The bridge to possible

Terminal Operations Digitization and Security

New operational efficiencies in container handling and terminal yards

New operational efficiencies in container handling and terminal yards

Terminal and port operators are constantly looking for the best solutions to improve productivity and increase throughput, while at the same time reducing costs and enhancing safety and security. To achieve the business objectives presented in Figure 1, terminal operators and machine builders take advantage of increasingly advanced technology to automate their terminal operations; remotely control machines such as quay cranes/Ship-To-Shore (STS) cranes, Rubber-Tired Gantry (RTG) cranes, and/or Automated Straddle Carriers (AutoSC) in real time; gain visibility into high-value assets; increase asset utilization, berth availability, and occupancy patterns; reduce network and application downtime; optimize maintenance; and reduce operational costs. Port operators can leverage new Internet of Things (IoT) technology to provide better environmental monitoring such as tidal and weather conditions, salinity, and water levels so that ships' arrival times can be better planned with real-time information on berth availability. In addition, truck and rail turn time can be improved through real-time traffic monitoring and integration with Terminal Operating Systems (TOS). The workforce productivity at both ports and terminals can be improved with extended Wi-Fi access and more effective collaboration tools. Industrial networks at ports and terminals require better-integrated Operational Technology (OT) and Information Technology (IT) security and safety to enable greater visibility into the system and assets, protect the network from cyberattacks, and provide a faster response when incidents and issues happen. All of these capabilities are key to the success of the port and terminal digitization process, which is dependent on a network infrastructure that is secure, scalable, reliable, and resilient. Cisco's networking products and solutions provide the necessary foundation for such infrastructure. Cisco's industrial IoT products are proven to meet the unique requirements of operating a port and/or terminal.

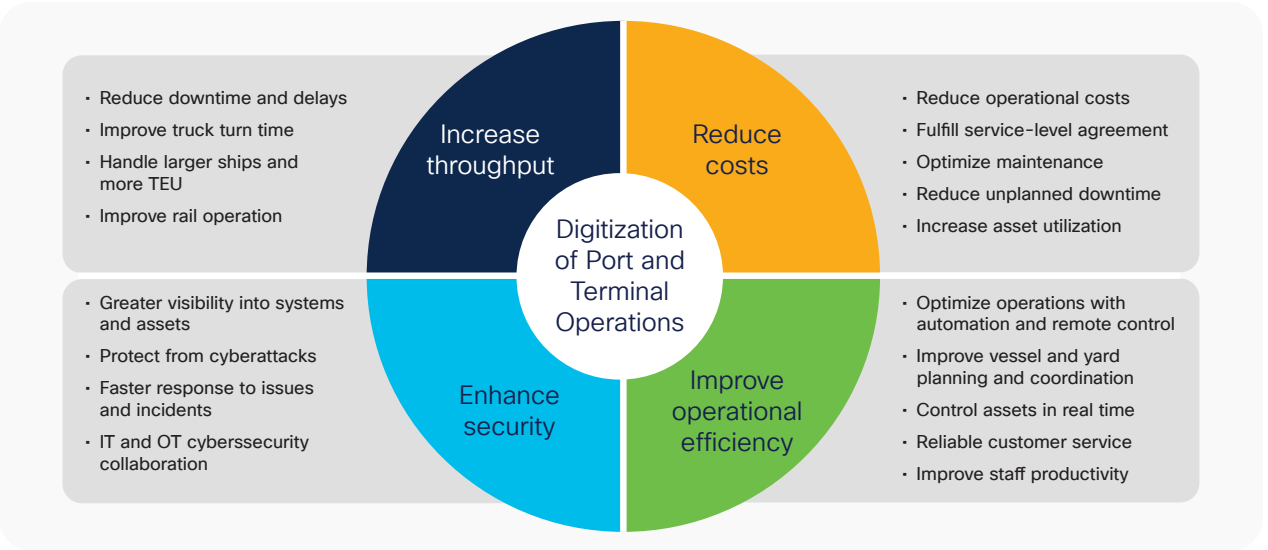
The bridge to possible

Benefits

A network foundation for improving the safety, efficiency, and service levels of your terminal and port operations

- Secured, scalable, and reliable critical infrastructure
- High bandwidth, low latency, and seamless handoff
- Enhanced asset visibility
- Support for edge intelligence to act on data faster and closer to its source
- Simplified device onboarding and centralized policy control

Figure 1. Business objectives in port and terminal operations



Network challenges

When port and terminal operators deploy a network foundation for their operations, they typically have to address a range of challenges. These include a network infrastructure that needs to adapt to challenging environments, a complex infrastructure that needs to support both legacy and state-of-the-art systems, a solution that must provide network and data security and improve worker safety and physical security, and a resilient and reliable network infrastructure that can support growing digitization.

