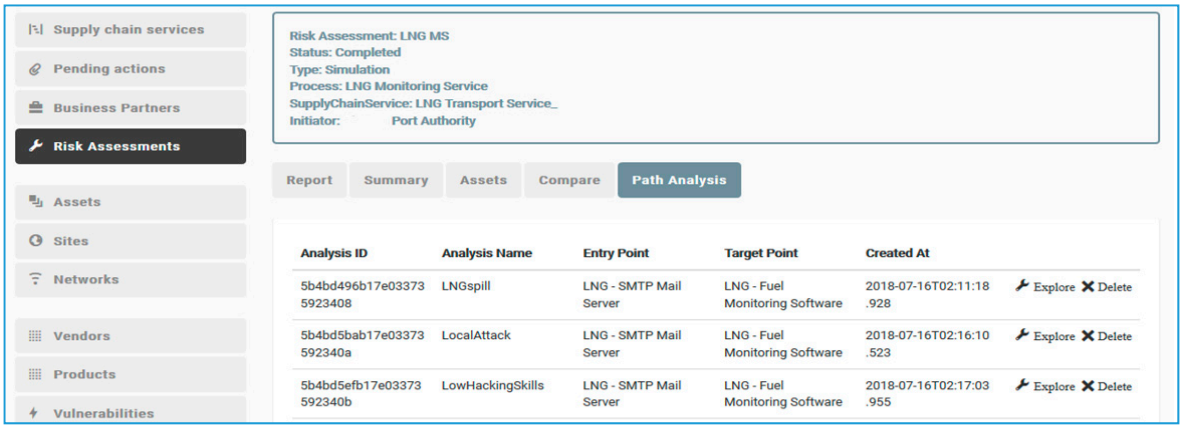

Figure 14. The path analysis query results inventory of the Attack Path Simulation Service grouped by the specific attack path parameters of the created attack path queries.

6.7. Supply Chain Risk Management (SAS-7)

Risk assessment is supported by the Supply Chain Risk Analysis (SAS-5) and the Supply Chain Risk Management (SAS-7) services in the MITIGATE system. The most complex risk assessment operations are (a) the ad-hoc calculation of the graph; (b) the replication of the asset mapping per each business partner; (c) the calculation of the individual risk assessment metrics and (d) the calculation of the attack chains that are bound to the graph. The MITIGATE RA services deliver various reports, such as the asset criticality and the most possible attacks per individual asset. In order to explore and manage the LNG Transport Service cyber risks, we may run alternative attack path analysis scenarios (depicted in Table 2) setting: (i) high-risk assets as entry points, such as the LNG Database and the SMTP Mail Server and review the attack path analysis results and (ii) set cyberdependency assets either as entry or target points and study the attack path sub-graphs. The cumulative risk for each attack path, according to the qualitative scale presented in Section 4.2.5, is shown in Table 2. For example, the risk exposure of reaching the specific asset "Fuel Monitoring Software" is "Very High" in case the adversary succeeds to enter into the LNG Transport Network by attacking the "LNG-SMTP Mail Server".

Table 2. Alternative Attack Path Analysis scenarios concerning different attack path metrics.

Analysis	Path Nodes	Cumulative Risk Level (Very High: VH, High: H, Moderate: M, Low: L, Very Low: VL)
LNG spill (Locally)	**LNG—Database** *(LNG Transport Network)* → **LNG—mailstation DesktopApp1** *(LNG Transport Network)* → **LNG—Fuel Monitoring Software**	H
LNG spill (Network)	**LNG—SMTP Mail Server** *(LNG Transport Network)* → **LNG—Fuel Monitoring Software**	VH
	LNG—SMTP Mail Server *(LNG Transport Network)* → **LNG—HMI software** *(LNG Transport Network)* → **LNG—Fuel Monitoring Software**	H
Attack on Control Stations (Network)	**LNG—mailstation DesktopApp1** *(LNG Transport Network)* → **LNG—HMI software** *(LNG Transport Network)* → **LNG—PLC OS**	H
	LNG—mailstation DesktopApp1 *(LNG Transport Network)* → **LNG—Engineering workstation** *(LNG Transport Network)* → **LNG—PLC OS**	H

Despite the individual RA report, another crucial source is the comparison between two RAs that has been performed on two different dates. Within one process of the MLoSC, many things can be altered. Initially, an asset can be replaced or even patched. Moreover, additional controls may have been enforced. Finally, additional vulnerabilities may have been disclosed for one asset. Hence, there is a business need to compare the output of these RAs regarding a specific process for two different timestamps (SAS-7). An indicative example of this security assessment utility is presented in Figure 15. In particular, an RA "LNG MS" simulation service is implemented on the assets of the LNG Monitoring Service process. Then, a new RA simulation is created and before executed, we set up a security control that mitigates the threat "Improper Restriction of Operations within the Bounds of a Memory Buffer" (CWE-119) on the following specific assets; PLC OS, Fuel Monitoring Workstation and Engineering Workstation. Additionally, we set up another security control on the asset "LNG-HMI Software" that mitigates its vulnerabilities. A new RA is then executing ("LNG TS with security controls" RA

simulation), which depicts that the declared security controls manage to mitigate the threat score on these SCADA assets, as shown in Figure 15.

