White Paper

Applying Wireless to EtherNet/IP Automation Systems

Gary Enstad & Jim Ralston
ProSoft Technology®, February 2009
www.prosoft-technology.com/wireless

Introduction

The use of Ethernet for industrial networking is growing rapidly in factory automation, process control and SCADA systems. The ODVA EtherNet/IP network standard is gaining popularity as a preferred industrial protocol. Plant engineers are recognizing the significant advantages that Ethernet-enabled devices provide such as ease of connectivity, high performance and cost savings.

While EtherNet/IP has many advantages, cable installation is often expensive, and communications to remote sites or moving platforms may not be reliable or cost-effective. Wireless Ethernet technologies have emerged that can now reliably reduce network costs while improving plant production.

However, applying these technologies is not a simple matter as industrial Ethernet systems vary greatly in terms of bandwidth requirements, response times and data transmission characteristics. This paper will explore applying IEEE 802.11a/b/g and proprietary frequency hopping wireless technologies to EtherNet/IP based networks for industrial automation systems.

EtherNet/IP Characteristics

Ethernet Industrial Protocol (EtherNet/IP) is a network protocol defined by Open DeviceNet Vendor Association (ODVA). As an open standard, vendors may implement EtherNet/IP communications in their devices without licensing fees. Many vendors have adopted EtherNet/IP including Rockwell Automation, who selected the protocol as one of three preferred networks on their popular Logix controllers (DeviceNet and ControlNet are the other two).

An important part of the EtherNet/IP standard is definition of Common Industrial Protocol (CIP) messaging. CIP defines the information packet with recognition that the message attributes will vary as applications do. Thus CIP message definition takes into account a wide range of applications including programming/diagnostics, data collection, PLC data exchange and I/O communications.

EtherNet/IP uses the standard 7 layer OSI model for protocol definition as shown in Figure 1.

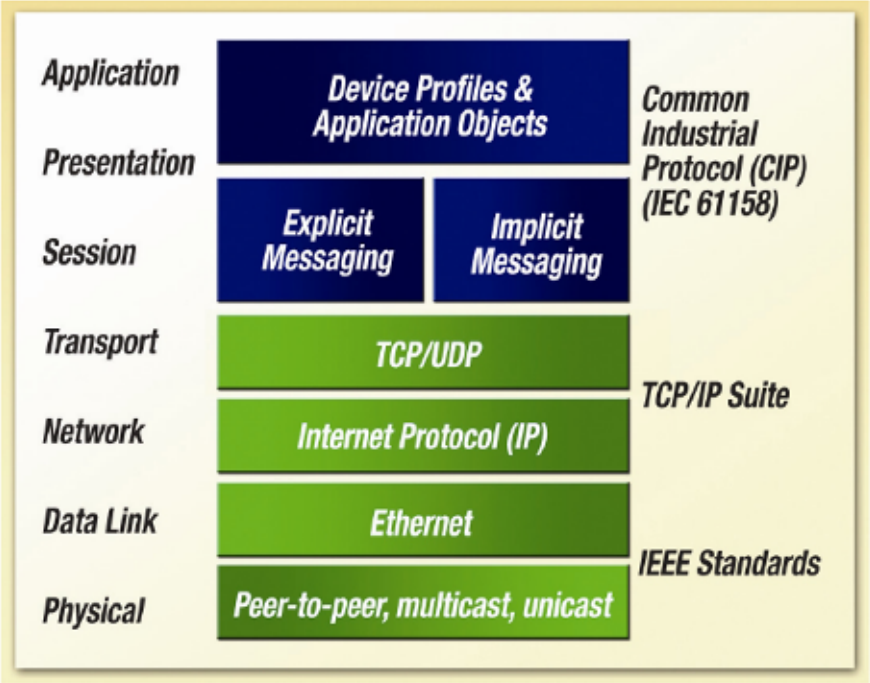


Figure 1: EtherNet/IP Protocol Stack

Implicit vs. Explicit Messaging

CIP defines two different types of connections. The first type is Explicit CIP which uses TCP/IP for its communications protocol. Explicit messages are unscheduled and use a request/response communications procedure or client/server connection. Examples of Explicit: executing a MSG statement between PLCs, HMIs, device diagnostics and program uploads/downloads.

The second type of CIP is Implicit; Implicit uses UDP/IP for its communication mechanism. Implicit connections are time critical, are scheduled and use a requested packet interval (RPI) parameter to specify the rate at which data updates.

Implicit connections use UDP packets for produce/consume data over an Ethernet/IP network. The UDP packets are usually multicast if there are more than one consumers of the data. This multicast address is assigned by the Ethernet/IP interface and is unique for each produced tag. Multicast IP addresses are used to make the network more efficient. A producer of data can produce data for multiple consumers. By using multicast packets, many devices can receive or consume this packet without the producer having to send it to each individual consumer.

EtherNet/IP I/O blocks may support two major implicit connection types: direct and rack optimized. A direct connection is a real-time, data transfer link between the controller and a single I/O module. Rack optimization is a connection option where multiple discrete I/O modules in a chassis can be consolidated to use a single connection. Analog modules typically can not be rack optimized and each analog channel uses a separate CIP connection.

Proper network design is critical for implicit networking systems in order to achieve predictable “deterministic” I/O performance and to ensure that I/O traffic does not “leak” outside of the automation network causing network degradation. ODVA recommends specific design strategies to ensure optimized network performance such as segmentation (isolating sub-networks), the use of managed layer three switches (IGMP snooping and multicast packet filtering) and high speed network infrastructure (100Base-T or faster). Wireless design is particularly critical as the wireless media is by nature slower than wired networks.

CIP Safety

CIP safety is an extension of standard CIP. CIP Safety simply extends the application layer by adding a CIP safety layer to it. CIP Safety has generally been used where reliable communications is a must or stop on a failure is required. It has many triggers in place to detect critical and non critical errors and to close the connections in order to assure a safety condition.
New Specifications enhancements have been added to allow safety applications to have longer fault tolerances and the ability to assist in maintaining operations over wireless networks. Some of these enhancements include extending the RPI multiplier and the ability to configure the packet time expectation. These parameters are especially helpful in the wireless world where latency tends to be higher. This setting also could allow for re-transmission of RF packets if required to assure the safety packets get though. These changes lend themselves to make CIP safety well suited for wireless communications.

