White paper
Cisco public

Choose Wireless That Is the Best-Fit and Not a Force-Fit for Your Industrial Network

Contents

Executive summary

Historically, wireless technology in many industrial settings has been limited to less-than-critical sensing applications and connecting IT devices. With rapid digitization of industrial operations and ever-more-mobile applications, the need for high-throughput, scalable, reliable, broad wireless connectivity is rising. Wireless connectivity technologies have evolved to support bandwidth-intensive worker productivity applications, reliable mobility for critical assets, and increased data collection from all areas of the plant. All of which significantly boost operational efficiencies and production uptime.

Initially, wireless technologies were designed to serve specific market needs and offered distinct characteristics just for those use cases, such as ubiquitous connectivity for smart devices, cellular communications, wireless sensing applications, etc. That has changed significantly. Wireless technologies now support reliable low-latency communications, high throughput, and significantly increased density of devices. All of these are useful in many industrial scenarios.

Modern wireless technologies have radically increased the options for connecting devices and applications in industrial zones. In making their technology decisions, organizations must carefully consider different aspects of each technology in a context of end-to-end IP data flow and evaluate them in the organization's own specific use cases and deployment needs. It is important that they choose the technology best suited for their use case without making compromises on IP networking, cybersecurity, automation, and performance.

In this paper, we will focus on high-throughput, highly reliable technologies, namely Wi-Fi, 5G, and Cisco® Ultra Reliable Wireless Backhaul (URWB), as they could be valid alternatives in many use cases and making a clear differentiation between them is essential.

For each of the use cases in the selected industries, this paper describes the applicability of wireless and the use-case requirements that you need to consider choosing the right technology for the job. We do not discuss the architectural considerations in depth but provide references where you can find the details you need, and we present selection criteria that will help you make an informed decision for your circumstances and priorities.

Industrial use case summary

Industrial systems have long had a need for wireless networking to support mobile personnel and machinery and connect devices where cables are not a viable option. But as wireless technologies have advanced, the set of use cases for these technologies has also increased. The pandemic accelerated these trends, compelling many in the workforce to work remotely and heightening the demand for video collaboration, remote consulting, autonomous operations, and remote control, among other solutions.

Table 1. Industrial wireless use case summary

Industry	Representative use cases
Manufacturing	• Using Automated Guided Vehicles (AGVs), robots (AMRs), and other mobile equipment on the factory floor • Providing reliable voice, video, collaboration, and Augmented Reality and Virtual Reality (AR/VR) tools to the factory workforce • Controlling rotating and conveyance systems • Downloading software and data to manufactured products • Supporting mobile Human-Machine Interface devices (HMIs) and handheld tooling
Connected rail	• Communications-Based Train Control (CBTC) • Onboard connectivity (passenger Wi-Fi, workers' access to applications, live Closed-Circuit TV (CCTV), digital displays, Point Of Sale (POS) for onboard purchases, etc.) • Vehicle telemetry and real-time asset monitoring, including track infrastructure • Station passenger services such as Wi-Fi, wayfinding, and digital kiosks
Ports and terminals	• Connecting cranes and handling vehicles to Terminal Operating Systems (TOS) • Using tele-remote devices (Rubber-Tired Gantry (RTG), ship-to-shore, and quay cranes and straddle carriers) • Enabling autonomous operations (AGVs, AMRs, etc.) • Providing voice, video, and collaboration applications for terminal workers and visitors • Enabling port access control, traffic management, and video surveillance
Mining	• Connecting mining equipment and control systems • Enabling autonomous and teleremoten operation of mining equipment • Providing voice, video, and collaboration applications for mine workers • Providing access control and video surveillance
Oil and gas	• Monitoring remote operations equipment • Connecting and controlling midstream assets • Performing video surveillance in large, distributed sites
Connected communities (smart and safe cities)	• Connecting sensors that monitor conditions around the city such as public transport, traffic, etc. • Providing Wi-Fi access points in public areas such as parks, libraries, etc. • Installing CCTV for public safety • Providing short-term networking needs for special events

Wireless technology selection criteria

Unlike wired transport, which is for the most part quite uniform, wireless methodologies differ substantially from each other in their maturity, capabilities, and operational considerations. In this section we describe some of the criteria for selecting the right technology.

