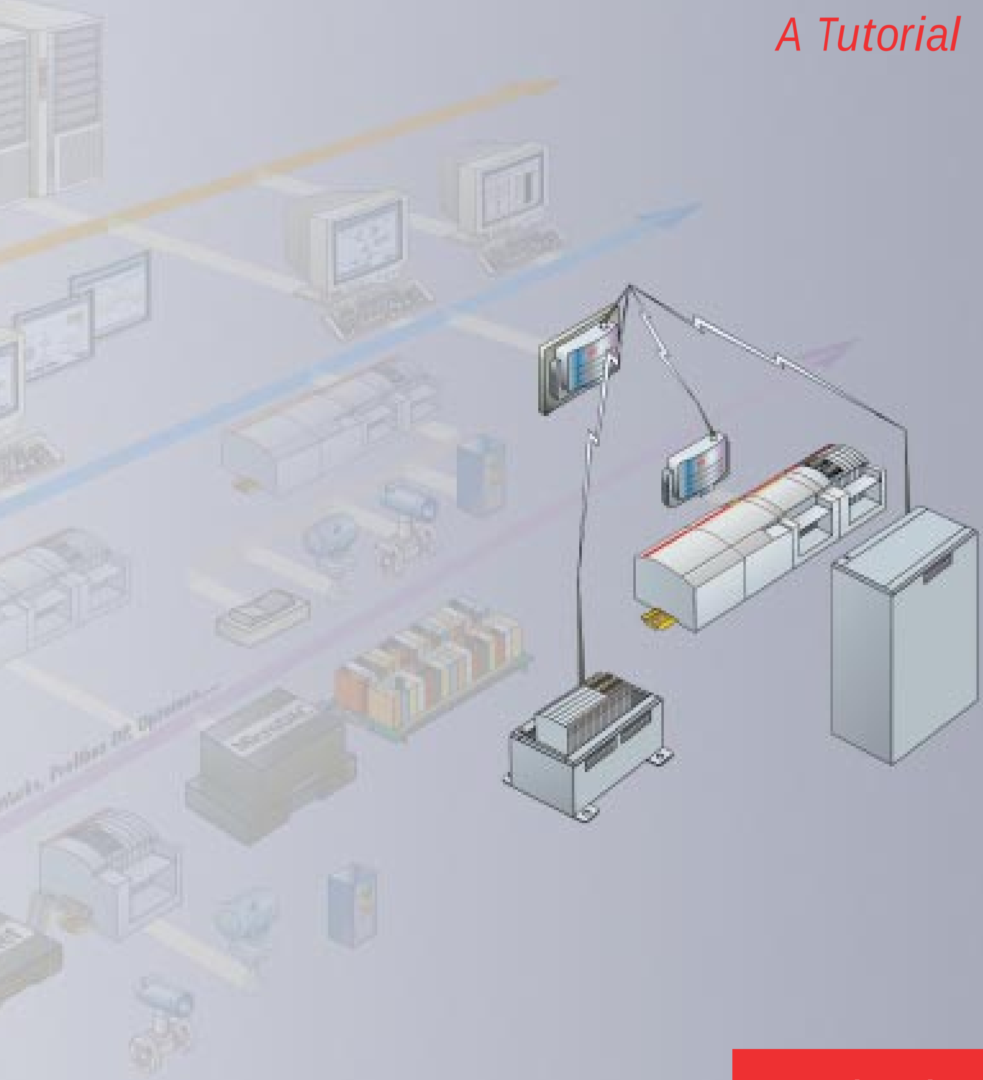
$\$14^{95}$

Wireless Communications for Industrial Automation

A Tutorial



By Bob Hochreiter

Table of Contents

Today's Reliable Wireless Local Area Networks: An Executive Overview

Until recently, the networks which interconnect computers and equipment in industry have been seriously limited. The limitation? Wire.

Local Area Networks (LANs) run on wire cable. Wire is expensive to install. It is difficult to reconfigure for changes in the production environment. It is susceptible to picking up electrical noise. It does not allow for mobility, and there are certain places it can't go. Because of these limitations, many companies are not networked to the degree they would like.

The wireless technology available today allows you to expand your wire network by the addition of radio transceivers. These transceivers send and receive signals across parts of the network which are not connected by wire. The transceivers do all the work of translating the electronic signals on the network into radio signals and send them over the airwaves. The radio signals are received by the transceiver at the other end, which translates them back into network signals and sends them along that part of the network.

To the computers, PLCs, controllers, sensors and actuators on an industrial network, wireless technology is totally "transparent."
A network which includes wireless technology operates exactly the same as one that is totally wire. No special hookups or programming are needed.

There is more good news: Wireless products used to expand a network often cost less than the expense of installing wire. Wireless portions of the network are also easily reconfigured, which gives companies the flexibility they need to make changes. Plus, wireless transceivers are easy to install, maintain network speed, and match or exceed the reliability of wire.

The Demand on Today's Networks: Speed and Flexibility

Today's manufacturing and processing industries need to provide quality products and services quickly. To accomplish this, the production process must provide four crucial elements, all of which depend on interconnected microprocessors, software and equipment:

- ***Flexibility*** – To beat the competition, you must constantly update and improve your products and processes. This means reconfiguring assembly lines and redesigning processing facilities.
- ***Quality Control*** – Today's QA/QC demands high levels of coordinated data acquisition and analysis.
- ***Inventory Control*** – Just-in-time business strategies mean lower overhead by reducing or eliminating warehousing needs. But poor inventory control can bring an assembly line to a standstill for lack of materials – quickly wiping out those warehousing savings.
- ***Speed*** – The people who need your products or services are also operating on just-in-time principles. If you can't get deliver promptly, they lose production time. And you lose customers.

