SHIP-TO-SHORE CRANES MANUFACTURED IN CHINA

Background

What are Ship-to-Shore cranes?

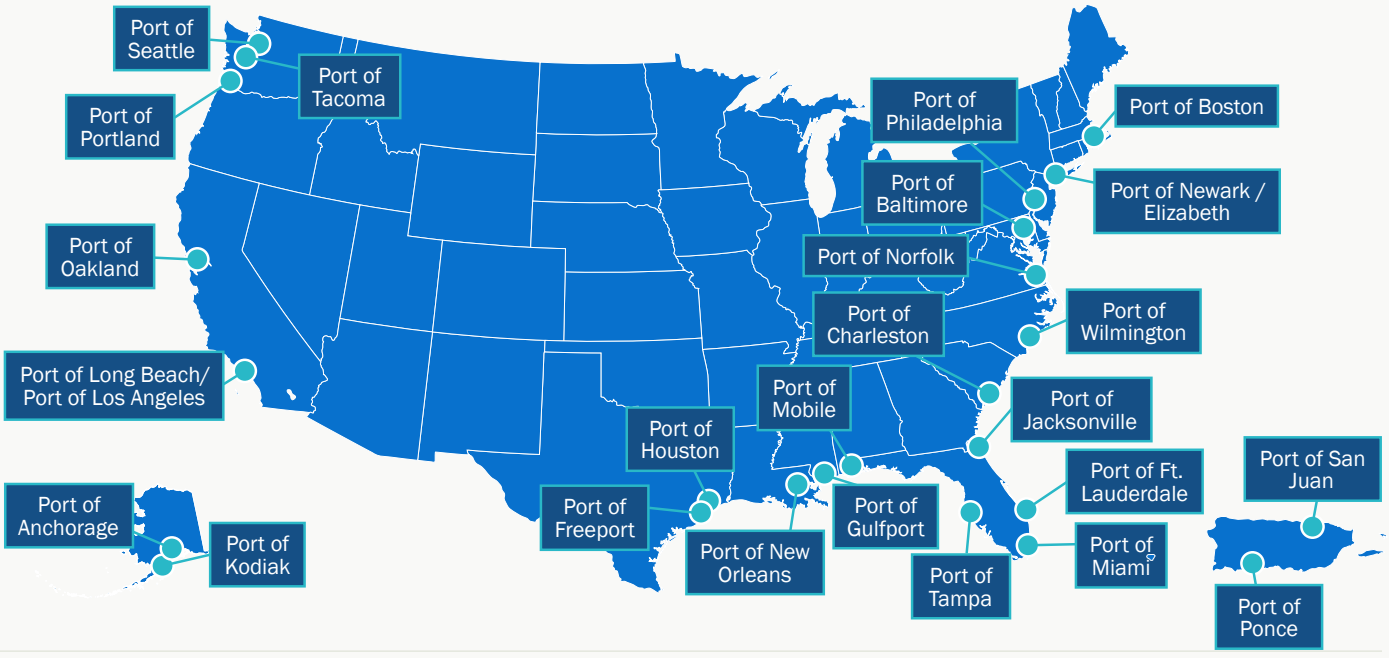
Ship-to-Shore (STS) cranes are colossal steel structures weighing nearly 2000 tons. They are self-propelled through powerful electric motors, and are built to hoist containers weighing up to 100 tons from cargo ships as high as 200 feet in the air. These machines are essential to load and unload container ships in all major ports across the world. According to UN Trade and Development (UNCTAD)[1] 70% of non-bulk cargo worldwide is transported on container ships.

ZPMC cranes being shipped to Hamburg, Germany. By GeorgHH - Self-photographed, Public Domain, https://commons.wikimedia.org/w/index.php?curid=2326283

US Reliance on Cranes Manufactured in China

The United States has been increasingly reliant on cranes manufactured in China. According to the September 12, 2024 Investigation by the House Select Committee on the Communist Chinese Party,[2] approximately 80% of STS cranes used in the United States are manufactured by Shanghai Zhenhua Heavy Industries Co., Ltd., (ZPMC), a Chinese state-owned enterprise (SOE). SOEs are controlled by the government of China and have access to reduced-cost labor and subsidized pricing for materials such as steel, allowing them to manufacture and sell cranes at non-competitive prices to capture an overwhelming global market share. Further, under China's Cybersecurity Law Article 5, critical infrastructure operators such as ZPMC must allow Chinese authorities to review source code, store their data within China, and permit comprehensive inspections by Chinese authorities. There are other China-based companies that manufacture cranes; however, ZPMC constitutes the majority of such cranes in the United States and across the globe.

