Cyber-Physical Security For Ports Infrastructure

Iosif Progoulakis [1][i], Nikitas Nikitakos[2], Dimitrios Dalaklis [3] and Razali Yaacob [4]

[1,2] Department of Shipping Trade and Transport, University of the Aegean, Chios,Greece,

[3] World Maritime University, Malmö, Sweden, dd@wmu.se

[4] Netherland Maritime Institute of Technology, Johor Darul Takzim, Malaysia, razaliy@nmit.edu.my

E-Mail: iprogoulakis@aegean.gr, nnik@aegean.gr, dd@wmu.se, razaliy@nmit.edu.my

1. ABSTRACT: Taking advantage of the benefits associated with digital means has become a main priority for ports globally. The effective and smooth integration of Information Technology (IT) applications and those systems that support the conduct of operations (Operational Technology (OT) systems), along with the accurate "adjustment" of the human factor elements should be viewed as a very critical pillar for optimized safe and efficient operations in ports.

The afore mentioned assimilation characterizes cyber-physical systems and entails an extended number of IT and OT modules, systems and tasks involving various data transmission routes that are advancing in a technological and operational level alongside plausible cybersecurity threats. These cybersecurity risks, threats and vulnerabilities are depicted in this article to emphasize the progression of cyber- physical systems in the wider maritime industry and port domains, along with their rising cybersecurity vulnerabilities. Existing and applicable industry and government standards and mandates associated with cybersecurity attempt to impose regulatory compliance and increase asset cybersecurity integrity with reduced emphasis however, in the existing OT (Operational Technology) components and systems. The use of security risk assessment tools and processes that are used in other industrial sectors, such as the Security Risk Assessment (SRA) and the Bow Tie Analysis methods, can support the evaluation of IT/OT infrastructure for cyber-physical security susceptibilities and then assign suitable reactive measures. The implementation of cybersecurity safeguards that arise through the implementation of the MITRE ATT&CK Threat Model can enhance the cybersecurity posture of those assets that support the logistics chain, assuming that they are intermittently adapted following evaluations for their effectiveness and suitability. Finally, the improvement of stakeholder communication and cyber-awareness along with the increase in cyber- physical security resiliency can further be aided by the effective convergence of the segregated cyber and physical security elements of waterside or landside-based IT/OT infrastructure.

Keywords: *Information Technology (IT), Operational Technology (OT), Ports Cyber-Physical Security, Cybersecurity, IT/OT Convergence*

2. INTRODUCTION

Ports, also referred to as seaports, are considered a major part of the critical infrastructure of a country [1]. Critical infrastructure refers to the framework of infrastructure, man-made networks and systems that provide needed goods and services to the general public [1]. Ports in turn are defined as the geographical area where ships are brought alongside the shore to load and discharge cargo [2]. Ports provide a critical interface between land and sea [2] and sustain a country's economy and prosperity. In order for the ports to function efficiently they need to provide more than a safe and secure location for vessels to discharge or load cargo or for service providers to support maritime operations. A framework of additional infrastructure is interconnected to a port which creates a complex web of assets, processes, systems and operations. Ports can include an array of facilities including equipment storage facilities, fuel storage and refueling terminals, cargo terminals, utility services and infrastructure, industrial facilities, processing facilities, road and rail transport infrastructure. In order for the ports to be efficient and provide safe and secure services they also embrace automation in their procedures and systems. IT (Information Technology)/OT (Operational Technology) components have become indispensable tools and as more complex equipment and processes are in use, they include a number of SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems) components.

The terrorist attacks of September 11, 2001 did initiate a worldwide domino effect in the development and adoption of a number of security initiatives, directives, standards and policies in ports and maritime assets in general. Measures for the security and protection of maritime assets and infrastructure were implemented and the ISPS (International Ship and Port Facility Security) code from the International Maritime Organization (IMO) was universally adopted. Cybersecurity has been included in the general concept of security, but as worldwide threats evolve, it needs to adapt and progress as well.

In 2020 it was reported that cyberattacks on the maritime industry's OT systems had increased by 900% over the last three years [3]. Since then, further attacks have been reported in ports around the world. In July 2021 four major ports in South Africa were paralyzed by a major cyberattack which caused a "force majeure" due to a complete disabling of IT systems [4]. In August 2021 the port of Houston was attacked by hackers taking advantage of IT system vulnerabilities [4]. The result of such attacks has always been the financial loss due to diminished operations both at a local and international level. The deployment of forces, both governmental and private, to mitigate such incidents has also caused the re-evaluation of vulnerabilities which in turn have led to the investment in additional resources to reinforce the cybersecurity infrastructure and systems' posture.

