

*White Paper*

---

## **Wireless Communications for Industrial Applications**

*Cirronet, Inc.  
Summer 2002*

---



## **OVERVIEW**

Data buses like Modbus and Profibus are no longer the de facto standard for industrial communications; both have been overtaken by Ethernet. Ethernet accommodates a wide range of applications, has become universally supported by communications equipment manufacturers, and counts ease of configuration and low cost among its many advantages. Ethernet also easily encapsulates industrial equipment protocols and is quickly becoming the standard of choice for many short-range communications links.

For all of its advantages, however, wired Ethernet shares one significant drawback with other wired industrial networking approaches: Cabling. Distance and cost limitations associated with wired links surface quickly on sprawling factory floors and in large industrial settings, and running cable to new or relocated equipment can interrupt production. These hardwiring drawbacks have led many to seek a longer range and more flexible alternative in wireless Ethernet.

“Wireless Ethernet,” the general descriptor applied to wireless links within an Ethernet network, is any over-the-air connection between Ethernet network nodes or devices. For example, wireless Ethernet is often used to bridge physically separated network segments or to connect remotely located equipment to another Ethernet device or network.

As is often the case with new technology applications, there are a wide range of wireless Ethernet implementations on the market, and there is no single wireless Ethernet standard. Wireless Ethernet solutions typically fall into one of two classes of over-the-air protocols: those based on IEEE 802.11 (usually 802.11b), and those based on proprietary protocols designed specifically for industrial environments.

This paper examines the ability of these two approaches to address the unique requirements and challenges of industrial communications and provides an overview of Cirronet wireless Ethernet products designed specifically for industrial applications. The information presented serves as a guide for systems integrators and end users responsible for factory floor automation, industrial control, SCADA, telemetry and related data communications applications.

## **COMMUNICATIONS IN INDUSTRIAL ENVIRONMENTS**

In nearly every factory floor and industrial setting, communication links carry vital information between machinery, control, and monitoring devices. From periodic updates to ongoing process and manufacturing management, reliable data flow is critical to operations.

Much of the control and status information transferred in industrial settings—actuator position, temperature, or liquid levels, for example—is carried in short “bursts” which require relatively little bandwidth and connection speed. At the other extreme, large file transmission, such as activity logs from a production run, requires moving a lot of data very efficiently.

Whatever the specifics of the data being moved, all industrial communications share one critical requirement: Timely delivery without failure. Hardwired Ethernet delivers data quickly and reliably but within the limits associated with cabling.

## **THE TROUBLE WITH CABLING**

Cabling necessarily tethers equipment to fixed locations, thus reducing flexibility in equipment placement and reorganization. Cabling can also be very expensive to install and maintain in terms of both material and labor costs. New runs, moves, or upgrades easily disrupt operations while cable is accommodated, and re-positioning or upgrading equipment can necessitate completely new runs. Moreover, as the distance between equipment and control or monitoring devices increases, cable run length maximums are quickly exceeded.

## **WIRELESS ETHERNET ALTERNATIVES**

Turning to wireless Ethernet technology addresses the cabling drawbacks of hardwired connections. As it uses radio technology, however, selecting an appropriate wireless Ethernet solution requires examining wireless Ethernet's transmission and operational characteristics. In industrial and factory settings, the right approach must deliver high-performance communications without sacrificing speed, flexibility, range, or reliability.

### **WIRED VS. WIRELESS**

There are two "ports" on any wireless Ethernet device: the radio interface that enables the wireless link and the wired Ethernet connection. Using a standard IEEE 802.3 (10Base-T) interface, the wired side connects to a network or directly to an Ethernet-enabled device such as a computer or industrial programmable logic controller (PLC).

The hardwired port on the wireless Ethernet device must clearly comply with the IEEE 802.3 standard in order assure interoperability among Ethernet devices. By contrast, as long as the devices that establish the wireless link use the same protocol, there are no fixed over-the-air protocol requirements for wireless Ethernet data transmission.

As described below, many wireless Ethernet devices, such as those designed for intra-office connectivity, employ an IEEE wireless Ethernet standard. Industrial applications, on the other hand, are typically best served by wireless Ethernet devices using protocols designed specifically to perform in the tough operational conditions presented by these environments.