Value of Wireless EtherNet/IP

While EtherNet/IP networks grow in popularity, Ethernet infrastructure is not always easy, practical or cost-effective to install. The proper implementation of wireless Ethernet can reduce costs and in many situations improve reliability and increase plant production.

Wireless as an alternative to cable installation

The cost of installing cable in industrial plants is a function of the material costs plus the labor charges. Cable installation costs have been estimated as ranging from $20 to $2,000 per foot depending on installation challenges (distances, obstacles), environment and local labor costs. Factors that impact total cable installation costs include:

- Distance and number of locations
- Conduit design and installation
- Trenching
- Fiber optic cable & infrastructure (e.g. fiber switches)
- Hazardous location regulations

Once the total cost of cable installation is calculated, a comparison can be made to wireless. Similar to cable installation though, the *total* cost of wireless should be examined. This not only includes the wireless hardware (including wireless nodes, antennas and cables), but also antenna installation (if applicable) and personnel training. However, even when factoring in these additional costs, the savings realized by wireless is often dramatic and significant.

Additionally wireless (when implemented properly), offers better reliability than cabled systems because there are fewer mechanical connections to fail. If the cable is broken by moving equipment, severed during construction or damaged by vibration, production may be down for hours until the problem is located and corrected. Wireless also offers electrical isolation as fiber optics do, eliminating potential surge damage from ground plane transients.

Finally, a significant benefit of wireless is reducing project time. Wireless systems are typically much quicker to install than wired systems. This is especially beneficial in systems that move over time such as mining operations or the reconfiguration of production equipment on the factory floor.

Wireless in Motion

Where wireless can significantly benefit production is in processes using motion such as material handling systems where controllers and I/O are on moving platforms. Examples

include overhead cranes, transfer cars, stacker/reclaimer cranes, automatic guided vehicles (AGVs), conveyor systems and rotating packaging machines.

Mechanical methods of Ethernet communications (Figure 2) such as festoon cable systems, flex cable, slip rings and rails are prone to frequent maintenance and sudden failures. These systems are often relatively expensive, especially when supporting Ethernet.

Wireless may be less expensive and, if implemented correctly, significantly more reliable. Today, many of these mechanical systems are being retrofitted with wireless as production shutdowns become more frequent. Designing wireless into the system upfront could have reduced installation costs and increased plant production.

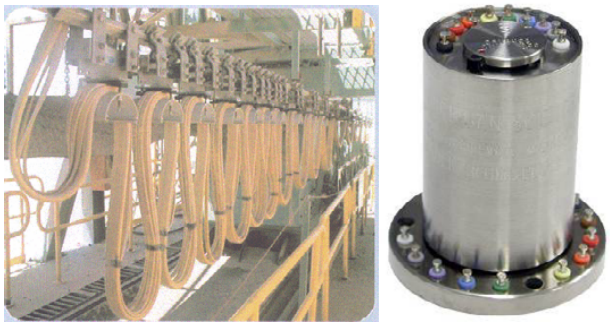


Figure 2: Festoon and Slip Ring Communication Systems

Wireless as a Leased Telephone Line Alternative

For distant sites, leasing phone lines for Ethernet communications is common. Most phone companies offer a range of digital services from 56 Kbps up to multiple Mbps.

Unfortunately, many remote industrial sites (such as pump stations, well heads and storage tanks) may be too far away from the telecomm infrastructure to support higher speed services. This can sometimes lead to telephone line reliability issues, which often frustrates production and maintenance engineers as the phone companies are notorious for slow service to industrial customers. Private RF systems (such as spread spectrum) are managed by the end user and do not rely on any third party services.

Cost is another problem when leasing of telephone digital circuits. Monthly charges may be as high as several hundred dollars per site, or even higher. Because these re-occur every month, a significant budget just for communication must be set. The initial cost of a private RF system may be higher, but there are no significant reoccurring costs. Return on investment for a complete wireless system may only take several months.

Industrial Wireless Considerations

TCP/IP or UDP/IP

Before selecting the wireless technology, it is important to consider the EtherNet/IP application and determine if it will be based on TCP/IP, UDP/IP or a combination of the two. This is important because TCP and UDP protocols behave differently over wireless networks.

UDP/IP is typically used in implicit messaging systems where controllers communicate to I/O blocks over Ethernet media. TCP/IP is much more common as it is the basis for explicit

messaging between controllers, HMIs, remote programming and data collection. Ultimately the automation architecture will determine the EtherNet/IP protocol type and appropriate wireless technologies.

Proprietary FHSS vs. 802.11 DSSS/OFDM

The most common approach to wireless Ethernet is RF transmission in the spread spectrum bands. Globally, the 2.4 GHz and 5.8 GHz bands are available for license-free use in most countries.

Spread Spectrum literally means spreading the RF energy across the entire (or wide portion of the) spectrum. This technique permits relatively high speed communications while being designed to operate in noisy environments where multiple RF systems are present. There are three major methods of spreading RF energy: Direct Sequence (DSSS), Orthogonal Frequency Domain Modulation (OFDM) and Frequency Hopping (FHSS). Each method has advantages and disadvantages for industrial wireless communications.

Direct Sequence and OFDM uses a wide channel within the band to simultaneously modulate a highly encoded bit pattern (see Figure 3.)

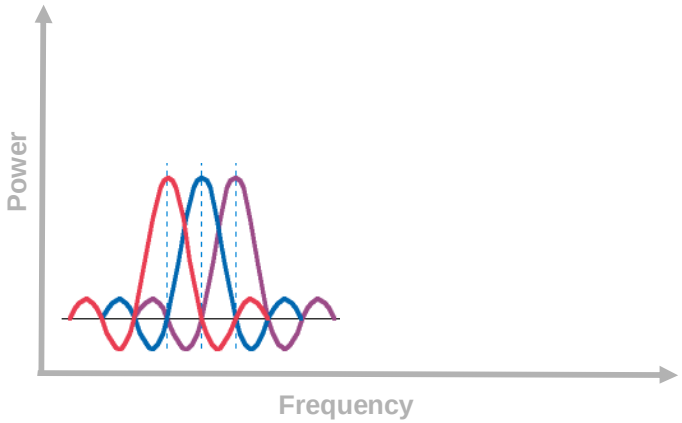


Figure 3. OFDM Waveform with Subcarriers

Direct Sequence and Orthogonal OFDM offer the fastest spread spectrum data rates as the wide channel permits transmission of complex modulation schemes. OFDM uses a complex modulation technique and is capable of high data rates and low latency (the transmission time a packet takes from one end to the other). OFDM is also significantly more immune to multipath fading, a problem due to RF reflections that high data rate systems frequently have. (Note that slower speed frequency hopping systems are relatively immune to multipath).

