Connected Ports and Terminals

Ports play an important role in promoting international trade and regional development. Ports are catalysts for economic development as they enable trade and support supply chains. Operational efficiency is crucial for ports, given that seaborne trade accounted for 80% of the total volume and 70% by value of global trade in 2016. See:

https://unctad.org/webflyer/review-maritime-transport-2018

Overview and Network Requirements

There are various kinds of ports – Container Ports, Bulk Ports, Dry Ports, Cruise Ship/Passenger Ports. The subject of this document is Container Ports.

The key challenges for ports and terminals are:

- Growing volume of operations. Digitization of ports drives increases in data traffic volume. IDC expects by 2025 operation data volume up 210% from 2021, which demands reliable and scalable infrastructure
- Cyber security OT/IT concern
- Increasing labor costs
- Heavy labor intensity, harsh working environments, and insufficient personnel
- Improving Workplace Safety and Security to mitigate risk (loss prevention, worker safety)
- Meeting regulatory requirements – sustainability and environmental targets

Reducing costs and improving efficiency through automation have become the industry’s overarching goals. Digital innovations and artificial intelligence (AI), big data, Internet of Things (IoT), autonomous vehicles and tele-remote operations provide new impetus for port automation.

Higher levels of automation are being used at container terminals to help improve productivity, efficiency, and ensure competitiveness. As the shipping throughput increases year after year, global ports/terminals are undergoing reconstruction to achieve a higher level or automation. As congestion concerns and demand for transport services increase, advanced automation is being implemented as one tool to improve port/terminal operations.

Smart ports and terminals require communications systems that support low latency, high bandwidth, low loss, and high reliability communication services in order to handle control data, safety systems, and multi-channel video data of port equipment.

Ports and Terminals Digital Transformation

There is an overwhelming trend for better integration of ports into the extended supply and value chain. Transport, intermodal facilities, all the way to the customer - port authorities, customs, quarantine, services, transport authorities, and so on.

The decision to automate a port is the relentless drive for effective, efficient, fast, and continuously monitored supply chain processes. Full automation enables port and terminal managers to meet and exceed client requests and market demands, while allowing flexibility and dependability.
Automation has transformed the way cargo moves across global supply chains, but also the real time capabilities of monitoring and controlling these movements. Port and terminal management becomes more reliable and sustainable through automated berthing operations, automated scheduling of ships, services, and cargo handling, as well as the monitoring and controlling of fixed and mobile equipment.

Advantages of Automating Ports and Terminals

As congestion concerns and demand for transport services increase, advanced automation is being implemented as one tool to improve port operations. Some of the advantages of automating ports and terminals include:

- Operational and maintenance cost savings
- Improved efficiency and availability
- Improved worker safety
- Reduced environmental impact in terms of reduced emissions and noise pollution
- Reduced labor cost
- Increased revenue from decreased downtime

Ports and Terminals Use-cases

Terminal Operating System

There is a strong trend toward remote operations of terminal operations – centralizing expertise and skills, safety by removing people from hazardous operational areas, and reducing costs. The Terminal Operating System (TOS) software controls the logistics of a terminal, including key functions such as vessel planning, container inventory maintenance, job order creation, and gate operations. TOS software is provided by several commercial companies and many terminal operators themselves. In a modern container terminal, some Container Handling Equipment (CHE) may be unmanned and operated by a computer and navigation system (autonomous operations) while part of them may be manually operated. The manual operation consists of two different modes:

- the operator physically sits inside a cabin on the vehicle
- personnel operates the vehicle remotely from a central control room (Tele-Remote).

There is little difference between these modes for TOS itself, however, where differences occur, it usually where remote drivers improvise container moves from a computer room.

Several advanced TOS are available on the market which provide functions to control the operation in the yard as well as interfaces to interact with CHE. TOS pre-calculates and creates stacking jobs using Rubber Tired Gantry cranes (RTG) or Rail Mounted Gantry cranes (RMG) or transport jobs using Automated Straddle Carriers (AutoSC) for CHE and will control the execution of respective jobs and/or a certain sequence of jobs.

Typical features of a TOS influencing the operation of CHE are:

- Standard handling and sequence of stacking activities for CHE
- Management of stacking/put-away rules in the yard
- Container target positions on the yard
- Working areas for handling equipment
- Pooling of CHE in working areas
- Load balancing of jobs over equipment per working area
Connected Ports and Terminals

- Position detection and calculation of travel distances
- Sending and control stacking and transport jobs to selected CHE
- Calculating necessary shifting jobs

In brownfield automation projects, automated handling equipment needs to be integrated with the TOS as well as into existing conventional equipment still in use. In a conventional terminal environment with human operated, non-automated equipment, the typical interface between the TOS and the handling equipment would be a job control monitor installed on a Vehicle Mounted Terminal (VMT) in the cabin of a crane. The operator sees his or her next job(s) on the monitor, and can select, execute, and confirm tasks accordingly.

To enable applications such as TOS, Tele-Remote, or Optical Character Recognition (OCR), all the vehicles need to have network connectivity. For the occasional exception where a vehicle can have fiber connectivity, the connectivity to the vehicles needs to be provided using a highly reliable and secure wireless link. The wireless technology must also provide seamless handoffs with minimal latency and packet loss between various infrastructure access points scattered around the terminal as the vehicles move around to accomplish their tasks.

Tele-Remote Operations

As the pressure mounts to improve efficiency, safety, and the port environmental footprint, the means to make all of that happen are already within reach. And, contrary to what organized labor might think, it’s not about reducing headcounts.

Port operations and logistics have significantly changed over the years, yet the core of this line of work remains dangerous, polluting, and repetitive. Autonomous technologies and teleoperation have the ability to change the nature of industrial drudgery, increasing productivity and efficiency, while reducing its harmful nature to both employees and to the environment.

Tele-Remote Operations and a Remote Operation Center (ROC) enable operators to control container cranes from the safety and comfort of a remote location. It delivers a complete crane control solution from operator login, carrying out operations, to operator logout. The Remote-Control Station (RCS) location can be anywhere as long as the RCS prerequisites are considered, such as network requirements.

RCS assists operators in carrying out their control tasks by presenting task-dependent information on a customized human–machine interface.
The Remote-Control Operation System typically consists of:

- One or several RCSs
- One RCS Server
- One Remote Control interface per crane
- Several cameras per crane

The operator uses the Human Machine Interface (HMI) on the RCS to control a crane from a remote location. To provide situational awareness to the operator, the RCS HMI provides live video streams from the remote-controlled crane combined with e.g. graphical information.

The operator controls the crane using hardware and software controls. The hardware controls should include an emergency stop push button, master controllers for controlling crane movement and buttons for frequently used crane functions.
Use-cases and advantages of Tele-Remote Operations within Ports/Terminals

Tele-remote operations in ports can be used in two main scenarios. In the first, it allows one operator to directly control one vehicle continuously throughout the completion of a task. The vehicle does not have to be an autonomous vehicle, although it will require integration to a teleoperation kit. In this scenario, the vehicle can be used to conduct hazardous activities, like operating a tractor in the belly of a coal ship or conduct non-routine operations that are not relevant for autonomous operations, like short distance transport by terminal tractors.

In the second scenario, tele-remote operation can support autonomous vehicles such as RTGs/RMGs that will mostly operate autonomously. Tele-remote operation will allow these vehicles to navigate edge cases that require human intervention for situations such as abnormal stops, lost self-positioning, incomplete jobs or changes to the operational environment. In this scenario, one operator can support several vehicles as they only require the human operator’s attention for a few moments at a time. Once the vehicles receive that help, they continue autonomously.

Although autonomous vehicle technology is advancing toward providing a complete solution to all logistics and port operation scenarios, for the foreseeable future, it’s easier and safer to have a human help operate these vehicles remotely using tele-remote operation technology.

The advantages of tele-remote operation go beyond economic efficiencies and safety as they can also contribute to reductions in emissions. Tele-remote operated vehicles require less energy and operate less hours – they don’t need to run the air conditioning/heating, and they do not need to transport a driver back and forth around the port, as their operators control the vehicles from the comfort of their office.

Ports and Terminals Network Requirements

Reliable, resilient, and secure data transfer is especially important when introducing remote-controlled or automated solutions. Video data in particular has to be transferred as real time data for the operator to be able to control equipment remotely. Usually fiber is the preferred connectivity mode when reliability is concerned, however even fiber has difficulty providing High Availability (HA) and reliable service to mobile assets. An example of where fiber is problematic in mobile assets is Quay Cranes and Overhead Gantry Cranes that employ rotary fiber couplers (typically within high voltage power cables) that deteriorate over time. Radio networks are hence an essential component for network connectivity within ports/terminals. All network technology needs to be designed appropriately for HA environments. Radio systems have evolved over time to offer better HA capabilities in more recent years.

Terminal Operating System

TOS is a store and forward system, therefore any information collected or retrieved is stored for delivery at first opportunity of connection. The bandwidth requirements for a TOS system are typically < 1 Mbps per vehicle. The latency requirements are not that stringent compared to some of the other applications such as Automated Guided Vehicles (AGVs), Tele-Remote Operations, Optical Character Recognition (OCR) or Video Surveillance.

Autonomous and Tele-Remote Operations

Autonomous and Tele-Remote operations for vehicles around the terminal requires the network link to support high throughput, 30 Mbps for Auto Straddle Carriers and 60 Mbps for RTGs with a maximum latency of 30 mSec. The traffic consists of a combination of PLC control traffic and live video feeds to allow the remote operator to view the terrain.

Remote Control of Gantry Cranes

A single gantry crane needs to upload anywhere between 5-to-16 channels of surveillance videos, and 1080p videos requiring a cumulative bandwidth of about 30 Mbps. In addition, PLC communications between the central control room and a gantry crane require a network latency of less than 50 mSec. In a typical deployment, about 60 gantry cranes are deployed within a 1 sq. Km area. The handoff requirements vary by manufacturer with most of them requiring handover times < 50 mSec and some < 10 mSec.
Remote Control of Ship-to-Shore/Quay Cranes

The main service unit in the berth/quay area is the Ship-to-Shore (STS)/Quay crane. The height of a quay crane is 60-70 meters/200-230 feet and wireless networks are required to provide network coverage in operation areas. Quayside container cranes have communication requirements for both remote control and monitoring. In the remote control scenario, there are more than 20 cameras on a single quayside container crane and the uplink bandwidth is estimated to be up to 50 Mbps. In addition, the deployment of quayside container cranes is relatively dense. Typically, 8 to 12 cranes are deployed along 1 km port coastline.

As most container terminals are built along seashores, berths must be sufficiently submerged in water and may be equipped with bollards and fenders. For this reason, wireless network devices need to serve the production and monitoring purposes of quayside container cranes and TOS components, while also providing network coverage for berthing vessels in some cases.

Automated Horizontal Transport

When designing a network to be used by any kind of Autonomous Horizontal Transport system, such as Automated Stacking Cranes or Automated Guided Vehicles (AGVs), coverage must be guaranteed across the entire working zone by facilitating overlapping radio-coverage zones from the infrastructure radios. Bandwidth requirements are comparatively low (~1 Mbps for AutoSC/AGV), however interruptions in signal and gaps during handover are not acceptable. There is constant data traffic to/from the on-board PLCs, and interruptions in data flow will cause the relevant solution to experience operational delays, or in extreme cases might cease the operation altogether.