Challenging environment

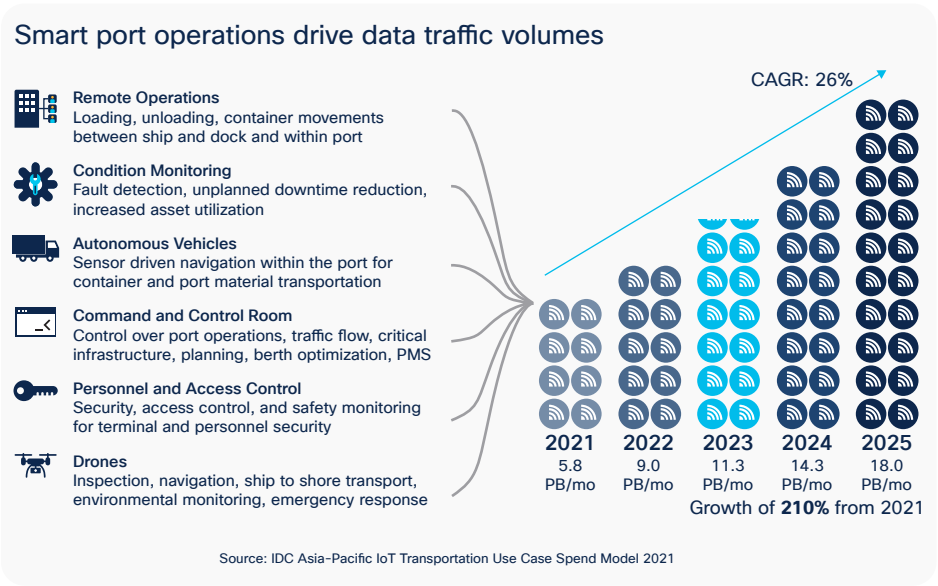
Ports and terminals operate under harsh coastal weather with extreme conditions. This requires the networking equipment deployed to sustain wide temperature ranges, shock and vibration caused by the operation of big machines and the transport of heavy containers, and the presence of water and dust.

The physical environment of a port and terminal is dynamic and unpredictable, due to the enormous volume of constantly moving containers, cranes, land vehicles, trains, and giant marine ships such as cargo vessels that hold 10,000 to 20,000 Twenty-foot-Equivalent Unit (TEU) containers. Such challenging environments can introduce a great amount of interference and pose restrictions on the range of the wireless communication required to support the port's and terminal's operations.

Growing digitization

Through digitization and automation, port and terminal operators increase their competitiveness and enhance operational efficiency. Digitization helps operators streamline the business process, create new business opportunities, and make the right business decisions, and it is achieved through access to relevant and reliable data. Digitization of smart ports drives significant increases in data traffic volume. According to a recent estimates for Asia-Pacific IoT Transportation use case spend, based on the IDC IoT Access and Traffic Model (2021), IDC expects that smart port operations will drive data traffic volume growth from 5.8 petabytes per month in 2021 to 18.0 petabytes per month in 2025, with a Compound Annual Growth Rate (CAGR) of 26%. These data points are collected from sources such as sensors, video cameras, control systems, and voice and data applications that support use cases such as terminal operating systems, remote operations, autonomous vehicles, and remote asset monitoring.

Figure 2. Smart port operations drive data traffic volumes



Source: IDC Asia-Pacific IoT Transportation Use Case Spend Model 2021

Complex infrastructure

Port and terminal operations deal with massive machines such as quay cranes/STS cranes, RTG cranes, rail-mounted gantry cranes, reach stackers, and AutoSCs. These are complex and have a much longer life span than other types of equipment. This can mean that there is an aging infrastructure that needs support and maintenance. Different security and operational needs lead to multiple segregated networks, adding complexity and incurring high maintenance costs.

Digitization demands a next-generation architecture that is highly resilient and scalable. This architecture needs to support different applications with diverse communication requirements. Terminal operations and automation require multiple access technologies for success. The choice of technologies is largely dependent on the types of devices to be connected, the application requirements in terms of latency, roaming, and throughput, the deployment scenario, and the implication of CapEx and OpEx.

Cybersecurity

As port and terminal operations move toward greater digitization, more machines, people, and applications are networked together, more equipment and applications are brought online to enable the automation, and more attack surfaces and vulnerabilities are created. According to a study in 2020 (https://www.marineinsight.com/shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years/#), cyberattacks on the maritime industry's OT systems have increased by 900% over the last three years. A simple malicious attack can bring down the entire network, create an unprecedented backlog for the supply chain, disrupt the network infrastructure and terminal operations for weeks, and cause great financial loss to the port and terminal operators. For example, in June 2017, ransomware called NotPetya hit the Maersk shipping company, locking down access to the system that it uses to operate its shipping terminals worldwide. The attack cost the company nearly $300 million and took two weeks to fix. (https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html)

The bridge to possible

Why Cisco?

Cisco provides a comprehensive portfolio including routing, switching, wireless, collaboration, data center, IoT, and security. Whatever a customer's goals might be, Cisco is able to offer a trusted end-to-end solution that combines our portfolio with technologies from a robust ecosystem of partners. Cisco's Intent-Based Networking (IBN) technology transforms hardware-centric, manually configured networks into controller-led networks that capture network managers' business intent and use automation to translate intent into policies that are applied consistently across the network and monitored comprehensively to help ensure proper ongoing operation at scale. Some of the world's largest and most vital networks have embraced Cisco® IBN because it brings new levels of network performance, security, and reliability to the network at larger scale, and with less effort.

Cisco's Connected Ports and Terminals solution combines those industry-leading IBN capabilities with the specific and distinct needs of the IoT networks used for port and terminal operations. The Cisco IoT networking and security portfolio addresses the unique requirements that are needed in an industrial outdoor environment. In addition, the Industrial Automation Cisco Validated Design (CVD) is the blueprint to implement a resilient and secure network infrastructure that supports Industrial Automation and Control Systems (IACS). Cisco's Connected Ports and Terminals solution leverages this well-designed and tested solution to enable digitization and automation, improving business operation outcomes. More detailed information about the Industrial Automation CVD can be found in Networking and Security in Industrial Automation Environments Design and Implementation Guide.