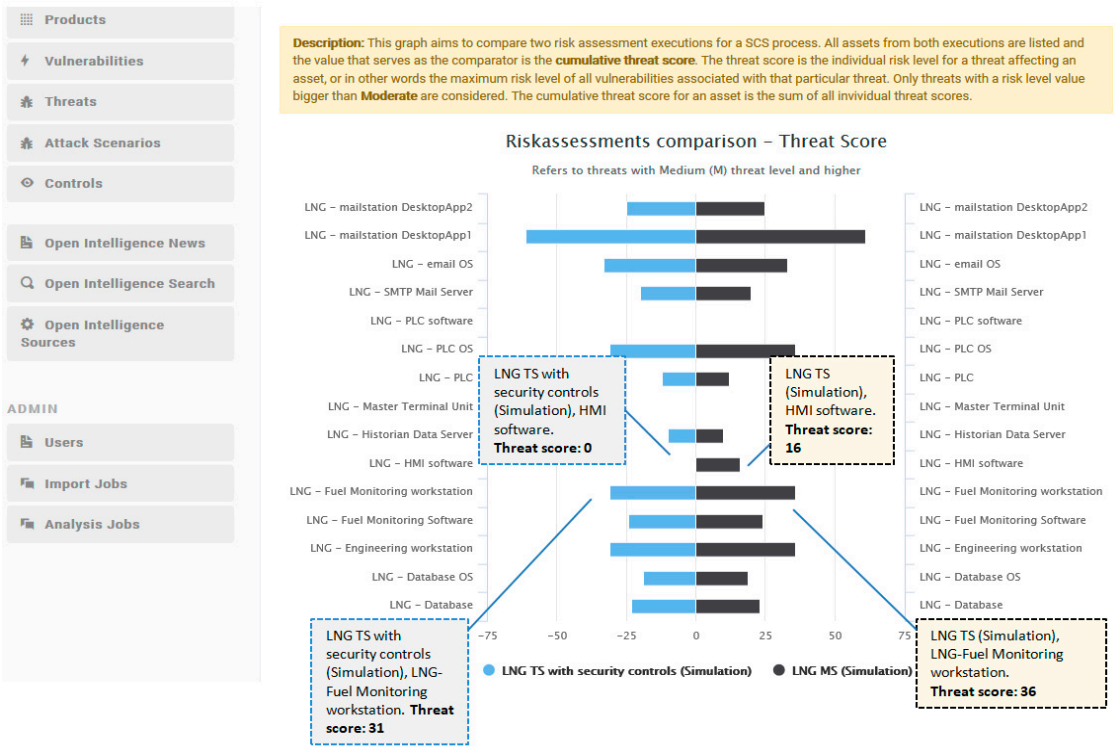

Figure 15. The Risk Assessments comparison diagram showing to the security officer whether the defined security controls are capable of mitigating cyber-assets risks.

6.8. Social Engineering and Open Intelligence (SAS-8)

The open repositories facilitate the required information during the risk assessment process and functions are satisfied by the Social Engineering and Open Intelligence MITIGATE service, as presented in Figure 6. Hence, normative metamodels using XSD notation are fully compatible with de-facto metamodels (CVE and CPE) providing the freedom to connect with multiple sources using an adapter pattern. The Open Intelligence Controls sub-service relates mainly to Threats and Controls. Threat and Attack type are used interchangeably. A threat or vulnerability can be mitigated by a control element.

The MITIGATE system uses the collected operational data describing the configuration of systems and software (e.g., network topologies and existing vulnerabilities) as well as static data describing the general risk (e.g., if an identified vulnerability has an exploit that is publicly available). MITIGATE also requires from the MLoSC security team to specify the (suspected/potential/possible) attacker profile (e.g., regarding knowledge and skill), the possible attacker source (e.g., from the Web) as well as the possible attacker targets (e.g., SCADA devices that are critical for the under examination LNG Transport Service). Accordingly, the MITIGATE would proceed to calculate an attack graph for this configuration and compute a probabilistic network (Individual, Cumulative and Propagated risks) on top of this attack graph.

7. Evaluation and Findings

In recent years, complex and heterogeneous CIs developments and their interdependencies within the Maritime Logistics Industry (i.e., port authorities, customs, shipping agencies and IoT enterprises) have been dictating the importance of protecting their systems' integrity and resilience. Most current risk management policies insufficiently consider the composite nature of ICT-empowered

infrastructures (i.e., SCADA and AIS systems) and forget to take into account the global supply chain interdependent environment to define the security processes.

