WHITE PAPER

Navigating Digitalization and Cybersecurity in the Maritime Industry

Alicia Wang
Product Manager

MOXA®

1. Executive Summary

The maritime industry, which facilitates 80% of global trade, is at a pivotal juncture where digitalization and cybersecurity are becoming essential for its sustained growth and resilience.

This whitepaper delves into the key trends shaping the industry, including geopolitical challenges, the drive towards sustainability, and the rapid adoption of digital technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI). As the maritime sector becomes increasingly reliant on these technologies, it faces significant cybersecurity threats that could disrupt operations, compromise safety, and lead to severe financial losses.

To mitigate these risks, international regulations like ISO 23799:2024, ISO 16425:2024, IMO MSC 428(98), and IACS UR E26 and E27 were established. Compliance with these standards is essential for maritime operators to protect their assets and ensure operational safety.

Moxa, a leader in industrial networking and cybersecurity, offers a range of maritime-certified products designed to meet these stringent requirements. This whitepaper provides an analysis of the current landscape and demonstrates how Moxa's solutions can assist maritime operators in navigating the complexities of digitalization and cybersecurity compliance.

2. The Maritime Industry: Trends and Challenges

2.1. The Critical Role of Maritime in Global Trade

The maritime industry is the backbone of global trade, responsible for transporting goods across vast distances and connecting economies around the world. With 80% of global trade being seaborne,[1] the performance of the maritime sector is a reliable indicator of economic health and geopolitical stability. As the world economy continues to evolve, the maritime industry is under increasing pressure to adapt to new challenges and seize emerging opportunities.

[1] Ocean shipping worldwide - statistics & facts

Released on November 11, 2024

2.2. Geopolitical Tensions and Economic Growth

In recent years, geopolitical tensions have significantly impacted the maritime sector. Global conflicts—such as the war between Russia and Ukraine and the ongoing trade disputes between the United States and China—have created an unpredictable environment for global shipping.[2] These tensions have led to disruptions in established shipping routes, increased costs, and delivery delays. Maritime operators must navigate these challenges while maintaining efficiency and profitability, a task that is becoming increasingly difficult in a volatile global landscape.

2.3. Sustainability and Regulatory Pressures

The maritime industry is also facing growing pressure to adopt sustainable practices in response to stricter environmental regulations and rising customer demand for eco-friendly solutions. The International Maritime Organization (IMO) has set ambitious goals to reduce greenhouse gas emissions from shipping, aiming for a 90% reduction by 2040 and complete decarbonization by 2050.[3] Achieving these goals requires significant investment in new technologies and the adoption of green shipping practices.

The drive towards sustainability is also leading to the development of alternative fuels, such as green ammonia and methanol, which are expected to play a crucial role in the future of maritime shipping. For example, the agreement between Iberdrola and Trammo to purchase and sell up to 100,000 tons of green ammonia annually from 2026 underscores the industry's commitment to reducing its environmental impact.[4] Additionally, the integration of IoT devices—which is projected to reach 30.9 billion units by 2025—will enhance the industry's ability to monitor and optimize environmental performance in real time.[5]

3. Digitalization in Maritime Operations

3.1. The Rise of Maritime IoT and AI

Digitalization is transforming the maritime industry, with technologies such as IoT and AI driving significant improvements in operational efficiency, safety, and sustainability.[6]

The concept of Maritime IoT refers to the integration of various sensors, networking devices, and data analytics platforms that enables real-time monitoring and control of maritime operations. These technologies allow operators to optimize routes, monitor fuel consumption, predict maintenance needs, and enhance overall operational efficiency.

AI, on the other hand, plays a critical role in processing the vast amounts of data generated by IoT devices, enabling predictive analytics and decision-making. For instance, AI-driven systems can analyze historical data to predict equipment failures, allowing operators to perform maintenance before issues arise. This not only reduces downtime, but also extends the lifespan of critical equipment.

