The International Maritime Transport and Logistics (MARLOG 15) - ISSN 2974-3141
http://dx.doi.org/10.21622/MARLOG.2026.15.1.103
Smart & Resilient Logistics Corridors Future Gateway to the Green Trade

ENHANCING PORT CYBER RESILIENCE THROUGH CYBER PHYSICAL SECURITY ASSESSMENT

Iosif Progoulakis [1,2], Nikitas Nikitakos [1,3], Theodoros Lilas [1,4] and Ioannis K. Dagkinis [1,5]

(1) Department of Shipping Trade and Transport, University of the Aegean, Chios, Greece.

(2) i.progoulakis@aegean.gr

(3)nnik@aegean.gr

(4) lilas@aegean.gr

(5) idag@aegean.gr

Keywords: Ports; OT; IT; Resilience; Cyber physical security assessment; Cold iron plant; Bow Tie Analysis

ABSTRACT

Marine ports are critical elements of the global supply chain and maritime transportation sector, facilitating the transportation of goods, energy, and information across the globe. Ports as part of the critical infrastructure sector, experience rapid transformation driven by digitalization, sustainability requirements and the need for the reduction of carbon emissions and environmental impact. This has led to the intensified exposure of ports to multiple and diverse cyber threats stemming from the vulnerabilities and the wider attack surface created through the integration of operational technologies (OT) with information technologies (IT) and the development of more efficient but complex cyber- physical systems. Ports now face a growing threat landscape where cyber attacks can disrupt both digital systems and infrastructure as well as physical operations, leading to cascading effects on international trade and economic stability. This article explores the imperative of strengthening port resilience through comprehensive cyber physical security assessment. It presents a case study of a cyber attack on a cold iron plant—a facility that supplies shore-side electrical power to docked ships—highlighting how a targeted breach led to operational paralysis and safety hazards. Using bow tie analysis, the study maps the causal pathways from threat sources to consequences, identifying critical barriers and recovery measures. This method provides a structured framework for visualizing risk scenarios and enhancing decision-making in security planning. By examining the intersection of digitalization and physical infrastructure in marine ports, the article underscores the need for proactive security strategies that bridge cyber and physical domains. It advocates for the adoption of integrated assessment models that not only detect vulnerabilities but also quantify potential impacts and guide mitigation efforts. Ultimately, enhancing port resilience requires a

paradigm shift—from reactive cybersecurity to holistic cyber physical security governance—ensuring that ports remain robust, adaptive, and secure in the face of increasingly sophisticated cyber threats.

1. INTRODUCTION

Maritime ports, the cornerstones of the global economy, have undergone a profound digital transformation incorporating new technologies in systems and processes (Progoulakis et al., 2023, [1]; Tijan et al., 2021, [2]; Papageorgiou, 2020, [3]). Port processes involving container cranes, gate operations, terminal management systems, customs systems, cargo tracking, and vessel traffic control are now becoming automated relying on interconnected IT (Information Technology) and OT (Operational Technology) systems. Further operational efficiency is achieved through the integration of IoT sensors, AI-powered analytics, remote automation, and cloud services, which at the same time increases the cyber attack surface. This increasing interconnection of digital systems and physical operations increases the likelihood of a cyber disruption leading to data loss as well as physical safety incidents, environmental damage, or system-wide outages.

The convergence of IT and OT in ports presents unique operational and technical vulnerabilities. Operational systems with previously no network connectivity are now often connected and exposed to cyber threat actors. Possible scenarios of the cyber breach of crane control or terminal automation leading to misroute containers, disabling of safety interlocks, or even damage critical infrastructure, are now more plausible. Moreover, the fragmented operational and ownership structure of ports with multiple stakeholders: port authorities, terminal operators, shipping companies, customs authorities, and third-party service providers, makes cyber risk governance challenging.

As the cyber attack surface increases with digitalization of ports so does the implementation of regulatory frameworks. In Europe, the NIS 2 Directive (Network and Information Systems) classifies port operations as "essential entities," obliging them to implement robust risk management, reporting, and resilience measures. Agencies such as ENISA (European Union Agency for Cybersecurity) have issued detailed guidelines to help ports develop cyber risk frameworks, but adoption and maturity vary greatly among port ecosystems.

The increased evolution of cyber threats and the possible devastating effects of incidents in the maritime transportation sector, makes cyber resilience in ports a necessity. Cyber resilience demands the ability to: anticipate, withstand, respond and recover from cyber-physical incidents. This requires integrated planning across IT, OT, safety, and business continuity domains; an efficient organizational and governance structure with continuous threat monitoring and a cyber-awareness culture. Cyber resilience must also be integrated into safety planning and the physical safety systems of cranes, power systems, and environmental controls which must be designed to tolerate, detect, and recover from malicious or accidental cyber-induced faults.

In this paper, the emerging cyber threat landscape for ports is examined, focusing into cyber-physical security and safety issues. A case-study centered on a "cold-iron" plant (shore-power) cyber-attack is presented, analyzing it through the Bow-Tie-Analysis methodology. Finally, key findings and proposed systemic measures for port stakeholders (authorities, operators and regulators) are recommended in order to strengthen their cyber resilience posture.

