SANS | Research Program

White Paper

General Quarters! Cybersecurity Challenges in the Maritime Industry

Written by **Marco Ayala**, **Jason Dely**, and **Sean Plankey**

October 2024

FORTINET

The Lifeblood of the World Economy

The maritime industry is vast and complex, serving as the lifeblood of global trade and transportation. The industry encompasses a spectrum of activities, including vessels navigating the world's oceans. Container ships are the workhorses of international trade, ferrying 52% of the world's cargo.[1] Their design, centered on the standardized shipping container, allows for seamless integration with other transportation modes, such as rail and truck. No less important are tankers, carrying approximately 66% of the world's liquid energy. These specialized ships transport liquid cargo such as crude oil, refined petroleum products, chemicals, and liquefied natural gas (LNG). These tankers play an essential role in maintaining the steady flow of fuel supplies that power economies worldwide.

Drill ships and mobile offshore drilling units (MODUs) represent another critical segment of the maritime industry. These vessels are equipped for exploratory and extraction operations in offshore oil and gas fields, operating in deep waters far from shore. Separately, cruise ships offer luxury travel experiences on the high seas. These vessels are essentially floating cities, complete with complex onboard systems that require meticulous management and maintenance.

The smooth operation of vessel transit in and around ports is supported by services such as vessel traffic services (VTS), which monitor and manage vessel traffic within port areas and coastal waters via radar and human-centered coordination over radio. These shore-based systems are vital for ensuring safe and efficient navigation in busy or hazardous waters where the risk of accidents or collisions is high.

Beyond vessels and vessel navigation, the maritime industry also includes related sectors such as shipbuilding, where the design, fabrication, assembly, and outfitting of ships take place. This industry is highly specialized, with shipyards constructing everything from small boats to massive supertankers and aircraft carriers. Commercial ports and terminals are another critical component, serving as the hubs where cargo is transferred between ships and land-based transportation. These ports are the linchpins of maritime trade, often handling millions of tons of cargo annually, with terminals specializing in various types of goods, from containers to bulk and liquid cargo.

Integral to port operations are the key infrastructure equipment, such as handling or gantry cranes and automated guided vehicles (AGVs), which facilitate the loading, unloading, and transportation of cargo within the port. These systems are often electronically controlled and increasingly automated, relying on advanced control technologies to efficiently move cargo across the port.

[1] "Facts & Figures," World Shipping Council, www.worldshipping.org/facts-figures

Essential, but Not Invincible

The industry's critical role in maintaining the global supply chain underscores the importance of ensuring the security and resilience of maritime operations. The various corners of the industry are in operation using legacy and aging systems. Vessels, as an example, whether they are container ships, tankers, or drill ships, are designed to last 25 years or more in service with minimal technical and operational changes. This longevity presents unique challenges, especially the need for continuous maintenance and system upgrades, including cybersecurity measures.

Any disruption to maritime operations can have far-reaching consequences, impacting the flow of goods and the stability of global markets. The diversity of stakeholders—from shipping companies and port operators to regulatory bodies and technology providers—adds layers of complexity, making coordination and communication essential. This complexity is particularly pronounced in cybersecurity, where evolving threats continually heighten the stakes.

The maritime industry must prepare for a range of potential disruptions, from natural disasters to geopolitical tensions. Building resilience into maritime operations—including cybersecurity resilience—is essential for ensuring the industry's continued ability to operate under challenging conditions. To continue fulfilling its vital role in the global economy, stakeholders must be proactive in addressing emerging trends. This white paper will explore the critical role of cybersecurity in safeguarding maritime operations.

Challenges and Realities

Traditionally, maritime operations relied heavily on mechanical and manual processes, with navigation, communication, and logistics managed by seasoned seafarers with minimal technological aid. As global trade expanded, the demand for more efficient and reliable operations grew, so the industry began to adopt more sophisticated technologies. The advent of satellite navigation, automation, and digital communication systems revolutionized how vessels are operated and managed, leading to significant advancements in efficiency, safety, and overall productivity. The shift from isolated mechanical systems to interconnected automated ones opened the door to a new set of vulnerabilities. Initially, the focus was on enhancing operational capabilities, with cybersecurity concerns as an afterthought. However, as cyber threats grow in frequency and consequence, the industry must change to prevent crises.