Well-designed automated software and systems running on local area networks (LANs) on the plant or factory floor can help your company achieve these goals economically. In the following pages, we'll look at what is running on the typical industrial LAN and how it can be improved.

The Task of Local Area Networks in Industry

Industrial local area networks (LANs) are used to establish communication between computers, programmable logic controllers (PLCs), and a variety of industrial devices such as I/O modules, motor starters, sensors, actuators, valves, and so on. LANs can have several control points governing functions cooperatively or all functions can be controlled from a central location.

Many industrial facilities lack the network coverage needed to operate effectively. Most have isolated islands of automation. That is, various operations of the manufacturing or processing plant are automated, but the whole is not integrated. The left hand does not know what the right hand is doing. Coordinating this type of a manufacturing enterprise is highly labor-intensive.

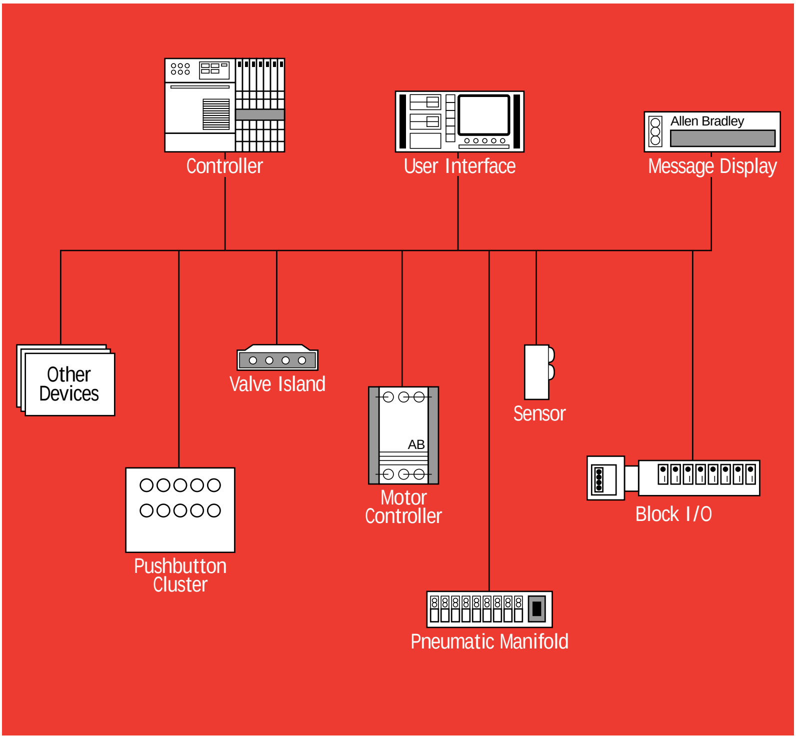
The challenge is to get all of these components to communicate together and function as a system. To do this they must first, of course, be connected. The typical industrial LAN will have everything interconnected with wire cable.

The second challenge to coordinating the network is that all components must use the same protocol (understand the same electronic code coming from the computers, PLCs, etc.) and run on the same buses. The problem is that in any industrial facility, there will already be a variety of protocols in place – protocols such as Ethernet, ProfiBus, Modbus, DeviceNet and dozens of others – with the corresponding hardware buses on which they run. Replacing the equipment that runs on these protocols and buses could be prohibitively expensive.

So we have two major problems to contend with in networking the industrial enterprise: wire and protocols/buses.

The Limitations of Wire Networks

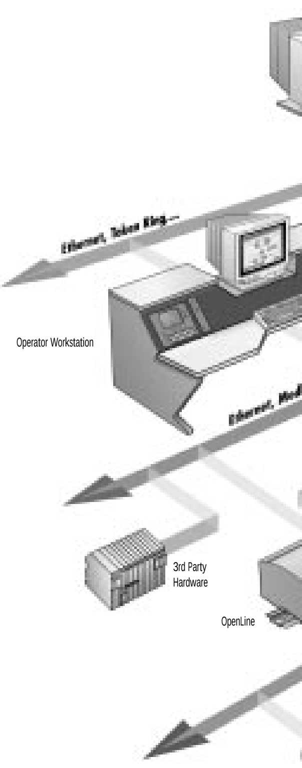
Figure 1. Typical Hard-Wired Industrial Network



While LANs that are totally interconnected by wire are generally reliable, they do have their limitations:

- ***Physical limitations and problems*** – Wires break; bad connections can cause ‘standing waves,’ which degrade performance. In addition, wires pick up electronic noise.
- ***Cost of installation and maintenance*** – Designing and installing wiring is usually a time-consuming and costly task. Maintaining outdoor wiring usually puts technicians up on a pole or down in a hole just to access the wire. And then, locating the problem can be extremely difficult.
- ***Protocol incompatibility*** – Existing systems in industrial facilities are frequently tied to incompatible protocols. Connecting these systems and getting them to “talk” to one another is a difficult task at best.
- ***Lack of mobility and adaptability*** – When your products or processes change, your production facilities must change. Wiring must be replaced or re-routed to accommodate the changes. This can be a huge headache and expense.
- ***Distance and space limitations*** – The longer the wire, the more susceptible it becomes to electrical noise and the more difficult it will be to locate problems when they occur. Wire can be damaged, crimped and cut in hard-to-find places. If wire must run outdoors, it is difficult to protect it from the extremes of weather. It is also not practical to run wires in places where they could be exposed to extreme temperatures, get in the way of moving machinery, etc.
- ***Wire logistics*** – In sophisticated configurations, the complexity of the wiring can be overwhelming. The insides of panels begin to look like spaghetti bowls. This means a slower set-up time and longer repair delays.