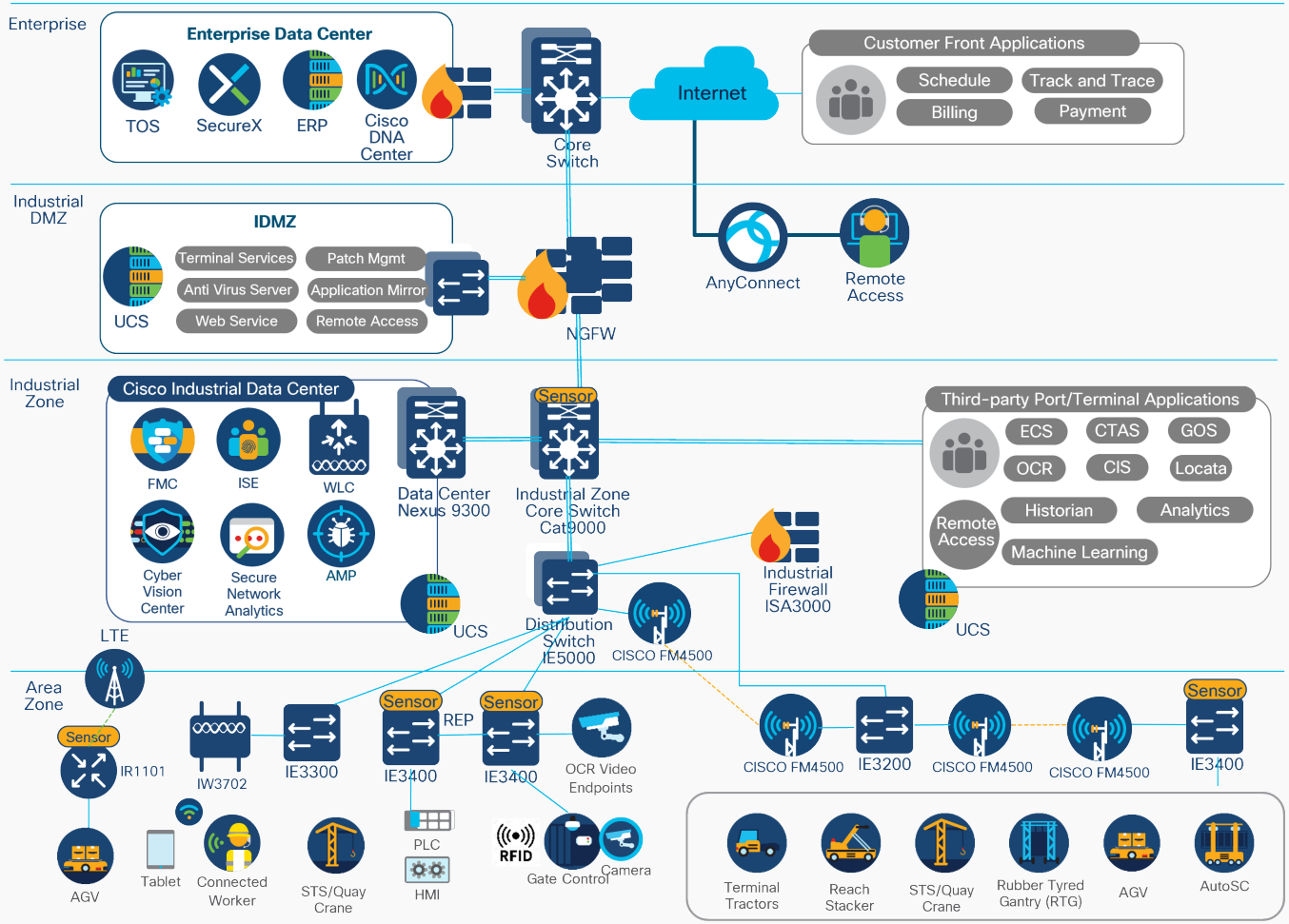
Network security should be included from day one and not as an afterthought. An effective cybersecurity strategy requires a comprehensive, systematic, coordinated approach to protect against a broad and continuously evolving set of threats. Cisco offers an ever-expanding, industry-leading portfolio of cybersecurity products to provide comprehensive protection for IT and operations networks. Cisco's portfolio includes Cisco Cyber Vision, provides visibility into industrial devices and data traffic flows; Secure Network Analytics (formerly Stealthwatch), which can monitor data flows and detect traffic anomalies that can be used to enhance network segmentation policies; a policy platform called Cisco Identity Services Engine (ISE), which helps define and manage user profiles and access policies at scale; Cisco Malware Defense (formerly Advanced Malware Protection) to provide up-to-date monitoring and detection of malware threats; Cisco Umbrella® to prevent passengers or workers from accessing malicious network domains; and Cisco DNA Center and SD-Access to automate and simplify security policy implementation and assurance across all network devices. Additionally, Cisco SecureX™ provides a consolidated view for simplified management of the overall security approach.

Cisco has an established and growing ecosystem of technology and solution partners who can help design, implement, and operate end-to-end solutions that build on Cisco's Connected Ports and Terminals architecture and fulfill the business needs of port and terminal operators. Building port and terminal solutions on a Cisco Validated Design helps ensure that Cisco has tested and validated the architecture, which greatly reduces implementation risk and provides extra peace of mind for customers and solution delivery partners alike. Cisco partners include machine and software manufacturers, software solution providers, channel partners, and consultants. Ecosystem partners are vital in the successful deployment and operation of the Connected Ports and Terminals solution.