Cyberattacks targeting the maritime sector highlight the industry's vulnerabilities and underscore the need for robust cybersecurity measures. A notable example is the Volt Typhoon attack in February 2024.[2] This cyber espionage campaign, attributed to a state-sponsored actor, targeted critical infrastructure, including maritime operations, to gather intelligence and pre-position themselves for future disruptive or destructive cyber activity. The attack, identified by the Cybersecurity and Infrastructure Security Agency (CISA), exposed significant weaknesses in the maritime sector's cybersecurity posture and emphasized the threat posed by state-sponsored cyber actors.

In August 2021, Port Houston identified an attempted intrusion into its business systems and isolated the system while working with its security vendors and local federal agencies.[3] The attempt used a zero-day exploit (an undocumented or not publicly known vulnerability in software or hardware) to gain access or corrupt the system. Thankfully, Port Houston noticed the anomalous activity and acted, stopping the adversary's attempt.[4]

Perhaps the most infamous cyberattack on the maritime industry was the NotPetya malware attack in 2017, which had a profound impact on Maersk, one of the largest shipping companies in the world.[5] NotPetya, initially disguised as ransomware, was a destructive wiper malware that spread rapidly across Maersk's global network, crippling its operations. The attack rendered the company's IT systems inoperable, leading to a massive disruption in its shipping and logistics operations. Maersk estimated that the attack cost the company between $300 million and $400 million, a stark reminder of the catastrophic financial impact a single cyber incident can have. The aftermath of the NotPetya attack forced Maersk to rebuild its entire IT infrastructure—a monumental task that took months and required unprecedented cooperation across the company.

Beyond ransomware, the maritime industry faces other cyber threats that can disrupt operations and compromise safety. GPS spoofing and jamming are among the most common types of cyberattacks targeting navigation systems. These attacks can deceive a vessel's navigation system by providing false GPS data, potentially leading the vessel off course or into dangerous waters. A detailed examination of GPS vulnerabilities was highlighted in a 2020 paper presented at the International Naval Engineering Conference (INEC).[6] The paper discussed how GPS spoofing and jamming could be used to manipulate a ship's position, with potentially disastrous consequences. More recently, similar studies show the extent of Russian GPS jamming in the Nordic and Baltic regions.[7]

---

[2] U.S. Department of Homeland Security, "Opening Statement by CISA Director Jen Easterly," https://content.govdelivery.com/attachments/USDARD/2024/02/07/file_attachments/2776182/SPARKS%20-%20Cybersecurity%20%28Attachment%29.pdf

[3] "Hackers Breached Computer Network at Key US Port but Did Not Disrupt Operations," September 2021, www.cnn.com/2021/09/23/politics/suspected-foreign-hack-houston/index.html

[4] "Portman Questions Cybersecurity Officials in Wake of ManageEngine Vulnerability and Increased Cyberattacks," Homeland Security and Governmental Affairs, September 2021, www.hsgac.senate.gov/media/reps/portman-questions-cybersecurity-officials-in-wake-of-manageengine-vulnerability-and-increased-cyberattacks/

[5] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[6] "Claims of State-Sponsored Cyberattack in the Maritime Industry," https://library.imarest.org/nanna/record/7663/files/INEC_2020_Paper_30.pdf

[7] "Dual-Satellite Geolocation of Terrestrial GNSS Jammers from Low Earth Orbit," April 2023, https://radionavlab.ae.utexas.edu/wp-content/uploads/clements-direct-geolocation.pdf

The operational challenges from cyber threats within the maritime industry are compounded by the complexity of the systems on board vessels. Modern ships are equipped with a multitude of interconnected systems, ranging from navigation and communication to cargo management and engine control. These systems are often built by different manufacturers and operate on various technological platforms, making them difficult to secure uniformly. Moreover, the rapid pace of technological change means that ship owners and operators must constantly upgrade their systems to stay competitive, introducing new connectivity, threat surfaces, and potential vulnerabilities with each upgrade.

Operational dependency on critical systems is another key concern. The reliance on third-party remote access for maintenance and system updates is a double-edged sword. Although it allows for efficient management of ship systems, it also introduces significant cybersecurity risks. Remote access may be exploited by malicious actors to gain unauthorized entry into ship systems, potentially leading to data breaches and loss of visibility, control, or availability in critical systems. The intersystem dependencies on board modern vessels further exacerbate this risk, because a compromise in one system can quickly cascade to others, causing widespread disruption.

The maritime industry also faces challenges related to the maturity of its cybersecurity practices. Despite growing awareness of the importance of segmentation and secure architecture design, many vessels still operate with legacy systems that are poorly segmented, increasing the risk of lateral movement in the event of a cyberattack.