Optical Character Recognition

Optical Character Recognition (OCR) is an Automated Identification and Data Collection (AIDC) technology. It is heavily used in modern ports/terminals to identify and track containers. OCR systems that process the data locally on the cranes or RMGs do not require a high amount of bandwidth, a constant connection and continuous stream of data. Only if OCR needs to be processed off machine and live is a constant connection needed and a higher throughput of 15-20 Mbps required. Interruptions in received signal and gaps during handovers are not acceptable, as these may cause the relevant equipment to experience operational delays. Up to 50 mSec of network latency depending on the chosen OCR vendor.
## Summary of Wireless Requirements

### Table 1  Terminal Automation Wireless Network Requirements

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Overall Requirement</th>
<th>Wireless Network KPI Requirements</th>
<th>Latency</th>
<th>Bandwidth</th>
<th>Reliability</th>
<th>RF Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Operating System (TOS)</td>
<td>Low Bandwidth and High Reliability</td>
<td></td>
<td>&lt; 1 Sec</td>
<td>450 Kbps to 1 Mbps</td>
<td>99.9%</td>
<td>Good Port-wide Coverage</td>
</tr>
<tr>
<td>Autonomous and Tele-Remote Operations</td>
<td>Low Latency, High Reliability, Constant PLC Traffic</td>
<td></td>
<td>&lt; 50 mSec</td>
<td>30 Mbps for AutoSC 60 Mbps for RTG</td>
<td>99.999%</td>
<td>Coverage across working area</td>
</tr>
<tr>
<td>Autonomous Horizontal Transport (Automation for PLC applications)</td>
<td>Low Bandwidth and Low Latency</td>
<td></td>
<td>&lt; 50 mSec</td>
<td>~ 1 Mbps for AutoSC/A GV</td>
<td>99.999%</td>
<td>Overlapping Coverage across the working area</td>
</tr>
<tr>
<td>Off-Machine Live Optical Character Recognition (OCR)</td>
<td>High Bandwidth</td>
<td></td>
<td>&lt; 50 mSec</td>
<td>15 – 20 Mbps</td>
<td>99.999%</td>
<td>100% Coverage</td>
</tr>
</tbody>
</table>

A terminal automation network requires a 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 a later chapter, to overcome these challenges and satisfy the stringent requirements.

There are lots of the other wireless use-cases within the port/terminal vertical like mobile worker communication with the terminal and on the ship, drone surveillance, connectivity for IoT sensors, etc. however those are not covered within the scope of this document.
Connected Ports and Terminals – Reference Architecture

This chapter provides an overview of a recommended network design for a Ports and Terminals network deployment. Also covered in this chapter are OT security considerations for this deployment.

High-Level Network Design

The Cisco Connected Ports and Terminals reference architecture, depicted in the figure below, follows the blueprint of ISA-95 and is based on the Cisco reference architecture for Industrial Automation and Control Systems (IACS). This reference architecture is composed of four major functional modules that include the Area Zone, Industrial Zone, Industrial Demilitarized Zone (IDMZ), and Enterprise. The following sections explain the functions and capabilities of each module in more detail.

Figure 2  Connected Ports and Terminals – Cisco Reference Design

Industrial Zone

The Industrial zone is important because all the applications, devices, and controllers critical to monitoring and controlling the terminal operations reside within this zone. To enable smooth and secure operations and functioning of the ports and terminals applications and devices, the Industrial zone requires clear logical segmentation and protection from the Enterprise 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 a 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 in this regard.

The Cisco industrial datacenter follows the best practices from Cisco datacenter 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 Cisco Identity Services Engine (ISE), dedicated wireless controllers to manage wireless connections within the industrial zone, and Cyber Vision and Secure Network Analytics to gain visibility into the production asset and application flows. ACI or Cisco Secure Workload also provide application security compliance, flow visibility and layered segmentation of compute-based control systems outlined in IEC 62443-3.

Third-party applications that are responsible for port and terminal operations are located in the server farms at the industrial datacenter. These applications include equipment control systems, crane interface systems, 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 cyberattacks, and the Cisco Secure Firewall ISA3000, located in this zone is designed to segment the traffic for different OT assets and protect them from potential threats.

An important point to note is that the ISA3000 is not capable of performing inter-industrial datacenter flow security, this capability is provided by Cisco’s mainstream firewalls such as ASA or Firepower and datacenter domain managers such as ACI or Cisco Secure Workload. The ISA3000 is appropriate at production zone security (below the industrial datacenter) and employed along with other segmentation concepts such as TrustSec micro-segmentation.

The site operations and control level is generally “carpeted space”- meaning it has HVAC with typical 19-inch rack-mounted equipment in hot/cold aisles utilizing commercial grade equipment. This is where applications related to port and terminal operations reside. Examples of services at this level would be Historians, control applications, TOS, OCR, Gate Control, Video Surveillance, and network security services. The systems and applications that exist at this level manage terminal wide operations. These operations typically need to be up and running 24x7 and any downtime has a huge and direct impact on revenue and end customer satisfaction.

The applications within the Industrial zone need to communicate with devices in the Area zone. These applications are primarily based on standard computing equipment and operating systems (Unix-based or Microsoft Windows). For this reason, these systems are more likely to communicate with standard Ethernet and IP networking protocols.

Additionally, because these systems tend to be more aligned with standard IT technologies, they may also be implemented and supported by personnel with IT skill sets.

Area Zone

The operations 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 telemtry 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 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 ingress. Industrial control protocols such as PROFINET and EtherNet/IP are supported natively on the Cisco Catalyst® Industrial Ethernet (IE) switches.

Multiple access technologies: Depending on the application requirements, deployment scenario, and existing network infrastructure, multiple access technologies, including both wired and wireless, might be needed for successful operations. 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 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.

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, loss 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, Parallel Redundancy Protocol (PRP) or High-Availability Seamless Redundancy (HSR) can be also leveraged and is supported on the Cisco Catalyst IE3400, IE4000, and IE5000 Series.

Security: Security in the operations area zone needs to be viewed as a subset of the 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. Also, at the application layer, within the control layers of ISA 95, ACI or Cisco Secure Workload can provide inter application and application to control asset security.

The operations area is where the most critical operations for a port and terminal such as container loading/unloading, container movement, container storage, container tracking, etc. take place. The commonly used handling equipment in container ports include the following:

- STS/Quay cranes perform loading/unloading activities between vessels and quayside
- Straddle carriers pick up and transport containers between quayside and storage yard
- AGVs are used to transport containers between quayside and yard
- RMG cranes are used for container acceptance, delivery, and stacking operations in a container yard or rail terminal
- RTG cranes on rubber tires are typically used for acceptance, delivery, and stacking at a container yard
- Reach-stackers (RSs) are vehicles used to transport a container for short distances and load/unload containers onto a truck or train
- Top lifters are lift trucks that can lift a container by using its spreader
- Side loaders are lift trucks fitted with lifting attachments operating on one side for handling containers
The vehicles listed above can be operated manually, semi-autonomous or in a fully autonomous mode. Most of the vehicles above also need to integrate with TOS to receive their schedule and set of instructions. A ruggedized tablet (typically running a Windows OS) is installed within each of these vehicles and needs connectivity to the TOS server installed within the Site Control room. A few of the TOS vendors have also started hosting the TOS server in the Cloud. In those scenarios secure Cloud connectivity is needed to the Cloud. In rare cases where the TOS application server is hosted within the Enterprise datacenter, the appropriate ports need to be opened up to allow TOS traffic to traverse between the vehicles and the TOS server on both the DMZ and Enterprise firewalls.

Gate control systems are used to process entry and exit of external trucks to retrieve or deliver containers by connecting the hinterland road to the container yard. Network connectivity needs to be provided to each of the gates to transport control information to the gate from the Gate Control System located in the Industrial Zone and transport video feeds from the gate to the Gate Control System. Most likely there is also interaction needed between the TOS application and the Gate Control system. The network connectivity to each of the gates can be achieved either using a fiber or a wireless link.

Three other important zones where network connectivity needs to be provided are:

- Weighbridge
- Container Turnaround area
- Truck Waiting area

An in-depth overview of the wireless design and deployment best-practices to support TOS application will be covered in the following chapters.
Enterprise Zone

The Enterprise Zone is where the centralized IT systems and functions exist. Enterprise resource management, business-to-business, and business-to-customer services typically reside at this level. Often the external partner or guest access systems exist here, although it is not uncommon to find them in lower levels of the framework to gain flexibility that may be difficult to achieve at the enterprise level. However, this approach may lead to significant security risks if not implemented within IT security policy and standards.

The ports and terminals applications and systems must communicate with the enterprise applications to exchange operational data. Direct access to the ports and terminals applications is typically not required. One exception to this would be remote access to the terminal equipment for management (configuration, troubleshooting) by employees or partners such as system integrators and machine builders. Access to data and the operations network must be managed and controlled through an industrial DMZ zone to maintain the security, availability, and stability of the operations network.

The services, systems, and applications at this level are directly managed and operated by the IT organization.

Industrial DMZ

Although not part of the Purdue reference model, the design includes a DMZ between the Industrial and Enterprise zones. The industrial DMZ is inserted to separate the enterprise networks and the operational domain of the ports and terminals environment. Downtime in the operations network can be costly and have a severe impact on revenue, so the operational zone cannot be impacted by any outside influences. Network access is not permitted directly between the enterprise zone and the industrial zone. However, data and services are required to be shared between the zones, thus the industrial DMZ provides an architecture for the secure transport of data between the industrial and enterprise zones. Typical services deployed in the DMZ include remote access servers and mirrored services such as Windows Update Servers, Anti-Virus Servers, etc.

As with IT network DMZs, the industrial DMZ is there to primarily be a buffer between the ports and terminals operations area and the Enterprise or the Internet, placing the most vulnerable services, such as email, web, and DNS servers, in this isolated network. The industrial DMZ not only isolates the port operations network from the outside world, but also from its own enterprise networks. The primary reason this additional isolation is recommended is that, unlike enterprise services, the port operations area contains the most critical and revenue generating part of the business. Often devices and applications being used within the ports and terminals operations area are antiquated, running on vulnerable operating systems such as Windows 95. The industrial DMZ provides another level of security for these vulnerable systems.

Another key use of the industrial DMZ is for remote access, aiding in remote configuration and troubleshooting of production equipment deployed within the ports and terminals operation. The industrial DMZ hosts the jump servers that can be logged into to access equipment within the terminals operations area.

Wired Network Components

Cisco Catalyst 9300 Access Layer Switch

Figure 4  Cisco Catalyst 9300 Access Layer Switch

The Cisco Catalyst 9300 Series Switches are the next generation of enterprise-class, stackable, aggregation layer switches. They provide full convergence between wired and wireless networks on a single platform.
Connected Ports and Terminals

Connected Ports and Terminals – Reference Architecture

- Delivers 480 Gbps stacking bandwidth capacity.
- Flexible uplinks: Cisco Multigigabit, 1 Gbps, 10 Gbps, 25 Gbps, and 40 Gbps. Fixed (C9300L) and modular (C9300) options.
- Flexible downlinks: Cisco Multigigabit, 5 Gbps, 2.5 Gbps, or 1 Gbps copper, or 1 Gbps fiber. Perpetual Cisco UPOE+, Cisco UPOE and PoE+ options.
- Supports ETA, AVB, Cisco Umbrella cloud security, MACsec-256 encryption, hot patching, NFS/SSO, redundant power and fans.

Cat-9300 Datasheet and switch model selector:

The Cat-9300 switches are positioned within the access layer within the industrial zone. These can be deployed on some of the large ports and terminals vehicles in order to provide access layer connectivity to cameras and sensors.

Figure 5 Catalyst 9500 Distribution/Core Layer Switch

The Cisco Catalyst 9500 Series Switches are the next generation of enterprise-class, stackable, core layer switches.
- 4-core x86, 2.4-GHz CPU, 16-GB DDR4 memory, and 16-GB internal storage
- Up to 6.4-Tbps switching capacity with up to 2 Bpps of forwarding performance
- Up to 32 nonblocking 100 Gigabit Ethernet QSFP28 ports
- Up to 32 nonblocking 40 Gigabit Ethernet QSFP+ ports
- Up to 48 nonblocking 25 Gigabit Ethernet SFP28 ports
- Up to 48 nonblocking 10 Gigabit Ethernet SFP+ ports

Cat-9500 Datasheet and switch model selector:

The Cat-9500 switches are positioned within the distribution or core layer of the industrial zone.
Cisco IE3x00 Rugged Industrial Switches

Cisco Catalyst IE3200 Rugged Series switches feature advanced, full Gigabit Ethernet with a modular, future-proof design. Expandable up to 26 ports in a compact form factor, these rugged switches are optimized for size, power and performance.

Cisco Catalyst IE3300 Rugged Series switches deliver high-speed up to 10 Gigabit Ethernet connectivity in a compact form factor, and are designed for a wide range of industrial applications where hardened products are required. The modular design of the Cisco Catalyst IE3300 Rugged Series offers the flexibility to expand to up to 26 ports of Gigabit Ethernet or up to 24 ports of Gigabit Ethernet and 2 ports of 10 Gigabit (10G) Ethernet with a range of expansion module options.

