White paper
Cisco public

The bridge to possible

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. On the other hand, today's wireless technologies also support industrial sensors that generate only low data rates but operate on batteries at low power.

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 (Cisco 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 ise-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, forcing many in the workforce to work remotely, and increased the need for video collaboration, distant consulting, autonomous operations, remote control, etc.

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 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.

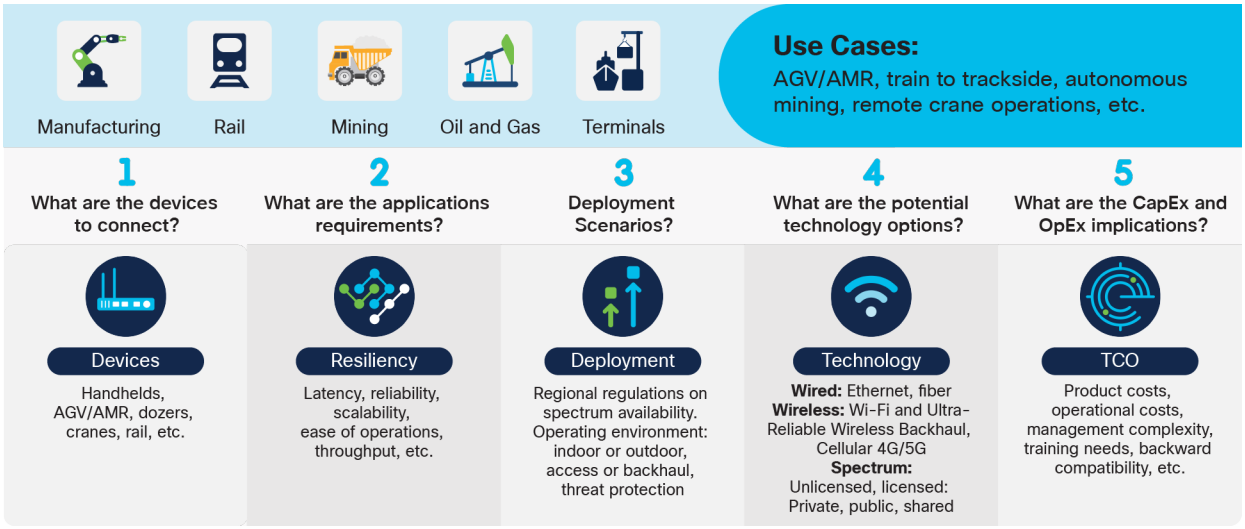

Figure 1.
Decision factors for selecting wireless technology

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. Wi-Fi and Cisco URWB tend to have higher upfront (CapEx) costs, while cellular/5G tends to have higher operational costs (OpEx) due to the nature of the technology.

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.

