SCIENTIFIC JOURNAL OF MARITIME RESEARCH [POMORSTVO]
University of Rijeka FACULTY OF MARITIME STUDIES

https://doi.org/10.31217/p.40.1.6

Cybersecurity of Onshore Power Supply (OPS) Systems: Overview of EU Standards, Regulations, and Audit Procedures

Matej Plenča[1*], Saša Aksentijević[1], Edvard Tijan[1], Srđan Skok[2]

[1] University of Rijeka, Faculty of Maritime Studies, Studentska ulica 2, 51000 Rijeka, Croatia; e-mail: matej.plenca@pfri.uniri.hr; sasa.aksentijevic@pfri.uniri.hr; edvard.tijan@pfri.uniri.hr

[2] University North, 104. brigade 1, 42000 Varaždin, Croatia, e-mail: srdan.skok@unin.hr

[*] Corresponding author

ARTICLE INFO

Review article
Received 3 September 2025
Accepted 28 October 2025

Key words:
Maritime cybersecurity
Energy sector cybersecurity
Shore power integration
Critical infrastructure protection
Operational technology security
Cyber-physical systems
Maritime-energy convergence

ABSTRACT

This paper reviews cybersecurity standards, regulations, and audit procedures relevant to EU Onshore Power Supply systems. These systems link maritime and energy infrastructures via high-capacity ship-to-shore connections. Such hybrid operational technology environments introduce vulnerabilities that neither maritime nor energy sector standards fully address. Using a qualitative, comparative review, the authors evaluate key frameworks. Analysis reveals gaps in authentication, mutual assurance, runtime monitoring, incident response, and management of legacy operational technology. The findings provide a foundation for risk-informed, cross-sector cybersecurity audits and highlight the need for harmonized yet adaptable security requirements to safeguard Onshore Power Supply-enabled ports against evolving cyber threats.

1 Introduction

The maritime and energy sectors are on the brink of an unprecedented technological convergence that fundamentally reshapes the cybersecurity landscape of both industries. The European Union's FuelEU Maritime regulation, which entered into force on January 1, 2025, mandates that container ships and passenger vessels above 5,000 GT connect to onshore power supply (OPS) systems when calling at EU ports from 2030 onwards [1]. New regulatory requirement, coupled with the Alternative Fuels Infrastructure Regulation (AFIR), created a critical cybersecurity challenge: the direct integration of mobile maritime operational technology (OT) systems with stationary energy infrastructure networks [2]. This convergence represents more than a simple electrical connection; it establishes a direct cyber pathway between two previously isolated critical infrastructure domains. When ships connect to shore power systems, they create temporary but high-capacity data and control channels that bridge maritime vessel networks with terrestrial electrical grids, port management systems, and broader energy infrastructure networks. This integration introduces novel attack vectors that neither sector's existing cybersecurity frameworks adequately address, creating a significant security gap in critical infrastructure protection.

The cybersecurity implications of this convergence are profound. Maritime OT systems, traditionally designed with air-gapped architectures that assumed physical isolation from external networks, suddenly interface directly with energy sector infrastructure that operates under fundamentally different security paradigms. Shore power connections create bidirectional pathways for cyber threats, where malware could potentially propagate from compromised ship systems to

port electrical infrastructure, or conversely, from compromised energy systems to vessel control systems [3]. This creates scenarios where a cyberattack targeting a single vessel could cascade through shore power infrastructure to affect multiple ships, port operations, or even regional electrical grids.

The convergence of maritime and energy systems through shore power connections presents cybersecurity challenges that are qualitatively different from those faced by either sector independently. Traditional maritime cybersecurity frameworks, such as the International Maritime Organization's Resolution MSC.428(98) and the International Association of Classification Societies' Unified Requirements E26 and E27, were developed primarily to address threats to isolated ship systems or ship-to-shore communications via satellite links [4]. These frameworks assume that ship systems can maintain operational security through network segmentation and controlled access points.

Similarly, energy sector cybersecurity standards, including the IEC 62443 series and European implementations of the NIS2 Directive, were designed to protect stationary infrastructure with predictable connection patterns and controlled access environments [5]. These standards assume that all connected devices can be catalogued, monitored, and maintained according to consistent security policies over extended periods.

Shore power operations fundamentally challenge both sets of assumptions. Ships arrive at ports with unknown cybersecurity postures, potentially carrying malware or system vulnerabilities acquired during their voyages [6]. The temporary nature of shore power connections means that energy infrastructure must accommodate frequent connections and disconnections of systems that cannot be continuously monitored or maintained to consistent security standards. This creates what cybersecurity experts describe as a "trust boundary problem" - the need to establish secure communications between systems that operate under different security policies and threat models [6].

The scale and complexity of this challenge are amplified by the mandatory nature of shore power connections under EU regulations. Unlike voluntary technology adoptions that can be implemented gradually with extensive security testing, the FuelEU Maritime requirements create compliance deadlines that may pressure rapid deployment of shore power infrastructure without adequate cybersecurity consideration [1]. The regulation's requirement for container and passenger ships to connect to shore power at major EU ports by 2030, and all EU ports with available shore power by 2035, means that thousands of vessels and hundreds of ports must implement these connections within a compressed timeframe.

The cybersecurity risks associated with shore power connections extend far beyond individual vessels or ports to encompass broader critical infrastructure vulnerabilities. Modern electrical grids operate as interconnected systems where localized disruptions can cascade to create regional or national impacts [3]. The integration of multiple ships with shore power systems creates new pathways for such cascading effects, particularly given the high-power demands of large commercial vessels.

Container ships and passenger vessels requiring shore power connections typically demand several megawatts of electrical power, comparable to small industrial facilities [3]. This high-power consumption means that shore power systems often connect directly to medium-voltage distribution networks rather than low-voltage consumer circuits. Consequently, cybersecurity vulnerabilities in shore power operations could potentially affect electrical distribution systems serving broader port areas or even regional grids.

The critical infrastructure implications are further amplified by the concentration of shore power operations at major European ports. Ports such as Rotterdam, Hamburg, Antwerp, and others manage significant percentages of European maritime trade. A coordinated cyberattack targeting shore power systems at multiple major ports could simultaneously disrupt maritime logistics and electrical infrastructure across multiple EU member states, creating cascading economic and security impacts [7].

Geopolitical tensions during 2020s have heightened concerns about state-sponsored cyberattacks targeting critical infrastructure. NATO's Cooperative Cyber Defence Centre of Excellence has specifically identified maritime ports as targets for state-linked cyber operations, noting that Russia, Iran, and China have launched sophisticated attacks against port infrastructure [8]. The integration of shore power systems creates additional attack surfaces that could be exploited by nation-state actors seeking to disrupt European energy and transportation infrastructure.