[2] Geopolitics and its Impact on Global Trade and the Dollar
[3] Revised GHG reduction strategy for global shipping adopted (imo.org)
[4] Trammo, Iberdrola sign up to key offtake agreement
[5] Understanding the importance of IoT for web development
[6] Rapid tech-driven transition

3.2. The Growing Cybersecurity Threat

The maritime industry has seen a dramatic increase in cyberattacks, with Allianz Global Corporate & Specialty (AGCS) reporting a 400% rise in incidents between February and June 2020.[7] This surge correlates with the sector's accelerated digitalization and interconnectedness, making it an attractive target for cybercriminals.

Despite 77% of maritime professionals recognizing the high risk of cyberattacks, only 64% of organizations have implemented business continuity plans, and just 24% of these plans are tested regularly.[8] The average cost of a cyberattack in the maritime sector has surged to approximately US$550,000, with ransom demands escalating by over 350%, reaching US$3.2 million on average.[9]

The complexity of maritime operations, coupled with the convergence of IT and OT systems, makes the industry particularly vulnerable to cyberthreats. Approximately 75% of maritime professionals now consider OT system security a higher priority than just two years ago.[10] Recent cybersecurity incidents—such as the ransomware attack on DNV's ShipManager servers—highlight the severe consequences of inadequate cybersecurity measures, including operational disruptions, compromised data, and threats to crew and vessel safety.[11]

3.3. Key Cybersecurity Challenges

The maritime sector faces several unique cybersecurity challenges. First, there is a general lack of understanding of OT systems, which are often overlooked in cybersecurity strategies. OT systems control critical functions such as navigation, propulsion, and cargo management, making them prime targets for cyberattacks. Additionally, the convergence of IT and OT systems in modern vessels has created new vulnerabilities, as many organizations lack the expertise to secure these interconnected networks.

Limited visibility into OT networks is another major challenge. Many maritime operators do not have the tools or processes in place to monitor their OT networks effectively, leaving them blind to potential threats. Unsecured wireless networks are also a significant concern, as they provide an easy entry point for attackers to gain access to critical systems.

Finally, there is a shortage of cybersecurity awareness within the industry, with many organizations underestimating the potential impact of cyberattacks on their operations.

[7] Shipping losses at record low, but Covid-19 impact and political tensions cloud the horizon
[8] A Comprehensive Guide to Maritime Cybersecurity
[9] Maritime Cyber-risk Report: Shipping Industry Remains “Easy Target”, Pays Average US$3.2m In Cyberattacks
[10] Maritime professionals warn of insufficient investment in cybersecurity as risks escalate in the era of connectivity
[11] Cyber-attack on ShipManager servers – update

4. Navigating International Regulations

4.1. Overview of Maritime Cybersecurity Standards

As the maritime industry becomes more digitalized, the need for robust cybersecurity measures has never been greater. Several international standards and regulations have been developed to address the unique cybersecurity challenges faced by the maritime sector, providing a framework for operators to secure their IT and OT systems, protect against cyberthreats, and ensure operational safety.

4.2. Key Standards and Regulations

One of the most critical standards is ISO 23799:2024, which outlines the procedures and requirements for assessing onboard cybersafety. This standard focuses on the risk assessment of onboard systems, including bridge operations, cargo management, propulsion, power control, and access control. It provides a comprehensive framework for identifying, analyzing, and evaluating cyber-risks, ensuring that maritime operations are conducted safely and securely.[12]

ISO 16425:2024 provides comprehensive specifications for ship communication networks, targeting ship owners, designers, and technical stakeholders responsible for implementing onboard communication systems. The standard places significant emphasis on security management requirements, including the identification of vulnerabilities, implementation of protection and detection measures, and the execution of regular security protocols such as software updates, log monitoring, and security audits. These elements are critical for maintaining the integrity, reliability, and security of ship communication networks in increasingly complex maritime environments.[13]

The IMO MSC 428(98) resolution mandates that ship operators integrate cyber-risk management into their Safety Management Systems (SMS). This resolution, adopted in 2017, requires ship owners to develop and implement onboard procedures to mitigate cyber-risks, ensuring the safety of vessels and crew members. The resolution became mandatory in 2021, underscoring the importance of cybersecurity in the maritime industry.[14]

IEC 61162-460 sets the requirements for high-speed communication interfaces between shipboard navigation and radio communication equipment, addressing the security needs of these critical systems.[15] The standard outlines specific requirements and testing methods to ensure that communication systems on board are secure and resilient to cyberthreats.