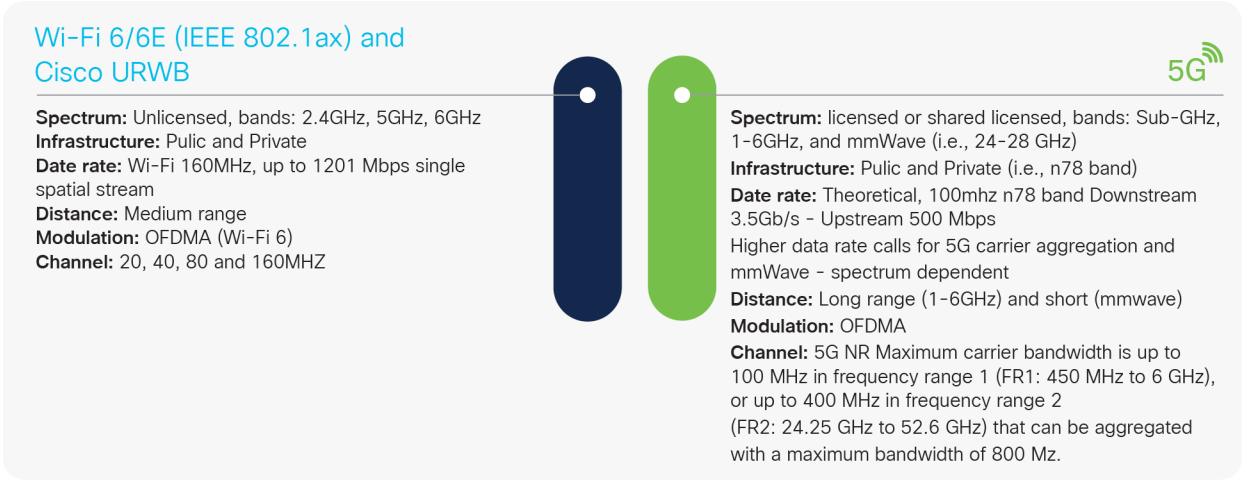

Figure 2.
A technical comparison of industrial wireless technologies

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, and the latest versions, Wi-Fi 6 and 6E, or IEEE 802.11ax, dramatically increase network capacity and bandwidth and reduce latency. And the additional spectrum offered by Wi-Fi 6E offers a chance to provide dedicated spectrum for certain applications. It also improves battery efficiency.

For industrial use cases, Wi-Fi 6 and especially Wi-Fi 6E can help accelerate adoption of IoT devices. Operating in the new 6-GHz spectrum, Wi-Fi 6E offers additional bandwidth and less congestion. The Wi-Fi 6 and 6E standards also offer 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 is the strong Wi-Fi Protected Access 3 (WPA3) encryption it offers.

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 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 6, 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 designed to offer reliable wireless connectivity for mission-critical applications, whether they are stationary or mobile. Cisco URWB provides low-latency, highly reliable, long-range, and high-bandwidth connections that can handle endpoints moving at high speeds with zero-delay handoffs. Operating in unlicensed frequencies, Cisco URWB can be deployed anywhere and can be an excellent alternative to fiber in industrial sites, campuses, or even cities.

Sharing the same technology underpinnings as Wi-Fi allows Cisco 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.

Cisco URWB is especially suited for connections requiring fiber-like 1-Gbps or higher data rates where no fiber is available or where pulling fiber would be prohibitively expensive. 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, Cisco URWB offers several benefits:

- **Cost:** Cisco 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:** Cisco 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.
- **Deployment:** Cisco URWB is as easy to deploy as a Wi-Fi access network. 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:** Cisco URWB benefits from the advances in Wi-Fi standards. The new Wi-Fi 6E standard opens the new 6-GHz band, which enables a 160-MHz channel, and Wi-Fi 7 may potentially use a 320-MHz channel. Therefore, Cisco URWB has great potential to increase the data rate in upcoming releases.
- **Reliability:** Cisco URWB combined with Cisco Multipath Operations (MPO) adds an additional level of reliability. New generations of Cisco URWB products will provide dual radios able to support Cisco MPO, enhancing reliability while improving latency without changes in applications.

Table 2. A brief comparison of wireless technologies for industrial use cases

Attribute	Wi-Fi	5G	Cisco URWB
Type of service	Network access with built-in radio in client devices.	Network access with built-in radio in client devices.	Access with a separately attached Cisco URWB radio to client devices and backhaul between Cisco URWB radios.
Operating characteristics	Short range, high bandwidth. Indoor and limited area outdoor use.	Long range, high bandwidth, low latency, high availability.	Medium range, high bandwidth, low latency, seamless handoffs.
Spectrum	Unlicensed. 2.4, 5, or 6 GHz.	Licensed. Multiple bands from low speed (600 to 900 MHz), mid speed (2.3 to 4.7 GHz), and high speed (24 to 47 GHz).	Unlicensed. 2.4, 5, or 6 GHz.
Range	A single AP has limited range to enable 360-degree coverage within transmit power regulations. Multiple APs required for density of client devices.	Range is inversely proportionate to frequency spectrum used, with lower frequencies providing longer range and the ability to provide indoor coverage. Range may also be affected by regulations governing maximum transmit power.	Custom-made infrastructure allows for antennas delivering a broad indoor/outdoor range.
Mobility	At low speed due to slow handoffs between APs.	At any speed with minimal packet loss.	At any speed with no packet loss (“make before break” radio link creation).
Availability	Ubiquitous (6-GHz variant may not be certified in all countries).	Varies depending on country and service provider.	Available today.
Ease of deployment	Easy to deploy. Enterprise owned.	Complex to deploy. Requires radio planning and core network configuration or selecting one from a Mobile Network Operator (MNO).	Easy to deploy. Enterprise owned. Requires radio planning.
Automation, provisioning, management	Enterprise. Fully automated, monitored, and assured with modern network management systems.	Complexity (packet core, radio network, devices) or managed services with monthly service provider fees.	Enterprise. Medium complexity (as Wi-Fi).
Connecting industrial devices	Generally built-in radio.	5G-enabled devices or any device with Wi-Fi or Ethernet through 5G IoT router.	Any device with Wi-Fi or Ethernet.
Cost of ownership	Low	High	Low