Despite the mandatory nature of shore power connections under EU regulations, neither the FuelEU Maritime regulation nor the AFIR explicitly addresses cybersecurity requirements for these systems. This regulatory gap creates uncertainty for both maritime operators and port authorities regarding their cybersecurity obligations when implementing shore power infrastructure. While the NIS2 Directive establishes broad cybersecurity requirements for maritime transport operators and port facilities, it does not provide specific guidance for managing the cybersecurity risks created by shore power operations [9].

Existing maritime cybersecurity standards, including the IACS Unified Requirements and IMO guidelines, focus primarily on shipboard systems and ship-to-shore communications via traditional channels such as satellite communications [10]. These standards do not adequately address the cybersecurity requirements for

direct electrical and data connections between ships and shore infrastructure. Similarly, energy sector cybersecurity standards were developed for stationary infrastructure and do not account for the unique challenges of temporary connections with mobile systems that cannot be continuously monitored or controlled. This standards gap is particularly concerning given the complexity of shore power operations. Modern shore power systems incorporate sophisticated control and monitoring technologies, including smart meters, automated connection systems, load management capabilities, and integration with port management systems [11].

This paper addresses the emerging cybersecurity challenges of mandatory shore power integration by systematically examining the adequacy of existing standards and regulations at the maritime energy interface. The central hypothesis is that the novel integration of energy systems into maritime operations requires systematic analysis and the application of harmonized cross-sector frameworks in information systems auditing, to ensure resilient, secure, and compliant shore power operations.

The research examines the applicability of the NIS2 Directive to maritime energy convergence, reviews IMO and IACS requirements for shore power operations, evaluates IEC 62443 standards for hybrid systems, and identifies regulatory and technical gaps [9]. It also considers emerging cybersecurity technologies and risk management approaches, focusing on European frameworks but including international standards to reflect the global nature of shipping.

The first chapter introduces the regulatory and technological context of maritime – energy convergence and formulates the research hypothesis. The second chapter details the qualitative, comparative research methodology based on a systematic review and standards analysis conducted under the PRISMA framework. The third chapter presents the analytical results, focusing on the cyber-physical integration of maritime and energy infrastructures, identifying shared vulnerabilities, and evaluating the relevance of sector-specific cybersecurity frameworks. The fourth chapter discusses the overlapping and fragmented nature of current regulations, emphasizing interoperability challenges, standard redundancies, and the necessity of continuous auditing and adaptive governance mechanisms. The final chapter concludes with recommendations for harmonized cross-sector standards, coordinated incident management, and the development of dynamic cybersecurity strategies to ensure resilient and secure OPS-enabled port operations.

2 Materials and methods

This review article employs a qualitative, comparative methodology to analyse and synthesize existing cybersecurity standards relevant to the maritime and energy sectors, with a particular focus on the emerging intersection created by mandatory shore power connectivity under EU regulation. The methodology integrates three principal dimensions: regulatory review, standards analysis, and risk-focused contextual interpretation.

The selection of documents and frameworks for analysis was guided by three primary criteria: (1) formal recognition by international or European regulatory bodies; (2) sectoral relevance to operational technology (OT) or industrial control systems (ICS); and (3) practical applicability to integrated port and ship environments [7]. Key standards include the IEC 62443 series, the ISO/IEC 27000 family, IMO guidelines, IACS unified requirements, and the EU NIS2 Directive. Although U.S.-based frameworks such as the NIST Cybersecurity Framework and NERC CIP are not legally binding in the European context, they were included for their methodological depth and established industry relevance.

A systematic literature review was conducted using primary sources such as international standards, regulatory directives, and sector-specific technical guidelines. Supplementary analysis was derived from academic publications, technical reports, and audit documentation provided through professional engagement. The article also incorporates findings from previously conducted audits and national-level case studies, including audit reporting standards from other industries, to ground theoretical frameworks in practical audit outcomes.

This multi-source, multi-framework comparison enables the identification of regulatory overlaps, gaps, and areas of misalignment. The goal is to assess the sufficiency of current cybersecurity frameworks in addressing the cyber-physical convergence that characterizes shore power infrastructure. The outcome of this methodological approach is not only a descriptive account of existing standards but also a normative evaluation of their ability to safeguard critical maritime-energy interfaces.

To deepen the understanding of cybersecurity challenges emerging from the convergence of maritime and energy infrastructures, a comprehensive literature review was conducted, following the simplified PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure methodological rigor and transparency in the literature review process [12]. The objective of this systematic review was to identify, evaluate, and synthesize existing research addressing cybersecurity in Onshore Power Supply (OPS) systems, the integration of maritime operational technology (OT) with energy infrastructure, and relevant regulatory and technical frameworks.

The search strategy combined the keywords *"maritime cybersecurity," "onshore power supply," "critical infra-*

structure protection," "energy systems," and *"operational technology"* using Boolean operators (AND/OR). Searches were performed in major academic databases including *Web of Science*, *Scopus*, and *ScienceDirect*, covering journal articles, book chapters, and conference papers published in English language between 2021. and 2025.

A total of 47 papers were initially identified through targeted database searches. Additional 11 publications were obtained from secondary sources, including reference list cross-checking, citation tracing, and author recommendations. After removing duplicates, 52 papers remained for detailed review.

Following the title and abstract screening, 31 papers were excluded due to limited relevance to the cybersecurity aspects of Onshore Power Supply (OPS) systems, lack of technical depth regarding industrial control systems (ICS) or operational technology (OT), or insufficient methodological quality. Consequently, 29 studies were included in the final qualitative synthesis, providing a solid foundation for identifying patterns, regulatory gaps, and future research directions in maritime-energy cybersecurity integration.

This systematic process ensured that the literature review captured the most relevant and recent academic and technical contributions addressing the cybersecurity implications of OPS implementation. The complete selection procedure is summarized in Figure 1, which presents the PRISMA flow diagram outlining the stages of identification, screening, eligibility assessment, and inclusion.