The Cisco Catalyst IE3400 Rugged Series switches deliver advanced, high-speed Gigabit Ethernet connectivity in a compact form factor, and are designed for a wide range of industrial applications where hardened products are required. The modular design of the Cisco Catalyst IE3400 Rugged Series offers the flexibility to expand up to 26 ports of Gigabit Ethernet with a range of expansion module options.

All of the above platforms are built to withstand harsh environments in manufacturing, energy, ports and terminals, transportation, mining, smart cities, and oil and gas.

These switches run Cisco IOS®XE, a next-generation operating system with built-in security and trust, featuring secure boot, image signing, and the Cisco®Trust anchor module.

Cisco IC3000 Industrial Compute Gateway

The Cisco IC3000 Industrial Compute Gateway extends data intelligence to the edge of the Internet of Things (IoT) network. For the ports and terminals, the Cisco Cyber Vision sensor can be installed for deployments where the sensor cannot be embedded into supported switches.
Security

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)

With an increase in the number of attacks on industrial installations, a smart port and terminal needs to have its cyber security in order. There is a large degree of data exchange with many third parties, increasing the risk of receiving malware or viruses that can spread to others. The fact that containers carry high-value goods also makes them a potential target of cyber crime. Finding the right container by hacking into the system and setting up an illegal delivery is not a hypothetical scenario. This means that cyber security must be part of the daily IT process; making sure that staff are aware of the risk is key, as people are always the weakest link. It has become obvious that cyber security also needs to be a top priority for container terminals, especially at the board level. Reliance on IT and data, and their responsibility for valuable goods, are simply too great to ignore, yet there remains much to do.

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, which provides visibility into industrial devices and their traffic flows; Secure Network Analytics, which can be used to 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; and Cisco Umbrella® to prevent passengers or workers from accessing malicious network domains. Additionally, Cisco SecureX™ provides a consolidated view for simplified management of the overall security approach.

Securing the industrial network is a journey

Industrial control networks connect devices that have been deployed over a period of many years — sometimes even decades — beginning back when cyber security wasn’t a concern. When organizations attempt to secure their industrial IoT networks, they encounter three primary issues:
A lack of visibility: Enterprises often don’t have an accurate inventory of what’s on their industrial network. Without this, they have limited ability to build a secure communications network architecture.

A lack of control: A lack of visibility also means enterprises are often unaware of what devices are communicating, and where those communications are going.

A lack of collaboration: OT devices and processes are managed by the operations team. Cybersecurity is generally driven by the IT and security teams. All these stakeholders need to collaborate to build the specific security policies and enrich events with context so that security does not disrupt production.

Addressing these issues and building a secure industrial network will not happen overnight. To help ensure success, Cisco promotes a phased approach in which each phase builds the foundation for the next, so that you can enhance your security posture at your own pace and demonstrate value to all stakeholders when embarking on this journey.

The figure below depicts the step-wise journey you can embark on integrating IT and OT security within your IT operations.

**Figure 8** The 4-step journey to secure your industrial network

Cisco’s integrated security portfolio helps customers through this journey

Extending IT security to OT through effective collaboration

To successfully secure the OT environment, all stakeholders must work together. Operations understands the industrial environment — the devices, the protocols, and the business processes. IT understands the IP network. And the security team understands threats and vulnerabilities. By working together, they can leverage existing security tools and expertise to protect the industrial network without disrupting operational safety and uptime.

Cisco security solutions are built into the industrial networks to monitor operations, feed security platforms with OT context, and enable this crucial collaboration.

Network managers will appreciate the unique simplicity and lower costs of Cisco’s edge architecture when looking to deploy OT security at scale. Operations will gain real-time insight into the industrial processes, so they can maintain system integrity and operations continuity. Security teams will have visibility into industrial assets and communications with context enriched by control/OT engineers.
Cisco ISE

Cisco Identity Services Engine (ISE) is a centralized Identity and Policy Management Server. It provides Dynamic Endpoint Visibility which can then in-turn be used to drive Visibility-based network segmentation. ISE also integrates with other Cisco security and third-party security services to provide automated threat containment. Cisco ISE is available as either a physical appliance or as a virtual machine.
Cisco ISA3000

Figure 11  Cisco ISA3000 Ruggedized Industrial Firewall

Cisco's ISA3000 is an industrial security appliance which is a foundational component of your IoT security journey. It bundles the proven security of Cisco Secure firewalls with the visibility and control of industrial protocols and applications from automation vendors such as Omron, Rockwell, GE, Schneider, Siemens, and others. The ISA3000 is the ideal ruggedized firewall to segment industrial networks, protect OT assets from potential threats, and build compliance so that you can capture the benefits of your industrial digitization efforts.

OT Security Challenges

Some of the challenges to OT security are as follows:

- Some OT assets cannot be patched
- Legitimate instructions can disrupt processes
- As more and more devices connect to the network the attack surface increases which means the airgap is not sufficient anymore
- Low visibility into what type and number of OT assets are present within the network. Low visibility over disconnected endpoints
- Multiple third-parties might be involved in day-to-day operations

Standard IT cyber security solutions and methodologies are not sufficient to fulfill OT cybersecurity requirements. Securing OT networks requires new IT procedures and tools. This is where Cisco Cyber Vision comes to the rescue.
Cisco Cyber Vision brings unprecedented scale and simplicity to IoT security. Industrial control systems (ICS) are ever more connected to corporate IT networks. You are now also deploying Industrial Internet of Things (IIoT) technologies. This deeper integration between IT, cloud, and industrial networks is creating many security issues that are becoming the primary obstacles to your industry digitization efforts.

Cisco Cyber Vision gives you full visibility into your ICS, including dynamic asset inventory, real-time monitoring of control networks and process data, and comprehensive threat intelligence, so you can build secure infrastructures and enforce security policies to control risk. Combining a unique edge monitoring architecture and deep integration with Cisco’s leading security portfolio, Cisco Cyber Vision can be easily deployed at scale so you can ensure the continuity, resilience, and safety of your industrial operations within your Port and Terminal deployment.

Cyber Vision Key Features:

- **OT Inventory and Security Assessments**: Kick-start your OT security journey by building an accurate list of all your industrial assets, baseline the network topology and communication patterns between the network devices and applications. Apart from helping you detect and build an OT asset inventory, Cyber Vision highlights device vulnerabilities and provides a risk score for each vulnerability.

- **Network Segmentation**: Prevent attacks from spreading and build a network that can be effectively monitored with adaptive, dynamic network partitioning.

- **Converged IT/OT SOC**: Feed your SOC (security operations center) with OT context and leverage the time and money you have invested in IT cyber security to secure your OT network.

- **Threat Detection**: Behavioral anomaly detection. Snort Intrusion Detection (IDS) with Talos signatures. Integration with Cisco SecureX for threat investigation.

- **Governance and Compliance**: Take OT security to the next level. Have detailed information to comply with regulations and enable effective collaboration between OT and IT experts.
Cisco Cyber Vision Architecture

Cisco Cyber Vision leverages a unique 2-tier architecture consisting of a Central Server and distributed Edge sensors. The Cyber Vision Sensor is responsible for capturing network traffic at the edge of the network and run a Deep Packet Inspection (DPI) on the application flows. The Cyber Vision Center is a centralized server which performs all the analytics and integrates with other security platforms such as firewalls or Security Information and Event Management (SIEMs) for instance. The strength of the edge sensor is that the software can be embedded into Cisco network equipment (IoT switches, routers, access points, or industrial compute platform). With Cyber Vision, industrial cyber security is built into your network equipment and fully integrated with your existing IT security platforms.

Deploying OT cyber security can quickly become complex. For your OT cyber security project to be successful you must be able to scale it easily and at a reasonable cost.

Advantages of Cisco Cyber Vision:

Cisco Cyber Vision is the only solution on the market that embeds OT security within your industrial network.

- No dedicated security appliance needed
- No need to build-out a separate out-of-band monitoring network to send industrial traffic to a central security server, no need for any additional cabling
- Rather than sending the entire network traffic to the Cyber Vision Center, the sensors decode the traffic locally at the edge of the network and only send the required meta-data, which typically represents only 2 to 3% of the network traffic

Application of Cyber Vision to Ports and Terminals

The Cyber Vision Center is the central platform for gathering data from the edge sensors with which to monitor, analyze, and manage them. It can be deployed as a virtual machine or a dedicated hardware appliance. And as seen in the reference architecture, it is best installed in the datacenter to minimize latency.

The Cyber Vision sensors are installed in the industrial network as either a dedicated device or running as a software package on a switch or router. As seen in the reference diagram below, there are a number of places the Cyber Vision sensor can be installed for maximum visibility.
The sensor requires a management interface to communicate with the Cyber Vision Center and send the metadata, which includes device attributes, packet headers, and operational events, from the captured IoT traffic. It is recommended to use the switch management interface for this communication.

The other required interface is for the data collection. On a switch platform this is accomplished using a SPAN session to an RSPAN VLAN which is private to the switch. On the IC-3000, there must be at least two physical interfaces used, one for the management network and one for the capture network. When using the IR-1101, only the routed gigabit Ethernet port is supported for the SPAN session to the sensor application. The management traffic can also use this routed port, the cellular interface, or even the LAN ports.

Ideally, the sensor would be installed on every switch with IoT devices connected to it. In the ports and terminal operations context, this would include any vehicles or structures with PLCs or other sensors. This provides Cyber Vision Center with the most information about the connected devices and their traffic flows. For instance, when a controller communicates with a PLC on board a crane, the sensor can monitor this communication and create a baseline for future monitoring. Any deviations from this baseline would be flagged as an anomaly. If this installation guideline is not reasonable given cost or platform limitations, the traffic flows must be analyzed to pick the best sensor placement. In the case of a centralized distribution switch, like the Catalyst 9x00, installing the sensor there will provide the ability to monitor all north/south communications.

This deployment model, however, will not provide any visibility into any east/west communication whether between access switches or within the access switch itself. In cases where upgrading the access switch to a supported model is not feasible, an IC-3000 with the Cyber Vision sensor installed on it can be deployed at that location. However, because the IC-3000 is not in the data path, a SPAN session on the switch must be configured to mirror all the IoT traffic to the IC-3000.

Refer to the deployment guides for more detailed installation instructions:


When installing the sensor, it can be installed in Active or Passive mode. The differences are outlined below.
If an asset communicates regularly, then a passive approach will be sufficient to profile the device without adding to the traffic load. A passive approach is also recommended if the devices do not communicate using the active discovery protocol. These protocols are EtherNet/IP (Rockwell Automation), PROFINET, and S7 Communication (Siemens). Otherwise, if an asset communicates very infrequently and a full picture of the network is desired quickly, an active discovery is recommended.

After Cyber Vision Center has started collecting data from the assets, it will profile the devices and categorize the data. This will enable the port operator to see which devices are communicating, what kind of data is being transmitted, and whether any issues have been identified. Some examples are below.

