USING SECURE IOT

FOR EFFICIENT SMART PORT OPERATIONS

Maciej Kranz, Vice President, Strategic Innovations, Cisco Systems, California, US

In 2017, 1.8 billion dead weight tons of goods will be transported by ship, according to the United Nations Conference on Trade and Development. That figure has nearly doubled in the past decade, due in part to mega-ships and their massive payloads.

But ports, especially those located in dense cities, are struggling to accommodate this growth since they cannot physically expand. At the same time, cybersecurity and physical security threats are also growing.

Add to this list mandates around reducing carbon emissions, improving worker safety, and perennial issues such as labor management. It is clear that ports are facing tremendous pressures from every direction.

Is technology the answer to those challenges? No. Not on its own. However, digitization and Internet of Things (IoT) technologies are powerful enablers that forward-thinking port operators are using in order to improve efficiencies, better manage traffic, empower their workforces to increase throughput, and decrease carbon emissions while making traffic safer. One such operator is the Hamburg Port Authority (HPA), which manages Europe's third largest port.

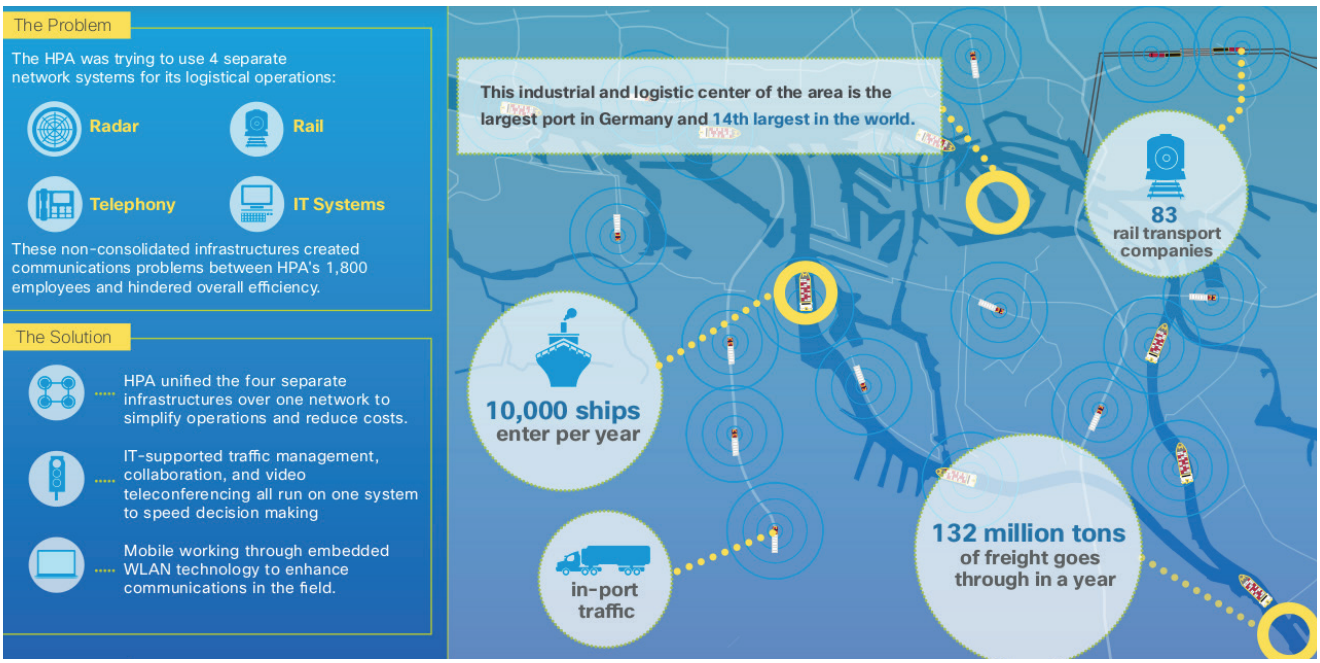
In 2009, HPA engaged Cisco to lead a major upgrade of the port's communications systems as part of a larger initiative to modernize and integrate IoT technology into the facility. It is faced with growing demand—the port processed 8.9 million TEU in 2016 but expects that figure to double by 2025. Yet, the port cannot grow beyond its current footprint of 74 square miles along the Elbe River, near downtown Hamburg, Germany. Our goal, therefore, was to create a unified communication system to help the port meet growing demand though improved traffic flow and faster turnover of freight moving into and out of the port.