The systematic approach illustrated in Figure 1 establishes the methodological foundation for the subsequent analysis, thereby ensuring that the examination of existing standards and frameworks in the following sections is grounded in a comprehensive, coherent, and rigorously validated body of research. This structured

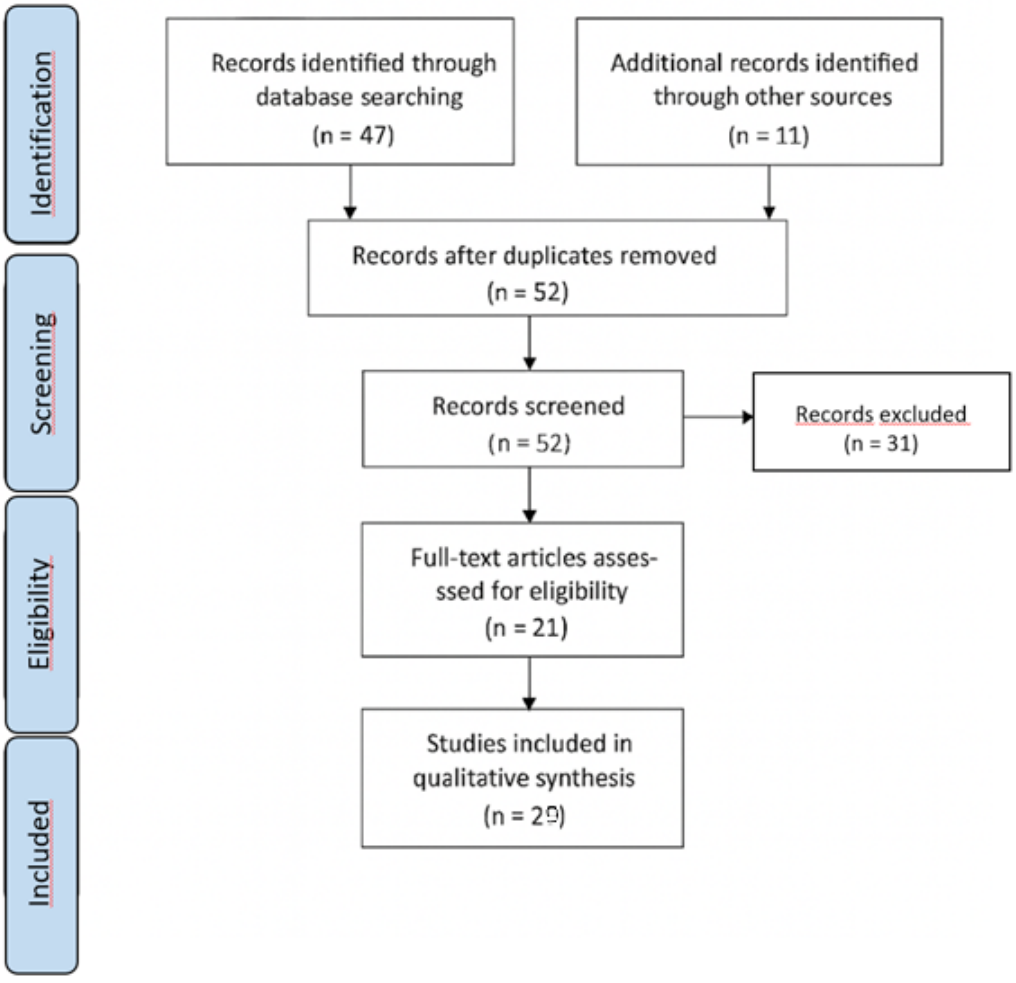

Figure 1 PRISMA Flow Diagram of the Systematic Literature Review Process

Source: Created by the Authors

foundation enables a consistent analytical perspective, facilitating the integration of diverse regulatory, technical, and operational dimensions of OPS cybersecurity into a unified and evidence-based evaluative framework.

3 Results

This chapter provides results of the structured analysis of the cyber-physical integration between maritime operational technologies and energy systems, focusing on the conceptual mechanisms and security architectures that underpin Onshore Power Supply (OPS) operations.

Several studies have analyzed maritime cybersecurity from a strategic and regulatory perspective. Kavallieratos and Katsikas [6] explored cyber risk management for cyber-enabled ships, emphasizing the need for layered defences and procedural risk assessment. Their study introduced a structured approach to ship-level cybersecurity management, aligning with the IMO's Safety Management System requirements. However, as their research focused primarily on shipboard OT, it did not address the challenges of direct connectivity between ships and onshore infrastructure, which is the central issue of OPS integration. Similarly, Tombak et al. [3] identified cybersecurity risks at ports, highlighting the vulnerabilities of port information systems and control networks. Their work underscored the systemic nature of maritime cyber threats but stopped short of analyzing how these risks extend through energy distribution systems, a gap directly addressed in this paper.

From the energy sector perspective, Alomari et al. [7] and Ige et al. [14] examined cybersecurity in smart grids and renewable energy systems, identifying malware, unauthorized access, and cascading failures as key vulnerabilities. Both studies employed a technical and conceptual approach, proposing a layered defence strategy that resonates strongly with the risks in OPS environments. Their findings support the argument that energy sector frameworks such as IEC 62443 can provide a foundation for securing hybrid maritime–energy infrastructures.

At the regulatory level, Melnyk et al. [18] offered an international overview of cybersecurity governance in maritime transport, emphasizing discrepancies between IMO guidelines, EU directives, and national regulations. Their analysis pointed out that while global conventions establish general obligations, sector-specific adaptation is essential for operational environments like ports and OPS systems. This view is supported by the European Parliament's NIS2 Directive [9], which mandates minimum cybersecurity measures across critical sectors, including energy and maritime transport, but leaves the technical implementation open to sectoral interpretation.

The International Maritime Organization's Resolution MSC.428(98) and the IACS Unified Requirements UR E26 and UR E27 are pivotal maritime standards discussed in several identified sources [4,16]. Potamos et al. [16] focused on integrating operational technology sensor data for improved situational awareness in ship cybersecurity, illustrating the growing importance of OT monitoring in preventing cyber incidents. However, these standards and studies remain ship-centric and do not explicitly address shore-based system interoperability, underscoring the need for cross-sector alignment.

On the industrial control side, Cindrić et al. [12] mapped Industrial Internet of Things (IIoT) applications to IEC 62443 standards, demonstrating their relevance for system design and secure network architecture. Their approach reinforces the adaptability of IEC 62443 to hybrid maritime–energy environments. Similarly, Ryu et al. [15] proposed a layered defence model for energy IT infrastructure, highlighting malware resilience and proactive monitoring, both critical for OPS security.

The academic debate also includes analyses of technological convergence in smart port environments. Akyildiz [11] conceptualized port cybersecurity and threat domains, stressing the importance of organizational awareness and proactive defence. De Peralta et al. [17] examined the legal and operational challenges of maritime cyber protection, identifying gaps in compliance and inter-organizational coordination. Both studies reinforce the premise that cybersecurity in ports must be managed holistically, accounting for both IT and OT systems connected through shore power operations.

In addition to academic literature, several technical and regulatory documents provide essential context. The European Commission's Directorate-General for Mobility and Transport [4] outlines the policy framework underpinning the FuelEU Maritime and AFIR regulations, which form the legal foundation for OPS deployment. Likewise, Sulzer [8] and Zgaljic et al. [19] addressed the broader implications of port security, resilience, and performance, particularly in the context of hybrid threats and modal shifts in transport systems.

The reviewed literature consistently highlights the fragmented nature of current cybersecurity frameworks when applied to the hybrid maritime–energy domain. While maritime research largely concentrates on vessel-level risks and operational continuity, and energy research focuses on grid security and automation, few studies integrate both perspectives. This paper therefore builds on the identified gaps by synthesizing existing standards – including NIS2, IEC 62443, IMO MSC.428(98), and IACS UR E26/E27 – and proposing an analytical framework for harmonized, cross-sector cybersecurity governance in Onshore Power Supply systems.