[12] ISO 23799:2024(en) Ships and marine technology — Assessment of onboard cyber safety

[13] ISO 16425:2024(en) Ships and marine technology — Specifications for the installation of ship communication networks for shipboard equipment and systems

[14] Maritime cyber-risk

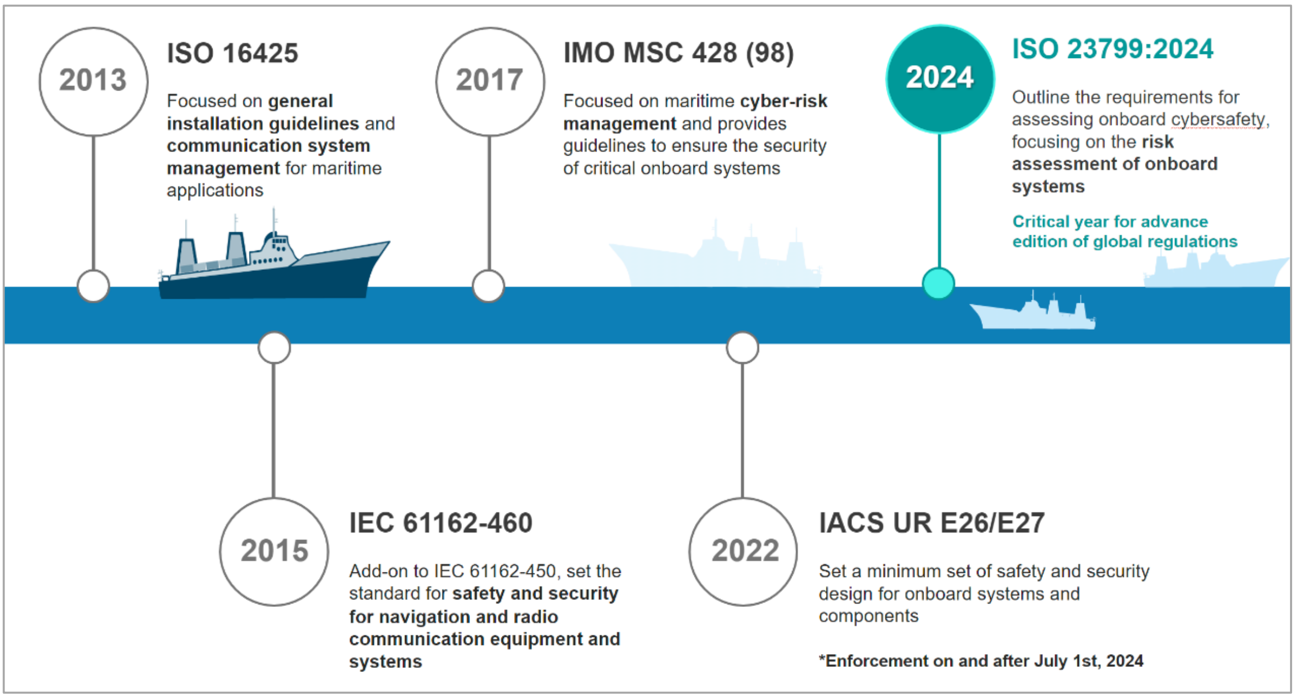
[15] IEC 61162-450:2024

Finally, the IACS UR E26 and E27 standards, which became mandatory in 2024, focus on ensuring the cyber-resilience of ships. UR E26 establishes minimum functional and performance standards for vessel networks that cover five key areas: Identify, Protect, Detect, Respond, and Recover. UR E27 focuses on system integrity, requiring third-party equipment suppliers to ensure that their systems are secure and resilient. These standards are crucial for maintaining the cybersecurity of maritime operations.[16]