The following graphic shows an approximate distribution of STS cranes manufactured in China across the United States.



[1] https://unctad.org/system/files/official-document/rmt2023ch1_en.pdf
[2] https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/Joint Homeland-China Select Port Security Report-compressed.pdf

Supply Chain Risks

ZPMC cranes contain a variety of subcomponents sourced from different countries. Frequently, these subcomponents are assembled and configured within China before being shipped to their final destination. This critical process occurring within China, combined with the requirements placed on SOEs to cooperate with the Chinese government, creates the potential for a supply chain compromise. Such a compromise could grant China-affiliated malicious cyber actors remote access to conduct espionage, manipulate, or disrupt US-based cranes.

Supply chain attacks have proven to be highly effective in recent history, affecting both hardware and software supply chains. For example, in 2020, the Russian Foreign Intelligence Service compromised the code base of the SolarWinds cybersecurity product and distributed the compromised software to nearly 18,000 customers. Using this access, they targeted a small subset of high-value customers for espionage purposes.[3]

Another example involved a several years-long scheme where hundreds of millions of dollars' worth of counterfeit Cisco network switches were procured by civilian and government entities, including for use in military aircraft. These devices were not manufactured by Cisco, but rather low-quality switches built in China and Hong Kong. In June 2023, the Justice Department obtained a guilty plea in the case from an individual who was sentenced to six years and six months in prison and ordered to pay $100 million in restitution.[4]

While not all the examples above involve China-affiliated malicious cyber actors, it is clear that critical infrastructure components that rely on supply chains involving nation-state adversaries are at increased risk of supply chain-based attacks.

[3] Source: https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

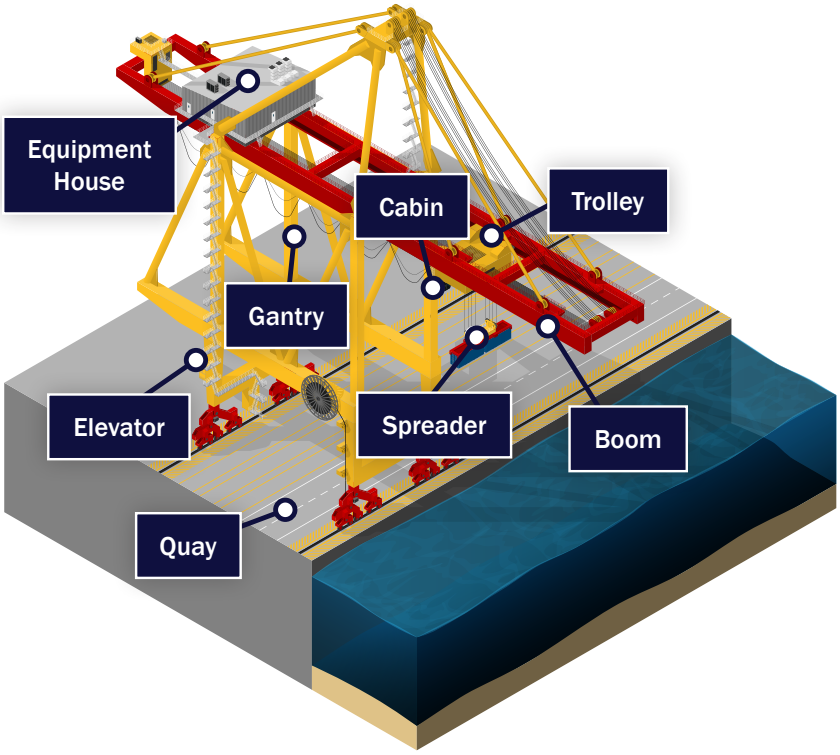
[4] Source: https://www.justice.gov/archives/opa/pr/leader-massive-scheme-traffic-fraudulent-and-counterfeit-cisco-networking-equipment

Crane Technical Overview

A modern STS crane is a complicated system of systems. Below is a review of the essential components necessary for understanding CPT cybersecurity findings and their impacts.