What is a WLAN?



A Wireless Local Area Network (WLAN) is a LAN that uses transceivers that exchange radio signals to substitute for some or all of the wires. (Transceivers are radios that can both send and receive). WLANs do not typically replace wired LANs. They allow you to expand the LAN to places where wire is inconvenient, cost-prohibitive, or ineffective.

There are two parts to a wireless LAN: the access point transceiver and the remote client transceivers (see Figure 2). The access point is the stationary transceiver that attaches to the main wired LAN. The remote client transceivers link the remote parts of the LAN to the main LAN via radio waves. The main LAN and the remote parts of the LAN have no physical contact, but from the point of view of all the computers, equipment, sensors and actuators, they operate exactly as if they were one large, hard-wired LAN.

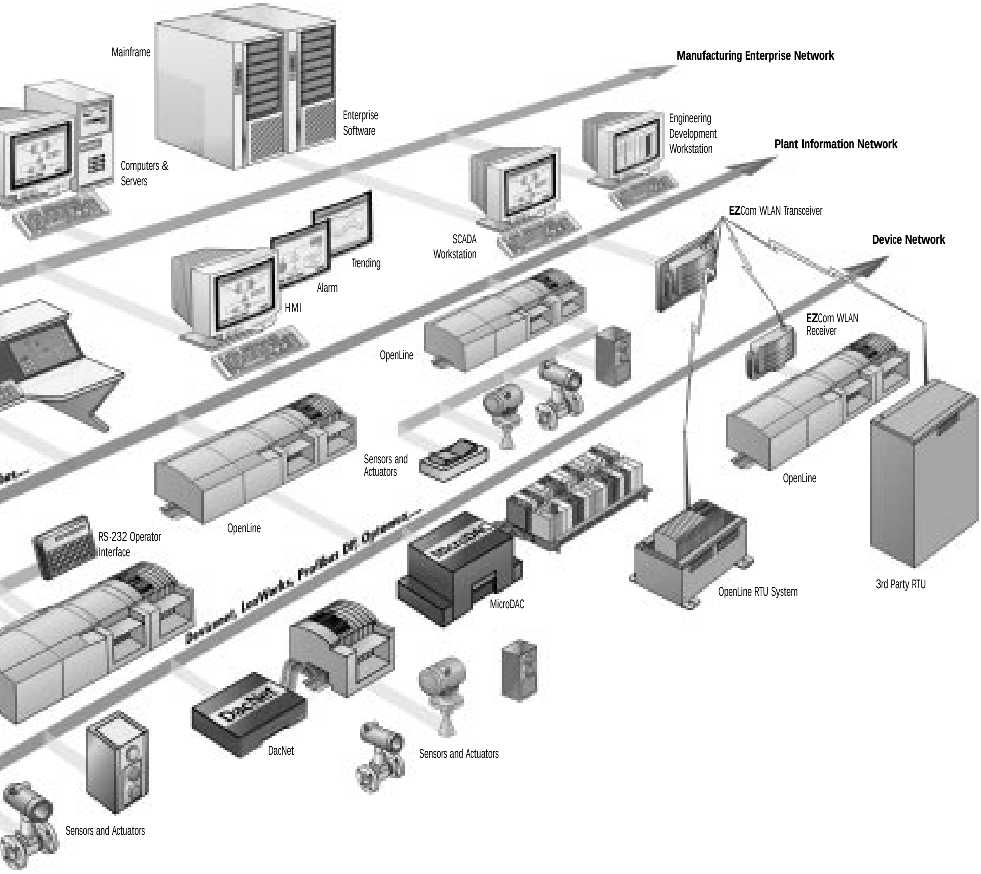
(Note that there are also wireless modems today that provide a partial networking solution. They require special software, programming, and a direct hookup to the PLC. Because of the difficulty of installation and operation, these wireless modems are an inferior solution.)

The advantage of adding WLANs is in increased flexibility, mobility and the ability to reconfigure. Equipment no longer has to be anchored to a fixed spot. The user no longer has to work from a stationary workspace. Parts of the WLAN can be located across spaces that are impossible to bridge by wire.

Protocol “Gateways” and “Bridges”

In addition, the transceivers of a WLAN can form protocol “gateways” and “bridges.” A gateway works like this: The access point transceiver communicates in one protocol with the main LAN while the remote transceiver communicates with the remote LAN in another. The WLAN

Figure 2. Wireless Industrial Network



In a WLAN, remote components are connected to remote client transceivers which send and receive signals to and from the access point transceiver on the main LAN.

transceivers do all the work of making the previously incompatible equipment speak to one another. Protocol "gateways" among as many as fourteen different industrial protocols are in the works. (See Figure 10).

Protocol bridges are used to link to LANs that use the same or very similar protocols. They do not require as much "translation" functionality as gateways.

Advantages of WLANs

Impossible Wiring Problems Solved – How do you maintain electrical contact over the heat of a blast furnace? Across a burning desert? A frozen tundra? A busy street? With a WLAN, wiring isn't necessary. Radio waves pass easily through heat, cold, traffic, and the flames of a furnace.