As vessels become more reliant on digital systems, the role of the crew in maintaining cybersecurity becomes increasingly important. There is frequently a lack of knowledge and awareness among crew members, who may not be fully trained in cybersecurity best practices. This lack of training can leave vessels vulnerable to basic cyber social engineering attacks that exploit human error. Effective training programs are essential to ensure that all crew members, from the captain to the deckhands, understand the risks and know how to respond to potential threats.

The maritime industry is at an inflection point, where the benefits of technological advancement are tempered by the realities of cybersecurity threats. Industry must develop strategies that protect critical systems and ensure the safety and resilience of global maritime operations.

Regulations and Standards: Government Influence in Maritime Cybersecurity

From 2021 to 2023, the US Coast Guard deployed cyber protection teams to investigate approximately 45 cybersecurity incidents each year in the US maritime sector.[8] These cases involved attacks against information technology systems and operational technology (OT) systems. At least one of the investigations attributed the cyberattack to a nation-state actor. In addition to cyber response activities, these cyber incidents spurred government and credentialing authorities to establish regulations, guidance, and security frameworks for the maritime sector.

International Requirements and Guidance

In June 2022, the International Maritime Organization (IMO) provided an update to its 2017 Guidelines on Maritime Cyber Risk Management. These updated standards provide high-level requirements of risk management programs to safeguard the shipping community from cybersecurity threats.[9] Although technically non-binding and broad, the actions by the IMO create a follow-on focus area for nations to advance maritime cybersecurity.

In 2022, the European Union (EU) issued comprehensive requirements for cybersecurity across critical infrastructure sectors of the EU and cross-border businesses. These requirements are captured in the EU National Directive for Information Security 2 (NIS 2), which takes effect in October 2024.[10] A significant aspect of this directive is the time-bound requirement to issue downstream notifications of any cyber incidents that may impact or disrupt business. This notification means companies will learn about cyberactivity occurring upstream and may become liable for the cascading impact when their services halt. Additionally, NIS 2 requires companies to conduct risk assessments of their supply chain and security posture, which may then become evidence in court if requested after a breach.

US Requirements and Guidance

In December 2020, the US government published the National Maritime Cybersecurity Plan (NMCP), which focused on maritime-related national security issues.[11] This strategy highlighted a focus on OT systems, directed risk modeling for the industry, and reduced dependency on and risk from equipment supplied by adversarial nations. Building on this strategy, in February 2024, President Biden issued an executive order (EO) on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States.[12] This EO provides the captain of the port (COTP; the senior US Coast Guard officer in a port) broad authority to search for and remove any device, person, or vessel from the port or waterfront facility. Additionally, the EO allows the COTP to take control of any vessel as allowed by US

---

[8] US Coast Guard, "2023 Cyber Trends and Insights in the Marine Environment," www.uscg.mil/Portals/0/Images/cyber/CTIME_2023_FINAL.pdf

[9] "Guidelines on Maritime Cyber Risk Management," June 2022, wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf

[10] "Directive (EU) 2022/2555 of the European Parliament and of the Council," December 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

[11] "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security," December 2022, https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/12.2.2020-National-Maritime-Cybersecurity-Plan.pdf

[12] "Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States," February 2024, www.whitehouse.gov/briefing-room/presidential-actions/2024/02/21/executive-order-on-amending-regulations-relating-to-the-safeguarding-of-vessels-harbors-ports-and-waterfront-facilities-of-the-united-states/

jurisdiction. Although this may have exceptions or different impacts for foreign-flagged vessels, all US vessels, harbors, ports, waterfront facilities, and people in such places are subject to search and removal of their digital devices.

The US Coast Guard also updated its reporting requirements for breaches of security, suspicious activity, transportation security incidents, and cyber incidents.[13] This guidance provides clarity for laws and regulations requiring *any* vessel, harbor, port, or waterfront facility to report all cyber incidents (among other security incidents) to the Federal Bureau of Investigation (FBI), CISA, and US Coast Guard.

Directly impacting the port and terminal environment, the US Coast Guard issued Maritime Security Directive 105-4: Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies.[14] This document builds on the NMCP to require specific actions by owners of ship-to-shore cranes supplied by China. Owner/operators may engage their local US Coast Guard representatives to understand the requirements.

Finally, the US Coast Guard published national proposed rulemaking (NPRM) for Cybersecurity in the Maritime Transportation System.[15] This NPRM foreshadows regulations to require cybersecurity assessments, inspections, and testing for all US-owned or operated vessels and facilities. The final rules are expected in 2025, but will likely increase the credentialing, inspection, and assessment currency requirements for US-flagged vessels.