- **Spreader** – The device at the end of a crane's cabling that attaches to containers. These devices are named "spreaders" because they can adjust their length to match containers of different lengths.
- **Elevator** – Cranes have small elevators, similar in size to elevators at building construction sites, which allow operators to ascend/descend from the cabin without climbing the stairs.
- **Boom** – The arm that extends out from the crane over a ship. The boom is raised when a crane is not in operation and prior to a container ship's arrival to ensure collisions do not occur. The cabin travels along the boom.
- **Gantry** – The beam structure that supports the crane's trolley and hoist. The gantry provides a stable platform for the crane's lifting equipment and helps to ensure that the crane can safely and accurately lift and move heavy loads.
- **Trolley** – A mobile platform that moves along the crane's gantry, allowing the crane to position its hoist and lifting equipment over the desired location. The trolley typically carries the hoist, spreader, and other lifting equipment, and is designed to move smoothly and precisely along the gantry.
- **Cabin** – This is where the crane's human machine interfaces (HMIs) are housed. The crane operator sits inside of the cabin which trollies along the boom, over a ship, with the spreader hanging directly below the cabin. This allows the crane operator to observe the spreader as it is lowered or raised to transport a container.

- **Electric Motors** – Most cranes have four to six medium voltage industrial electric motors in the equipment room that power crane operations, with an additional large motor at separate locations to power gantry movement.
- **Equipment Room** – This is a prominent structure situated at the apex of the crane, located on the shoreside of the stationary section of the boom. It houses large reels of steel cabling that facilitate the movement of the cabin along the boom and enable the raising and lowering of the spreader. Additionally, the equipment room contains Variable Frequency Drives (VFDs) for controlling the electrical motors. The crane's Programmable Logic Controllers (PLCs) and industrial switches are also housed within this room.
- **Crane Monitoring Station (CMS)** – The number and location of CMS computers varies. Traditionally, there will be at least two, one in the cabin and one in the equipment room. Some cranes may have a CMS located in a small room at the base of the crane which technicians use to avoid scaling a crane.
- **Crane remote operator location** – Frequently there is an electrical box located at the base of the crane which contains buttons and switches to control some of the crane functions. These controls align with some of the controls available in the cabin, but not all features can be controlled from this location.
- **Quay** – Lanes where trucks drive under the crane to be loaded / unloaded.



Crane Technology

The Information Technology (IT) devices on the cranes are largely used for monitoring the thousands of Operational Technology (OT) devices that enable safe and efficient operation of a crane and include the HMIs in the crane cabin and the CMS(s). Despite being primarily used for monitoring purposes, the IT hosts are also used for reading and programming of the Programmable Logic Controllers (PLCs), frequently referred to as the "brains" of an OT system. PLCs are computer devices specifically designed to ensure extremely high reliability and availability throughout the entirety of a device's lifespan. A PLC is then loaded with a program/configuration specific to the environment it will be operating in; two identical PLCs installed in two identical cranes will have similar but different configurations to accommodate extremely detailed specifics and small variations between the two cranes. These configuration files contain a very fine level of technical detail for a crane and are therefore considered highly sensitive by all crane stakeholders.

Modern Crane Features

Modern STS cranes typically have features to greatly expedite the transfer of cargo. When older cranes unload a container from a ship, the crane operator must learn to catch the container as it lowers and approaches the pier to prevent a pendulum motion. Modern cranes have a feature called anti-sway which, when enabled, automatically controls the movement of the cabin to precisely counteract the sway. This allows even novice crane operators to match the transfer of containers per hour rate of their vastly more experienced counterparts.