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 3.
Multiaccess wireless technologies for manufacturing

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 3. 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.	Because of multiple needs, a multiaccess approach is necessary. CURWB or 5G for their high-availability and low-latency are recommended for machinery control and connecting mobile equipment such as AGVs. Wi-Fi or 5G is recommended for worker connectivity.
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.	A production floor also needs multiple wireless technologies: Cisco URWB and 5G are best suited for connecting 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 and/or 5G 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.

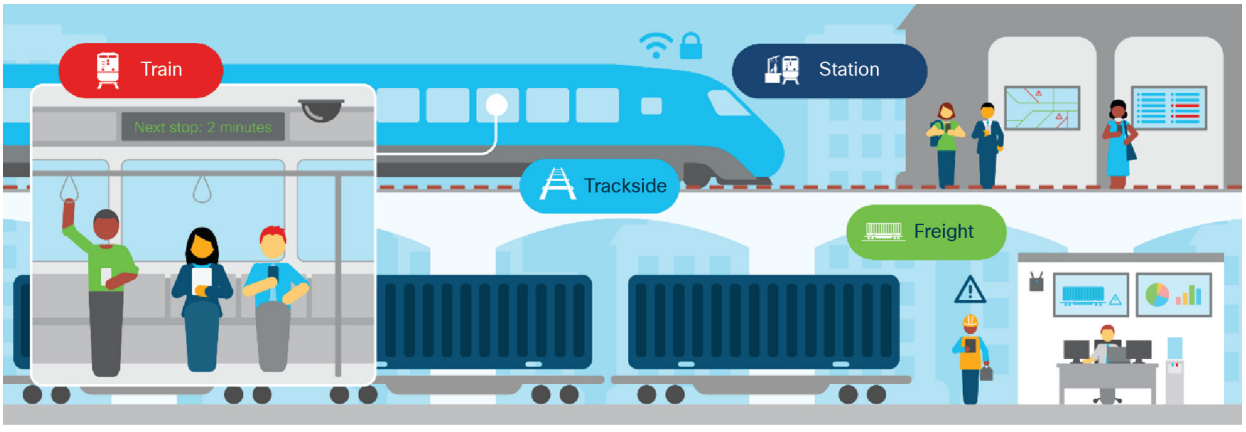

Figure 4.
Connected rail use cases

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, 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 4. 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 Access Points (APs) within cars provide connectivity for passengers, POS systems, etc. Cars also need to be equipped with radios to communicate with an external backhaul network. Cisco URWB radios 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 radios to build their own private mobile network. 5G antennas do cover a larger area but may not be available in remote or rural areas, as it may not be economical for service providers, in which case the train operator may be asked to bear the installation costs. A deployment may consist of a combination of Cisco URWB and 5G in different sections of the track.
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.
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. Cisco URWB could be used for offloading data and bulk data transfers if Wi-Fi is not already present.

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 5. 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.	Both Cisco URWB and 5G can be used and will require equipping cranes and vehicles with the appropriate radios. Both offer seamless handoffs, low latency, and broadband speed. The determining factor could be the availability of adequate 5G services able to deliver the required bandwidth over the area and the need for careful radio planning to manage radio interferences in such a harsh environment.
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 could use any wireless backhaul network with adequate reliability without special considerations.
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.	Considerations are similar to the terminal operations use case. While both 5G and Cisco URWB could support the required high-res video streams, 5G would need to operate at higher frequency with a larger spectrum to be effective.
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, Cisco 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 5G or Wi-Fi. Chances are they will have Wi-Fi radios built in. Wi-Fi APs required could be connected to a wired network or a Cisco URWB node backhauling traffic to the ground applications.
Port operations	Environmental sensors require a network with a large coverage area, whereas traffic monitoring and connectivity for users would require a high-bandwidth network.	A low-powered, low-bandwidth LoRaWAN network for sensors, Wi-Fi for workforce, Cisco URWB or 5G for traffic monitoring (from cameras installed along the road).