### **THE IEEE 802.11 STANDARD**

Building on the success and prevalence of wired Ethernet, the IEEE defined a wireless Ethernet standard under the IEEE 802.11 umbrella of specifications. Designed specifically to promote office LAN product interoperability, 802.11 (and more recently 802.11b and a) defines an over-the-air interface between a wireless client and a base station, or between two wireless clients. All 802.11 variants are therefore optimized for high speed/short range communications, with a typical open office maximum range of about 300 feet.

### **INDUSTRIAL WIRELESS PROTOCOLS**

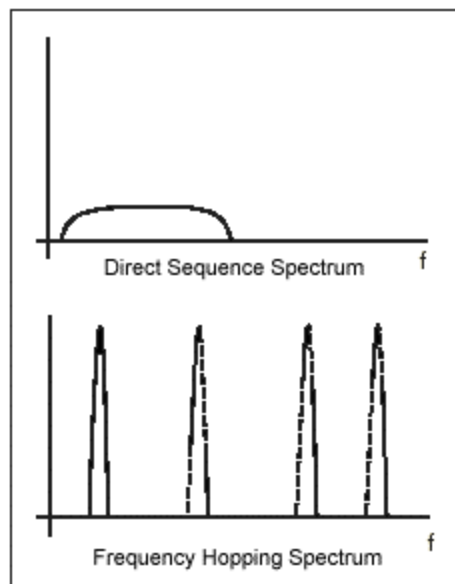
Industrial and factory environments pose substantial challenges for wireless communications. Reliable industrial performance is possible only when the wireless protocol used by the devices accounts for the operational obstacles typical of these radio-hostile environments. Key criteria for industrial wireless Ethernet performance are described below in the section on Industrial Criteria.

## 2.4 GHz ISM OPERATION

Wireless Ethernet radio devices transmit and receive on the license-exempt 2.4 GHz industrial, scientific, and medical (ISM) radio band. The band's license-free status streamlines implementation and compliance worldwide, as no permits or fees are required for equipment setup or use. This ISM band's frequency range is very appropriate for roaming and longer range fixed wireless communications, offers greater bandwidth than other allocations (e.g., the 900 MHz ISM band), and is more suitable for data-centric commercial and industrial applications.

## SPREAD SPECTRUM TRANSMISSION

Spread spectrum radio transmission technology distributes a signal over greater bandwidth than is used by conventional narrowband radio transmission. The technique's principal advantage is minimized interference from other signal sources and reduced susceptibility to monitoring. There are two dominant approaches to spread spectrum as used by wireless Ethernet devices: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS).



**Figure 1:** Comparison of direct sequence and frequency hopping methods for spread spectrum transmission. Direct sequence transmits over a static band of spectrum whereas frequency hopping shifts rapidly among multiple discrete frequencies.

DSSS spreads a narrow-band source signal by multiplying it with a pseudo-random noise signal. The resulting signal is then spread over a large range of continuous frequencies. This introduces redundancy into the transmission, enabling a receiver to recover the original data even if parts of it are damaged during transmission.

Rather than transmitting over a static spectral segment, frequency hopping spread spectrum (FHSS) radios pseudo-randomly vary carrier frequency, quickly "hopping" through multiple channels while sending data. Interference is avoided by hopping over different frequencies, each of which has a different interference effect or characteristic.

## **MEETING INDUSTRIAL CRITERIA**

Any wireless communications technology considered for industrial deployment must be evaluated in terms of performance and flexibility relative to environmental threats. The following discussion presents industrial wireless performance criteria with a corresponding look at how they are addressed by prevalent wireless Ethernet approaches.

### **MULTIPATH FADE AND RF INTERFERENCE IMMUNITY**

Multipath fade and radio frequency (RF) interference are the two primary factors that affect wireless communications indoors. Multipath fading, or interference, occurs when multiple copies of a source signal arrive at a receiver through different reflected paths. The phase variance in the signal copies can result in destructive interference that reduces signal strength, effective range, and data transfer rates.

RF interference occurs when other RF signals are present in the same or related frequency interval as the desired signal. In the 2.4 GHz ISM band, for example, microwave ovens, industrial heaters, RF lighting, and welding equipment are common sources of RF interference.