Direct Sequence and OFDM are the methods used by all popular open Wi-Fi standards today including IEEE 802.11b, 802.11g (both transmitting in the 2.4 GHz band) and 802.11a (transmitting in the 5 GHz band). IEEE 802.11n is nearing ratification at the time this paper was written, and will also incorporate these techniques. While the wide band modulation offers high speed, it unfortunately is more prone to noise problems when multiple systems are operating in close proximity. For example, IEEE 802.11b/g has thirteen available channels (eleven channels in North America), but only three channels don't overlap (see Figures 4 and 5).

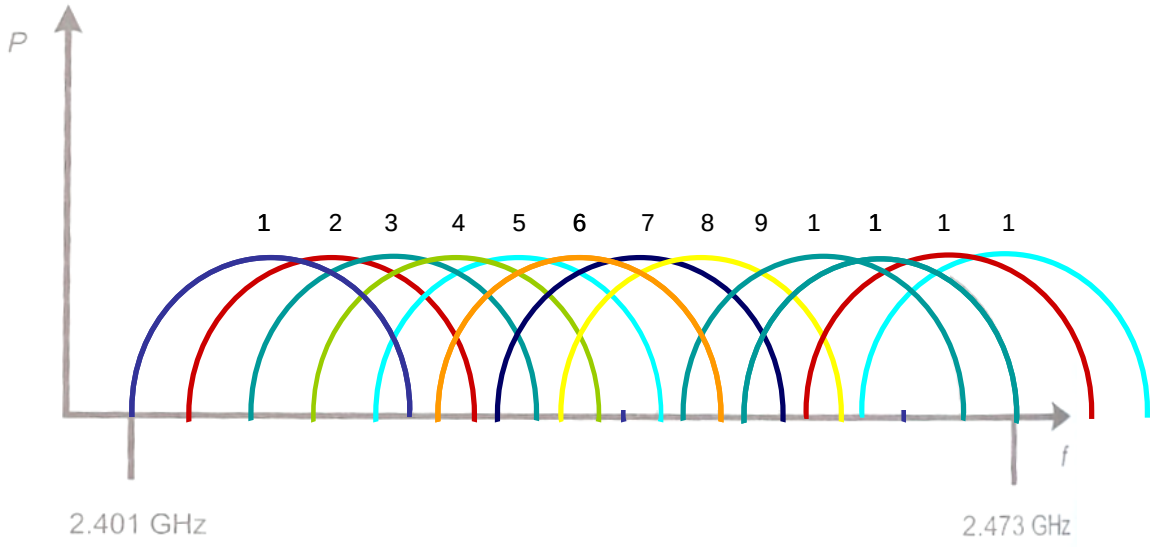


Figure 4. 802.11b/g Channels

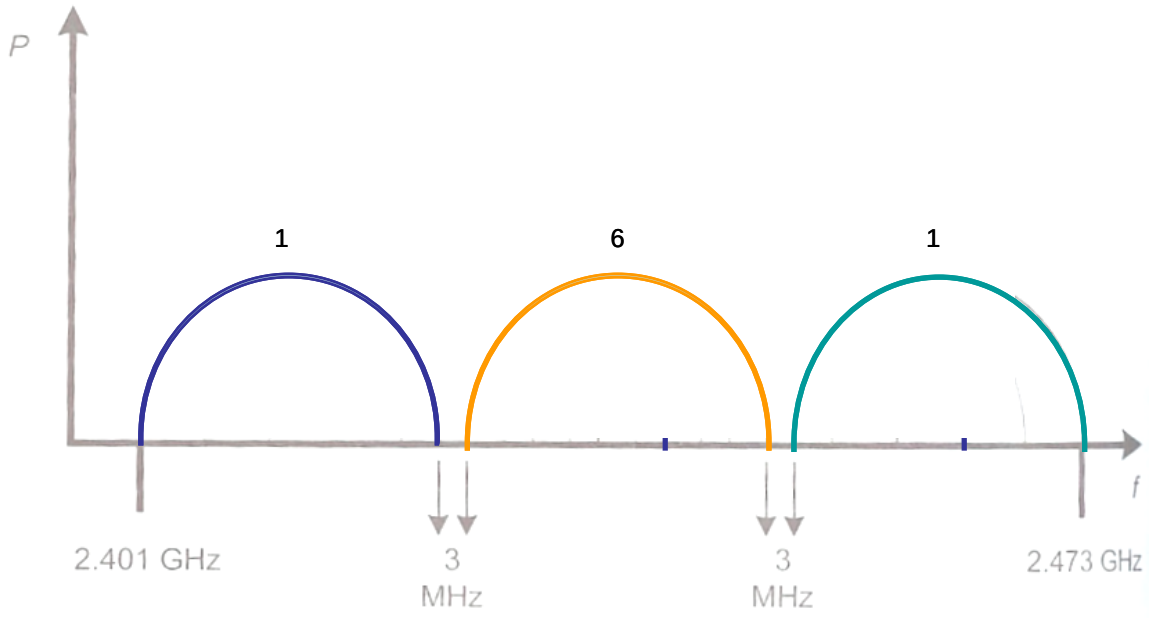


Figure 5. Non-overlapping 802.11bg Channels (1, 6 & 11)

Due to overlapping channels and the popularity of Wi-Fi systems in plants, band crowding and RF saturation can lead to poor wireless performance.

Frequency Hopping is a very popular technique for industrial systems because it has outstanding noise immunity techniques. Unlike Direct Sequence and OFDM, Frequency Hopping uses many smaller channels in the spectrum and rapidly changes channels or “hops around” from channel to channel (see Figure 4).