Connected Ports and Terminals reference architecture

The Cisco Connected Ports and Terminals reference architecture, shown in Figure 3, follows the blueprint of ISA-95 and is based on the Cisco reference architecture for IACS. This reference architecture is composed of four major functional modules that include cell/area zone, industrial zone, Industrial Demilitarized Zone (IDMZ), and enterprise. The following sections explain the functions and capabilities of each module in detail.

Figure 3. Connected Ports and Terminals reference architecture



Cell/area zone

The cell/area zone is the access layer located at the edge of the industrial network that provides either wired or wireless connectivity to industrial devices. These devices include not only industrial devices at Levels 0 through 2 in the ISA-95 model, such as actuators, controllers, and sensors that communicates via traditional control protocols such as PROFINET, but also devices such as Wi-Fi or Bluetooth-enabled handheld devices, voice communication radios, access points, cameras, vehicle telemetry sensors, and weather sensors that leverage traditional network protocols such as IP or serial links for communications.

The cell/area zone module delivers the following very important characteristics:

- Industrial characteristics: The platform choices are heavily influenced by the environmental conditions at the port and terminal. The Cisco IoT product portfolio delivers hardware that is hardened with a small form factor, can sustain an extended temperature range and shock and vibration, and provides protection against water and dust. Industrial control protocols such as PROFINET and EtherNet/IP are supported natively on the Cisco Catalyst® Industrial Ethernet (IE) switches, presented in Figure 4.

Figure 4. Cisco Catalyst Rugged Series Industrial Ethernet switches

- Mutiple access technologies: Depending on the application requirements, deployment scenario, and existing network infrastructure, multiple access technologies, including both wired and wireless, are required for the success of the operation. The Cisco IoT wireless portfolio includes LTE and 5G, suitable for wide mobility and high throughput; Wi-Fi 6 and Cisco Ultra-Reliable Wireless Backhaul (formerly Fluidmesh), depicted in Figure 5, for mobility and fixed infrastructure with high throughput, low latency, and ultra-reliable, resilient mesh; and LoRaWAN for massive scale and broad coverage. The Cisco IoT wired product line offers Ethernet connections over copper or fiber, as well as serial and DSL connections from internet service providers.

Figure 5. Cisco Ultra-Reliable Wireless Backhaul

- Highly resilient network: An IACS network must be highly resilient, with latency, reliability, scalability, and performance taken into consideration in the network design. For industrial control traffic, packet latency and jitter have a huge impact on the underlying industrial process. Network availability and convergence time are also key metrics for critical IACS communication. The Cisco Resilient Ethernet Protocol (REP) available on IE switches is typically suitable for IACS applications that can tolerate up to a 100-ms network convergence recovery time. When zero-second convergence time is required, the Parallel Redundancy Protocol (PRP) can be also leveraged and is supported on the Cisco Catalyst IE3400, IE4000, and IE5000 Series.

- Security: Security in the cell/area zone needs to be viewed as a component of an overall end-to-end security architecture within the port and terminal. It is critical that security capabilities span the breadth of the port and terminal in order to be effective, yet this may pose a challenge when the IT and OT are not well integrated and are managed by different groups. The fundamental requirements are visibility into current network devices and industrial assets, grouping and separation of network assets and applications through segmentation, anomaly detection and mitigation, and network hardening on the management plane, control plane, and data plane. All these can be achieved through Cisco Cyber Vision, Cisco TrustSec®, and Cisco Secure Network Analytics, and its integration with Cisco ISE.

Industrial zone

The industrial zone in this architecture refers to a zone that all industrial and mission-critical port and terminal applications are confined to. It is composed of Cisco industrial data center and third-party port and terminal application services. Due to the sensitive nature of the assets and data flow in the industrial zone, a pair of redundant firewalls located in the industrial DMZ blocks all the traffic in and out of the industrial zone and allows only traffic that is explicitly defined. This may cause a challenge when communication patterns are not well understood, particularly in cases where communication between the industrial zone and the upper levels is required. That is why application visibility is so important and why technologies such as Cyber Vision and Secure Network Analytics can be very beneficial.

The Cisco industrial data center follows the best practices from Cisco data center design. The platform choice of the Cisco Catalyst 9000 family for the industrial zone core switch and the Cisco Nexus® 9300 for the data center switch enables Cisco intent-based networking with Cisco DNA Center management and data center solutions such as Cisco Application Centric Infrastructure (Cisco ACI®). To minimize the need for communication between Level 3 (the industrial zone in the Industrial Automation reference architecture) and upper levels, key infrastructure services should be located within the industrial data center. These include dedicated identity services such as Active Directory (AD) and ISE, dedicated wireless controllers to manage wireless connections within the industrial zone, and Cyber Vision and Secure Network Analytics to gain visibility into the asset and application flows.

Third-party applications that are responsible for port and terminal operations are located in the server farms at the industrial data center. These applications include equipment control systems, crane interface systems, Optical Character Recognition (OCR) servers, container terminal automation systems, and gate operating systems. By having these essential services and applications located in the industrial zone, the operation is less likely to be disrupted in the event that external connectivity via the IDMZ is lost or the upper-level network is brought down by a cyberattack. This does not mean the air-gapped industrial zone will be immune from cyberattack, and the Cisco Secure Firewall ISA3000, illustrated in Figure 6, located in this zone is designed to segment the traffic for different OT assets and protect them from potential threats.

Figure 6. Cisco Secure Firewall ISA3000

IDMZ

The IDMZ resides in a level between the industrial and enterprise zones, commonly referred as Level 3.5 in the ISA-95 reference architecture. An IDMZ environment consists of numerous infrastructure devices, including firewalls, VPN servers, IACS application mirrors, remote gateway services and reverse proxy servers, in addition to network infrastructure devices such as routers, switches, and virtualized services.