In nearly all indoor and outdoor settings, industrial and factory equipment produces electromagnetic (EM) and RF interference that wreaks havoc on wireless performance. The transmission method employed by a wireless device must therefore offer a sufficient level of immunity to these inevitable sources of interference.

As an example, consider 802.11-based wireless Ethernet. While the original definition employs both FHSS and DSSS, the newer—and more common—802.11b variant employs only DSSS. This introduces greater susceptibility to interference from reflections and electrical noise than FHSS. In addition, due to spectral constraints and inherent receiver complexity, DSSS systems typically employ only minimal spreading; the method's ability to overcome signal fade and interference is therefore relatively weak.

FHSS-based wireless Ethernet devices, because they pseudo-randomly “hop” among frequencies, have superior interference and multipath fade immunity. If one frequency is affected, for example, the data is soon transmitted over another, clear channel. This gives the technique greater coverage, channel utilization, and resistance to noise and multipath fading than comparable direct sequence systems.

### **DATA THROUGHPUT CAPACITY AND LATENCY TOLERANCE**

Throughput is the amount of data transferred per unit time, and latency is the maximum acceptable delay between data transmission and reception between nodes. Latency and throughput are generally counterproductive, however. Longer packets may lead to decreased overhead, but it comes at the cost of higher latency as it means other devices in the network have to wait while long packets are transferred.

While the 802.11b standard cites a maximum over-the-air data rate of 11 Mbps, this speed is seldom possible in practical terms, especially in industrial settings. In fact, low signal strength or quality (as results from interference or fade) causes the devices to throttle speed back progressively until, in many cases, they operate at just 10% of their theoretical capability. The resulting transmission delays deliver far less than optimal performance or reliability.

The best industrial designs do not overestimate throughput. Instead, they closely match actual application data rate to quantity and time requirements. Moreover, in radio-hostile environments, where latency increases as the result of multipath fade and RF interference, industrial designs

incorporate configurable and variable latency settings to ensure high operational resiliency and performance.

## **NETWORK ARCHITECTURE FLEXIBILITY**

The nature of wireless applications generally leads to a star configuration: an access point communicating with one (point-to-point) or more (point-to-multipoint) remote devices and connected to a wired network.

As multiple links are employed in a single location, the ability of the wireless device to operate in the presence of other devices must be considered. For example, typical 802.11b devices have just three non-overlapping channels due to their direct sequence-based design. This means that only three separate links can be operational at the same location. By contrast, a properly designed industrial system—particularly those based on FHSS—supports many more co-located systems due to the relatively larger number of frequencies used.

## **NODE AND ANTENNA PLACEMENT OPTIONS**

Wireless Ethernet devices are generally co-located with the network elements to be interconnected, up to the distance allowed by the interconnecting Ethernet cable. A separately locatable radio (rather than one integrated into the Ethernet device) and antenna type options are significant pluses, as these features allow for the placement and type to be customized according to specific site needs.

To achieve maximum range in outdoor applications, antennas should be installed as high as possible and within line of sight of corresponding wireless Ethernet devices. In indoor applications, line-of-sight is typically not necessary (or is unavailable), as the RF signal will bounce off walls and objects to reach the other radio. Directional antennas generally provide better performance than omnidirectional ones, not because of their associated gain increase, but because their backside rejection reduces multipath cancellation.

## **OPERATIONAL RANGE**

Range is the most difficult of criteria to assure; it is easier to predict outdoors due to the relatively larger amount of multipath observed in indoor environments. If transmission range is insufficient, an application may simply not work or may require repeaters or additional access points. Effective range is influenced by physical obstructions (walls and other structures or furniture) and electrical interference (other wireless devices or electrical noise) present in the environment.

A basic industrial wireless Ethernet solution must exhibit reasonably long range performance without the aid of supplementary devices. The 802.11b standard, which has a typical maximum operating range of 300 feet, falls short of expectations on the typical factory floor. To extend its range, an 802.11b-based system requires repeaters and extra base stations, adding expense, unnecessary network complexity and, ironically, extra cabling. Suitable industrial wireless Ethernet links, on the other hand, provide operational range on the order of miles without additional equipment.