Aiming in exploring the cyber-physical concepts of cybersecurity for ports infrastructure and realizing the current state of threats in the cyber domain, this paper will provide a concise assessment of the major attributes of cyber-physical security in the maritime industry to include the sector of ports. The known security threats and vulnerabilities faced by ports' infrastructure will also be discussed. An overview of the major initiatives by the industry and governmental entities aiming in enforcing the necessary measures at an organizational and operational level, will also be provided. A number of assessment methods for the evaluation of cyber-physical security threats and vulnerabilities will also be briefly presented to show the potential of tools available in the industry.

3. CYBER-PHYSICAL ASPECTS IN PORT INFRASTRUCTURE AND OPERATIONS

Cyber-physical systems in general pertain to the integration of IT and OT systems along with human factors [5]. This combination is shown in Figure 1 and represents the majority of operational and technical components found in ports' infrastructure. Maritime assets such as ports' infrastructure are operated by people and encompass an IT and OT operational and technical element that links procedures, systems, components, and technical and operational performance [5]. Similar to ships, ports' infrastructure involves multiple platforms of Systems of Systems (SoS) which contain IT and OT components, aiming in the automation of processes and optimum efficiency [6]. This architecture of IT, OT and human operators is further evolving adapting emerging technological features of Industry 4.0, the Internet of Things (IoT), cloud computing, data analytics, robotics to structure an evolving systems landscape [7].

The automatic procedures that are carried out in ports include cargo management, supply chain information exchange, financial transactions and contract management. Maritime security is also provided in ports for both ships and shore assets and operations. These processes involve communication with authorities, customs, shipping companies, logistics providers, service providers, ship crews, customers and other stakeholders. As such communication at a global scale is paramount for business continuity but also creates challenges for the IT and OT cyber architecture, in achieving the basic objectives of confidentiality, integrity, and availability for cybersecurity. These challenges need to be highlighted as they pertain to cybersecurity of IT/OT systems, components and processes that digitally store, transmit or process data related to operations, financial transactions and personnel management.

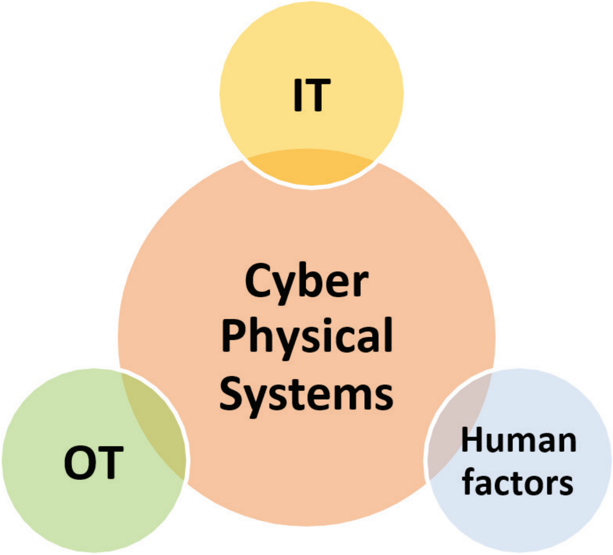

Figure 1: Cyber-physical systems interface.

4. CYBER-PHYSICAL THREATS AND VULNERABILITIES IN PORT INFRASTRUCTURE

Cybersecurity risk in the maritime industry relates to plausible threats to the confidentiality, integrity, and availability of systems and digital information and translates to the ever-present vulnerabilities in IT and OT systems and components. Port components and corresponding risks include [8]:

a) Facility access: This may involve the degradation or disruption of systems used in cargo, transportation and personnel management, which may lead to a complete halt of all operations.

b) Terminal headquarters: This may involve data access by malicious actors aiming to manipulate sensitive data related to cargo and customers. It may also include the destruction of data through malware attacks.

c) OT systems: The compromise of OT systems and components such as cargo handling equipment and fuel systems can lead to operational disruptions, physical damage to cargo and facilities and increased safety and environmental risks in case of an accident taking place.

d) Positioning, Navigation, and Timing (PNT): Loss of PNT services would lead to disruption to logistics systems and vessel maneuvering. It could also lead to physical damage to infrastructure, major safety and environmental incidents such as collisions and allisions, release of hazardous material, fires, loss of life, vessel sinking, and blocking of a navigable channel.

e) Vessel: The operational and technical compromise of vessel or port facility systems could lead to the compromise of additional waterside or landside systems. This can occur due to the interconnectivity of a vessel to shore facilities through Wi-Fi, network connections, USB storage devices, etc.