Many modern cranes use Optical Character Recognition (OCR), which uses the Internet Protocol (IP)-based cameras on a crane to read information printed on the exterior of containers. This information can be fed into a Terminal Operating System (TOS) to increase port automation and improve inventory accuracy. The images from the crane's cameras are typically transmitted through a cloud connection to a third-party vendor, commonly ABB, where the images are processed, and a text response is returned to the vendor's computer on the crane. Although technology exists to locally convert information in an image into text, ABB's OCR feature in ZPMC cranes currently requires images to be transmitted to ABB for deciphering and a response transmitted back across the internet to the customer.

One of the newest features is a wireless remote control (see image on right) with which crane technicians may take full control of all crane functions, superseding all other control, including from an operator in the cabin. To accomplish this, there are four wireless antennas installed on the crane to maximize connectivity with the wireless controller. Wireless control of all crane equipment has several use cases. The simplest case is properly positioning a crane on a pier prior to a ship's arrival. Crane technicians and/or operators are instructed where to pre-position a crane relative to a ship's berth based on a load/unload plan; allowing workers to position cranes from the ground saves multiple trips up/down elevators. Crane technicians may also choose to use the wireless controller when troubleshooting crane component failures. Traditionally, a crane technician would use two-way radios to instruct a crane operator to command a particular function that is not operating properly. Providing a crane technician the ability to control every device on a crane from anywhere within the vicinity of the crane allows a single individual to troubleshoot/correct a failure. Security controls are built into the wireless controller feature; however, the Coast Guard has yet to assess the overall security of this feature.

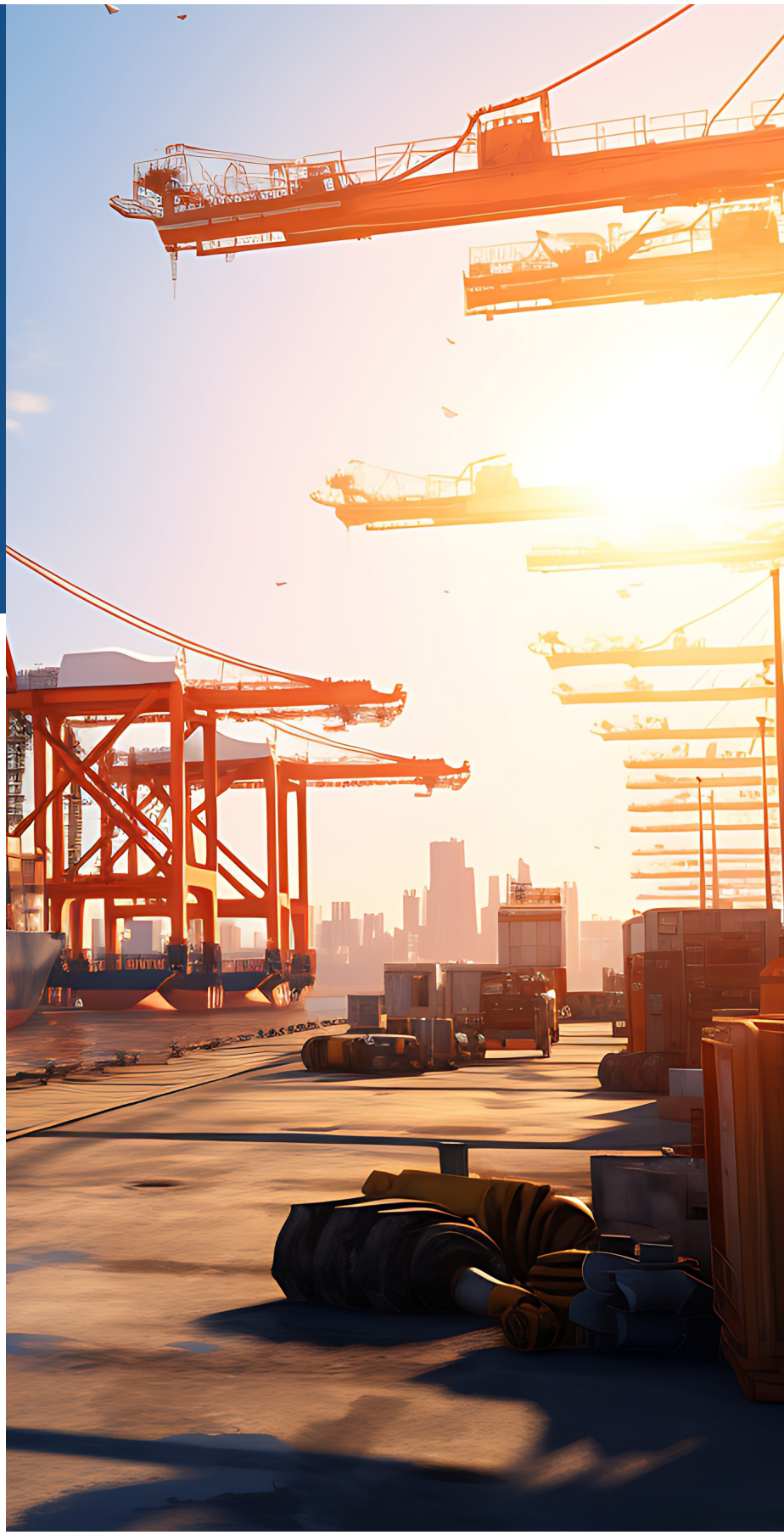
Image of an ABB manufactured crane remote controller for ZPMC STS cranes