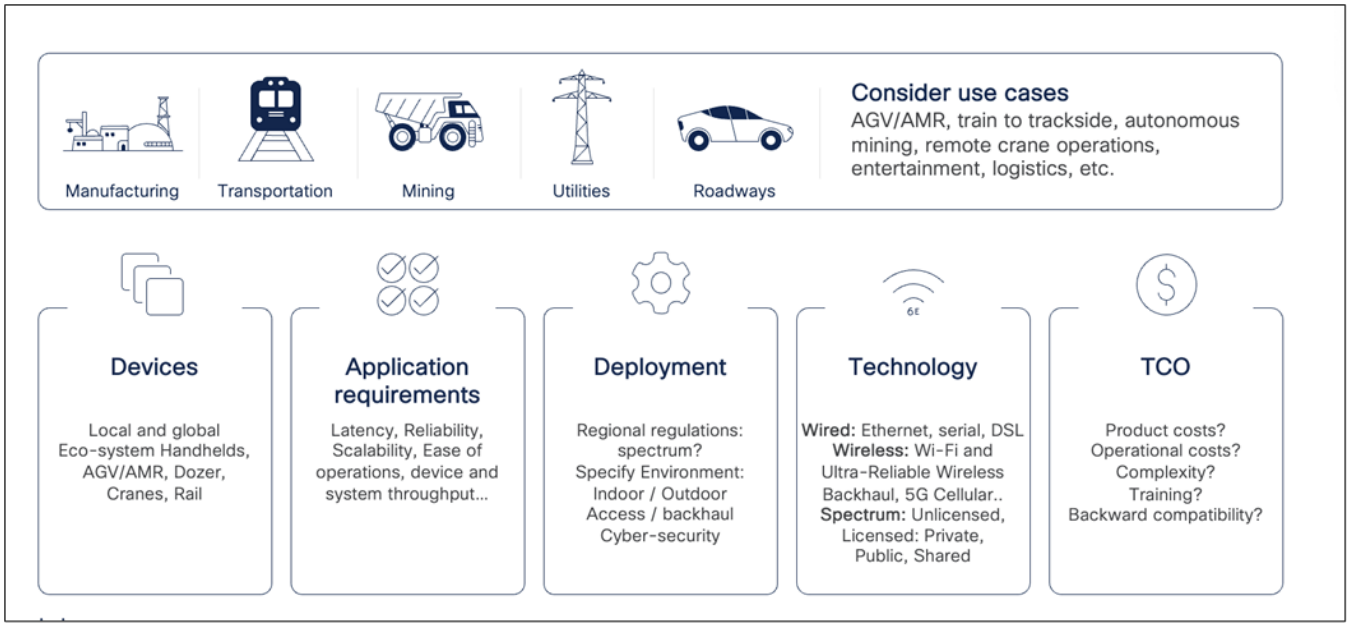

Figure 1.
Decision factors for selecting wireless technology.

Type of use case

Your choice of wireless will depend a great deal on the use case. The use case usually defines the throughput, location (e.g., indoors, or outdoors), resiliency, latency, range, and types of devices that need connectivity. Wireless may also be used to connect devices directly or to backhaul data from worksites, building, or vehicles. Getting a good understanding of these requirements will go a long way toward identifying the appropriate technology (or technologies).

Choice of spectrum

Spectrum refers to radio frequencies that wireless signals travel over. The portion of the total available spectrum used for wireless communication ranges from about 20 kHz to 300 GHz. The available spectrum for IP networking is usually broken down into three bands: low, mid, and high. Low-band spectrum (under 1 GHz) travels longer distances and can penetrate through obstructions but offers relatively low data speeds. High-band spectrum (above 7 GHz) travels much shorter distances but offers high capacity and ultra-fast speeds. Mid-band spectrum (between 1 and 7 GHz) blends the characteristics of both the low- and high-band spectrums, providing a mix of coverage and capacity. Additionally, some wireless technologies, such as 5G and Wi-Fi, operate in a range of spectrums, offering additional flexibility to meet requirements.

Spectrum can be licensed or unlicensed. Licensed spectrum is bought by and earmarked for exclusive use by specific providers in a given country or region. Unlicensed spectrum is open to use by anyone. Wi-Fi and Cisco URWB rely on unlicensed bands, whereas cellular technologies such as 4G and 5G generally operate in licensed bands. Licensing of spectrum is done by governments, and the frequencies and availability vary from country to country. The wireless provider for licensed frequencies must be certified for a wide range of spectrums. Unlicensed bands are available worldwide, but there may still be regulations that govern the maximum transmit power that can be used.

Coverage area, power considerations, and density

Wireless technologies differ in the area they cover, how much power they use, and the number of devices they can service. Cellular networks are built to cover large areas and dense deployments of users and are generally available countrywide, although they may provide the best service in urban areas. Wi-Fi networks are generally limited to service within buildings and surrounding outdoor areas, although hotspots are used to provide Wi-Fi access in many situations. But they also support dense deployments of users. The range of any wireless technology is dependent on the spectrum, with low-frequency spectrums having greater range than high-frequency spectrums.

Network resilience and performance

Your choice of technology should also be determined by the throughput you require. Streaming of several high-resolution video streams and AR/VR for remotely controlled operations require a low-latency, high-throughput network, whereas periodic text-based messages from sensors do not.

Resiliency is also an important consideration. Wireless technologies for mobile applications have enhancements to help users and devices maintain their connection while roaming. These include mechanisms to switch between access points quickly and seamlessly, as well as to maintain multiple connections and replicate packets to reduce or eliminate the loss of data. The use case usually defines the criticality of maintaining communications while roaming or moving.

In terms of availability and resiliency, an organization may prefer a network that it owns, operates, and controls, as it can more easily customize such a network to its unique requirements. If using a managed network, a Service-Level Agreement (SLA) should be defined and enforced with the service provider.

Cost of ownership and operations

Total cost of ownership of wireless includes the cost of equipment (and spectrum, if licensed) itself (CapEx), the cost of managing it (OpEx), and any licensing or subscription fees that need to be paid (if a service provider is involved). This is one of the biggest variables between many of the wireless technologies.

Overview of industrial wireless technologies

This section provides a comparison of wireless access methods to provide an understanding of the factors that are in play for selection purposes. It is possible that for certain deployments wireless may not be suitable. It is also possible that a mix of wired, and one or more wireless access technologies is the right answer for you.

Industrial Wi-Fi

In use for over two decades, Wi-Fi networks are now ubiquitously used to connect all sorts of enterprise and consumer devices, are inexpensive to provide, operate in the unlicensed spectrum, and are available almost anywhere in the world. The standards have been advancing rapidly.