This limited number of relevant sources indicates that the topic is still insufficiently researched and that

there is a notable gap in the academic literature concerning the cybersecurity aspects of Onshore Power Supply (OPS) systems and their intersection with maritime and energy infrastructures.

Figure 2 illustrates the bidirectional flow of data and control between shipboard operational technology (OT) and onshore industrial control systems (ICS), highlighting the shared cybersecurity vulnerabilities, regulatory overlap (IMO, IACS, IEC, NIS2), and the potential attack vectors created by temporary high-capacity connections. The model emphasizes the need for harmonized cross-sector frameworks to manage the evolving threat surface.

Historically, maritime vessels and energy networks operated as discrete critical infrastructures. Ships relied on air-gapped OT systems for propulsion, navigation, and safety, while energy facilities developed their own control environments to ensure grid stability [4]. With the push towards decarbonization and smarter port operations, these once-isolated systems now intersect via sophisticated shore power connections and automated port management platforms [7]. The rapid advance of digitalization within critical infrastructure has dissolved traditional sectoral boundaries, giving rise to highly interconnected cyber-physical systems. In the maritime and energy sectors, the introduction of shore power requirements, mandating direct connection between ships and port electrical infrastructure, exemplifies this integration [13]. While the environmental and operational benefits of such systems are evident, the convergence of maritime and energy operational technologies (OT) with information technology (IT) presents unprecedented security challenges that transcend the scope of legacy approaches [14]. This chapter presents research of the emerging cyber-physical reality at the maritime-energy interface and reviews the standards landscape shaping its security paradigm.

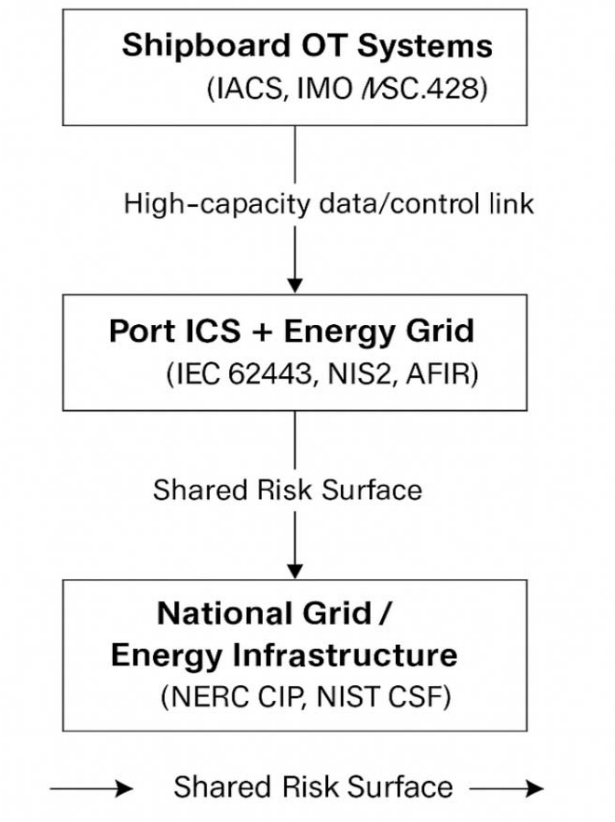

Figure 2 Conceptual Model of Cybersecurity Convergence at the Maritime – Energy Interface

Source: Created by the Authors

The main security dilemma introduced by cyber-physical integration is the erosion of traditional security perimeters. Ships interface with shore-based OT, often via transient but high-capacity links, exposing otherwise isolated OT environments to risks, such as malware transmission, unauthorized access, or disruption by malicious actors [15]. The risk profile evolves dynamically based on connections established, protocols used, and the underlying trust models.

In the new paradigm, threat actors may exploit weaknesses in either the vessel's onboard systems or the port's energy management systems to compromise the other [16]. The spectrum of attack scenarios now includes manipulation of propulsion or steering via the shore link, infection of port control platforms by compromised vessels, and even grid disturbances originating from vessel-side cyber faults.

Existing cybersecurity standards approach the problem from sector-specific perspectives. The International Maritime Organization's MSC.428(98) and IACS Unified Requirements E26 and E27 provide the backbone for maritime cyber management, focusing on the ship as the primary asset [14]. In parallel, the energy sector employs IEC 62443 for industrial control system security and, in the EU, falls under the cross-sectoral NIS2 Directive [9].

IEC 62443 stands out as the most technically comprehensive, offering frameworks for secure design, implementation, and operation of interconnected ICS/OT. It is increasingly viewed as a bridge standard capable of informing both ship- and shore-based cybersecurity practices, particularly at the electric interface [9]. However, neither maritime nor energy sector standards alone provide a holistic solution for cyber-physical integration. Gaps persist in the areas of authentication during connection, mutual security assurance, runtime monitoring, incident response coordination, and the management of legacy OT that was never intended to interface directly with external systems [17].

The NIS2 Directive, while regulatory rather than technical, creates a cross-sector governance structure. It mandates incident reporting, supply chain security, and minimum risk management, applicable to both ports