Crane manufacturers are also offering fully autonomous STS cranes that claim to be capable of performing nearly autonomous full cargo transfers of container ships.[5] The Coast Guard is not aware of any U.S. ports which have opted for this feature.

[5] Source: https://new.abb.com/ports/solutions-for-marine-terminals/our-offerings/container-terminal-automation/sts-crane-automation

Consolidated Findings

The Coast Guard is the leading government agency assessing cybersecurity for cranes manufactured in China, conducting 11 missions and spending hundreds of days sensored on cranes. CPTs note that the depth of sensoring varies from mission to mission. For example, some missions included sensors placed within cranes to include the crane's industrial switch that directly communicates to operational technology (OT) elements via PROFINET or similar OT protocols, while other missions included sensors at the IP gateway to a network that includes multiple cranes.



Most Common Findings

Regardless of sensor depth and mission scope, all missions evaluated the overall cybersecurity posture of the crane systems, to include how isolated the cranes are from external attack vectors. With a few exceptions, our most common findings for STS crane networks are very similar to what our common findings for any typical OT system: network isolation, legacy software, and identity/access management.

In all cases, CPTs recommended mitigations to better isolate the STS cranes and reduce remote access threat vectors. IT systems associated with crane systems were frequently running Operating Systems (OSs) that have surpassed End-of-Life (EoL) and are susceptible to critical Known Exploited Vulnerabilities (KEVs). Almost universally, the password policies and use of privileged accounts did not adhere to industry standard best practices.

1. **Improper network segmentation:**
   a. Inadequate firewall/routing table configurations.
   b. Improper isolation between Virtual Local Area Networks (VLANs).
   c. Lack of proper monitoring and logging of inbound/outbound network traffic.
   d. Secure Shell (SSH) exposed to public internet.
   e. External network access of monitoring workstation.
2. **Legacy protocols:**
   a. Link-Local Multicast Name Resolution (LLMNR) – Highly susceptible to brute forcing, pass-the-hash, and remote code execution attacks. Deprecated in April 2022.
   b. Server Message Block version 1 (SMBv1) – Allows for relay attacks, remote code execution, and enumeration. Deprecated in June 2013.
   c. Virtual Network Computing (VNC), Telnet, and File Transfer Protocol (FTP) – Transmission of credentials and other data in plaintext.
3. **End of Life Operating Systems:**
   a. Windows XP Embedded SP2 EoL was January 11, 2011.
   b. Windows Server 2003 EoL was July 14, 2015.
   c. Windows 7 EoL was January 14, 2020.
   d. Cisco 2950 EoL was October 20, 2013.
4. **Weak password policy and improper account privileges:**
   a. Non-essential use of elevated access.
   b. Shared passwords and accounts, including administrator accounts.
   c. Password reuse.
   d. Weak password policy/complexity.
   e. Easily crackable/guessable passwords.
   f. Authentication bypass.
   g. Default passwords.
   h. Cleartext credentials.
5. **Unexpected services – "upgrades" not included (or realized by crane owner) in original contract**
   a. Cellular modems on crane spreaders.
   b. Security camera systems.

