Article

Four Keys to Successful Industrial Wireless Deployments

Industrial wireless applications, both in-plant and external, offer big benefits of more simplified, streamlined, and lower-cost operations, plus greater flexibility, visibility, efficiency, and profitability. Successful deployments require careful consideration of four key factors in planning and execution.

As many of the world's industries embark on massive overhauls of aging production infrastructures, most will forego wired networks, installing industrial wireless local area networks (iWLANs) instead as their operational and communications backbones. Among their reasons are less costly wiring; more flexibility and scalability in plant layouts; and the introduction of mobile vehicles and robots.

iWLAN application examples include:

- Automated guided vehicles (AGVs), mobile robots, overhead cranes and monorails
- Wireless access for performance monitoring, remote diagnostics, service, and configuration
- People movers, amusement rides, big-wheel attractions, ski lifts (fail-safe wireless needed)

Another related trend involves the use of wide area network (WAN) technologies for external industrial communications applications, ones deployed outside of factory, warehouse, and logistic environments. Ruggedized 802.16e WiMAX and cellular 4G LTE (soon 5G) technologies can provide terrestrial, long-range communications for municipal operations, utilities, vehicle fleet operations, pipeline operations, and more. With autonomous vehicles soon to debut, these external applications will only grow. WAN application examples include:

- Upstream oil and gas exploration and production, midstream pipelines
- Steel works, refineries, and other sprawling industrial operations
- Harbor applications and container terminals
- Pit mines, mine shafts, and tunnel networks
- Municipal water treatment and management
- Power utility transmission lines and substations

Whether industrial plants and municipalities are deploying applications of iWLAN or WAN technologies, they will typically gain substantial advantages of cost-savings, plus greater operational flexibility, agility, and visibility. But in contrast to enterprise IT office networks, they need extraordinary reliability and, especially on plant floors, *deterministic* transport of three different industrial data types – information-based, real-time, and mission-critical.

"Deterministic" refers to the need for time-sensitive control and safety data to get where it must go in milliseconds. If, for example, a valve doesn't open or some actuator fails, a process can be disrupted, potentially causing the costly scrapping of an entire batch of product. Worse, a toxic release or explosion could occur, risking the life and environmental safety of site personnel as well as any surrounding communities.

This contrasts with office data, such as email, file transfers, printer commands, and so forth that can be delayed even seconds without consequence or users even knowing. Table 1 lists the differences between operational technology (OT) and IT requirements, many of them significant.

By Cole Holland, RUGGEDCOM Product Marketing Manager, Siemens; and Jonathan Simpson, Industrial Networking Product Manager, Siemens

Attribute	Industrial OT	Enterprise IT
Environment	Harsh conditions (e.g. temperature,moisture, electromagnetic interference)	Climate-controlled offices
Installation	Extensive site surveys required, plus back-haul cabling done in the field	Site surveys are minimal if needed at all; back-haul cables are pre-fabricated
Topology	Plant-specific configurations (e.g., line, star, tree, ring)	Typically, star configurations
Availability	Network downtimes cannot be tolerated	Downtimes of up to several minutes can be tolerated
Redundancy	MRP, high-speed redundancy, standby failover networks	Link aggregation, RSTP, MTP
Administration	OT engineer or trained technician	Certified IT specialist
Health, Safety & Environment (HSE)	Fail-safe, critical	Fail-safe, non-critical
Cybersecurity	Super-critical	Critical

Table 1. Key differences between industrial OT and enterprise IT wireless communications requirements.

For reasons of these differences, the 802.11 Wi-Fi technology and components used in enterprise IT office networks will typically fall far short of the rugged, reliable, and deterministic demands of iWLAN and WAN gear needed for industrial use. Surprisingly, and despite the clear differences in requirements, many industrial enterprises nonetheless deploy office-grade Wi-Fi equipment in their production environments, putting their operations at risk of disruption.

These OT/IT network distinctions are also why the respective OT and IT staffs must cooperate in designing and implementing networks that serve both environments, while also serving the overall mission of the entire enterprise, whether front/back-office or plant floors, warehouses, and other industrial facilities.