Risk analysis methods have been introduced based on both qualitative (i.e., NIST 800-30 [43], OCTAVE [36]) and quantitative [20] or combined (ISO 27005 [10]) approaches, which either disregard or use quite primitive computational techniques that lack exploring and comparing risk assessment results. Security assurance techniques for large-sized enterprises applied both to composite and basic systems (i.e., NIST 800-30 [43], IT-Grundschutz [44]) have been presented with limitations in analyzing management and operational issues and give low collaborative capabilities. Bayesian risk assessment methodologies (i.e., AURUM [35], OCTAVE [36]) main disadvantages refer to their partial subjectivity, the need for a potentially vast amount of training data and the difficulty of being applicable to new situations (subjective choice and Bayesian updates of the a-priori models).

An effective risk assessment approach for SCADA systems may reflect the characteristics presented in Section 3. In this context, the MITIGATE methodology addresses the following issues: (i) Complex systems, such as SCADA systems, require the collaboration and interaction of supply chain stakeholders and their cooperating systems to set effective risk and impact indicators [8]. The MITIGATE EU Project [12] introduces a collaborative, evidence-driven Maritime Supply Chain Risk Assessment (MCSRA) approach for MLoSCs, which alleviates the limitations of state-of-the-art risk management frameworks; (ii) The MITIGATE security assessment services use knowledge management [55], open source intelligence techniques and social engineering to provide accurate and updated information for vulnerabilities, threats and provide rule-based mechanisms to manipulate the extracted knowledge and to generate attack paths; (iii) Mitigate builds the risk assessment performance on an open simulation environment, which allows stakeholders to simulate risks and evaluate risk mitigation actions; (iv) Represents and explores scenarios according to global supply chain requirements; (v) Regarding risk assessment methods on SCADA systems, few approaches provide system-asset analysis, vulnerabilities and countermeasures [8]. The MITIGATE methodology applies a systematic asset-centric thorough model analysis in supply chain processes to define assets interdependencies, address vulnerabilities, threats, individual, cumulative, propagated risks and their cascading effects and indicate mitigation policies and payoffs; (vi) It is compliant with international risk management standards and security frameworks (i.e., ISO 27k and ISO 28k family standards). The demonstration of the simulated LNG scenario of SCADA components has shown that MITIGATE security assessment services are applicable to ICT-based infrastructures and complex environments of SCADA and AIS systems.

The report evaluates the internal and external results of user-tests for the MITIGATE system [64]. Internal and external tests were conducted for a period of 15 months. The tests have been divided into two phases (internal and external) and carried out simultaneously in four countries: Greece, Spain, Germany and Italy. During the internal phase, the MITIGATE system and its services were first tested among port operators participants. In the external phase, the MITIGATE system was demonstrated to external professionals (experts from Transport and Logistics enterprises and security consultants) who evaluated and assessed the MITIGATE system and its corresponding services. Their comments and suggestions have been collected. The feedback and experience gained have been continuously and promptly passed on to the developers, who then incorporated it into system improvements.

Moreover, the tests sites reported in total the participation of 235 internal and 452 external participants, mostly representatives from maritime, transport and logistics sectors, which are spread over the individual test sites (Table 3).

Table 3. Internal and External Test Participants per Country.

Country of the Test Site	Number of Internal Participants	Number of External Participants
Spain	50	32
Germany	39	32
Greece	108	375
Italy	38	13

A total of 113 non-technical and four technical questionnaires have been collected (Figures 16 and 17). However, totally 18 of the respondents can be assigned an IT background based on their positions they entered in the questionnaire, e.g., "SCADA/EMS Operator", "Senior Software Architect" or "Manager Network, Security & Infrastructure IT". Furthermore, at least 16 respondents can be assumed to have a security-related background, since "security" and/or "safety" is a part of their job title, e.g., "PFSO" ("Port Facility Security Officer"), "Chief Security Officer" or "Head of Safety and Security". Summarizing, 34 out of 113 are considered to have IT or Security related knowledge. Respondents answered questionnaires and provided their assessment using a 4-point Likert scale; A. Strongly disagree; B. Disagree; C. Agree; D. Strongly agree.

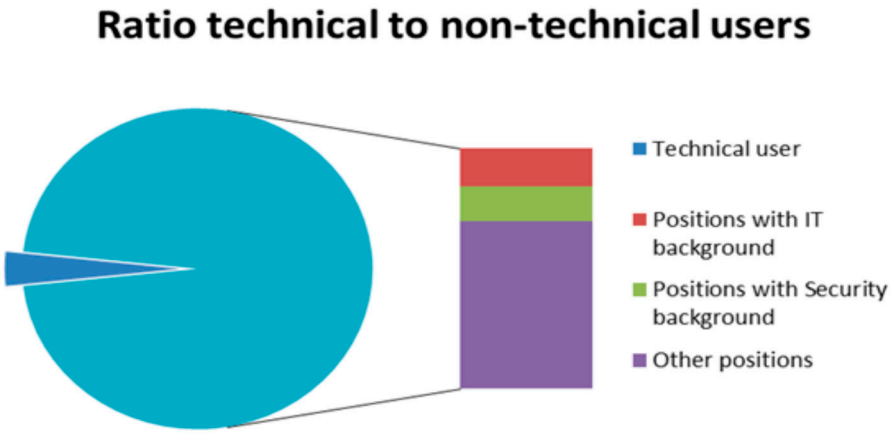

Figure 16. Ratio technical to non-technical user.