### Table 2 Differences between CV Sensor Active vs. Passive Mode

<table>
<thead>
<tr>
<th>Property</th>
<th>Passive</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery Method</td>
<td>Captures packets sent by the device as part of its operation.</td>
<td>Actively sends hello messages using select protocols to search for devices.</td>
</tr>
<tr>
<td>Network or Device Impact</td>
<td>Traffic is passively listened to on monitored ports. Impact is higher when network traffic is duplicated to sensor outside of data path.</td>
<td>Constantly sending hello packets to devices increases network load as well as load on asset.</td>
</tr>
<tr>
<td>Asset Discovery</td>
<td>As long as the sensor is in the data path of a communicating device, it will be discovered.</td>
<td>The assets must be responsive to the sensor’s requests and depending on the frequency of the active discovery hellos, it could take some time before assets are discovered.</td>
</tr>
<tr>
<td>Asset Information</td>
<td>Only the information the asset transmits can be used for discovery. If data is not transmitted for a long time, it will go undiscovered.</td>
<td>If the asset is online and responds to the active discovery, then all the relevant information is discovered. Otherwise, it can be marked as unresponsive or offline.</td>
</tr>
<tr>
<td>Asset Discovery Timing</td>
<td>Timing is completely dependent on how quickly an asset sends all the relevant information.</td>
<td>Discoveries can be performed on demand for quick information gathering. Excessive discoveries could be perceived as a Denial of Service attack.</td>
</tr>
</tbody>
</table>
Figure 14  Cyber Vision Asset Visibility

Figure 15  Cyber Vision Asset Communication Map
Figure 16  Cyber Vision Detected Vulnerabilities

84 Vulnerabilities

10 most matched vulnerabilities

- CVE-2017-11780 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices

- CVE-2017-0279 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices

- CVE-2017-0143 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices

- CVE-2017-0146 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices

- CVE-2017-0144 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices

- CVE-2017-0145 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices

- CVE-2017-0280 • Windows SMB Denial of Service Vulnerability
  4 affected devices

- CVE-2017-0147 • Windows SMB Information Disclosure Vulnerability
  4 affected devices

- CVE-2017-0275 • Windows SMB Information Disclosure Vulnerability
  4 affected devices

- CVE-2017-0273 • Windows SMB Denial of Service Vulnerability
  4 affected devices

Vulnerability severity legend:  NONE  LOW  MEDIUM  HIGH  CRITICAL
**Figure 17** IT and OT Vulnerabilities detected by Cyber Vision

<table>
<thead>
<tr>
<th>Vulnerability Title</th>
<th>CVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows SMB Remote Code Execution Vulnerability</td>
<td>CVE-2017-0279</td>
</tr>
<tr>
<td>WiWorks TCPIP Block (IPNET) Urtens/11 Vulnerabilities: Heap Overflow in DHCP Offload Function Inside巴菲</td>
<td>CVE-2019-12257</td>
</tr>
<tr>
<td>Rockwell Automation CompactLogix 3370 - Stack-based Buffer Overflow Vulnerability</td>
<td>CVE-2019-10954</td>
</tr>
<tr>
<td>Rockwell Automation CompactLogix 3370 - Uncontrolled Resource Consumption Vulnerability</td>
<td>CVE-2019-10952</td>
</tr>
<tr>
<td>WiWorks TCPIP Block (IPNET) Urtens/11 Vulnerabilities: TCP Urgent Pointer Space Confusion due to Race Condition</td>
<td>CVE-2019-12263</td>
</tr>
<tr>
<td>WiWorks TCPIP Block (IPNET) Urtens/11 Vulnerabilities: ICMP Information Leak via CMP1 Static Membership report</td>
<td>CVE-2019-12263</td>
</tr>
<tr>
<td>Open Realtime Vulnerability in Rockwell Automation MicroLogix 1400 and CompactLogix 3370 Controllers</td>
<td>CVE-2019-10955</td>
</tr>
<tr>
<td>WiWorks TCPIP Block (IPNET) Urtens/11 Vulnerabilities: TCP Urgent Pointer + 2 leads to integer overflow</td>
<td>CVE-2019-12255</td>
</tr>
<tr>
<td>WiWorks TCPIP Block (IPNET) Urtens/11 Vulnerabilities: Handling of unsolicited Reverse ARP replies (Logical F \mbox{\textit{C}}}</td>
<td>CVE-2019-12262</td>
</tr>
<tr>
<td>WiWorks TCPIP Block (IPNET) Urtens/11 Vulnerabilities: TCP Urgent Pointer Stack Confusion during commit to ministack</td>
<td>CVE-2019-12261</td>
</tr>
<tr>
<td>Rockwell Automation 1771-58206 / 58206-1040 Reflection Cross Site Scripting Vulnerability</td>
<td>CVE-2016-26152</td>
</tr>
<tr>
<td>Schneider Electric Modbus Protocol - Multiple Authentication Bypass Vulnerabilities</td>
<td>CVE-2017-6058</td>
</tr>
<tr>
<td>Schneider Electric Modbus Protocol - Multiple Authentication Bypass Vulnerabilities</td>
<td>CVE-2017-6054</td>
</tr>
</tbody>
</table>
Ports and Terminals CURWB Wireless Deployment – Architecture and Best Practices

Wireless Network Requirements

**Figure 18** Terminal Automation and Digitization – High-Level Wireless Network Requirements

The figure above depicts the key high-level wireless network requirements for Terminal Automation and Digitization.

Cisco Ultra-Reliable Wireless Backhaul Overview

**Figure 19** Key capabilities of CURWB

Key technical requirement met by CURWB for the Ports and Terminals Vertical:

- Operates in globally available ISM frequency bands
- Enables customized/full terminal RF service coverage
- Under total control of the terminal operator
**Connected Ports and Terminals**

**Ports and Terminals CURWB Wireless Deployment – Architecture and Best Practices**

- Compatible with, and validated by all main market vendors
- Supports PROFINET and CIP safety
- Uptime of 99.999%
- Ultra-Low latency of < 10 mSec
- Seamless roaming (handoff) - Multi-frequency capability with 0 m/s handoff
- Fast failover (TITAN)
- High Bandwidth (up to 500 Mbps)
- Load-Balancing
- Easy Installation

**CURWB – Key Technology Pillars**

Three key technologies underlay the foundation for the Cisco Ultra-Reliable Wireless Backhaul (CURWB) solution:

- **Prodigy 2.0**: MPLS-based transmission protocol built to overcome the limits of standard wireless protocols.
- **Fluidity**: Proprietary fast-roaming algorithm for vehicle-to-infrastructure communication with a 0 mSec roam delay and no roam loss for speeds up to 200 Mph or 360 km/hour.
- **TITAN**: Proprietary fast-failover high-availability mechanism that provides hardware redundancy and carrier-grade availability.

**Prodigy 2.0 – MPLS Overlay**

CURWB uses a proprietary wireless-based MPLS transmission protocol Prodigy to discover and create label-switched paths (LSPs) between mesh-point radios and mesh-end(s). Prodigy helps with making the wireless mesh networks resilient and helps for both Fixed as well as Mobility networks. MPLS provides an end-to-end packet delivery service operating between levels 2 and 3 of the OSI network stack. It relies on label identifiers, rather than the network destination address as in traditional IP routing, to determine the sequence of nodes to be traversed to reach the end of the path.

**Fluidity**

Fluidity enables a vehicle that is moving between multiple infrastructure APs to maintain end-to-end connectivity with seamless handoff between APs. Vehicle radios negotiate with the infrastructure APs and form a new wireless connection to a more favorable infrastructure AP with better signal quality before breaking or losing its currently active wireless connection.

As can be seen in the figure below, because of the unique make-before-break handoff algorithm, the vehicle radios always operate on the top line (RSSI Envelope), handing over from the currently connected radio to the next available radio as soon as the difference in RSSI meets the configured threshold.
TITAN – Hardware Redundancy and High-Availability

TITAN is a proprietary fast-failover function providing high-availability and protection against hardware failures. The feature virtually guarantees uninterrupted service for mission-critical applications where safety and/or operations would otherwise be compromised by failure of a single radio or gateway device. Leveraging an MPLS-based protocol, TITAN is able to achieve device failovers within 500 mSec within both L2 and L3 networks.

CURWB L2 Fluidity Deployment - Network Components

CURWB Mesh End Gateway

All Fluidity / fixed infrastructure deployments need a mesh end. It functions as a gateway between wireless + wired. It is highly recommended that all systems using Fluidity use a redundant pair of mesh end gateways to terminate the MPLS tunnels, aggregate traffic and act as interface between the wired and wireless network. Mesh End gateways can also be thought of as MPLS label edge routers (LERs) on the infrastructure network. The Mesh End gateway is responsible for encapsulating the traffic coming in from the wired network into the Fluidity overlay network using MPLS and de-encapsulating MPLS and delivering standard datagrams onto the wired network.

CURWB gateways are rugged, industrial grade network appliances that make setup and management of medium and large-scale CURWB Fluidity and Fixed Infrastructure deployments fast and easy. Gateways allow the Fluidity wireless infrastructure to scale to hundreds of radio devices, without impacting the performance of the overall network.
The FM4500 MOBI comes in a rugged die cast aluminum housing that has been purpose built for harsh environments such as those found within Ports and Terminals. It consists of industrial-grade anti-vibration M12 ports and QMA connectors, EN50155 certified. Optionally, one can also order the fiber-enabled FM4500 MOBI which supports a fiber port with an XCO connector.

The Ethernet model has 2 x 10/100/1000 M12 ports. The Fiber model has 1 x Dual LC ruggedized SFP XCO connector (transceiver not included) and 1 x 10/100/1000 M12 port. The radio can either be powered using PoE+ output from a switch or 48V DC input from an onboard power source.
Note: It is highly recommended to have a DC-to-DC converter on board vehicles to provide stable/clean power at the appropriate voltage level to the radio to avoid any damage. This is applicable when powering on the radio using the vehicle battery.

The FM4500 MOBI is the recommended radio model to be deployed on board the vehicles, since it is vibration resistant.

For deployments where one is able to run M12 cables up the High Mast Lamp Poles (HMLP), FM4500 can be considered for the infrastructure radio. Since M12 cabling is more expensive as compared to an RJ45 cable, more investment in cabling is needed. Where existing RJ45 cabling has already been run on the HMLPs, FM3500 is the preferred model. In scenarios where the distance between the switch and the radio exceeds 100 meters/328 feet, fiber cabling with the FM4500F can be leveraged.

FM-Horn-90 Antenna

The FM-Horn-90 is a connectorized symmetrical horn antenna with carrier class performance. The FM-Horn-90 antenna offers unique RF performance in a very compact package. Scalar horn antennas have symmetrical beams with identical patterns in the Vertical and Horizontal planes. Extremely small side lobes result in greatly decreased interference. FM-Horn-90 antennas are ideal for covering areas with close in clients where null zone issues occur. High density AP clusters and radio co-location is now practical due to its radiation pattern and a compact size. The FM-Horn-90 antenna is equipped with N-female connectors.
Figure 23  FM-Horn-90 Specifications

<table>
<thead>
<tr>
<th>TECHNICAL DATA</th>
<th>PERFORMANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio Connection</td>
<td>2x N Female Bulkhead Connector</td>
</tr>
<tr>
<td>Antenna Type</td>
<td>Horn</td>
</tr>
<tr>
<td>Materials</td>
<td>UV-Resistant polycarbonate, Polypropylene, Aluminum Zinc, Stainless Steel</td>
</tr>
<tr>
<td>Environmental</td>
<td>IP55</td>
</tr>
<tr>
<td>Pole Mounting Diameter</td>
<td>15-86 mm</td>
</tr>
<tr>
<td>Temperature</td>
<td>-30°C to +55°C (-22°F to +131°F)</td>
</tr>
<tr>
<td>Wind Survival</td>
<td>160 km/hour</td>
</tr>
<tr>
<td>Mechanical Tilt</td>
<td>≤ 25°</td>
</tr>
<tr>
<td>Weight</td>
<td>1.7 Kg / 3.7 lbs - single unit</td>
</tr>
<tr>
<td></td>
<td>2.8 Kg / 6.2 lbs - single unit incl. package</td>
</tr>
<tr>
<td></td>
<td>N/A Kg / lbs - carton (N/A units)</td>
</tr>
<tr>
<td>Single Unit</td>
<td>Retail Box: 31 x 20 x 22 cm*</td>
</tr>
<tr>
<td>N/A Units</td>
<td>Carton Box: N/A</td>
</tr>
</tbody>
</table>

*Estimation based on pre-production units. Subject to change.

<table>
<thead>
<tr>
<th>PERFORMANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency Range</td>
</tr>
<tr>
<td>Gain</td>
</tr>
<tr>
<td>Azimuth/Elevation Beam Width-3 dB</td>
</tr>
<tr>
<td>Azimuth/Elevation Beam Width-6 dB</td>
</tr>
<tr>
<td>Front-to-Back Ratio</td>
</tr>
<tr>
<td>VSWR Max</td>
</tr>
<tr>
<td>Polarization</td>
</tr>
<tr>
<td>Impedance</td>
</tr>
</tbody>
</table>

FM-Horn-90 is the best choice for Ports and Terminals because most of poles in ports are structured in a way that the radios have to be installed on top of HMLP (35 meter/115 feet) and installing OMNI antennas at such a height does not provide low ground vehicles with good coverage. The Horn-90 directional antenna can be tilted downwards and due to being symmetrical can provide good coverage for a small vehicles that are operating in 2 meter/7 feet height like Terminal Tractors and other ground vehicles.