Wi-Fi 6, and 6E, or IEEE 802.11ax, dramatically increase network capacity and bandwidth and reduce latency. In the new 6-GHz spectrum, Wi-Fi 6E offers additional bandwidth and less congestion. Wi-Fi 6 and 6E also improve battery efficiency offering power management features that are well suited for battery-operated devices. Their spectral efficiency allows dense deployments, and their Orthogonal Frequency-Division Multiple Access (OFDMA) feature allows devices to share the available channel bandwidth with other devices to increase overall capacity. Another advantage of Wi-Fi 6 and 6E is the strong Wi-Fi Protected Access 3 (WPA3) encryption it offers.

Wi-Fi 7, the latest release in Wi-Fi technology, is based on the IEEE 802.11be amendment, also known as Extremely High Throughput (EHT). Wi-Fi 7 doubles the channel width of the previous generation to 320 MHz and increases the modulation to 4K QAM (Quadrature Amplitude Modulation) to deliver higher data rates. It also introduces Multi-Link Operation (MLO), which allows clients to send traffic to the same access point on more than one band at a time, including 2.4 GHz, 5 GHz, and 6 GHz. This increases speed and reliability while reducing latency.

Presently, the Wi-Fi 7 client ecosystem is limited and will take a couple of years to mature. However, when a more significant number of clients supports Wi-Fi 7, more applications will emerge that require higher speed and lower latency.

For industrial applications, the benefits of Wi-Fi 7 at this point will be incremental compared to those of Wi-Fi 6E, as the most important requirement for industrial applications is reliability, not throughput.

Even though Wi-Fi operates in unlicensed bands, it is strictly regulated by countries. Local regulations define maximum power levels of access points to avoid interference between users. This in turn determines range, coverage, penetration, and signal strength. In high-density deployments where hundreds of user devices may be operating, or where there may be sources of electronic interference, more access points may be needed.

Wi-Fi is well suited to many industrial use cases and is a technology that numerous industrial companies have experience with. The market for Wi-Fi end devices is extremely mature and has been built into a huge range of industrial end devices.

Public and private 5G

5G wireless technology is designed to enhance the 4G LTE standard by delivering higher data speeds, lower latency, increased reliability and availability, better coverage, and higher device densities.

The 3rd Generation Partnership Project (3GPP) tries to address three facets of requirements when specifying 5G technology. 5G Massive Machine Type Communications (mMTC) connects low-powered IoT devices but is not well deployed at this time. 5G Enhanced Mobile Broadband (eMBB) supports bandwidth-driven use cases that require high data rates. This is the predominant version of 5G that is deployed. 5G Ultra-Reliable Low-Latency Communications (URLLC) is meant for real-time use cases.

5G has been touted as revolutionizing almost every aspect of IoT and Machine-To-Machine (M2M) communications in industries such as agriculture, shipping, logistics, autonomous driving, and manufacturing, among others, once it is deployed on a large scale and is ubiquitously available.

5G and Wi-Fi 6, 6E and 7 are sometimes called complementary solutions, in that both support dense IoT environments, high-bandwidth applications, and deployment at scale. It is envisioned that Wi-Fi, private 5G, and public 5G will work together for better connectivity indoors, plantwide, and worldwide, with each providing a similar quality of service across the board.

A private 5G network allows the organization to customize the network to its needs. Whereas the public 5G infrastructure might provide the same level of service to all transiting data and potentially expose the enterprise devices to the rest of the network, the organization can tailor its private 5G network so that it provides the desired level of speed, security, latency, coverage, bandwidth, range, and user experience. Private 5G may also integrate with the existing enterprise IT environment, making it seamless and easier to manage. However, while 5G is global when covering the mobile carrier market, it is not the same for a private environment. Depending on your location, you may or may not get private 5G services or establish roaming agreements with public mobile carriers. In addition, most organizations lack the expertise and experience to deploy and manage 4G/5G infrastructure and networks. Further, 5G end devices are limited primarily to smartphones and tablets and few industrial end devices are deployed with 5G due to cost and complexity.

New features and enhancements in 5G are expanding the value of what private cellular networks can support, including an additional focus on deploying private 5G as a LAN solution for industrial IoT use cases.

Despite all that is being promised for 5G, it is not a panacea for all industrial use cases. To fulfill high-bandwidth requirements, millimeter wavelengths are needed, which requires a larger array of antennas to provide coverage. Several of the industrial interest in 5G is based on the URLLC and mMTC varieties, that may not be options available in today's generation of products, or in all locations, which limits its use in industries such as mining or intercity rail transportation. Working in licensed bands, 5G is also subject to regulations, such as preemption for emergency needs (for example, FirstNet in the U.S.), etc.

Cisco Ultra-Reliable Wireless Backhaul

Cisco Ultra Reliable Wireless Backhaul (Cisco URWB) is a Wi-Fi technology extension designed to offer reliable wireless connectivity for mission-critical applications, whether they are stationary or mobile. URWB provides low-latency, highly reliable, long-range, and high-bandwidth connections that can handle endpoints moving at high speeds with zero-delay handoffs. URWB operates in unlicensed spectrum. and can be an excellent alternative to wired connectivity in industrial sites, campuses, or even cities.

Sharing the same technology underpinnings as Wi-Fi allows URWB to evolve alongside Wi-Fi. For example, Cisco URWB benefits from advances in data rate and additional spectrum in Wi-Fi 6 and 6E, and from further progress envisioned for W-Fi 7 and beyond.

URWB is especially suited for connections requiring fiber-like data rates where wired connectivity is not available or too costly. Use cases include Layer 2 connectivity to extend a single network between multiple locations a few miles apart, providing connectivity to moving vehicles, and meeting temporary connectivity needs.