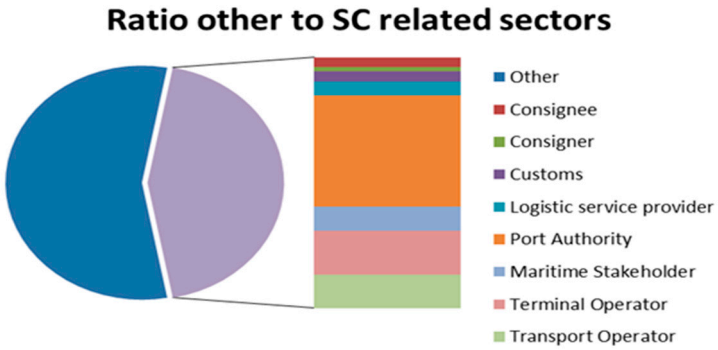

Figure 17. Business Activities.

The respondents were asked whether the system fulfils its purpose of mapping general characteristics of the methodology, if the system enables a collaborative approach for supply chain participants, whether it provides convenient possibilities to exchange data (Figure 18) with other software. Almost all respondents agreed that MITIGATE can successfully exchange data, satisfies the methodology-characteristics mapping and that it is easy to learn enabling a collaborative approach for supply chain participants to take care of their Critical Infrastructure.

Additionally, almost a quarter of the respondents answered that they were unaware of to say if an organization improves its compliance with security standards using MITIGATE. The majority of the responders agreed ("strongly agree": 52%, "agree": 44%) that the MITIGATE-system provides important decision support for improving the organizations' risk situation (Figure 19). The 4% (of the test users who did not agree with this statement seem to have done so at least in part because of the development status of the prototypes: One of the comments pointed out implies that "the MITIGATE system could provide important decision support".

Concerning the overall impression of the MITIGATE system utility, as shown in (Figure 20): Over 78% of the test users responded positively that the required time for the MITIGATE RA is reasonable, over 87% of the test users imply that they have felt comfortable using the MITIGATE-system, while 19% responded negatively that the MITIGATE system is easy to learn. Moreover, 64% strongly agreed and 23% agreed that the MITIGATE system will help them to become more productive.

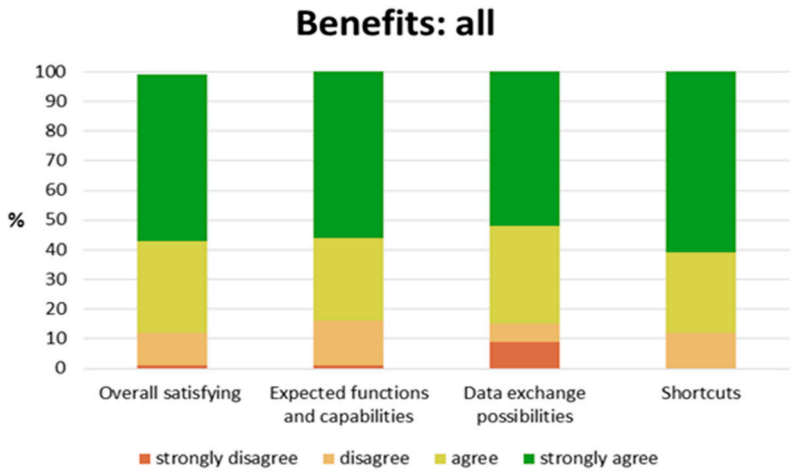

Figure 18. Overall impression of the respondents regarding the benefits of the MITIGATE security assessment services.

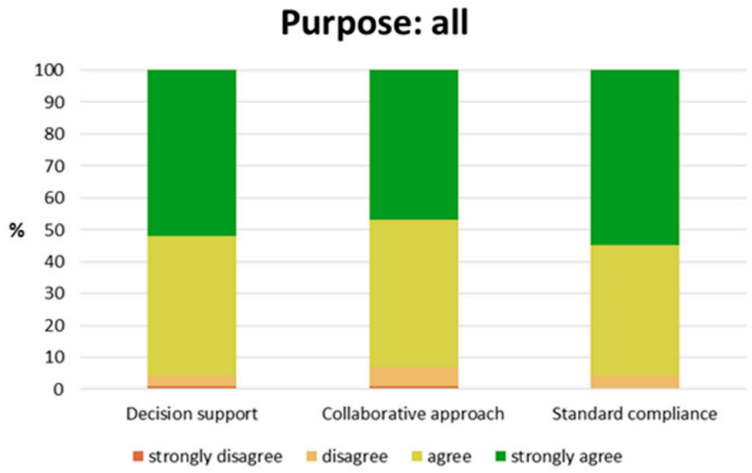

Figure 19. Overall impression of the respondents concerning the utilization of the MITIGATE system services.