IDMZ firewalls apply defense-in-depth principles at the industrial perimeter by blocking all traffic into and out of the industrial zone and allowing only traffic that is explicitly defined. Accordingly, communication patterns must be well understood, since some use cases require communication between Level 3 and upper levels, with Terminal Operating Systems (TOS) being a prime example of this scenario, as the application server is normally located in the enterprise zone. The traffic between the devices in the industrial zone and TOS needs to be explicitly permitted in the IDMZ.

It is also recommended that IDMZ systems be granularly isolated in individual VLANs as much as practically possible. This increases the firewall's visibility into individual server data streams to identify potentially compromised hosts. Redundant IDMZ firewalls and distribution/aggregation switches are required so that specific systems, such as remote desktop gateways and OS patch servers, can be securely hosted in the IDMZ. The IDMZ is designed in such way that all IACS traffic from either side of the IDMZ should be terminated in the IDMZ. No IACS traffic should directly traverse the IDMZ. If traversal is required, it should go through gateway or proxy functions in the IDMZ. Non-IACS traffic can implement IDMZ traversal through whitelisting.

Enterprise

The enterprise zone is isolated from the industrial zone via the IDMZ. This zone is usually a traditional enterprise data center where server-based enterprise systems are deployed safely and efficiently in a physically secure and air-conditioned environment and where data center best practices are strictly enforced. Corporate remote access solutions should be implemented so that employees can access the enterprise zone in a secure and controlled fashion. Depending on the nature of the customer's applications, they can be hosted either in the enterprise data center, private cloud, or public cloud. The enterprise data center is also shielded from the internet by a pair of redundant firewalls.

The bridge to possible

Cisco Connected Ports and Terminals use case themes

The Cisco Connected Ports and Terminals reference architecture is designed to support various use cases in port and terminal operations. As listed in Table 1, those use cases are categorized into three major themes: terminal automation, cyber and physical security, and port operations and monitoring.

Table 1. Cisco Connected Ports and Terminals use cases

Use case theme	Use cases	Business outcomes
Terminal automation	▪ Terminal Operating System (TOS): asset management, asset scheduling, integration with OCR, enterprise Wi-Fi ▪ Remote operations for STS and RTG cranes ▪ Automated RTG (ARTG) and automated rail-mounted gantry (ARMG) cranes ▪ Autonomous vehicles (automated guided vehicles [AGV] and AutoSC) ▪ Vehicle telemetry data	▪ Improved planning due to a holistic view into berth availability and occupancy patterns ▪ Ability for ships to plan their arrival at the terminal with real-time information on berth availability ▪ Increased operational efficiency ▪ Improved ship turnaround time and terminal throughput ▪ Improved application and equipment uptime ▪ Reduced operation and maintenance costs
Cyber and physical security	▪ Cybersecurity ▪ Physical security: Surveillance and video analytics, access control, worker health and safety, collision avoidance, regulatory requirements best practices	▪ Improved digital safety of port and terminal infrastructure ▪ Visibility into operational assets ▪ Common view of incidents across agencies ▪ Encourages collaboration between port agencies
Port operations and monitoring	▪ Environmental monitoring: Tidal conditions, weather conditions, water levels, current, and salinity ▪ Traffic monitoring and management: Vehicle and rail traffic monitoring, ship traffic monitoring ▪ Workforce communication and collaboration	▪ Improved decision-making by harbor master and pilots ▪ Optimized ship schedules, such as berthing, loading/unloading, and departure times ▪ Optimized gate control to reduce time spent by trucks in entry and exit procedures ▪ Reduced operations costs ▪ Additional revenue through demand-based parking pricing and more accurate ticketing of parking violations

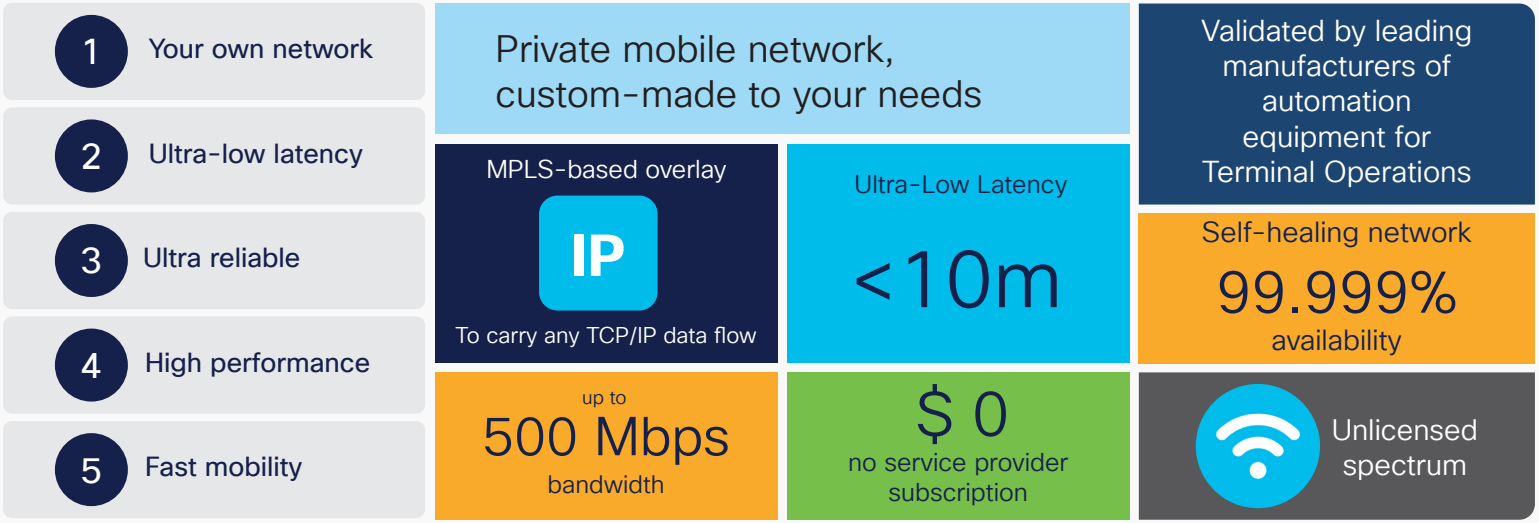
This solution brief focuses on terminal automation, which includes major use cases such as connecting the TOS with OCR integration and remote operations for STS and RTG cranes and autonomous vehicles such as AGVs and AutoSCs. Table 2 lists some of the typical key network requirements for these use cases.