Key Guidance and Regulations:

- **Vessels: IACS UR EA 26, UR EA 27, ISM MSC.428(98), EU NIS 2, NVIC 02-24, NPRM**
- **Ports: EU NIS 2, USCG MARSEC Directive 105-4, NVIC 02-24, NPRM**
- **Shipyards: IACS UR EA 26, UR EA 27, EU NIS 2[1], NPRM**

Classification Societies Requirements

In 2023, the International Association of Classification Societies (IACS) issued unified requirements (URs) on cybersecurity for all new ships built after January 1, 2024. These baseline requirements for cyber resilience in the design, construction, commissioning, and operation of vessels and the shipboard systems provide a set of standards that credentialing companies utilize in certifying a ship for operation. E26 focuses specifically on the cyber resilience of the ship,[16] and E27 focuses on the hardening of shipboard systems by suppliers.[17]

Coverage by Fortinet Solution

A common challenge when selecting and implementing the technology to meet regulatory requirements, such as UR E27, is ending up with a mixed technology stack spread across multiple vendors. This increases complexity and cost during the implementation and maintenance of the various technologies between various vendors. Although there may be controls that require additional coverage, Fortinet has a comprehensive suite of technologies that minimizes the number of vendors required in the cybersecurity controls in the technology stack. Through either product selection or configuration management, Fortinet is able to assist in the compliance requirements of UR E27 regulation.

[13] "Navigation and Vessel Inspection Circular No. 02-24," February 2024, www.uscg.mil/Portals/0/Images/cyber/BOS_SA_Cyber%20Reporting%20NVIC.pdf

[14] "Issuance of Maritime Security (MARSEC) Directive 105-4; Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies," February 2024, www.federalregister.gov/documents/2024/02/23/2024-03822/issuance-of-maritime-security-marsec-directive-105-4-cyber-risk-management-actions-for-ship-to-shore

[15] "Cybersecurity in the Marine Transportation System," February 2024, www.federalregister.gov/documents/2024/02/22/2024-03075/cybersecurity-in-the-marine-transportation-system

[16] "Cyber Resilience of Ships," November 2023, www.classnk.com/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf

[17] "IACS Adopts New Requirements on Cyber Safety," https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/

Frameworks to Secure Maritime Systems

The integration of advanced technology and digital systems in maritime is a necessity and a vulnerability. Protecting these advanced systems, along with any legacy systems, from cyber threats requires a comprehensive and scalable approach that aligns with the industry's maturity levels. Maritime organizations are faced with objectives outside of regulatory compliance:

- What are the most effective minimums to begin
- How can cybersecurity controls be effectively measured against real-world attacks
- What comprehensive frameworks exist to further reduce risk

The SANS Five ICS Cybersecurity Critical Controls white paper[18] offers an outcome-focused approach to securing industrial control systems (ICS) across various stages of maturity. These controls emphasize alignment with real-world threats with an organization's maturity level, ensuring that cybersecurity measures are scalable and adaptable. This framework guides the selection, prioritization, and implementation of controls, focusing on their effectiveness and maintainability. As quoted from the paper, these first five controls "ask organizations to identify the scenarios they want to be prepared against." For maritime operations, this means tailoring security controls to the needs of each vessel and operation, ensuring practicality and sustainability.

Another key tenet of any cybersecurity framework is the concept of protection and detection in depth. This approach advocates for layered security measures, ensuring that if one defense fails, others remain in place to protect the vessel's critical systems. Many maritime systems utilize both legacy systems and systems with lacking security controls. A defense in depth approach provides needed protection of those systems. For example, in the maritime context, this could involve implementing robust network segmentation, secure access controls, and continuous monitoring to detect and respond to potential intrusions. By integrating layers of defense, maritime operators are protected against a range of threats, from targeted cyberattacks to inadvertent internal security breaches.

The International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443 standards are globally recognized as a comprehensive set of guidelines for cybersecurity across the entire life cycle of industrial automation and control systems, including fulfilling the UR E26 and E27 requirements. For the maritime industry, aligning with these standards ensures security in the design, implementation, and operation of ship systems. The 62443 standards also emphasize the importance of collaboration between all stakeholders—from shipbuilders to operators—to create a unified and secure operational environment.[19]

See our white paper for insight into effective deployment of the IEC 62443 at www.sans.org/white-papers/39960

[18] "The Five ICS Cybersecurity Critical Controls," November 2022, www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

[19] www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Security assessments and audits are a valuable way to ensure the frameworks and principles of a cybersecurity program are correctly instituted and in compliance with both industry standards and regulatory requirements. Due to the complexity in shipbuilding, two identical ships built at the same shipyard could have different topologies and system deployment strategies. On-scene assessments and audits can identify irregularities. During periodic maritime security assessments, various aspects of the vessel's cybersecurity posture are assessed, from the integrity of its network architecture to the effectiveness of its incident response plans. Key areas of focus include the implementation of critical security controls, the robustness of data protection measures, and the preparedness of the crew to handle cybersecurity incidents. By conducting these activities, maritime operators can identify potential weaknesses and take proactive steps to address them.