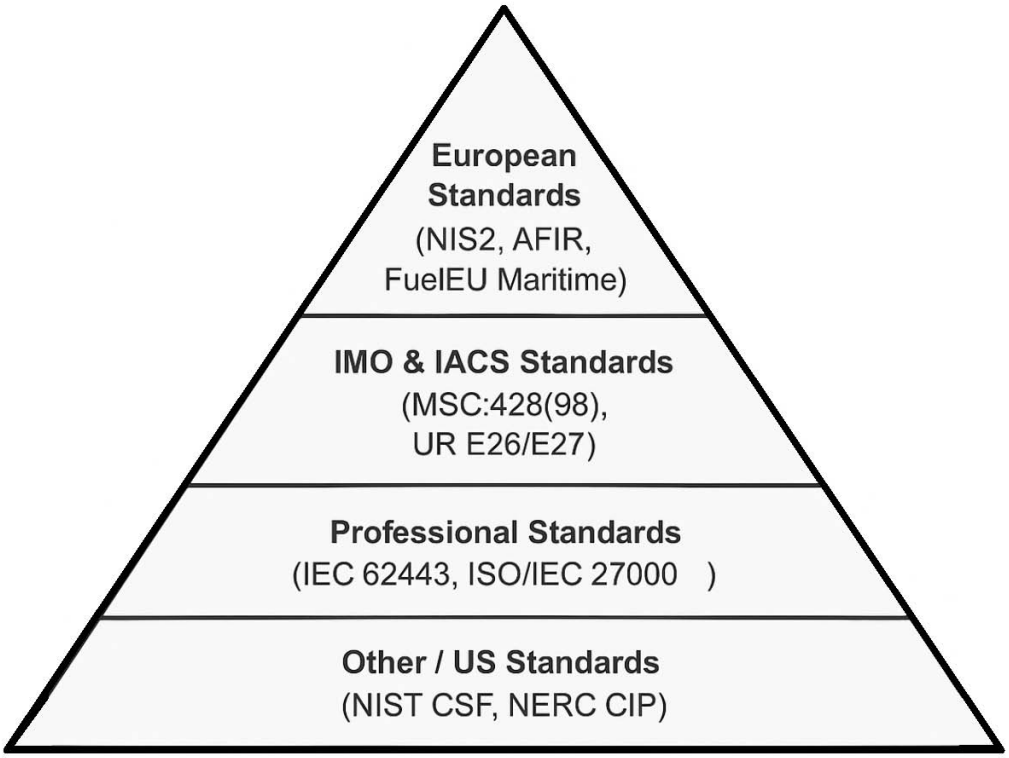

Figure 3 Hierarchical Structure of Cybersecurity Standards Relevant to OPS Systems

Source: Created by the Authors

and energy operators [5]. However, its implementation depends on sector-specific harmonization, making collaboration and joint interpretation essential for securing cyber-physical processes such as shore power.

Despite their strengths, all existing frameworks require adaptation to fully address cyber-physical integration when used at the intersection of the maritime and energy sectors. Effective security must account for both the IT-centric threats and OT-centric operational hazards, prioritizing resilience, safety, and business continuity across the interconnected system [18].

Industrial cybersecurity standards serve as foundational frameworks to secure operational technology and industrial control systems (ICS) that underpin critical infrastructures such as energy grids and maritime operations. The following overview groups key standards and frameworks, highlighting their scope, applicability, and relevance to the maritime-energy convergence, especially in the context of shore power connections. [10]

As it is evident in Figure 3, the hierarchical structure situates European regulatory instruments (e.g., NIS2, AFIR, FuelEU Maritime) as overarching frameworks, succeeded by international maritime regulations (IMO MSC.428(98), IACS UR E26/E27), professional and industrial standards (IEC 62443, ISO/IEC 27000), and globally influential U.S. frameworks (NIST CSF, NERC CIP). This stratified configuration underscores that ensuring OPS cybersecurity effectiveness necessitates comprehensive alignment and coordination across regulatory, organizational, and technical domains.

Although not legally binding in Europe, the NIST CSF's comprehensive risk management approach is valuable in the energy sector and offers transferable concepts for managing the cyber risks presented by the integration of shipboard OT with shore-based energy infrastructure [19]. Its adaptability makes it a useful benchmark when addressing the growing complexity of connected maritime and energy systems.

3.1 European Union NIS2 Directive

The Network and Information Security Directive 2 (NIS2) represents a harmonized European regulatory framework that mandates risk management, incident reporting, and supply chain security across eighteen critical sectors, including maritime transport and energy providers. NIS2 introduces binding obligations for port authorities, shipping companies, and energy operators, aiming to enhance the cyber resilience of critical infrastructure throughout the European Union.

NIS2's cross-sector scope and unified governance model provide an essential regulatory foundation to address the cybersecurity challenges arising from maritime-energy integration via shore power systems.

However, the directive intentionally remains high-level, requiring sector-specific guidelines and standards to fill in detailed operational cybersecurity requirements for shore power setups [9].

3.2 IEC 62443 Series

Developed by the International Electrotechnical Commission (IEC), the IEC 62443 series targets security for Industrial Automation and Control Systems (IACS) across diverse sectors, including both maritime and energy industries. This standard framework addresses cybersecurity across the full lifecycle of systems, from initial design to operation and maintenance, emphasizing a "security-by-design" philosophy [20].

IEC 62443 is widely adopted internationally as the principal industrial cybersecurity standard. Its applicability to shore power integration is critical because it offers detailed guidance on network segmentation, system hardening, identity management, and risk assessment tailored to OT environments. The standard directly supports securing the interaction between ship control systems and shore-side energy infrastructures where ICS and OT converge.

3.3 IMO Resolution MSC.428(98)

The International Maritime Organization's Resolution MSC.428(98) marks a pivotal advancement in maritime cybersecurity by mandating the incorporation of cyber risk management within the International Safety Management (ISM) Code. This resolution requires shipowners to consider cybersecurity as part of their safety management systems, ensuring that risks are identified and mitigated during compliance audits and operational procedures.

While foundational for maritime cybersecurity, this standard's primary focus remains on shipboard systems and communications channels traditionally used onboard. Consequently, the resolution does not explicitly address the novel cybersecurity risks introduced by shore power connections and the consequent OT/ICS integration challenges at ports.

3.4 IACS Unified Requirements UR E26 and UR E27

The International Association of Classification Societies (IACS) introduced Unified Requirements UR E26 and UR E27 as mandatory frameworks for newbuild vessels from July 2024. These requirements seek to establish a robust baseline for cyber resilience of shipboard systems and specific onboard equipment, respectively. They focus on protecting critical operational systems such as propulsion, steering, power generation, and navigation from cyber threats.

Although these unified requirements improve ship cyber resilience, their direct applicability to shore power infrastructures remains limited. The standards primarily address ship internal cybersecurity and provide an opportunity for extension to formally encompass the interface and interaction with shore-side energy networks.

3.5 NIST Cybersecurity Framework (CSF)

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a voluntary guidance tool designed to help organizations manage and reduce their cybersecurity risks. Initially developed in the United States, the framework is universally recognized internationally as a reference point for establishing cybersecurity programs. It organizes security activities into five core functions: Identify, Protect, Detect, Respond, and Recover, providing a flexible structure to shape an organization's cybersecurity maturity [5].

3.6 NERC Critical Infrastructure Protection (CIP) Standards

The North American Electric Reliability Corporation (NERC) CIP standards enforce mandatory cybersecurity requirements aimed at protecting the Bulk Electric System within North America [8]. These standards address a broad spectrum of controls including asset identification, incident reporting, access control, and supply chain risk management.

These standards are not legally enforceable in Europe, but they are widely respected as robust best practices in energy cybersecurity. For stakeholders working on shore power interoperability, NERC CIP provides a useful benchmark to understand advanced levels of regulatory rigor and technical controls typical in mature energy sectors, helping to inform improved cybersecurity postures in European maritime-energy interfaces.

Together, these standards and regulations create a multifaceted cybersecurity environment where sector-specific requirements meet cross-sector regulatory mandates. IEC 62443 stands out as the most comprehensive technical standard for industrial control systems and provides a shared language to manage OT cybersecurity risks both afloat and ashore. IMO and IACS standards establish maritime cybersecurity baselines focused on shipboard systems, while NIS2 directs overarching governance and risk management across sectors.