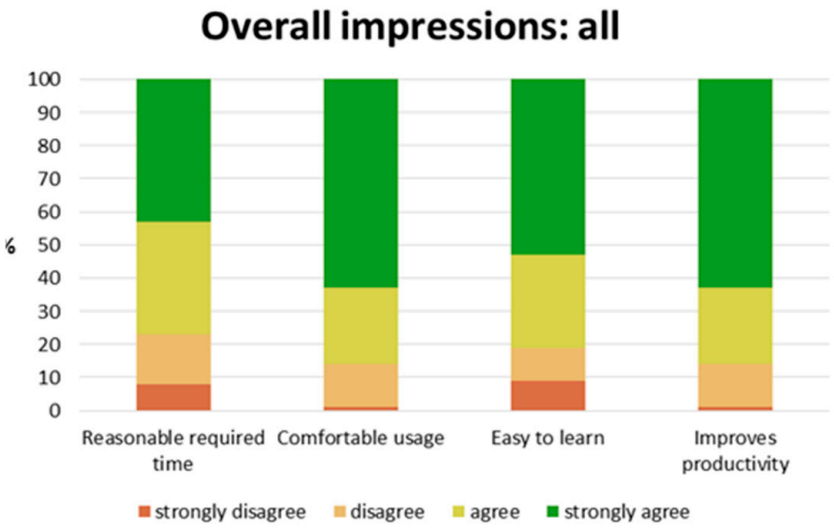

Figure 20. The impressions of the overall respondents for the MITIGATE system.

Eventually, the internal and external testing phases have provided many recommendations and suggestions for improvements to the developers. Much of the potential for improvement has already been implemented in the subsequent releases during the test phase. The tests were able to successfully provide feedback for the improvements of the system during the project period in terms of a targeted TRL (technology readiness level) of 7, as well as for further development towards a finished product or a TRL of 9.

8. Conclusions and Discussions

Maritime Logistics and Supply Chains (MLoSC) are composite interconnected systems playing a vital role in the transportation, storage and delivery of goods and services. MLoSC services usually involve various and multiple types of Critical Infrastructure, mainly in the transportation sector and exhibit intra-sector and cross-border dependencies. This type of complex infrastructure is the SCADA systems, which require the collaboration and interaction between supply chain stakeholders and their cooperating assets to set effective risk and impact indicators [8]. The primary goal of MITIGATE is to assess the individual, cumulative and propagated risk of an IT-based supply chain, having in mind the cyber interconnections and interdependencies between the various entities within an MLoSC. MITIGATE assesses the threats affecting all the business partners involved in the MLoSC and estimates the threats of the MLoSC as a whole via a collaborative environment. This helps to protect the expected individual, cumulative and propagated risks within it. The derived risk values are used in order to generate a baseline security strategy for MLoSCs, identifying the least necessary security controls for each participant within the supply chain. This enables MLoSC participants to fine-tune their security strategies according to their business role as well as their dependencies.

It should be noted that in order to validate the MITIGATE methodology, case studies based on real-world maritime scenarios and data were used. The evaluation results are promising, especially considering the impact of previous versions on the results: A large majority of MLoSC stakeholders consider the MITIGATE system to be efficient and useful in terms of its collaborative approach and decision support for improving their organizations' risk situation, having clearly organized information and being equipped with all of the expected functionalities. The response to the question, if they are satisfied with the system as a whole, is positive by a vast majority, which seems to be a good rating for a prototype in the beta stage.

Consequently, this work illustrates that maritime, logistics and transport supply chain services have common characteristics and face similar challenges concerning cybersecurity. In this context, MITIGATE can meet their requirements and particularities. To this end, the MITIGATE system

supports a number of security assessment services that can be used by various different, heterogeneous MLoSC infrastructures of different types, sizes and business activities. This work has implemented the risk assessment services on an indicative SCADA scenario and has proved that the MITIGATE approach can be successfully applied to complex MLoSC systems, such as SCADA infrastructure, can estimate effectively their cyber-risks and drive the risk mitigation actions.

However, the MITIGATE evidence-driven Risk Assessment methodology provides security assessment services while considering only the cyber-nature of CPSs. Future work can be carried out on the integration of incident management practices to estimate and handle the combination of physical and cyber-risks on such infrastructure.

Author Contributions: E.-M.K. and S.P. constructed the presentation of the methodology and conceived the SCADA example for the utilization of the security assessment services. H.M. encouraged to further analyse the demonstration of the methodology and supervised the entire work. The described attack scenarios were fabricated by S.P. and E.-M.K. E.-M.K. and S.P. contributed to the writing of the manuscript. N.P. reviewed the work during the writing process and contributed to the writing of the first section. All authors discussed the content of the research and contributed to the final manuscript.