Four guiding principles to successfully deploying industrial wireless networks

The IEEE 802.11 WLAN standards span the physical and data link layers (Layer 1 and 2, respectively) of the Open Systems Interconnection (OSI) model put forth by the International Organization for Standardization (ISO). IEEE 802.3 – better known as Ethernet – also spans these two layers, a fact which facilitates the necessary wiring to support iWLANs, as well as the use of wired and wireless networks in combination. Figure 2 shows the different wireless technologies available for industrial applications.

To successfully deploy iWLANs or WANs, we suggest using the following four principles as guidance:

1 Use wireless technologies for appropriate applications

Plant floors have evolved in recent years and will continue to do so with more and more automation and digitalization. For example, where workers may have once moved feedstocks and finished goods, now automated conveyor systems may do so, whether they're overhead cranes, monorails, or AGVs. Where workers may have once assembled goods or kept watch on industrial processes, robots or industrial control systems may be handling the tasks. Where technicians may have once conducted equipment maintenance on schedules and diagnostics onsite, conditioned-based maintenance has reduced or eliminated such schedules and remote diagnostics can often handle troubleshooting.

Point is, iWLANs and WANs don't need to be deployed to support every application. Some applications, usually higher-level ones, such as manufacturing execution and manufacturing operations systems, don't need wireless communications. Video surveillance applications, which typically have fixed cameras and require lots of bandwidth, are usually best served by wired, if not fiber-optic, networking.

Applications that can benefit from wireless technologies are mobile AGVs, robots, and conveyor systems. These need real-time data with minimal latencies to safely operate and be "aware" of their surroundings, especially personnel coming and going unpredictably around them. Other use cases involve support of production lines that may need to change their configurations frequently – or often enough to make rewiring them excessively costly. Finally, applications covering long distances can especially benefit from WAN technologies, often eliminating the need for workers to periodically drive and check on operating assets, such as the pumps of a far-flung water treatment system or pipelines.

2 Conduct proper site surveys, RF engineering, and planning

As mentioned, enterprise IT office WLANs are relatively simple to install compared to iWLANs. That's because the former operates in comparatively uniform and predictable environments. Current 802.11 Wi-Fi technologies, such as those operating with IEEE 802.11n and 802.11ac standards, provide plenty of radio coverage. Their reach can extend up to 150 feet indoors and twice that outdoors. Their radio waves can easily penetrate all but the thickest masonry walls, which most modern office buildings lack.

In contrast, iWLANs must contend with walls, reflective metal machinery, and a host of other factors, not the least of which is the existing radio frequency (RF) environment. This can require careful engineering to address sources of RF interference, such as cell phones and wireless handsets or even employee badge readers. Shelving and large inventories of metal stocks or finished goods can either absorb or reflect RF signals. Motion control of robotics and material handling also pose RF engineering challenges by causing intermittent shadowing and reflections.

Outdoors, especially WAN applications, must negotiate terrestrial topologies to ensure line-of-sight requirements are met. Signal strengths and cabled backhaul needs must be considered. In all cases of iWLAN and WAN applications, deployments must address cybersecurity and fail-safe concerns, too.

Most industrial enterprises and municipalities lack the skilled resources to conduct site surveys and do the RF engineering on their own. That's why engaging a qualified RF expert can help with this critically important step. Such an expert, whether an individual or consulting firm, should provide a detailed model of the planned coverage area and sources of RF interference. These two factors greatly impact channel selection and placement of antennas and access points (APs) in the case of iWLANs and WAN equipment for long-range, outdoor deployments.

3 Choose the right components

In operation, iWLANs must meet the rigorous demands from their operating environments, enduring harsh ambient conditions, such as extreme temperatures – hot, cold and swings between each – as well as weather for hardware that must operate outdoors. At the same time, iWLANs must be fail-safe in their transmissions. In addition to conducting site surveys and RF engineering, expert consultants can help select the appropriate wireless equipment – base stations, antennas, and APs – that has been properly designed, engineered, and manufactured for industrial conditions.