A UNIFIED NETWORK

Previously, the port relied on four disparate networks, from various vendors, to manage traffic and provide communications across the facility. A stand-alone radar system communicated with and tracked ships. Another network managed train traffic. A third network supported telephone communications and a forth supported the port's IT platform. In order to integrate these systems into a single platform, we used a suite of Cisco networking products, which are designed to reduce operational expenses and simplify network deployment, operations, and management.

Our Nexus and Catalyst switches, paired with Catalyst wireless controllers and security routers, formed the hardware foundation of the network, while our Call Manager software brought voice, video, and teleconferencing capabilities to personnel through their mobile phones. For enhanced security, call manager is also paired with adaptive security appliance firewall software, which supports cryptographic algorithms and encryption standards. The firewall integrates with the Cisco Cloud Web Security solution to provide web-based threat protection.

The resultant unified communication network, dubbed HPAnet, formed the foundation not only for simpler, more fluid communications across the port and with outside clients, it also supports a network of 300 sensors, installed on roadways and bridges. The sensors provide port managers a real-time view of congestion, and this visibility plays a key role in HPA's ability to orchestrate the movement of ships, railcars and trucks



more efficiently. Sensors on other assets such as cranes and pallet loaders allow port managers to see in a simple interface which such assets are available and where they are located.

For example, through integration with ship radar, HPAnet alerts port managers as a container ship approaches the port. To accommodate it, the port will need to raise a truck or railcar bridge.

Before the IoT network was installed, knowing how to optimally route the ship for the least disturbance to rail or truck traffic involved some guessing. The sensor network now provides visibility into the amount of traffic on arteries across the port, which removes the guess work and enables the manager to select the option least disruptive to traffic.

Plus, since it no longer supports four disparate networks, the HPA has halved the number of network management devices it must maintain, from 400 to 200. Thanks to server virtualization, the port also decreased the number of onsite servers from 242 to 48.

On an average day, trucks make 40,000 trips across the port. By improving the orchestration of those vehicles throughout the port, the network also helps reducing engine idling, thereby cutting carbon emissions. Sensor data will also give HPA insights into long-term usage patterns related to roads, bridges and other infrastructure elements. By using this data, HPA can schedule and conduct preventative maintenance on the port, aimed at avoiding any significant use-related damage that could harm port operations.

Over the next five years, HPA's operational costs are expected to decline by 70%.

SECURITY

Without a doubt, security remains the greatest barrier to IoT adoption across industries. Security requirements for IoT networks are different than they are for traditional IT environments because they are composed of a wide range of different types of devices, from simple sensors to actuators to advanced autonomous vehicles, which support a long list of different business functions.

When networks operate in silos, it is impossible to achieve the types of efficiencies that HPAnet has provided the Port of Hamburg. But IoT networks also introduce new types of cybersecurity threats that require organizations to bolster and continually update their data security infrastructure. And in many cases, IoT deployments operate in mission-critical situations, where a security breach could have wide-ranging negative impacts or even, in the case of a container port, force it to temporarily halt operations.

Cisco collaborated with a host of technology vendors to deploy networks such as HPAnet, but these vendors are highly vetted for their adherence to cybersecurity best practices. Plus, in the wake of a 2016 Distributed Denial of Service (DDoS) attack that targeted IoT devices, most hardware manufacturers are taking security more seriously.