Table 2. Terminal automation network requirements

Description	Network requirements
Terminal Operating System (TOS) Terminal tractors, reach stackers, RTG cranes, and similar applications	450 Kbps to 1 Mbps Variable traffic Good coverage Up to 1-second latency
Optical Character Recognition (OCR) TOS server integrated into OCR system	15 Mbps to 20 Mbps Constant traffic 100% coverage 10- to 50-ms latency
Autonomous and teleremote RTG cranes	30 Mbps for AutoSC 60 Mbps for RTG cranes Constant PLC traffic Constant video traffic 0-ms handover Coverage across the working area 50-ms latency
Autonomous horizontal transport (automation for programmable logic controller [PLC] applications)	1 Mbps for AutoSC/AGV Constant PLC traffic 0-ms handover Overlapping coverage at the working area 50-ms latency

Terminal automation depends on flexible and reliable wireless technology that can provide full coverage, extremely low latency, zero packet loss, fast handoff, high bandwidth, and easy installation, provisioning, and management. Cisco Ultra-Reliable Wireless Backhaul technology is designed with such requirements in mind and delivers unique capabilities, as outlined in Figure 7, to overcome those challenges and exceed those stringent requirements.

Figure 7. Cisco Ultra-Reliable Wireless Backhaul capabilities

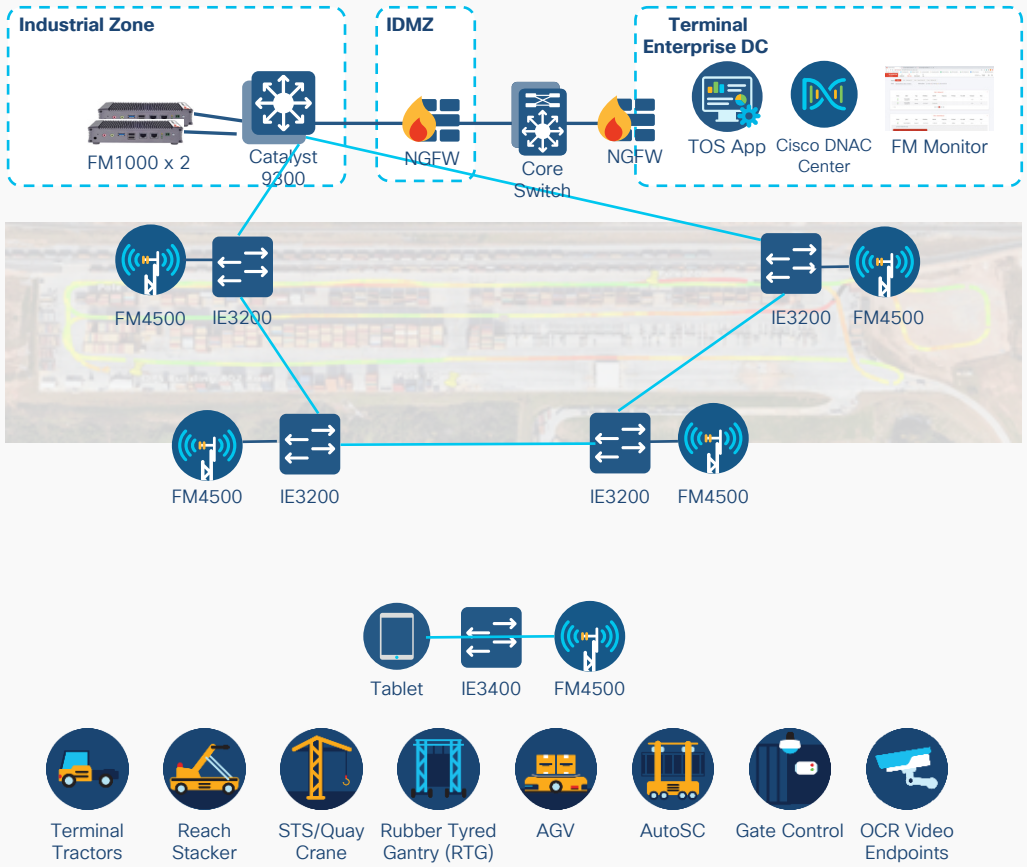


Connecting terminal operating system

Malta Freeport Terminals, located at the center of the Mediterranean Sea, is a premier trans-shipment hub, having successfully operated for over 30 years as a vital part of the Mediterranean containerization market. The Freeport is located at the crossroads of some of the world's most important shipping routes, making it an ideal intersection point for any shipping lines. It covers almost 2500 meters of deep-water quays, with 21 STS cranes, 65 RTG cranes, and ancillary yard equipment, amounting to a total of 250 pieces of container-handling equipment. Automation plays a vital role in the Freeport to boost the efficiency of the terminal operation, and is a strategic step to exploit the full potential in the future. The Freeport has updated its Navis Terminal Operating System with the migration to N4/XPS to keep up with the demand for optimum efficiency. To cope with demand and future growth, the Freeport needs a wireless network that can overcome the harsh environmental challenges