Creating a "Port of Things": moving toward IoT and automation

By solving communications network challenges, sea ports can reap the rewards of automation, as **Gary Anderson**, of Rajant Corporation, explains

Today's shifting technology landscape has monumentally changed how we communicate, how we do business and how we trade. The internet of things (IoT) has crossed the aisle from consumer applications to industrial uses to create, enhance and extend networked connectivity so industrial settings such as ports can connect to, communicate with and control all their high-value moving assets.

This level of port connectivity has the potential to not only maximise operational efficiency and productivity, but also to transform port business models by giving operators the ability to predict equipment health and performance, support autonomous applications and deliver new services. Outdated networks still limit many ports, restricting expansion and moving the goal of creating a connected "Port of Things" out of reach.

A host of network challenges

There are a number of challenges operators must overcome to create a "Port of Things", including:

- Aging and/or outgrown wired infrastructure. The majority of the world's major ports have been functioning for decades and many sea-port operations have expanded and outgrown the communications capacity of their static wired network, especially as the data volume demands for SCADA, RFID, CCTV and related applications have increased and the need for mobile communications has become essential. By adding wireless technology, whether cellular/LTE, point-to-point (PTP), or point-to-multipoint (PtMP) solutions, port operators may be able to realise incremental mobility gains, but the capabilities of such wireless solutions still fall short.
- Signal interference due to large shipping containers. As an example, in 2016, the Port of Los Angeles recorded 877,564 TEUs flowing through its port in one month. Movement of these massive containers can create interference and restrict signal range for many wireless communication systems because radio frequency (RF) waves cannot penetrate the metal containers, thus disrupting data flow. A network can be designed to minimise the effects of signal interference, but only in a static, predictable environment.
- Security. With approximately 90 per cent of the world's trade carried by the international shipping industry, ports have become high-risk targets for terrorism and other malicious breaches – on both the physical and cyber-security fronts. Many ports have implemented layered security systems, which may include fencing, sensors, access control, CCTV, radar, sonar, as well as land and waterside patrols; they may still be lacking the adequate network security needed to protect their data from advanced threats like ransomware attacks. Regardless of the type of security threat, increasing volumes of cargo and data make security more complex to assess and resolve satisfactorily. Applications such as video surveillance and real-time asset tracking can help to manage the physical security of assets across a sprawling port, but these data-intensive applications require a significant amount of bandwidth. In parallel, the network must expand its physical coverage to connect more assets moving throughout a growing port, and scale without creating weaknesses that cyber threats can target.
- Harsh coastal environments. Weather and temperature extremes are common to sea-port environments and they can wreak havoc on wired and some wireless systems.

Automation adds complications

Being able to integrate automation into standard operations is becoming more important for port managers, who are always looking to improve overall productivity and reduce operating costs as well as ensure worker safety. Using unmanned ground vehicles (UGVs), automated guided vehicle (AGV) control, autonomous equipment communications and unmanned aerial vehicles (UAVs, or drones) gives ports the opportunity to streamline operations as well as improve safety when loading and unloading massive container ships. When software runs massive cranes, or when automated systems lock and unlock containers on cargo ships, there is less room for human error. Additionally, the human workers involved can be stationed in an operations centre and away from the possibility of injury.

An obvious added benefit is that more efficiency in getting cargo on and off ships waiting in port translates into more money saved for carriers. In many ports human workers can't keep up with the amount of cargo coming in and, as container ships get bigger, this problem will be exacerbated. Ports can preserve jobs while improving safety and productivity by pairing humans and robots to complete these tasks, allowing humans to perform higher level work from offices or remote locations while robots handle the tough, dangerous manual labour.

The challenge that comes with these benefits, however, is that automation and the constant transfer of data it requires – especially when coupled with current applications' network needs– will strain many ports' networks.

Traditional wi-fi and even standard mesh networks simply aren't built to thrive in mobile, dynamic port environments. These networks use a "break-before-make" or "make-before-break" paradigm of connectivity. This means mobile nodes also only make one connection at a time, via a single frequency, so they therefore must continually break and re-establish connectivity as they move between access points.

They also assess routes based only on received signal strength indicator (RSSI), not accounting for other significant performance


leisuretime70/Shutterstock.com

factors like interference or congestion. Every break results in a temporary loss of communications. If a node is not able to connect easily to its next closest access point due to line of sight issues or bottlenecks at the master controller node, lag time can be long enough to cause substantial operational disruption.

Port operators can think outside the box, however, and move away from standard fixed and wireless networks to other types of wireless networks that can stand up to the challenging environment in a port.

Six key features of a port's wireless network

Because of both traditional and newfound challenges, port operators are exploring new wireless networks that can enhance operations and enable automation. There are several key features to look for:

1. **Integrates into current infrastructure:** most sea-port information systems have evolved in time into a complex, massive infrastructure that uses a wide variety of devices and technologies. IT managers need to be able to leverage legacy infrastructure, consolidate highly fragmented operations under one communications network and enable mobile access to mission-critical applications, so a wireless network must easily integrate into any current infrastructure a port wants or needs to keep.
2. **Scalable and reconfigurable:** containers, vehicles, workers and ships are constantly moving around a port. Standard design and equipment cannot support a port's nomadic state, so a network should have assets that allow operators to reconfigure and move radios and network infrastructure as the environment changes. For example, if sensors need to be placed on individual containers for tracking purposes, a scalable, re-deployable network makes it easy to move the containers on and offline, expanding and contracting the network as needed, while the network continues to operate with the same reliability. Shutdown should be limited to the initial installation, saving on the costs associated with downtime.
3. **Multi-frequency**: docking ships that use higher-frequency networks than the port can jam a port's network. A network that uses multiple frequencies mitigates some of that interference, so the network stays up and running. A multi-frequency network also helps alleviate signal interference due to the metal containers; when there is enough equipment sending and receiving multiple signals at once, it ensures highly reliable connectivity, even if the signal must navigate around massive metal containers stacked 10 high.
4. **Military-grade security:** because of terrorist and cyber threats to the shipping sector, an airtight network is an absolute must-have, to protect the supply chain. Networks with military-grade security and configurable per-hop, per-packet authentication are ideal for sea ports. A network should offer end-to-end encryption – meaning when encrypted information flows through the network and comes out another radio, it stays encrypted all the way through and is not decrypted until it is delivered to its final destination.
5. **Overcomes environmental issues**: while wireless networks offer the advantages of mobility without the limitations of wired infrastructure, the equipment must be battle-tested to perform reliably in the weather and temperature extremes common to sea-port environments.
6. **Supports real-time data**: to enable automation as well as standard activities, command and control centres require real-time information to direct the flow of goods, personnel and vehicles. Likewise, to protect worker safety and port security, a communications network must support video monitoring and surveillance with real-time broadband connectivity. Security officers, inspectors, employees and tenants require secure, anytime-anywhere access to data, voice and video.

Solving network challenges

More ships, more cargo, more equipment and more personnel traverse a port every day, to ensure safety, improve throughput volumes and transform their operational advantage, operators need the ability to connect to and communicate with them all. To achieve this, ports must identify a network that can bridge the gap between their current infrastructure and the integrated port they desire, where connectivity adapts, moves and grows with their ever-evolving, always-changing operating environment.

The challenges facing modern sea ports are not small, but neither are they impossible to overcome. With automation and IoT capabilities supported by a reliable mobile wireless network, operators can achieve their goal of a "Port of Things," enhancing safety, productivity and efficiency while reducing costs. *MRI*


Gary Anderson

Gary Anderson, senior vice president, business development, at Rajant Corporation