The role and responsibilities of various stakeholders in maritime cybersecurity are clearly defined but require close collaboration to be effective. As an example, Figure 1 breaks down the roles and responsibilities for ships.

Figure 1. Primary Stakeholders for Ships

Network Segmentation, Zones, and Conduits

Separating the various technology systems based on network and purpose is an essential cybersecurity measure. The Purdue model, shown in Figure 2, is a common framework that is useful for defining the network, technologies, and purpose of operational technology on ships and in ports. The technologies and subsystems use different network and system bus technologies such as CANbus, Profibus, and Modbus. These technologies are used in critical control systems for engines, power management, and other vital functions. Unlike the Ethernet-based networks that form the backbone of a vessel's IT and OT infrastructure, these bus systems operate in specialized environments where data transfer protocols and hardware interfaces are unique.

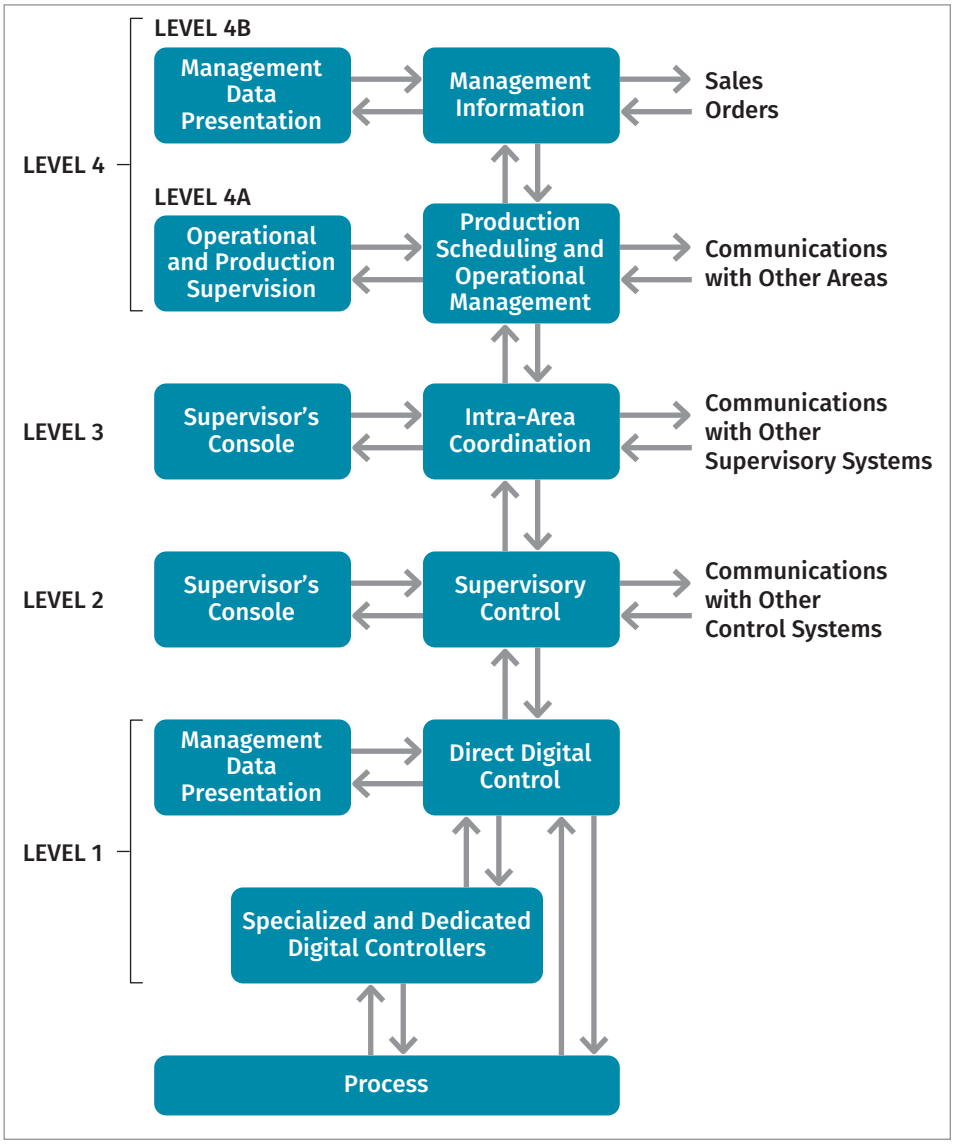

Figure 2. The Purdue Model

Proper segmentation supports many additional cybersecurity benefits. For example, it can prevent a breach in one system from spreading to others, contain potential damage, and maintain overall system integrity. Zones and conduits are an extension of network segmentation and essential aspects of securing maritime systems. According to the ISA/IEC 62443 standards, a "zone" is a grouping of physical or logical assets that share common security requirements. A "conduit" is the communication link between these zones. Though similar elements of technology exist between vessels, how those systems are designed, implemented, and maintained will vary. This is to be expected with the desire for improved operations and evolution of technology over time. When identifying and designing segmentation, zones, and conduits, these variations must be considered during the design process to ensure the design provides a secure architecture.

A significant cybersecurity challenge in these subsystems is the interconnections, often spanning multiple zones within the ship's network architecture. These connections may not always be captured or adequately addressed in cybersecurity assessments or audits primarily focused on Ethernet-based networks and conduits. As a result, vulnerabilities can persist in these lower-level systems, creating potential attack vectors for malicious actors. The presence of serial and protocol gateways, which are commonly used to bridge different communication protocols between these subsystems, further exacerbates the risk. These gateways may not be as rigorously secured or monitored as other parts of the network, leaving them vulnerable to exploitation. Architects and operations should consider the necessity of gateways when assessing or designing system architecture.

Coverage by Fortinet Solution

The white paper Effective ICS Cybersecurity Using the IEC 62443 Standard[20] outlines what the standard entails as well as how to effectively approach using the standard. It also highlights Fortinet solution mapping and compliance.

Demilitarized Zone (DMZ)