Long-Distance Capabilities – Interconnecting production or processes in a large facility or a network of facilities can use up many miles of wire. The transceivers of today's WLANs have ranges of 5 to 15 miles and can be extended almost limitlessly with the use of repeaters.

Flexibility – With WLANs, changes to production line or process configuration can be made quickly – without closing it down for lengthy periods for costly and time-consuming rewiring.

Reduced Wiring Costs – With wireless components connecting key parts of the LAN, there is less wire to install and to maintain.

Mobility – Workers on the go can use portable terminals to send inventory, production, or shipping and receiving information to a central data-collecting computer.

Noise Resistance – The new WLANs using spread spectrum technology are impervious to industrial electrical noise.

Reliability – The new wireless communications are actually more reliable than wire. They are virtually jam-proof.

No Service Provider Needed – No hidden costs. You do not require a license or a service provider (as with cellular phones, ESMR mobile radios, and pagers) to operate on the radio wavelength WLANs use.

Data Security – It is extremely unlikely that the electronic signals on your industrial WLAN could be readable by anyone anyway – but because of spread spectrum technology (see page 14), the transmission is virtually impossible to intercept by unauthorized "listeners." WLAN-transmitted processes cannot be jammed or intercepted by the competition.

Would Your Operation Benefit from a WLAN?

The growth in the use of WLANs is increasing rapidly as the technology improves and prices become more competitive. Many industries, or sectors of industries, already accept wireless technology as the norm. This includes many water and wastewater treatment plants, oil and gas facilities, electrical utilities, irrigation systems and more.

Other uses, such as facility and machine maintenance, are beginning to experience rapid growth. And with the latest WLAN technology the way is finally open for all kinds of manufacturing and processing applications, particularly in data acquisition and control networks. The field is poised for an explosion of applications.

(For more details on applications, see the section *Current and Emerging Applications*, page 21.)

Spread Spectrum Technology

The basic spread spectrum technology that makes wireless local area networks possible has been around for a long time. The United States military developed spread spectrum radio during World War II as a way to send radio signals that resisted jamming and were hard to intercept.

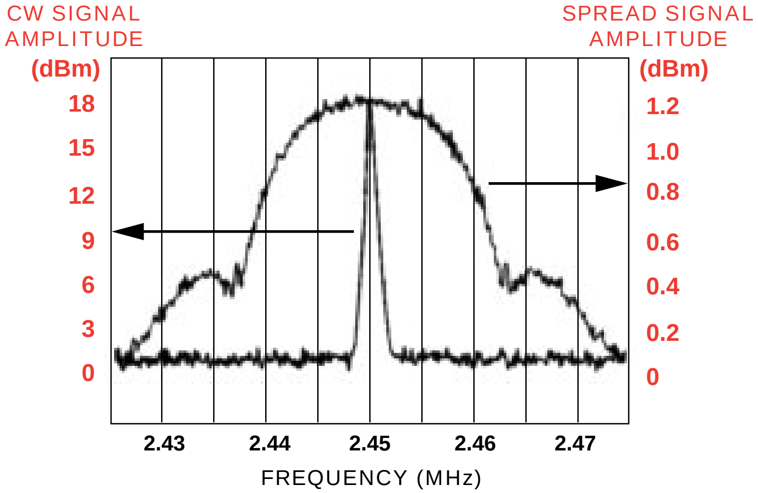
Spread Spectrum refers to a class of modulation techniques characterized by wide frequency spectra. A true spread spectrum signal meets two criteria:

1 The transmitted signal bandwidth is much wider than the information bandwidth (see figure 3). Instead of a narrow, specific frequency like that used by an FM radio station, the signal is much wider than is actually necessary for the information being transmitted. The actual data being transmitted is modulated across the wide waveband and sounds like noise to unauthorized receivers.

2 Some pattern or code other than the data being transmitted determines the actual transmitted bandwidth. It is the use of these codes that allows the authorized receiver to pick out the needed information from the signal. The width of the signal and the structure of the code allow the data being transmitted to be understood even if parts of the signal were to be blocked by electrical noise.

Because spread spectrum is immune to interference in this way, it's a natural for industrial network applications. The FCC has set aside three bands for commercial spread spectrum use: 900 MHz, 2.4 GHz, and 5.7 GHz. Products operating in these bands are operating where very little industrial noise is present. No FCC site licensing is required in the ISM band.

Figure 3. Spread Spectrum



Spread Spectrum takes its name from the wide bandwidth it uses. The wide bandwidth is part of what makes it immune to interference. Compare to the narrow FM band shown in the center of the graph.

Selecting the Right Spread Spectrum System

Of the various spread spectrum systems that have been adapted for commercial use, the two most commonly used are:

Direct sequence spread spectrum (DSSS) systems encode the data to be transmitted by using a seemingly random sequence of binary values. This is called a pseudo-random noise (PN) code. The combined digital data and PN are scrambled and spread over a fixed range of the frequency band. Because the PN code has a frequency bandwidth much higher than the bandwidth of the data, the transmitted signal will have a spectrum that is nearly the same as the wideband PN signal.

On the other end, a receiver correlator picks up the signal. This SS correlator is ‘tuned’ so it only responds to signals that are encoded with the specific PN code. The correlator filters out all the garbage and extracts the needed coded information. This allows several sets of transceivers to operate using different codes in the same geographical area without interfering with each other. This is called Code Division Multiple Access (CDMA).