2. MARITIME CYBER THREAT LANDSCAPE FOR PORTS AND THE SHIPPING INDUSTRY

The contemporary cyber threat landscape for maritime ports and the broader shipping industry is both dynamic and increasingly hazardous. Several combined factors lead to an increased risk profile: digital transformation, increased attack surface, geopolitical tensions, regulatory pressure, and evolving threat actors and attack tactics. Figure 1 shows the types of cyber breach incidents observed in ports from 1980 to 2025, highlighting the greater occurrence of Denial of service and ransomware type incidents.

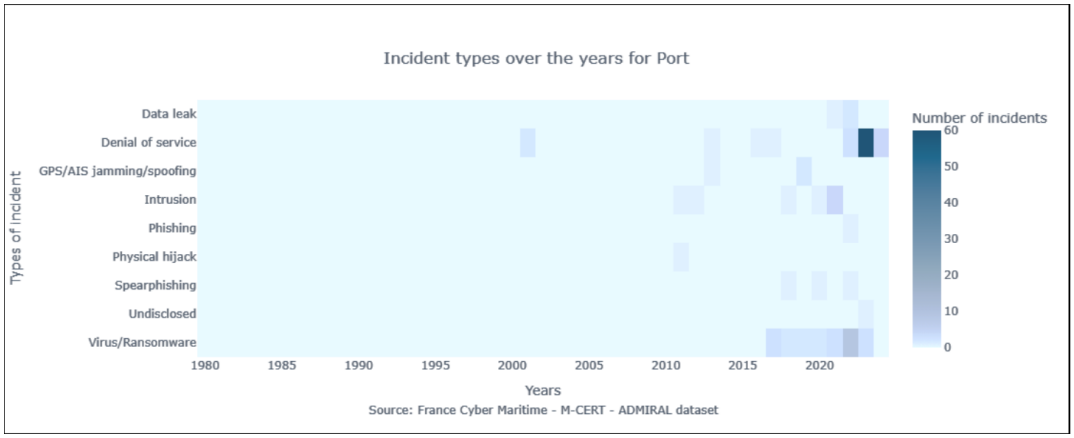

Figure 1: Port cyber incidents over the years (1980-2025) (Source: https://www.m-cert.fr/admiral/Port.html [4]).

Similarly, a systematic literature review on cyber-attacks in maritime supply chains identifies DDoS (Distributed Denial of Service) and malware/ransomware as among the top threats against shipping companies, port operators, and other maritime actors. The review further highlights navigation system attacks (such as GPS spoofing, jamming, or AIS manipulation), phishing/social engineering, and identity fraud as persistent and high-impact attack vectors (Mesa, et al., 2024, [5]). Ransomware is a particularly disruptive risk. Because port operations rely on integrated, centralized systems (e.g. terminal operating systems, gate and yard management, crane control) of which the encryption or corruption of critical data can paralyze operations. The ENISA "Port Cybersecurity" report (ENISA, 2019, [6]) outlines scenarios in which ransomware could force temporary shutdown of terminal operations, causing cascading delays.

Maritime supply chain cyber attacks are of high concern as port ecosystems depend heavily on third-party vendors (software providers, automation vendors, cloud services, IoT device manufacturers). A compromise in any one of these maritime supply chain nodes can spread risk into terminal or port- wide operations. The ENISA "Cyber Risk Management for Ports" guidelines (ENISA, 2020, [7]) emphasize the need for port operators to document dependencies of inventory on third parties and incorporate them into risk assessments.

State-sponsored actors are also increasingly targeting ports as strategic targets national critical infrastructure, for geopolitical or economic disruption. Such cyber attacks may support broader national objectives such as trade embargoes, economic coercion, or espionage. The risk is increasing as ports become "digital gateways" for trade and energy flows.

Considering the human factors involved in port operations, further cyber vulnerabilities are realized. Phishing, spear-phishing, social engineering, and insider threats continuously appear as emerging cyber attack vectors into port IT/OT infrastructure. Many ports are characterized by an unbalanced capacity in cyber awareness, inadequate training, and

siloed organizational responsibility. Per Argyriou et al. (2024) [8], the adaptation of cyber measures is often hindered by a lack of cyber awareness and organizational alignment.

Regulatory and compliance pressures further influence the cyber risk environment. The EU's NIS 2 Directive increases obligations for port operators to conduct risk assessments, implement security measures, and report major incidents. Failure to comply not only exposes ports to cyber risk but carries regulatory, financial, and reputational penalties.

In sum, the cyber threat landscape confronting maritime ports includes high-impact ransomware and malware, increased supply chain risk, state-sponsored actors, human factor vulnerabilities, and systemic regulatory pressures among others. The interconnection of IT and OT, combined with segmented cybersecurity governance and limited threat sharing, makes cyber resilience both challenging and essential.

2. CYBER-PHYSICAL SECURITY AND SAFETY IN MARITIME PORTS

2.1. Cyber-Physical Security Assessment

Considering that ports are cyber-physical systems (CPS) and key elements of the critical infrastructure sector of any maritime transportation system, there are a number of qualitative and quantitative security assessment methods that can be used. In general terms most of these assessment methods consider parameters such as the assets, their interdependency, the threat scenarios, vulnerabilities, consequences, risk analysis and required resiliency. An indicative list of such security assessment methods applicable to the maritime domain and ports and presented in scientific publications from 2010 to 2024 can be found in Table 1.

Table 1. List of cyber-physical security assessment methods applicable to ports.

Method Description	Author/Source
Commercial supply chain risk management as part of CIP	Häyhtiö, M., & Zaerens, K. (2017) [9]
Fuzzy RAMCAP	Alidoosti, A., et al. (2012) [10]
All-hazards catastrophe analysis framework, based on network science and normal accident theory	Lewis, T. G., et al. (2011) [11]
Threat, vulnerability, and consequence analysis using operations research, prospect theory, network science, and normal accident theory	Taquechel, E.F. & Lewis, T.G. (2017) [12]
Limited Memory Influence Diagram (LIMID) using Bayesian Networks	Misuri, A., et al. (2019) [13]
Defender–Attacker–Defender (DAD) sequential model analysis for CIP	Alderson, D.L., et al. (2011) [14]
Vulnerability analysis method for interdependent infrastructure systems in CIP	Ouyang, M. (2016) [15]
Criticality assessment method for critical energy infrastructure	Augutis, J., et al. (2016) [16]
Deterrence quantification method for CIP using game theory and probabilistic utility functions	Taquechel, E.F., et al. (2012) [17]
Security analysis using the Collaborative Security Management (CYSM) System method for Critical Information Infrastructure (CII) and maritime CIP	Karantjias, A., et al. (2014) [18]
Model-Based Vulnerability Assessment (MBVA) for the protection of interdependent critical infrastructure	Valencia, V.V., et al. (2012) [19]
Attack-strength-degradation model	Wu, B., et al., (2016) [20]
Cyber Risk Assessment for Ships (CRASH): a qualitative risk analysis method using severity, probability, and criticality ratings	Oruc, a, et al. (2024) [21]
CYber-Risk Assessment for Marine Systems (CYRA-MS): a modified Cyber Preliminary Hazard Analysis (CPHA) to IEC 62433 parameters.	Bolbot, V. et al. (2020) [22]
CRAMMTS (Cyber Risk Analysis Method for Maritime Transportation	Tatar, U. et al. (2024)

Systems): a survey-based quantitative risk analysis method that modifies the ISRAM (Information Security Risk Analysis Method) risk analysis method, considering IMP criteria and industry stakeholder feedback	[23]
Qualitative vulnerability assessment method for port and ship ecosystem components, implementing a System-of-Systems cyber risk analysis approach	Kapalidis, C. et al. (2022) [24]
Security Vulnerability Assessment, Prevention, and Prediction (SVAPP): A safety barrier assessment methodology adapted for industrial assets for physical and cyber-attack scenarios	van Staalduinen, M. et al. (2016) [25]
Cyber PHA (Process Hazard Analysis): a safety-oriented cyber security risk assessment methodology for industrial control systems (ICSs) and safety instrumented systems (SISs), based upon ISA 62443-3- 2, ISA TR84.00.09, ISO/IEC 27005:2018, ISO 31000:2009, and the NIST Special Publication (SP) 800-39.	Marszal, E. M., et al. (2019) [26] and Ginter, A. (2023) [27]

From a preliminary review of the assessment methods presented in Table 1, it can be devised that these focus on IT, OT or physical elements, however, the safety and resiliency aspects are not tackled in detail. The plethora of available security assessment methods applicable to maritime and port-specific cyber-physical systems, needs to be evaluated in field conditions. Port authorities and stakeholders that know their unique operational and technical requirements need to assess the validity of possible assessment methods and tools considering the following criteria:

- Asset inventory & dependency mapping
- Threat modeling & scenario planning
- Risk assessment & business impact analysis
- IT/OT vulnerability verification
- Governance compliance and stakeholder alignment
- Integrated resilience

2.2. Safety and Cyber Security

Understanding the link between cyber security and safety is critical, because of the potential effect to physical safety due to a cyber breach incident in port systems. Such incidents can lead to the following possible scenarios:

a) Compromise of safety-critical OT systems: Possible scenario: The compromise of a crane's

control system or manipulation of gate barrier logic, could cause collisions, dropped containers, or human injury. Any cyber measures shall support functional safety, not substitute it.

b) Incident response integration: Cyber incident response plans must be integrated into traditional safety or emergency response plans. Possible scenario: Compromise of terminal automation should activate emergency procedures that safely shut down cranes or isolate critical systems.

c) Redundancy and fail-safe design: Adopt a safe-by-design approach. Design systems with redundancy (e.g., backup sensors, parallel control paths) and fail-safe mechanisms. Sensor fusion and change-detection techniques can alert operators to anomalies in physical systems, as shown in marine navigation resilience research (Argyriou, et.al., 2024, [8]).

d) Training & human factors: Safety officers, crane operators, maintenance teams, and ICS engineers must be included in cyber training. Human error is often a vector for cyber-physical failure, so cross-domain training is critical.

e) Policy and regulatory compliance: Cybersecurity governance should align with safety and security regulations such as the ISPS Code. ENISA's good practices for ports recommend embedding cyber risk management within broader security and safety governance frameworks (ENISA, 2019, [6]).

Considering the operational and consequential link between cyber security and safety, there is a need for the adoption of assessment methods that can accommodate both cyber and physical process dimensions. Such methods include among others the Cyber PHA (Process Hazard Analysis), the Rings Of Protection Analysis (ROPA) and the Bow-Tie-Analysis (BTA) methods. The Cyber PHA is a safety- oriented cyber security risk assessment methodology for industrial control systems (ICSs) and safety instrumented systems (SISs), based upon ISA 62443-3-2, ISA TR84.00.09, ISO/IEC 27005:2018, ISO 31000:2009, and the NIST Special Publication (SP) 800-39 (Marszal et al., 2019, [26]; and Ginter, 2023, [27]). The Rings Of Protection Analysis (ROPA) is an adapted version of the Layer of Protection Analysis (LOPA) method for the cyber security of process control systems (Baybutt, P., 2004, [28]).

Bow-Tie Analysis (BTA) is a qualitative Process Safety Management (PSM) method, widely used in oil, gas, chemical, and processing industries (AIChe, 2018, [29]). It supports proactive safety/security reviews and reactive post-incident analyses. The method is also applicable in the maritime sector, examining interconnections of vessel and port equipment, systems, and processes during safety or security incidents. In cyber–physical security, BTA identifies barriers and mitigation measures for IT/OT assets (Progoulakis, et al., 2022 [30], 2023 [1]). By integrating safety and security perspectives, BTA provides a structured framework for managing risks across industrial and maritime environments. The use of BTA in cyber-physical security assessment has been decided in this paper due its direct relation to process safety assessment and proven usability in the investigation of safety/accident and security case studies.

2.3. Port Cyber Resilience

Resiliency as a term can generally be defined as the capacity and capability to sustain continuity of operations or technical integrity to a level acceptable either to continue operations or allow for safely transitioning to a ramp down of operations; after a disruptive or destructive event stemming from a breach of safety or security or both. In order for ports to achieve operational and cyber resilience the focus from protection from and detection of threats needs to shift to the capacity and capability to recover from cyber attacks and adaptability to new operational conditions. As shown in Figure 2, for maritime port cyber resilience the elements of maritime operations, industrial cyber resilience, maritime cyber security, Critical Infrastructure Protection all constitute the necessary capacity and mitigation capabilities.

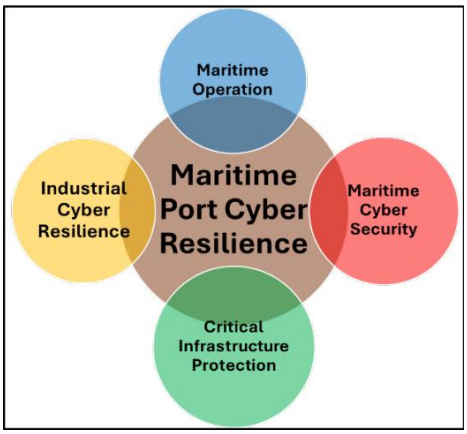

Figure 2: Capacity and capability elements of Maritime Port Cyber Resilience.

The key components in port cyber resilience include:

1. Resilience Frameworks: Adopting a holistic, risk-based cyber-resilience framework. Implementing strategies that cover pre-incident (preparation), detection & response, recovery, and learning phases. Use adaptive response mechanisms that consider human factors (Nganga, et al.,2024, [31]) in port operations. In essence built the capacity in compliance, processes, skills that can lead to capabilities.

2. Incident Response & Recovery Planning: Deploy capabilities built to develop and test integrated plans involving skilled IT/OT cyber professionals, such as cyber analysts, OT engineers, operations staff, and safety teams. These key stakeholders should operate with clearly defined roles, communication protocols, backup strategies, and restoration and post-incident recovery procedures. These built capabilities should include back-up procedures to sustain operations with automation system such as: manual provisioning of shore-power, manual control of cranes or gate systems, manual reporting of container movements.

3. Monitoring & Detection: Deploy monitoring tools across the IT and OT attack surface. Centrally assess data logs, alarms, sensor feedback, and process data. Utilize anomaly detection, behavior- based monitoring, and threat intelligence to obtain solid understanding of threats in the maritime domain (Nganga, et al.,2024, [31]).

4. Information Sharing & Collaboration: Ports may be locally based but are internationally connected. Port authorities and stakeholders should participate in industry groups at a local and international level, sharing threat intelligence and benchmark mitigation measures. Collaboration with regulators, other ports, shipping companies, and vendors should be pursued in order to establish shared resilience goals.

5. Continuous Training & Culture: Embrace a cyber-aware culture across all stakeholders. Provide continuous training, simulation-based exercises (including cyber-physical scenarios), phishing campaigns, and tabletop exercises. Utilize after-action reviews, root-cause analysis, and updating security controls to establish lessons-learned knowledge from past incidents.

6. Governance & Leadership: Embracing of cyber resilience from executive management team. Definition of clear accountability for cyber risk at the organizational and inter-

organizational levels. Embedding of cyber resilience metrics into port Key Performance Indicators.

7. Adaptation & Learning: Incorporate incident and exercises review to establish lessons' learned knowledge that allow for the update of risk assessments and control measures. Maintain monitoring of resilience Key Performance Indicators and state of operational and emergency management capacity in order to adapt to evolving threat scenarios.

3. CASE STUDY: CYBER ATTACK ON PORT COLD-IRON PLANT

To illustrate the cyber-physical risk and resilience dynamics in a port environment, this case study examines a hypothetical but plausible cyber-attack on a cold-iron (shore-power) plant at a container terminal.

3.1. Scenario Description

In this scenario, a threat actor (e.g., cybercriminal syndicate or state-sponsored group) targets the OT infrastructure of the port's cold-iron system. The cold-iron plant provides shore-power (electrical power) to docked vessels, allowing them to shut down their engines, reducing emissions, noise, and fuel consumption. The objective of the threat actor is to disrupt shore-power supply and other port operations. The security breach scenario has the following stages as shown in Figure 3.

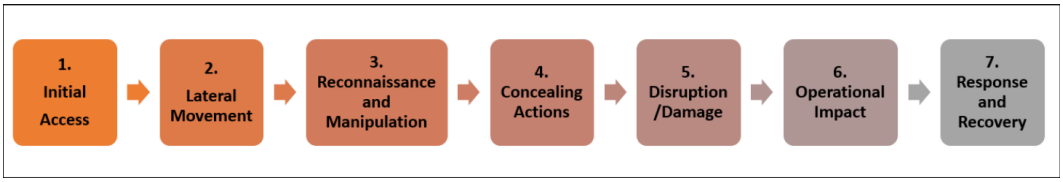

Figure 3: Sequence of events of cyber breach incident.

In stage 1 (Initial access) a maintenance technician receives a spear-phishing email. The email is designed to look like an internal invoice or maintenance request and contains a malicious link. The technician inadvertently installs malware onto his workstation after clicking the email link.

In stage 2 (Lateral movement) remote access is granted to the attacker through installed malware. Due to weak network segmentation, the attacker is able to gain access to OT systems through the IT network. The SCADA server, PLC controllers for power converters, and HMI panels are identified as targets.

In stage 3 (Reconnaissance and manipulation) the attacker studies the system operation parameters (voltage, current, load) and begins to falsify sensor readings. Small overvoltage deviations are introduced to the power control setpoints, causing voltage fluctuations.

In stage 4 (Concealing actions), a Denial-of-Service (DoS) attack is launched against the network segment hosting the SCADA interface in order to maintain the initial undetected breach. The alarm logic on the HMI is also manipulated to suppress or delay alerts to operators.

In stage 5 (Disruption / Damage), the overvoltage stress damages converter hardware, triggers thermal overload, and eventually leads to failure of key components of the shore-power system.

In stage 6 (Operational impact) the cold iron plant shuts down with electrical safety hardware (circuit breakers, fuses, emergency trip push buttons, and manual disconnect switches, etc) being activated. Docked vessels are forced to restart their engines, increasing emissions, noise, and environmental risk. Container operations at the terminal are

delayed or halted due to lack of power backup systems. Additional disruption in gate systems and berth operations may appear.

In stage 7 (Response and recovery), incident response teams from the port authority/operator are deployed. The OT network is isolated and back-up systems are reinstated. Vessel coordination is taking place in parallel with replacement of damaged converters and restoration of control logic. In the mean time the regulatory authority may be involved reputational damage ensues.

3.2. Bow-Tie-Analysis

Using the Bow-Tie-Analysis, causes, controls, and consequences of this cyber breach incident are mapped and analyzed. In this scenario the Top Event is the compromise of the cold-iron plant OT systems leading to overvoltage and system failure. The hazard is the external cyber aggressors. The Bow-Tie Analysis is shown in Figure 4.

The cyber-Threats and safety incident causes are:

- Phishing / spear-phishing leading to malware installation
- Weak network segmentation resulting in lateral movement of cyber-aggressor in IT/OT system environment.
- Poor credential hygiene or lack of least-privilege access which enables aggressor to access system PLCs.
- Unpatched or insecure firmware in PLCs / SCADA
- Insufficient system monitoring resulting in manipulation of system operational settings remaining unnoticed.

The Preventive barriers are the following:

- Regular phishing training raising cyber awareness levels.
- Network segmentation allowing IT and OT network separation.
- Strong access control with multi-factor authentication or other means.
- Updated IT/OT firmware part of a patch management policy.
- Monitoring and logging of systems detecting abnormal access or credential use.

The identified threat escalation factors degrading preventative barriers, are the following:

- Lack of OT visibility allowing manipulation of ICS operational settings remaining undetected.
- Manipulation of ICS and HMI deactivating or concealing operator alerts.
- Absence of redundancy in critical power conversion equipment.
- Inadequate incident response planning for OT cyber breach events.

The Top Event Consequences are the following:

- Hardware damage such as to power converters.
- Shore-power outage resulting in loss of vessel power supply.
- Environmental impact due to vessel's engines restart increasing emissions, noise and pollution.
- Operational disruption leading to terminal delay, gate or crane operational issues.
- Financial losses: repair cost, downtime, reputational damage
- Safety risks: if power failure causes unsafe conditions

The Mitigating and recovery barriers are the following:

- Emergency shutdown and fail-safe mechanisms in converters

- Independent sensor validation for the field verification of voltage/current via redundant measurement
- Incident response plan for scenarios involving IT, OT and safety systems and functions.
- Backup systems. Using spare converters and transitioning to manual control if automations fail.
- Post-incident root cause analysis with lessons-learned sessions involving the analysis of all steps undertaken.
- Stakeholder communication with vessels, port authority, regulatory bodies

The Consequence escalation factors leading to degrading of mitigate barriers are the following:

- Lack of scenario-specific cyber-physical exercises (i.e. overvoltage compromise, OT system attacks, etc)
- Lack of threat intelligence data fusion
- Lack of continuous system field monitoring and regulatory compliance

Note that the actual successful implementation of scenario-specific cybersecurity/mitigation exercises involving all stakeholders (including red-teaming exercises) and utilizing effective threat intelligence and field system monitoring could lead to the enhancement of resilience, contributing to the continuity of operations.

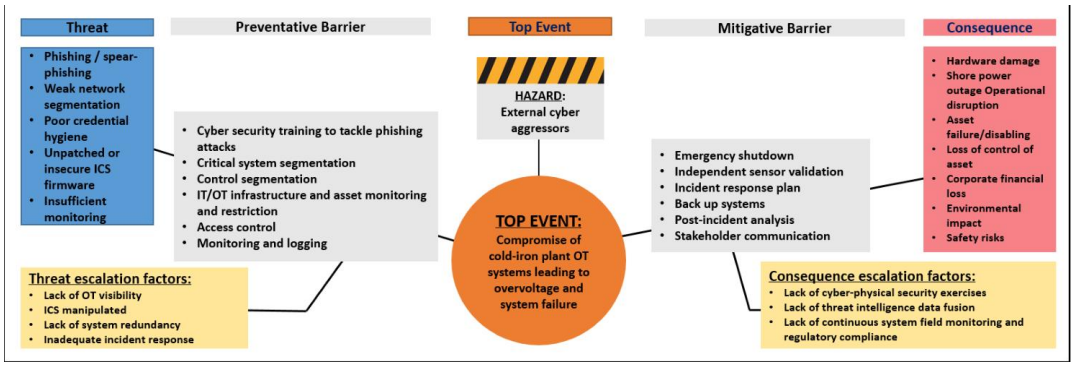

Figure 4: BTA diagram of incident in cold iron plant.

4. CONCLUSIONS AND DISCUSSIONS

4.1. Key conclusions

1. Maritime ports are cyber-physical systems of systems: Modern ports operate as complex cyber- physical systems. The tight coupling between operational technology (cranes, gates, power systems) and IT systems makes cyber risk an existential safety concern.

2. Cyber threat landscape is evolving faster than the defenders' capacity and capability for mitigation: Ransomware, DDoS, supply chain compromise, navigation spoofing, and state-sponsored actors all threaten port operations. The convergence of physical infrastructure with digital control amplifies the consequences of a breach.

3. Complexity in regulatory compliance hinders resilience: Ports are often managed by a plethora of stakeholders (port authority, terminal operators, shipping lines, service providers), complicating unified cyber risk governance, incident response, and accountability.

4. Human factor remain relevant and central: Phishing and insider threat risk remain among the most common and severe vectors. Without ongoing cyber education and cross-domain training, resilience will continue to be fragile.

5. Adopt a cyber-safe-by-design approach: Cybersecurity implementation cannot be separated from safety. Incident response must involve safety protocols, back-up procedures, and redundant control systems to manage compromised OT. Cyber-safety must be integrated in system architecture and processes.

6. Resilience requires continuous monitoring and enforcement: Cyber resilience is not incidental. Continuous risk assessment, monitoring, threat intelligence sharing, exercises, and lessons- learned frameworks are required to obtain the capacity and capability for cyber resilience.

7. The use of BTA and other interdisciplinary and process safety and security related assessment tools improve the required threat and vulnerability assessment for ports and related critical components.

4.2. Recommendations and discussion

It has to be understood that cybersecurity incidents in the maritime domain are not simply technical issues confined to IT systems, but they do have the potential to disrupt ship-to-shore operations, cause delays in cargo deliveries, and risk safety in ship and port operations. Despite these critical operational consequences, a significant number of organizations continue to mistakenly categorize cyber incidents as simple IT problems rather than recognizing them as operational crises.

Achieving resilience necessitates the convergence of cybersecurity and safety planning. A robust maritime incident response strategy must go beyond the typical steps of containment and recovery, aiming instead to sustain mission continuity even in challenging and often disconnected maritime environments. This strategy needs to be planned considering both operational and tactical level mitigation measures, with a number of pro-active steps:

• Integrating the cybersecurity response framework directly into the existing Safety Management System (SMS), in accordance with IMO resolution MSC.428(98). Developing specific Operational Technology (OT)-focused guidelines for critical port and ship systems—such as berthing, cargo handling, propulsion, power, and navigation—that cannot be easily deactivated during an incident.

• Conducting joint training exercises that involve the vessel, engineering, and IT/OT teams, moving beyond scenarios that only include cybersecurity professionals.

• Pre-staging recovery assets that can be used offline to compensate for limited bandwidth or connectivity when necessary.

• Preemptively establishing relationships with external entities with the capability to respond in cyber security crisis scenarios which can be Government entities, contractors and specialized vendors.

Ultimately, cyber resilience in the maritime sector is more than just enduring an attack as it involves tasks to retain control, communication, and confidence while under extreme pressure. In a critical infrastructure sector where any period of downtime can result in massive financial loss and endanger human life, preparation is paramount to achieve integrity and protection.

5. REFERENCES

[1.] Progoulakis, Iosif, Nikitas Nikitakos, Dimitrios Dalaklis, Andreas Christodoulou, Andreas Dalaklis, and Razali Yaacob. "Digitalization and Cyber Physical Security Aspects in Maritime Transportation and Port Infrastructure." In Smart Ports and Robotic Systems, edited by T. M. Johansson, D. Dalaklis, J. E. Fernández, A. Pastra, and M. Lennan, 229–248. Studies in National Governance and Emerging Technologies. Cham: Palgrave Macmillan, 2023. https://doi.org/10.1007/978-3-031-25296-9_12

[2.] Tijan, Edvard, Maja Jović, Siniša Aksentijević, and Andreja Pucihar. "Digital Transformation in the Maritime Transport Sector." Technological Forecasting and Social Change 170 (2021): 120879.

[3.] Papageorgiou, Michael. "Digital Transformation in the Shipping Industry Is Here." NAFS: Bimonthly Review for the Shipping Industry, 2020.

[4.] France Cyber Maritime. ADMIRAL Dataset: Detailed Maritime Cybersecurity Statistics for Port, accessed November 25, 2025. https://www.m-cert.fr/admiral/Port.html

[5.] Clavijo Mesa, María V., Carlos E. Patino-Rodriguez, and Freddy J. Guevara Carazas. "Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains." Information 15, no. 11 (2024): 710. https://doi.org/10.3390/info15110710

[6.] European Union Agency for Cybersecurity (ENISA). Port Cybersecurity – Good Practices for Cybersecurity in the Maritime Sector. Athens: ENISA, 2019. https://www.enisa.europa.eu/publications/port-cybersecurity- good-practices-for-cybersecurity-in-the-maritime-sector

[7.] European Union Agency for Cybersecurity (ENISA). Guidelines – Cyber Risk Management for Ports. Athens: ENISA, 2020. https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for- ports

[8.] Argyriou, Ioannis, and Theocharis Tsoutsos. "Assessing Critical Entities: Risk Management for IoT Devices in Ports." Journal of Marine Science and Engineering 12, no. 9 (2024): 1593. https://doi.org/10.3390/jmse12091593

[9.] Häyhtiö, Markus, and Klaus Zaerens. "A Comprehensive Assessment Model for Critical Infrastructure Protection." Management and Production Engineering Review 8, no. 4 (2017): 42–53. https://doi.org/10.1515/mper-2017-0035

[10.] Alidoosti, Ali, Morteza Yazdani, Mohammad Majid Fouladgar, and Mohammad Hossein Basiri. "Risk Assessment of Critical Asset Using Fuzzy Inference System." Risk Management 14 (2012): 77–91. https://doi.org/10.1057/rm.2011.19

[11.] Lewis, Ted G., Thomas J. Mackin, and Rudy Darken. "Critical Infrastructure as Complex Emergent Systems." International Journal of Cyber Warfare and Terrorism 1, no. 1 (2011): 1–12. https://hdl.handle.net/10945/45469

[12.] Taquelchel, Eric F., and Ted G. Lewis. "A Right-Brained Approach to Critical Infrastructure Protection Theory in Support of Strategy and Education: Deterrence, Networks, Resilience, and 'Antifragility'." Homeland Security Affairs 13 (2017): 50–83. https://www.hsaj.org/articles/14087

[13.] Ivanc, Blaž, and Tomaž Klobučar. "Attack Modeling in the Critical Infrastructure/Modeliranje napadov v kriticni infrastrukturi." Elektrotehniški Vestnik 81, no. 5 (2014): 285–292.

[14.] Alderson, David L., Gerald G. Brown, W. Matthew Carlyle, and R. Kevin Wood. Solving Defender- Attacker-Defender Models for Infrastructure Defense. Monterey, CA: Naval Postgraduate School, Department of Operations Research, 2011.

[15.] Ouyang, Min. "Critical Location Identification and Vulnerability Analysis of Interdependent Infrastructure Systems under Spatially Localized Attacks." Reliability Engineering & System Safety 154 (2016): 106–116. https://doi.org/10.1016/j.ress.2016.05.007

[16.] Augutis, Juozas, Benas Jokšas, Ričardas Krikštolaitis, and Rolandas Urbonas. "The Assessment Technology of Energy Critical Infrastructure." Applied Energy 162 (2016): 1494–1504. https://doi.org/10.1016/j.apenergy.2015.02.065

[17.] Taquelchel, Eric F., and Ted G. Lewis. "How to Quantify Deterrence and Reduce Critical Infrastructure Risk." Homeland Security Affairs 8 (2012): 1–28. https://www.hsaj.org/articles/226

[18.] Karantjias, Athanasios, Nineta Polemi, and Spyridon Papastergiou. "Advanced Security Management System for Critical Infrastructures." In Proceedings of the IISA 2014, 291–297. Chania, Greece, July 7–9, 2014.

[19.] Valencia, Vhance V., and Alfred E. Thal Jr. "Applying the Model-Based Vulnerability Assessment Technique to Interdependent Infrastructures." In Proceedings of the IIE Annual Conference, Orlando, Florida, USA, May 19–23, 2012.

[20.] Wu, Baichao, Aiping Tang, and Jie Wu. "Modeling Cascading Failures in Interdependent Infrastructures under Terrorist Attacks." Reliability Engineering & System Safety 147 (2016): 1–8. https://doi.org/10.1016/j.ress.2015.10.017

[21.] Oruc, A., G. Kavallieratos, V. Gkioulos, and S. Katsikas. "Cyber Risk Assessment for SHips (CRASH)." International Journal on Marine Navigation and Safety of Sea Transportation 18, no. 1 (2023): 115–124. https://doi.org/10.12716/1001.18.01.10

[22.] Bolbot, Victor, Gerasimos Theotokatos, Evangelos Boulougouris, and Dracos Vassalos. "A Novel Cyber- Risk Assessment Method for Ship Systems." Safety Science 131 (2020): 104908. https://doi.org/10.1016/j.ssci.2020.104908

[23.] Tatar, Unal, Bilge Karabacak, Omer F. Keskin, and Dominick P. Foti. "Charting New Waters with CRAMMTS: A Survey-Driven Cybersecurity Risk Analysis Method for Maritime Stakeholders." Computers & Security 145 (2024): 104015. https://doi.org/10.1016/j.cose.2024.104015

[24.] Kapalidis, Chronis, Stavros Karamperidis, Tim Watson, and Georgios Koligiannis. "A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships." Journal of Marine Science and Engineering 10, no. 10 (2022): 1486. https://doi.org/10.3390/jmse10101486

[25.] van Staalduinen, Mark Adrian, Faisal Khan, and Veeresh Gadag. "SVAPP Methodology: A Predictive Security Vulnerability Assessment Modeling Method." Journal of Loss Prevention in the Process Industries 43 (2016): 397–413. https://doi.org/10.1016/j.jlp.2016.06.017

[26.] Marszal, Edward M., and James McGlone. Security PHA Review for Consequence-Based Cybersecurity. Research Triangle Park, NC: International Society of Automation (ISA), 2019.

[27.] Ginter, Andrew. Engineering-Grade OT Security: A Manager's Guide. Calgary, AB: Abterra Technologies Inc., 2023.

[28.] Baybutt, Paul. "Cyber Security Risk Analysis for Process Control Systems Using Rings of Protection Analysis (ROPA)." Process Safety Progress 23, no. 4 (2004): 284–291.

[29.] American Institute of Chemical Engineers. Center for Chemical Process Safety. Bow Ties in Risk Management: A Concept Book for Process Safety. Hoboken, NJ: John Wiley & Sons, Inc., 2018.

[30.] Progoulakis, Iosif, Nikitas Nikitakos, Dimitrios Dalaklis, and Razali Yaacob. "Cyber-Physical Security for Ports Infrastructure." Paper presented at the International Maritime and Logistics Conference "Marlog 11," Alexandria, Egypt, March 20–22, 2022. Malmö: World Maritime University, 2022. https://commons.wmu.se/lib_papers/10/

[31.] Nganga, Allan, Joel Scanlan, Margareta Lützhöft, and Steven Mallam. "Enabling Cyber Resilient Shipping through Maritime Security Operation Center Adoption: A Human Factors Perspective." Applied Ergonomics 119 (2024): 104312. https://doi.org/10.1016/j.apergo.2024.104312