In general, similar to physical security, the cyber threats faced by ports' infrastructure and their cyber-physical elements can be categorized as internal, external, or colluded [5]. An insider threat can be an individual, ship crew member or port personnel, that intentionally or unintentionally causes the breach of preventive cybersecurity measures (such as IT platforms and software tools) by practicing poor cybersecurity hygiene. From using a virus-infected portable USB device to the reading of malware infected unsolicited emails, the effects of poor "cyber-hygiene" can be detrimental to ports' cyber infrastructure and components. External threats can be defined as those posed by competitors, ordinary cyber-enabled criminals, hackers, hacktivists, state adversaries or terrorists using highly advanced techniques to damage, destroy or take control of IT/OT systems [9]. Colluded threats combine the operation of internal threat actors under the guidance by external adversaries.

5. GOVERNMENTAL AND INDUSTRY INITIATIVES

The combined cyber and physical security for port infrastructure and maritime assets in general is covered mainly through the more common subject of cybersecurity. Various directives, guidelines, standards and other publications from the maritime industry and standardization organizations and various government agencies have been released to tackle the subject. Some of these are described briefly in the below subsections.

5.1 Maritime Industry Organizations

Cybersecurity to include the cyber-physical domain is covered by Resolution MSC.428(98) [10] and Guidance MSC-FAL.1/Circ.3 [11] released by the International Maritime Organization (IMO). MSC.428(98) and MSC-FAL.1/Circ.3 complement the IMO International Ship and Port Facility Security (ISPS) code for vessels with the application of maritime risk management in vessels' safety management systems (SMSs) as required by the ISM (International Safety Management) Code.

5.2 Standardization Organizations

The US National Institute of Standards and Technology (NIST) has created the NIST Cyber Security Framework [12] and a series of standards which are widely used in various industrial sectors, including the maritime industry.

The NIST Cyber Security Framework comprises of five elements: (1) Risk identification for cybersecurity of systems, assets, data and operations; (2) The implementation of safeguards for the cybersecurity protection of assets; (3) Detection of cybersecurity related incidents; (4) Response to cybersecurity related incidents; (5) Recovery from cybersecurity related incidents. The NIST Cyber Security Framework is supplemented by other NIST Special Publications 800-30 [13], 800- 37 [14], and 800-82 [15], that cover the assessment and management of cybersecurity risk for Industrial Control Systems (ICS). NIST has also published Special Publications 1500-201 [16], 1500-202 [17], and 1500-203 [18], which consist of the NIST Framework for Cyber–Physical Systems. The NIST Framework for Cyber–Physical Systems studies the interface of IT and OT systems and components defining the System of Systems (SoS) state of cyber infrastructure. It also delivers a useful aid for the evaluation of cyber-physical systems and is applicable to IT/OT systems in the maritime transportation and infrastructure sectors.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have released ISO/IEC 27001 [19] which can be used in the maritime sector as it assists in the evaluation and management of cybersecurity risks. Published IEC-62443 consist of a series of standards which cover cybersecurity on industrial communication networks for IT/OT systems. IEC- 62443-4-2 [20] specifically outlines the requirements for Industrial Automation and Control Systems (IACS) and presents ways for the management of cybersecurity vulnerabilities. IEC 62443-3-3 [21] explains the security levels of control systems and ISO/IEC 21827 [22] outlines the Systems Security Engineering—Capability Maturity Model® (SSE-CMM®), illustrating the procedure for security engineering for organizations and assets. ISO/IEC 18045 [23] gives guidelines for the assessment of IT systems security. ISO/IEC 15408-1 [24] covers the evaluation of cybersecurity for IT systems and components, defining the Target of Evaluation (TOE) concept. ISO/IEC 27032 [25] tackles the security and protection of critical information infrastructure, data and networks, providing guidance for cybersecurity reinforcement.