Siemens, for example, offers its broad line of SCALANCE W wireless products for iWLAN deployments for use with SCALANCE S Level 2 and 3 managed and unmanaged industrial switches. The portfolio also includes SCALANCE M cellular products for additional deployment options, plus specially designed fail-safe components to meet availability requirements. These products come with web-based tuning capabilities that dramatically reduce the time of deployment and system tuning.

Preserving existing investments. All SCALANCE W components are compatible with IEEE 802.11 a/b/g/n/ac standards. Backward compatibility with 802.11 a/b/g standards helps preserve legacy investments in those technologies. They offer built-in support both for 2.4 and 5 GHz spectrum bands and for PoE (Power over Ethernet), to minimize electrical cabling costs.

The SCALANCE components also offer a unique, patented solution to minimizing transmission latencies. The originators of IEEE 802.11 didn't envision applications requiring real-time communications with low cycle times, much fewer moving clients like AGVs, mobile cranes, amusement rides and so forth. They never imagined clients that would need to always be transitioning their communications from one AP to the next as they moved through a highly engineered RF landscape.

Minimizing latencies. In response, Siemens developed its iPCF (industrial Point Coordination Function) technology. As a highly deterministic algorithm, it provides for the fast communications – as fast as 16 milliseconds – required by industrial control systems, especially those governing fast roaming and safety applications. Building on that technology, Siemens developed a variation called iPCF-MC especially for continuously moving APs, such as those aboard AGVs and cranes, to enhance performance further.

For easy maintenance and device replacement, a thumbnail-sized, plug-in card called a C-PLUG enables automatic backup of network configuration and project data in SCALANCE W modules and APs. A more comprehensive swap media card called a KEY-PLUG contains all the C-PLUG's functionality, plus enables easy access to the iPCF deterministic algorithm.

Another KEY-PLUG capability is Siemens unique industrial Range Extension Function (iREF) that enables a Wi-Fi/ WLAN network to cover a longer distance or larger area with just one AP by allowing its antennas to cover multiple areas with maximum transmit power, which reduces the number of channels and APs used.

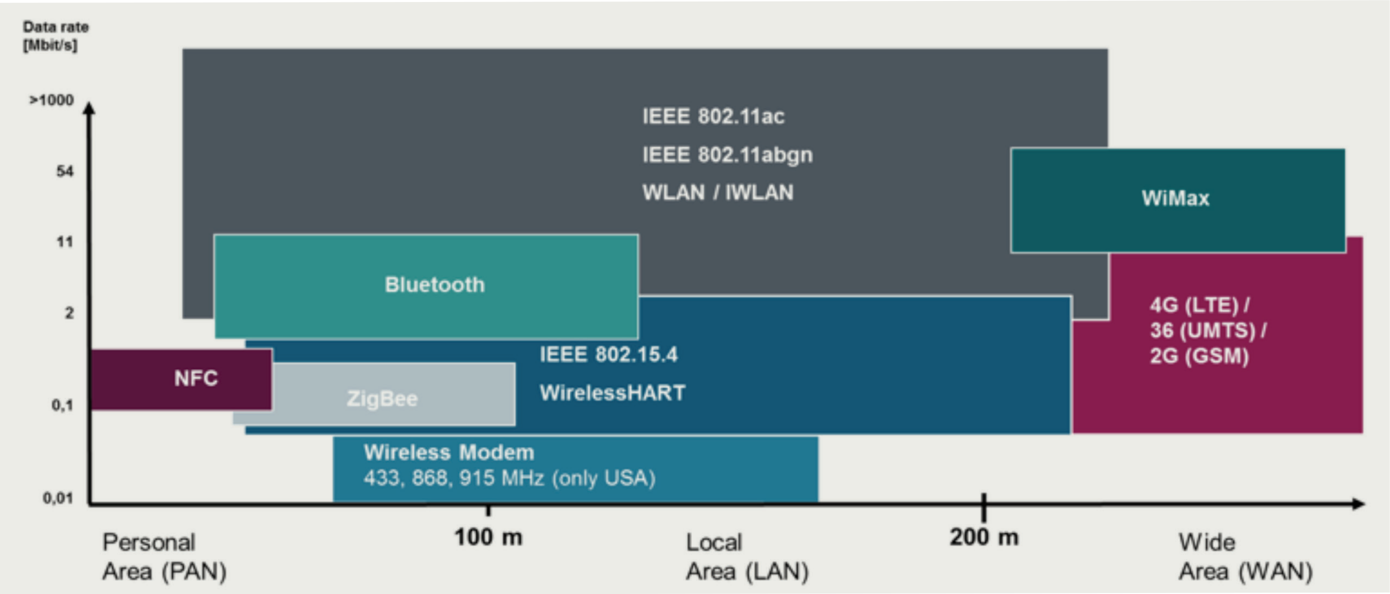

Figure 1. Wireless technologies based on different ranges and data rates.

Going the distance. For outdoor and long-range applications, Siemens offers the RUGGEDCOM portfolio. Its components can provide solutions based on 802.11 Wi-Fi, 802.16e WiMAX, cellular technologies, or hybrid solutions that mix the technologies. Importantly, as the brand name suggests, RUGGEDCOM components are not standardized models "hardened" with add-on e nvironmental protections. Instead, they are designed and engineered from the start for ultra-reliable performance in a wide range of hazardous and extreme environmental conditions.

RUGGEDCOM components comply with ANSI/NFPA Class I, Division 2 standards to prevent explosions, given their potential use in areas of flammable hydrocarbon gases, vapors or liquids. They can operate in extended temperature ranges from as high as 167°F (75°C) to as low as -40°F (-40°C) temperatures that fall well within the range of Arctic and equatorial extremes. Last, they are IEC IP67-rated against intrusion by dust and blasts of corrosive saltwater.

4 Choose the right partner

The investment in an RF consultant's knowledge and experience should more than pay for itself by minimizing the implementation time, effort and overall project cost. To help find a qualified resource, Siemens has thousands of certified Solutions Partners worldwide, accessible via the Siemens website's Partner Finder feature. For companies with their own RF engineering resources, Siemens also offers a free, downloadable configurator tool that simulates the coverage of different APs and their respective antennas. It's available at www.siemens.com/snst

Industrial wireless offers big returns but requires careful planning

As more and more industries worldwide migrate from field bus technologies to industrial Ethernet like PROFINET, their opportunities to deploy iWLAN and WAN technologies, such as Siemens SCALANCE and RUGGEDCOM portfolios, will increase. These networks will provide the backbones for securely transmitting the different data types from the automation and digitalization technologies that are transforming industrial enterprises around the world.

Already in widespread use across a wide range of industrial applications, both fixed and roaming, iWLANs and WANs continue to prove their worth as complements, if not alternatives, to costlier and less flexible fixed wired networks. Technologies like Siemens exclusive iPCF have eliminated the issues of latency in process control and safety applications by effectively enabling real-time communications, especially what's needed for highly dynamic environments.

But for all their promise, iWLANs and WANs require careful RF engineering and planning before they can deliver their promised returns in terms of greater flexibility, scalability and efficiency for production and logistics operations. They also need the close collaboration of both OT and IT staffs to ensure proper network segmentation, cybersecurity safeguards, and compliance with IT governance frameworks, so the entire enterprise can benefit from these advanced technologies. The sooner these technologies are deployed, the sooner their companies can realize their competitive advantages and operational benefits.

Security information
Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit htttps://www.siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/industrialsecurity

Published by
Siemens Industry, Inc. 2019.

Siemens Industry, Inc.
5300 Triangle Parkway
Norcross, GA 30092

For more information, please contact
our Customer Support Center
Phone: 1-800-241-4453
E-mail: info.us@siemens.com

usa.siemens.com/ruggedcom

Order No.: NTWP-WRLPF-0219
Printed in U.S.A.