THE NEW ERA OF CONTAINER PORTS

THE INDUSTRIAL INTERNET

Sampo Pihkala, Product Manager: Industrial Internet, Konecranes Port Cranes, Hyvinkaa, Finland

A new era is beginning in the container handling industry thanks to the rise of the Industrial Internet, the world's hyper-connectivity, and the automation of container terminal operations. New business and operating models are being revealed that offer great opportunities. With that new risks are also being revealed. Opportunities can be exploited and risks can be minimised by building a sound IT network architecture.

THE INDUSTRIAL INTERNET

The Industrial Internet (more commonly called the Internet of Things) is the next phase in the period of evolution that began with the industrial revolution and continued with the Internet/IT/digital revolution. The Internet has been profoundly changing our way of life over recent years. People are now more connected, privately and professionally, than ever before in human history. This dynamic is now moving, thanks to advances in communication technology and connectivity, to the world of machines.

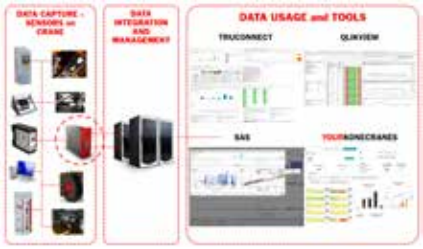
In the container handling industry, we can imagine an Industrial Internet world where every container crane is interconnected in the container terminal and throughout the logistical chain from point of shipping to point of delivery. The interconnectivity could include the goods owner, the point of the shipping container terminal, the shipping line, the receiving container terminal, the railway and trucking company, freight forwarders, and intermodal operators. In this scenario there are enormous opportunities to optimise delivery efficiency and reliability. All points in the container distribution chain are interconnected in theory – what might happen if they become interconnected in reality?

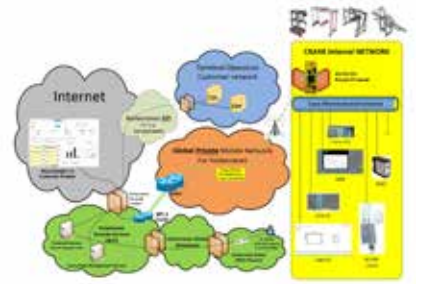
Machine service and maintenance is the area in which the Industrial Internet can bring the most immediate improvement. We are already seeing significant progress in this area. Crane manufacturers are delivering container cranes with built-in remote connectivity to crane manufacturing service centers. The cranes generate usage data on e.g. energy consumption, working hours, diagnostics sensors, safety alerts, and so on. The data is sent in real-time to the remote service center, where it is stored and analysed programmatically. The goal is to move from regularly scheduled maintenance regime to a real-time need approach, and on to a pre-emptive approach that can greatly reduce unscheduled downtime.

THE INTERNET IS THE BIGGEST THREAT

The Industrial Internet is an infrastructure of connected machines, a platform and foundation for real-time services. It contains many different levels of data, of varying degrees of importance and sensitivity, but it all needs to be transferred and handled reliably and securely. A sound IT network architecture is the key to this, and to successful TOS implementation and automated container handling.

When discussing the Industrial Internet, we need to use the word "Internet" with caution. The public Internet is the biggest cybersecurity threat imaginable to the IT network architecture that a container terminal needs to have. An Industrial Internet platform should never rely on public Internet connectivity – no matter how attractive and affordable an option it seems to be. The Industrial Internet should





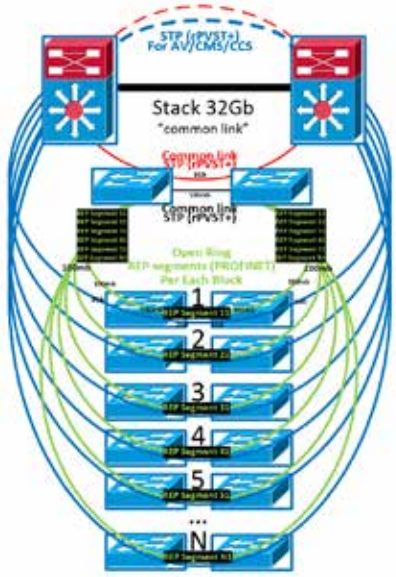


Figure 1 (top). The Konecranes Industrial Internet platform, the foundation for its real-time digital services: TRUCONNECT® is a remote service capability that is delivered as a standard feature with virtually all Konecranes lifting equipment; Figure 2 (middle). The Konecranes Industrial Internet architecture. The reliable connectivity platform offers API's for new requirements such as SOLAS/CGMV to be utilised by any TOS/ERP system; Figure 3 (left). Automated container handling system: IT network redundancy ring topology. The most time-critical safety/control bus communication has dedicated physical network interfaces to secure the data flow, maintaining crane operation even if link/hardware failure occurs