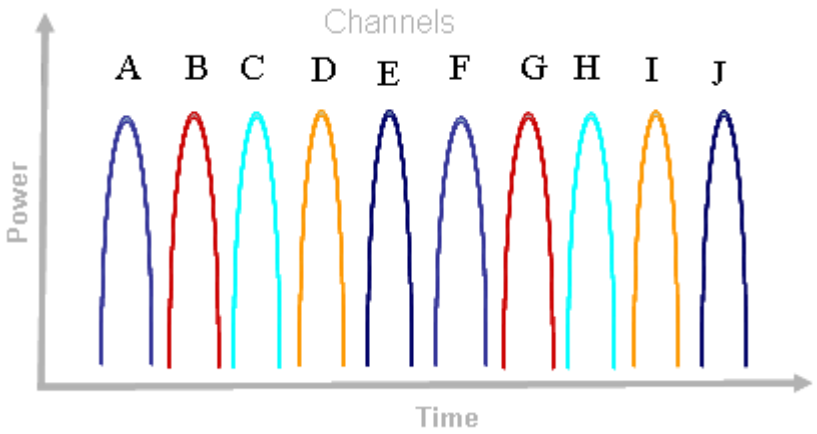


Figure 6. Frequency Hopping Channel Sequence

Frequency hopping has a high RF energy per bit ratio, and by incorporating error correction techniques, frequency hopping offers the best chance for successful data transmission as the transmitter will send the packet over and over again using different channels until an acknowledgement is received.

The disadvantage of Frequency Hopping is that it is slower than Direct Sequence/OFDM and has longer data latency. Most Frequency Hopping systems are limited to 1 Mbps or less RF data rate. But if the data rate is fast enough for the application, the reliability of frequency hopping is tough to beat especially in high noise environments.

IEEE 802.15.1 (BlueTooth) is one of the few open standards incorporating frequency hopping. Because of the distance limitation of IEEE 802.15.1 BlueTooth devices are seldom applied to wireless Ethernet systems. Most industrial frequency hopping modems are proprietary, meaning that each manufacturer uses their own technique and vendor X will usually not communicate with vendor Y. While this is potentially a disadvantage for commercial systems, it can be desirable for industrial systems for two reasons: Security and isolation from the wireless IT system.

Because industrial frequency hopping technologies are not typically based upon an open standard, the manufacturer can use unique authentication processes and sophisticated encryption techniques To ensure very high levels of security. While security has significantly improved in Wi-Fi systems with WPA and WPA2 standards, hackers will continue to look for holes. Fortunately many industrial Wi-Fi manufacturers now include an option to hide the access point by not transmitting its SSID beacon effectively, hiding the access point from potential hackers. Other security techniques include cryptographic encryption, key management and rogue access point detection providing a high degree of security just as frequency hopping systems provide.

Frequency hopping also offers plant managers the ability to operate their own wireless network separate from the IT department. Because of the popularity of 802.11 technologies for wireless network access, warehouse barcode systems and video surveillance, proprietary frequency hopping systems may be the best choice for industrial systems and keep the peace between department managers.

Frequency Band Selection

There are many considerations when selecting the frequency band for EtherNet/IP communications including required data rate, distance, line-of-sight obstructions, modulation technique, band availability (government regulation) and band saturation (crowding). There are also spectrum management issues to consider if wireless is already in place or planned for the future.

License-free communications using the spread spectrum bands is very popular for industrial Ethernet systems. There are three major spread spectrum bands available in the Americas and Australia:

- 902 to 928MHz
- 2.4 to 2.483 GHz
- 5.1 to 5.8 GHz

Most countries in Europe, Africa and Asia permit license-free communications in the 2.4 and 5 GHz bands, but local regulations vary and should be investigated to assure compliance.

Generally, frequency band and range (distance) are inversely related; i.e. the higher the frequency the shorter the range (all other factors being equal). However, data rate and frequency band are directly related; i.e. the higher the frequency, the faster the potential data rate. Data rate and distance are the first major considerations in frequency band selection.

The other major consideration is band usage and management. Many industrial plants use the 2.4 GHz extensively for IT and inventory systems. Therefore, the 900 MHz band (for slower speed systems) or 5 GHz band (for higher speed) may be the best choice for industrial wireless systems.

Importance of Line-of-Sight

Along with distance, antenna placement is a key consideration. Spread spectrum systems always perform best with clear, unobstructed line-of-sight (LOS) between antennas. If there are obstructions (such as metal structures, concrete walls/floors, trees, etc.), then communications will be impeded. In many industrial systems though obtaining clear LOS may not be practical or possible. Fortunately, the lower frequency 900 MHz band offers relatively good reflectivity and penetration characteristics. Using frequency hopping techniques in the 900 MHz band has the best chance to provide reliable data transmission in applications without clear line-of-sight though at relatively slower speeds. Applications without line-of-sight should always be thoroughly tested before implemented.

For longer range, outdoor systems clear line-of-sight between antennas is even more critical. Additionally, RF transmission theory dictates that the earth can reflect the signal in such a way to improve or impede it. A buffer zone in between the earth and the LOS is also needed for maximum signal levels. This area is called the Fresnel Zone (Figure 7), and is important when engineering the antenna system, particularly antenna height.

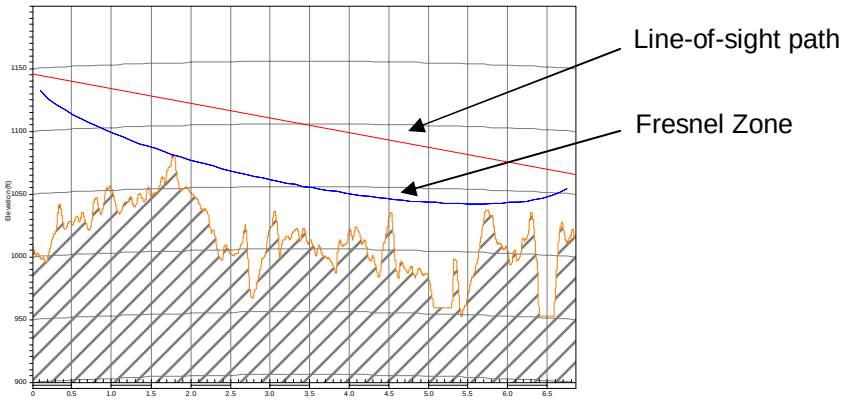


Figure 7. RF Path Terrain Profile

Multipath

Mutipath is caused when the directed and reflected signals arrive and combine with different delays and amplitudes (see Figure 8). The delayed signals are produced by reflected and scattered signals arriving at the receiver from different paths resulting in propagation delay. These additional signals may cancel the original signal completely out called multipath fading, or be combined by superposition to create delay at the receiver. This Delay is referred to as delay spread and is defined as the difference in propagation delay between the directed (LOS) signal and the reflected signal. The tolerance of the delay spread varies among different radio manufacturers; often lower cost radios will have a lower number and be more susceptible to the multipath issue.

