AI, AUTOMATION AND CYBER SECURITY: RISING TO THE CHALLENGE

Automation and artificial intelligence (AI) are transforming the global marine, transportation and logistics sector at a faster rate than many had predicted. The potential to transform businesses and contribute to economic growth is undeniable, but it does not come without risk and insurance has a valuable role to play.

Automated container terminals are nothing new, they have been around since the early 1990s having first been developed in the Port of Rotterdam. These early initiatives were designed to operate on a 'closed loop' or 'point to point' basis - for example the Port of Rotterdam was an early adopter of automated unmanned rail mounted gantry cranes and unmanned automated guided vehicles for horizontal quay-yard container transfers.

What we are now witnessing is the transformation to fully automated integration of ships, port facilities, trucks, trains and warehouses in a bid to reduce costs and occupational health and safety risks and increase productivity. It's suggested that automated terminals can result in TEU throughput reaching 10,000 TEUs per acre or more, almost double traditional operations where 5,000-7,000 TEUs per acre is the norm. What's more, labour requirements that usually equate to 50% of a terminal's costs can be reduced 40%-70%.

The Victoria International Container Terminal [VICT] in Melbourne, Australia became the world's first fully automated container terminal in 2017. A McKinsey report in December 2018 highlighted that US$10 billion had been invested in port automation, and predicted that momentum would accelerate with a further US$10-15 billion investment in the next five years. By mid-2019 there were 49 fully or partially automated container terminals around the world.

Automation and AI is not just happening in container terminals. There are examples in rail freight, freight trucks and warehouse operations, not forgetting that in February 2020 we witnessed the launch of the world's first electric and fully autonomous container ship, Yara Birkeland. The 120 TEU open top container ship will reduce NOx and CO2 emissions by reducing diesel-powered truck transport by around 40,000 journeys per year. Whilst it cost US$25 million, three times that of a conventional vessel, it is forecast to cut operating costs by 90%.

What is TEU?

The twenty-foot equivalent unit (TEU) is an inexact unit of cargo capacity often used to describe the capacity of container ships and container terminals.

CYBER SECURITY ISSUES

A global AI survey published by McKinsey in December 2019 garnered responses from a broad range of industries across the world, including those involved in transportation and logistics. It cited cyber security as the most widely recognised risk. While many cyber events are minor, major incidents result in consequential commercial losses which can be in the hundreds of millions of dollars.

As the risk in these new generation technologies is significant, they are often retrofitted to legacy assets. This creates even greater technical challenges including the integration of cyber physical systems; converging multiple communication protocols necessary for seamless quality of service; and a dramatically larger network surface increasing potential vulnerability. It is these vulnerabilities that threat actors are continually looking to exploit.

Recognising the changing nature of risk and major industry organisation cyber regulations and guidelines (such as those published by the International Maritime Organisation) insurance brokers and (re)insurers are looking to expand cyber coverage to better address the 'silent' cover disconnect and uncertainties between traditional hull and machinery, cargo and marine liability policies and cyber risk.

Recent policy innovation by insurance brokers is beginning to point the way, with programs directed at the convergence of ships, ports, trucks, trains and warehouses with data addressing the needs of risk managers.

This raises the challenge of managing complex insured incidents which can occur with automated assets. Recent cyber-attacks on semi-automated shipping, port and landside transport and warehousing assets have shown that the integrated supply chain can be shut down, resulting in significant losses. These losses – in terms of both cause and effect – have no conventional precedents and require expert loss adjusting expertise able to understand the related emerging technologies. Indicating the rate at which these emerging technologies will become fully autonomous, a 2018 survey of AI researchers found the consensus view was that by 2027 the abilities of autonomous truck driving agents will surpass human drivers.

For these reasons, having the right team that understands logistics as well as current and emerging technology stacks is critical from the initial notification of loss, as when claims eventuate there is no room for 'learn as you go'.

Integra Technical Services has assembled the appropriate experts who can investigate these losses involving the integration of marine and technology; and applying the circumstances to the contract of insurance.

MEET THE AUTHORS

Andrew Gibson is a Chartered Loss Adjuster and qualified lawyer, shipbroker and arbitrator who has worked in the marine transportation and logistics sector since 1981. andrew.gibson@integratechnical.com

Gerard Ward is a cyber insurance specialist and holds a Masters Degree in Information Security and Digital Forensics. gerard.ward@integratechnica.com
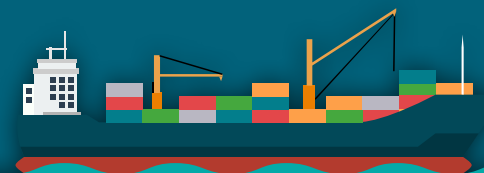
PORT AUTOMATION DEFINED

Automation in ports has five components. Whilst there are individual benefits, the full value will only be unlocked if they are integrated and coordinated:

1. Automated equipment
2. Equipment-control systems
3. Terminal control tower
4. Human–machine interactions
5. Interactions with the port community