To create HPAnet, we partnered with IoT solutions provider Worldsensing to source sensors, big data services provider AGT International which provided analytics software, intelligent lighting provider Philips, and telecommunications provider T-Systems. SAP and T-Systems provided HPA with another key element of its modernization effort. Called Smartport Logistics, it uses T-Systems' telematics services to aggregate traffic data around the port and uses this to create notices to drivers, based on their current location, regarding port traffic. SAP powers the app through its HANA cloud-based services. The app might alert a given truck that the shipment it is arriving to collect has been delayed. Or it could direct the truck to the precise location of the shipment in the port for faster transfer.

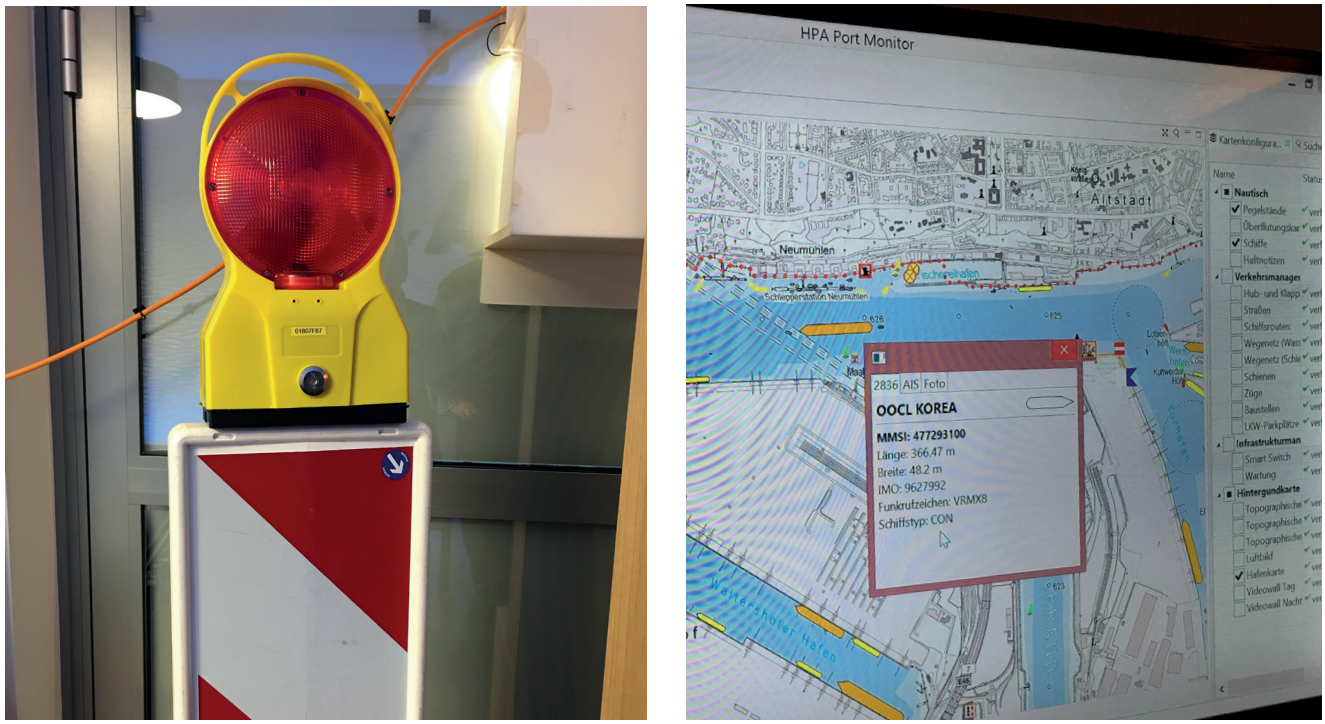
DISRUPTING DISRUPTIONS

Seaport managers are used to dealing with unpredictable and sometimes unrelenting disruptions, whether they are related to weather, mechanical problems, labor issues, or myriad other variables. Integrating IoT technology is also disruptive. While it hasn't changed the port's business model, it has changed the means by which port employees communicate with each other and with customers, requiring staff training and patience as personnel adjust to the unified platform.