FM-OMNI-5-KIT Antenna

The FM-OMNI-5-KIT antenna consists of two antennas, a FM-OMNI-5-H which is a horizontally polarized antenna and an FM-OMNI-5-V which is a vertically polarized antenna.

FM-OMNI-5-H horizontally polarized omni-directional antennas are designed for long-lasting operation with outdoor access points.

The FM-OMNI-5-V vertically polarized omni-directional design utilizes a linear array, encapsulated in a heavy-duty fiberglass radome with a thick-walled mounting base for reliable, long term use.

This rugged design of the above antennas withstands harsh environments, making the antennas ideal for Industrial Wireless applications. The antennas are DC grounded for ESD protection of radio components.
The FM–OMNI–5–KIT antenna is used on:

- Vehicles that move 360–deg inside the terminal

Infraestructure radios that need to provide 360–deg coverage. An important point to note here is that the omni–directional antennas when used on the infrastructure radios should ideally be installed about 3 meters/10 feet above the vehicles that are receiving coverage.

Power Injectors for CURWB Radios

In the event that there is a switch that does not support PoE power or when no switch is available, power injectors can be used to power up the CURWB radios.

**Table 4**

<table>
<thead>
<tr>
<th>PID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLMESH–HW–PWR–1</td>
<td>On board in-line Power Conditioner providing 48V OUT.</td>
</tr>
</tbody>
</table>

**RACER**

CURWB RACER is a centralized cloud–hosted server that can be used for provisioning of the entire CURWB system including configuration, firmware upgrade, and plug–in activation. It allows all the radio configuration to be done in a single pane and uploaded to the radios in real time or offline. RACER supports all the configuration options (basic and advanced). RACER can be used to create configuration templates and apply them to multiple CURWB devices of the same type. RACER templates can be applied in either online mode (if the CURWB devices have internet access) or offline mode (if the CURWB devices have no Internet access). The advantage of using RACER is that along with the device configuration it also upgrades the firmware to the latest version available and also applies the configured plug–ins. This is the preferred method for configuring CURWB devices for any size deployment.
**FM-Monitor – Centralized Management of CURWB Infrastructure**

FM-Monitor is a network-wide, on-premises monitoring dashboard, allowing any CURWB customer to proactively maintain and monitor one or multiple wireless OT networks. FM-Monitor displays data and situational alerts from every CURWB device in a network, in real time.

FM-Monitor supports fixed and roaming network architectures and allows easier end-to-end troubleshooting. It can be operated as a standalone system or in parallel with a sitewide Simple Network Management Protocol (SNMP) monitoring tool. It is designed to support network installations used in smart cities, rail, mining, ports and terminals, entertainment, smart factories, and military applications.

**Figure 25  FM-Monitor Topology View**

Features and benefits:

- On-premises monitoring tool for CURWB networks
- Wizard setup for quick and easy installation and deployment of FM-Monitor
- Real-time dashboard displaying uptime, throughput, latency, jitter, and other network KPIs
- Customizable section view to easily check groups of radios
- Customizable monitoring alerts for prompt response
- Radio-by-radio data logging with a minimum sampling interval of 300 mSec
- Real-time information display for quick and accurate troubleshooting
- Side-by-side comparison of radio KPIs over time and over vehicle position
- Alerts/events can be forwarded to a Syslog server
Radio KPIs such as RSSI, LER, PER, and so on can be exported to a CSV file for graphing.

One of the biggest advantages of FM-Monitor is the ability to configure alerts for a group of radios based on certain KPIs. Imagine needing to support an application mix of Automation and CCTV. The set of radios supporting the Automation application can be grouped and alarms configured for KPIs such as latency, jitter, RSSI, etc. while the group of radios supporting the CCTV network can have alarms configured using different KPIs such as Link Error Rate (LER), MCS rate, etc.

L2 Fluidity Architecture

The figure above depicts the high-level L2 Fluidity mobility architecture for a single frequency deployment. A prerequisite for L2 Fluidity is that all the CURWB devices (mesh-end gateways, access radios and mobile radios) need to be within the same VLAN/IP subnet/L2 broadcast domain and also be configured with the same passphrase.

The distribution/core layer consists of a redundant pair of mesh-end gateways. The role of the mesh-ends is to terminate the MPLS tunnels from each of the vehicle radios and act as a demarcation point between the wired and the wireless domains. The mesh-ends are responsible for de-encapsulating the MPLS header and then forwarding the traffic to the distribution/core switch. For the traffic originating from the wired network and going towards the mobility domain, the mesh-ends act as the default gateway and are also responsible for the MPLS encapsulation and forwarding the traffic to the appropriate vehicle radio.

The access radios are configured as mesh points in L2 Fluidity mode with the same passphrase that is configured on the mesh-ends. The role of the access radios is to provide RF coverage for the mobility domain. The access radios are distributed across the area where wireless coverage is required while the vehicles roam. In the above architecture all the access radios are configured to operate in the same frequency.

For the mobility domain there are two primary kinds of deployment models. A vehicle can either have a switch on board or no switch on board.

Redundancy and Fast Failover at the Core Layer

Catalyst-9500 StackWise Virtual High-Availability

Cisco StackWise Virtual is a two-node solution providing a Unified Control Plane Architecture by assigning one switch as active and the other as a hot-standby. Both switches play an active role when it comes to data forwarding. Two Cat-9500 switches are connected together using a StackWise Virtual Link (SVL). The SVL helps bring the two switches...
together forming a single logical switch. Both the switches can be managed as a single entity. Because the control plane, management plane, and data plane are integrated, the system behaves as a single switch. The advantage of configuring the switches in a StackWise pair is that it provides hardware redundancy and fast failover.

**FM1000/FM10000 Mesh End Redundancy and TITAN Fast-Failover**

The FM1000/FM10000 Mesh End gateway is a critical component within the network that terminates all the MPLS tunnels, aggregates all the traffic coming from the wireless network and is the demarcation point between the wired and the wireless domain. Hence, it is highly recommended to purchase and apply the TITAN high-availability plug-ins for a pair of redundant FM1000/FM10000 Mesh Ends to be used within the ports and terminals deployment.

Once configured, TITAN is completely autonomous and ensures stable and reliable connectivity without the need for any human intervention. If data exchange ceases because of the failure of the primary mesh-end device, TITAN will detect the failure and re-route the traffic through the designated secondary device, re-establishing connectivity within a maximum of 500 mSec. When the failed primary mesh end device comes back online, the secondary mesh end device automatically reverts back to its standby role.

It is highly recommended to power each of the FM1000/FM10000 gateways using a different power source and connect them to different switches within the 9x00 StackWise pair. This provides protection against power outages and switch hardware failure.

**CURWB Access Layer - Fast Convergence on Failure**

**Link Backhaul Check – Handoff Inhibition**

Leveraging the Link Backhaul Check feature, an access radio unit detects a carrier loss on its Ethernet/fiber port hence losing its ability to deliver mobility traffic to the mesh-end. The affected radio unit immediately advertises its status as ‘Unavailable’, by transmitting a ‘handoff inhibition’ message over the wireless channel. Upon receiving the ‘handoff inhibition’ message any existing mobile radios connected to this particular radio unit will try and search for another access radio to connect to. All mobile radio units currently connected to this unavailable access radio will find and connect to an alternative access radio unit within a few hundred milliseconds, typically within < 400 mSec. Also any handoff attempts from any other mobile radios to this affected access radio will be rejected. It is highly recommended to enable the Link Backhaul Check feature on the access radios within a Ports and Terminal deployment.
In the figure above it is shown that the link between the infrastructure radio and the HMLP switch is down. Assuming that the radio is not powered using PoE but via an external power source the radio is still up and providing good wireless connectivity to the vehicles. However since the wired link is down and the radio is not able to forward traffic to the wired network, the radio goes into handoff inhibition mode.

Mesh-End Backhaul Check – Handoff Inhibition

Leveraging the Mesh-End Backhaul Check feature, an access radio unit detects that it is not able to reach the active mesh end. This failure is triggered when L2 MAC reachability is lost to the active mesh end for 250 mSec. The affected radio unit immediately advertises its status as ‘Unavailable’, by transmitting a ‘handoff inhibition’ message over the wireless channel. Upon receiving the ‘handoff inhibition’ message any existing mobile radios connected to this particular radio unit will try and search for another access radio to connect to. All mobile radio units currently connected to this unavailable access radio will find and connect to an alternative access radio unit within a few hundred milliseconds, typically within < 400 mSec. Also any handoff attempts from any other mobile radios to this affected access radio will be rejected. It is highly recommended to enable the Mesh-End Backhaul Check feature on the access radios within a Ports and Terminal deployment.
In the figure above it is shown that the HMLP switch loses its fiber connectivity to the core switch, the infrastructure radio is powered on and providing good coverage and connectivity to vehicles but since the radio is not able to forward traffic to the mesh end located within the control room, it will go into handoff inhibition mode.

**Note:** The Mesh-End Backhaul Check feature is only supported for wired (ethernet or fiber backbone) connected Mesh Points. Disable this feature when using wireless backhaul connectivity.

**CURWB Mobility Radio Redundancy and TITAN High-Availability**

For deployments leveraging dual-radios on board a vehicle it is highly recommended to apply the TITAN HA plug-in on the pair of radios. Both radios need to be connected to the same switch on board the vehicle. Once TITAN is configured both radios exchange high-frequency keepalives between them to enable failure detection and fast failover within 500 mSec.
CURWB L2 Fluidity deployment for Ports and Terminals

The figure above depicts the CURWB Fluidity L2 high-level network architecture comprising of 4-zones:

- Vehicle Mobility Network
- Access Network
- Backbone Network
- Core Network

CURWB systems for port and terminal operations are compatible with all Terminal Operating Systems. CURWB network applications include, but are not limited to Optical Character Recognition for cranes, easy retrofits of existing terminal vehicles, (including STS/Quay Cranes, RTG cranes, AGVs, reach stackers, and stacking cranes), wireless tele-remote crane control, real-time video pan-tilt-zoom and CCTV feeds for vehicle operation and security, safety and telemetry inputs and outputs, failover networks for fiber spools, GPS correction data for Automated Guided Vehicles and Automated Stacking Cranes, and Wi-Fi network backbones.

In this reference design the focus will be on the CURWB architecture and deployment best-practices to enable TOS. TOS usually needs lower bandwidth than other ports/terminals applications – typically a maximum of 1 megabit per second per vehicle. Wireless coverage of the full operations area is mandatory to support the TOS application. Network latency requirements are generally very lenient, although latency requirements may depend on specifications given by the Terminal Operating System vendor.

There is a high likelihood that there will be other type of traffic on the network along with TOS traffic, such as Webex or Skype for audio communications, Anydesk for maintenance, Syslog messages from RTGs, etc. It is important to apply the appropriate QoS and Traffic Shaping policies for the different types of traffic and always prioritize TOS application traffic over all other kinds of traffic in order to ensure the smooth operation of the port/terminal.

It is important to ensure that only traffic intended to be on the wireless network should be allowed. For e.g. if the CURWB wireless network has been designed for TOS application only and a 1 Mbps bandwidth plug-in has been applied on the radios, the expectation should be set correctly and it should not be expected that other kinds of traffic such as Webex/Skype, Anydesk, Syslog can be run over the same infrastructure. This will cause severe degradation of the TOS application.

If the requirement and expectation is to use the CRUWB wireless network for traffic other than TOS then it might need a different RF design and a need for higher bandwidth plug-ins on the CURWB radios.
Connected Ports and Terminals

Ports and Terminals CURWB Wireless Deployment – Architecture and Best Practices

CURWB L2 Fluidity – Network Zones

Vehicle Mobility Network

The vehicle mobility network comprises of vehicles installed with either a single or dual CURWB radios on board. The onboard radios connect wirelessly to the Access Network radios and perform handoffs as the vehicle moves about the terminal. Some of the larger vehicles have a ruggedized Cisco IE3x00 switch on board. Each vehicle has an onboard ruggedized tablet for TOS which is either connected wired directly to the second port of the CURWB radio, or to one of the switchports on the IE3x00 switch, if there is a switch on board the vehicle. VLAN tagging if needed can be done on the CURWB radio in the absence of an onboard switch, however there is a limitation that only one client VLAN tagging can be supported.