not contain even the remotest possibility that peoples' heart pacemakers, or a container terminal's STS crane control systems, could be accessed from the public Internet, regardless of the "impenetrability" of its surrounding security, encryption and access management. This is not about paranoia; it is about being uncompromising with safety.

DRAWING FROM EXPERIENCE

Konecranes has been developing its Industrial Internet capability and reach for about ten years. At the outset, it was understood that two-way communication and secure connectivity were required, which disqualified Internet-based solutions. A private APN and a cellular-based global connectivity platform was selected and implemented.

A lot of progress has been made in the last five years. Today, over 12,000 cranes are connected and online in some 80 countries. About 1,000 container cranes and lift trucks are connected and online, most of them located in places where Konecranes does not have a local service presence. This population of online lifting machines gives exciting possibilities to develop digital services. Konecranes' service business is collecting, sifting and analysing the growing body of data that is being generated.

This is just the beginning. Konecranes has an ambitious vision of the Industrial Internet. But getting this far required the complete commitment of the company's top management and the right technology decisions.

PRINCIPLES OF SOUND IT NETWORK ARCHITECTURE

The IT network architecture needs to be designed and built with top management commitment, based on clear business requirements and a long-term technology strategy with scalability. This is entirely doable. A container terminal will get far by starting with general compliance with laws and regulations, using off-the-shelf products for network build and implementation. An established Prepare/Plan/Design/Implement/Operate/Optimise approach will work well to reduce the network's 'Total Cost of Ownership', improve the agility of operations, increase access speed to applications and services, and increase the availability of required applications and services. To date, many container terminals have done only the "Implement" part.

When designing an IT network architecture for automated container handling systems (ARMG, ARTG) certain basic principles should be followed. The most time-critical safety and control data flows should be isolated from all the other data communication streams – both virtually and physically. A redundancy topology should be designed and built to meet the terminal's operational specifications in case of hardware failure. The convergence of the redundancy protocol needs to be quicker than the permitted timeout of the safety bus communication. A traditional STP is not quick enough to keep the automated operation running if topology changes occur in the IT network infrastructure.

The control and safety data traffic is very time-critical but the network also needs to handle potentially hundreds of HD-capable video streams needed for remote operation station operation in ARMG and ARTG systems. There is an obvious need for high bandwidth: the video and audio streams need to be in real-time. Carefully designed multicast routing with prioritised traffic definitions are the key elements for smooth handling of the AV data streams.

CYBER SECURITY AND CONTAINER PORTS

Security is extremely important throughout the IT network build process, affecting the IP and VLAN design, L2 and L3 ACL setups, and so on. A complete inventory of the production data flows should be taken: this is the fundamental information for implementing access control in the network. When the permitted traffic is known, defined and verified, security back-doors can be eliminated. The security of the network is only as strong as its weakest link.

Cyber-attacks have occurred in every industry in recent years. Soft targets are attacked first and most often. Understanding the security issues, and designing security into the IT network architecture at every phase of its build are the keys to bringing your container port safely into the Industrial Internet.

ABOUT THE AUTHOR

Mr. Sampo Pihkala is Product Manager, Industrial Internet, Konecranes, Port Cranes, Technology and R&D. He holds a B. Sc. degree in Telecommunications. Before joining Konecranes in 2008, he worked for 6 years in the telecommunications industry in Finland. He has been building and developing the Konecranes Industrial Internet platform and working as an IT Network Architect in automated container handling projects.

ABOUT THE ORGANISATION

Konecranes is a world-leading group of lifting businesses, serving a broad range of customers, including manufacturing and process industries, shipyards, ports and terminals. Regardless of your lifting needs, Konecranes is committed to providing you with lifting equipment and services that increase the value and effectiveness of your business.

ENQUIRIES

Konecranes Plc
P.O. Box 661 (Koneenkatu 8)
FI-05801 Hyvinkää, Finland
Tel. +358 20 427 11
Fax +358 20 427 2099
http://www.konecranes.com/