Remote Access & Segmentation Challenges

Ideal security would have critical systems air-gapped from the public internet; however, many use cases make this infeasible. In the case of STS cranes, some ports use the OCR feature to improve the accuracy of container tracking (which requires cloud connectivity). Unless vendors begin to offer on-premises OCR features, this potential threat vector will remain on OCR equipped STS cranes.

STS crane installations may not be air-gapped because of computer maintenance and administrative needs. The responsibility for routine maintenance and administration of the computer systems on a crane frequently falls on the crane technicians, rather than IT or cybersecurity professionals. Crane technicians are not typically trained in IT administration or cybersecurity best practices; therefore, it is typical for vendor remote assistance to be requested to address issues with crane computer equipment. Please refer to the Best Practices – Administrative Controls section for recommendations to best institute security protocols.

The third reason we have observed ad-hoc remote access implementations into crane systems is for convenience. STS cranes are installed on piers across the country that can be several miles from a central location, and the central components that make up the IT and OT systems are invariably located at the top of a crane that is the height of a 20-story building. Elevators to a crane's cabin are slow, small, and may be unavailable to a crane technician, depending on crane operations. Crane technicians are then left with one alternative: to climb the stairs. For all these reasons, after-market solutions installed by crane technicians are prevalent to provide remote access to the systems they maintain and administer. Common vulnerabilities in these after-market implementations have historically fallen into all five categories outlined in the Most Common Findings section.

Cellular Modems

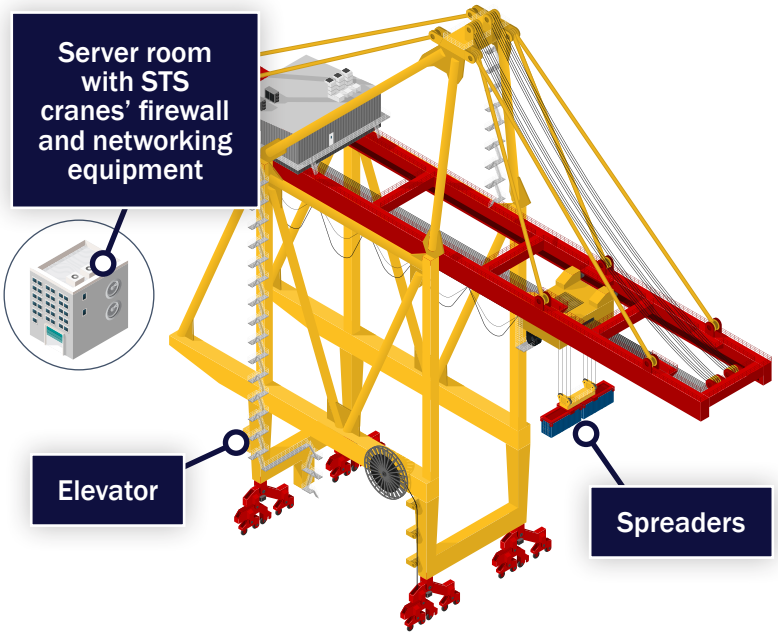
Coast Guard CPTs have discovered cellular modems installed on STS cranes manufactured in China. One cellular modem located on a crane spreader was not identified on the electrical schematics for the equipment. This finding was initially identified through a Coast Guard CPT hunt mission and publicly reported on March 12, 2024 through the investigation by the House Select Committee on the Chinese Communist Party that expands on this finding by saying that the "...devices were not part of the equipment contracts, nor could port officials determine why the components had been installed."[7]

These modems were connected to a Linux based HMI device that had full control of all technology on the spreader, completely circumventing all perimeter and internal network security and monitoring systems. A malicious actor with access via the modem could use the connection to the spreader HMI to disrupt or deny spreader use, likely superseding control over the crane operator. The cellular modems served no purpose to enable normal crane operations and were removed from the cranes, raising questions about their intended purpose.