Vehicle Radio Deployment

All mobile units in a terminal are called ‘Vehicles’ and make up the Vehicle Mobility network.

Typical vehicles in a container terminal include STS cranes, reach stackers, terminal tractors, straddle carriers, and RTG cranes.

A vehicle mobility network can be equipped with:

- Single radio (no redundancy) or dual radios (hardware redundancy and fast-failover with TITAN plug-in)
- Omni-directional or directional antennas, depending on operational area, angle of movement of the vehicle and the type of application running on the vehicle.

Figure 30 Vehicle onboard radio deployment examples

Access Network

The access layer network consists of:

- CURWB access radios installed on HMLPs to provide wireless coverage to low height ground vehicles which move around the terminal.
- CURWB access radios installed on HMLPs to provide wireless coverage to high height STS/Quay cranes.

Note: It is mandatory that all infrastructure radios need to be connected to the infrastructure backbone network using either a wired or wireless backhaul link.

In both of the deployment scenarios listed above the pre-dominant antenna type used is the 90-degree horn antenna. In the first scenario providing RF coverage for lower height ground vehicles which move about the entire terminal and in between piles of high containers, the 90-degree horn antenna is tilted towards the ground providing coverage in the
aisles created by the high metal containers stacked one above the other. In the second scenario the 90-degree Horn antenna for the access radio is pointed directly towards the 90-degree horn antenna for the vehicle radio installed on the STS/Quay crane.

Note: As all STS/Quay cranes are higher than the HMLPs it is highly recommended that the STS/Quay cranes network be separate from the rest of the wireless network and is deployed on a separate channel.

**CURWB Fixed Infrastructure - Wireless Backhaul**

When fiber is not available at a light pole for the access radios, it is recommended to request the fiber be installed to maintain the highest throughput and lowest latency. If this is not an option and the throughput and latency requirements are minimal, CURWB radios can be deployed as a fixed infrastructure. In this configuration, it is recommended that a radio be installed at a pole with fiber connectivity and the wirelessly connected poles are no more than 1 radio hop away.

When deployed alongside L2 Fluidity, the radios should be configured as mesh points with the same passphrase as the mesh end deployed for Fluidity. Bridge mode can also be used if a small number of poles need a wireless backhaul connection. Bridge mode is a variation on point to point in that the radios do not use MPLS encapsulation and cannot be expanded into a multipoint configuration. Because of this limited flexibility, mesh point is the preferred method over bridge mode. It is important to remember to use different frequencies for the fixed infrastructure radios which do not overlap with the access radios. Examples of both a point-to-point and a point-to-multipoint deployment are depicted below.

When a wireless backhaul is used for an access radio that does not have fiber connectivity, the access radio and the backhaul radio need to be connected back to back using the LAN2 ports. If using POE injectors to power-up the radios, the LAN1 port on the POE injectors can be used to connect the two radios to each other. On the CURWB radios both LAN1 and LAN2 ports are bridged together so the radios can be connected back to back using any of the ports. In certain scenarios it might be possible that there would be a switch on the HMLP but there is no fiber connectivity from the pole to the core network.

**Figure 31 Example of PtP and PtMP Wireless Backhaul**

*Note:* In order to avoid RF interference and high channel utilization, it is mandatory to select a different non-overlapping RF channel for each of the wireless backhaul link (unless they are really far apart and cannot interfere with each other). Also, the RF channel(s) used for the fixed infrastructure should be different compared to the RF channel used within the access layer.
VLAN Design

On the CURWB radios, VLAN support is provided by an optional plug-in. Installing and enabling the VLAN plug-in is recommended to control how tagged and untagged traffic is propagated through the network. When enabled, two VLANs are configurable in the radio user interface, one for management and the other for the native traffic. The management VLAN is used for control plane communication between the radios. The native VLAN determines how untagged traffic will be tagged as it passes through the radio. Setting the native VLAN to 0 is a special case where all untagged traffic is dropped and only tagged traffic can pass.

The ability to control the VLAN tags is important in the ports and terminal context because a radio may not always be connected to a managed switch with the ability to segment traffic into different VLANs. In this scenario, all end device traffic would normally be untagged when put onto the switched network. The fiber connected radio could be installed on an access port, but this would force all untagged traffic into a single VLAN. Using the CURWB solution, any radio connected to an end device could configure a native VLAN matching the type of device connected. For instance, if a crane has numerous devices segmented behind a network switch using multiple VLANs, the radio connected to that switch will pass the traffic without modifying the VLANs. If another vehicle has one of those devices connected directly to a radio, the native VLAN can be used to put that untagged traffic into the correct VLAN to maintain consistency on the switched network. Because the native VLAN is for untagged traffic, using different native VLANs on the Mesh Points from the Mesh End will enable the initially untagged traffic to exit the Mesh End with the VLAN intact. See below for examples showing this behavior.

Figure 32  Same Native VLAN on Mesh Point and Mesh End

It is recommended to use a native VLAN on the mesh end that is not used for any other traffic in the network. This will enable the mesh point to control which VLAN the connected device is placed into.

When installing a switch behind a CURWB radio, the interface connected to the radio should be in trunk mode. The native VLAN on the switch should also match the native VLAN on the radio for consistency. In this scenario, the switch ports are configured for the correct VLANs necessary for the end devices and all traffic will be tagged or untagged by the switch.
QoS

CURWB implements DiffServ inspired QoS to provide end to end classification of user traffic. When enabled, the CURWB radio will inspect every packet and look for DSCP or COS markings. This value is then translated into 1 of 8 priority levels based on that marking. When the traffic is transmitted over the wireless interface, the eight priority levels are further mapped into four access categories based on IEEE 802.11e as seen below.

Note: CURWB radios cannot perform any QoS marking. The radios only inspect the user traffic QoS marking and schedule based on those values.

Table 5  Mapping between packet priority and Access Category

<table>
<thead>
<tr>
<th>Priority</th>
<th>Access Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>BEST EFFORT (BE)</td>
</tr>
<tr>
<td>1</td>
<td>BACKGROUND (BK)</td>
</tr>
<tr>
<td>2</td>
<td>BACKGROUND (BK)</td>
</tr>
<tr>
<td>3</td>
<td>BEST EFFORT (BE)</td>
</tr>
<tr>
<td>4</td>
<td>VIDEO (VI)</td>
</tr>
<tr>
<td>5</td>
<td>VIDEO (VI)</td>
</tr>
<tr>
<td>6</td>
<td>VOICE (VO)</td>
</tr>
<tr>
<td>7</td>
<td>VOICE (VO)</td>
</tr>
</tbody>
</table>

It is highly recommended that if the wireless network has been deployed to enable TOS application, then only TOS traffic should be transported over the CURWB wireless network. If there is a need to transfer other traffic over the CURWB wireless network, then ensure that the TOS traffic is marked with the highest priority so that it gets preference over all other traffic contending for the CURWB resources.

For vehicles that have the Cisco IE3x00 switches on board, the switch should perform the QoS classification and marking closest to the edge device and scheduling on the port facing the CURWB radio. For vehicles that do not have a switch on board to classify and tag traffic with QoS, the radio’s native VLAN can be used to identify and tag with QoS on the northbound access radio switch.

Cisco IE3x00 QoS

The Cisco IE3x00 switch supports Quality of Service (QoS) which allows a certain type of traffic to be treated differently at the expense of others, so the performance of high priority traffic such as TOS can be assured. Classification and marking are the first steps to implement QoS. Classification differentiates traffic type by examining the packet header. A packet can be classified based on the DSCP, the COS, and the IP precedence value in the header. It can also be classified with VLAN ID and Access control list (ACL).

Classification and marking are recommended at the entry point of the network. After the traffic is classified, certain QoS features can be applied in the policy map depending on the ingress or egress direction of the traffic. In the case of input policy applied to ingress traffic, the IE3x00 can be configured either to trust the marking from the client device or set it to a different value based on business requirements; for output policy that is applied to egress traffic, you can assign a percentage of bandwidth, shape transmission to certain rate, or set a queue-limit for specific traffic type. IE3x00 supports multiple queueing models such as class-based weighted fair queuing (CBWFQ), and priority queuing. CBWFQ is recommended in this solution to allocate a percentage of bandwidth for a specific application.

For vehicles that have a Cisco IE3x00 switch on board it is advisable to mark egress TOS traffic originating from the vehicle to the control room with the highest priority so that it gets precedence over all other kinds of traffic.
Security - AES Encryption

All client traffic within the MPLS tunnel is kept private using the system passphrase, however for additional security the CURWB solution also supports enabling AES encryption to encrypt all traffic over the wireless medium.

Note: To enable AES encryption feature, an AES plug-in needs to be installed on the radio. When configuring AES encryption it is mandatory to enable AES encryption on all the radios within the system. Enabling AES only for a sub-section of the system is not supported and will cause a breakage.

CURWB for TOS Reference Architecture

Based on the reference architecture above the figure below depicts a reference architecture that can be used to support TOS.

As can be seen in the figure below, the design consists of the FM4500 radios installed on HMLPs, each HMLP consists of an IE3x00 switch that provides PoE+ power to the FM4500 radio and also provides fiber connectivity to the backbone network. The FM4500 radios installed on the HMLPs provide RF coverage to the different ground vehicles as well as the RTG cranes. Depending on the vehicle density and the amount of traffic traversing the wireless system along with TOS application traffic, either a single frequency design can be used for a small deployment or a dual/multi-frequency design can be used for larger ports with a high vehicle density.

On the smaller ground vehicles an FM4500 radio is installed with the Omni-5-Kit consisting of one horizontally polarized and one vertically polarized antenna. There is no need for an IE3x00 switch to be installed on the smaller vehicles. Hence the TOS tablet is directly plugged into the second port of the FM4500 radio using an RJ-45-to-M12 cable. Also, since there is no IE3x00 switch on board to provide PoE+ power to radio, the radio can be powered using either DC power or a low-input power injector.

On the larger vehicles such as RTGs, there can either be a single or dual FM4500 radio deployment with the Omni-5-Kit antenna. The RTG has an IE3x00 switch installed on board which can provide PoE+ power to the radio(s). Also, in this case the TOS tablet can be connected to the switch.

Note: The FM3500 radios can also be used on board the RTGs and cranes since the vibration is low and these vehicles move slowly and PoE power is available. Depending on the movement of the RTG, in some ports RTGs only move in the left and right direction so do not make 360-degree turns (especially within Tele-Remote and Automation applications), it is better to go with directional antennas, since having omni-directional antennas adds more interference.

Note: It is recommended to install the Cisco IE3400 on all ports and terminal vehicles that have a PLC on-board. This provides the ability to run the Cyber Vision sensor natively on the IE3400 to provide visibility into the PLC communication traffic and detect any anomalous behavior.
All the traffic from the vehicle to the control room gets encapsulated within the MPLS overlay network and terminates on a redundant pair of FM1000/FM10000 gateways. MPLS encapsulated traffic coming from the vehicles terminates on the FM1000/FM10000 gateway which de-encapsulates MPLS and drops the standard Ethernet frame onto the CAT-9300 switch for northbound travel. For traffic going towards the vehicle network, the FM1000 acts as the default gateway. It receives all traffic destined towards the vehicles, encapsulates the packets within MPLS and sends it towards the intended vehicle.

The TOS Application Server, the Cyber Vision Center server, and the FM-Monitor CURWB monitoring application are located in the central control room.

Within a L2 Fluidity deployment all the infrastructure and vehicle radios are part of the same VLAN / subnet (L2 domain). The TOS application traffic is segmented onto a different subnet / VLAN.