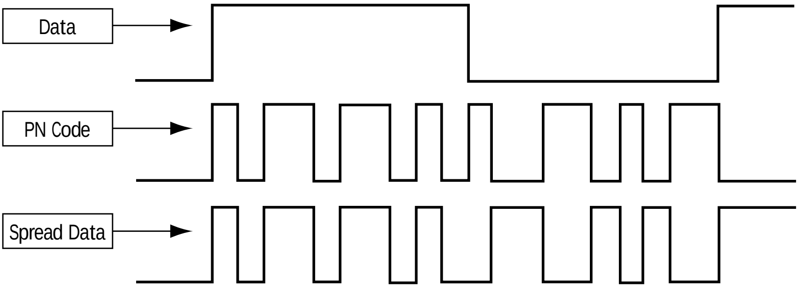
Frequency hopping spread spectrum (FHSS) means the signal is spread over a wide band by transmitting for a short burst and then ‘hopping’ to another frequency. The order of the hops depends on the code sequence.

Two key elements are needed for FHSS systems to function. First the hopping pattern must be known to the receiver. Second, the radio designated as “master” must provide the synchronization so that other radios using the same pattern can follow and hop at the same time.

Although different, both FHSS and DSSS products are well-suited to industrial applications due to their noise immunity and ruggedness.

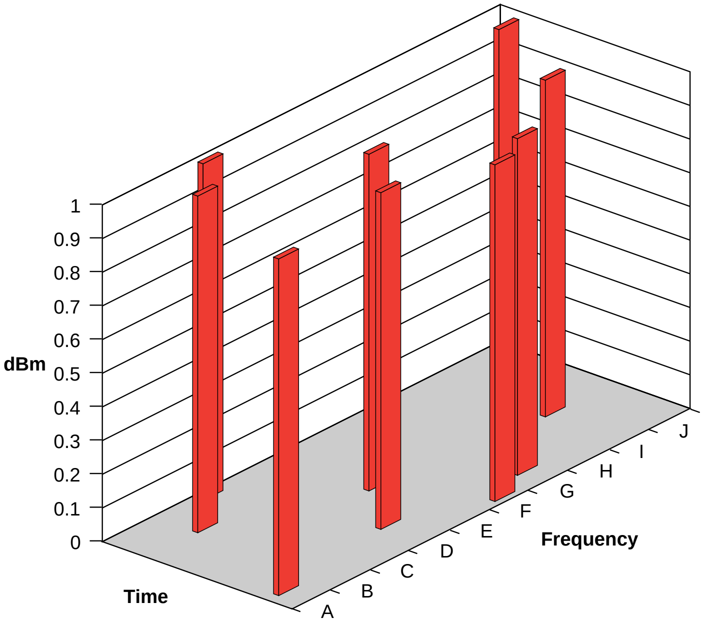
Grayhill **EZ**Com wireless includes products that use FHSS and products that use DSSS spread spectrum.

Figure 4. Direct Sequence Spread Spectrum



The spreading of the data is achieved by modulating the data by a pseudo-random sequence of binary values called a PN code.

Figure 5. Frequency Hopping Spread Spectrum



FHSS spreads the signal by transmitting for a short burst and then "hopping" to another frequency. It dynamically and automatically adjusts to changing interference profiles for superior performance.

WLAN Reliability

Spread spectrum technology enables WLAN radio communications to reliably take the place of wired system components by allowing for:

Multiple-channel capabilities – Using spread spectrum technology means a number of wireless communications devices can transmit in the same work environment at the same time. This is done by establishing a different channel to run each device. Different channels are created by using different sequences of frequency hops in an FHSS system, or by different code patterns in a DSSS system.

Multiple Access is obtained by using Carrier Sense (CS) Multiple Access (MA) with Collision Avoidance (CA). Carrier Sense means the device will ensure that nothing else on its channel is being transmitted before sending out information. Multiple Access means any radio can transmit when no carrier is present on its channel. Collision Avoidance uses a scheme where the transmitter must first send out a Request to Send (RTS) packet. This allows all transceivers on that channel to take turns sending and receiving without ever "speaking" on top of one another.

Alleviating 'dead spots' – Transmissions can be uniform throughout the work environment despite any obstacles by the strategic placement of antennas and by the appropriate use of repeater units to receive and send on signals around obstacles like large metal machinery.

Reliability is King

Most competing wireless devices use automatic request for resend as the main line of defense against faulty transmissions. But if it's garbled the first time, what prevents it from being garbled the next time? Grayhill codes transmissions so that if data comes through skewed, the message can still be restored.

Dynamic Forward Error Correction (DFEC) – If the message doesn't go through, the transceiver will resend it with additional coding. The additional coding adds redundancy to the signal to help it be understood despite interference. If the signal is still poorly received, levels of coding continue to be added until the transmission goes through clearly.
The transceiver keeps track of the level of coding needed for clear communication. It automatically adapts based on these link statistics.
If necessary, it adds interleaving to the coding.

Interleaving – In addition to channel coding, interleaving can be created by loading information in rows and transmitting it in columns. The receiver then receives the information in columns and turns it back into rows. If a part of the signal gets jammed, the loss is distributed over the whole information string – in other words, there are several small gaps instead of one large hole. Since error correction can piece together information more effectively with small gaps in the information, interleaving allows the message to be fully restored.

Orthogonal Codes – Grayhill's channels are orthogonally independent. Any two channels are only at the same frequency or code for a very short period. This is another part of the technology that allows independent wireless networks to operate in the same area without interfering with each other.