While standards-based wireless Ethernet devices offer excellent connectivity in many settings, their performance profile undergoes dramatic alterations when deployed for applications beyond their design objectives. Such is the general case with 802.11b-based wireless Ethernet solutions in industrial and factory settings.

To deliver industrial-grade data communications with the needed speed and reliability, a wireless Ethernet solution must meet or exceed the outlined performance criteria with comprehensive flexibility and scalability features.

## **CIRRONET SOLUTIONS**

Cirronet, Inc. offers a full range of high-speed wireless solutions for industrial and factory data communications applications. Proven patented technology, robust error checking, and front end filtering enable the company's industrial products to excel in the most challenging of control and monitoring applications. Unique Cirronet product attributes include:

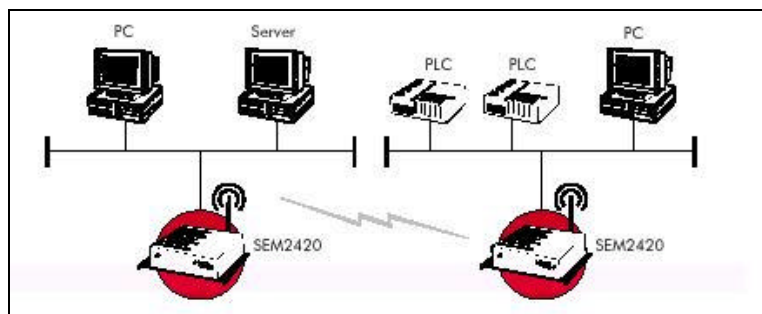
- **Cirronet FHSS Technology.** Developed and refined over a period of ten years, Cirronet's innovative FHSS engineering has earned the company five patents. More than just theoretically successful, both real world and in-lab testing show that Cirronet's FHSS-based products outperform others, particularly in tough factory and industrial settings. The protocol is especially fast and reliable, offering superior performance and unparalleled immunity against jamming and interference.
- **24-bit Cyclic Redundancy Check (CRC).** Comprehensive error detection and correction algorithms are critical protocol components for reliable data transmission. Cirronet's 24-bit CRC ensures error-free data delivery by checking the integrity of each data packet received.
- **Automatic Repeat-Request (ARQ).** ARQ enables transparent data retransmission in the event an error is detected by the CRC mechanism. ARQ uses an acknowledgement to indicate that data was received without error; if an acknowledgement is not received, data is retransmitted. The approach offers significantly lower overhead than Forward Error Correction (FEC)—when data is received without error, the only overhead is the acknowledgement—typically a few bytes.
- **Data Security.** Star topology allows only remote-to-base communications and provides inherent security against outside intrusion. Systems allowing peer-to-peer communications (such as 802.11) allow foreign device to tap into unprotected wireless networks. If the factory floor network is tied to the corporate MIS network, for example, sensitive corporate information can be exposed. By rapid and continuous change of frequency, Cirronet's FHSS provides an additional layer of security and makes the transmission very difficult to detect.

## CIRRONET WIRELESS ETHERNET BRIDGES

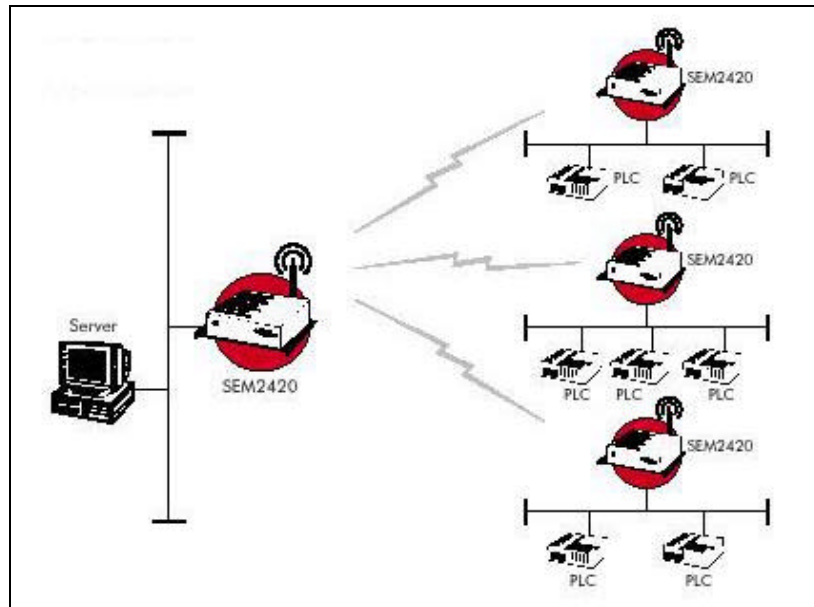
Cirronet's spread spectrum Ethernet bridges (SEMs) provide long range, high-speed wireless connectivity among Ethernet devices in industrial settings and over distances far exceeding typical cable run length maximums. SEMs have many uses, including network bridging, PLC networking and SCADA among other industrial automation and data collection applications. SEM features include:

