Port Crane Cybersecurity Threats -

Irrational fear? Huge risk? What can be done about it?

Authored by Liftech Consultants...

Much has been written and discussed about ship-to-shore (STS) container handling crane cybersecurity risks since last year. Different and often conflicting opinions have been presented, usually without specific recommendation on what a crane owner or user can do about the risks being raised. In this article, Liftech will present its understanding of the concerns expressed by others, crane cybersecurity vulnerabilities, and recommendations for mitigating vulnerabilities.

Background

There are growing concerns regarding potential cybersecurity vulnerabilities in port equipment, particularly STS cranes. Many recent articles focus on concerns that the cranes could be used for illicit intelligence gathering. While Liftech has no credible knowledge of cranes being used for espionage, we agree there is some potential risk. There is also a potential risk from sabotage, such as through remote, or even local, access to the crane control systems or terminal operating systems. Most of these risks are present regardless of country of origin or manufacturer of the crane, supplier of the control components, or the control system integrator.

Container handling cranes are an important part of the increasingly complex and connected data environment at ports around the world. Their control systems vary greatly in both complexity and connectivity to port data systems and external networks. Crane cybersecurity needs and potential vulnerabilities are drastically different between types of installations, regardless of the equipment manufacturer and control system supplier. It is not possible to make general statements that accurately cover the variety of crane installations at all ports.

Liftech has long advocated for cybersecurity protection on port cranes, including local software protection and defence-in-depth systems, and isolating container handling equipment from external networks where practical to help mitigate both remote and local cyberattack risks.

We recommend careful and customised evaluation of cybersecurity vulnerabilities for all types of container handling equipment and other information systems unique to each terminal environment. Liftech has been working with our clients and industry experts to develop guidelines for best practices in assessing and addressing port equipment cybersecurity.

Overview of STS Crane Security Concerns

The American Association of Port Authorities (AAPA) has stated there have been no known security breaches of cranes at US ports. However, this does not mean there are no security risks, especially in today's society of interconnectivity. Security concerns about port cranes and their operation have been discussed for some time and include:

- *Impairment or sabotage*
- *Devices built into cranes for unmonitored or unauthorised remote communication*
- *Remote takeover and control*
- *Vulnerabilities in automation systems*
- *Intelligence gathering and espionage*
- *General cybersecurity shortcomings*

Impairment or Sabotage

Improper cybersecurity exposes crane owners and operators to potential damage to cranes, downtime, and injury, whether intentional or not. Crane control systems are complex, often with thousands of lines of logic and many hundreds of input/output parameters. Small changes to the control software can be difficult to detect and can alter crane behaviour in ways that bypass important safeguards.

On modern port cranes, many of these safeguards exist only in software without hardware analogs. While modern cranes have safety rated systems to help protect against electronic hardware malfunctions, most do not have effective means to check for unauthorised changes to the software or overrides of input/output values. Often even authorised changes can have unintended consequences that result in damage or downtime.

Devices Built into Cranes

Cellular modems have reportedly been found built into cranes when not requested or authorised by crane owners. The stated purposes of these devices were to monitor and track maintenance remotely and to assist with troubleshooting. Other suspicious devices have been alluded to; however, there are no other publicly available details of those findings.

In February 2024, the US Coast Guard (USCG) reported examining port cranes in the US for such devices, but results have not yet been made available.

Remote Takeover of Cranes

Worldwide, some cranes do have remote control capability that can be used to operate the cranes or troubleshoot issues with the manufacturer. It is extremely rare for US ports to use such remote-control operations in non-automated terminals.

However, heavily automated terminals do exist on both the East and West coasts of the US that have remote control capabilities, such as for automated stacking cranes in

container yards and for intermodal cranes. It is especially important to have strong security protections for such cranes to prevent unauthorised motion. We are unaware of any STS cranes in US ports that have remote operations outside of their facilities.

Crane Automation

According to a publication in the industry, foreign crane manufacturers "have marketed automation and remote connectivity and monitoring tools to US port operators, but these systems are not in use at US ports."

According to the AAPA, there is a deliberate policy at US ports to assess security vulnerabilities from every threat vector, and that there are dedicated "trip wires" for things that could threaten US port operations. At least four US ports are now considered "automated" for yard operations, and we expect that further automation will inevitably generate additional cybersecurity concerns.