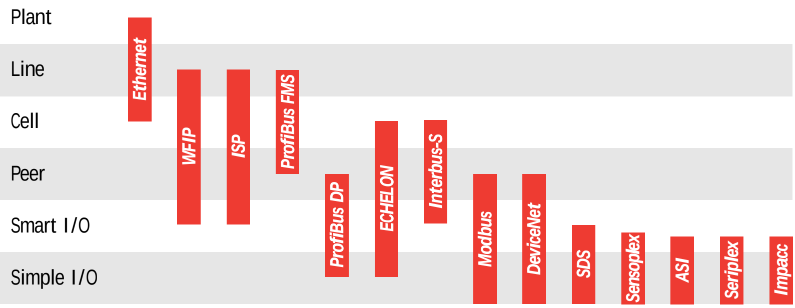
All in all Grayhill **EZ**Com Spread Spectrum transceivers are very smart radios.

Protocols

The wireless access point transceiver must be able to interface directly with the industrial network. To do this, they must share the same protocol. In today's workplace there is no single protocol dominating industrial LAN usage. Grayhill's **EZ**Com products will ultimately be compatible with the most popular protocols which comprise a majority of the networks.

Figure 6. Major Industrial Open Protocols

Comparison of Different Industrial Networks

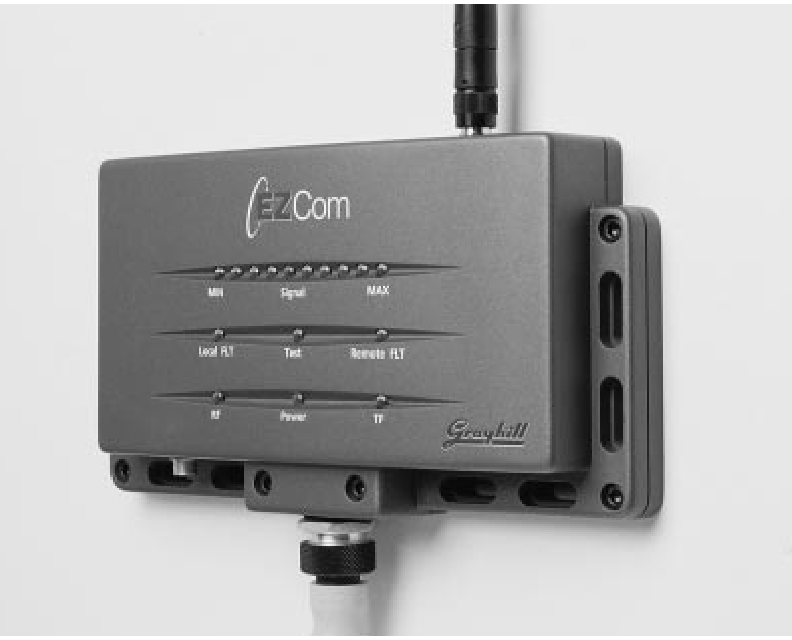


Control architectures employ multiple types of industrial networks. Sensorbus is the lowest level control architecture. Devicebus systems are intermediate level systems controlling sensors, switches, valves, and relays. At the highest level, fieldbus networks are more complex. They are generally used to communicate between controllers and host CPUs.

Grayhill **EZ**Com products are built to support devicebus and fieldbus level architectures.

This is Not Your Father's WLAN

Figure 7. Grayhill EZCom



Perhaps the biggest obstacle for acceptance of WLANs today is the problem with perception. Earlier wireless technologies have had drawbacks that have given rise to biases against wireless components that have little to do with today's WLANs.

Perception: WLANs are too expensive.

Reality: Like other computerized systems, WLANs are dropping in price due to advances in technology and competitive forces. Wireless systems are now competitive with and often more cost-effective than wired systems.

Perception: WLANs are unreliable.

Reality: Early generations of wireless devices suffered from inadequate or noisy signals. Technology has improved and site surveys can help determine any problem areas. Before installation, technicians locate areas where signals would be obstructed. These problems can be alleviated by antenna placement or adding redundancy in transceivers.

Perception: Transmissions are easily jammed.

Reality: Now that spread spectrum technology is used in WLANs, signals are impervious to jamming.

Perception: Wireless devices are too slow.

Reality: Today's top products clock in at 500 kbps, fast enough to support the most data-intensive application.

Perception: Anybody can intercept wireless transmissions, which means big headaches in keeping information secure.

Reality: Spread spectrum technologies were developed during World War II so radio transmissions couldn't be intercepted by the enemy. FHSS and DSSS techniques have been refined to make the radio signals nearly impossible for unauthorized receivers to decode. Levels of encrypted code can be added to many products to protect especially sensitive information. However, few WLANs are likely to be carrying security-sensitive information.

Perception: How can I trust wireless communications to run my production line when I can't trust my cellular phone not to cut off my conversations?

Reality: You can't judge WLAN components by cellular phone or other radio technology. Cellular phones move through huge spaces that are nearly impossible to cover effectively. WLANs are specifically set up for your facility and are built to be interference-proof. They also run on radio frequencies that are not overcrowded with the exploding market for cellular phones.

