*Applied Human Factors and Ergonomics (AHFE2025),* Vol. 199, 2025, 2302–2308
https://doi.org/10.54941/ahfe1007042

# Secure Resilient Maritime Logistics: Seaport Threat Analysis

**Markus Sihvonen**

University of Jyväskylä, Jyväskylä, Finland

## ABSTRACT

Maritime logistics form the backbone of global trade by handling approximately 90% of worldwide commerce by volume. Since global supply chains grow more interconnected and demand for just-in-time delivery increases, the resilience and robustness of maritime logistic systems have become more critical than ever. Today digital systems manage every aspect of the logistic operations. Therefore, protecting maritime logistics from cyber threats is essential to guarantee flow of goods globally. From port infrastructure to shipping route stability, the ability to maintain efficient logistic operations in the face of digital systems disruptions is essential for economic stability and growth of many countries. Maritime sector evolves due to development of new digital technologies. This offers new attack opportunities for hackers that are too often protected by rogue nations. Therefore, robust maritime logistic system that integrates well with on road and railway transportation is no longer a luxury but a necessity. Building such systems requires investment, innovation, and international collaboration. The future of maritime logistics depends not only on how fast and far goods move, but how reliably and securely they do so under any condition. Therefore, it is important to fully understand what are potential threats for global maritime logistics. A robust maritime logistic digital system is one that can anticipate, absorb, adapt, and recover from disruptions, whether they are caused by natural disasters, cyberattacks, geopolitical tensions, pandemics, or economic shocks. Robustness is not about avoiding disruption entirely but about minimizing impact and ensuring rapid recovery. Key pillars of robustness include understanding real-time operational status, maintain adequate backup systems, plan and utilize available resources dynamically, conduct risk assessment and plan crisis response. Resilience is not solely a maritime issue. It depends heavily on how well sea transport integrates with land logistics such as rail and road transportation. Therefore, robust maritime systems require coordinated infrastructure development with land based logistic operators that utilize latest technologies such as automated driving and autonomous vehicle fleet management. No nation can ensure maritime resilience alone. Global supply chains demand cross-border cooperation and policy alignment. This paper analyses potential threats for maritime logistic systems in seaports that are critical focal points for goods enroute to final customers.

**Keywords:** Cyber and cyber physical threats, Threat discovery, Maritime logistics, Seaport security

 

## INTRODUCTION

Seaports function as major logistic hub between land and sea transportation systems. For secure, efficient operations seaports must provide safe operational environment for its operations (Progoulakis, Nikitakos, Dalaklis and Yaacob, 2022). Therefore, for a resilient seaport operation, one must have thorough understanding of human and technology factors and processes in seaports. Human factors in threat analysis refer to how humans interact with IT/OT systems, technologies, environments, processes and how these interactions influence cyber security status and robustness of maritime logistic operations. Digital technologies are essential for vessels operating in the seas and in seaports operated by people (Pseftelisa and Chondrokoukis, 2021). The focus is in understanding how people interact with critical logistic IT/OT systems, what behaviours they are likely to exhibit under pressure or distraction, and how design of critical logistic system, training of personnel, and policy can influence vulnerability of a critical logistic system. Human factors' threat sources can be classified for two main types: 1) Insider threat, and 2) human error including negligence. The study has shown that human carelessness is significant safety factor for maritime IT/OT systems (Kanwal, Shi, Kontovas, Yang and Chang, 2022).

