WHITEPAPER

DRAGOS
SAFEGUARDING CIVILIZATION

ICS/OT Cybersecurity Considerations for Maritime Transportation

Threats, Challenges, and the Need for a Standardized Approach

LIZ MARTIN | CHANNEL SOLUTION ARCHITECT
DRAGOS, INC.
BLAKE BENSON | SENIOR CYBER ADVISOR
GLOBAL GOVERNMENT SERVICES ABS GROUP

JANUARY 2023

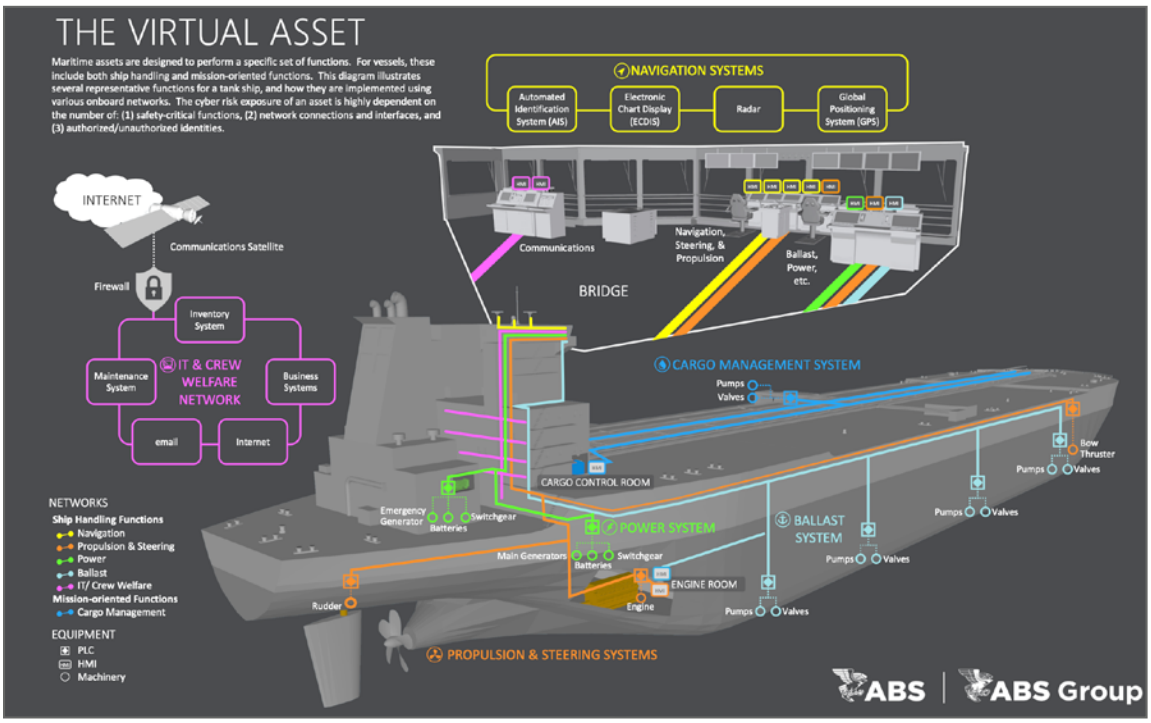
ABS Group

Transportation modes are broken into multiple sub-sectors, consisting of highway, surface, transportation, aviation, maritime and pipeline as defined by the Department of Homeland Security (DHS). These modes rely on industrial control system/operational technology (ICS/OT) devices to perform critical operations and safety functions. Maritime encompasses ports, vessels, and inland waterways in and surrounding the United States.[1] Under the Maritime Transportation Security Act of 2002 (MTSA) the United States Coast Guard (USCG) is the major, governing organizational authority for maritime. One of the greatest challenges facing the maritime arena is the lack of regulations that have specifically addressed ICS/OT security.

Critical Assets and Protocols in Maritime

Maritime ICS/OT contains similar systems and software components to what is seen in land-based critical infrastructure installations, such as building management, power, manufacturing, and oil and gas (ONG).[2]

A typical maritime installation includes a dedicated central processing unit (CPU) that runs a controller device, which monitors data input adjusting speed, temperature, or pressure. When the expected, programmed values diverge, an actuator will make necessary adjustments to increase or decrease the motor speed or temperature and open/close a valve. A commercial merchant ship relies on hundreds of ICS processes to manage propulsion, support navigation, communications, fire suppression systems, safety systems and cargo loading and unloading. Support vessels such as pilot boats, tugboats, fireboats, and oil spill response vessels, maintain and monitor safety and security of cargo entering and leaving ports.