A terminal automation network requires 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.

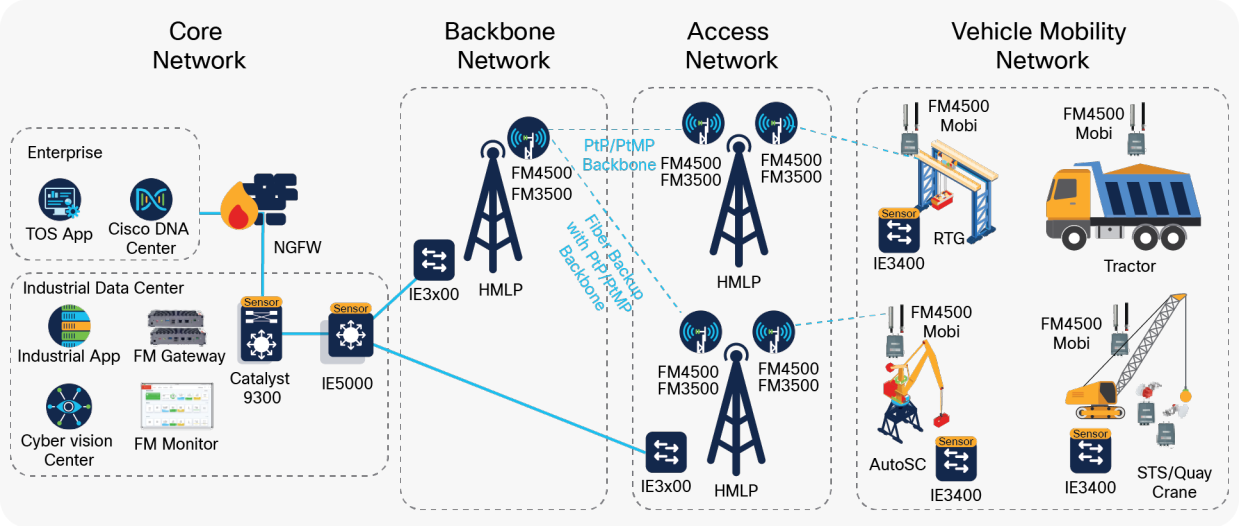

Figure 5.
Wireless connectivity architecture for terminal operations

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.

Figure 6.
Mining use cases

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 6. 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 using industrial Wi-Fi. Cisco URWB is the ideal alternative to a wired network, as wired networks will need to be modified every time the mining environment changes.
Autonomous operations	Reliability, zero packet loss, and low roaming times are essential to ensuring continuous operations.	Wireless backhaul to interconnect the extraction zones to local sitewide operational services. Can be accomplished with either Cisco URWB or 5G.
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.	Cisco URWB communications between mining vehicles and the control center satisfy the high-bandwidth, low-latency, and quick-handoff requirement. 5G is also a possibility provided its infrastructure is available to meet the stringent requirements. Cisco URWB or Wi-Fi are recommended for remote operations underground.
Connected workforce	High-bandwidth network for collaboration. Must have availability in all operational areas.	Industrial Wi-Fi or 5G connectivity is needed for worker connectivity and collaboration.