As your own private wireless IP infrastructure, URWB offers several benefits:

- **Cost:** URWB operates on Wi-Fi frequencies, that is, in the unlicensed band, without having to purchase or pay for licensed spectrum. As a result, customers can leverage the entire 2.4-, 5-, and 6-GHz spectrum to benefit from high throughput without additional cost. This spectrum is unlicensed and available worldwide, with the same regulations as regular Wi-Fi.
- **Availability:** URWB is owned, deployed, and managed by the organization, which decides where to place antennas and what areas to cover. Radio planning is done specifically for the owner's use case, guaranteeing ideal coverage for the application and their specific environment.
- **Deployment:** URWB deploys similar to Wi-Fi, saving you time and costs associated with training your team. Because it is a native IP technology, it does not require any complex back-end system to connect it to your business applications and other IT resources. It is a proven Cisco solution that has been deployed in many large industrial organizations and critical infrastructures and is backed by extensive design and implementation guides.
- **Evolution:** URWB is built upon 802.11 technology and evolves alongside it. It takes advantage of the standard's inherent backward compatibility and can leverage advancements in future standards improvements as needed.
- **Reliability:** URWB's Cisco Multipath Operations (MPO) adds an additional level of reliability sending high-priority packets via redundant paths on uncorrelated frequencies at the same time to multiple access points. It can duplicate protected traffic up to eight times, exploiting time, spatial, and frequency diversity. This functionality, combined with cutting edge hardware capability, can further reduce latency and improve reliability, addressing both interference and hardware failures.

Industrial use cases for wireless

In this section, we discuss the business and technical needs underlying the most common use cases for selected industries.

Manufacturing

The manufacturing sector has been heavily reliant on wired Ethernet connectivity. Historically, wired connections were considered to be more resistant to interference, to provide better bandwidth, and to offer more security than wireless. And given the need to provide power to most devices, the cabling either comes with or is deployed alongside the power. More mobility needs and the more recent ability of wireless to support higher throughput at lower latency, coupled with higher levels of security, are now compelling manufacturers to reevaluate the use of wireless for more applications.

The elimination of network and cables due to the use of wireless technologies offers manufacturers the ability to run their operations more efficiently, increase productivity, reconfigure plant floors more easily, and reduce costs. However, manufacturers must consider their factory setup, networking topology, number of devices, potential RF interference, bandwidth requirements, etc., before settling on a particular technology. In fact, a single access method may not even be sufficient, requiring the manufacturer to deploy multiple wireless access technologies as per their connectivity needs.

Figure 2.
Mission-critical moving assets such as AGVs in manufacturing require a technology like URWB that delivers near-zero latency and seamless handoffs to ensure uninterrupted connectivity.

Use cases for manufacturing can be broadly classified into these groups:

- **Warehouse operations:** Includes moving materials within the factory, between the factory and the warehouse, and connecting AGVs and other vehicles.
- **Factory line operations:** Broadly encompasses connectivity needs for industrial automation, such as connecting robots, industrial systems, and autonomous vehicles on the factory floor. This category covers the needs of digital operations by connecting machines, sensors, and control systems with industrial wired and wireless networks to improve operations, margins, quality, and safety.
- **Connected workforce:** Includes connectivity needs for the mobile digital workforce to improve interactions between plants and field workers, remote colleagues, and experts.

Networking for manufacturing has some of the most stringent requirements among the industrial use cases. Any glitch in the operational network could mean stoppage of the production line, leading to lost revenue and wasted materials. Therefore, wireless access methods must be as strong and security as tight as possible.

Table 2. Wireless use cases for manufacturing

Use case	Requirements	Recommendations
Warehouse operations	Connect machines, sensors, scanners, and video systems with secure, standards-based connectivity to improve operations, supply chain visibility, productivity, and safety.	URWB for its high-availability, ultra-low-latency and seamless handoffs are recommended for machinery control and connecting mobile equipment such as AGVs. Wi-Fi is recommended for worker connectivity and other Wi-Fi enabled client devices.
Factory line operations	A wireless solution for mobile AGVs, robots, etc., must provide robust connectivity in areas of heavy interference due to the presence of machinery.	URWB is best suited for connecting mission-critical mobile equipment and robots, and Wi-Fi for stationary equipment and worker device connectivity is recommended.
Connected workforce	Provide reliable voice and video communications to the plant floor from any location at any time.	Wi-Fi using radios available natively within user devices, with adequate bandwidth for video collaboration.

Visit Cisco Industrial IoT Solutions for Digital Manufacturing to learn how Cisco solutions can help you establish a secure and reliable network foundation for digital transformation and Industry 4.0.

Connected rail

To achieve their objectives of safety, punctuality, superior service, and affordable costs, rail operators are turning to advanced technology that improves asset visibility, helps offer new and value-added services, enhances the passenger experience, and opens new revenue streams.

Freight rail carriers can use remote control, automation, and new IoT data to keep workers safe, streamline operations, and minimize the freight cost per mile, so they remain competitive with other modes of overland freight transportation. Passenger rail providers can offer services such as high-speed internet access, infotainment, mobile ticketing, and security systems on trains and in stations to enhance the passenger experience and increase ridership. In addition, critical signaling and control systems such as European Rail Traffic Management System (ERTMS), Communications-Based Train Control (CBTC), and Positive Train Control (PTC) are needed for safe operation.