NIST CSF and NERC CIP, although primarily American in origin, offer valuable perspectives and technical benchmarks for European operators seeking to enhance energy and maritime cybersecurity, particularly in the evolving shore power domain.

Table 1 Comparative Overview of Key Cybersecurity Standards for OPS Integration

Standard / Framework	Issuing Body	Scope & Focus	Relevance to OPS Integration	Key Limitations
NIS2 Directive	European Union	Cross-sector cybersecurity governance; mandatory reporting and risk management	High - establishes governance for both maritime and energy operators	Lacks OPS-specific technical guidance
IEC 62443 Series	International Electrotechnical Commission	Industrial control system and OT cybersecurity	Very high - provides technical measures for network segmentation, authentication, and lifecycle security	Not sector-specific; requires contextual adaptation
IMO MSC.428(98)	International Maritime Organization	Cyber risk management in ship safety systems	Moderate - applicable to vessel-side operations	No guidance on shore-based interfaces
IACS UR E26/E27	International Association of Classification Societies	Shipboard OT and system-level cyber resilience	High for onboard systems	No coverage of port - ship data integration
NIST Cybersecurity Framework (CSF)	National Institute of Standards and Technology (US)	Risk-based cybersecurity management	Useful benchmarking tool	Voluntary, non-binding in EU context
NERC CIP Standards	North American Electric Reliability Corporation	Critical infrastructure protection in energy sector	Relevant for grid-side security	Region-specific; limited direct applicability in EU

Source: Created by the Authors

Table 1 presents a structured comparison of the scope, primary focus, applicability to OPS operations, and identified limitations of each standard. This comparative overview highlights the fragmented yet interrelated and complementary nature of the existing regulatory and technical frameworks, underscoring the necessity for their harmonized integration within the OPS cybersecurity domain.

Yet, none of these standards singularly address the full complexity of securing the maritime-energy interface where ships connect temporarily but critically to shore electrical grids. This gap underscores the urgent need for integrative cybersecurity frameworks that harmonize maritime and energy sector standards, ensuring secure shore power implementation aligned with evolving European regulations.

4 Discussion

As it has already been established, the integration of maritime and energy sectors, especially through shore power, poses unique and multidimensional cybersecurity challenges. At the heart of these challenges is the patchwork of standards and regulations governing both domains[21]. Each standard reflects the legacy priorities, risk tolerance, and operational realities of its sector of origin; yet no single framework alone can effectively encompass the new cyber-physical risk landscape formed at the maritime energy interface.

At the European level, the NIS2 Directive is the binding legal instrument that sets minimum cybersecurity risk management, governance, and reporting obligations on critical sectors, including both maritime transport and energy infrastructure. NIS2 compels ports, shipping companies, and relevant energy actors to implement robust, regularly reviewed policies and technical controls, and to report incidents in a timely manner [8]. While it drives harmonization and cross-sector collaboration, NIS2 delegates detailed implementation to sector-specific standards and national regulatory authorities, creating both opportunity and complexity.

Internationally, the IMO Resolution MSC.428(98) remains the primary regulatory anchor for maritime cybersecurity, requiring cyber risk to be managed within the Safety Management Systems (ISM Code) of all ships. This broad mandate is strengthened at the system level by the IACS Unified Requirements UR E26 and E27, effective for newbuild vessels since July 2024, which introduce prescriptive requirements for cyber resilience of critical shipboard OT and embedded control systems [22]. Despite their scope, these instruments focus mainly on internal vessel operations rather than on the specifics of the interface with shore-based infrastructure.

Within the professional standards domain, the IEC 62443 series stands as the global benchmark for cybersecurity within ICS and OT environments. Its layered, lifecycle-centric approach is highly relevant for both stationary (port, grid) and mobile (shipboard) ICS, and

it has been increasingly referenced in port modernization initiatives [23].

Other internationally influential standards include the NIST Cybersecurity Framework (CSF) which provides a risk-based, iterative framework valued for its adaptability. Although not binding in Europe, it is commonly invoked by operators seeking to benchmark against North American best practices, and its structure resonates with process-driven European standards [22]. The NERC Critical Infrastructure Protection (CIP) standards, while mandatory only in North America, are frequently cited in scientific literature as the gold standard for auditability and continuous compliance in the energy sector. NERC CIP's emphasis on asset identification, logical network segmentation, incident reporting, and documented audits offers substantial guidance for European energy operators tasked with securing new shore power interfaces.

Overlaying all of these is the EU's NIS2 Directive, a binding legal instrument imposing minimum cybersecurity risk management, governance, and reporting obligations on critical sectors, including both maritime transport and energy infrastructure. NIS2 compels ports, shipping companies, and relevant energy actors to implement robust, regularly reviewed policies and technical controls, and to report incidents in a timely manner [5]. Importantly, while NIS2 drives harmonization and cross-sector collaboration, it delegates implementation detail to sector-specific standards and to national regulatory authorities, thereby creating both opportunity and complexity.

The simultaneous operation of multiple cybersecurity frameworks at the ship - shore electrical interface gives rise to several complex challenges. One significant concern is the issue of interoperability. As vessels from various flag states, each subject to cybersecurity protocols audited under IMO and IACS regimes, arrive at European ports, they must interact with port and grid systems governed by EU, national, and IEC-derived standards [20]. Achieving effective interoperability in this context requires not only mutual recognition of certificates and procedural checklists but also an alignment in the real-time assessment of cyber risk postures, an area that remains insufficiently addressed by any single standard [24].

Another challenge involves the considerable overlap and redundancy found across cybersecurity regimes. Critical functions such as risk assessment, incident reporting, and access control are subject to parallel regulatory requirements for ports, ships, and energy infrastructure operators [20]. While this redundancy can enhance system resilience and offer layered defences, it also introduces inefficiencies and leads to audit fatigue. In some cases, this results in "compliance theatre," where formal adherence to requirements takes precedence over meaningful improvements to cybersecurity posture.

A further issue lies in the persistent gaps between policy and practice. Maritime cybersecurity standards have yet to fully account for the physical-cyber characteristics of shore power systems, including dynamic authentication mechanisms, collaborative ship–shore monitoring of cyber threats, and coordinated emergency responses across sectors [22]. On the energy side, legacy industrial control systems and grid security architectures are still undergoing necessary updates to mitigate the risks associated with routine, high-power connections to external shipboard operational technology. Existing standards seldom provide prescriptive, real-time guidance for these complex hybrid environments and often lack clear demarcations of responsibility in the event of cyber incidents [21].

Together, these challenges underscore the pressing need for continued research, enhanced cross-sector policy coordination, and the development of practical tools aimed at harmonizing audit and compliance activities across the maritime and energy domains. This need for alignment and coordination is further amplified by the growing requirement for continuous audit and monitoring across all relevant frameworks [25].

A defining feature of the whole regulatory landscape is the ever-increasing requirement for continuous audit and monitoring. Unlike older, periodic approaches, where annual or biennial reviews sufficed modern cyber - physical environments, demand near real time assurance [26]. Vessel operators must demonstrate the ongoing effectiveness of their ISM cybersecurity procedures (via the IMO and IACS frameworks), while ports and energy distributors must document their risk assessments, mitigate findings, and report incidents continuously to authorities under NIS2 and, where adopted, IEC 62443 and NERC CIP regimes [9].

Audit, and the technical infrastructure supporting it, is no longer a periodic administrative burden but a live operational function. This includes automated logging, vulnerability scanning, penetration testing, supply chain risk assessments, and human-factor training, all of which must be evidenced and retrievable for regulatory review. As a result, compliance is no longer a static state but a dynamic process requiring coordination across sectoral and even international boundaries [6].

For multi-national operators and port authorities, this creates a fragile equilibrium: they must align disparate standards, ensure mutual recognition of compliance processes, and maintain the capability to scale audits as connections and operations multiply, often with limited cyber expertise and in the face of rapid technological change [27]. This operational balancing act is compounded by the complexity of legislation and overlapping regulatory frameworks that govern the maritime - energy interface.

While legislation such as NIS2 marks a historic advance in harmonizing cybersecurity governance, its im-

plementation in hybrid sectors is inherently complex and will remain so for the near future. The layering of international conventions (IMO), technical standards (IEC/IACS/NIST), and supranational regulation (EU) creates a framework that is broad in ambition but fragmented at the operational level [26].

The central issue lies in the need for both standardization and adaptability [26]. Standardized minimum requirements are essential to protect the weakest node in transnational maritime-energy chains. At the same time, the rapid evolution of attack vectors, digital transformation (including artificial intelligence and smart port automation), and the unique characteristics of each location require a flexible, risk-informed, and evolution-ready approach to both compliance and practice [11].

Securing the cyber - physical integration of maritime and energy systems demands a change in basic assumptions, from compartmentalized defence strategies to holistic, cooperative methods. Port authorities, ship operators, and energy suppliers must agree upon shared protocols for identity, authentication, access control, and anomaly detection at the ship-shore interface[28]. This includes joint exercises, information sharing, and coordinated incident response plans that acknowledge the unique challenges of temporally and geographically distributed assets[10].

Research increasingly points to the necessity of defence - in - depth, zero-trust architectures, and cybersecurity risk assessments that transcend organizational and sectoral boundaries. Technical measures such as robust segmentation, encryption at the interface, OTA patches, and real-time security monitoring, backed by clear legal and procedural frameworks, are presented as priorities in both academic and regulatory guidance [26].

There is also a critical need for ongoing training and awareness programs that reach vessel crews, port technicians, and energy IT/OT operators alike. Misalignments in skills, policies, or priorities across these sectors can themselves become security liabilities [29]. Therefore, a unified approach to training, risk evaluation, and continuous improvement underpinned by harmonized standards is essential for the resilience of the integrated whole.

5 Conclusion

The onset of mandatory shore power connections under European Union regulations marks a pivotal moment in the evolution of critical infrastructure cybersecurity. This paper has explored the increasingly complex landscape where maritime and energy sectors converge, creating a novel cyber-physical interface that exposes hitherto isolated systems to shared digital risk.

Throughout the research, it has become evident that while robust cybersecurity standards and regulatory frameworks exist within the maritime and energy domains individually, their direct applicability to the shore power interface is partial and fragmented. International maritime standards, such as IMO Resolution MSC.428(98) and IACS Unified Requirements UR E26 and UR E27, establish important baselines for shipboard cyber resilience. Meanwhile, energy sector frameworks, including IEC 62443, the NIS2 Directive, and, in North America, NERC CIP, address secure operation of stationary industrial control systems with detailed technical prescriptions and mandatory governance.

However, the unique challenges posed by shore power requirements, characterized by transient but high-capacity connections between mobile vessels and terrestrial electrical grids, demand a more integrated and adaptive approach. The existing regulatory patchwork requires harmonization to address cyber-physical integration risks effectively. This includes clarifying responsibility boundaries, establishing mutual trust verification protocols at connection points, and integrating incident response procedures that span both maritime and energy stakeholders.

Moreover, the necessity for continuous, real-time audit and monitoring underscored in this research emphasizes that cybersecurity compliance in these sectors is no longer a static checkpoint but an ongoing operational imperative. The evolving threat landscape, fuelled by increasing digitization, automation, and emerging technologies such as artificial intelligence, further complicates this environment and underscores the importance of dynamic governance.

In conclusion, addressing the cybersecurity challenges of maritime-energy convergence demands:

- Harmonized cross-sector standards that reflect the realities of cyber-physical integration;
- Regulatory frameworks that enforce continuous audit, transparent reporting, and joint incident management;
- Industry collaboration focusing on unified risk assessment methodologies and shared best practices;
- Investment in cybersecurity technologies and workforce competencies tailored to hybrid OT/ICS environments.

The main limitations of this research lie in its reliance on existing literature, standards, and regulatory texts without direct empirical testing of cybersecurity measures in operational shore power environments. Additionally, the scope is geographically weighted toward the European Union, which may limit the applicability of certain conclusions in non-EU contexts. Simulation-based risk modelling would provide further validation of the identified gaps.

This research thus provides a foundational synthesis of applicable standards, legislative requirements, and operational imperatives, serving as a basis for policy-

makers, port authorities, maritime operators, energy providers, and researchers to develop resilient, future-ready security architectures. Future research could expand by conducting empirical field studies and real-time cyber risk assessments in active port–vessel shore power connections. Comparative analyses between EU and non-EU regulatory environments could offer insights into global harmonization potential. It could also extend towards exploring the integration of artificial intelligence, blockchain-based verification systems, and advanced intrusion detection mechanisms to strengthen the security of maritime–energy cyber-physical systems. As the EU's shore power mandates approach full implementation, initiative-taking, coordinated action will be essential to safeguard the integrity, reliability, and sustainability of European and global critical infrastructures in an increasingly connected world.

Acknowledgement: This paper is a part of the research under the project line 581 NPOO of the University of Rijeka, for the project uniri-iz-25-13; and "*Konvergentni IT-OT sustav upravljanja energijom (EMS) za tranziciju lučkih zajednica u pametna niskougljična energetska čvorišta (PortEMS)*" - IP.1.1.03.0070.

Funding: The research presented in the manuscript did not receive any external funding.

Author Contributions: Research, Matej Plenča; Writing, Matej Plenča and Saša Aksentijević; Review and Editing, Saša Aksentijević and Edvard Tijan; Formal Analyzes, Matej Plenča; Conceptualization, Matej Plenča and Saša Aksentijević; Supervision, Saša Aksentijević; Validation, Srđan Skok; Verification, Edvard Tijan, Final approval, Srđan Skok and Edvard Tijan.