A DMZ is an important element for network security that serves as a buffer zone between the vessel or port system's internal networks and external networks, such as those used by port authorities or third-party service providers. The DMZ allows for controlled access to critical systems, reducing the risk of unauthorized access while still enabling necessary communication and data exchange. For ship-to-shore (STS) cranes, this means control systems may be securely accessed for maintenance or operational purposes without exposing the vessel's or port's core networks to potential cyber threats.

A critical component of maritime infrastructure is ship-to-shore (STS) crane systems used in port operations. These cranes facilitate the loading and unloading of goods from vessels. These cranes are often automated and networked, making them targets for cyberattacks. Protecting STS crane systems involves more than just securing the cranes; it requires implementing robust cybersecurity measures within the broader port infrastructure, including the creation of a demilitarized zone (DMZ) and the establishment of zones and conduits.

For STS cranes, zones might include the crane control system, the port's operational network, and the vessel's cargo management system. Establishing secure conduits between these zones ensures that data can be transmitted between them without exposing sensitive systems to unnecessary risks.

Coverage by Fortinet Solution

Many organizations begin the deployment of a DMZ through the design of a clearly enforced network security perimeter, typically leveraging the core functions of a traditional firewall. Fortinet FortiGate Next-Generation Firewalls support these core functions as an initial maturity step. As the demand for maturity grows, FortiGate integrates with the Fortinet OT Security Platform and enables centralized management, application control, advanced threat detection, and secure SD-WAN.

[20] "Effective ICS Cybersecurity Using the IEC 62443 Standard," December 2023, www.sans.org/white-papers/39960

Visibility and Monitoring

Vessels at sea rarely have an IT or cybersecurity professional on board. This reality necessitates the development of systems and procedures that are both user-friendly and resilient. For example, automated monitoring and alerting systems can be employed to detect and respond to potential threats, minimizing the need for direct human intervention. Additionally, implementing strong access controls and encryption can protect sensitive data and systems, even in the absence of specialized cybersecurity personnel.

Coverage by Fortinet Solution

The Fortinet solution brings visibility to existing product vulnerabilities within on-board systems while also monitoring for threats within the environment. Its simplified deployment for remote vessels includes a zero-touch configuration, with rugged hardware models available to support the needs of maritime.

Remote Access

Given the critical operational dependencies of these systems, ship owners must secure third-party remote access, ensure robust network segmentation, and maintain inter-system integrity. Third-party remote access, often necessary for maintenance and system updates, must be tightly controlled to prevent unauthorized access. This includes using secure communication channels, multifactor authentication, and real-time monitoring to detect and block any suspicious activity.