Funding: This research received no external funding.

Acknowledgments: This work has been supported by the European Union's Horizon 2020 research and innovation program under grant agreement No. 653212 project "MITIGATE". The authors would like to thank all the project members for their valuable insights.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Mattioli, R.; Moulinos, K. *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*; ENISA: Attiki, Greece, 2015; ISBN 978–92-9204-135-9.
2. International Maritime Organization (IMO). *Maritime Cyber Risk Management in Safety Management Systems*; MSC-FAL.1/Circ.3; IMO: London, UK, 2017.
3. Polemi, N. *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains*; Elsevier: Amsterdam, The Netherlands, 2017; pp. 1–193.
4. Jackson, K. Chinese Hackers Target Logistics & Shipping Firms with Poisoned Inventory Scanners. Available online: https://www.darkreading.com/attacks-breaches/chinese-hackers-target-logistics-and-shipping-firms-with-poisoned-inventory-scanners/d/d-id/1297182? (accessed on 9 July 2018).
5. Kravets, D. FEDS: Hacker Disabled Offshore Oil Platforms' Leak-Detection System. Available online: https://www.wired.com/2009/03/feds-hacker-dis/ (accessed on 9 July 2018).
6. Kate, B. Maritime Cyber Attacks: Changing Tides. Available online: https://www.maritime-executive.com/blog/maritime-cyber-attacks-changing-tides (accessed on 25 May 2018).
7. Theocharidou, M.; Giannopoulos, G. *Risk Assessment Methodologies for Critical Infrastructure Protection. Part II: A New Approach Report EUR 27332*; Luxembourg Publications Office of the EU: Luxembourg, 2015.
8. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **2016**, *56*, 1–27. [CrossRef]
9. National Institute of Standards and Technology—NIST. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*; SP800-37 Rev.1; NIST: Gaithersburg, MD, USA, 2010.
10. ISO/IEC 27000-Family of Information Security Standards. Available online: https://www.itgovernance.co.uk/iso27000-family (accessed on 9 July 2018).
11. 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: https://www.iso.org/standard/45654.html (accessed on 9 July 2018).
12. MITIGATE EU Project. Available online: https://www.mitigateproject.eu/ (accessed on 25 May 2018).
13. Zio, E. The Future of Risk Assessment. *Reliab. Eng. Syst. Saf.* **2018**, *177*, 176–190. [CrossRef]
14. National Academy Press. *Risk Assessment in the Federal Government: Managing the Process*; Committee on the Institutional Means for Assessment of Risks to Public Health, National Research Council; The National Academies Press: Washington, DC, USA, 1983.

15. Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A. *Guide to Industrial Control Systems (ICS) Security*; NIST special publication SP800-82 Rev.2; NIST: Gaithersburg, MD, USA, 2015.
16. ISO. *ISO/IEC 13335-1:2004, Information Technology-Security Techniques-Management of Information and Communications Technology Security*; ISO: Geneva, Switzerland, 2004.
17. Ralston, P.; Graham, J.; Hieb, J. Cyber security risk assessment for SCADA and DCS networks. *ISA Trans.* **2007**, *46*, 583–594. [CrossRef] [PubMed]
18. Wyss, D.; Durán, F. *OBEST: The Object-Based Event Scenario Tree Methodology*; Sandia National Laboratories: Livermore, CA, USA, 2001.
19. Schneier, B. Attack trees. *Dr. Dobb's J.* **1999**, *24*, 21–29.
20. McQueen, M.A.; Boyer, W.F.; Flynn, M.A.; Beitel, G.A. Quantitative cyber risk reduction estimation methodology for a Small SCADA control system. In Proceedings of the 39th annual Hawaii international conference on system sciences, Kauia, HI, USA, 4–7 January 2006.
21. Cheminod, M.; Durante, L.; Valenzano, A. Review of security issues in industrial networks. *IEEE Trans. Ind. Inform.* **2013**, *9*, 277–293. [CrossRef]
22. Gertman, D.; Folkers, R.; Roberts, J. Scenario-based approach to risk analysis in support of cyber security. In Proceedings of the 5th International Topical Meeting on Nuclear Plant Instrumentation Controls, and Human Machine Interface Technology, Albuquerque, NM, USA, 12–16 November 2006.
23. Beggs, C.; Warren, M. Safeguarding Australia from cyber-terrorism: A proposed cyber-terrorism SCADA risk framework for industry adoption. In Proceedings of the 10th Australian information warfare and security conference, Joondalup, Australia, 1–3 December 2009; p. 5. [CrossRef]
24. Ericsson, G.N. Information security for electric power utilities (EPUs)-CIGR developments on frameworks, risk assessment and technology. *IEEE Trans. Power Deliv.* **2009**, *24*, 1174–1181. [CrossRef]
25. Francia, G.A., III; Thornton, D.; Dawson, J. Security best practices and risk assessment of SCADA and industrial control systems. In Proceedings of the 2012 world congress in computer science, computer engineering, and applied computing, Las Vegas, NV, USA, 16–19 July 2012.
26. Markovic-Petrovic, J.D.; Stojanovic, M.D. An improved risk assessment method for SCADA information security. *Elektron. Elektrotech.* **2014**, *20*, 69–72. [CrossRef]
27. Verendel, V. Quantified security is a weak hypothesis: A critical survey of results and assumptions. In Proceedings of the 2009 Workshop on New Security Paradigms Workshop, Oxford, UK, 8–11 September 2009; pp. 37–50.
28. Cardenas, A.; Amin, S.; Lin, Z.-S.; Huang, Y.-L.; Huang, C.-Y.; Sastry, S. Attacks against process control systems: Risk assessment, detection and response. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011; pp. 355–366.
29. Ten, C.-W.; Manimaran, G.; Liu, C.-C. Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Trans. Syst. Man Cybern. Part A Syst. Hum.* **2010**, *40*, 853–865. [CrossRef]
30. Byres, E.; Franz, M.; Miller, D. The use of attack trees in assessing vulnerabilities in SCADA systems. In Proceedings of the International Infrastructure Survivability Workshop, Lisbon, Portugal, 5–8 December 2004.
31. Marwa, K.; Moustafa, N.; Sitnikova, E.; Creech, G. Privacy preservation intrusion detection technique for SCADA systems. In Proceedings of the Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 14–16 November 2017; pp. 1–6.
32. Marsden, T.; Moustafa, N.; Sitnikova, E.; Creech, G. Probability Risk Identification Based Intrusion Detection System for SCADA Systems. In Proceedings of the International Conference on Mobile Networks and Management, Melbourne, Australia, 13–15 December 2017; Springer: Cham, Switzerland, 2017; pp. 353–363.
33. Yuksel, O.; den Hartog, J.; Etalle, S. Reading between the fields: Practical, effective intrusion detection for industrial control systems. In Proceedings of the 31st Annual ACM Symposium on Applied Computing (SAC), Pisa, Italy, 4–8 April 2016; pp. 2070–2073, ISBN 978-1-4503-3739-7.
34. Haimes, Y.Y.; Horowitz, B.M. Adaptive two-player hierarchical holographic modeling game for counterterrorism intelligence analysis. *J. Homel. Secur. Emerg. Manag.* **2004**, *1*, 121. [CrossRef]
35. Ekelhart, A.; Fenz, S.; Neubauer, T. Automated Risk and Utility Management. In Proceedings of the 6th International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 27–29 April 2009; pp. 393–398.

