Industrial Wireless

Selecting a Wireless Technology

Industrial environments present extreme challenges for wireless communications

SmartPath™ outdoor Wireless Access Point (LWN602HAE)

SmartPath™ 602HAE Outdoor Kit (LWN600A-OUT)

SmartPath™ 30W Power Kit with Cord, UK (LWN600PS-UK)

Table of Contents

Introduction

Industrial environments are uniquely different from office and home environments. High temperatures, excessive airborne particulates, multiple obstacles, and long distances separating equipment and systems are special challenges that make it difficult to place and reach sensors, transmitters, and other data communications devices.

These—and many other factors—create a unique, complex, and costly challenge for establishing data communications channels that are reliable, long-lasting, and cost-effective in industrial environments.

The primary difficulty faced by many companies is the need to connect remote equipment sensors to central monitoring systems in difficult environments. For example, the environment inside a steel mill is extremely intense: high heat, heavy machinery, large distances, and high levels of EMI significantly shorten the lifespan of wires and network equipment. Even a tank farm, which doesn't deal with harsh environments, runs into distance and cost issues with faraway sensors and equipment.

These are two extreme cases and, of course, the industrial world contains everything in between, in varying degrees of complexity. This white paper addresses the challenges posed by data communications in an industrial environment.

Historical Challenges with Industrial Wireless

Wireless communications in industrial settings has had a rocky past and has typically not performed well enough to endure the harsh demands of industrial applications. There are several reasons for this:

- Signal Echo — Typical 900-MHz and 2.4-GHz open radio frequencies used within today's wireless data communications applications have a reasonable penetration rate through office cubicles, drywall, wood, and other materials found in an office or a home. However, these signals tend to bounce off larger objects, metals, and concrete. This bounce can redirect the data signal and return it to the original transmitter, causing an "echo" or "multi-path." First-generation wireless systems became easily confused with this type of interference and would cancel transmission all together. The result was a state referred to as "radio null," which prevented data communications.
- Noise— The electromagnetic emissions created by large motors, heavy equipment, high power generation and use, and other typical industrial machinery creates high levels of electrical noise that interfered with early wireless equipment. In these noisy environments, transmitters and remote nodes were unable to hear each other, resulting in frequent data loss.
- Channel Sharing and Interference — Radio frequency space has become enormously crowded. FCC approved frequency spectrums are shared by many devices, including those using Wi-Fi® (IEEE 802.11) and IEEE 802.15.4. Frequently, the result was data confusion as receivers and nodes gathered and sent information on the same channel as other devices in the area.
- Industrial Protocols Not Supported — The vast majority of early wireless devices were designed for office or home use only. Because of this, very few engineers were addressing the industrial protocols such as Modbus or the need to move from wireless to RS-232, 422, or 485 supports. Additionally, housings, circuitry, and connections were designed for lightweight use and were inadequate for rugged industrial settings.
- Distance— The sheer distances between central control systems and remote sensors and equipment limited the feasibility of early wireless systems, which had a range of only a few hundred feet.
- Security— Early adoption of the IEEE 802.11 standards created a large number of security issues. These standards continue to require a high level of countermeasures to ensure the safety of data and business systems.

Although the fundamental premise of wireless was a clear answer to many industrial data communications challenges, the reality was that, unless these obstacles could be overcome, wireless was not a solution at all.

New Methods and Technologies Solve Wireless Issues

Over time, this has changed, as new technologies have entered the picture. Today, there is a wide array of data communications solutions that could resolve challenges facing industrial environments.

Here is a snapshot of the options you have with some corresponding pros and cons. When looking for the best industrial wireless solution for your situation, carefully consider these factors:

Echo, Noise, and Channel Interference

Several transmission and modulation methods have been developed to counter the effects of echo, noise, and interference caused by channel sharing. Here are two of the best:

- FHSS (Frequency Hopping Spread Spectrum) — Data is transmitted on a single channel at a time, but the channel is rapidly and constantly changing or "hopping." This scheme requires low bandwidth.
- DSSS (Direct Sequence Spread Spectrum) — Data is transmitted simultaneously over every available channel, making it a bit more reliable in "noisy" environments but also bandwidth intensive.