Coverage by Fortinet Solution

A Fortinet solution facilitates agentless secure remote access to manage, monitor, and protect remote access by all third-parties, contractors, and auditors. The streamlined implementation and management of all Fortinet solutions can benefit a single vessel or an entire fleet.

Training

Finally, the industry must continue to improve the maturity levels of its cybersecurity practices, particularly in terms of knowledge and awareness among crew members. This includes regular training and drills to ensure that all personnel can respond effectively to cyber incidents. This includes not only understanding the technical aspects of cybersecurity but also recognizing the importance of adhering to established protocols and being vigilant against potential threats. As an extension of this training, the crew should include cyber-related risk events in their safety and operation drills.

Coverage by Fortinet Solution

The Fortinet Network Security Expert (NSE) Certification program offers specialized OT cybersecurity training through its NSE 7 OT Security certification. This program provides:

- **Hands-on labs for practical experience in securing industrial systems, a deep dive into Fortinet's specific OT security tools**
- **Industry-recognized credentials, adding credibility to both system integrators and vessel operators**
- **Access to Fortinet's global support and resources, ensuring long-term success in managing and securing maritime OT environments**

Coverage by SANS Institute

The SANS Institute provides many cybersecurity courses focused on industrial control systems. These courses not only lay down the foundational knowledge across the SANS Five ICS Cybersecurity Critical Controls,[21] but also provide the required skill sets to initialize and support the cybersecurity life cycle throughout its various activities and to increase its maturity.

[21] "The Five ICS Cybersecurity Critical Controls," November 2022, www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

Moving Forward

The first activity all maritime system owners and operators must perform is a cybersecurity risk assessment specific to their systems. This activity is the catalyst in determining the strategic and tactical direction a system owner must take to improve cybersecurity. The results of these assessments become the baseline in defining a strategy that includes planning the security design, deployment, and measurement of cybersecurity investment. Risk assessments are a continuous or periodic process because changes do occur in both the system and the environment.

The next activity is an internal discussion on alignment between key security controls and regulations/standards. It is logical that compliance with regulatory requirements will dominate this activity, and this endeavor will enhance the culture and mindset around cybersecurity. However, only complying with the necessary regulations rarely provides the necessary capabilities to mitigate all the risks identified in the risk assessment. Planning early in the life cycle for outcomes beyond the regulatory needs will allow security architects to maximize investment by selecting cybersecurity technologies that can support additional capabilities further down the road.

Three continuous activities that are regularly overlooked but must be considered as short- and long-term objectives early and throughout the maturity process are vulnerability management and continuous monitoring and auditing of deployed cybersecurity controls.

Many strategic plans are programs that operate in five-year stints. Regularly reviewing the plan to evaluate or perform activities outside of the program, such as the activities outlined in the SANS Five ICS Cybersecurity Critical Controls,[22] will help the team achieve their cybersecurity requirements and goals through a changing threat environment.

[22] "The Five ICS Cybersecurity Critical Controls," November 2022, www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

Compliance Mapping to UR E27

Shipping UR E27 Alignment				Fortinet Solution Mapping and Compliance		
Base Controls		Where Systems are Networked to Untrusted Assets (Supplemental Controls)		Relevance	Compliance	Solution Description
Cyber Event Type	Control Item Number	Associated Security Mechanism	Control Item Number	IACS/Fortinet	Full/Partial/None	P: Product | C: Configuration | N: Note
Casual or coincidental access by unauthenticated entities	1			Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiPAM C: Product(s) integration
		Multifactor authentication for human users	31	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken C: Product(s) integration
		Software process and device identification and authentication	32	Both	Full	P: FortiEDR, FortiClient, FortiGate C: Product(s) integration
				Both	Full	P: FortiEDR, FortiClient, FortiGate C: Product(s) integration
Casual or coincidental access by unauthenticated entities	2			Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
	3			Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
	4			Both	Partial	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration N: Fortinet does not offer hardware security modules such as HSM or TPM for IACS, however, Fortinet product(s) meet the requirement.
	5			Both	Full	P: FortiAP/FortiWiFi, FortiGate, FortiAuthenticator, FortiToken C: Product(s) integration
	6			Both	Full	P: FortiGate, FortiAuthenticator C: Product(s) integration
Casual or coincidental access by unauthenticated entities	7			Both	Full	P: FortiGate C: Network traffic encryption if/where applicable
		Unsuccessful login attempts	33	Both	Full	P: FortiGate, FortiAnalyzer, FortiManager C: Product(s) integration
		System use notification	34	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer C: Product(s) integration
		Access via untrusted networks	35	Both	Full	P: FortiGate C: Security policies
		Explicit access request approval	36	Both	Full	P: FortiGate, FortiAuthenticator, FortiPAM, FortiManager C: Product(s) integration
Protect against casual or coincidental misuse	8			Both	Partial	P: FortiGate, FortiAuthenticator, FortiPAM, FortiManager C: Product(s) integration N: IACS asset owner or manufacturer or integrator need to ensure such capability is available within the IACS. Fortinet product(s) can complement with additional features (e.g., multifactor authentication to meet the requirement).
	9			Both	Full	P: FortiAP/FortiWiFi, FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
	10			Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
	11			Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiSandbox C: Product(s) integration
	12			Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
		Remote session termination	37	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
Protect against casual or coincidental misuse	13			Both	Full	P: FortiGate, FortiAuthenticator, FortiPAM, FortiAnalyzer, FortiManager, FortiSIEM, FortiSOAR C: Product(s) integration
	14			Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration
	15			Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration
	16			Both	Full	P: FortiGate, FortiSwitch, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration N: The product(s) can function as NTP server to provide time to the network connected assets. Precise time synchronization functionality over network (e.g., IEEE 1588v2 PTP is available only in select product[s]). Capability is limited to any network asset(s) connected to/via the product(s).