Intelligence Gathering and Espionage

Regarding intelligence gathering, some crane systems have limited container information such as container numbers, weights, and vessel stowage positions, but such systems would not have details of container contents or cargo origin and destination. Similarly, some systems have video feeds from cameras that could be remotely accessed to gather visual information about the container terminal or nearby facilities. In nearly all cases, such data is expected to be of little value.

However, it is important that adequate security be provided to prevent the cranes from becoming an entry point to more sensitive areas of terminal information systems, which could contain more detailed information on cargo being handled or other business sensitive data.

General Cybersecurity

Unauthorised access to port equipment and terminal operating systems (TOS) have shut down major ports elsewhere in the world with reported events in Europe and Asia. The recent US Executive Order finds that "at US ports the security of the United States is endangered by persistent and increasingly sophisticated malicious cyber campaigns" targeting American ports. We agree that cybersecurity should be an important concern.

Update on US Government Actions

The US government has recently become highly involved in port security for STS cranes. The Biden-Harris Administration announced an Executive Order in February resulting in significant funding, in part for improvements to port cybersecurity and authorising the USCG to have a larger role in responding to malicious activity. The order establishes new regulatory authorities for the Department of Homeland Security and authorises USCG officials to create new rules imposing minimum cybersecurity requirements for port users. It further empowers the USCG to inspect and control vessels and shoreside activities on the basis of even "suspected cyber threat."

The United States Department of Transportation's Maritime Administration (MARAD) issued MSCI Advisory 2024-002 to alert maritime stakeholders of potential vulnerabilities to maritime port equipment, networks, operating systems, software, and infrastructure.

In May of 2024, the USCG requested certain crane owners and operators to contact their local USCG Captain of the Port to obtain copies of Maritime Security (MARSEC) Directive 105-4. The directive gives new "cyber risk management actions" to follow. The USCG also plans to publish proposed minimum guidelines on cybersecurity standards and requirements for reporting cyberattacks at US ports.

The US government is also investing $20 billion into new security technology at US ports over the next five years.

Liftech Recommendations

Port cranes are increasingly no longer just unconnected pieces of heavy equipment. It is important that crane owners and operators view cranes as sophisticated networked computer devices requiring IT safeguards and management.

We recommend port crane owners and operators, along with their procurement teams, implement the minimum actions described below as a matter of standard best cybersecurity practices and precautions regardless of STS crane origin or software control system origin.

Be Familiar with and Follow Best Information Technology (IT) Security Practices

Most businesses today have IT departments following a well-documented Information Security Management System (ISMS). These contain best practices and clear policies for enforcement of access control to systems, firewall setups to block any untrusted traffic, maintenance of backups, network isolations, and similar requirements. Cybersecurity plans should include risk assessment, risk treatment, security controls, performance measurement and tracking, and continual improvement and updating processes. Terminal operators should have IT departments adopting these practices along with established IT standards and protocols to ensure robust information security practices are in place.

For new cranes, cybersecurity issues should be addressed during procurement according to recognised standards. For used cranes, systems should be reviewed and addressed as appropriate; in many cases, new operating systems and protection systems may be needed.

Stay Alert to Government Advisories, Guidelines, and Legal Changes

Changing regulatory requirements may require policy, system, and process changes. US port crane owners and operators should check on and request MARSEC Directive 105-4 and be familiar with cyber incident definitions and reporting requirements.

Include Cyber Security in Contractual Agreements

Owners and operators of port cranes should be familiar with not just the physical specifications of the cranes, but also with all crane features and how the crane will integrate into the terminal operating systems and terminal IT plan. These features and requirements should be contained in contractual agreements for the purchase of new cranes and ongoing maintenance and operations services. The owner's IT group, crane manufacturers, and software control vendors should meet ahead of purchasing to review port crane security requirements, expectations, and deliverables.

Liftech continues to help crane purchasers with this process by providing guidelines and technical specifications for use in purchases and modifications of port cranes.

Conclusion

Port cybersecurity is receiving increased attention, particularly concerning STS cranes. Port cranes need to be integrated into port operation IT and security plans, preferably starting during procurement. The US government is increasing involvement, and we expect will be issuing evolving directives, laws, and guidance. WPD