Typically large open areas with reflective surfaces, such as metal, are more prone to this phenomenon. But some wireless technologies are more prone to multipath fading issues than others. Frequency hopping systems are nearly immune to this problem, while older direct sequence modulation is very prone. OFDM is much better at handling multipath than direct sequence, so is a good choice when needing high speed data transfer.

802.11 based systems may also offer the option for a second receive-only antenna. By mounting a second antenna a few inches away from the main antenna, the radio receiver can determine which signal is best to use. This is referred to as “antenna diversity” and is one way to reduce multipath problems. Sometimes making just slight adjustments to antenna positions in systems experiencing difficulties can dramatically reduce problems as well.

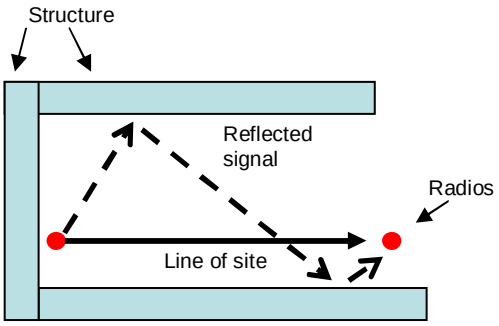


Figure 8. Multipath Phenomena

Contention

In most working environments these days there are other wireless devices of some kind in use. The IEEE 802.11 specification makes it possible for these devices to work well in the same

proximity as each other. Contention is the ability to capture the RF channel, use it, and share it with other RF devices on the same frequency. If there are too many transmitters on the same frequency, contention can be an issue since getting on the channel may be difficult and time consuming as other users contend for it as well. CSMA and CCA (Carrier Sense Multiple Access and Clear Channel Assessment) is the collision detection mechanism used to ensure no two radios on the same channel transmit at the same time.

As previously discussed, frequency band management and channel allocation is good practice to ensure dependable wireless performance. This is especially crucial when wireless is applied to high speed I/O systems. Dedicated "clear channels" are best for these demanding applications and ensure reliable coexistence of multiple RF systems.

Interference
Many plant engineers are concerned that emissions generated by industrial equipment may interfere with wireless systems. DSSS, OFDM and FHSS are all quite capable of reliable transmission in "noisy" industrial plants where Variable Frequency Drives (VFDs), high voltage substations and even arc welders are in operation. Most interference problems are the result of other wireless systems operating in the same band or channel, and not from industrial equipment.

Wireless EtherNet/IP Reliability & Performance

Many factors impact designing reliable wireless EtherNet/IP systems that will meet the performance requirements of automation systems. We have explored many of these factors in the previous section, but perhaps the most important consideration is selecting (and correctly implementing) the best technology for the automation network. This section will focus on wireless design of specific EtherNet/IP network architectures.

Industrial wireless applications can be divided into two broad categories: Those requiring high speed, low latency performance, and those permitting slower speed with longer packet latency. Wireless technologies are available to accommodate both.

A common error though is assuming that faster technologies are better. If the application can handle slower speeds, then using relatively slower frequency hopping technology may be the best approach. Frequency hopping is the most robust especially regarding communications in high RF noise areas, and easier to implement. As applications demand higher speeds, then more considerations and engineering challenges are typically encountered.

Wireless for Explicit Messaging between PLCs
One of the most popular uses of wireless is in sharing I/O information between PLCs. As previously discussed, Explicit Messaging uses TCP/IP based communications. Because these messages are unscheduled at the protocol layer, slower wireless Ethernet technologies may be used. MSG blocks in PLC ladder code may be programmed to accept long delays in transmission. If the application (process) is not time-critical, then a slower (but robust) frequency hopping technology may be the best choice.

There are many factors influencing how fast an explicit MSG may be executed. Generally, applications requiring 200 ms response time or slower are a good candidate for FHSS. Faster response times may require faster technologies such as OFDM available in IEEE 802.11a and 802.11g standards.