The following tables describe the focus of each standard and when they were released:

Standard	Scope	Focus	Target Audience
ISO 23799:2024	Onboard cybersystems	Risk assessment	Ship owners, operators, designers
ISO 16425:2024	Maritime industry	Cybersecurity management system	Maritime organizations
IMO MSC 428 (98)	Maritime security	Physical and cybersecurity	Ship and port facility operators
IEC 61162-460	Maritime communication systems	Cybersecurity for maritime communication systems	Maritime communication system providers and users
IACS UR E26 E27	Shipboard cybersecurity	Cybersecurity for ships	Ship owners, operators, designers, and builders

Table 1: Key Standards and Regulations Overview



2013
ISO 16425
Focused on **general installation guidelines** and **communication system management** for maritime applications

2017
IMO MSC 428 (98)
Focused on maritime **cyber-risk management** and provides guidelines to ensure the security of critical onboard systems

2024
ISO 23799:2024
Outline the requirements for assessing onboard cybersafety, focusing on the **risk assessment of onboard systems**
Critical year for advance edition of global regulations

2015
IEC 61162-460
Add-on to IEC 61162-450, set the standard for **safety and security for navigation and radio communication equipment and systems**

2022
IACS UR E26/E27
Set a minimum set of safety and security design for onboard systems and components
*Enforcement on and after July 1st, 2024

Table 2: Global Regulation Highlights

[16] IACS UR E26 and E27

5. Best Practices and Case Sharing: Managing Network Security under UR E26/E27

In the maritime industry, network security is a critical concern, particularly under the UR E26/E27 regulations, which demand transparency and robustness in design and cybersecurity measures. Below, we will discuss part of these requirements and interpret them from Moxa’s perspective.

5.1. Requirements behind a view of E26

UR E26 not only emphasizes and provides a minimum set of requirements for the cyber-resilience of ships, but also defines Identify, Protect, Detect, Respond, and Recover requirements to be fulfilled under the responsibility of stakeholders involved in the design, building, and operation of ships, including shipowners/companies, ship designers/shipyards, system integrators, suppliers, and classification societies. The Identify and Detect requirements are discussed in more detail below.

Identify

System integrators are often asked to assist in responding to E26 requirements. The goal of this element is to develop an organizational understanding to manage cybersecurity risks to onboard systems, personnel, assets, data, and capabilities. A qualified vessel asset inventory, including application programs, operating systems, firmware, and other software components of the CBSs within the scope of UR E26 applicability, as well as networks connecting these systems onboard or ashore, must be provided and kept up to date throughout the life of the ship. Supplier responsibilities are similar to those of system integrators, who must submit a vessel asset inventory to societies.

Any equipment supplier, such as a network device supplier, is required to provide relevant and traceable records containing the following information:

- History of software and hardware modifications, especially those that involve new vulnerabilities or modify functional dependencies. This will also depend on whether the company has a commitment, a clear service policy, and a product security incident response team **(PRIST)**.[17]
- Capability of providing **account management** to manage relevant devices if confidential information is included for different access control policies.
- For each Computer-based System (CBS), a block diagram and display of all node-connected information through an easily configurable and manageable interface or **management tool** would be an ideal solution for authorized personnel.

[17] Moxa’s security advisories

Detect

The goal of this element is to develop and implement appropriate measures to detect and identify the occurrence of a cybersecurity incident onboard. **Monitoring network operations** and **CBS diagnostic functions** are the two primary scopes where these measures need to be applied. Operation safety and utilization while sailing are crucial for operators, and they cannot be allowed to tolerate any uncertain risk for downtime during sea transportation. For instance, when network devices are used in networks with propulsion/engine control or navigation, measures to monitor networks would key since the function of those systems determines the sailing direction of a vessel.