The centralized FM-Monitor server located in the control room can be used for monitoring and troubleshooting of the entire CURWB deployment from a single place. It depicts which vehicle is connected to which infrastructure AP providing information around all the key wireless KPIs (RSSI, SNR, PER, LER, MCS Rate, Throughput, etc.).
Ports and Terminals - RF Planning, Design, and Installation

Wireless Site Survey

A wireless radio frequency (RF) site survey is highly recommended before the permanent installation of any radio equipment. The purpose of an RF site survey is to conduct a detailed engineering study to create a competent wireless network design that, once installed, will address the needs of the individual use cases that have been identified for a particular operating environment. At the same time, the site survey gathers site-specific information that will aid in the installation of support infrastructure such as network and RF cabling, electrical, antenna selection and mounting, and AP hardware installation needs.

A proper site survey involves the temporary setup of a suitable AP and antenna combinations in specific static locations to test and measure the RF propagation characteristics within a given environment or area. Several parameters and key metrics are collected during the wireless survey, such as overall coverage area, signal strength and quality, supported data rates, signal overlap, potential sources and existence of RFI/EMI, and environmental conditions that can impact RF behavior and performance. This data is then analyzed to determine the correct hardware, antennas and install locations before undertaking the larger project costs of drilling holes, routing cables and conduit, and mounting equipment.

Without a proper RF site survey or wireless design study, the equipment might be installed in sub-optimal locations. Not only could this greatly reduce equipment performance, resulting in coverage gaps and therefore application issues, the resolution to such a scenario would require additional time and engineering resources to identify and address any coverage gaps. This leads to an increase in overall project costs, prolonged project timelines, unplanned downtime and disruptions to production, which would more than likely far outweigh the cost of simply conducting a proper RF site survey.

Pre-Survey Data Collection

Prior to conducting a site survey, it is imperative the RF engineer ascertains the customer’s requirements. This step ensures the applications and use cases that ultimately need to be supported by the wireless deployment are well understood. Integrating these requirements into the survey process ensures that the resultant design accommodates the proposed performance criteria as stated by the customer’s equipment and application vendors.

Requirements Gathering Process and Key considerations:

- Map of the terminal with locations of all HMLPs with fiber drops
- Map of terminal showing the types of vehicles (along with their height) and their operating locations.
- Type of light poles: It is critical to understand what type of light poles are available in the terminal to select proper antennas for different type of vehicles to provide best coverage. Can any equipment be installed in the middle of the light pole or does it have to be on top of the pole? Any other mounting restrictions?
- Application Requirements (Latency, Jitter, Packet Loss, Out-of-Order Packets). The types of traffic that will traverse the wireless network need to be known. For example, if the wireless network is primarily being designed for TOS traffic, will there be any other traffic other than TOS that will use the same wireless infrastructure?
- Bandwidth requirements for the applications (TOS, OCR, AGVs/IGVs, Tele-Remote, etc.)
- Location and concentration of vehicles (RTGs, STSs, Reach Stackers, Ground Vehicles) requiring wireless connectivity
- Specific areas that require wireless coverage to support specific applications, as well as areas that do not require coverage
- Contiguous RF coverage to facilitate fast roam times to support real-time applications
- Support for future applications (excess capacity and performance)
RF Site Survey

A thorough RF site survey consists of multiple activities in order to achieve the desired outcome. One, as mentioned previously, is the actual site survey activity, which involves the placement of APs in different locations within a defined area, in order to understand RF coverage and potential performance characteristics. Another is an RF spectrum analysis. While it is imperative to validate that the wireless design and the resultant deployment are capable of meeting the application requirements, it is equally important to understand what other RF devices might be operating in close proximity that can end up adversely impacting the wireless deployment.

Figure 34  RF Site Survey to ascertain any wireless coverage gaps

RF Spectrum Analysis

A RF spectrum analysis is used to thoroughly inspect the localized radio spectrum. This analysis is commonly conducted to identify sources of radio frequency interference (RFI) where suspected communication interference can be of concern. The analysis data can be helpful for equipment channelization and interference avoidance.

The principal goal of a spectral analysis is to search for and locate potential sources of RF interference and to find clean RF channels that can be used for the CURWB deployment.

If the terminal is not new and there is already a wireless system operating, one could consider blocking the 5 GHz bands from the old wireless system before doing the site survey and spectrum analysis.

An RF spectrum analysis needs to be performed at the very beginning of the project to help determine which clean frequencies/ channels are available in the port/terminal. An estimate of the application throughput is needed and the vehicle density is also extremely useful in order to select an appropriate channel width. It is also important to determine the exact frequencies/channels and channel width since this information needs to be provided within the RACER configuration templates to configure the radios.
A spectrum analysis should be performed multiple times at various operational times of a day or week. What is often overlooked are the incoming trucks having cellular hotspots, where they turn on Wi-Fi to connect to wireless devices inside each truck. Experience shows, frequency usage will vary throughout a standard operational day. It is for this reason why a professional spectrum analyzer is recommended, as it can be setup to scan over a period of time, whereas a radio scan is a one-time scan thus requiring multiple manual scans.

In addition to the initial RF analysis at the beginning of the project, it is also recommended to install a few FM3200 Radios for permanent RF analysis in multiple locations within the port/terminal. These units are located to run spectral analysis whenever the System Administrator wants to have an idea of APs operating in different frequencies in the area. FM3200Es with the FM-OMNI-5-KIT antennas are the best choice, as they help collect 360 degrees worth of RF data. Note that the FM4500 radio does not have spectrum scan capability.

Implementation Considerations

As already mentioned, many factors should be considered when designing and deploying a wireless network. Each of the topics listed below has a unique ability to impact wireless communications and must be considered or uncovered during the site survey and installation process. Ultimately, these considerations and their handling need to harmonize with the overall solution requirements. This will provide more assurances that both the design and subsequent resulting deployment will be able to meet service level expectations and application requirements.

Common RF Installation Considerations

- Fresnel zone
- Knife-edge diffraction
- Obstruction shadowing
- Environmental attenuation
- Reflection and scattering
- Multipath - Multipath is a 100% guarantee in Container terminals, due to the large steel walls of container stacks going up and down daily.
- Delay spread values
- Antenna polarization, isolation
- Reactive near-field, Radiating near-field
- In-band RFI and out-of-band RFI / Harmonics
- EMI
- RF Noise floor
- Equipment specifications
- Antenna field of view
- Antenna E and H planes
- Antenna Type (Omni-directional, Directional - Sector, 30/60/90-deg Horn, Panel, etc.)
- Antenna Gain
- Antenna Beamwidth
- Antenna Horizontal / Vertical Polarization
Survey characteristics:

- Coverage
- RSSI
- SNR
- Data rate
- Retries/loss
- Overlap/redundancy
- Required Infrastructure
- High installation costs

RF Planning

During high-level frequency planning for the port or terminal site, it may be decided that part or all of the system may use only a single radio channel or may use two or more radio channels. These stipulations will be based on connectivity needs and the result of spectral analysis of the port environment.

The minimum-height value assumes that there are no obstacles in the Fresnel zone, and that the link is parallel to a flat surface, like the sea. If there are obstacles in the middle of the Fresnel zone, such as trees or buildings, you will need to add the height of the obstacles to the antenna’s minimum height.

For TOS application within ports, three different types of vehicles and their RF coverage need to be considered:

- Small vehicles operating at ~2 meter/7 feet height such as Terminal Tractors and Reach Stackers
- RTGs operating at a height of ~25 meters/82 feet

Tall STS/Quay cranes with an ~ height of 40 meters/131 feet where-in the antennas can be installed at different locations either on the legs of the crane or on top of the crane. It is important to note that the height of installation of the antennas must be above the maximum height of the container stacks within the terminal.

Align each antenna with care, referring to the link profile diagrams that were generated during high-level system design. Always maintain clear line-of-sight, making sure there are no physical obstacles, especially metallic obstacles, between radios that are connected using a wireless peer link. Be aware that at least 60% of the Fresnel zone between the two radios must be clear and free of any physical obstacles.
As a best practice it is recommended to order 3% additional radios of each model of radio used within the deployment as spares. Ensure to order the corresponding plug-ins. This will help in instant replacement of a failed device to ensure continuity of business operations with the port/terminal, rather than wait for the RMA replacement to arrive.

DFS Considerations

Dynamic Frequency Selection (DFS) is a reserved services detection and avoidance function where select 5 GHz frequencies are scanned for generally reserved radar, satellite and weather radar. DFS is a major concern within any ports/terminals deployment. The DFS operation within CURWB is different from typical Wi-Fi deployments. While Wi-Fi based solutions use multiple channels dynamically within the entire port including DFS frequencies (if selected within the controller), CURWB uses fixed channels with minimum use of spectrum to deploy critical applications. Deploying CURWB using multiple channels is possible (Vehicle radios configured in auto-scanning mode) and if only one of the Infrastructure radios (there is no capability for vehicle radios to detect DFS) operating in the DFS frequency band detects the radar signal, only that particular radio (even if other infrastructure radios are configured within the DFS range) will disable itself for 30-min and the other radios which have not detected the radar signal will keep operating normally.

Post Installation: RF Tuning and Optimization

While the output from the survey work is critical for the planning and design phase of a project, there is still additional work that needs to be performed, post-deployment and installation. To validate the installed solution aligns with the specifications of the design, and meets application requirements, it is necessary to conduct another survey once the wireless equipment has been deployed within the port/terminal. This validation may be done over time in phases, which align with a phased construction and implementation schedule. However, the fundamental purpose is to conduct an RF survey, using previously described tools and techniques, to tune and optimize the wireless system, ensuring it provides the necessary coverage and meets the design requirements. Due to the dynamic nature of a container terminal, RF tuning is an ongoing requirement and cannot be ignored.

Ports and Terminals specific RF considerations

In the case of a new greenfield port, the initial site survey and installation might have been done with a few or not many stacks of containers at the port. As the port starts getting busy, loads of containers and vehicles might block the RF LoS and Fresnel zone. An area which previously had good RSSI might now have become an RF dead zone due to a stack of tall containers in between the area and the access radio. Therefore, it would be prudent to re-do the RF site-survey and adjust the following to address any gaps in RF coverage:


- Number and location of infrastructure radios
- Might need to add some additional radios to provide coverage to RF dead zones due to a new obstruction that popped up
- Infrastructure Radio/antenna placements, height, direction, angle, power, gain
- Vehicle Radio/antenna height, power, gain

The port needs to be designed in a way that loads of container should not have an effect on the RF. The RTGs and STS cranes always operate above maximum container stack height, so all antennas are going to be installed above the maximum container stack height. For small vehicles as mentioned before one could consider the maximum container stack of the terminal and make sure all antennas are above that level. Also ensure the alignment of antennas is proper and covering the interested area.

Ports and Terminals are very dynamic environments, the RF environment can change quite a bit from day-to-day. For existing brownfield ports it is recommended to take at least a couple site-surveys on different days and times to assess any gaps in RF coverage due to the dynamic nature of the RF environment at a port. Again, any coverage gaps can be addressed by modifying a few or all of the items in the list above.

After the design phase and deploying the system, further testing and heat map generation should occur. Based on the results further tuning should happen. The tuning steps are as follows:

1. Add more radios to locations with poor performance (Some radios need to be kept to add to system in this step)
2. Align the antennas if the RSSI level is lower than expected
3. Implement Static Multi-frequency and load balance vehicles across different frequencies if congestion is more than expected (or increase the channel width on system).

Terminal Map with Locations of all HMLPs with Fiber Connectivity

The figure below depicts a typical comprehensive map of a container terminal showing the locations of all available HMLPs equipped with fiber drops. Remember, the greater the number of available fiber drops, the smaller the number of radio-based backbone links that will be needed.
Type of Light-Pole

It is important to evaluate what kind of light poles are available within the terminal. Most terminals usually have circular light poles on which nothing can be installed on the pole itself. Radios can only be installed on the very top of the HMLP on a circular metal rod. These kind of light poles have the possibility to install the radios/antennas at 35 meter (115 feet) height. Different sets of radios/antennas are used here, one providing coverage to the high STS/Quay cranes and the second radio/directional antenna pointing down toward the lower ground vehicles.
The second type of light pole seen within the ports/terminals is a tower where one has the ability to install radios/antennas at various heights providing deployment flexibility. On such types of light poles one set of radio/antenna can be installed at a height of ~ 3–4 meters/10–13 feet to cater to smaller height vehicles such as Terminal Tractors (TTs) and Reach Stackers (RSs). The next set of radio/antenna can be installed at ~ 25 meter/82 feet height to cater to RTGs. The third set of radio/antenna can be installed at a height of ~ 40–46 meters/130–150 feet to provide coverage to STS/Quay-crane.
Providing Wi-Fi Connectivity within Ports

There are some areas within a port/terminal where Wi-Fi connectivity for hand-held devices needs to be provided. For e.g. under STS cranes there are some workers with a tablet in hand working and they need Wi-Fi connectivity for their tablets. In this case service cars can be used. The service cars are the port/terminal’s normal vehicles that are equipped with a CURWB radio operating in the 5 GHz spectrum and a Cisco Wi-Fi access point operating in 2.4 GHz spectrum. These service cars can move anywhere within the port/terminal and provide WiFi connectivity when there is need.