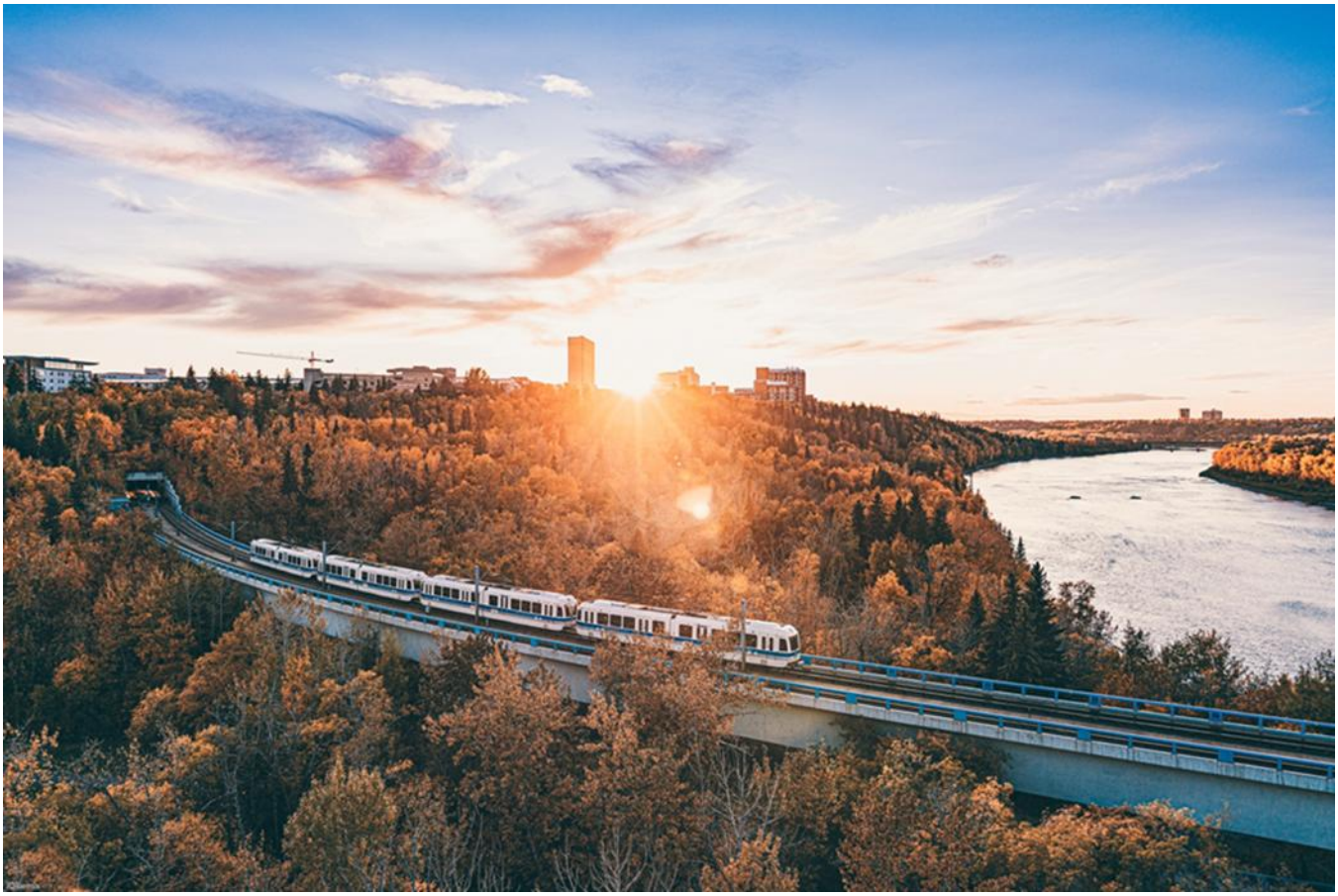

Figure 3.
Mission-critical applications in rail such as Communications-Based Train Control (CBTC) require a technology that can provide ultra-reliable connectivity such as URWB. Passenger and worker devices need access that can be provided by Wi-Fi.

Use cases for connected rail include:

- **Connected trains:** This onboard network provides connectivity to various devices aboard the train such as cameras, digital signage, Wi-Fi APs, various sensors, onboard controllers, Point-of-Sale (POS) systems, and train-to-ground radios.
- **Connected trackside:** These networks provide ground connectivity for moving trains as well as for sensors that monitor track status, signaling, and level crossings. Other services include point systems, axle counters, utilities, etc.
- **Connected stations:** These networks provide connectivity for digital signage, CCTV systems, asset tracking, wayfinding, and passenger Wi-Fi services at train stations.

Table 3. Wireless use cases for rail transportation

Use case	Requirements	Recommendations
Connected trains	Control systems networking requires low latency, high availability, and coverage throughout the route, including within tunnels. Passenger services require high bandwidth.	Wi-Fi within cars provide connectivity for passengers, POS systems, etc. Cars also need URWB to communicate with an external backhaul network. URWB along the rail tracks provide train-to-ground connectivity. Train operators may benefit from fiber laid along tracks, and if so, they can easily deploy Cisco URWB to build their own private mobile network.
Connected trackside	A converged secure IP network to support multiple services – signals, crossings, substation utilities, and a long-line PA system for the driver to communicate with ground controllers. The connected trackside infrastructure provides resilient communication paths between connected trains, connected trackside, connected stations, and the operations control centers.	The connected trackside network is generally wired and uses the backhaul network to communicate with the operations center. URWB can be used as a backhaul to extend trackside connectivity in areas without wired backhaul.
Connected stations	Wired PoE switching ports for surveillance cameras, kiosks for wayfinding, information displays, and ticketing. High-throughput Wi-Fi for passengers. High bandwidth required for bulk data transfer from onboard systems to ground.	Industrial Wi-Fi APs, on platforms and yards, provide passenger and staff network access. URWB could be used to extend connectivity to where wired connectivity is not available.

Visit the Cisco Connected Rail page for a detailed description and read the solution brief.

Ports and terminals

Marine or inland ports and cargo terminals have gone through major wireless network challenges over the last decade. Increased cargo movement requires more automation to accelerate loading and unloading and optimize the use of cranes and container handling equipment.

Terminal automation relies on innovative technologies such as Optical Character Recognition (OCR) to read information on containers, real-time vehicle geolocation to optimize movement on the dock yard, HD/4K video cameras to secure operations and enable autonomous vehicles, etc. All of which require broadband wireless connectivity to control centers.

Covering wide terminal areas that are prone to RF interference from container piles, moving cranes, and metallic installations requires careful and close placement of antennas and careful monitoring to minimize dead spots.

Modern port and terminal automation depend on flexible and reliable wireless technology that can provide full coverage, extremely low latency, seamless handoff with zero packet loss, high bandwidth, and easy installation, provisioning, and management.

Use cases for ports and terminals include:

- **Terminal Operating Systems (TOS):** Real-time control of movement of cargo around the port or terminal for proper loading and unloading. This includes connectivity for tractors, stackers, RTGs, and cranes to the TOS and leverages OCR and vehicle geolocation.
- **Autonomous operations:** Enablement of autonomous operations of moving equipment such as AGVs and Automated Rubber-Tired Gantry cranes (ARTGs) around the terminal.
- **Remote operations:** Remote control of RTG cranes, ship-to-shore cranes (or quay cranes), and straddle carriers.
- **Gates and warehouses connectivity:** Access control of terminal entry and exit, surveillance of warehouses and temporary storage areas, etc. This includes connecting HD/4K cameras in permanent or temporary locations, providing connectivity to workers' handheld devices and barcode scanners in roll-on-roll-off terminals, etc.
- **Port operations and monitoring:** Different from terminals, port operations consist of monitoring tidal conditions, weather conditions, water levels, current, and salinity, as well as monitoring and managing traffic, including vehicles, rail traffic, and ship traffic, and providing the workforce communication and collaboration tools.

Table 4. Wireless use cases for ports and terminals

Use case	Requirement	Recommendations
Terminal operations	Robust coverage is required over a large but very specific area, which simplifies radio planning. Latency must be very low and handoff seamless.	URWB is ideal to connect autonomous and automated vehicles and teleremote applications. URWB delivers ultra-reliability and has mechanisms to ensure connectivity port-wide for uninterrupted connectivity despite RF caused by obstacles such as container stacks.
Autonomous operations	Connected autonomous cranes do not require a high-bandwidth network, as they are equipped to make local decisions. However they still need connectivity to the TOS and require a reliable, low latency network.	Communications from autonomous cranes using URWB deliver the reliability and latency needed to send real-time data to TOS applications.

Use case	Requirement	Recommendations
Remote operations	Remote operation of cranes requires a high-bandwidth, low-latency, high-throughput, and fast-handoff capable network for streaming high-resolution video from onboard cameras to the controlling operator.	URWB's near-zero latency ensures real-time data transfer, enabling operators' remote commands to be executed immediately.
Gate and warehouse connectivity	Permanent or temporary broadband connectivity to access control systems, CCTV cameras, handheld devices, etc. to care for an ever-changing environment.	Locations requiring permanent connectivity might have wired networks installed. Otherwise, URWB is an ideal solution to install wire-speed connectivity without incurring the cost and delays of construction work. Handheld devices can be connected via Wi-Fi.

Figure 4.
Terminal operations require flexible and reliable wireless technology that can provide full coverage, extremely low latency, seamless handoff with zero packet loss, high bandwidth, which can be achieved with a combination of Wi-Fi and URWB.

Visit Cisco IoT Solutions for Terminal Operations and Ports to learn how you can reduce downtime, improve efficiency, and secure your critical infrastructure.

Mining

Mines are typically located in harsh, constantly changing environments. Managing equipment and assets and protecting employees can be challenging, and there is a need to respond to new conditions at mines amid changing market demands. Gaining real-time visibility into each step of the mining process, monitoring output, equipment, and worker location, and using this visibility to secure operations are essential. Dangerous locations, where workers cannot or should not go, require unmanned vehicles and trucks that can be remotely operated by skilled operators.

Figure 5.
Mining operations require connectivity is remote areas where wired connectivity may not be available as well as a reliable wireless network to support teleremote and autonomous operations.

Use cases for mining are similar to those for ports and terminals and include:

- **Mine operations:** A network that covers the entire area consisting of multiple operational domains, such as extraction, crushing, smelting, refining, waste disposal, and transportation.
- **Autonomous operations:** Autonomous trucks haul resources from shovels or front-end loaders in a mine to a crusher area. When fully automated, trucks may continuously operate at optimum performance. Autonomous operations may also include drilling, blasting, and other mining functions.
- **Remote operations:** This capability allows operators to work from the safety of a control room and operate machinery located in a high-risk environment (possibly underground) and improves operational efficiency by reducing downtime and improving visibility.
- **Connected workforce:** Enables a safe and efficient digital workforce using mobile technology to improve interactions between field workers, remote colleagues, and experts.

Table 5. Wireless use cases for mining

Use case	Requirements	Recommendations
Mine operations	A secure, robust infrastructure that provides visibility and enterprise-wide connectivity and supports the required mobility.	A combination of wired and wireless networking, utilizing Wi-Fi and URWB, is an ideal solution. Wireless technologies offer greater flexibility to adapt to changes in the mining environment. Compared to wired connectivity, they are faster, easier to relocate, and better suited for supporting various areas of the mine. URWB is particularly effective for mission-critical applications, including mobility, and for providing connectivity in areas where wired infrastructure is either unavailable or cost-prohibitive. Wi-Fi ensures seamless access for Wi-Fi-capable devices and machines.
Autonomous operations	Reliability, zero packet loss, and low roaming times are essential to ensuring continuous operations.	URWB is ideal to interconnect the extraction zones to local sitewide operational services. URWB's near-zero latency and seamless handoffs ensure uninterrupted connectivity of autonomous vehicles.
Remote operations	Networks need to connect moving machinery over a vast area. For remote operations, stringent networking requirements include strict handover times, high throughput, and low latency.	URWB communications between mining vehicles and the control center satisfy the high-bandwidth, low-latency, and seamless handoffs requirements
Connected workforce	High-bandwidth network for collaboration. Must have availability in all operational areas.	Wi-Fi is needed for worker connectivity and collaboration.

Visit Cisco for Mining to see how Cisco networking solutions can make underground and surface mining operations safe, reliable, and efficient.

Oil and gas

Challenges faced by today's oil and gas industry include increased material and production costs, strict regulations, operations in remote areas, the need to safeguard employee safety and health, and the need to increase productivity. Legacy networking capabilities are proving inadequate to address these challenges. A network that can provide a converged, standards-based architecture for applications that monitor and gather data right down to the sensor level can help organizations improve operational efficiency, adjust business processes, and comprehensively manage field and refinery sites.

Figure 6.
Oil and gas environments needs wireless that is reliable with access points with the appropriate certifications for HazLoc operations.

Wireless use cases for oil and gas operations can be broadly classified into these groups:

- **Upstream:** Refers to the extraction of crude petroleum and gas from underneath the ground. The use case is like mining but does not involve as many moving vehicles, although it does involve connecting many fixed assets.
- **Midstream:** Refers to the transportation of crude and gas from extraction sites to refineries and from refineries to point-of-sale locations. The pipelines may run over long distances in remote rural areas.
- **Downstream:** Refers to the refineries that convert crude and purify natural gas.

Table 6. Wireless use cases for oil and gas

Use case	Requirements	Recommendations
Upstream operations	A robust and secure industrial communications infrastructure for real-time plant and field operations.	Given that these operations are usually in rural areas, URWB is a more budget friendly and easier alternative to building a fiber network. URWB can be used to connect mission-critical applications and Wi-Fi to provide worker connectivity.
Midstream operations	Networking requirements include connecting pumps, sensors, etc. along the length of the pipeline	URWB can be used to extend connectivity to specific areas of the pipeline that includes sensors and pumps.
Downstream operations	Networking requirements for refineries are very similar to those for manufacturing.	A combination of high-performance wired and wireless networks is necessary. URWB is recommended for mission-critical applications that need ultra-reliability and Wi-Fi to provide access to Wi-Fi enabled client devices.

Visit Cisco for Oil and Gas to learn how Cisco solutions make upstream, midstream, and downstream operations safe, reliable, and efficient.

Connected communities (smart and safe cities)

A connected community uses digital technology to connect, protect, and enhance the lives of citizens. IoT sensors, video cameras, social media, and other inputs act as a nervous system, providing the city operator and citizens with constant feedback so they can make informed decisions.

Figure 7.
Smart cities require different wireless technologies to support different use cases.

Use cases for connected communities can be classified into the following:

- **Sensors:** A connected community uses data collected from a variety of sensors placed around an urban area to monitor conditions, manage assets, and improve city services. Sensor locations may include the city's public transportation systems, roadways and traffic signals, power plants, utilities, water supply, waste management, schools, libraries, parking decks, and other services that the city provides to its citizens.
- **Public Wi-Fi:** A municipality may provide Wi-Fi services by means of public access points in locations such as the city center, town hall, parks, bus stops, train stations, and other public places.
- **CCTV:** Cameras may be deployed around the city for citizen safety and security purposes, as well as for traffic monitoring.
- **Short-term needs:** Seasonal or special needs for fairs, sports events, etc., that require provision of Wi-Fi hotspots or CCTV coverage for a few days.

Table 7. Wireless use cases for connected communities

Use case	Requirements	Recommendations
Sensor connectivity	These sensors require only low-bandwidth connections, but as they are spread out across the city, they require broad coverage. Because these sensors may be battery powered, the network must minimize the power consumption of these devices.	Sensors can be connected via Wi-Fi.
Public Wi-Fi	Wi-Fi access points placed around the city need connection to a high-bandwidth network to backhaul data.	Data backhaul can be achieved using fiber if available. If not, URWB can be used to extend connectivity to unconnected areas and communities.
CCTV	Like the Wi-Fi use case, cameras placed around the city need high-bandwidth backhaul connections.	Fiber, if available, can be used for data backhaul. URWB can be used to extend connectivity to cameras that are located where wired connectivity is not available. Wi-Fi can be used if the location of the camera has reliable Wi-Fi signals.
Short-term needs	Special events typically require high-bandwidth connections for CCTV coverage and for internet access by many people in a relatively small area.	URWB is an excellent solution for cities looking to extend connectivity during events and fairs where wired infrastructure may be insufficient to support large crowds simultaneously. Wi-Fi provides reliable access for Wi-Fi-enabled devices, ensuring seamless connectivity for attendees.

Visit Cisco Connected Communities Infrastructure to learn how Cisco solutions can shape empowered communities of the future.

Management considerations

Rapid expansion of industrial digitization, addition of user devices, and increasing dependence on their functions require that industrial networks be intelligently managed. The management system must be able to quickly add new devices, reconfigure them as needs change, update as new firmware becomes available, and monitor their performance to make sure they remain fully available.