Current and Emerging Applications

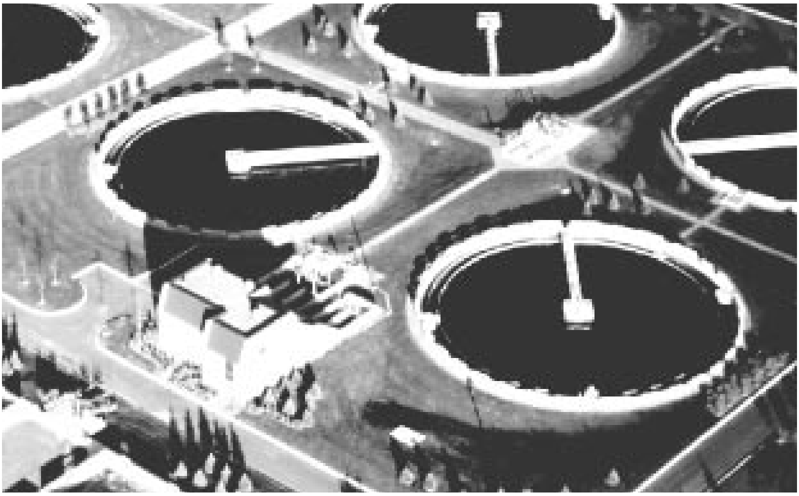
Wireless networks are being applied to a greater number of tasks in a wider range of industries than ever before. In general, whenever wiring obstacles make projects too complicated or when the data collection points need to be mobile, wireless LANs are the solution.

Water Treatment Facilities

Outdoor processing facilities like water treatment plants are a natural for WLANs. Water treatment units are often spread out on miles of land. They use both data acquisition and control technologies, and could benefit from integration through networking. Wiring the far-flung units is not only expensive but difficult to maintain. Networking via WLANs is the far more reliable and cost-effective solution.

For the same reasons, WLANs will provide advantages to oil refineries, multi-building processing and manufacturing facilities, and other large-scale enterprises.

Figure 8. Water treatment facility



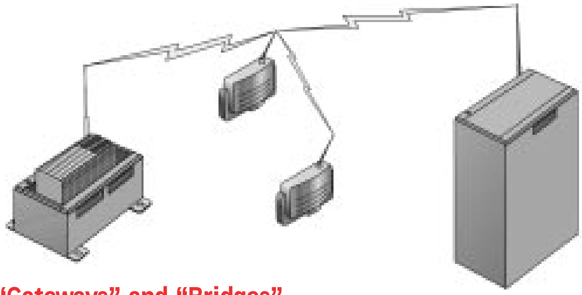
Flexibility in Manufacturing

Manufacturers today redesign their products continually. Automobiles change every year. Computers, printers and peripherals change nearly every month. And so production lines come and go and reconfigure constantly. WLANs make those changes far easier.

RTU

WLAN technology can be paired with controller technology to create an RTU (Remote Terminal Unit). The controller is used to control and monitor remote Input/Output points, while the WLAN transceiver connects the controller with the main LAN, a master station or other "host" unit. **EZ**Com transceivers and OpenLine control systems from Grayhill provide everything you need for RTU applications.

Figure 9. Grayhill EZCom & OpenLine RTU solution

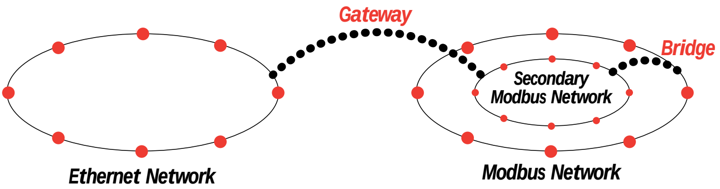


Protocol "Gateways" and "Bridges"

How do you connect an isolated "island of automation" to the main LAN when the island uses an incompatible protocol? WLANs provide the solution. Grayhill is working on the development for a number of protocol gateways. These will connect a main LAN with a remote LAN working on different protocols. Grayhill's goal is to provide gateways to connect the most popular industrial protocols.

Protocol bridges are used to link to LANs that use the same or very similar protocols. They do not require as much "translation" functionality as gateways. (For an explanation of how Gateways and Bridges work, see page 8).

Figure 10. Gateways and Bridges



Hospitals

The medical field has already embraced wireless technology. With wireless technology, such equipment as EKG or blood-pressure monitors need not remain in one spot. Any room in the hospital can become intensive care, simply by rolling in the needed equipment. Devices known as Multiple Parameter Telemetry (MPT) send information to the medical staff about the wearer's heart rate, blood pressure, and pulse. The hospital becomes more flexible and more cost-effective, because equipment can be more fully utilized.

Municipal Traffic Control

Traffic control uses wireless devices buried in the ground to send signals to collection points atop traffic lights. These are robust systems that remain effective through rain, ice and extreme temperatures.

Railroads

Railroads use wireless devices to help regulate traffic. In addition, WLANs could be used to increase the information exchange. As a train comes within radio range, a complete roster of passengers could be transmitted to the station. Local weather, traffic conditions, and other information could be transmitted back to the train, as well as data on track numbers to use, etc. Handling the logistics in a freight yard or at a railroad dock offers even more applications, including alerting the systems and personnel for unloading and tracking cargo.

Drive-By Data Collection

Power and gas utilities now install meters that send usage information to meter readers equipped with drive-by wireless devices. The time-savings is enormous.

And More Applications

The list of new WLAN applications gets bigger all the time. A sample of other applications include:

Agricultural/irrigation control equipment

Arcade and gaming machine monitoring

Computer-aided dispatch

Electronic display control

Environmental monitoring

Facilities and machine maintenance

Hazardous material monitoring

Inventory data acquisition

Machine-to-machine synchronization

Manufacturing control

Oil field monitoring

Pollution monitoring equipment

Robotic remote control

SCADA and telemetry

Security, alarm systems and building access control

Supervisory control

Water/wastewater facilities

Weather monitoring

The Grayhill Advantage

Grayhill brings its reputation as a leading manufacturer of electronic components and data acquisition and control products to the wireless LAN field. Our 50+ years of experience in creating and supporting products mean that you have a proven performer in your corner.