Another deployment option is to use Cisco Wi-Fi access points operating in 2.4 GHz spectrum installed in a fixed location using CURWB fixed infrastructure to backhaul the Wi-Fi traffic.

Radio Density based RF Planning

Due to their requirement for uninterrupted connectivity, a multi-frequency setup may be required for TTs and RSs in scenarios with a high vehicle density. The figure above depicts an example CURWB multi-frequency deployment at a Port/Terminal in order to support a high density of TTs and RSs.

Radio Location and Antenna Type

Pay close attention to the topography of the port or terminal site. Which areas are likely to cause line-of-sight issues or radio reflections? Are there any known ‘dead zones’ on the site? These factors will have a direct influence on the selection of omni-directional and unidirectional antennas at every point in the backbone and access networks.
The above figure depicts an example multi-frequency CRUWB deployment to enable TOS. The green radios are configured to operate on Freq-A and the red radios are configured to operate on Freq-B. The green radios provide coverage to the RTGs and TTs. The red radios provide coverage to the STS/Quay cranes. Since the height of the...
RTGs/TTs is much lower than the height at which the green radios are installed, the Horn-90 directional antennas are pointed downwards to provide appropriate coverage. The Horn-90 directional antenna for the red radios are pointed towards the radios installed on the STS/Quay-crane.

Because RTGs and TTs typically move all around the port, make turns and potentially move around 360-degrees, they are installed with omni-directional antennas. The STS/Quay cranes are deployed with the Horn-90 directional antennas directed toward the red infrastructure radios.

The solution is deployed in a manner where redundant coverage is provided across the entire port in case of a failure of any one of the infrastructure radios. For example, the red radio on HMLP-1 provides coverage to STS-1. In the event of failure of the red radio on HMLP-1, the red radio on HMLP-2 will provide adequate coverage to STS-1. The same concept of overlapping coverage applies to the green radios providing coverage to the RTGs/TTs. The green radio on HMLP-5 provides coverage down the entire aisle all the way until HMLP-8. Similarly, the green radio on HMLP-8 provides coverage down the entire aisle all the way until HMLP-5. So they act as backup radios to each other. If any one of them at either end of the aisles fail, the radio at the other end of the aisle still provides adequate coverage for the entire aisle.

For small ports having low vehicle density (< 50 vehicles) a single-frequency deployment model can be adopted where all the radios can be configured to operate on a single frequency. For large ports having high vehicle density (> 200 vehicles), an additional infrastructure radio can be installed and configured to operate on a third frequency (Freq-C) to dedicate a separate set of radios providing coverage to RTGs vs. TTs. This helps reduce the co-channel interference and channel utilization on each of the frequencies.

CURWB Radio and Antenna Installation Best Practices

Access Radio Installation

FM-Shield Ruggedized Enclosure

The FM-SHIELD is a proprietary ruggedized enclosure designed to ensure long-term durability and reliability of radios that are installed in outdoor environments.

If a 3200-series, 3500 ENDO, 4200-series or 4500-series radio is installed in outdoor conditions, it is compulsory to install the radio inside an FM-SHIELD. It provides additional protection from impact, salt air, and water.

FM-Shield Features:

- Steel protective enclosure with Polycarbonate cover, designed to protect against high-pressure water spray and impacts from heavy, fast-moving objects
- Proven in high-vibration environments, including all vehicles operated in a terminal environment
- N-Female antenna connectors for easy integration, and minimal RF signal loss
- Designed for installation within automation cabinets, and on vehicle hand railings, antenna poles, and can be installed in either a horizontal or vertical position, while maintaining a vertical position of the radio
- Semi-transparent front panel with self-retaining screws for easy inspection
Access Radio Antenna Types and Application

It is worth examining the roles of different antennas in Access networks and Mobility networks.

Within an Access network:

Omni-directional antennas are well-suited for:

- TOS and other applications with modest bandwidth needs
- For vehicles that change their orientation through 360°
Directional antennas are well-suited for:

- OCR, automation, and other applications needing greater connection reliability and hence reduced interference
- Applications in which the network may be vulnerable to radio interference, and in areas with relatively high levels of congestion across the radio-frequency spectrum
- On vehicles that do not move 360-degrees (e.g. for STS/Quay Cranes)
- Longer distance focused coverage
- Areas where omni-directional antennas might cause radio interference

It is worth noting that ports and terminals are usually located within short distances of major population centers. For this reason, they typically feature higher levels of activity across all parts of the radio spectrum. For this reason, the available RF spectrum within a port or terminal may be somewhat limited.

Access Radio Deployment using 90-degree Horn Antennas

Access radios within a Ports and Terminals deployment are typically mounted on HMLPs. HMLPs with fiber connectivity are always preferred over HMLPs with no fiber connectivity. In the event where certain HLMPs have no fiber connectivity the design can incorporate having a wireless backhaul link.

The areas within the terminal that need uninterrupted radio coverage depend on what is taking place in each relevant area. To establish whether uninterrupted radio coverage can be applied from a suitable height above the ground, a comprehensive map of the terminal showing the location and height of all available light poles and which of the poles have fiber drop links nearby is needed. Also information about the expected locations where vehicles will be moving and need coverage, the number and types of moving vehicles that need connectivity is also required. Also bear in mind, the greater the number of available fiber drop links, the smaller the number of wireless backbone links that will be needed.

To ensure a proper design, data on the height of each vehicle must be taken into consideration. It will help determine at what height the access radio should be installed, which type of antenna(s) to select, and at what angle the antennas need to be tilted.

Access radios can use one of two 90-degree Horn Antenna configurations:

Radio with one antenna design - offers long-range coverage in the intended direction

Radio with dual antenna design - offers coverage in two directions but divides the overall transmission power of the radio between the two antennas. This design involves inserting 2 x splitters in between the radio unit and the horn antennas, resulting in a 3-dB insertion loss.

90-deg horn antennas are the preferred antenna type to use within a ports and terminal deployment due to their appropriate 90-deg horizontal and vertical beamwidth. These antennas can be tilted downwards to provide appropriate coverage within the aisles formed by the tall stacks of containers. One radio with a 90-deg horn antenna tilted downwards can be installed at an approximate height of 15-meters/50-feet to provide coverage to ground vehicles moving about the port. A second radio with a 90-deg horn antenna can be installed higher at an approximate height of 23-meters/75-feet to provide coverage to RTG cranes which have a significantly higher height compared to ground vehicles like TTs or RSs. Note that installing radios/antennas at different heights is not possible on HMLPs where equipment can only be installed on the metal ring at the very top of the pole (~ 35-meters or 115-feet).
In a scenario where the same radio needs to cover two 90-degree sectors, the radio can connect to two horn antennas. However, in order to achieve this, splitters need to be installed between the radio unit and the antennas. With this design, a cumulative coverage that is 180-deg wide is provided as opposed to 90-deg wide when using a single horn antenna. However, since the signal is divided between two antennas, the signal emanating from any one of the antennas is only half as powerful and hence does not travel as far. Also, note that the splitters introduce a 3.8 dB insertion loss. In summary this design provides double the coverage angle at less than half the distance as compared to using a single horn antenna.
The above figure depicts an example deployment of dual-radios on board an STS/Quay-crane to provide redundancy at the mobility layer on board the vehicle. In this case, the HORN-90 directional antenna associated with each of the onboard radios is pointing toward two separate infrastructure radios on neighboring HMLPs. This deployment model serves the dual purpose of providing hardware redundancy on board the vehicle as well as redundant coverage from two different infrastructure radios providing resiliency against HMLP power failure or fiber link breakage.

Dual Horn Antenna Cabling for FM3500/4500 Access Radio

The image below demonstrates the correct horizontal and vertical transmission connections of a setup featuring a Single Access infrastructure radio, equipped with splitters and two horn-type antennas. The correct connections are essential to avoid cross-polarization, and consequent drops in network performance. Note the three different types of cable used in this installation.
NOTE: The radios do not have any knowledge about Horizontal (H) and Vertical (V). It is very important to ensure that the same order for the Horizontal and Vertical polarization is maintained across the entire deployment. If the right antenna port is selected as Horizontal and the left antenna port is selected as Vertical, this convention should be followed across all radios in a given deployment. If not, it will result in cross-polarization and signal degradation.

Vehicle Radio Installation

OMNI-5-KIT Antenna Cabling for FM4500 Vehicle Radio

The OMNI-5-KIT omni-directional antenna is recommended to be installed on ground vehicles as they are able to receive and send signal in all directions, and this functionality is needed as these vehicles move around the terminal and as the vehicle makes turns.

This image below depicts the cabling diagram for the OMNI-5-KIT containing 1 x horizontally polarized antenna and 1 x vertically polarized antenna to an FM4500 vehicle onboard radio. Note the three different types of cable used in this installation. The length of the RF cable from radio to antenna should not exceed 6ft if using an LMR240 size cable because too much loss would be introduced. It is recommended to use LMR400 for lengths longer than 6ft up to 30ft.

The FM4500 radio on board the vehicle can be powered up using either POE+ from an onboard switch if available or using a DC power-supply.
Note: The radios do not have any knowledge about Horizontal (H) and Vertical (V). It is very important to ensure that the same order for the Horizontal and Vertical polarization is maintained across the entire deployment. If the right antenna port is selected as Horizontal and the left antenna port is selected as Vertical this convention should be followed across all radios in a given deployment. If not it will result in cross-polarization and signal degradation.

Clear Line-of-Sight and Fresnel Zone

Below are examples where the LoS and Fresnel Zone have been blocked by other metal obstructions around the antenna. Keep in mind that unidirectional antennas can also suffer from line-of-sight and Fresnel zone blockages. Careful planning and logistics are needed to ensure that antennas are placed high enough to avoid any blockages.
Always take care to install each individual antenna in a way that takes full advantage of its radiation propagation pattern. This requires one to know the differences between each type of antenna within each given antenna category. On some light poles, you may need accessories to mount antennas high or low enough to clear all obstacles that may interfere with the LoS.

Do not install downward-facing antennas above lights, as the lights will more than likely present physical obstacles to beam propagation. In these cases, it may be better to sacrifice a meter or two of height, to guarantee freedom from line-of-sight blockages.
To avoid co-location interference, avoid installing radios and antennas close to any other wireless equipment, even if the other equipment operates on frequencies that are different to the CURWB equipment.
Figure 49  Roll-out (Best-Practices): Avoid proximity to other wireless gear
Glossary of Terms

AGV – Automated Guided Vehicle
AIDC – Automatic Identification and Data Collection
AutoSC – Auto Straddle Carrier
CRD – Cisco Reference Design
CPT – Connected Ports and Terminals
HMI – Human Machine Interface
HMLP – High Mast Lamp Pole
IP – Internet Protocol
IT – Information Technology
LoS – Line of Sight
MPLS – Multi-Protocol Label Switching
OCR – Optical Character Recognition
OT – Operations Technology
PtP – Point-to-Point
PtMP – Point-to-Multi-Point
RCS – Remote Control Station
RMG – Rail-mounted Gantry Crane
ROC – Remote Operations Center
ROS – Remote Operations System
RTG – Rubber-tired Gantry Crane
RS – Reach Stacker
STS – Ship-to-Shore/Quay Crane
TT – Tractor Trailer
QoS – Quality of Service
VMT – Vehicle Mounted Terminal