Shipping UR E27 Alignment				Fortinet Solution Mapping and Compliance		
Base Controls		Where Systems are Networked to Untrusted Assets (Supplemental Controls)		Relevance	Compliance	Solution Description
Cyber Event Type	Control Item Number	Associated Security Mechanism	Control Item Number	IACS/Fortinet	Full/Partial/None	P: Product | C: Configuration | N: Note
Protect the integrity of the CBS against casual or coincidental manipulation	17			Both	Full	P: FortiGate, FortiAnalyzer, FortiManager C: Product(s) integration
		Cryptographic integrity protection	38	Both	Full	P: FortiGate, FortiAnalyzer, FortiManager C: Product(s) integration
	18			Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiManager, FortiSandbox C: Product(s) integration
	19			Both	Full	P: FortiTester and FortiResponder N: The product can be offered as a service.
		Input validation	39	Both	Partial	N: Fortinet product(s) are compliant with the requirement however, IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
Protect the integrity of the CBS against casual or coincidental manipulation	20			Both	Partial	N: Fortinet product(s) are compliant with the requirement however, IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
		Session integrity	40	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiAnalyzer, FortiManager C: Product(s) integration
		Invalidation of session IDs after session termination	41	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiAnalyzer, FortiManager C: Product(s) integration
Casual or coincidental access by unauthenticated entities	21			Both	Full	P: FortiGate C: Using the product(s), implement encryption of relevant information in transit C: Using the product(s), implement encryption of relevant information in transit for untrusted networks C: Using the product(s), implement protection/encryption of relevant information in transit between the zones
Prevent the unauthorized disclosure of information via eavesdropping or casual exposure	22			Both	Partial	N: IACS asset owner or manufacturer need to ensure such capability is available within the IACS. Fortinet product(s) have built-in capability to meet the requirement.
Monitor the operation of the CBS and respond to incidents	23			Both	Partial	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration C: With regard to FortiAnalyzer, integration with IACS may be required for provisioning access to the logging and monitoring information available within Fortinet product(s) (e.g., via syslog etc.)
Ensure that the control system operates reliably under normal production conditions	24			Fortinet	Full	P: FortiGate C: Using the product(s), implement DoS protection, SYN flood protection, rate-limit, traffic shaping policies
	25			Both	Full	P: FortiGate C: Using the product(s), implement, rate-limit and connection restriction policies
	26			Both	Partial	P: FortiEDR Manager, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions C: The product(s) support configuration backup for Fortinet products and can be integrated with Fabric-Ready partner solutions that offer capability to meet the requirement. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
	27			Both	Partial	P: FortiEDR Manager, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions C: The product(s) support configuration backup for Fortinet products and can be integrated with Fabric-Ready partner solutions that offer capability to meet the requirement. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
	28			Both	Partial	N: Fortinet product(s) are available with redundant power inputs/supplies and can be configured in high-availability and fault-tolerant configuration. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
	29			Both	Full	P: FortiGate, FortiAnalyzer, FortiManager N: Fortinet product(s) support baseline configuration and dedicated management interface for configuration and operations management.
	30			Both	Full	P: FortiGate, FortiEDR, FortiClient C: Product(s) integration and implementation of security policies to restrict unnecessary functions/ports/protocols/services

Sponsor

SANS would like to thank this paper's sponsor: