ADVANTECH
Enabling an Intelligent Planet

Technical White Paper

WiFI – The New Key to Industrial Control and Safety

Author: Advantech

E-mail: eainfo@advantech.com

WiFi and wireless mesh are the new keys to economically managing your industrial systems and safety.

WiFi, short for "wireless fidelity," is the common name for the whole series of devices that conform to the IEEE 802.11 standard. The purpose of WiFi, as marketed by the WiFi Association, was to remove the complexity of the IEEE 802.11 standard from the public view, so that the market size would increase in the consumer space. The point is that users do not need to understand the standard, or the complexities of it to use the devices that conform to and are interoperable under IEEE 802.11

WiFi is so common it has become almost invisible in industrial and commercial settings. There are WiFi networks everywhere. When most people think of wireless in the industrial environment, they think of wireless sensor networks. While that's one segment of the use of wireless, it isn't the only one, and it is by far the smallest. Notwithstanding all the hoopla around wireless field device standards like Zigbee and Wireless HART, the real workhorse for wireless in the industrial space is IEEE 802.11 or WiFi.

The Opportunity for Wireless in the Industrial Plant

Almost 100 years ago, when Edgar Bristol of Foxboro invented the single loop controller, it was a pneumatic instrument, running on 3-15 psig air. It was a single loop control. Transmitters were expensive, so in order to control using a single variable, the user had to select the one variable that would be the most useful.

What advantage would an operator and engineer have if they could outfit a cracking tower with 200 or 300 temperature sensors? That many sensors could be used as Mat lab or other simulation software inputs and could quite easily do three dimensional near real time modeling of the inside of the cracking tower.

Visualize the same sort of capability in the discrete manufacturing industry. What could engineers do with all that information?

Motors, blowers and pump shafts turn. As they begin to show wear, their temperature changes and their vibration signature changes too. The traditional answer has been to send people out to put a stethoscope on the motor, pump, blower, or shaft (if they can) and listen for changes in vibration signatures. Recently, handheld temperature sensors have made that process somewhat easier, but vibration sensors are still expensive and require an operator or maintenance tech to go out in the plant to each motor, drive, blower, pump, and shaft individually.

Now suppose those motors, blowers, pumps and shafts could be instrumented in a cost effective way and feed real time information back to control system, maintenance and asset management software packages.

The average age of operators and maintenance techs is over 40 years old. Experienced operators and techs are retiring and sometimes being laid off due to economic conditions. This has produced a serious deficiency in the institutional knowledge bases of plants and has also forced plant personnel, especially maintenance departments, to function with fewer employees. This means that it is sometimes difficult or even impossible for plants to afford to dedicate one or more maintenance techs or operators to doing “gauge rounds”—taking a clipboard or a barcode reader out and manually inputting the value and the status of the variable that was deemed not valuable enough to use a dedicated transmitter for when the plant was built, maybe as long as 50 years ago.

Now suppose that it was possible for operators and maintenance techs to be anywhere in the plant and continue to have full oversight and control over the process or assembly procedure. Suppose each of those gauges and other variables could be instrumented the same way as with the motors, drives, pumps and shafts.

Discrete assembly facilities have many sensors, just like process plants, and they are handled the same way. Rarely are there multiple sensors for a single function on a line, because the wiring costs many times more than the sensor.

Now suppose it was economically feasible to mount multiple sensors for backups and quality monitoring.

Out in the plant, operators, engineers and technicians often have to take three or four communications devices in order to talk to the various parts of the plant. Walkie-talkies, cell phones (both standard and push-to-talk), all-calls and even laptops are all used in the plant environment—and most of them don’t intercommunicate.

Now suppose it was possible to have a single device or two devices at most, that would allow the operator, engineer or technician to access any information they need, and contact anybody they need to talk to.

We’ve “supposed” some very radical changes in the way plants are run and maintained. But all of those things are within our reach. The key is wireless.

The Key to the Future is Wireless in the Plant

The cost of wiring new sensors and wired network infrastructure is not going down. If anything, it is becoming more costly because of the cost of materials and labor.

In part, the reason for only using selected sensors is still valid, if it is assumed that the transmitter must be wired to a marshaling cabinet full of I/O and then to the control system. In point of fact, the cost of wiring a transmitter, even something as simple as a position sensor, is usually several times the actual cost of the transmitter itself.

Worse yet, installing wired transmitters and network infrastructure usually means that the plant, or the portion of the plant in which the work is being done, must be shut down. So not only does adding sensors, controllers and network infrastructure cost capital expenditure, but it also means that product is not going out the door during the installation.

Wireless devices, on the other hand are relatively easy to install, and usually do not require shutdowns for the installation. The price of wireless sensors and network devices is rapidly coming

down, probably pursuant to Moore's Law. Many of them are COTS (Commercial off the Shelf) devices. Some are industrially hardened versions of commercial devices, and some are purpose built for the industrial environment.

Installing wireless sensors and networking devices means that the costs of wiring, including increasing the size of marshaling and I/O cabinets, adding more I/O to field controllers, and the cost of shutdowns, disappear. Even if a wireless sensor or actuator or router or gateway were to cost twice what its wired counterpart would, the overall economics of wireless mean that the project can be done significantly faster *and* for less cost.

The benefits of WiFi

Combined with low-cost wireless sensors, WiFi can be used to measure non-traditional process variables (not just flow, level, pressure and temperature). WiFi can be used to effectively replace wired Ethernet networking in areas where running wires is difficult, expensive or impossible. There are many places in the industrial environment where that is the case.

Wireless is being used right now for a wide variety of applications. It makes re-configuring assembly lines much simpler and orders of magnitude less expensive if the re-configuration does not also include re-wiring every single sensor to every single controller. There are wireless adapter systems for every variety of programmable controller, whether PLC or PAC, or embedded controller.

One of the large pharmaceutical companies built in 2008 a four-story research and development lab using WiFi and a wireless sensor network as its entire networking infrastructure. All of the components in the lab are on skids, and can be wheeled into place on the plant floor, or taken by freight elevator to another floor in the plant, where the skid simply hooks onto the wireless network on that floor. This unprecedented flexibility is made possible by wireless networking and infrastructure.

In addition to the traditional use of WiFi for connecting laptops and other mobile devices, it can be used for line-of-sight transmission from one building network to another on the plant site. This is substantially less expensive to install and can operate more than 1.5 miles of Ethernet over fiber cable.

WiFi is already in common use for automatic guided vehicles (AGVs). AGVs move inventory around plants from location to location without human intervention, based on their wireless communications. AGVs take raw materials to the production area, and take finished goods to inventory. They are guided by 802.11-based control signals

The key to wireless in the plant is IEEE 802.11, the WiFi standard.

802.11n includes many enhancements to the earlier a/b/g versions of the protocol. These improvements include an increase in speed, range and reliability.

Versions g and b operate at the 2.4GHz frequency and a operates at 5GHz, the advantage of n is that it can operate at both whilst also being able to support simultaneous 802.11a and

802.11n at 5GHz or 802.11b, g and n at 2.4GHz . For use in Greenfield sites the access point can be configured not to be backward compatible with other versions. To improve the range, throughput and reliability of the wireless networks 802.11n had made three core innovations: MIMO, packet aggregation and channel bonding, thereby giving a fivefold increase in performance over 802.11a/b/g networks.

MIMO systems are built using multiple vector antennas at both the transmitter and the receiver and it is this multiplicity that makes a MIMO system. Since it can utilize both the diversity and muxing of simultaneous data streams it can potentially increase system capacity by three times or more and has been adopted into IEEE 802.11n

Depending on where MIMO signals are processed a MIMO system can be classified into three types: receiver processing only, transmitter processing only, both transmitter & receiver processing systems.

Receiver Processing Only

Receivers do not need MIMO signal processing but multiple front ends, therefore, antennas at the receiver are connected to multiple independent front ends with separate data streams, which are then muxed into a single data stream providing a much higher data rate than a single antenna system.

Transmitter Processing Only

In this scenario it's really easy: a transmitter is just a transmitter. A single data stream is demuxed into multiple sub streams. When the signals from different antennas arrive at the receiver, MIMO signal processing must be performed using one of three schemes: space-time coding, vertical Bell Lab Layered Space-Time (V-Blast), and maximum likelihood detection (MLD). MLD provides the best performance of the three.

Both Transmitter and Receiver Processing

The best of both worlds but with better performance? Well partly, but it comes at a price, as these are very complicated to configure and administer. The most popular method of performing the two functions is called singular value decomposition which diagonalizes the MIMO channels to form independent channels, to which water filling schemes can be applied to maximize overall system capacity.

Thanks to the high processing power of Advantech's mesh routers all types of MIMO systems can be applied however, for ease, transmitter-processing-only MIMO is applied from mesh routers to mesh clients and receiver-processing-only MIMO for links from the routers to the clients.

Packet Aggregation

Packet aggregation increases efficiency by aggregating multiple packets of an application in a single transmission frame and enabling them to be sent with a fixed overhead cost of just a single frame. Packet aggregation works best for data applications such as file transfers, for real-time applications like voice or video packet aggregation has no effect and it's better to minimize the number of "packed" packets to reduce latency and eliminate jitter contentions.

Channel Bonding (40MHz Channels)

Where 802.11a/g only supports 20MHz to carry a maximum of 54Mbps of raw data per channel, 802.11n increases that to 150Mbps per channel, and by using a technique called channel bonding, combines two adjacent 20MHZ channels into a single 40MHz channel, thereby doubling the throughput to over 300Mbps. Channel bonding works best at 5Ghz because of the far larger (over 100) number of channels, whereas at 2.4GHZ only three non-overlapping 20MHz are available

.

Comparison of different 802.11 transfer rates (source: Intel Labs)

IEEE WLAN Standard	**Over-the-Air (OTA) Estimates**	**Media Access Control Layer, Service Access Point (MAC SAP) Estimates**
802.11b	11 Mbps	5 Mbps
802.11g	54 Mbps	25 Mbps (when .11b is not present)
802.11a	54 Mbps	25 Mbps
802.11n	**300 Mbps**	**150 Mbps**

WiFi automatically uses the Ethernet and TCP/IP protocols, making them entirely transparent. Whether your network is wired or wireless, it operates the same way.

There are, in fact, multiple radios operating within a WiFi wireless device. The first broadly used devices conformed to 802.11b, which was distance and bandwidth limited and had very limited throughput speed—only about 11 Mb. Then devices using the 802.11g specification were released—these devices have both an 802.11b and an 802.11g radio and can operate on either specification, or both. In 2009, devices operating on 802.11n began to be released. 802.11n has much higher throughput speed—well over 100 Mb in good reception areas and can be used over much greater distances than 802.11b and 802.11g.

In North America, 802.11a operates on the 5 GHz band, 802.11b and 802.11g devices operate on the 2.4 GHz band, and 802.11n devices can operate on both the 2.4 GHz and 5 GHz bands. These radio frequencies are known as the ISM bands, because they were at one time reserved for Industrial, Scientific and Medical uses, as well as amateur radio (hams). Now many devices use those bands, including cell phones, wireless telephones, and even microwave ovens.

While most devices for the industrial communications market are 802.11g, there are new devices, such as the Advantech EKI-6311GN, an IEEE 802.11n industrial wireless access point. The EKI-6311GN, because it is an 802.11n device, delivers three times the throughput rates of a normal 802.11g. Like all 802.11 devices, the EKI-6311GN is fully backward compatible with legacy 802.11b/g frequencies. With the support of STP, WMM, and IGMP snooping protocols, the EKI-6311GN effectively improves the reliability of wireless connectivity.

It is only by the inclusion of the four algorithms, MIMO and IEEE 802.11n technologies that Advantech are able to create the tools necessary to transmit data continuously across large distances regardless of the difficulties and obstacles put in the way of the signal. Advantech's EKI radio devices are specifically designed for the rigors of harsh environments and too send data as quickly as the technology allows without any interruptions.

N-based devices like the EKI-6311GN can be used at up to 150 Mb, and up to 5 km distance, where B- and G- based router devices were limited to up to 11 or 54 Mb respectively and usually less than 100 feet (30 meters) of distance. The 802.11n specification and devices are significant improvements over the previous specifications.

There is a new 802.11 specification being worked on: 802.11s. This is a very low power mesh network design that is expected to be for PAN (personal area networks), M2M (machine to machine) control and wireless sensor networks. It is thought that this standard may replace the other wireless sensor network standards currently in place, such as Zigbee, Wireless HART and ISA100.11a. Like all the other iterations of 802.11, it is required to be interoperable with 802.11b-n systems. Until the release of 802.11s, through using mesh networking protocols like Advantech's Mesh, standard 802.11 systems can be used as mesh networks, providing the noise immunity and redundancy that mesh networking were designed for. Interestingly, the Internet itself is a mesh network.

802.11-- Robust and Ubiquitous

For industrial wireless users, the point is that IEEE 802.11 is a robust and ubiquitous standard, with devices intended for every facet of use—home, business and industry.

In addition, the industrial wireless user can find lots of assistance from the company IT department, since 802.11 is the dominant wireless standard in the enterprise office space as well. It is extremely useful when running into problems of bandwidth and interference to have people who are experienced with wireless networking already available.

There are many books and articles available on the 802.11 standard and the technologies behind it. But the point of WiFi is that users, even users in the industrial environment, don't need to know the technology, just the applications and use cases

Industrial Grade Wireless

Just because 802.11 is a COTS (commercial off the shelf) standard doesn't mean that COTS products can be used in the industrial environment. Industrially hardened access points like the EKI-6311GN will survive in the industrial environment when exposed to extremes of temperature, dust, humidity, hazardous vapors and other common situations. When selecting your industrial wireless products, be certain to determine their suitability for the service you wish to use them in.

Mesh technology

A Mesh network topology, considered to be one of three varieties of ad hoc network i.e. one without a preexisting infrastructure {mobile (MANET), and wireless (WSN) are the other two} requires that each node must not only capture and disseminate its own data, but also serve as a relay for other nodes i.e. It must collaborate in the propagation of data in the network.

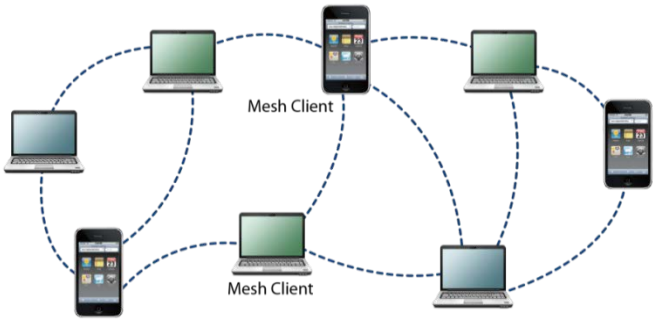
A mesh network can be designed using the routing technique. Routing propagates the message along a path, by hopping from node to node until the destination is reached. To ensure the availability of a path, a routing network must allow for a continuous connection and reconfiguration

around broken or blocked paths, using self-healing algorithms. Self-healing capabilities enable routing based networks to operate when one node breaks down or a connection goes bad. As a result, the network is considered to be very reliable since there is often more than one path between a source and a destination in the network.

The three types of Mesh are explained below and all have different uses with Hybrid having the most uses.

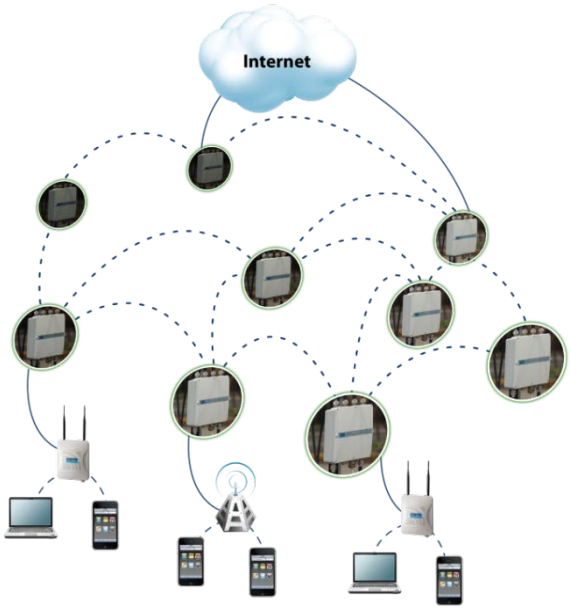
1. Client

Using one type of radio device e.g., an EKI-6340-3, as a client mesh provides peer-to-peer networks among client devices and the client nodes to perform routing and configuration functions.



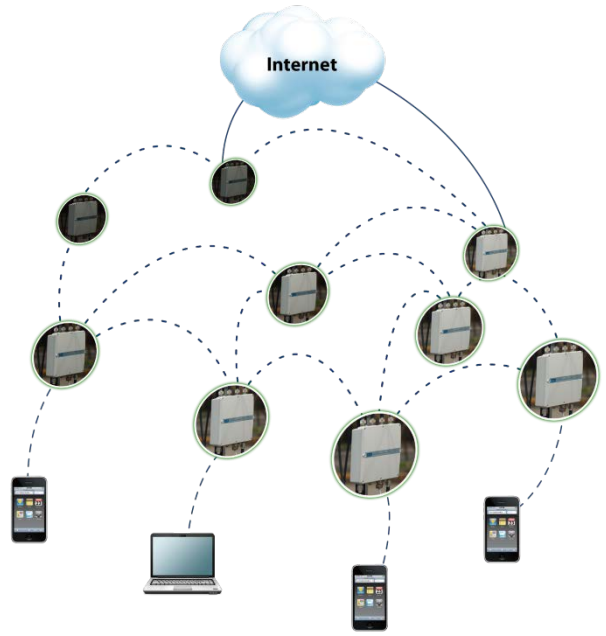
2. Infrastructure

By using routers as the infrastructure for clients that connect to them, the routers form a mesh of self-configuring, self-healing links. With their inherent gateway functionality mesh routers can also be connected to the Internet, thereby providing a backbone for traditional networks and allowing the integration with existing wireless networks.



3. Hybrid

A combination of the previous two architectures, hybrid architecture performs the functions of infrastructure and client and as such can access the network through mesh routers as well as communicating with other mesh clients. This flexibility makes it the most suitable configuration for a majority of applications.



Key Features

In addition to these three designs, there are also three types of key features that can be applied to each of them.

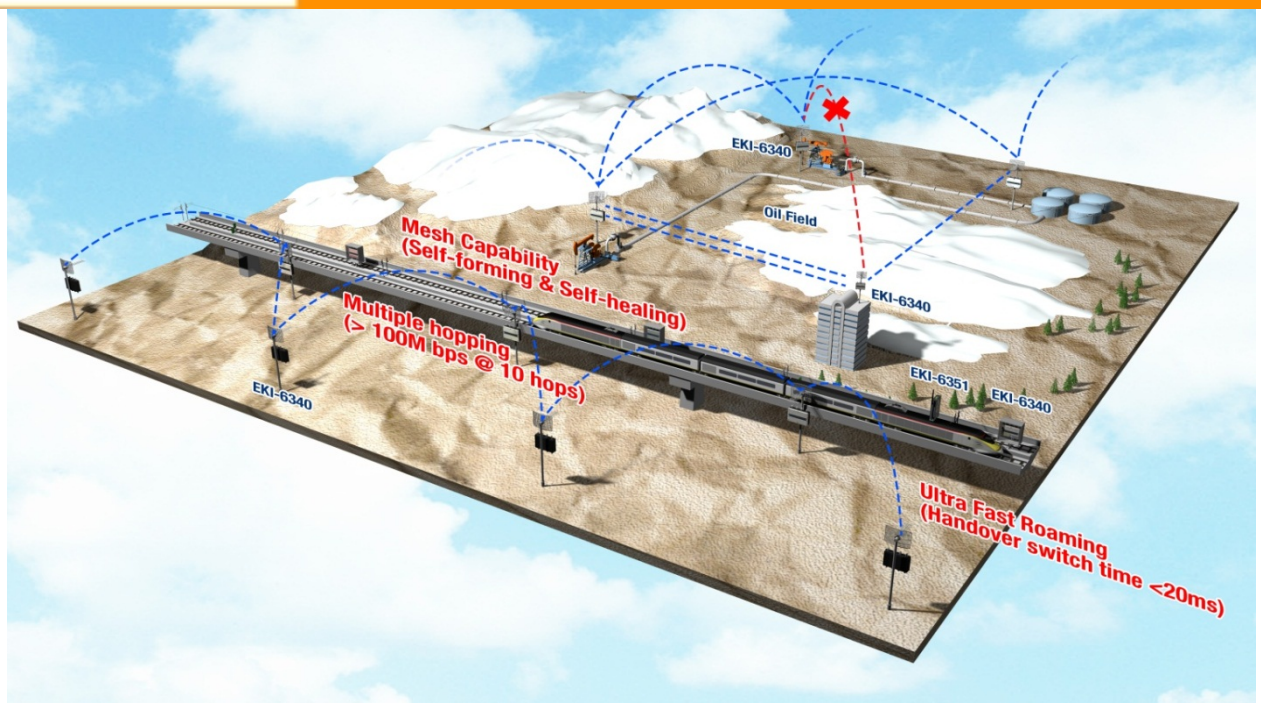
1. Self-healing and Self-forming

Intelligent Mesh capabilities with self-healing and route choosing algorithms (self-forming) follow the calculation of a number of hops and radio signal quality. Each wireless connection in a wireless mesh network will have a "*path score*" to represent the signal quality between nodes. The *path score* calculation includes: RSSI (Received Signal Strength Indication), noise level and bandwidth flow information to be the reference for calculation. The number of hops from source to destination is a minor consideration in a routing algorithm.

2. Multiple Hopping

Intelligent wireless Mesh systems have a throughput of higher than 150 Mbps at 2 hops and can still be 100 Mbps at as many as10 hops. Such high throughput rates ensure less concern about loss of video images which may cause security issues. Furthermore, the self-healing function saves the burden of maintenance and the cost of trouble shooting. Ideal for use in monitoring the status of remote oil fields since each derrick will have an EKI-6351 that transmits data to an EKI-6340 and from there to a control center.

In order to best describe the importance of self-healing, self-forming and multi hopping algorithms, consider their use in oil refineries. These huge sites have many separate areas that need to be continuously monitored and managed, but due to the nature of the business, fires are real possibility and may destroy the EKI-6340 that's monitoring that section. In many network configurations, once the link has been broken other routers, before the damaged one, wouldn't be able to send their data back to the control center. Thanks to self-healing & forming algorithms and multiple hopping algorithms the data can still get through.



3. Ultra-Fast Roaming for Mobile Connectivity

A Mesh solution consists of one Mesh Gateway (one way connected with Switch by Ethernet cable and one way connected with Mesh Node or Mesh AP via radio), some pieces of Mesh Nodes (one way connect with Mesh Gateway via radio and one way connect with Mesh AP via radio) and some pieces of Mesh APs (one way connect with Mesh Nodes via radio and one way connect with Mesh Stations or regular Wi-Fi clients via radio). The Mesh Nodes are dependent upon the throughput requirements.

Fast roaming is a unique feature of a Mesh Station (not regular Wi-Fi clients) and its handover time between two Mesh APs can be pretty short (20ms). The reasons are as below:

a. The Mesh APs are set to periodically & proactively broadcast information to nearby Mesh Stations.
b. The Mesh Stations, those who are under the coverage of Mesh APs, can periodically generate a list of "path scores".
c. Once a new "path score" is generated and it's better than the "path score" of current link, the Mesh Station will handover to another Mesh AP without having to be authenticated & associated.
d. The reason that a Mesh Station doesn't need to process the authentication & association at each handover is because those two steps were performed when the Mesh Station first joined the Mesh System.

An Advantech wireless Mesh system using an ultra-fast roaming algorithm is ideally suited for enabling communication between fast moving trains and the side of the rail. By installing the EKI-6351 inside a train and the EKI-6340 along the side of the rail, the fast roaming speed of 20 ms doesn't cause connection loss. Even in an environment where fiber links to the AP cannot be installed, our EKI-6340-3, which has three radios, constitutes a wireless backbone by means of its two spare radios.

Potential Risks, Repairs and Security

Radio is subject to interference and signal quality issues that do not face practitioners of wired networking. Issues of range, antenna design and placement, interference, roaming, and signal quality must be dealt with.

In the office environment, wireless generally works simply and easily. Conditions rarely change, so the network is very stable and not failure-prone.

In the industrial environment, however, wireless communications are not quite so simple. There is noise (electrical noise, EMF) which can interfere with radio broadcasts. Welding, for example, gives off noise in the same bands as wireless networks use. Cell phones and walkie-talkies produce interference in the WiFi bands, as well.

The industrial environment often consists of large pieces of machinery, metal structures, tanks and vessels that are extremely hard to propagate radio waves through. In addition, scattering and bouncing radio signals off these structures causes a specific type of interference called “multipath” which is the reason that FM radio sometimes sounds fuzzy or has dropouts. This is called picket-fencing signals, because the signal comes and goes with the regularity of a picket fence. Multipath is caused when the signal takes two or more paths to reach the receiver, and depending on the length of the paths, phase cancellation is produced and the signal goes to zero.

One of the considerations in selecting wireless devices is output power. More power does two things. First, obviously, it lets the signal go farther. But higher power also allows the signal to cut through much more noise, and in the industrial environment with myriad sources of RF and electrical noise, that’s a key feature.

The most effective and simplest way to fix an interference problem is to either stop the source of the interference or move the radio to where the interference doesn’t swamp or destroy the signal. The availability of “bridges” can be used to place an additional router where it can be line-of-sight from the first router to the next, thereby removing the interference.

In the industrial environment, the use of high signal strength 802.11n based devices and the use of 802.11a on the 5 GHz band goes a long way to minimize interference.

Security of Wireless Networks

Wireless networks are potentially insecure, but significant work has been done to improve the security of the 802.11 networks. WPA and WPA2 encryption are the current standard for security of a wireless transmission, and it is considered extremely strong, when accompanied with a very strong passphrase.

WiFi based networks in the plant environment should adhere to good security practices, including using DMZs and firewalls, just as they do in the enterprise office environment. The use of port-based authentication, based on the 802.1x standard, and the use of RADIUS authentication servers on top of WAP2 encryption make it extremely difficult to penetrate an industrial wireless network.

Conclusion -- WiFi is the future for industry

Digital radio communications have come a long way from the pioneering telemetry systems of the early manned space program. We find them everywhere, in cell phones, mobile phones, and in all manner of wireless communications. Because of its use in both the commercial and industrial sectors, the cost of WiFi enabled products is continuing to decrease. This will provide the ability to make more and more sensors and devices wireless, and move the industrial environment closer to a factory without wires.