The American Society for Testing and Materials (ASTM), has issued standard F3286-17 [26] which utilize the NIST Cyber Security Framework for maritime assets and critical infrastructure and relates to the mitigation of cybersecurity attacks and the reduction of the impact from such security breach incidents. ASTM standard F3449-20 [27] provides guidance for the integration of technical and operational cybersecurity features into vessel safety management systems (SMS), in accordance to the International Safety Management

(ISM) Code and IMO Resolution MSC.428(98).

5.3 Government Agencies

In the USA, the US Congress issued Bill S. 4023 "Enhancing Maritime Cybersecurity Act of 2020"
[28] delegates the implementation of cybersecurity protection strategies and measures to the US Cyber Security and Infrastructure Security Agency (CISA) and the Maritime Administration (MARAD). The US Coast Guard (USCG) issued Navigation and Vessel Inspection Circular (NVIC) 01-20 [29], titled "Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities" [29] guides MTSA-regulated facilities for the assessment and management of vulnerabilities in computer and network systems. NVIC 01-20 promotes the use of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cyber Security and NIST Special Publication 800-82.

The USCG issued Vessel Cyber Risk Management Work Instruction CVC- WI-027 (rev.2, 2021) [30], relates to the reduction of cyber risk to the Marine Transportation System (MTS) through the assessment of cyber risks and vulnerabilities in vessels. In the United Kingdom (UK), a Good Practice Guide in Cybersecurity for Ports and Port Systems (2020) [9] was published by the Institution of Engineering and Technology (IET), the Department for Transport (DfT), the Defense Science and Technology Laboratory (Dstl) and the National Cyber Security Centre (NCSC). This document applies to systems and facilities of ports and encourages the incorporation of cybersecurity into their general security planning process for infrastructure.

Similarly, the Code of Practice for Cybersecurity for Ships (2017) [31] has also been released, providing guidance on the management of operational risk due to cyber-related incidents that could impact the safety and security of the crew, passengers, or cargo of a vessel.
In Europe, the European Union Maritime Security Strategy (EUMSS) Action Plan (2018) [32] addresses cybersecurity for the maritime industry with the intent to strengthen and improve the European Union's (EU) capacity to manage security and enhance the cyber-defense of maritime infrastructure and related systems. EU Regulation 2016/679 [33], also known as the General Data Protection Regulation (GDPR), safeguards the processing of information for various industry sectors to include the maritime industry. EU directive 2016/1148/EU [34] and the EU Cybersecurity Act (2019/881/EU) [35] delegate the operational cybersecurity to the European Union Agency for Network and Information Security (ENISA) and handle the cybersecurity of IT networks. The European Union has also developed a cybersecurity strategy through JOIN/2013/01 [36] in order to apply strategic mitigation tools and policies aiming in the increase of cybersecurity resilience. ENISA has also released related guidance reports in the subjects of cyber risk management [37] and port cybersecurity [38] for ports.

6. CYBER-PHYSICAL SECURITY ASSESSMENT FOR PORTS

The assessment and management of cyber-physical security for assets within the seaport sector requires methodologies that can adapt in the operational and technical parameters of such assets. The maritime transportation sector and its port facilities combine types of operations and assets that fall into the critical infrastructure sector and combine both industrial, facilities and maritime functions. As such the assessment of cyber-physical security risks and vulnerabilities in a proactive and reactive manner needs to adopt methodologies that consider multi-industry technical and operational parameters and provide an "outside-the-box" perspective. This section will provide a brief overview of some useful assessment tools that derive from the cyber and physical security domains in general as well as the oil and gas and industrial sectors.

6.1 API (American Petroleum Institute) Security Risk Assessment (SRA)

The Security Risk Assessment (SRA) methodology derives from the oil and gas sector and is defined in API (American Petroleum Institute) standard (STD) 780 (2013) [39]. It is applicable for a variety of security incidents to include theft, sabotage and terrorism for fixed and mobile assets. SRA can be also applied to various industrial infrastructure and operations including maritime transportation operations. The API SRA methodology manages security risks through a risk-based, performance-oriented management process safeguarding the security and safety of assets, the environment, personnel and business continuity. As per API STD 780 (2013) [39] SRA is a 5-step process which involves: 1) The asset/facility characterization, 2) The assessment of security threats, 3) The assessment of vulnerabilities, 4) The evaluation of risk and 5) Risk treatment.