- **High Speed, Reliable Data Throughput.** Up to 1 Mbps throughput, with 1.23 Mbps total over-the-air bandwidth.
- **Long Range Operation.** SEMs provide wireless connectivity for Ethernet network nodes up 1.5 miles apart with the standard whip antenna. Optional gain antennas substantially extend operating range.
- **Standard Ethernet Connection.** 10Base-T and/or 100Base-T connections (depending on model). Wirelessly networks all Ethernet-equipped devices, including sensors, PLCs, and PCs.
- **Patented FHSS Technology.** Proven frequency hopping performance for quick and reliable transmission of critical data.
- **Interference Immunity.** Superior resistance to RF interference and multipath fade.
- **License-free Operation.** Globally license-free 2.4 GHz ISM band.
- **Rugged Packaging.** Industrial and weatherproof enclosures assure solid, error-free data communications harsh and outdoor environments.
- **Fully Configurable Operation.** SEMs' operational parameters, including radio transceiver and network settings, can be customized to meet specific site requirements.

SEMs operate in point-to-point (see Figure 2) or point-to-multipoint (star) configurations (see Figure 3), allowing systems integrators and end users to easily configure highly complex network topologies.



**Figure 2:** An example of a point-to-point Cirronet SEM bridge configuration used to bridge separate Ethernet network segments and PLCs.



**Figure 3:** A point-to-multipoint Cirronet SEM bridge configuration used to interconnect a remote server to multiple Ethernet network segments.

## SEM WIRELESS ETHERNET BRIDGE MODELS

The range of available SEM wireless Ethernet products include Cirronet's transmission and robust performance characteristics and differ only in data throughput and packaging details, as described below.

- SEM2411** High-speed wireless Ethernet bridge: up to 1 Mbps throughput (500Kbps full-duplex) and 1.23 Mbps total over-the-air bandwidth. Provides up to 1.5 mile communications range with a 4" unity gain antenna; range easily extended with optional gain antennas. 10/100Base-T Ethernet port.
- SEM2411X** A SEM2411 packaged for harsh and outdoor environments. Uses a remote, weatherproof radio housed in a polycarbonate, NEMA 4X enclosure.
- SEM2410** Wireless Ethernet bridge featuring 200 Kbps of full-duplex data throughput and 460 Kbps total over-the-air bandwidth. 10-BaseT Ethernet port.
- SEM2410X** A SEM2410 with a remote weatherproof radio housed in a NEMA 4X enclosure.

## **ABOUT CIRRONET, INC.**

For more than 14 years Cirronet has been a leading supplier of solid, high performance wireless products for industrial and commercial applications. Cirronet's offerings include a full array of roaming, base station, and bridging products to interconnect monitoring and control equipment over substantial distances, reliably and cost-effectively.

Cirronet product applications include SCADA, medical telemetry, mining vehicle control, fleet management, remote overhead crane control, factory automation and nuclear power plant radiation monitoring. The products are also key in telemetry and control systems for Tokyo Disney, mechanical dinosaurs used by the motion picture industry, and lighting at New York City's Times Square.

All Cirronet products are FCC and ETSI certified and operate in the globally license-free 2.4 GHz ISM band. For more information, visit [www.cirronet.com](http://www.cirronet.com).