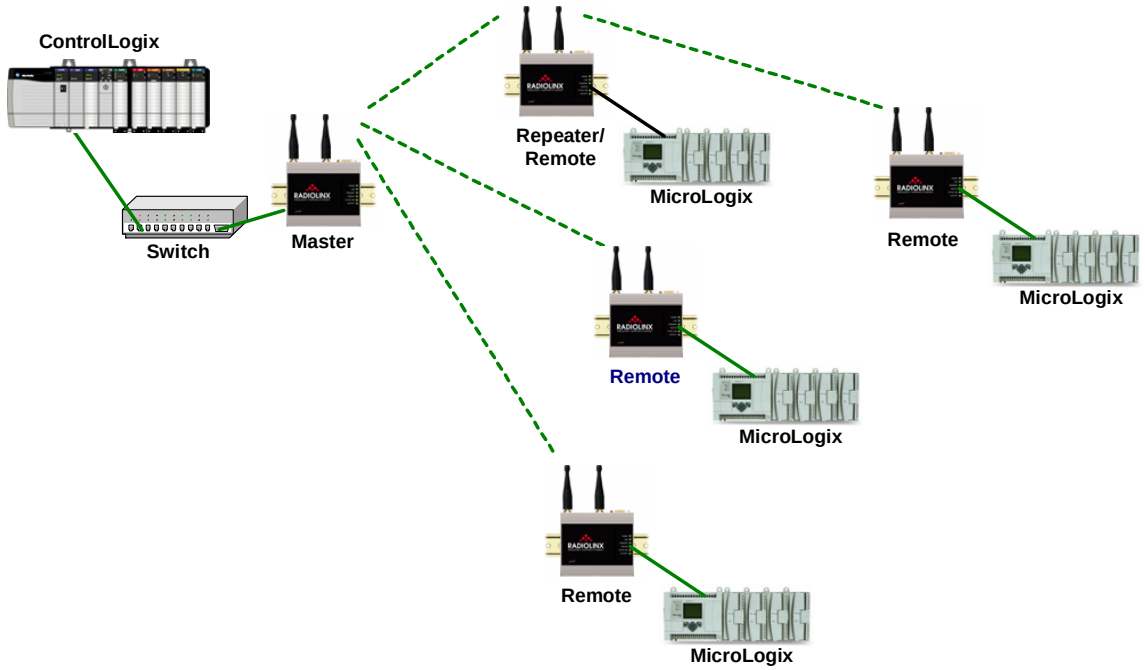


Figure 9. Wireless TCP/IP System using *Explicit Messaging* for Data Exchange

Wireless for HMI Networks

Another popular application for wireless is connecting Human Machine Interfaces (HMIs) to plant networks or machines. HMIs use TCP/IP communications and are not time critical other than to meet the needs of the process and, most importantly, the operator.

While HMI screens may look very complex and data intensive, usually the actual data being transmitted (updated) is minimal. If programmed efficiently, slower wireless technologies (such as Frequency Hopping) may be used. The key consideration is update times and the amount of information actually being transmitted.

FHSS may be the best choice if appropriate. However, if portable computers or PDAs are used, then the industrial wireless network must support the standard built into these portable devices. 802.11b and 802.11g (Wi-Fi) are the most common. This technology supports mobile operators while providing high speed, low latency communications.

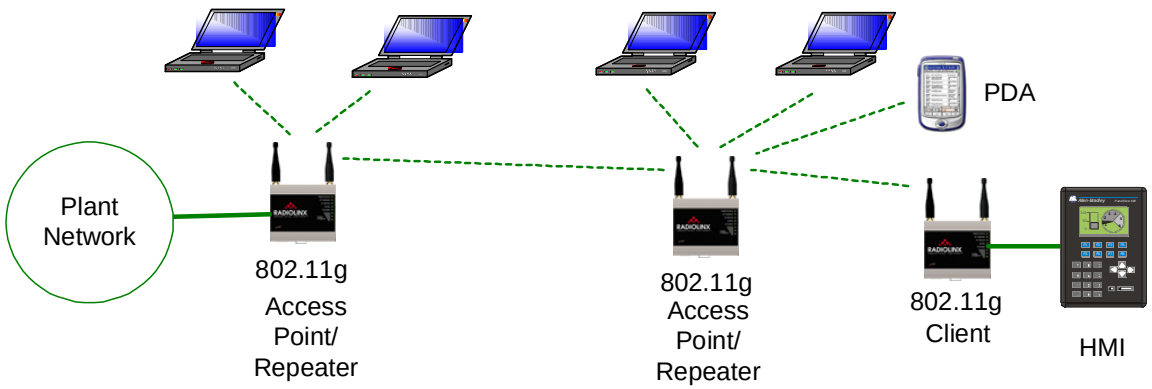


Figure 10. Wireless TCP/IP System for HMI Connectivity

Remote SCADA Systems

One of the most popular industrial uses of RF is for remote Supervisory Control and Data Acquisition (SCADA) communications. Utilities extensively use remote SCADA networks where remote pump stations, tanks, sub-stations and pipelines are controlled and monitored from a central site.

Wireless is a very good alternative to leasing phones lines as previously discussed. The main challenge with remote SCADA is distance and terrain between the sites. Wireless technologies that support EtherNet/IP speeds require unobstructed line-of-sight (LOS) and adherence to the Fresnel Zone for optimal performance. Analyzing the terrain and LOS obstructions is vital in determining the feasibility of wireless EtherNet/IP. Fortunately, repeater sites are often available to achieve LOS and many FHSS radios have store-and-forward repeating capabilities.

Most EtherNet/IP SCADA systems do not require very fast communications as Explicit Messaging is used to communicate from the remote PLCs back to the central plant. Frequency Hopping is often the best choice here because FHSS offers the longest range due to excellent receiver sensitivity and support of the 900 MHz frequency band.

Bandwidth is limited in FHSS systems, so careful examination of network traffic is prudent. There is sometimes a temptation to add in other types of communication (such as voice over IP, surveillance video, Internet connectivity, etc.) which will quickly exceed the capabilities of an FHSS wireless system. IEEE 802.11 based systems offer the highest speeds for multiple use remote communications, but are limited in distance as their receiver sensitivity is lower and they do not support the 900 MHz band.

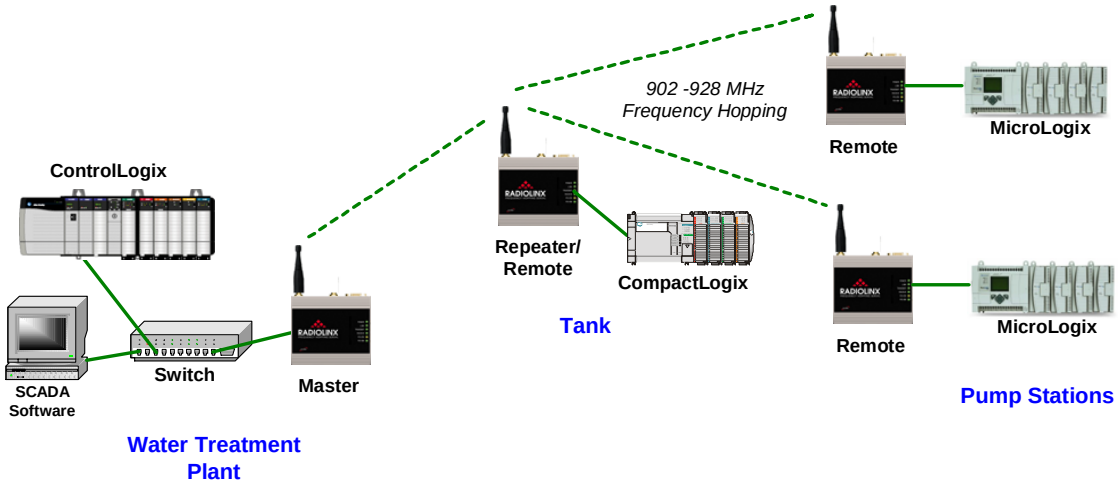


Figure 11. Remote Wireless SCADA System using EtherNet/IP TCP/IP

Wireless for Ethernet I/O (implicit messaging)

An emerging application for wireless is communications to distributed I/O blocks using EtherNet/IP. Wireless offers many advantages in these applications including elimination of mechanical coupling methods used in moving systems (e.g. rails, slip rings) and general cost savings due to reduction of Ethernet infrastructure.