Technology factors are essential for understanding vulnerabilities and attack surfaces in maritime logistics. This includes integration of new digital systems, automation, and critical IT/OT systems into logistic operations. Technological transition from legacy logistic systems towards modern, automated systems, requires a robust regulatory framework that enables resilient operations (Hu and Yang, 2024). Technology focused threat analysis emphasizes characteristics, configurations, interdependencies, and limitations of used hardware, software, networks, and cyber-physical systems that support the logistic operations. Also, third-party integrations are included to the analysis. Legacy systems are manifested often by old, not updated operating systems, poorly segmented local area networks and networks' system architecture, inadequate intrusion and anomality detection. Particularly in seaport threat analysis, technology factors shape the attack surface and determine how well a critical system can resist, detect, and recover from cyber and physical threats. A thorough seaport threat analysis should map all technology assets, assess vulnerabilities and interdependencies. Therefore, properly designed and implemented digital maritime infrastructure is essential for robust and reliable maritime logistic operations (Pöyhönen and Lehto, 2023).

A threat analysis for processes in maritime logistic systems focuses on identifying and assessing risks across the operational workflows that support the movement of cargo, vessels, and information through maritime transport chains especially at ports and in integrated logistics hubs with road and rail transportation. The focus is in the end-to-end processes, including both technical and human elements, data exchanges, and inter-organizational dependencies. Typical processes are vessel's arrival to seaport, berthing and departure. While a vessel is at seaport, main processes are its cargo handling

including cargo's integration to with road and rail logistics, custom clearance and port community systems (PCS) operations.

It is important to address both cyber threats and cyber-physical threats in maritime logistics simultaneously since it is a hybrid environment of IT systems, OT infrastructure, and physical processes. Therefore, it is vulnerable to both categories of threats often in interconnected ways. Cyber threats target information systems, data, and digital services. Cyber-physical threats cause physical effects on equipment, infrastructure, or people and are due to a criminal or unintentional cyber actions.

## THREAT MODELLING

Performing cyber threat and cyber-physical threat analysis for maritime logistics and seaports involves understanding unique operational and information technologies used in the industry. Additionally, it is required to understand physical systems used in seaports, ships and in transportation generally. Then it is possible to identify and analyse potential attack vectors, threat actors, and potential impacts to critical maritime logistic operations. The distinction between cyber threats and cyber-physical threats is crucial for understanding risk across both digital and operational domains. Maritime logistics, being a hybrid of IT systems, OT infrastructure, and physical processes, is vulnerable to both categories of threats and often in interconnected ways. Therefore, threat analysis objectives are to:

- identify threats that disrupt, degrade, or manipulate critical maritime logistics processes
- highlight cyber, cyber-physical, and organizational risks
- find process interdependencies and supply chain exposures
- recommend mitigations on technical infrastructure
- recommend mitigations for the process.

Commonly used threat modelling tools STRIDE, MITRE and PASTA support efficient threat discovery for critical systems. The STRIDE threat modelling framework is a systematic approach developed by Microsoft to help identify security threats during the design phase of software systems (Microsoft Corporation (n.d)). It provides a structured way to think about potential vulnerabilities by categorizing them into six types of threats. Applying the STRIDE threat modelling framework to a seaport environment to critical IT/OT systems helps to identify and categorize security threats that could impact port operations, logistics, cargo handling, navigation and safety. The MITRE threat modelling framework generally refers to tools and methodologies developed or curated by the MITRE Corporation to support cyber threat intelligence, defensive security, and threat modelling (MITRE Corporation. (n.d.)). MITRE ATT&CK is a knowledge base of real-world adversary behaviour, focusing on the Tactics, Techniques, and Procedures (TTPs) that attackers use at each stage of an attack. The PASTA threat modelling framework, short for Process for Attack Simulation and Threat Analysis, is a risk-centric and attacker-focused methodology

designed to help organizations model threats in a structured and business-aligned way. It differs from simpler frameworks like STRIDE by being more comprehensive, especially for complex systems such as critical infrastructure, OT/IT environments, and enterprise applications. PASTA is a 7-stage threat modelling process that aligns technical security analysis with business impact and risk management (Velez and Morana, 2015).

## VULNERABILITY ASSESSMENT

A vulnerability assessment is the process of identifying, quantifying, and prioritizing security vulnerabilities in systems, networks, applications, and infrastructure. It helps organizations understand their attack surface and take proactive steps to reduce security risk. A good vulnerability assessment has seven steps that are described in the Table 1.

**Table 1:** Vulnerability assessment process.

| Phase | Description |
|---|---|
| Define Scope | Decide what to evaluate: Systems, networks, web apps, OT devices, cloud assets? |
| Asset Discovery | Identify all assets hardware, software, services that in defined scope. |
| Vulnerability Scanning | Select tools to detect known vulnerabilities. |
| Analysis & Validation | Evaluate findings, remove false positives, and validate critical issues. |
| Risk Prioritization | Rank vulnerabilities based on exploitability, asset value, and business impact. |
| Reporting | Document vulnerabilities, affected assets, risk levels, and recommended remediations. |
| Remediation & Re-testing | Fix discovered vulnerabilities. Redo vulnerability scanning to verify fixes. |

The Common Vulnerability Scoring System (CVSS) is widely used for ranking of vulnerabilities (Forum of Incident Response and Security Teams, 2023). It considers exploitability, impact and remediation complexity of discovered vulnerability and user interaction required to solve it. The CVSS score can be from 0.1 to 10.0 where the highest score indicates critical severity of a vulnerability (Mell, Scarfone and Romanosky, 2007). The benefits of the vulnerability assessment are to identify security gaps based on known risks and therefore attack surface is reduced. It is also easy to execute, cost effective and helps organization comply with cyber security regulations.

## SEAPORT THREAT ANALYSIS

In seaport's operational environment, resilience is anticipation of threats and contingency planning for disruptions of critical operations. High level

of resilience in seaports is capability to continue delivering services to its clients despite potential threats to its critical operational systems (Tsoulfas, 2025). The maritime operational environment has unique challenges including outdated legacy systems, different cyber security maturity levels and heterogeneous system architectures among stake holders (Clavijo, Patino-Rodriguez, and Guevara, 2024). This section analyses vulnerabilities and cyber threat focusing on commonly used OT systems, IT systems, network solutions and external interfaces in seaports in Finland.

The threat analysis is using publicly available information from Finland's most active cargo seaports. The seaports operations deal with bulk materials such as timber, paper, chemicals, ore and flammable liquids. They have facilities for container ships and tankers. Critical OT systems include loading cranes, Vessel Traffic Service (VTS), Programmable Logic Controllers (PLCs), Closed-Circuit Television (CCTV) system, Supervisory Control and Data Acquisition (SCADA) system, access gates and various sensors. The seaports have also Terminal Operating System (TOS), Port Management System (PMS), Enterprise Resource Planning (ERP) system, and integration, customs' systems and other external interfaces for shipping companies, logistic providers and other government agencies. They also have local area fibre and wireless networks and remote access is enabled to certain level.

The Table 2 depicts results of the seaports threat analysis where STRIDE and MITRE threat frameworks where utilised. Applied risk assessment helps to identify risk level for a given threat category and its impact for a seaport's operations if realised. It directs seaport administrators to conduct further detailed cyber threat analysis of the most critical systems at first. Next step would be executing analysis with PASTA for business impacts caused by discovered threats for a seaport.

**Table 2:** Seaport threat analysis.

| Category | Threat | Impact | Risk Assessment |
|---|---|---|---|
| Spoofing | Leaked credentials for TOS and VPN access. | Unauthorized access to cargo management | Risk level – High<br>Impact – High |
| Spoofing AIS | Fake vessel location | Maritime safety disruption | Risk level – Medium<br>Impact – High |
| Tampering | Data tampering in customs declarations and cargo manifests | Smuggling illegal substances<br>Avoidance of duties and taxes | Risk level – Medium<br>Impact – Very High |
| Repudiation | Insider denies performed manipulation of data | Loss trackability, accountability, and compliance failure | Risk level – Low<br>Impact – Medium |
| Information Disclosure | Leak of cargo manifests, customs data | Industrial espionage cargo theft | Risk level – Low<br>Impact – medium |