and bring high bandwidth (scale to 50 Mbps), low latency (less than 5 ms), and fast roaming communication to 250 pieces of equipment, which move at speeds up to 25 km/hr across the entire terminal. Cisco Ultra-Reliable Wireless Backhaul exceeded the Freeport's expectations, delivering a solution that can achieve data speeds of 50 to 60 Mbps with extremely low latency of less than 3 ms and zero packet loss over distance of 600 to 800 meters. It not only meet current deployment requirements for TOS, but is also able to scale to accommodate future use cases such as remote operation of RTG cranes. Figure 8 presents a sample topology with solution components and key business outcomes.

Figure 8. Connecting to the TOS

Connecting Terminal Operating System (TOS)



Use cases and key requirement

- Real-time berth occupancy
- Berth availability and planning
- Real-time alerting
- Yard and vessel operation planning
- Application downtime caused by unreliable network connections and poor coverage

Solution

- High throughput, low latency, fast handoff, highly redundant, and reliable wireless backhaul (Cisco Ultra-Reliable Wireless Backhaul)
- IE3200, IE3300, and IE3400 Series secured and managed switches
- Simplified device onboarding and centralized policy control

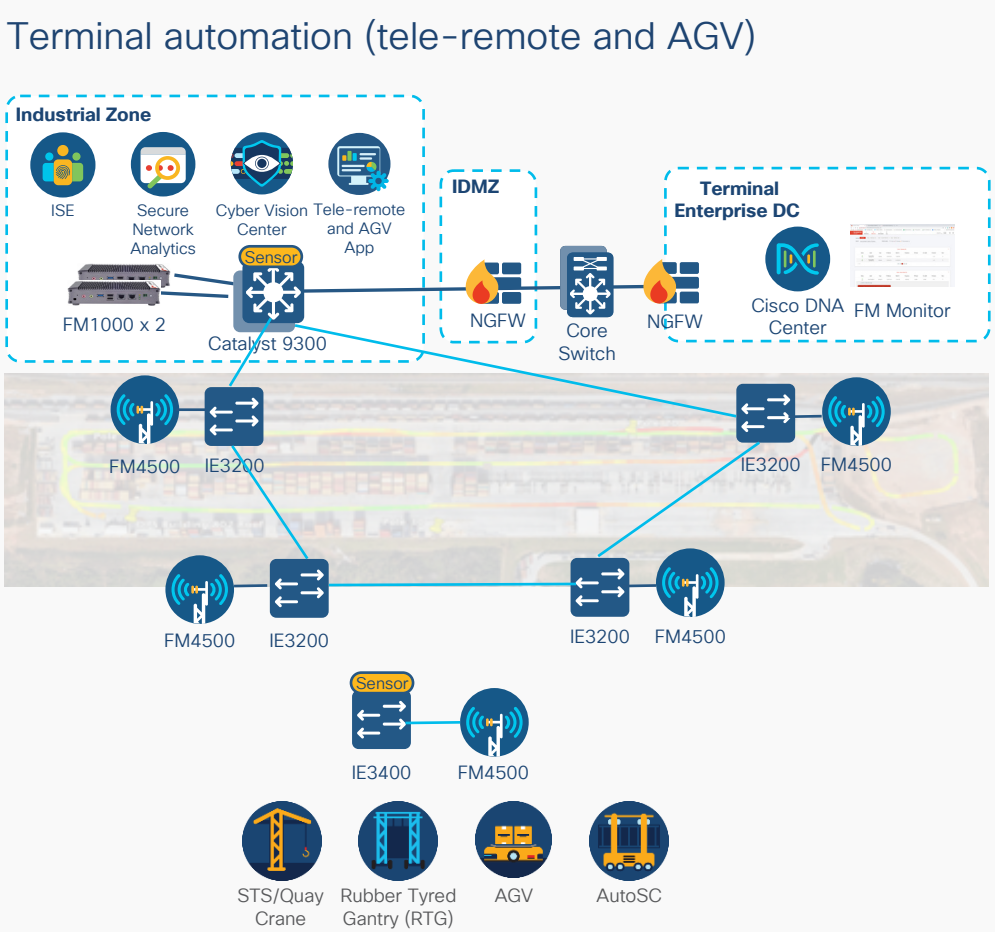
Outcomes

- Holistic view into berth availability and occupancy patterns helps in improving planning
- Ships can plan their arrival at the terminal with real-time information on berth availability.
- Increased operation efficiency
- Improved application uptime

Terminal automation (teleremote and AGV)

To date, the remote supervised and fully automated container cranes are electric powered, bundled with fiber optics to provide reliable control connectivity and data transfer to remote operating stations. This has been done with RTG cranes as well, but it has been limited to fully electric ones. Moving diesel-powered RTG cranes to a remote operation model has been held back by a lack of wireless communication technology that can meet operational requirements for high bandwidth, low latency, reliability, and security. RTG crane automation requires average 60-Mbps bandwidth, with sub-50-ms latency, minimum 99.5% system availability, and milliseconds handoff to operate at its full potential. The sample architecture of this use case is illustrated in Figure 9.