But over time, the benefits are clear. Not only does HPA staff now have visibility into the movement of vehicles and the status of shipments in a single interface, they can access this information across the entire port. Plus, because of the port-wide wireless network and mobile technology, they no longer have to get to a central location to communicate with a colleague or join a conference call. Instead, they can be where they are most needed, and the network, in a sense, comes to them.

TRANSPARENT, AUTOMATED PORTS

Cisco analysis finds that IoT technologies represent a US$1.9 trillion market for the logistics and supply chain market, but there is an even larger opportunity when one includes a range of quickly-maturing technologies that ports are starting to test. Robotics, which rely heavily on IoT



HPAnet sensors (left) and solutions (right) provide port managers with a real-time view of congestion and long-term usage patterns

technologies, are a natural evolution of technology for container seaports, which are already adopting increasingly mechanized systems to move and manage goods for more than a century. Market research firm Gartner believes that by 2020, 10% of large enterprises in supply-chain-dependent industries will hire a chief robotics officer.

Several elements make ports logical places to deploy robotics systems. For example, their controlled environments and ability to support sophisticated sensor networks and instrumented infrastructure makes them suitable for autonomous vehicles. Ports with ready AV infrastructures will find be among the first to receive autonomous long-haul trucks.

Also, blockchain technology will allow ports to share data across the supply chain in a transparent process and without relying on a central authority.

Blockchain is a digital ledger system that can verify or validate information through a series of transactions, across a shared record or database, using cryptographic keys that only authorized parties can access. The technology first gained attention for is use in digital currencies, but ports are beginning to investigate blockchains for a wide range of applications.

As with HPAnet, all of these technologies can support more efficient port operations, greater visibility across ports as well as across supply chains, and reduced energy consumption. The Port of Hamburg, like so many ports located in densely populated parts of the world, has no choice but to innovate by exploring the ways in which advanced technology can enable it to do more within its current footprint. HPA's success with HPAnet serves as a model for what is possible for a port willing to embrace change and adopt new technology.

ABOUT THE AUTHOR

Maciej Kranz has 30 years of networking experience leading to his current position as Vice President, Corporate Strategic Innovation Group, Cisco Systems. He heads the group focused on incubating new businesses, accelerating internal innovation, and driving co-innovation with customers and partners through a global network of Cisco Innovation Centers. Prior to this role, Kranz was General Manager of the Connected Industries Group at Cisco, a business unit focused on the Internet of Things (IoT). He built a $250 million business from the ground up in 18 months and relentlessly evangelized the IoT opportunity across Cisco and the market, making IoT one of Cisco's major priorities. Previously, Kranz led efforts across Cisco to define, prioritize, and deliver borderless network architecture and roadmaps. He also drove business and product strategy for the wireless and mobility business and led product management for the stackable Ethernet switching business unit through its expansion from $400 million to $6 billion in revenues.Before coming to Cisco, Kranz held various management positions at 3Com Corporation, where he drove a $1 billion Ethernet network interface cards (NICs) product line. He began his professional career at IBM Corporation.

In his *New York Times* bestselling book, *Building the Internet of Things*, Kranz offers practical advice to business decisionmakers on how and why to implement IoT today. He has formed a thought-leadership forum and newsletter to exchange industry insights on IoT developments. Kranz is also a faculty member of Singularity University, focusing on IoT and corporate innovations.

ABOUT THE ORGANIZATION

Cisco is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today. Cisco designs and sells a broad range of technologies that have been powering the Internet. Across networking, security, collaboration, and the cloud, our evolving intent-based technologies are constantly learning and adapting to provide customers with a highly secure, intelligent platform for their digital business.

ENQUIRIES

Websites: newsroom.cisco.com
www.maciejkranz.com