References

[1] L. Martin and B. Benson, ICS/OT Cybersecurity Considerations for Maritime Transportation, Dragos, Inc. and ABS Group, pp. 1–6, 2023.

[2] M. V. Clavijo Mesa, C. E. Patino-Rodriguez, and F. J. Guevara Carazas, "Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains," *Information (Switzerland)*, vol. 15, no. 11, 2024, doi: 10.3390/info15110710.

[3] M.-L. Tombak, B.-E. Zetterman, and U. P. Tapaninen, "Cybersecurity Risks at Port," *Transport and Telecommunication Journal*, vol. 26, no. 3, pp. 276–291, 2025, doi: 10.2478/ttj-2025-0021.

[4] European Commission, Directorate-General for Mobility and Transport, "Guidance on how to address cybersecurity onboard ships during audits, controls, verifications and inspections (MARSEC Doc. 9209)," 2023.

[5] A. Dimakopoulou and K. Rantos, "Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0," *J Mar Sci Eng*, vol. 12, no. 6, 2024, doi: 10.3390/jmse12060919.

[6] G. Kavallieratos and S. Katsikas, "Managing cyber security risks of the cyber-enabled ship," *J Mar Sci Eng*, vol. 8, no. 10, pp. 1–19, 2020, doi: 10.3390/jmse8100768.

[7] M. A. Alomari *et al.*, "Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions," *Energies (Basel)*, vol. 18, no. 1, pp. 1–34, 2025, doi: 10.3390/en18010141.

[8] RMIT University, Identifying Cybersecurity Best Practices for the Marine Renewable Energy Sector, RMIT Centre for Cyber Security Research and Innovation, 2023.

[9] European Parliament and the Council of the European Union, "NIS 2 Directive," *Official Journal of the European Union*, vol. 2022, no. November, pp. 80–152, 2022, [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[10] G. Kayişoğlu, B. Güneş, and P. Bolat, "ECDIS Cyber Security Dynamics Analysis based on the Fuzzy FUCOM Method," *Transactions on Maritime Science*, vol. 13, no. 1, 2024, doi: 10.7225/toms.v13.n01.w09.

[11] H. Akyildiz, "A Conceptual Model of Port Cybersecurity and Threats: Knowledge and Understanding," vol. GİDB Dergi, no. 21, pp. 23–32, 2022.

[12] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, article n71, 2021.

[13] J. Pöyhönen and M. Lehto, "Comprehensive cyber security for port and harbor ecosystems," *Front Comput Sci*, vol. 5, 2023, doi: 10.3389/fcomp.2023.1154069.

[14] I. Cindrić, M. Jurčević, and T. Hadjina, "Mapping of Industrial IoT to IEC 62443 Standards," *Sensors*, vol. 25, no. 3, pp. 1–32, 2025, doi: 10.3390/s25030728.

[15] T. Alsuwian, A. Shahid Butt, and A. A. Amin, "Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review," *Sustainability (Switzerland)*, vol. 14, no. 21, pp. 1–21, 2022, doi: 10.3390/su142114226.

[16] I. Ralby and A. Bochman, "Cybersecurity concerns for the energy sector in the maritime domain," Atlantic Council, Issue Brief, Washington, DC, USA, 2021.

[17] F. A. de Peralta et al., "Cybersecurity best practice guidance for marine renewable energy systems," PNNL, Richland, WA, USA, 2020.

[18] M. A. Ben Farah *et al.*, "Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends," *Information (Switzerland)*, vol. 13, no. 1, pp. 1–33, 2022, doi: 10.3390/info13010022.

[19] M. Thompson, A. Mink, and T. Cottle, *NIST IR 8406 Cybersecurity Framework Profile for Liquefied Natural Gas*, National Institute of Standards and Technology, U.S. Department of Commerce, 2023.

[20] Adebimpe Bolatito Ige, Eseoghene Kupa, and Oluwatosin Ilori, "Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources," *International Journal of Science and Research Archive*, vol. 12, no. 1, pp. 2978–2995, 2024, doi: 10.30574/ijsra.2024.12.1.1186.

[21] D. Ryu, S. Lee, S. Yang, J. Jeong, Y. Lee, and D. Shin, "Enhancing Cybersecurity in Energy IT Infrastructure Through a Layered Defense Approach to Major Malware Threats," *Applied Sciences (Switzerland)*, vol. 14, no. 22, 2024, doi: 10.3390/app142210342.

[22] G. Potamos, E. Stavrou, and S. Stavrou, "Enhancing Maritime Cybersecurity through Operational Technology Sensor Data Fusion: A Comprehensive Survey and Analysis," *Sensors*, vol. 24, no. 11, 2024, doi: 10.3390/s24113458.

[23] N. A. R. Al Ali, A. A. Chebotareva, and V. E. Chebotarev, "Cyber security in marine transport: Opportunities and legal challenges," *Pomorstvo*, vol. 35, no. 2, pp. 248–255, 2021, doi: 10.31217/p.35.2.7.

[24] J. P. A. Yaacoub, H. N. Noura, O. Salman, and K. Chahine, "Toward Secure Smart Grid Systems: Risks, Threats, Challenges, and Future Directions," *Future Internet*, vol. 17, no. 7, pp. 1–87, 2025, doi: 10.3390/fi17070318.

[25] J. Poyhonen, J. Simola, I. Khan, M. Lehto, and S. Wali, "Assessment of cyber security risks: A smart terminal process," *European Conference on Information Warfare and Security, ECCWS*, vol. 2023-June, pp. 366–373, 2023, doi: 10.34190/eccws.22.1.1060.

[26] O. Melnyk, O. Drozdov, and S. Kuznichenko, "Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures," *Lex Portus*, vol. 11, no. 1, pp. 7–19, 2025, doi: 10.62821/lp11101.

[27] M. Boeding, K. Boswell, M. Hempel, H. Sharif, J. Lopez, and K. Perumalla, "Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid †," *Energies (Basel)*, vol. 15, no. 22, pp. 1–22, 2022, doi: 10.3390/en15228692.

[28] D. Zgaljic, P. Badurina-Tomic, and M. Plenca, "The Importance of Port Security System in the Implementation of Transport Modal-Shift," in *Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges*, vol. 46, A. Niglia, Ed., in {NATO} Science for Peace and Security Series - {D:} Information and Communication Security, vol. 46 {IOS} Press, 2016, pp. 106–114. doi: 10.3233/978-1-61499-699-6-106.

[29] Y. Todorov, "Navigating Uncharted Waters: Tackling Maritime Cybersecurity Challenges in the Black Sea Region," *Information & Security: An International Journal*, vol. 55, no. 2, pp. 113–132, 2024, doi: 10.11610/isij.5509.