Coast Guard CPTs also observed modems installed on crane elevators that are intended to contact emergency services in the event of elevator entrapment. There did not appear to be digital connectivity from the crane elevators to the cranes' internal systems.

A cellular modem installed on a crane's spreader

Cellular modem antenna installed on a crane's spreader system



Observed cellular modem locations on STS cranes[8]

[7] Source: https://homeland.house.gov/2024/03/12/wtas-joint-investigation-intoccp-backed-company-supplying-cranes-to-u-s-ports-reveals-shocking-findings/
[8] Source: https://homeland.house.gov/2024/03/12/wtas-joint-investigation-intoccp-backed-company-supplying-cranes-to-u-s-ports-reveals-shocking-findings/

Hypothetical Attack Paths

When these findings are viewed holistically, we can hypothesize multiple possible attack paths.

1. **Initial Access.** Initial access to an STS crane owner/operator network can be obtained by common methods demonstrated by Coast Guard CPTs, such as phishing or exposed/improperly configured administrative interfaces. A more sophisticated actor could potentially gain access through supply chain compromise or a cellular modem to directly access OT components.
2. **Lateral Movement.** Inadequate network segmentation and lack of monitoring would allow an actor to move laterally throughout the environment undetected, gaining access to the OT environment and the critical components in the cranes. An actor could easily abuse Remote Code Execution (RCE) vulnerabilities on the EoL systems on the IT portion of the crane network to maximize access. Lateral movement could also be accomplished through password reuse and/or abusing limited identity management in many cases.
3. **Privilege Escalation & Persistence.** The most likely avenue for privilege escalation is taking advantage of overprivileged accounts. A common finding for Coast Guard CPTs is a lack of application of the principle of least privilege. Additionally, it is possible to abuse privilege escalation vulnerabilities on EoL systems. An attacker may obtain persistence through traditional IT persistence mechanisms.[9] A more advanced threat actor using a supply chain compromise may naturally have persistence if abusing a maintenance channel.
4. **Data Exfiltration.** An attacker targeting OT is not typically focused on data exfiltration, however access to OCR would allow an attacker to conduct reconnaissance operations to understand port inventories and general port operations.
5. **Effects.**
   a. A low-tier actor could execute ransomware on the IT components of this infrastructure, potentially causing significant economic disruption.
   b. A more advanced actor with in-depth knowledge of the cranes may be able to craft specific OT focused attacks that target PLCs to cause physical effects that deny, degrade, disrupt, destroy, or manipulate port operations. PLC configuration files are typically stored on vulnerable IT hosts and could serve as a baseline for such an attack.

Malicious Cyber Activity (MCA)?

While we have observed many significant vulnerabilities on STS cranes manufactured in China that a threat actor could exploit to disrupt crane/port operations, Coast Guard CPTs have not observed any active malicious cyber activity (MCA) on these crane systems. There may be a few reasons for this:

1. Most CPT crane missions have been focused on identifying exploitable vulnerabilities and risks associated with crane systems/networks as opposed to a identifying active MCA.
2. We expect any MCA to take the form of living off the land techniques, using built-in features of the crane systems to appear as legitimate activity. Without implementing some of the best practices listed here, including account non-repudiation and centralized logging, it is difficult to discern normal network activity from MCA with any certainty.

All this underscores the importance of removing any potential supply chain-induced access channels (cellular modems, remote maintenance, poor network segmentation).

[9] https://attack.mitre.org/tactics/TA0003/

Best Practices for Operators of Cranes Manufactured in China

STS cranes are operational technology and should be secured in accordance with best practices for any critical OT system. Maximum use of segmentation should be employed across IT and STS crane OT systems. OT systems should be fully air-gapped if feasible. Proper administrative and technical controls must be instituted to ensure port operations continue.

The first step for any owner/operator is to conduct a thorough audit of their enterprise. Having a complete and accurate inventory of all hardware and software in their environment, an understanding of every access point into their network, and what security tools/controls are in place will contribute to ensuring they can effectively protect critical assets.

We recommend all crane owners review and implement the following administrative and technical controls to harden their infrastructure.