Key functionalities should be provided by suppliers for the following:

- **Traffic Monitoring:** It is important to not only monitor but also configure thresholds for network traffic to ensure reliable data transmission. When using fiber modules for long-distance connections, monitoring and configuring thresholds for module power and temperature are important for connection stability. Additionally, event monitoring and notifications are often required; the common method is sending an email message to a specified recipient.
- **Protection Against Connection of Unauthorized Devices:** Rogue devices that transmit, whether over the air or through a wire, take network resources. Unauthorized transmissions may impact operational performance or not conform to defined security policies. **Rogue device detection** plays a crucial role in preventing unauthorized access and reducing the many entry points that exist in a system's network, becoming a target for hackers. It also helps ensure confidentiality and data integrity.
- **Implementation of Intrusion Detection Systems (IDS):** In the realm of network security, many customers prefer using IDS over Intrusion Prevention Systems (IPS) for daily operations. IDS primarily monitors and identifies potential threats without actively interfering with network data. This approach has minimal impact on network performance, which is crucial for organizations that prioritize maintaining service quality and network efficiency. It is also considered a cost-effective way to enhance security monitoring without the need for significant changes to existing network infrastructure. When selecting equipment, it is crucial to choose devices with IPS capabilities that can be activated when needed for a more proactive defense.

Moxa's MXstudio Industrial Network Management Suite offers a streamlined solution for maritime network security, addressing UR E26/E27 compliance through key functionalities in asset management and cyberthreat detection. The MXstudio suite brings together MXconfig, MXview One, and MXsecurity to create a comprehensive package that simplifies and centralizes industrial network management, monitoring, and security.

MXconfig simplifies network asset tracking, ensuring that system integrators can maintain updated inventories of hardware, software, and configuration changes as required by UR E26. For proactive network monitoring, MXview One and MXsecurity provide real-time traffic surveillance, configurable event notifications, and robust defenses against unauthorized device connections. The Intrusion Detection System (IDS) offers passive threat monitoring without affecting network performance, while the Intrusion Prevention System (IPS) can be activated for more proactive protection when needed.

Incorporating MXstudio ensures that maritime networks remain compliant, secure, and resilient, enhancing operational safety and efficiency.

5.2. Addressing E27 Requirements with Existing Topology

In situations where the network topology is closed and budget constraints prevent the addition of new devices, shipowners may question whether it is necessary to replace unmanaged switches with managed ones. Despite these constraints, it is still advisable to use managed switches at critical nodes to implement essential network security features. In scenarios where adding multiple devices is not feasible, all-in-one solutions like Moxa EDR Series products—which combine functions such as firewall, VPN, and routing—can provide the necessary boundary protection without requiring additional hardware. Ensuring that communication across zone boundaries is controlled and monitored is essential for maintaining the compartmentalization required by UR E27, and managed switches or integrated solutions can play a crucial role in achieving this.

5.3. The Importance of a Secure Development Life Cycle (SDLC)

An SDLC plays a crucial role in improving cybersecurity across different roles in the maritime industry, where technology, automation, and connectivity are growing rapidly. Implementing SDLC ensures that security measures are integrated into every phase of software or system development, from the initial design to deployment and maintenance.

Here’s why SDLC is critical for different stakeholders in the maritime sector:

Ship Owners and Operators

- **Importance:** As the owners and operators of maritime vessels, ensuring the security of navigation systems, onboard control systems, and communication platforms is essential. SDLC helps identify and mitigate potential vulnerabilities early, preventing cyberattacks that could disrupt ship operations, such as GPS spoofing or hacking of ship control systems.
- **Impact:** By adopting SDLC, owners and operators can ensure regulatory compliance with standards like IMO's (International Maritime Organization) cybersecurity guidelines and IACS (International Association of Classification Societies) UR E26 and UR E27, which require cyber-resilience in ships' systems.

