JYX JYVÄSKYLÄN YLIOPISTO UNIVERSITY OF JYVÄSKYLÄ

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Simola, Jussi; Pöyhönen, Jouni; Martti, Lehto

Title: Cyber Threat Analysis in Smart Terminal Systems

Year: 2023

Version: Published version

Copyright: © 2023 Jussi Simola, Jouni Pöyhönen, Lehto Martti

Rights: CC BY-NC-ND 4.0

Rights url: https://creativecommons.org/licenses/by-nc-nd/4.0/

Please cite the original version:

Simola, J., Pöyhönen, J., & Martti, L. (2023). Cyber Threat Analysis in Smart Terminal Systems. In R. L. Wilson, & B. Curran (Eds.), ICCWS 2023 : Proceedings of the 18th International Conference on Cyber Warfare and Security (pp. 369-378). Academic Conferences International Ltd. The Proceedings of the ... International Conference on Cyber Warfare and Security, 18. https://doi.org/10.34190/iccws.18.1.931

Cyber Threat Analysis in Smart Terminal Systems

Jussi Simola, Jouni Pöyhönen and Martti Lehto
University of Jyväskylä, Jyväskylä, Finland

Jussi.hm.simola@jyu.fi
jouni.a.poyhonen@jyu.fi
martti.j.lehto@jyu.fi

Abstract: Cyber threats create significant factors that challenge traditional threat prevention mechanisms in harbor areas and port terminals. It has been recognized that understanding security functionalities in the harbor area is based on a more traditional experience of what it requires. It is not enough that the maritime and harbor ecosystem repeats only physical security service routines regarding random checks of passengers and vehicles and customs functions on cargo and passenger transportation. Smart environments and infrastructures are widely expanded in urban areas and create more challenges if old practices are combined with new technologies and functionalities. Traditional threats have changed to a combination of threat types. While developing cyber or physical threats may evolve into hybrid threats, it may prevent everyday harbor activities so that damage can become long-lasting and harm business continuity management. Therefore, it is essential to analyze cyber threat factors in Smart Terminal Systems. The research provides cyber threat and vulnerability analysis and the main attack vectors in the Smart Terminal systems. This research belongs in Finland to the maritime Sea4Value (S4VF) research program that includes Smart Terminals (SMARTER) project for harbor's digitalization.

Keywords: Maritime Logistics, Smart Terminal Process, Cyber Security Analysis, Threats

1. Introduction

Global maritime and maritime logistic systems are essential parts of critical global infrastructures. Digitalization and increased levels of autonomy in logistic transport chains are expected to take leaps forward in the coming years. The development of modern logistics depends entirely on a cyber environment that provides dynamic services. In Finland Smart Terminals (SMARTER) research project consists of port digitization by the end of 2023. The mission of SMARTER is to create replicable models for digitalization, service innovation, and data usage and sharing in the harbor environment and prepare for the future by taking steps toward smart and autonomous maritime transportation. The project goals are conducted to the reduction of emissions by optimizing harbor operations and improving cargo and people flow while improving the experience for all stakeholders (DIMECC, 2020)

The structure of the project has three use cases. Those are ship turnaround, truck traffic, and passenger flow. Use cases are designed to support one another, and there is a linkage between the use cases. The applied research work is organized into five work packages, including cyber security research actions in Work Package 4. (DIMECC, 2020)

The port cases digitalization means the development of Information and Communication Technology (ICT), Information Technology (IT), and Industrial Control System (ICS) or Operation Technologies (OT) solutions. Cyber threats create significant factors that challenge traditional threat prevention mechanisms in harbor areas and port terminals. In the future, maritime ports will become increasingly digitalized system systems (SoS). Cyber threats are system-level threats and will be needed to be coordinated like hybrid responses with other threats. Thus, it is necessary to address the comprehensive and relevant cyber threat analysis and security management aspects of the overall maritime solutions. It is crucial to enhance trustable services meaning the usability, reliability, and integrity of systems continuity within the operating environment. ENISA Threat Landscape Report 2016 emphasizes all elements covered within an attack on a business process. It means that not all artifacts/components used are IT-related; there are steps/procedures used within an attack, that are performed by having knowledge or information about the details of the business process at stake (ENISA, 2017).

This paper follows our previous research papers in this SMARTER study concerning cyber threat challenges in maritime logistics in in harbor areas and port terminals. The paper includes an analysis of the cyber threats in port systems, threat prevention requirements, and what prevention measures is needed to build up the comprehensive cyber security architecture for port services by exploiting the threat analyzes for cyber security measures for the SMARTER project. This study answers to the question, "Why cyber security management is so important in future smart ports system of systems environment?"

We have seen in a short timelapse how essential factor workable fairways and ports functions are. War in Ukraine and its derivative effects generated pressure on the vital functions of many countries and overall

continuity management. Economic balance becomes unstable easily when basic needs cannot be taken care of. Hybrid warfare consists, e.g., of exploited physical and cyber extortions. In Ukraine, we have seen that both elements have been used. Realized cyber threats create essential obstacles to maritime traffic and business continuity. In international business, we have to ensure that the functionalities of passenger and cargo traffic do not stop.

Criminal influences are trying to make our atmosphere unstable. Hybrid influencing is changed to hybrid warfare. As Simola & et al. (2021) wrote, fundamental risks effects decision-making culture and the whole cyber ecosystem. It is crucial to protect the harbor's cyber- and the physical environment against threats. Why it is important to try to understand attackers' motivation. Why is it important to create threat scenarios?

As terrorist actions in the Baltic Sea area and energy extortion are proven, every trade partnership between East and West is an opportunity and a risk. If decision-makers invest too much in the risk trade, we also create the possibility of risks spreading as a chain effect. One realizing threat affects another sector. A moment ago, leaking and exploding gas pipelines limited cargo vessels and passenger traffic in the Baltic Sea. After the terrorist attacks, Russia continued to spread disinformation (Financial Times, 2022).

2. Situational awareness in smart ports

As Endsley (1995) argues, the formation of situational awareness depends on the capabilities of perception and other individual factors. Individual thinking depends on many variable factors. Feelings affect our understanding and relationships related to the environment under consideration. An automated or semi-automated system requires capabilities to maintain situational awareness. It has been seen as necessary to monitor IT and OT systems itself and networks, but there is a need for harmonized situational awareness of Command and control -functionalities. Information exchange about cyber-physical threats has to be one of the system's core functions. SItuation center in the Port area needs a backup system if activities of the situation center are interrupted.

At present, a Cyber-Physical system is more often a system where IT and OT are linked or unified with Artificial Intelligence-based features. In this context, transportation, including trains, cars, trucks, airplanes, vessels, and boats, form the central functional wholeness where the main aim is to govern all necessary transportation-related issues effectively and securely. AI-based or combined solutions such as the Industrial Internet of Things (IIoT) create challenges for business continuity management. Figure 1 below illustrates systems of system-level approach interacts with other relevant factors (cyber and physical layers with human interaction).

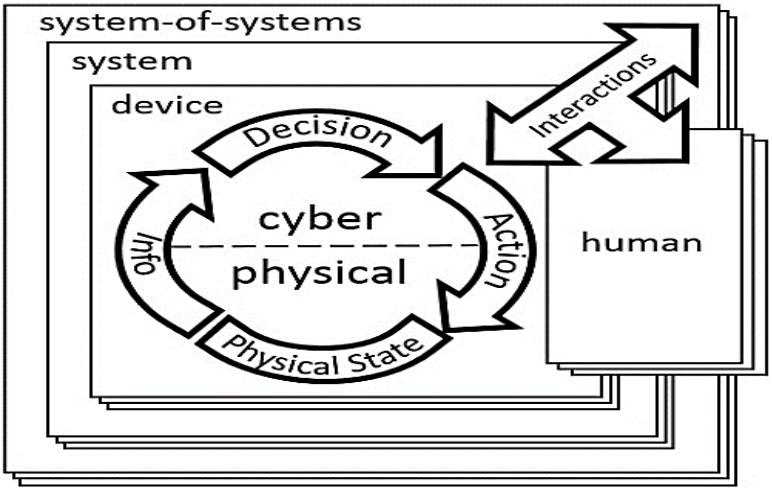

Figure 1: Cyber-Physical system of the system (NIST 2017)

Cyber-physical systems interact as part of the cyber ecosystem where cyber and physical stages combine work inputs. Human is still the primary decision-maker and actor that causes potential threats and challenges to business continuity management in many ways. It has been said that humans are the weakest players in work processes and procedures.

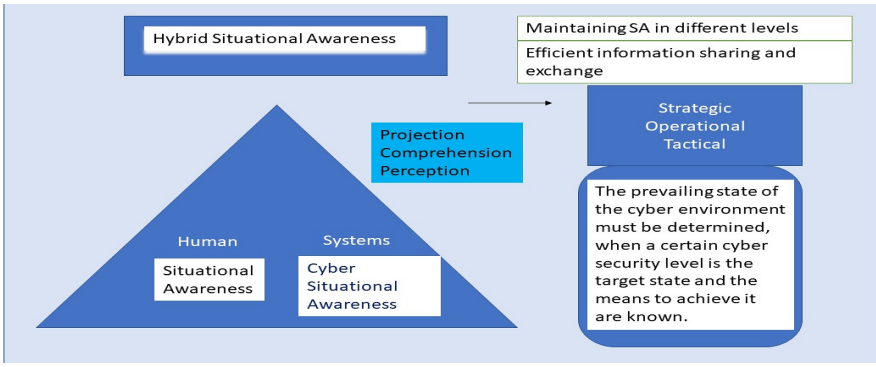

Figure 2: Formation of hybrid situational awareness in different levels

Stakeholders of the harbors have to create a preliminary risk assessment where every potential threat has been considered. As we have seen in previous studies related to Simola & et al. (2021) realized hybrid threats where cyber and physical risk elements are combined based on crucial human factors. It is not appropriate that risk classifications have been done separately from other risk assessments. Cyber risk assessment is one part of overall risk assessment. Figure 2 illustrates how the formation of hybrid situational awareness depends on determining the goal state of situational awareness in different analysis levels. Achieving and maintaining situational awareness at the goal state requires a coherent strategic, operational and tactical level of semantic functionalities where human and system-based information is shared understandably. The capability to understand threats and events creates a fundamental base to maintain everyday situational awareness. Prevention measures are equally important.

As Figure 3 illustrates, critical elements of the port have to analyze precisely. Port functionalities are an essential part of Critical Infrastructure. The risk management framework supports the decision-making process, in which critical infrastructure operators or partners undertake to cooperate in influencing the selection of risk management measures. It is designed to provide flexibility across all sectors, geographies, and across partners. It can be tailored to different operating environments and applies to all threats (DHS, 2013)

Figure 3: Critical Infrastructure Risk Management (DHS 2013)

The risk management concept allows operators of critical infrastructure (e.g., Security Operations Center) to focus on those threats and hazards that are likely to cause harm and to use approaches designed to prevent or mitigate the effects of these incidents. It also increases security and strengthens resilience by identifying and prioritizing actions to ensure the continuity of key operations and services and support enhanced response and recovery. In order to effectively risk management of critical infrastructure, port operators and stakeholders must identify (infra) the essential functions, systems, and networks necessary for their continued operation, taking into account the related dependencies and interdependencies. This dimension of the risk management process should also identify information and communication technologies that enable essential port services. Cybersecurity plans have to be a part of overall risk management activities, where policies, processes and procedures are defined and implemented.

We have many examples of how multi-activities in the maritime sector may expose stakeholders to cyber-physical influences, not only port activities. Harbors, ports, and fairways are crucial logistical parts of the critical infrastructure. NotPetya Malware affected, for example, A.P. Moller – Maersk In 2017. NotPetya was loaded onto one computer situated in the local office that was connected to the Maersk global network. Despite the fact that the company was not the intended target of the attack, it made all its applications and data unavailable. The whole logistical business chain and all operations were interrupted. The case proves that centralized ownership and control of functionalities create new business possibilities and also threats. If one employee would not open and respond to the infected email, or if the intrusion prevention mechanism had blocked the malware, the chain reaction would not have occurred (Stormshield, 2022).

3. Cyber-threat model for Smart Terminal

Identifying cyber threats is further complicated by the difficulty in defining the boundaries between national, international, public, and private interests. Because threats in cyberspace are global and involve rapid technological developments, the struggle to meet them is ever-changing and increasingly complicated (Lehto, 2013).

According to Bodeau, McCollum & Fox, (2018), the word threat is used to refer to the adversary or the attack depending on the context. In the paper of "Cyber Threat Analysis in the Remote Pilotage System" (Kovanen, Pöyhönen, Lehto, 2021) is drafted a classification model for six threats based on motivational factors: cyber vandalism, cybercrime, cyber espionage, cyber terrorism, cyber sabotage, and cyber warfare. The motives can be reduced to their very essence: egoism, anarchy, money, destruction, paralysis, and power. The model was modified from Myriam Dunn Cavelty's structural model (Dunn Cavelty, 2010; Ashenden, 2011; Lehto, 2013).

There is a need to describe the actual attackers and their actions behind archetypes. Mitre's ATT&CK database (Strom et al., 2018) provides an updatable list of detected techniques, tools, and groups. The groups are tied to tactics, techniques, and tools they have been observed to use.

All the knowledge about the actor, attack techniques, and vulnerabilities must be available. It requires precise shared terminology and a method for transferring knowledge and information. The terminology should be able to address issues of varying abstraction levels and evolve with new concepts (Red Canary, 2021; ESET, 2019). ATT&CK also supports ICS and mobile system attack descriptions (Alexander, Belisle, & Steele, 2020; Strom et al., 2018).

Often cyber-attacks are associated, for example, with social or economic disputes, and the actions in the cyber domain may follow or be uncorrelated with events in the physical world (Gandhi et.al., 2011). Identifying the circumstances that might trigger an attacker archetype can be valuable in predicting heightened risk related to various situations.

Understanding the motivations and capabilities of different archetypes limits the number of scenarios and thus makes evaluation feasible for the defender. The motivation affects the attacker's targeting and methods. While a vandal seeks visibility by defacing a website, a spy wishes to stay unnoticed to gain information. The varying level of capability restricts some of the attackers from achieving their goals (Bodeau, McCollum & Fox, 2018).

The cyber vandalism may cause a chain reaction in a case where communication between VTS and an unknown vessel via a VHF channel or email is interrupted by a state actor. The arrival of an unknown vessel in a harbor area might trigger a chain reaction. The extended problem may arise if the same ICT systems are also in use in an enemy state's maritime transportation (Fintraffic, 2022). The awareness about the adversary that carried out the cyber-physical attack may be unclear. Cyber espionage can include business or political espionage. Political factors may arise from national or international issues. From the national side, hacktivism supporting strikes in the harbor could be one scenario. In the worst case, international tensions in the region could escalate to military cyber operations against vessel traffic. The parameters of the attacker archetypes are presented in Table 1.

Table 1: Attributes of the attacker archetypes. Capability is derived from Bodeau, McCollum and Fox (2018), and impacts are derived from Mitre (2020, 2022a, and Kovanen, Pöyhönen, Lehto, (2021).

	Vandalism	Crime	Espionage	Terrorism	Sabotage	Warfare operations
Motivation and goal	Political change based on personal political or ideological motives. Egoism gain	Making money through fraud or from the sale of valuable information. Financial gain	An economic, political, or military advantage. Information gain	Social instability and influencing political decision-making. Anarchy gain	Instability, chaos, political change, and infrastructure paralysis. Paralysis gain	A destructive attack on a nation's digital infrastructure. Political or military dominance

	Vandalism	Crime	Espionage	Terrorism	Sabotage	Warfare operations
Target	Digital services of governments and companies, individuals' information systems	Digital services of governments and companies, individuals' information systems	Data and information about governments and companies	Data and information about governments and companies. Critical infrastructure	Nation's critical infrastructure	Nation's critical infrastructure (civilian or military).
Capability	Acquired Attackers with moderate or limited expertise	Augmented Attackers with moderate or limited expertise	Advanced Attackers with very sophisticated or moderate expertise	Advanced Sophisticated attackers, capable of multiple, coordinated attacks	Integrated Very sophisticated attackers, capable of multiple, coordinated, continuous attacks	Integrated Very sophisticated attackers, capable of multiple, coordinated, continuous attacks
Trigger	A social event, an action of a company or an individual	The opportunity for economic gain	The need for political, economic, and military information	Cultural, nation's political or military actions	Testing own offensive cyber-attack capabilities, preparing hybrid or military operations	Achieving political or military objectives through military cyber operations

For Smart port, the model of cyber-threat folds around the threat archetypes and their features. The actions they make are described with a set vocabulary provided by ATT&CK.

4. Smart Terminal System-of-systems architecture

The case of port in the maritime transportation system includes processes to produce all needed services, as the ship approaches from an open sea via a fairway to berthing to a pier, general port services, port logistics, and connections to land transportation. There are identified the key elements associated with processes used in the smart terminal in figure 4. These are Activities, Stakeholders, Organizational relationships, Security dimensions, Security capabilities, and Criteria. It is also evident that this entity needs communication systems within process elements and electricity systems to support the functions of processes. In all cases of port processes, the information requirements and the amount of information needed are related to the reliability of safety and security services. Cyber security awareness and information should cover all process elements. Figure 4 presents typical port elements for cyber security investigation.

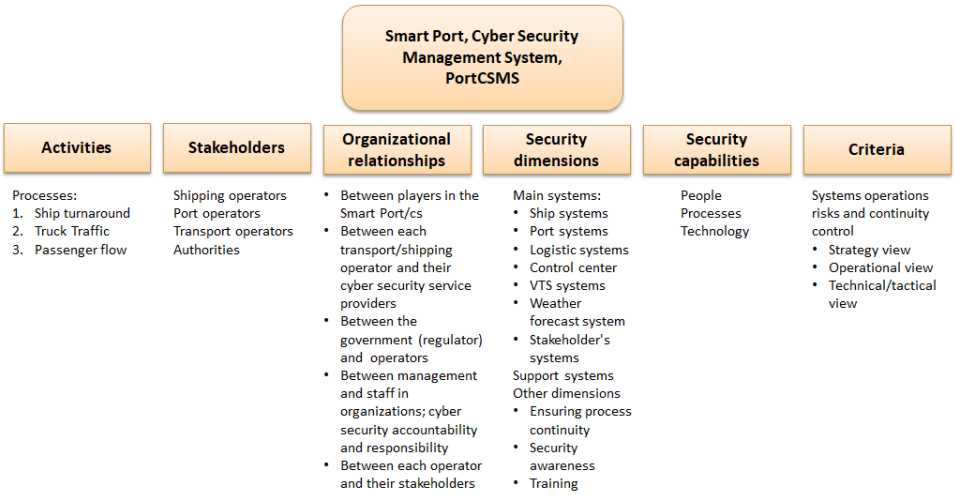

Figure 4: Elements of smart port cyber security management, Port CSMS.

In the SMARTER research project is acknowledged that there is a need for new technologies and solutions that are necessary to tackle the challenges set by the use cases (DIMECC, 2020). It is identified as a set of technologies and solutions that belongs to the terminology of Industry 4.0, like big data, data lake, data analytics, information fusion, AI, 5G, IoT, edge processing etc. It is reconditioned in the article of "Cybersecurity Risks and Automated Maritime Container Terminals in the Age of 4IR (Fourth Industrial Revolution)" by Peter Beaumont (2018) that the risks derived from the use of technology associated with the Fourth Industrial Revolution (4IR) are both real and dangerous unless appropriate control measures are implemented" (Beaumont, 2018). It is also important to recognize and have knowledge of legacy systems in use with a different timeframe of technology solutions. In that sense, the SoS environment of the port process is complicated from a technological point of view. In this SMARTER cyber security research, either new and legacy technologies should be covered in bout security dimensions, main and support systems of the case.

Smart ports cyber threats should need to be investigated and taking into account in system of systems (SoS) environment Information and Communication Technology (ICT) and Industrial Control Systems (ICS). The threat investigation of all systems should cover legacy and Industry 4.0 technology vulnerabilities because these systems are either critical for information security or cyber-physical effects. The findings from these systems provide the basement for evaluation and development of a cyber-threat analysis and are suitable for port cyber security architecture solutions.

5. Making threat analyses

We have used the Delphi method principle in order to make a relevant general threat analysis from the port systems. The members that have been involved in this analysis process are researchers and research methods. Cybersecurity experts from the research program advocate Delphi: “The Delphi method is an iterative process to increase consensus-building and at the end to have consensus among an experts from an examine case. The Delphi method is part of quantitative as a means to achieve an optimally reliable expert consensus.” It could have on one of three objectives (Garson, 2012): A) Forecasting future events, B) Achieving policy consensus on goals and objectives within organizations or groups, C) Identifying diversity in and obtaining feedback from stakeholders in some policy outcome.

Table 2 illustrates the results of Delphi method research on the port systems and subsystems. It has been done to forecast general or main future events conducted for the impacts and risk evaluation processes in the later phase of this research work. Cybersecurity researchers' and experts’ contributions are related to the main threats/attacks and the techniques. The evaluation has collected information about the threat agent involved, the attack that will be used, the vulnerability involved, and the possible approach of a successful exploit on the operation of the system. Categories of the systems are impossible to define clearly, because of the overlapping functions of the system's functionalities. Therefore same threat occurs in different system categories. It has also been challenging to determine clearly, was it IT or OT systems under the attack. Often cyber attacks affect both.

Table 2: Port systems and subsystems; main threats/attacks, related techniques (Mitre, 2020, 2022a, 2022b, 2022c, 2022d; Pöyhönen, J., Hummelholm, A., Lehto, M., 2022).