An agile network made possible by a capable network management system frees the organization to expand operations, customize products, improve efficiency, and reduce the time to market for new products and services. Therefore, you must think through the management of the wireless technology you select.

Security considerations

The need to secure industrial operations is paramount, and the role of the industrial network cannot be overestimated.

The network must provide detailed and granular visibility into the connected devices and their interactions. Such visibility not only will allow discovery of security holes, but also will find areas for gaining operational efficiencies.

Visibility will also allow security personnel to define access policies and carve out zones that segment the one physical network into several virtual ones. This segmentation blocks unnecessary and potentially unsecure communications and helps to contain threats and reduce risk.

Finally, a secure network must be able to help spot abnormal behavior that might indicate the presence of malware, report such incidents to a central Security Operations Center (SOC), and help in threat mitigation.

Cisco industrial networking solutions

We offer a comprehensive portfolio of wired and wireless networking solutions designed to meet the needs of various industries. Our solutions support a wide range of use cases and are available in different form factors with varying levels of ruggedization. These features enable our technologies to withstand challenging conditions such as water, dust, extreme temperatures, and vibration. Additionally, we provide compact form factors for easy deployment in small spaces and specialized access points for hazardous locations.

Industrial Wireless

Cisco offers a wide portfolio of access points and wireless clients, including the Cisco Catalyst® IW9167 and IW9165 Series. These access points come in different form factors so they can be deployed in a variety of industrial locations from a compact DIN-rail access point ideal for small spaces all the way to the harshest environments such as hazardous locations.

Together, Wi-Fi and URWB offer an unparalleled wireless solution, with Wi-Fi supporting high-speed, low-latency requirements and URWB ensuring reliable communication for applications that require ultra-low latency and seamless roaming. Many of our access points and wireless clients support both URWB and Wi-Fi.

Our innovative converged approach – a single piece of hardware that supports both Wi-Fi and URWB, enabling activation and set up of URWB capabilities in Cisco Wi-Fi access points via the Wireless LAN Controller (WLC), allowing management of ultra-reliable networks effortless through Cisco Catalyst™ Center – gives you unparalleled flexibility without added complexity:

- **Optimized investment:** Avoid duplicating infrastructure needed to support different wireless technologies.
- **Simplified deployment:** Easily enable URWB in the field, streamlining your setup.
- **Single management:** Manage Wi-Fi and URWB management from a single pane of glass, enhancing operations and extending end-to-end visibility to OT networks.
- **Cost effective operations:** URWB uses unlicensed spectrum, reducing costs and eliminating the complexities of staff training, licensing, and spectrum management.
- **Effortless connectivity:** Wi-Fi is readily available on the assets you need to connect, and you can attach an access point to connect assets with URWB with ease.
- **Comprehensive solution:** Wi-Fi with URWB access points in a variety of form factors supporting indoor, outdoor and industrial use cases eliminating complexities, time and gaps of dealing with point solutions and multiple vendors.

Visit our industrial and outdoor wireless page to learn more about our portfolio.

Cisco offers a complete and comprehensive portfolio of wired industrial network equipment that forms the backbone for all wireless technologies.

Industrial Switches and Routers

The Cisco Industrial Ethernet (IE) switching portfolio includes ruggedized, secure, easy-to-use switches built for extending the enterprise to harsh, industrial environments. The switches provide secure connectivity across challenging environments in industries such as manufacturing, utilities, transportation, oil and gas, mining, and smart cities. IE switches are available with a robust security feature set, including software-based segmentation, connected assets, and flow visibility for threat detection and isolation. Scaling is easy, with many management options.

The Cisco Catalyst industrial routers are a range of ruggedized modular platforms on which you can build a highly secure, reliable, and scalable communications infrastructure. All Cisco industrial routers share a core set of common characteristics. They are certified to meet harsh environmental standards and have modular designs that can help extend product life and lower costs. This flexible design enables WAN redundancy and is ready to handle 5G, public LTE, including FirstNet, and private LTE, including Citizens Broadband Radio Service (CBRS), as well as enhanced data throughput and differentiated services.

Visit the Cisco Industrial Switching and Industrial Routing pages and view the complete product portfolio.

Industrial security

Cisco industrial security solutions help you build and implement a converged IT/OT security strategy that incorporates deep and granular operational visibility, creation of zones and conduits by careful segmentation of your operational network, and detection, investigation, and remediation of cyberthreats.

Cisco products for industrial security include:

- Cisco Cyber Vision for visibility into OT and ICS assets, so that you can understand your OT security posture, detect threats and drive cybersecurity best practices.
- Cisco Security Equipment Access (SEA) for controlling remote access to your OT/ICS assets with Zero-Trust Network Access (ZTNA).
- Cisco Identity Services Engine for enforcing ISA99/IEC62443 zones and conduits and control access to critical OT assets with a zero-trust micro-segmentation framework.

Visit the Cisco Industrial Security page to see how these products and other products are applied to achieve an integrated industrial threat defense.

Conclusion

Industrial wireless networking can provide lower-cost and faster deployment options than wired networks and makes it possible to connect moving assets such as autonomous, automated and remote-controlled robots and vehicles.

Organizations considering using wireless in their operations are advised to evaluate available technologies and pick the one that best fits their particular use case. Apart from the technical criteria, such as bandwidth and latency, they should consider availability, cost of ownership, and the projected evolution in making their decision, while understanding that they will likely need more than one technology for their operations.

Cisco's industrial networking portfolio provides the full breadth of wireless equipment and the wired switches and routers for its foundation.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-2980062-01 06/25