36. Alberts, C.J.; Dorofee, A. *Managing Information Security Risks: The OCTAVE Approach*; Addison-Wesley Longman Publishing Co., Inc.: Boston, MA, USA, 2002.
37. Djordjevic, I.; Gan, C.; Scharf, E.; Mondragon, R.; Gran, B.A.; Kristiansen, M.; Dimitrakos, T.; Stølen, K.; Opperud, T.A. *Model Based Risk Management of Security Critical Systems*; WIT Transactions on Modelling and Simulation, Vol.31; WIT Press: Southampton, UK, 2002. [CrossRef]
38. Papastergiou, S.; Polemi, D. Securing Maritime Logistics and Supply Chain: The Medusa and MITIGATE approaches. *Marit. Interdiction Oper. J.* **2017**, *14*, 42–48.
39. ISO31000-Risk Management. Available online: https://www.itgovernance.co.uk/iso31000 (accessed on 9 July 2018).
40. Risikomanagement für Organisationen und Systeme-Begriffe und Grundlage. Available online: https://shop.austrian-standards.at/action/de/public/details/150292/ONR_49000_2004_01_01 (accessed on 9 July 2018).
41. ISO/IEC 20000-The International Standard for Service Management. Available online: https://www.itgovernance.co.uk/iso20000 (accessed on 9 July 2018).
42. NIST Standard Reference Materials Catalog 2002. Available online: https://www.nist.gov/publications/nist-standard-reference-materials-catalog-2002 (accessed on 9 July 2018).
43. Guide for Conducting Risk Assessments, SP 800-30 Rev.1. Available online: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (accessed on 9 July 2018).
44. Deutsch Federal Office for Information Security, IT-Grundschutz Catalogues. Available online: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html (accessed on 9 July 2018).
45. Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on Enhancing Ship and Port Facility Security, Capability Assessment Guidelines. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0725&from=EN (accessed on 9 July 2018).
46. Stewart, J.M.; Chapple, M.; Gibson, D. *CISSP: (ICS) Certified Information Systems Security Professional*, 7th ed.; CISSP: Clearwater, FL, USA, 2015; Available online: https://sybextestbanks.wiley.com/courses/102/data/ebook.pdf (accessed on 9 July 2018) ISBN 978-1-119-04271-6.
47. International Maritime Organisation MSC. 2004-06. Available online: http://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Maritime-Safety-Committee-(MSC)/Pages/MSC-2004-06.aspx (accessed on 9 July 2018).
48. ISO20858: 2007-Ships and Marine Technology-Maritime Port Facility Security Assessments and Security Plan Development. Available online: https://www.iso.org/standard/46051.html (accessed on 9 July 2018).
49. Risk Management Capability Assessment Guidelines. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015XC0808(01)&from=EN (accessed on 9 July 2018).
50. Zambon, E.; Etalle, S.; Wieringa, R.J.; Hartel, P. Model-based qualitative risk assessment for availability of IT infrastructures. *Softw. Syst. Model.* **2011**, *10*, 553–580. [CrossRef]
51. Trimble, D.; Monken, J.; Sand, A.F.L. A framework for cybersecurity assessments of critical port infrastructure. In Proceedings of the 2017 International Conference on Cyber Conflict (CyCon U.S.), Washington, DC, USA, 7–8 November 2017; pp. 1–7.
52. Igure, V.M.; Laughter, S.A.; Williams, R.D. Security issues in SCADA networks. *Comput. Secur.* **2006**, *25*, 498–506. [CrossRef]
53. DiRenzo, J.; Goward, D.A.; Roberts, F.S. The little-known challenge of maritime cyber security. In Proceedings of the 6th International Conference in Information, Intelligence, Systems and Applications (IISA), Corfu, Greece, 6–8 July 2015; pp. 1–5.
54. Kalogeraki, E.M.; Polemi, N.; Papastergiou, S.; Panayiotopoulos, T. Modeling SCADA Attacks. In Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability (WS4 2017), London, UK, 15–16 February 2017; Lecture Notes in Networks and, Systems, Yang, X.S., Nagar, A., Joshi, A., Eds.; Springer: Singapore, 2018; Volume 18, pp. 47–55, ISBN 978-981-10-6916-1.
55. Kalogeraki, E.-M.; Apostolou, D.; Polemi, N.; Papastergiou, S. Knowledge Management Methodology for Identifying Threats in Maritime/Logistics Supply Chains. *Knowl. Manag. Res. Pract. J.* **2018**. [CrossRef]

56. Papastergiou, S.; Polemi, N. MITIGATE: A dynamic Supply Chain Cyber Risk Assessment Methodology. In Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability (WS4 2017), London, UK, 15–16 February 2017; Lecture Notes in Networks and Systems. Yang, X.S., Nagar, A., Joshi, A., Eds.; Springer: Singapore, 2018; Volume 18, pp. 1–9.
57. Polatidis, N.; Pimenidis, E.; Pavlidis, M.; Papastergiou, S.; Mouratidis, H. From Product Recommendation to Cyber-Attack Prediction: Generating Attack Graphs and Predicting Future Attacks. In *Evolving Systems*; Pavlidis; Springer: Berlin, Germany, 2018; pp. 1–12.
58. Polatidis, N.; Pimenidis, E.; Pavlidis, M.; Mouratidis, H. *Recommender Systems Meeting Security: From Product Recommendation to Cyber-Attack Prediction, Proceedings of Engineering Applications of Neural Networks: 18th International Conference, Athens, Greece, 25–27 August 2017*; Boracchi, G., Iliadis, L., Jayne, C., Likas, A., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 508–519.
59. Rass, S.; König, S.; Schauer, S. Uncertainty in Games: Using Probability-Distributions as Payoffs. In *Lecture Notes in Computer Science, Proceedings of the Decision and Game Theory for Security, London, UK, 4–5 November 2015*; Khouzani, M.H.R., Panaousis, E., Theodorakopoulos, G., Eds.; Springer: Cham, Switzerland, 2015; pp. 346–357.
60. Rass, S. On Game-Theoretic Risk Management (Part One)-Towards a Theory of Games with Payoffs that are Probability-Distributions. *arXiv*, 2015, arXiv:150607368.
61. Polatidis, N.; Pavlidis, M.; Mouratidis, H. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Comput. Stand. Interfaces* **2017**, *56*, 74–82. [CrossRef]
62. Mouratidis, H. Secure software systems engineering: The Secure Tropos approach. *J. Softw.* **2011**, *6*, 331–339. [CrossRef]
63. AECID Technique. Available online: https://www.ait.ac.at/themen/cyber-security/projects/aecid/ (accessed on 25 May 2018).
64. MITIGATE Risk Management System. Available online: http://mitigate.euprojects.net/ (accessed on 25 May 2018).
65. CVE Details Portal. Available online: https://www.cvedetails.com/ (accessed on 25 May 2018).
66. Common Attack Enumeration and Classification (MITRE). Available online: https://capec.mitre.org/ (accessed on 25 May 2018).