System/ Subsystems	Main threats/attacks	Software	ATT&CK technique	Threat prevention technologies
Ship systems	• Brute Force • Credential Theft • Physical Access • Denial of service (DoS) • Eavesdropping	• S0437 Kivars Remote services • Hardware or Software Keylogger	• T1110.001 -003 Password guessing, cracking, spraying, • T1111,T1621 MFA interception & request generation • T1556 Modify Authentication Process • T1552 Unsecured credentials • T0847 Replication Through Removable media	• M1032 Multi-factor Authentication • M1018 User Account Management • M1036 Account use policies • M1027 Password Policies • M1017 User Training • M1053 Data Backup • M0934 Limit Hardware Installation • M0928 Operating System Configuration
Port systems	• Man in the Middle • Jamming • Changing setpoints	• Hardware or Software Keylogger • S0504 Industroyer	• T1557.001-003.Adversary-in-the-Middle • T0860 Wireless compromise	• M1017 user training • M0931 Network Intrusion Prevention • M0947 Audit • M0802 Communication authenticity

System/ Subsystems	Main threats/attacks	Software	ATT&CK technique	Threat prevention technologies
	• Physical Access	• S0603 Stuxnet	• T1087 Account discovery	
Port logistic systems	• Physical Access • Virtual Access • Eavesdropping via malware	• Hardware or Software Keylogger • S0603 Stuxnet • S0604 Industroyer	• T0839 Module Firmware • T0842 Network Sniffing • T1485 Data Destruction • TO860 Wireless compromise	• M0808 Encrypt Network Traffic • M0806 Minimize wireless signals • M1053 Data Backup
Control center systems	• Credential Theft • Ransomware	• S0603 Stuxnet • S0125 Remsec • S0604 Industroyer • S1009 Triton	• T1110-003 Password guessing, cracking, spraying, • T1111,T1621 MFA interception & request generation • T1556 Modify Authentication Process • T1552 Unsecured credentials • T1562 Impair Defenses • T0803 Block Command Message	• M1031 Network Intrusion Prevention • M1018 User Account Management • M1022 Restrict File and Directory Permissions • M1024 Restrict Registry Permissions • M0804 Human user authentication • M0807 Network Allowlists • M1053 Data Backup
VTS system	• Attacks from Internet • Insider Attacks • DoS Attacks • API based Attack	• S0266 Trickbot • S0363 Empire	• T1059 Command and Scripting Interpreter • T1562 Impair Defenses • T1056.004 Input Capture: credential API hooking • T1071 Application layer • T1499 Endpoint DoS	• M1021 Restrict Web-based content • M1031 Network Intrusion Prevention • M1037 Filter Network Traffic
Weather forecast system	• Attacks from Internet • Insider Attacks • Credential Theft • DoS Attacks • DDoS • API based Attack • Ransomware Attacks	• S0125 Remsec • S0604 Industroyer	• T0918 Wireless sniffing • T1548 Abuse Elevation Control Mechanism • T1087 Account Discovery: Local Account • T0803 Block Command Message • T1486 Data Enrcytped for Impact	• M0948 Application Isolation and Sandboxing • M0950 Exploit Protection • M0930 Network Segmentation • M1047 Audit • M0814 Out-of Band Comm. Channel • Black Energy -malware toolkit • M1040 Behavior Prevention on Endpoint
Stakeholder`s systems	• Phishing • Brute Force	• S0367 Emotet • S0266 TrickBot •	• T1566.001 Phishing: Spearphishing Attachment • T1087 Email discovery	• M9031 Network Intrusion prevention • M0930 Network segmentation • M1036 Account use policies
Power supply systems	• DoS - Impacts on the ICS (combined effects)	• S0604 Industroyer • S0603 Stuxnet	• T0855 Unauthorized Command Message • T0816 Device Restart	• M0801 Access Man. • M0802 Communication authenticity • M0937 Filter Network Traffic • M0930 Segmentation • M0813 Software Process and Device Authentication

In an ICT environment, it is essential to collect a knowledge base about the general-level port activities and how the systems are connected. For that analysis, Mitre has created a usable framework in this context (Mitre, 2022d). In the cyber-physical environment, we have to notice also signal-based threats such as Electromagnetic interference (EMI), which is an increasing threat factor in the wireless communication environment.

Because of digitalization, combined IT and OT systems often mean that the operational technology is linked to the system connected to the public network. Crucial threats from external factor cause challenges in port facilities because OT and IT Systems often communicate with each other in internal and external networks. It is essential how employees use their internet access. Adversaries may deploy vulnerabilities by scanning and sniffing the target network, e.g., by using spear-phishing attachments in emails or packet sniffer or wireless analyzer so that crucial port processes (for example, cargo handling or access control system) may stop. The malware can also get to the internal network via a USB plug-in. Human errors with poor identity & access management are essential threats. Therefore accurate responsibilities and tasks for key crew members have to be done. If port operations are suspended for a long time, it will affect the entire logistics supply chain and expenses will increase.

The similarity of the threats indicates the importance of protecting information and its sharing and storing practices. For that aim, the CIA technique consists of guides for policies to form information security within an organization. Confidentiality, Integrity, and Availability (CIA) feature. Confidentiality means that information is only accessible to those involved. Integrity or correctness of information means that the information must be true and correct. Availability means that information is available when you want to use the data subject's data.

Elements of the CIA should be implemented throughout the cybersecurity-managed IT services and other security-related management. The right to privacy or the rights of the data subject required by data protection cannot be fulfilled without the implementation of the data security attributes. Cyber threats create significant challenges for trusted information sharing. Protecting port activities require common guidelines for cyber security rules.

For example, ISO/IEC 29134:2017 gives guidelines for a process on privacy impact assessments (PIA) and a structure and content of a PIA report. It is applicable to all types and sizes of organizations, including public companies, private companies, government entities, and not-for-profit organizations (ISO, 2017).

The Mitre framework uses three terms in an ICS environment; *denial*, *loss*, and *manipulation*. Denial is a condition that occurs only while the attack is active. Loss refers to the sustained loss of an asset that continues after the active malicious interaction has ceased. Manipulation alters the asset and can be either loud and easy to detect or subtle and longer sustained. According to previous research (Kovanen, Pöyhönen & Lehto, 2021), we have described the attacks as follows:

- **Manipulation of view** is a more inconspicuous attack type than denial or loss of view. Slightly falsified data are harder to detect than missing data. Consequently, the affected system operator loses correct situational awareness. The effect spreads to all connected systems and operators using the manipulated view.
- **Denial of Service attacks** can be carried out by affecting the endpoint or the network that leads there. In either case, the service is unavailable for use.
- **Data destruction, data encrypted for impact, disk wipe and service stop,** prevent the use of the data and services. System shutdown/reboot can be used to make systems inaccessible faster by, for example, rebooting after wiping the master boot record.
- **Loss of Safety** is dangerous, especially with cyber physic systems as the result may cause injuries or death when the safety mechanism of a system is disabled. Even a threat of this type of circumstance can delay reaction to other impact types if a human operator is not able to initiate countermeasures due to a fear of unsafe working conditions.
- **Data manipulation** is harder to detect than data destruction if the manipulation is subtle. Systems and operators can continue to act but they base their decisions on false data.

6. Conclusion

The Finnish smart port research program concerns port services for ship turnaround, truck traffic, and passenger processes. Smart ports are enormous mixtures of legacy technology and the development of new apps. The potential for cyber attacks on systems is always present and evolving along with digitalization. All emerging vulnerabilities associated with the interconnection of ICT and ICS/OT layers in smart terminals must be thoroughly assessed.

The threat investigation of ICT and ICS/OT systems of smart ports poses a severe impact on maritime processes in harbor areas. The analysis indicates that system-level thinking is necessary when the purpose is to understand the dependencies of the threat sources and attack vectors. One threat factor affects another that may combine different threat levels from each other. Distributed systems with separate departments or functions may not provide protection in this case. Outsourced services create their challenge. Therefore, it is essential to deploy standards and other industry rules. Without a common understanding of procedures and processes regarding workflow, threat prevention is not possible to take control. Information security and technology have to be based on common standards, certificates, and protocols. Recommendations that we have on shipboard networks should be of the same level in the cyber port ecosystem as well. Business continuity management has to take into account every technical solution that is planned to deploy in this maritime ecosystem.

Port owners form an essential entity for management when the cyber ecosystem has to manage understandably and easily. There is a challenging example where control of the port entity is divided abroad and added challenges arise from a subsidiary arrangement. The system of system-level design depends on how the ecosystem is governed. Coordination and control of the activities influence how ICT and ICS/OT technologies support each other in the port area and other connected functions. Official National Cyber Security Center Traficom has a Havaro mechanism that monitors internet traffic by using a commercial Security Operation Center that gathers different companies under the sector-based communities. It is recommended to get all port actors involved and connected to the umbrella of the service. Additionally, it is necessary to increase attention to educating employees on cybersecurity activities. Human resource management affects how stable or weak human resources are in a digitalized cyber-physical environment.

This paper provides a research approach to threat identification of the system element of the smart terminal processes. The research approach uses the system of systems (SoS) thinking. The findings of the study are related to the coverage of multiple main threats in port services. Information flows in and between systems as well as electricity supplies in the port process.

References

Alexander, O., Belisle, M., and Steele, J. (2020). “Mitre ATT&CK® for Industrial Control Systems: Design and Philosophy”.

Ashenden, D. (2011). “Cyber Security: Time for Engagement and Debate”, Proceedings of the 10th European Conference on Information Warfare and Security, the Institute of Cybernetics at the Tallinn University of Technology.

Bodeau, D.J. and McCollum, C.D. (2018). “System-of-systems Threat Model”, The Homeland Security Systems Engineering and Development Institute (HSSEDI) MITRE, Bedford.

Bodeau, D.J., McCollum, C.D. and Fox, D.B. (2018) “Cyber Threat Modeling: Survey, Assessment, and Representative Framework”, Mitre Corp, Mclean.

DHS, (2013). NIPP 2013 - Partnering for Critical Infrastructure Security and Resilience.

DIMECC Oy, 2020. DIMECC Sea4Value/Smart Terminals (SMARTER). Project proposal for One Sea – autonomous maritime ecosystem.

Dunn Cavelty, M. (2010). “The Reality and Future of Cyberwar”, Parliamentary Brief, 30 March 2010, [online], www.parliamentarybrief.com/2010/03/the-reality-and-future-of-cyberwar.

Endsley, M.R. (1995). A taxonomy of situation awareness errors, human factors in aviation operations. Proceedings of the 21st Conference of the European Association for Aviation Psychology (EAAP). 3. 287-292.

ENISA. (2017). Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends.

ESET. (2019). “The MITRE ATT&CK Framework: Everything You Need to Know in Under 60 Minutes ”, [online], https://www.eset.com/us/business/resources/webinars/the-mitre-attck-framework-everything-you-need-to-know-in-under-60-minutes-1/.

Financial Times. (2022). Sabotage of gas pipelines a wake-up call for Europe, officials warn. https://www.ft.com/content/ad885fea-035f-4b93-98e7-c75da2c308f8

Fintraffic. (2020). GOFREP. https://www.fintraffic.fi/sites/default/files/2021-09/GOFREP_MG_2021_09_03.pdf

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. and Laplante, P. (2011) “Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political”, IEEE Technology and Society Magazine, Vol. 30, No. 1, pp 28–38. doi: 10.1109/MTS.2011.940293

Garson, G. D. (2012). The Delphi method in quantitative research. Asheboro, NC: Statistical Associates Publishers. Available from: https://faculty.chass.ncsu.edu/garson/PA765/delphi.htm, retrieved 25.1.2022

International Organization for Standardization (ISO). (2017). ISO/IEC 29134:2017 guidelines for privacy impact assessment. Retrieved from https://www.iso.org/standard/62289.html

Kovanen, T., Pöyhönen, J. & Lehto, M. (2021a). Cyber Threat Analysis in the Remote Pilotage System. Presented in ECCWS 2021 - 20th European Conference on Cyber Warfare and Security. 24th - 25th June 2021, Chester, UK. doi: 10.347190/EWS.21.067

Lehto, M. (2013). "The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies", International Journal of Cyber Warfare and Terrorism, Vol. 3, No. 3, pp 1–18.
Mitre. (2020). "ATT&CK®for Industrial Control Systems",[online], https://collaborate.mitre.org/attackics/index.php/Impact
Mitre. (2022a). "Impact", [online], https://attack.mitre.org/tactics/enterpise
Mitre. (2022b). "Software" [online], https://attack.mitre.org/software.
Mitre. (2022c). "ATT&CK Matrix for Enterprise", [online], https://attack.mitre.org/.
Mitre. (2022d). "Attack Navigator", [online], https://mitre-attack.github.io/attack-navigator/
NIST. (2017). Special Publication 1500-201 Framework for Cyber-Physical Systems: Volume 1, Overview
Pöyhönen J., Hummelholm A., Lehto M. (2022). Cybersecurity risk assessment subjects in information flows. 21st European Conference on Cyber Warfare and Security, 16th – 17th June 2022, Chester, UK, pages 222-230. doi: 10.34190/eccws.21.1.263
Red Canary. (2021). "2020 Threat Detection Report", [online], https://redcanary.com/threat-detection-report/.
Simola J., Lehto M., Rajamäki J. (2021). "Emergency Response Model as a part of the Smart Society", Proceeding of the 20th European Conference on Cyber Warfare and Security, pp. 382-391. doi: 10.34190/ews.21.079
Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G. and Thomas, C.B. (2018) "Mitre Att&ck: Design and Philosophy", Technical report.
Stormshield. (2022) Port cyberattack: hackers & maritime cybersecurity, https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/