Figure 9. Teleremote automation



Use cases and key challenges

- Teleremote operation for RTG and STS/Quay Cranes
- Autonomous operation for AGVs and AutoSCs
- Application downtime caused by unreliable network connections and poor coverage

Solution

- High throughput, low latency, fast handoff, highly redundant, and reliable wireless backhaul (Cisco Ultra-Reliable Wireless Backhaul)
- IE3200, IE3300, and IE3400 Series secured and managed switches, micro-segmentation and enhanced asset visibility
- Simplified device management and centralized policy control

Outcomes

- Increased operation efficiency
- Improved ship turn time and terminal throughput
- Improved worker safety
- Improved maintenance of machinery
- Improved application uptime

The bridge to possible

Conclusion

Port and terminal operators around the world are looking for innovative ideas to improve their operational effficency while keeping costs down, securing their critical infrastructure, improving safety for the workers and facility, and increasing operations and application uptime. All these cannot be achieved without a reliable, scalable, and secured infrastructure. Cisco, along with our partners, is able to deliver a solution that not only transforms business operation today but also helps the operators be well prepared for the future. Based on the industrial standard ISA-95 reference architecture, the Cisco Connected Ports and Terminals solution incorporates Cisco networking innovations such as intent-based networking with Cisco IoT networking and security, securely and reliably connecting sensors, devices, machines, and people to support use cases including terminal automation, cyber and physical security, and port operations and monitoring. Cisco's ecosystem of partners and Cisco professional services are available to help port and terminal operators design, deliver, and even operate the Connected Ports and Terminals solution as part of an end-to-end solution that meets your specific needs.

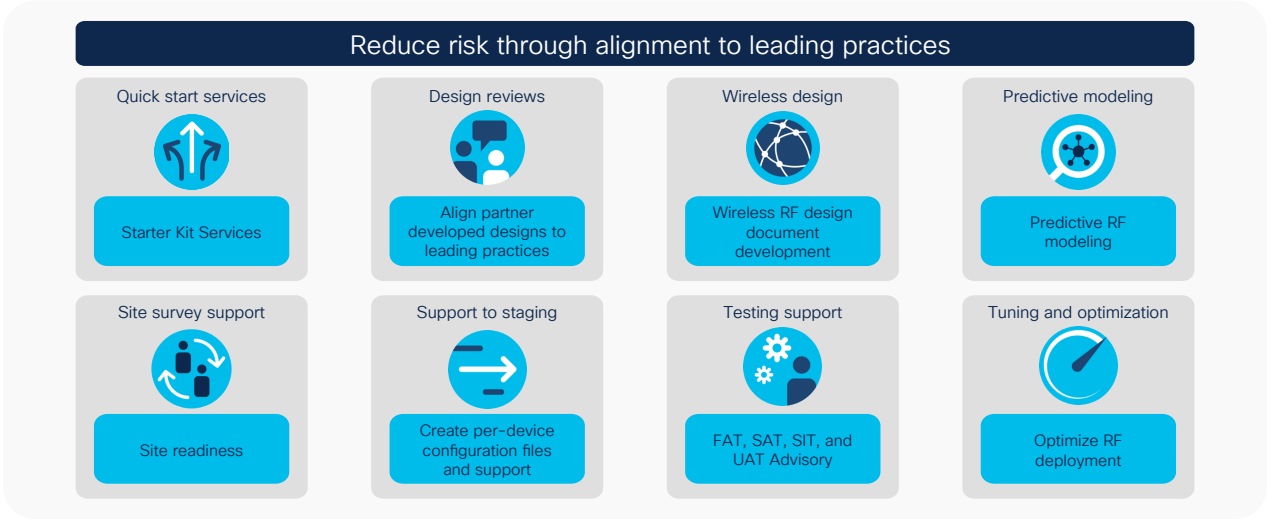
C22-2663669-00 10/21

Cisco Customer Experience

In today's rapidly evolving OT and industrial spaces, customers and systems integrators are challenged to keep pace with new technology trends to ensure that projects are delivered in a cost-effective manner. With Cisco's suite of Industrial Networking and Security services, our partners and customers can reduce solution implementation risk on projects that leverage Cisco IoT technologies in a true model of partnership with Cisco. With simplified packaging, a flexible consumption model, and advisory services covering each key project milestone, this suite of services can allow you to enter new markets with confidence to expand and grow your business.

Cisco's CX Industrial Networking and Security services help port and terminal operators accelerate the digitization of their existing operations using a unique architecture-based approach to service delivery. Cisco CX leverages strategy development, architectural assessments, network design, migration and deployment assistance, and support services to help Cisco's key ecosystem partners plan, build, and manage solutions. These solutions focus on business outcomes that result in improved operational efficiency, risk mitigation, higher productivity, improved worker safety, and deeper intelligence and insights, with security at the core of the end-to-end solution.

Figure 10. Cisco CX services



With more than 30 years of industrial networking experience, Cisco is uniquely positioned to address these new demands on industrial networks, which require a greater need for improved interconnectivity across industrial equipment and enterprise networks. Our proven processes and tools deliver consistent results based on best practices and strong communication. Our experts deliver services that allow organizations to accelerate the integration and transformation of their current infrastructure to the next-generation network, capable of evolving operations to continue to meet the evolving demands of the business.