1 L. Kaiser, "2013- 2023 Transportation Industrial Control Systems (ICS) Cybersecurity Standards Strategy." [Online]. Available: http://trbcybersecurity.erau.edu/files/Transportation-Standards-Plan.pdf

2 A. Andreu, "ICS Security Maritime," The Cyber Startup Observatory, Jul. 19, 2020. https://cyberstartupobservatory.com/ics-security-for-the-maritime-industry/ [accessed Sep. 09, 2022].

The navigation systems that support vessel traffic management systems used by the USCG contain OT components. Mechanical systems that operate locks and dams also contain OT. Components that are responsible for the dock container cranes, straddle-carriers and vehicles that load/unload and transport containers at ports that handle grain, ore, crude oil, diesel, toxic chemicals, and liquefied natural gas (LNG) all contain OT.[3]

When investigating the typical ICS/OT protocols in the MTS space, NMEA is a common protocol specific to vessel operations. The various standards of NMEA are 0180, 0182, 0183 and the latest NMEA 2000 standard. Most commercial vessels are found to be using NMEA 0183.[4] Other protocols you'll see on-board are more standard or universal protocols such as, CAN BUS, MODBUS and PROFIBUS, which are found on any given vessel depending on age of equipment and what stage of retrofitting the vessel is currently under.

For shore-side assets (port facilities) a variety of functions are performed dependent on whether there are nuclear, chemical additive operations or ONG petroleum-based operation. Each of those areas have common architectures that are found in any other facility networking any other facility network. Convergence of IT/OT is the true hurdle in any one of these areas. For example, a container port operation looking at optimization efforts to quantify and increase productivity and efficiencies might leverage sensors on the OT infrastructure responsible for performing safety critical functions. The architectures are differentiated slightly based on the level of integration—using container cranes as a case example—on-board the vessel, the deck crane is likely tied into a load management software primarily leveraged for shipboard stability.[5] Shoreside operations feature a variety of environments. In the most integrated environments, there will be sensors recording output from container cranes and highly integrated terminal operating systems (OS) with larger business networks to forecast supply chain information or general demand to key stakeholders. These examples further highlight just how significant the threat landscape is within MTS. Ensuring full visibility across all activities within facilities and monitoring of gate and truck movements, terminal inventory, vessel movements and crane operations are crucial to terminal operations and overall performance.[6]

Threats and Challenges

Maritime vessels, ports and waterways continue to adopt new technology to improve GPS, propulsion, safety and traffic management capabilities, which only increases security risk with limited standards and guidelines.

Commercial vessels have a vast cyber-attack surface, where the engines of these vessels are controlled by computers and those computers rely on electronic charting and GPS. The biggest challenge facing the maritime community is the lack of awareness that cybersecurity has an impact on the equipment and mission. That lack of awareness is what ultimately leads to little or no standards across the industry, negatively impacting the operational safety and security of maritime systems. In 2017 a shipping firm [AP Moller-Maersk] faced a ransomware attack that ended up costing the firm between $250 and $300 million.[7] In August of 2021 the Port of Houston Authority was targeted in a cybersecurity attack where unidentified hackers accessed a web server on Port Houston. The attacker took advantage

3 U.S. Department of Transportation, *"ICS Security in Maritime Transportation,"* Jul. 2013. **https://rosap.ntl.bts.gov/view/dot/10057/dot_10057_DS1.pdf**

4 *National Marine Electronics Association,"* NMEA. [Online]. Available: **https://www.nmea.org/nmea-0183.html**. [Accessed: 21-Nov-2022].

5 *"Cargomax for bulk carriers - herbert-abs,"* Herbert. [Online]. Available: **https://www.herbert-abs.com/cargomax-for-bulk-carriers**. [Accessed: 21-Nov-2022].

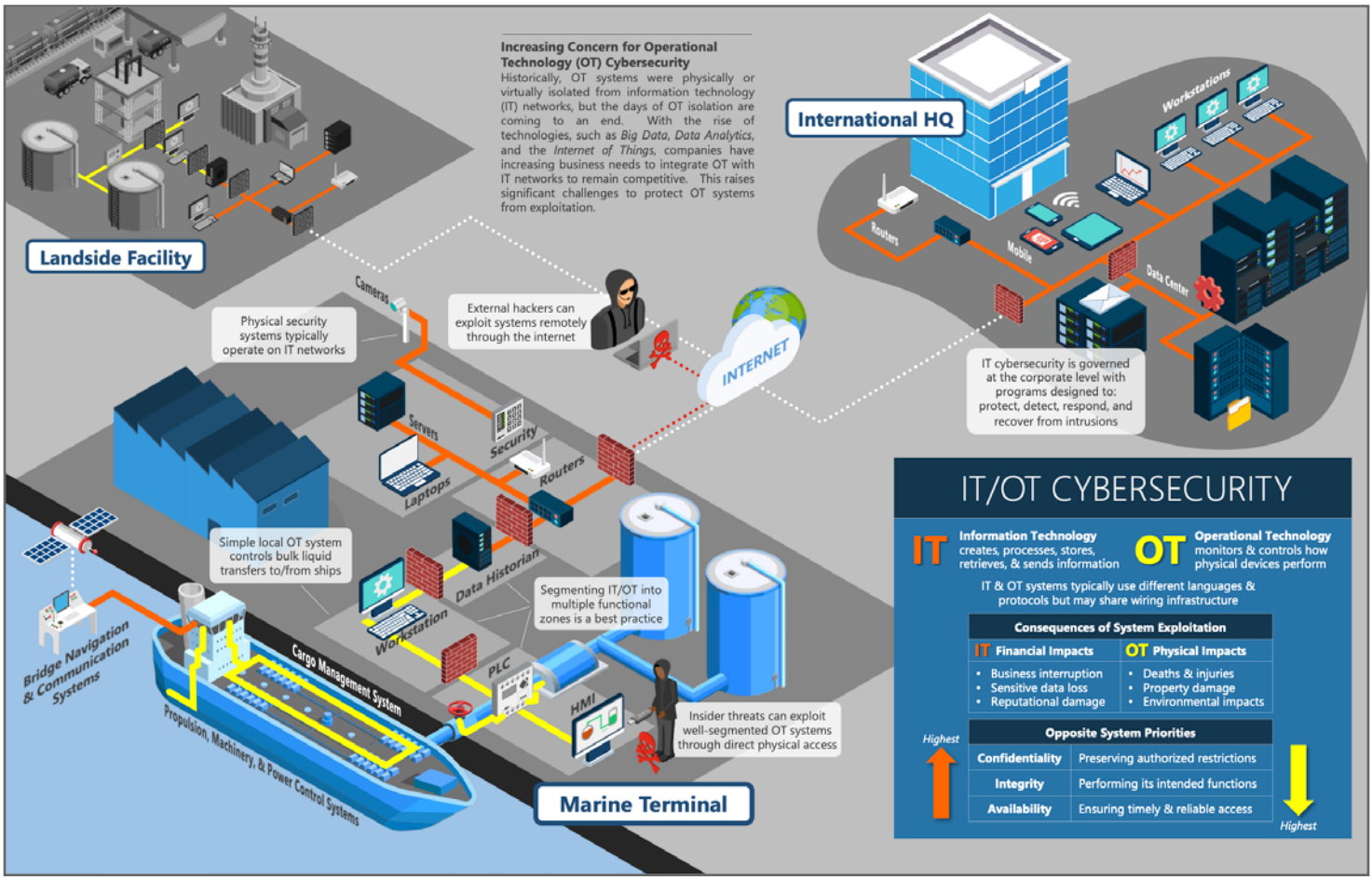
6 *"Terminal operating systems: Main features, integration, and providers overview,"* AltexSoft, 22-Jul-2022. [Online]. Available: **https://www.altexsoft.com/blog/terminal-operating-system/**. [Accessed: 21-Nov-2022]

7 L. O'brien, *"Port and Maritime Cybersecurity Vulnerabilities Finally Get More Attention,"* ARC Advisory Group. **https://www.arcweb.com/industry-best-practices/port-maritime-cybersecurity-vulnerabilities-finally-get-more-attention**

of a vulnerability within a software platform used for password management and single-sign-on (SSO). Luckily, the Port of Houston had a facility security plan in place in compliance with MTSA, which ultimately ensured no operational data or systems were impacted by the attack.[8]

In June 2022, Freeport LNG facility out of Texas suffered an explosion that caused speculation for months as to the root cause. The Pipeline and Hazardous Materials Safety Administration (PHMSA) reported several issues thus far. The incident exposed deficiencies in valve testing procedures, failure to adjust alarms that would alert operators increasing temperatures during operations and procedures that allowed operator discretion when making decisions to close valves that might otherwise cause LNG to remain trapped in pipes. Commercial processing remains halted until the facility becomes operational again, which was estimated to begin partial operations by early 2023.[9]

Virtually 90% of global trade is conducted by shipping, presenting the maritime industry as a prime target for adversaries. As previously noted, shipboard systems are composed of both IT and OT, introducing further risk into the environment that could ultimately impact the loss of control of a ship. Another obstacle for the maritime industry is the difficulty associated with delivering repeatable, tailored and scalable security training, given that ship crews are usually temporary and frequently rotating out. With most of the crew being contracted out through many levels



8 J. Donnelly, *"Port Houston targeted by suspected nation-state actor in cyber-attack,"* Port Technology International, 24-Sep-2021. [Online]. Available: **https://www.porttechnology.org/news/port-houston-targeted-by-nation-state-actor-in-cyber-attack/#:~:text=The%20Port%20of%20Houston%20Authority,Houston%20premises%20on%2019%20August**. [Accessed: 22-Nov-2022].

9 *"U.S. regulator releases report blaming Freeport LNG Blast on inadequate processes,"* Reuters, 16-Nov-2022. [Online]. Available: **https://www.reuters.com/business/energy/freeport-lng-provides-no-timeline-texas-export-plant-restart-2022-11-15/**. [Accessed: 22-Nov-2022].

of outsourcing, the assignment and responsibility of triaging and alerting on incidents affecting information systems or OT on vessels becomes next to impossible. The USCG encourages regular cybersecurity assessments of all vessels and facilities to ensure complete understanding and mitigation or remediation of cybersecurity vulnerabilities.[10]

Standards and the Regulatory Environment

On January 1, 2021, the International Maritime Organization (IMO) issued Resolution.MSC.428(98), a regulation applicable to all maritime vessels. The regulation recommends ships to include cyber risk management in their safety management systems in accordance with the international safety management (ISM) code. General guidelines have been developed and provided for curating a cyber risk management plan. According to IMO, "although current guidelines are not marine-specific, vessel owners can still leverage these guidelines to identify risks, protect critical assets, and respond to and recover from cyber incidents."[11]

In March 2022, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law. CIRCIA marked a key breakthrough along the path to improving our nation's cybersecurity through cyber incident reporting requirements managed by the Cybersecurity and Infrastructure Security Agency (CISA). These reports designated CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims.[12] The USCG falls under the same reporting requirements in which they must report any cyber incidents they come across as part of the domain(s) they govern. USCG CVC WI 027 adds additional requirements to highlight cyber in safety management systems/vessel security plans on U.S. Flagged vessels by requiring incident reporting guidelines and basic cyber hygiene that would impact the seaworthiness of a vessel. The USCG highlights the aforementioned IMO guidance as well as the five functional elements of the NIST cybersecurity framework as a compliance mechanism.

In addition to existing IMO regulations and CIRCIA, guidelines were pushed out to the community by CISA known as Cross-Sector Cybersecurity Performance Goals (CPGs). These guidelines define a baseline set of cybersecurity practices that apply broadly across critical infrastructure. CPGs also provide a benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity, a combination of best practices for IT and OT owners, a prioritized set of security controls; and addresses aggregate risk to the nation.[13]

Lastly, the International Association of Classification Societies (IACS) designated two unified requirements (UR) known as UR E26 and E27 to increase cybersecurity resilience of ships. IACS as an organization is increasingly focused on reliability and functional value of safety-critical, computer-based systems on ships. UR E26 ensures secure integration of OT and IT equipment into a vessel's network through all phases, which includes initial design, construction, commissioning and operational life of the ship. This UR views the ship as an entity representing cyber

10 A. Arampatzis, *"U.S. Coast Guard Releases Cybersecurity Measures for Commercial Vessels,"* The State of Security Tripwire, Jul. 14, 2019. **https://www.tripwire.com/state-of-security/government/us-coast-guard-cybersecurity-commercial-vessels/**

11 *"IMO regulations for cyber security,"* Marine & Offshore. **https://marine-offshore.bureauveritas.com/marine/cybersecurity** [accessed Sep. 09, 2022].

12 *"Cyber incident reporting for critical infrastructure act of 2022 (CIRCIA),"* Cybersecurity and Infrastructure Security Agency CISA. [Online]. Available: **https://www.cisa.gov/circia**. [Accessed: 23-Nov-2022].

13 *"Cross-sector cybersecurity performance goals (cpgs) common baseline ..."* [Online]. Available: **https://www.cisa.gov/sites/default/files/publications/Common_Baseline_v2_Controls_List_508c.pdf?trk=public_post_comment-text**. [Accessed: 23-Nov-2022].

resilience while also covering five, key aspects: equipment identification, protection, attack detection, response, and recovery. UR E27 ensures system integrity remains secure and hardened by third-party suppliers. Under this UR, cyber resilience of on-board systems and equipment must be maintained. The interface between users and computers, along with product design and development requirements for new devices before implementation must also be considered under cyber resilience.[14]

For more information about how to defend against cyber threats, schedule a consultation with one of our industry experts: https://www.dragos.com/request-a-demo

14 *"IACS adopts New Requirements on Cyber Safety,"* IACS. [Online]. Available: **https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/**. [Accessed: 23-Nov-2022].

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.

Copyright ©2023 Dragos, Inc. | All Rights Reserved. | Last updated January, 2023