SRA is applicable to cyber-physical security applications in the maritime industry, as it can assess the physical aspect of security incidents and vulnerabilities as well as the interaction of assets with IT/OT components and infrastructure. The application of the SRA method for a cybersecurity related incident involving a maritime asset has been illustrated by Progoulakis, Rohmeyer and Nikitakos in a recent publication [5].

6.2 Bow-Tie Analysis (BTA)

Bow-Tie Analysis (BTA) is a qualitative method for safety review and as part of Process Safety Management (PSM) is used in the petrochemical, and processing sectors. BTA is primarily used in safety related incidents for the classification of risks, hazards, and consequences in systems, processes and operations. BTA is also applicable for the identification of security mitigation measures for assets, their components and processes. Bow Tie Analysis can also be used in the maritime sector, and specifically for port facilities, for the assessment of interconnections between marine equipment, systems, and processes in safety and security incidents. For cybersecurity applications, Bow Tie Analysis can be utilized to assess the appropriate security mitigation measures for IT/OT assets and processes.

The application of the Bow Tie Analysis method in the cybersecurity of various industrial sectors has been shown through various publications [40, 41, 42, 43, 44]. Specifically, the use of BTA in a cyber-physical security scenario for a maritime asset has been proven by Progoulakis, Rohmeyer and Nikitakos [5]. Bernsmed et al. [45] has also used the Bow Tie Analysis method to analyze cyber-physical security risks in the maritime sector involving navigational communication systems. Shuang-Hua et al. [46] has incorporated BTA in a methodology to concurrently assess risks for security and safety of cyber-physical systems.

As shown in the Bow Tie Analysis (BTA) diagram of Figure 2, cause scenarios are depicted on the left side of the diagram which represent the pre-event side. Results of plausible consequences and scenario are depicted on the post-event and right side of the diagram, along with their corresponding barrier safeguards. The use of the Bow Tie Analysis model showcases the importance of preventive and recovery actions in dealing with security risk. In Bow-Tie Analysis, risk is specified as the probability of a Top Event (hazard release) occurring, combined with the severity of the aftermath of the event. In general Bow Tie Analysis has proved to be an effective method in evaluating cyber and physical security hazards, risks, consequences, and mitigation measures.

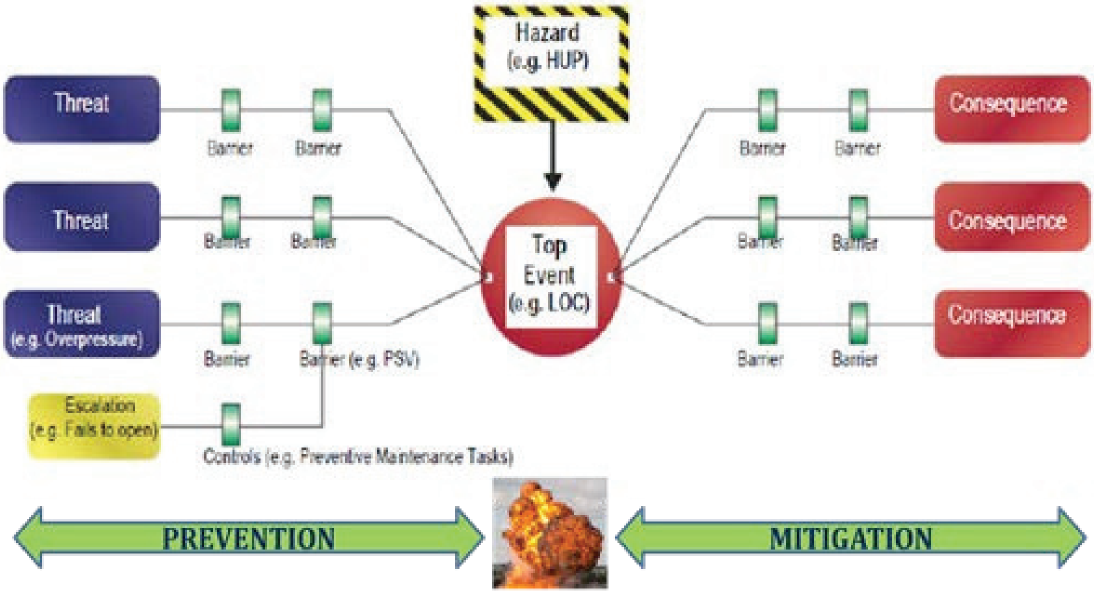

Figure 2 - Bow-Tie Analysis diagram (Source: [47] with information edited by the authors)

6.3 MITRE ATT&CK Threat Model

The MITRE ATT&CK Threat Model [48] is a vulnerability assessment tool capable of evaluating cyberattacks and organizational risks [49]. It can be used when assessment cyberattack behavior, tactics, and techniques of attackers and enables the structure of such data [50] to be utilized by the corporate Chief Information Security Officer (CISO) and cyber intervention team of the maritime asset. The MITRE ATT&CK Threat Model is known for its versatility as it enables the evaluation of IT infrastructure, cloud data storage, portable IT/OT devices, and industrial control systems (ICS) of an asset [49]. It also allows for the classification and certification of adversary behavior after a confirmed breach incident while working within IT and OT systems and infrastructure of the maritime asset.

7. CONCLUSIONS AND DISCUSSION

Ending this paper, the following conclusions and discussions points are derived:

(1) The evaluation of presented government and industry directives and standards has illustrated their inadequacy in covering the OT side of systems in ports infrastructure. Interoperability of IT and OT systems and the mitigation of credible threats are not tackled in a manner enabling the asset owners and operators in implementing the necessary measures and practices.

(2) The physical protection of assets, processes and IT and OT components needs to be enhanced so that credible threats by insider malicious actors are prevented. IT and OT components vulnerable to mishandling and manipulation need to be secured so that to mitigate potential cyber threats.

(3) The exploration of IT/OT vulnerabilities needs to be improved by port asset operators and owners. This can be achieved by the assessment of internal and external processes, stakeholder communications and IT/OT functions. Through this process existing mitigation measures can be evaluated, and potential vulnerabilities will be exposed.

(4) The use of available cybersecurity assessment methods from industrial sectors other than the maritime should be explored. The use of the API SRA method and the BTA method can be valuable tools in assessing technical and operational risks, vulnerabilities and measures in IT and OT components and functions. Their combination with the use of the MITRE ATT&CK Threat Model can enhance the insight of the attackers' behavior, and tactics and could be applied to industrial control systems (ICS), IT infrastructure, cloud storage and mobile devices.

(5) Training of port infrastructure personnel, vessel crews and maritime industry operatives in general should be pursued to a level higher that the current industry standards. It is apparent that human factors are very important in the integrity or failure of security measures in the physical and cyber domain of ports' infrastructure and operations.

(6) It is recommended that the convergence of cyber and physical security for the ports' infrastructure and vessels is pursued by asset owners and operators. This convergence involving operations and stakeholder management could improve the implementation of cyber and physical security policies, cyber risk reduction and threat mitigation.

8. REFERENCES

1. K.A. Pesch-Cronin and N.E. Marion, Critical Infrastructure Protection, Risk Management and Resilience – A Policy Perspective. CRC Press, Taylor & Francis Group, LLC, FL, 2017.

2. M. Stopford, Maritime Economics, 3rd Edition. Routledge, NY 2009.

3. "Maritime Cyber Attacks Increase 900%", https://www.maritimeprofessional.com/news/maritime- cyber-attacks-increase-360262, 2020, accessed 10 January 2022.

4. "Cybermarétique: a short history of cyberattacks against ports", https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/, 2021, accessed 10 January 2022.

5. Progoulakis, Iosif, Paul Rohmeyer, and Nikitas Nikitakos. 2021. "Cyber Physical Systems Security for Maritime Assets" Journal of Marine Science and Engineering 9, no. 12: 1384. https://doi.org/10.3390/jmse9121384

6. Dahman, J.S.; Baldwin, K.J. Understanding the current state of US defense systems of systems and the implications for systems engineering. In Proceedings of the 2nd Annual IEEE Systems Conference, Montreal, QC, Canada, 7–10 April 2008.

7. Zarzuelo, I.; Soeane, M.; Bermudez, B. Industry 4.0 in the port and maritime industry: A literature review. J. Ind. Inf. Integration. 2020, 100173.

8. U.S. Department of Homeland Security (DHS), Cyber Infrastructure and Security Agency (CISA), Port Facility Cybersecurity Risks Infographic, available online: https://www.cisa.gov/publication/port- facility-cybersecurity-risks , accessed 05 January 2022.

9. UK Institution of Engineering and Technology (IET) Good Practice Guide. Cyber Security for Ports and Port Systems; UK Institution of Engineering and Technology: London, UK, 2020.

10. International Maritime Organization (IMO) Resolution MSC. Maritime Cyber Risk Management in Safety Management Systems; International Maritime Organization: London, UK, 2017; Volume 428.

11. International Maritime Organization (IMO) Resolution MSC-FAL.1/Circ.3. Guidelines on Maritime Cyber Risk Management; International Maritime Organization: London, UK, 2017.

12. National Institute of Standards and Technology (NIST) Cyber Security Framework. Available online: https://www.nist.gov/cyberframework (accessed on 15 December 2021).

13. National Institute of Standards and Technology (NIST) Special Publication 800-30, Guide for Conducting Risk Assessments. 2012. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (accessed on 13 December 2021).

14. National Institute of Standards and Technology (NIST) Special Publication 800-37, Risk Management Framework for Information Systems and Organizations—A System Life Cycle Approach for Security and Privacy. 2018. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (accessed on 23 December 2021).

15. National Institute of Standards and Technology (NIST) Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security. 2015. Available online: https://csrc.nist.gov/publications/detail/sp/800- 82/rev-2/final (accessed on 20 December 2021).

16. National Institute of Standards and Technology (NIST) Special Publication 1500-201, Framework for Cyber-Physical Systems: Volume 1, Overview. 2017. Available online: https://doi.org/10.6028/NIST.SP.1500-201 (accessed on 26 December 2021).

17. National Institute of Standards and Technology (NIST) Special Publication 1500-202, Framework for Cyber-Physical Systems: Volume 2, Working Group Reports. 2017. Available online: https://doi.org/10.6028/NIST.SP.1500-202 (accessed on 29 December 2021).

18. National Institute of Standards and Technology (NIST) Special Publication 1500-203, Framework for Cyber-Physical Systems: Volume 3, Timing Annex. 2017. Available online: https://doi.org/10.6028/NIST.SP.1500-203 (accessed on 20 December 2021).

19. International Organization for Standardization/International Electrotechnical Commission standard ISO/IEC 27001. Information Technology—Security Techniques—Information Security Management Systems—Requirements; International Organization for Standardization: Geneva, Switzerland, 2013.

20. International Electrotechnical Commission standard IEC-62443-4-2. Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components; International Organization for Standardization: Geneva, Switzerland, 2019.

21. International Electrotechnical Commission standard IEC 62443-3-3. Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels; International Organization for Standardization: Geneva, Switzerland, 2013.

22. International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 21827. Information Technology—Security Techniques—Systems Security Engineering— Capability Maturity Model® (SSE-CMM®); International Organization for Standardization: Geneva, Switzerland, 2008.

23. International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 18045. Information Technology—Security Techniques—Methodology for IT Security Evaluation; International Organization for Standardization: Geneva, Switzerland, 2008.

24. International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 15408-1. Information Technology—Security Techniques—Evaluation Criteria for IT Security; International Organization for Standardization: Geneva, Switzerland, 2009.

25. International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 27032. Information Technology—Security Techniques—Guidelines for Cybersecurity; International Organization for Standardization: Geneva, Switzerland, 2012.

26. American Society for Testing and Materials standard ASTM F3286-17. Standard Guide for Cybersecurity and Cyberattack Mitigation; ASTM International: West Conshohocken, PA, USA, 2017.

27. American Society for Testing and Materials standard ASTM F3449-20. Standard Guide for Inclusion of Cyber Risks into Maritime Safety Management Systems in Accordance with IMO Resolution MSC.428(98)- Cyber Risks and Challenges; ASTM International: West Conshohocken, PA, USA, 2020.

28. U.S. Congress Bill S. 4023 Enhancing Maritime Cybersecurity Act of 2020. 22 June 2020. Available online: https://www.govtrack.us/congress/bills/116/s4023/text (accessed on 19 December 2021).

29. U.S. Coast Guard, U.S. Department of Homeland Security, Navigation and Vessel Inspection Circular (NVIC) 01-20 Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities. 26 February 2020. Available online: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01- 20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023 (accessed on 10 December 2021).

30. U.S. Coast Guard, U.S. Department of Homeland Security, Office of Commercial Vessel Compliance (CG-CVC) Mission Management System (MMS) Work Instruction (WI) CVC-WI-027 "Vessel Cyber Risk Management Work Instruction. 18 February 2021. Available online: https://www.dco.uscg.mil/Portals/9/CVC-WI-27%282%29.pdf (accessed on 23 December 2021).

31. UK Institution of Engineering and Technology (IET) Guidance document. Code of Practice: Cyber Security for Ships; UK Institution of Engineering and Technology: London, UK, 2017.

32. Council of the European Union, 10494/18. Council Conclusions on the Revision of the European Union Maritime Security Strategy (EUMSS) Action Plan; Council of the European Union: Brussels, Belgium, 2018.

33. European Union, Directive 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available online: https://eur-lex.europa.eu/legal- content/EN/TXT/?qid=1599862836456&uri=CELEX:32016R0679 (accessed on 10 December 2021).

34. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. Available online: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed on 13 January 2022).

35. European Union, Directive 2019/881/EU on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Available

online: https://eur- lex.europa.eu/eli/reg/2019/881/oj (accessed on 14 January 2022).

36. Joint Communication to The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Join/2013/01 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Available online: https://eur-lex.europa.eu/legal- content/EN/TXT /?qid=1553779410177&uri =CELEX:52013JC0001 (accessed on 15 January 2022).

37. ENISA Report. Cyber Risk Management for Ports: Guidelines for Cybersecurity in the Maritime Sector. 2020. Available online: https://www.enisa.europa.eu/publications/ guidelines-cyber-risk-management- for-ports (accessed on 27 December 2021).

38. ENISA Report. Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector. 2019. Available online: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector /at_download/fullReport (accessed on 28 December 2021).

39. American Petroleum Institute (API), May 2013, Recommended Practice (RP) 780: Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries.

40. Center for Chemical Process Safety (CCPS), The Energy Institute. Bow Ties in Risk Management: A Concept Book for Process Safety; John Wiley & Sons Inc.: Hoboken, NJ, USA, 2018.

41. American Bureau of Shipping (ABS). American Bureau of Shipping (ABS) Technical Report. In Bowtie Applications for the Marine and Offshore Industries; American Bureau of Shipping (ABS): Houston, TX, USA, 2013.

42. DRAGOS Inc and OSIsoft Inc White Paper: Using Bow Tie Risk Modeling for Industrial Cybersecurity, DRAGOS Inc., 2021. Available online: https://www.dragos.com/resource/using-bow-tie-risk-modeling- for-industrial-cybersecurity/ (accessed on 15 December 2021).

43. aeBlogs: The Benefits of Visualizing CyberPHAs Using Bowtie Diagrams. aeSolutions Inc. Available online: https://www.aesolutions.com/post/The-benefits-of-visualizing-cyberphas-using-bowtie- diagrams (accessed on 10 January 2022).

44. SANS Institute Information Security Reading Room White Paper: Evaluating Cyber Risk in Engineering Environments: A Proposed Framework and Methodology. Rebekah Mohr. 2016. Available online: https://www.sans.org/white-papers/37017/ (accessed on 10 January 2022).

45. Bernsmed, K.; Frøystad, C.; Meland, P.H.; Nesheim, D.A.; Rødseth, Ø.J. Visualizing Cyber Security Risks with Bow-Tie Diagrams. In Graphical Models for Security, GraMSec 2017; Lecture Notes in Computer Science; Liu, P., Mauw, S., Stolen, K., eds.; Springer: Cham, Switzerland, 2018; Volume 10744. Available online: https://doi.org/10.1007/978-3-319-74860-3_3 (accessed on 28 December 2021).

46. Ji, Z.; Shuang-Hua, Y.; Yi-jia, C.; Yuchen, W.; Chenchen, Z.; Liang, Y.; Yinqiao, Z. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process. Saf. Environ. Prot. 2021, 148, 1279–1291.

47. HAMZAH, S., Z., (ABS Consulting), 2012, Use Bow Tie Tool for Easy Hazard Identification. , Presentation to the 14th Asia Pacific Confederation of Chemical Engineering Congress.

48. The MITRE Corporation. “MITRE ATT&CK®”, The MITRE Corporation. 2016. Available online: https://attack.mitre.org/ (accessed on 4 December 2021).

49. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. Sensors 2021, 21, 3267. Available online: https://doi.org/10.3390/s21093267 (accessed on 4 December 2021).

50. MITRE Report MP180360R1. MITRE ATT&CK®: Design and Philosophy. 2020. Available online: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf (accessed on 4 December 2021).