Software Developers and System Integrators

- **Importance:** These professionals are responsible for developing and integrating software systems that manage vessel operations from navigation to engine controls. Implementing SDLC ensures that security best practices are embedded during the development of critical systems, such as the ECDIS (Electronic Chart Display and Information System) and AIS (Automatic Identification System).
- **Impact:** A robust SDLC helps developers identify vulnerabilities during code writing and testing phases, ensuring that the software is resistant to cyberattacks like malware infections or unauthorized access. This approach also reduces costs by addressing security flaws early, rather than after deployment.

Regulatory Bodies and Classification Societies

- **Importance:** Organizations like IMO and IACS are responsible for setting standards to ensure the safety and security of the maritime sector. SDLC provides a structured approach to verifying that software and systems meet these cybersecurity standards.
- **Impact:** Regulatory bodies benefit from SDLC by ensuring that ship operators and software developers meet the necessary cybersecurity benchmarks. It also enables the auditing of systems for compliance with cybersecurity guidelines such as NIS2 (Network and Information Security Directive).

Not only for the roles mentioned above—but also for crews and fleet managers, or even IT security and maintenance teams—complying with the SDLC and adopting products designed according to SDLC can greatly assist in maintaining systems and enabling more proactive protection in the future, minimizing security risks.

5.4. Moxa’s Support in E26/E27 Compliance

Moxa offers comprehensive support to ensure that shipowners and system integrators can meet the stringent requirements of UR E26/E27. Drawing on cybersecurity design expertise based on IEC 62443, Moxa provides compatibility tables, test cases, and guidance that help clients achieve E27 certification.

Moxa’s approach is twofold, focusing on both component-centric and customer-centric strategies. The component-centric approach leverages cybersecurity design knowledge to ensure compatibility, while the customer-centric approach provides system-level interpretation and guidance, particularly in the context of using Moxa’s products to accelerate the certification process.

Furthermore, Moxa’s rogue system detection continuously monitors the network, identifying any unauthorized devices. This proactive approach enables IT teams to quickly recognize potential security threats, allowing them to take immediate action to mitigate risks and maintain the integrity of the network.

6. Moxa's Role in Enhancing Maritime Cybersecurity

6.1. The Importance of Regulatory Compliance

In an increasingly connected world, the security, safety, and reliability of maritime systems are paramount. Compliance with international cybersecurity regulations is not only a legal requirement but also a critical component of operational resilience. Maritime operators must navigate a complex regulatory landscape to protect their assets, ensure the safety of their operations, and maintain the trust of their stakeholders.

Regulatory compliance is particularly challenging in the maritime industry due to the rapid pace of technological change and the growing complexity of maritime operations. As vessels become more digitally connected, the risk of cyberattacks increases, making it essential for operators to adopt robust cybersecurity measures. Compliance with standards such as ISO 23799:2024, ISO 16425:2024, IMO MSC 428(98), and IACS UR E26 and E27 is crucial for mitigating these risks and ensuring the safety and security of maritime operations.

6.2. Enhancing Compliance Readiness for Maritime Cybersecurity Standards

Moxa is a leading provider of industrial networking solutions, offering a comprehensive portfolio of products designed to meet the unique needs of the maritime industry. Moxa's solutions are certified by leading maritime classification societies, including DNV, ABS, LR, NK, and BV, ensuring that they meet the highest standards of safety and security.

Moxa's portfolio includes OT data devices, marine IPCs, networking solutions, and remote monitoring and management platforms, all designed to ensure the cybersecurity of maritime operations. These solutions are tailored to the specific requirements of the maritime industry, providing comprehensive protection across all stages of data management, from collection and storage to transfer and processing, helping maritime operators to reduce cyber-risks, enhance operational resilience, and accelerate the certification process.