Grayhill provides:

Application support – Could a WLAN help your production or automation needs? Our support people can tell you. If you could use wireless technology, they'll show you how to plug into your LAN in the most efficient way possible.

Site survey – Our professional communication engineers will travel to your facility in order to design a robust system to meet your needs. Our experts will find noise sources and/or obstacles in your environment and design antenna and transceiver configurations to work around them.

Installation support – Our systems are designed for easy installation. We are also available to give you telephone and on-site support, with services ranging from consultation through installation.

The Grayhill Technology Advantage

Three basic qualities are built into the design of Grayhill **EZ**Com WLAN products:

Reliability – Grayhill WLANs are as reliable as – or more reliable than – a wired LAN. For worker safety and production efficiency, you can rely on wireless devices from Grayhill.

Transparency – Adding a WLAN to a wired LAN requires no changes in the wired LAN. To every other microprocessor and device on the network, the LAN still operates as if it were completely interconnected with wire. Grayhill transceivers translate the electronic signals on the LAN to radio waves, and then back to electronic signals at the receiving end. Just plug it in and you are ready to go.

Throughput – Grayhill transceivers work at a data rate that supports the speed of your LAN.

EZCom Wireless Products

Grayhill's **EZ**Com products go far beyond the wireless products available from other companies. Many of these competing products are nothing more than radio modems. They require special application programming and a special communications channel. In other words, they are an entirely separate communications link with separate software and programming for you to learn.

Grayhill **EZ**Com does the work for you. Each **EZ**Com radio contains three computers: 1) a network interface processor that translates the information coming from the LAN into information for the airwaves (and back from the airwaves into information for the LAN), 2) a processor that performs the spread spectrum modulation work, and 3) a processor that handles radio transmission, reception and the error correction.

EZCom products use sophisticated media access control algorithms for reliable data delivery. Interleaving signals allow the receiver to piece together transmissions despite interference. They use forward error correction and 32 bit CRC to eliminate radio induced bit errors. The wireless products of other companies do not support forward error correction.

EZCom automatically keeps track of the devices on the LAN. It recognizes its own clients and then adapts by filtering out all the signals. This cuts down the amount of information that has to travel through the network.

EZCom supports redundant links. The radio determines when a signal is not getting through and jumps to another path – without having to go through the user interface. The result is transparent redundancy.

Product Features and Specifications:

Transmission in the 900 MHz and 2.4GHz range, (above the frequency of industrial noise).

Transceivers have two antennas, reducing the multipath fading effect on signals that can occur in an indoor environment.

Dual antennas can be removed and mounted remotely. A signal strength indicator on the face of the unit also aids during installation and troubleshooting.

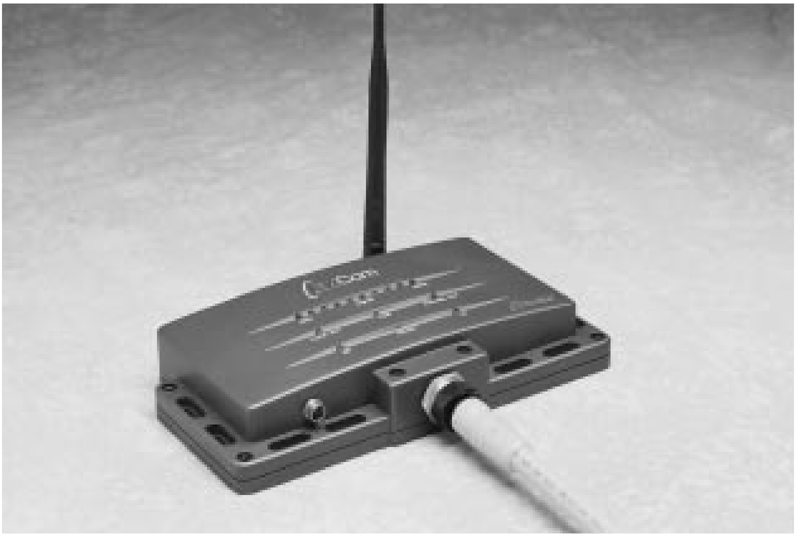
Data rates up to 500 kbps.

Minimum range of 500 meters indoors, 5 to 15 miles outdoors, which can be extended almost limitlessly with the use of repeaters.

Grayhill has designed **EZ**Com products to transmit at the maximum output allowed by the FCC.

Grayhill offers an access point transceiver for connecting with the main LAN, a remote client transceiver for connecting with remote devices, such as controllers, block I/O, sensors, etc., and a repeater for extending the range and reliability of transmissions.

Figure 14. Grayhill EZCom



Contact Grayhill

For more information call:

Phone: 708-354-1040
Fax: 708-354-2820
E-mail: ezcom@grayhill.com
On the Internet: http://www.grayhill.com

ISO-9001 Certification. In February, 1992, Grayhill became one of the first in its field to receive ISO 9001 certification. All materials are rigorously tested to ensure our products meet the stringent International Organization for Standardization requirements.

EZCom

Grayhill INC.
An ISO-9001 Company

561 Hillgrove Avenue
P.O. Box 10373
LaGrange, Illinois 60525-0873 USA

Phone: 708-354-1040
Fax: 708-354-2820
E-mail: ezcom@grayhill.com
On the Internet: http://www.grayhill.com