Continued

**Table 2:** Continued

| Category | Threat | Impact | Risk Assessment |
|---|---|---|---|
| Denial of Service | DoS attack on PMS or SCADA Wireless jamming of sensors or access gates | Halted operations, vessel queuing physical disruption, security risk | Risk level – High Impact – Medium |
| Privilege escalation | Exploiting a TOS vulnerability for admin access | Total system compromise | Risk level – High Impact – High |

## CONCLUSION

A robust global maritime logistic system is one that can anticipate, absorb, adapt, and recover from disruptions—whether they are caused by natural disasters, cyberattacks, geopolitical tensions, pandemics, or economic shocks. Robustness is not about avoiding disruption entirely but about minimizing impact and ensuring rapid recovery. Key pillars of robustness are: 1) Threat discovery, 2) understanding real-time operational status, 3) redundancy that is realized by maintain backup systems, and spare capacity, 4) flexibility that is ability to repurpose existing resources dynamically, 5) visibility which means having reliable real-time data and analytics across system nodes and, 6) resilience planning for risk assessment and crisis response. Seaports are in focal point in the logistic system since over 90% of globally transported goods go through them. Building of robust seaport operations start with understanding its potential cyber and cyber physical threats. At high level potential threats can be categorized for three groups: Potential threats by humans, technology and processes. Once potential threats are known at operational and system architecture level, it is possible to focus threat analysis all the way to system software of an individual sensor, identify weak links in processes and provide necessary training for personnel. Since each seaport is unique, even if they have same tools, devices and software in use, comprehensive threat analysis is tailor made and should be repeated periodically.

## REFERENCES

Clavijo Mesa, M. V., Patino-Rodriguez, C. E., & Guevara Carazas, F. J. (2024). Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defences in Maritime Supply Chains. Information, 15(11), 710. https://doi.org/10.3390/info15110710

Forum of Incident Response and Security Teams (2023). https://www.first.org/

Hu, Z., & Yang, M. (2024). Systematic literature review of threat modelling and risk assessment in ship cybersecurity. *Ocean Engineering*, *293*, 123084. https://www.sciencedirect.com/science/article/pii/S0029801824013970

Kanwal K, Shi W, Kontovas C, Yang Z, Chang CH. Maritime cybersecurity: Are onboard systems ready? Marit Policy Manag. 2022 Sep 16;51(3): 484–502. doi: 10.1080/03088839.2022.2124464. PMID: 38832094; PMCID: PMC11146163.

Mell, P., Scarfone, K., & Romanosky, S. (2007). A complete guide to the Common Vulnerability Scoring System version 2.0. https://www.first.org/cvss/v2/guide

MITRE Corporation. (n.d.). MITRE ATT&CK framework. https://attack.mitre.org/

Progoulakis, I., Nikitakos, N., Dalaklis, D., Yaacob R. (2022). Cyber-physical security for ports infrastructure. MARLOG Journal, Vol. 11 (2022). https://apc.aast.edu/ojs/index.php/MARLOG/article/view/MARLOG.2022.11.105

Pseftelisa, T., Chondrokoukis G. (2021). A study about the role of the human factor in maritime cybersecurity. Spoudai Journal of Economics and Business, Vol. 71(2021), Issue 1–2, pp. 55–72. https://spoudai.org/index.php/journal/article/view/90

Pöyhönen, J., & Lehto, M. (2023). Comprehensive cyber security for port and harbour ecosystems. Frontiers in Computer Science, 5, Article 1154069. https://doi.org/10.3389/fcomp.2023.1154069

STRIDE, Microsoft Corporation (n.d). Microsoft Threat Modeling. https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

Tsoulfas G. (2025). Port resilience: A systematic literature review. Maritime Economics & Logistics. https://link.springer.com/article/10.1057/s41278-025-00326-3

Velez T., Morana. M, Risk Centric Threat Modelling. ISBN 9780470500965, John Wiley & Sons Inc, 2015.