Caution: Note that all wireless transmitters, nodes and equipment on your network must support the same transmission scheme to operate properly.

In addition to these transmission methods, there are several design and development standards that play an essential role in establishing reliability, security, speed, distance, and efficiency. Determining your best solution depends on your application and needs. In outlining the various wireless options below, the "Pros and Cons" list is from a typical industrial environment.

- Wi-Fi (IEEE 802.11b/g/n)

Pros — This standard forms the staple of office and home networking, and is widely used for its high data-transfer rate abilities (maximum throughput of 54 Mbps with 12 Mbps being typical).

Cons — However, complying with the standard requires excessive overhead because of its power consumption, software requirements, and processor demands — as well as its short ranges (160 metres maximum) — making it less than effective in most industrial situations.

- Bluetooth (IEEE 802.15.1)

Pros — Bluetooth® has gained popularity because of its small physical size and instant network setup. Three classes allow Bluetooth to move data anywhere from 3 to 100 metres away.

Cons — Bluetooth has a relatively high duty cycle (especially in 2.0 and early versions), minimal data throughput (currently a maximum of 3 Mbps is possible), and requires a fairly defined line-of-sight because of its low penetration qualities.

- ZigBee (IEEE 802.15.4)

Pros — Relatively speaking, ZigBee is the new kid on the block, but it has several things going for it. It's far more power-friendly than Wi-Fi and Bluetooth because of its advanced sleep and sniff abilities. Additionally, it has high penetration ability and it operates with an even smaller physical footprint than Bluetooth.

Cons — Zigbee has low data rates—only up to 720 kbps—and has poor interoperability. Additionally, because it is relatively new, hardware developers are still refining and defining their systems.

- Proprietary RF (non-standard)

  Pros— Proprietary RF (PRF) provides you with an exact solution to meet your specific needs. Modulation schemes, distances, throughput, casing, and configurations can all be customised. With PRF, interference issues virtually disappear because you are no longer fighting for the exact same channel sequences that standardised protocols and formats use. PRF is often more power-friendly as well because the protocol and hardware configuration does not require an exact setup that may or may not be more energy efficient. For this same reason, costs can actually be lower. PRF can operate in both the 900-MHz and 2.4-GHz frequencies, giving you greater control over distance, penetration, and channel interference. Additionally, there are many PRF off-the-shelf solutions that may meet your needs, saving the time needed for customisation.

  Cons— PFR does not provide interoperability with any of the established wireless standards, which may mean that once you buy from one vendor, your system will only work with its products.

If you select an off-the-shelf wireless product that complies with one of the established wireless standards, you are limited by that standard's range, penetration, frequency, and data rate. If your application doesn't fit within these limitations, then you may want to examine proprietary RF. Here are some important factors to consider:

Range Considerations

Range is determined by four elements:

- Transmit Power — Transmit power refers to the amount of power that is emitted from the antenna port of the radio device. Proprietary RF is regulated in the U.S. for up to one watt. This provides substantial benefits when long ranges are needed because the higher the transmit power, the "louder" the signal and the farther it can travel.

Buyer's Guide | Comparing the various aspects of wireless standards

Product Feature	Wi-Fi	Bluetooth	ZigBee	PRF
Frequencies	2.4 GHz and/or 5 GHz	2.45 GHz	915 MHz (U.S.) 868 MHz (Europe) 2.4 GHz (Global)	900 MHz (U.S.) 868 MHz (Europe) 2.4 MHz (Global)
Channels	16 @ 2.4 GHz 80 @ 8 GHz	79	10 @ 915 MHz 26 @ 2.4 GHz	16 to 79 (Can Be Customised)
Range (Indoor)	70 m	Class 1 = 1 m Class 2 = 10 m Class 3 = 100 m	20 m	1000 m
Range (Outdoor)	160 m	100 m	100 m	64 km (with high-gain antenna)
Data Rate (Max.)	54 Mbps (with 12 Mbps typical)	3 Mbps	250 kbps	721 kbps to 72 Mbps
Transmission Scheme	DSSS	Adaptive FHSS	DSSS	FHSS or DSSS
Power Sources	Wired	Battery/Wired	Battery/Wired	Battery/Wired (Industrial Power Source Compatible)
Uses	Cable Replacement, Large Data Transfer, Networking	Short Distance Cable Replacement	Monitoring and Controlling	Cable Replacement, Monitoring, Controlling, Data Transfer
Nodes (Max.)	32	8	>64,000	Variable
Stack Size	1000 KB	720 KB	250 KB	Variable
Transmit Power (Max.)	—	—	—	1 W

- Receiver Sensitivity — Sensitivity defines how well remote receivers can pick up a wireless signal. Sensitivity is significantly impacted by antenna type and hardware configurations.
- Line of Sight — RF signals travel in curved elliptical paths, rather than in straight lines as light does, resulting in a signal path that resembles a football in shape. Interference can occur at any point within this area. For maximum communications, the fewer barriers along the line of sight between receiver and transmitter, the better. Frequency and transmit power levels have the most impact on how well the signal can negotiate physical and EMI line of sight barriers.
- Data Volume — Data rate and volume will also impact your range. Large data packets are more difficult to transmit than smaller packets and typically reduce range.

Penetration and Congestion Considerations: 900 MHz vs. 2.4 GHz

As you can see from the chart on page 5 , the 2.4-GHz band has become fairly crowded. Most popular current standards operate at this frequency, creating a fairly congested environment. Instances of problems caused by multichanneling and crossover are increased simply by the sheer volume of devices. 2.4 GHz also has a tighter, shorter wavelength, which inhibits its ability to penetrate physical barriers. These disadvantages are compensated for in some environments by its ability to carry larger data packets and increased transfer rates.

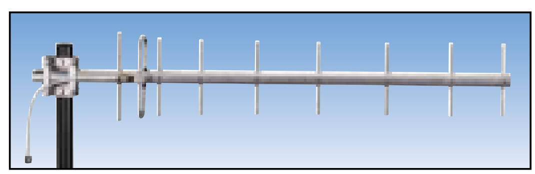
900 MHz has a much longer wavelength, which provides greater physical barrier penetration and is far less popular, which makes the frequency range less crowded. Because of these two factors, given enough transmit power and receptor sensitivity, 900-MHz communications can be extended to around 40 miles (64 km) with far greater obstacle penetration. However, if high data-transfer rates are needed, this slower frequency will not likely be adequate.

Antenna Considerations

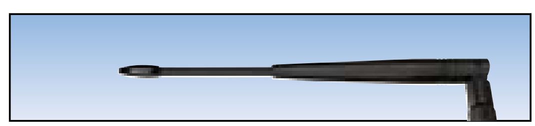
Antenna selection will depend on your communications needs, with system array and range being the biggest factors.

Two Types of Antennas

- Directional — Sends and receives the signal in a single direction. A directional antenna gives you the longest range. Examples: Yagi, Dish, and Panel.
- Omnidirectional — Sends and receives the signal in a radius. This antenna allows the largest number of nodes. Examples: Vertical Omnis, Ceiling Domes, and Rubber Ducks.



Directional Antenna



Omnidirectional Antenna

System Configuration Types

- Point to Point — Moves data from one single location to another single location.
- Point to Multipoint — Moves data from a single location to multiple locations.

Summary

With today's technology, the possibility of a wireless industrial data communications environment is stronger than ever. Issues that have plagued the wireless option are being minimised, especially as proprietary RF becomes fine-tuned to address specific challenges. Industrial companies can now create extensive data communications networks in the harshest of environments while achieving these advantages:

- Low Costs — Wireless equipment represents a substantial savings over the cost of cabling, installation, and configuration of wired networks.
- Longevity — Sensors, transmitters, and receivers can be designed for the harshest of environments with many operating at temperatures between -40 to +85° C. Concerns about wires deteriorating or needing to install multiple signal boosters over long distances are eliminated.
- Swift Deployment — Wireless systems can be almost instantly deployed, modified, and taken down, saving time—and money.
- Easy Configuration — Many wireless systems are plug-and-play, self-configuring and self-repairing. Proprietary RF systems often come with easy-to-use, free configuration software to make set-up and customisation quick and easy.