Communication to EtherNet/IP I/O blocks can also reduce automation costs compared to using remote PLCs. Programming is simpler using I/O instead of remote PLCs because MSG blocks are not required in the main controller's ladder program. But remember that Implicit

Messaging is UDP/IP based, not TCP/IP. Wireless networks must be carefully designed, and the plant RF environment more closely managed to ensure reliable communications.

Several factors should be carefully considered before choosing this architecture including:

- Lack of remote PLC control (intelligence) in case of communication failure
- Amount of I/O and required scan times (network traffic)
- Packet handling ability of wireless technology
- Efficiency of the RF technology with multicast UDP packets
- 802.11 clear channel availability

However if circumstances are right, wireless EtherNet/IP I/O can be a significant cost saver and actually improve system reliability when correctly implemented, especially in moving systems.

Prosoft Technology has performed extensive tests of its Industrial Hotspot technology with EtherNet/IP and has many successful customer installations. The following information is provided only as a guideline towards predicting wireless performance and should not be relied upon for any other purpose. Prosoft Technology always recommends field testing to confirm wireless performance and reliability.

Predicting Wireless I/O Performance

Because EtherNet/IP I/O messages are scheduled, it is possible to predict scan time performance over industrial wireless systems if the following conditions are met:

- Packets per second performance of wireless technology
- Wireless behavior in multipoint systems (handling of UDP Multicasts)
- Number of CIP connections

The first step in designing a wireless EtherNet/IP system is calculating packets per second which determines minimum wireless bandwidth requirements. Start by counting the number of CIP connections.

To calculate how many connections are in an I/O system, sum up all direct connections and rack optimized connections. To determine how many packets per second the system will be using, multiply each connection by two. It is multiplied by two because each CIP connection is bi-directional meaning that during every Requested Packet Interval (RPI), a produced packet is sent by each end of the connection.

For example, if there are five direct connections and two rack optimized connections (with six digital modules in each) equals 7 total CIP Connections, the total number of packets is then calculated:

7 CIP Connections x 2 = 14 Packets

Note that the six modules in each rack that are rack optimized only count as one connection. Rack optimization (if available in the I/O hardware) can significantly reduce wireless traffic.

Then multiply the packets by scan time (derived from RPI setting) to calculate packets per second (pp/s). Let's assume that in the above example, the required RPI time is 20 milliseconds (actual RPI time is application dependant), we know that there are 50 packets per second at an RPI time of 20 ms (1 / 0.02). We then multiply the 14 connections by the 50 packets per second to get the over all packets per second rate:

14 Packets x 50 per second = 700 packets per second (pp/s).

The overall packets per second rate for 802.11 a/g radios can be in the thousands. However it is best practice to not operate the radio network at maximum capacity. Rockwell Automation suggests reserving 10% of each adaptors bandwidth so it is possible to use its RSLogix 5000 software for remote programming.

It is also suggested that 30% of the radios packet per second rate be reserved for RF overhead. In a congested RF environment a radio contending for the RF medium will use valuable time if the radio determines the channel is busy by using its carrier sense mechanism. If the radios determine the medium is busy the radio will not send any packets while it runs its back off algorithm and then re-accesses the channel. All this accounts for time when the radio could be sending packets, but can not. A radio network that is in a highly congested RF environment can easily use 10% of its packets doing RF retries. RF retries can occur if a packet is lost or corrupt due to poor signal to noise ratio, antenna placement or multipath fading problems. Point-to-multipoint systems consume higher amounts of bandwidth Selecting a "clear channel" is good practice in wireless EtherNet/IP I/O networks.

The next step is to determine a reliable packet per second (pp/s) rate that the wireless technology will reliably support while keeping in mind that at least 40% should be reserved for other applications and RF overhead.

Impact of Multicast UDP Packets on 802.11 Systems

As previously discussed, produced CIP packets are multicast over the Ethernet network to accommodate multiple consumers. In wired systems, managed switches with IGMP querying are recommended to direct multicast UDP traffic to only the segments that need them. This ensures that high speed I/O data does not reduce performance of the plant Ethernet network, a major concern of IT managers.

Similarly, 802.11 based access points will re-broadcast multicast UDP packets to all active wireless clients. This represents a major problem because the unnecessary broadcast of high speed UDP packets will quickly clog an 802.11 channel significantly reducing performance and even dropping UDP packets which will cause system errors.

One way to correct this problem and optimize wireless performance is to invoke IGMP Snooping and multicast packet filtering at the RF layer. By determining which devices are actually consuming the packets, the radio can build a consumption table and eliminate needless re-broadcasts. In point-to-multipoint systems, this feature can improve throughput by as much as 30% while significantly reducing dropped packets.

By applying multicast filtering to the 802.11 standards, it is possible to predict packet-per-second performance even in multipoint systems. For example, ProSoft Technology's 802.11abg Industrial Hotspot has been determined to support 1,800 packets per second. This equates to a little over 1,000 packets per second available for EtherNet/IP CIP packets after subtracting 40% for RF overhead and other applications.

The table below shows how to calculate packets-per-second and highlights in green where an 802.11a or 802.11g wireless system may be used.

RPI Setting (ms)	CIP Connections						
	5	10	20	30	40	50	60
5	1,000	2,000	4,000	6,000	8,000	10,000	12,000
10	500	1,000	2,000	3,000	4,000	5,000	6,000
20	250	500	1,000	1,500	2,000	2,500	3,000
30	167	333	667	1,000	1,333	1,667	2,000
40	125	250	500	750	1,000	1,250	1,500
50	100	200	400	600	800	1,000	1,200
60	83	167	333	500	667	833	1,000
75	67	133	267	400	533	667	800
100	50	100	200	300	400	500	600
200	25	50	100	150	200	250	300

Table 1. Calculating Packets-per-Second (CIP Connections x [1/RPI] = pps)

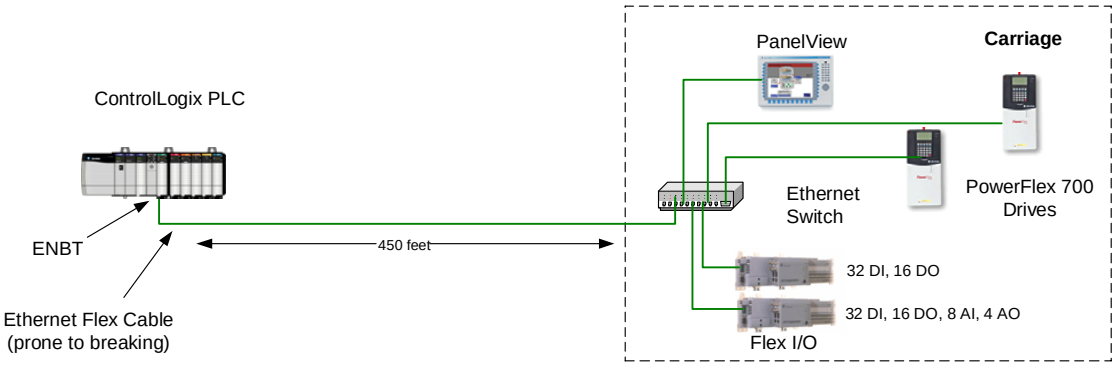
Wireless I/O Design Steps Summary

1. Calculate required packets per second of application
2. Select wireless technology capable of meeting pp/s requirement (with 40% reserve)
3. Ensure good line-of-sight antenna placement
4. Select a “clear channel” – perhaps consider 802.11a 5 GHz band if 2.4 GHz is crowded
5. Utilize IGMP Snooping/Multicast filtering at RF layer to optimize performance
6. Test system performance before commissioning

Wireless I/O Application Example – Manufacturing Carriage

A manufacturer had a problem with moving carriages in their production plant. Each carriage was controlled by a ControlLogix PLC to Flex I/O and drives onboard the carriage. EtherNet/IP was used over flex Ethernet cable. The carriages travel over a 450 ft track at moderate to fast speeds.

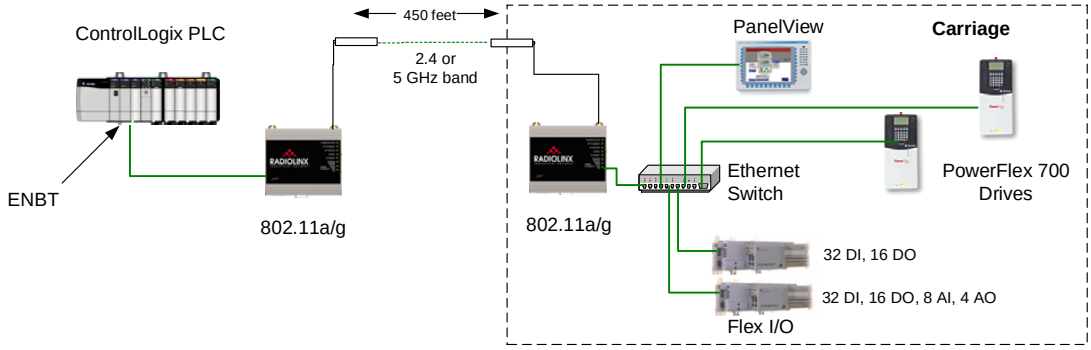
The problem occurred when the flex Ethernet cable would break due to the frequent motion of the carriage. When the cable failed, the Flex I/O system would create E-Stop condition shutting down the carriage. This created two problems. First, the carriage would abruptly stop without warning to the operator riding onboard. Second, production of the line could not continue until the cable was repaired.



The Plant Engineers researched the possibility of replacing the flex cable with a wireless Ethernet system. They calculated that they needed a wireless technology capable of supporting an RPI time of 32 and of supporting 12 side by side lines with no interference.

After consulting with ProSoft Technology Wireless Engineers, they selected the 802.11abg Industrial Hotspot. It was selected because it would support the RPI time, has 12 non-overlapping channels, excellent vibration specifications and diagnostics.

They installed a pair on a test line to prove to management (and themselves) that the wireless technology would be more reliable than the flex cable. This line performed without failure for over 30 days, and they have since converted three other lines to wireless.



Emerging Wireless Technologies

While this paper focused on widely available FHSS and IEEE standards such as 802.11a and 802.11g, there are several wireless standards on the horizon that promise higher performance and connectivity options for EtherNet/IP networks.

IEEE 802.11n
Not a ratified standard yet at time of this paper, 802.11n promises several features that are attractive for EtherNet/IP communications including dual band (2.4 GHz, 5 GHz) support, significantly faster packet transfer rates with a reported throughput up to 300 Mbps and RF propagation that actually takes advantage of reflected signals (quite common in industrial plants with lots of metal) using multi-input, multi-output (MIMO) antenna systems.

IEEE 802.16 (WiMax)
While popularly known as an emerging cellular technology, WiMax technology will soon be available in the spread spectrum (license-free) bands including 2.4 GHz. WiMax offers high speed (up to 70 Mbps) at potentially long range. WiMax technologies may dramatically improve data rates to remote industrial sites and SCADA systems.

ISA100.11a
The ISA is working on the ISA100.11a standard for wireless enabled devices, such as sensors. Operating in the 2.4 GHz band, the technology will "sense" existing 802.11b/g systems and work around them. While designed primarily for embedded devices, EtherNet/IP adapters and gateways will likely be supported.

About the Authors

Gary Enstad has a BS in Electrical Engineering and has been involved in wireless design and technical support for over nine years. His current role is Wireless Application Development Engineer for ProSoft Technology in their Madison, WI wireless division. Gary may be reached at genstad@prosoft-technology.com.

Jim Ralston has been involved with the design and support of industrial wireless systems for over 12 years. He is currently the Northeast Regional Sales Manager for ProSoft Technology and resides in the Pittsburgh, PA area. Jim may be reached at jralston@prosoft-technology.com.