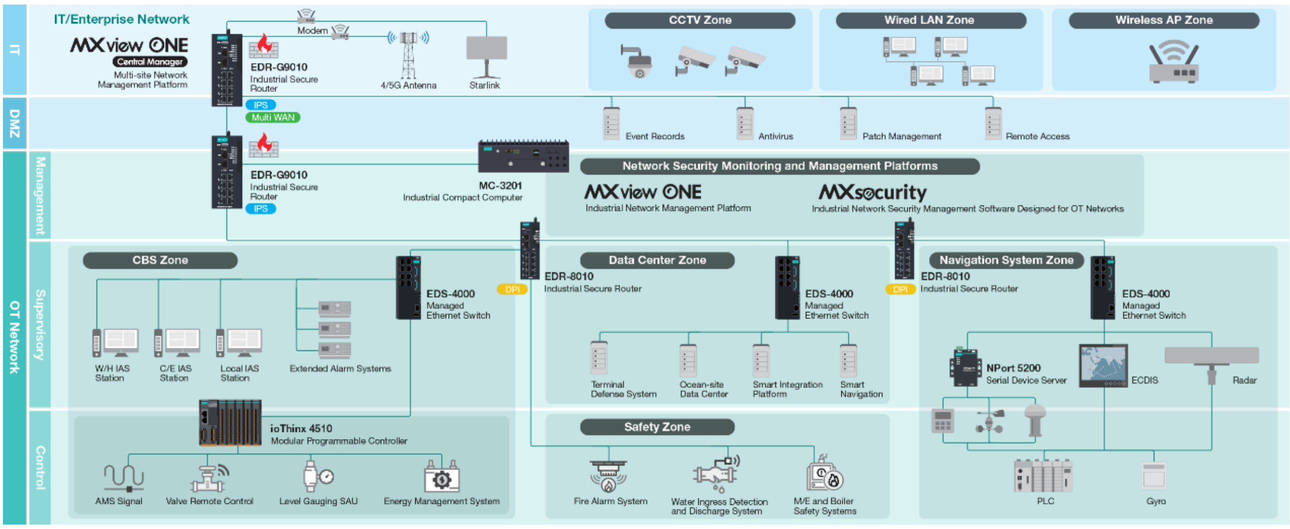


Table 3: Moxa's Comprehensive Solutions for Regulation Compliance

6.3. Supporting the Entire Maritime Supply Chain

Moxa's solutions are designed to support the entire maritime supply chain, from individual vessels to entire fleets. By providing real-time data and visibility into maritime operations, Moxa helps operators to manage their assets more effectively, optimize performance, and ensure compliance with international cybersecurity standards.

Moxa's cybersecurity solutions offer several key benefits, including enhanced protection against cyberthreats, reduced risk of operational disruptions, and improved safety for crew members and vessels. Additionally, Moxa's solutions are designed to be easy to deploy and manage, reducing the complexity of cybersecurity implementation and allowing operators to focus on their core business activities.

Moxa's commitment to supporting the maritime industry extends beyond product development. The company works closely with industry stakeholders to provide training, support, and guidance on cybersecurity best practices, helping operators to navigate the complexities of digitalization and regulatory compliance.

7. Conclusion

The maritime industry is undergoing a significant transformation, driven by the twin forces of digitalization and sustainability. While these changes bring numerous benefits, they also introduce new risks, particularly in the realm of cybersecurity. As the industry becomes more reliant on digital technologies, the need for robust cybersecurity measures has never been greater.

Compliance with international cybersecurity standards is essential for ensuring the safety and security of maritime operations. Moxa, with its comprehensive portfolio of maritime-certified cybersecurity solutions, is well-positioned to help maritime operators navigate these challenges. By leveraging Moxa's solutions, operators can enhance their cybersecurity posture, reduce operational risks, and ensure compliance with the latest regulations.

This whitepaper has outlined the key trends and challenges facing the maritime industry, the importance of digitalization and cybersecurity, and how Moxa's solutions can help operators meet these challenges. As the industry continues to evolve, Moxa remains committed to supporting the maritime sector with innovative, reliable, and secure solutions.

8. Additional Resources

For further information on Moxa's maritime solutions and cybersecurity best practices, please visit Moxa’s Maritime Microsite.

You can also explore case studies and whitepapers on related topics, which provide in-depth insights into the latest developments in the maritime industry and how Moxa is helping to shape its future.

Disclaimer
This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.