Administrative Controls

When these findings are viewed holistically, we can hypothesize multiple possible attack paths.

- **Scrutinize contract language** that requires remote access, installation of cellular modems, or other third-party maintenance procedures. Conduct routine physical audits to verify compliance with contractual agreements. The partners with the best crane security postures have been aggressive in challenging these access requirements through the contracting process.
- Establish policies and procedures to **restrict remote access from third-party vendors to minimum necessary**. If required, consider compensating controls to mitigate the risk this remote access introduces.
- If the cranes' systems are fully physically isolated (aka air-gapped) then **identify a single port and cable that can provide connectivity to the crane network**. Policy should dictate under what circumstances this connection can be made, by whom, and notification should be provided to cybersecurity personnel monitoring the network. When the purpose for crane connectivity has concluded, the systems should be disconnected and network isolation validated.
- **Establish and enforce user account management** policies in accordance with general best practices.[10]
- **Avoid shared accounts and enable non-repudiation**.[11] User and administrator accounts should not be shared.
- **Implement principle of least privilege**. If a user requires administrator level access, a separate admin account should be created for performing specific administrator actions. All user and admin accounts should have the least level of privilege necessary.
- **Enforce a password policy** in accordance with the National Institute of Science & Technology (NIST) Special Publication 800-63B.

[10] Source: Cybersecurity Performance Goals (https://www.cisa.gov/cybersecurity-performance-goals-cpgs)
[11] Source: non-repudiation - Glossary | CSRC (https://csrc.nist.gov/glossary/term/non_repudiation)

Technical Controls

- **Implement network segmentation.** If a physical separation or air-gap is not feasible, partners should strive to implement best practices discussed in the 2023 CTIME[12] including:
  - Multiple layers of network security should exist between a crane's IT and OT systems.
  - A firewall should be present at the boundary point of a crane network and be properly configured to implicitly deny all inbound and outbound traffic and explicitly allow only very specific traffic to transit the firewall.
  - Ensure the crane network exists in an isolated VLAN. All routing tables must ensure this VLAN and the crane IP schema is only communicable within the VLAN. If IPv6 is not in use, then it should be disabled on all hosts and explicitly blocked in all routing tables/firewalls.

- **Enable secure communications (i.e., PROFINET)** with sign and encrypt turned on for messages. Authenticating device communication makes it more difficult for a supply chain compromise to result in spoofed critical components and restricts legitimate devices to sending messages they would normally send.

- **Harden IT hosts across enterprise (both crane and non-crane networks).**
  - All IT devices should be updated to supported operating systems, if possible, with upgrades to modern hardware when hosts are no longer capable of running updated software.
  - Host-based firewalls should be enabled and configured to maximum restriction levels.

- IT hosts should be configured to send logs to a centralized location. **Centralized logging** is essential for identifying malicious or unauthorized activity.

- Implement security best practices on the **entirety of the port's network infrastructure** – beyond the crane.
  - Legacy and deprecated protocols should be disabled. Partners should have full knowledge of the remote access methods used on their networks.
  - System and security log retention should be configured to retain logs for at least the period between log review to avoid purging unreviewed logs (at least quarterly).

- **Ensure full visibility for remote access methods.** Reduce remote access options to the bare minimum necessary and implement centralized logging.
  - If not required for operation, all cellular modems and other access points which could allow potential backdoor access (if abused) should be removed from all parts of crane.
  - If crane technicians use a remote desktop capability, a secure method like Microsoft Windows Remote Desktop Protocol (RDP) should be used, requiring access by username, password, and Multi-Factor Authentication (MFA) if possible, and only accessible from within the isolated VLAN.

Third party remote desktop tools, especially those that require cloud access or use insecure authentication by default (e.g., TeamViewer, VNC, etc.) should be avoided.

For additional OT hardening recommendations please review CISA's Principles of Operational Technology Cybersecurity.[13]

[12] https://www.uscg.mil/Portals/0/Images/cyber/CTIME_2023_FINAL.pdf
[13] https://www.cisa.gov/resources-tools/resources/principles-operational-technology-cyber-security