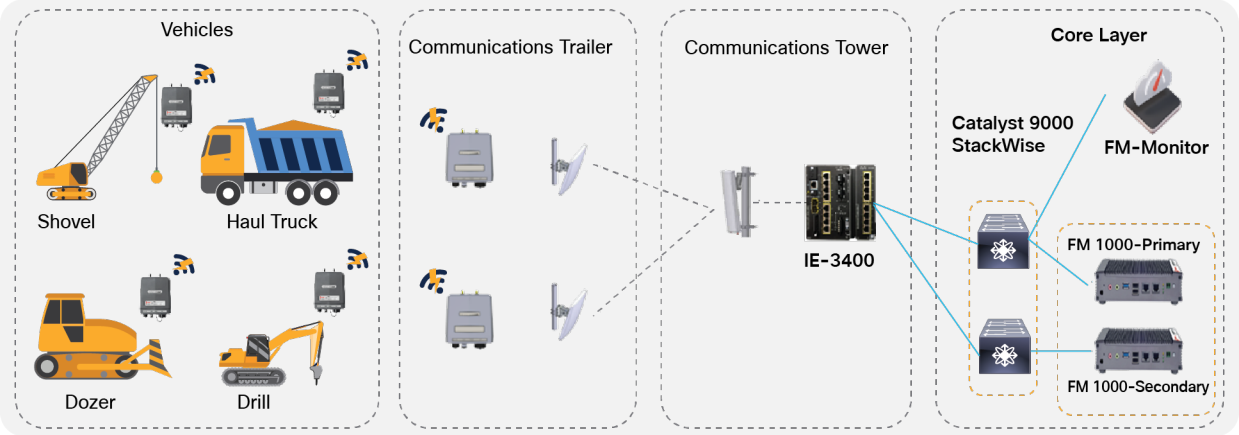

Figure 7.
Wireless connectivity architecture for mines

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.

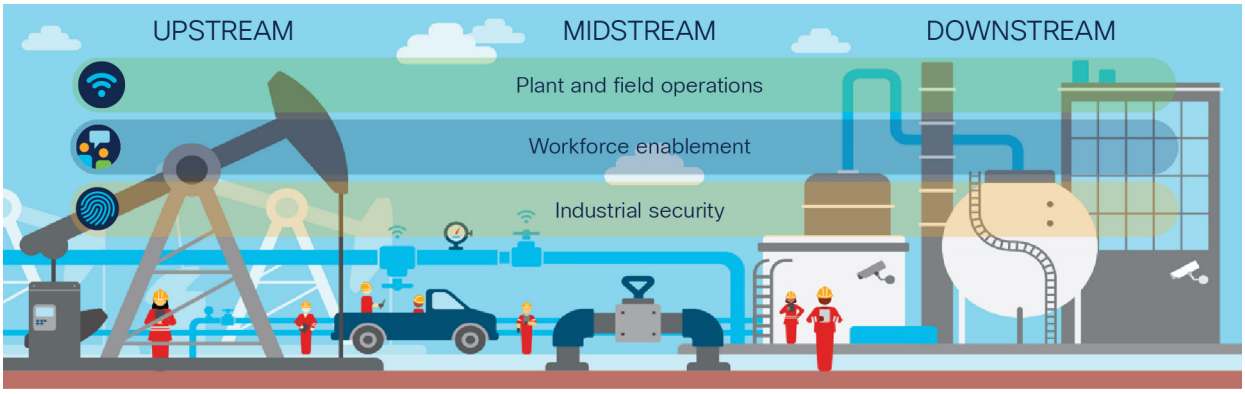

Figure 8.
Oil and gas use cases

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 7. 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, Cisco URWB may be a better alternative to building a fiber network or private 5G, which could be costly in these areas. Industrial assets can be connected via Wi-Fi or directly through Cisco URWB radios.
Midstream operations	Networking requirements include connecting pumps, sensors, etc. along the length of the pipeline	Given that the network needs to cover a vast, countrywide area, either 4G or 5G connectivity as available is recommended. Cisco URWB could be used if either cellular technology is not available.
Downstream operations	Networking requirements for refineries are very similar to those for manufacturing.	A combination of high-performance wired and wireless networks is necessary. Wireless can usually be covered by Wi-Fi aided by 4G/5G as available.

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.

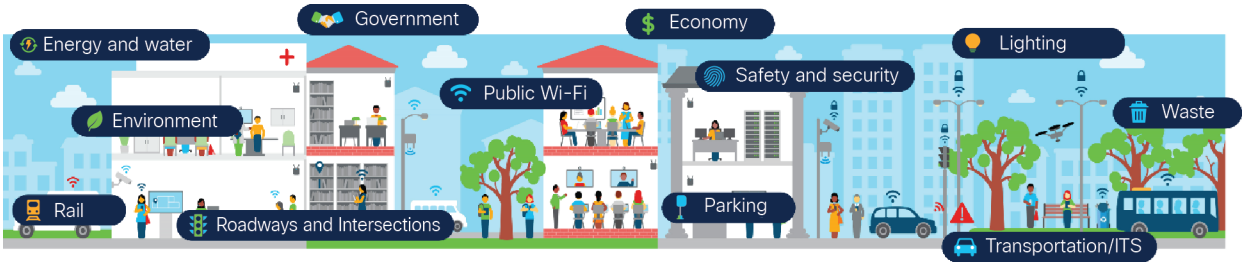

Figure 9.
Connected communities use cases

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 8. 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 are connected to a low-bandwidth wide area network such as a public or private LoRaWAN infrastructure. Service providers can also offer connectivity using 4G/LTE or 5G service, but choice of sensors might be limited.
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, Cisco URWB is recommended for its high-bandwidth connections.
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. If not, Cisco URWB can be used. 5G is also an option; however, video streams might need to be compressed to reduce usage costs and cope with the limited data rates available during peak hours. Note that the public cellular infrastructures (4G/LTE or 5G) might not be fully available during emergencies, either because local authorities might want to preempt network capacity, or because of network congestion.
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.	5G is an option if available, but might not offer enough bandwidth to support the large number of people that may gather at such events. Cisco URWB can be installed quickly, provides a dedicated network infrastructure, and delivers the availability, resiliency, and throughput needed for this use case.

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

The comprehensive range of wireless solutions from Cisco does not impose any artificial restrictions that may force you into making suboptimal decisions for your specific use cases. Cisco networking incorporates multiple technologies and allows you to architect your network with IP data flow from end to end with automation, assurance, and security.

Choosing the right industrial wireless solutions for your industry can be difficult. To make this process easier, Cisco has developed the Industrial Wireless Advisor Tool, that you can use to get our recommendations on the technology and our accompanying products and solutions.

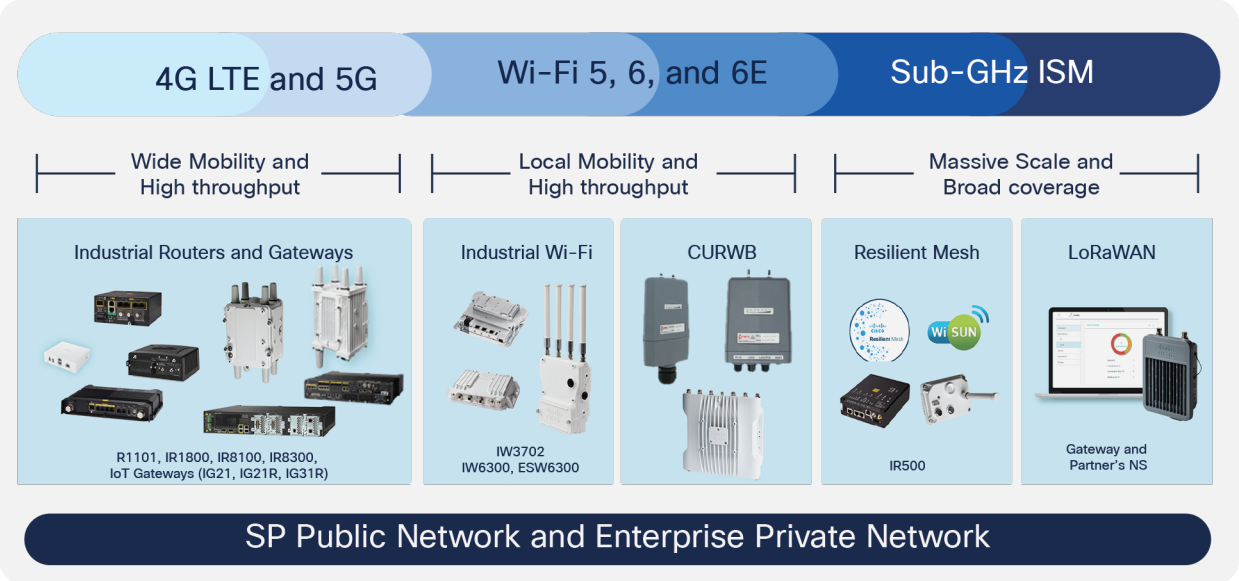

Figure 10.
Cisco industrial wireless product portfolio

Industrial Wi-Fi

Cisco offers a wide portfolio of Wi-Fi industrial access points, including the Cisco Catalyst® IW6300 Heavy Duty Series Access Points, Cisco 6300 Series Embedded Services Access Points, and Cisco Industrial Wireless 3700 Series. These access points are ruggedized and specifically designed to operate outdoors in extreme environments and hazardous locations. Onboarding and configuration of these access points can be automated, and their performance monitored, by Cisco DNA Center, making large deployments simple.

Please visit the Cisco Industrial Wi-Fi page for details on how you can extend Wi-Fi to industrial environments and provide resilient connectivity wherever you need it.

Private 5G

Cisco Private 5G is delivered as a service offering, eliminating nearly all financial risk to integrate the high speed, low latency, and device segmentation only 5G can provide to increase your business productivity. Cisco Private 5G is a future-ready way to deploy cellular service, complementing and enhancing existing networks and providing trusted coverage and mobility across unique business-critical environments.

Cisco Private 5G provides operational simplicity, SLA management, application awareness and identity management, cloud management, security, and seamless software and firmware upgrades.

Visit Cisco Private 5G to learn how Cisco takes the complexity out of private 5G and how you can securely integrate IoT across your wireless network deployments. Cisco Catalyst Industrial Routers are secure, high-performance routers in a modular design that support private LTE, FirstNet*, Wi-Fi 6, 5G, and Gigabit Ethernet.

Ultra-Reliable Wireless Backhaul

Cisco Ultra-Reliable Wireless Backhaul is a new generation of wireless technology that lets you achieve fiber-like performance for mission-critical applications. Like 5G URLLC, it features ultra-low latency to enable the most demanding real-time applications. Like fiber, it offers ultra-reliable broadband connectivity. It is easy to deploy, maintain, and operate, making it the ideal choice for IT and OT backhaul.

Cisco URWB has been successfully deployed by the world's largest industrial enterprises and in various applications, such as rail transportation, ports and terminals, smart cities, oil and gas, and manufacturing. It is a solid alternative to 4G and 5G cellular solutions and provides a comprehensive set of radio products to cover its many use cases.

Cisco URWB is managed by Cisco FM Monitor, which allows customers to proactively maintain and monitor their network. It allows easier installation, deployment, and troubleshooting, and displays data and situational alerts from every Cisco URWB device. Its comprehensive dashboard shows overall network performance and offers customizable segmentation of the network into clusters. This allows for easy monitoring of network sections or parts of a fleet of vehicles, maximizing network usage and performance.

Visit the Cisco Ultra-Reliable Wireless Backhaul page to learn how Cisco URWB can easily connect standard, mission-critical, and real-time applications anywhere you need them.

Industrial switches and routers

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

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. Enable intent-based networking to the IoT edge with Cisco Software-Defined Access (SD-Access), and easily manage your IoT network with the same tools that manage your IT network, such as Cisco DNA Center, which simplifies configuration and reduces the time and cost of deployment.

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 network management

Cisco DNA Center is a proven, intelligent, and comprehensive management platform for software-defined networks. Deployed in the largest enterprise networks globally, Cisco DNA Center increases operational efficiency by automating routine network maintenance tasks such as device configurations and software image updates, reduces downtime by optimizing performance by proactively identifying and resolving issues that could impact production, and helps you stay compliant by tracking updates, helping ensure that software images comply, and remaining aware of security updates.

Visit the Cisco DNA Center page and read the Solution Brief for Industrial Automation.

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, Cisco Identity Services Engine for access policy enforcement and segmentation, Cisco Secure Network Analytics to detect advance threats, and Cisco SecureX™ for an integrated IT/OT security platform experience. Visit the Cisco Industrial Security page to see how these products are applied to achieve an integrated industrial threat defense.

Conclusion

Industrial wireless networking can provide lower-cost and faster deployment options, can better monitor assets and operations, makes possible autonomous and remote-controlled robots and vehicles, and improves collaboration between mobile workers.

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 multiaccess 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 C11-2980062-00 05/22