PlantWeb University – Wireless 204

Wi-Fi Networks

15 minutes

In this course:

Overview

Wi-Fi technology – also commonly referred to as **IEEE 802.11** or **wireless Ethernet** – is the most widely used wireless networking protocol in the world.

You may already use Wi-Fi to connect your PC to an office or home network or to the Internet. There are also thousands of Wi-Fi access points or "hotspots" in public places such as hotels, airports, and coffee shops.

Wi-Fi technology is also becoming increasingly popular in process-industry applications. The same technology that lets you connect to your local network when you're sitting in an airport on the other side of the world can also communicate process and asset information from one area of your plant to another.

In this course you'll learn what makes Wi-Fi so popular, and how it can play an important role in delivering process and asset data where it's needed.

Hint

As you go through the topics in this course, watch for answers to these questions:

- Which standard is Wi-Fi based on?
- How does Wi-Fi deal with radio-frequency "noise"?
- Which current Wi-Fi security standard offers the highest level of protection?
- What are some appropriate applications of Wi-Fi in plants?

Standards-based

Standards-based technologies usually offer several advantages over proprietary solutions. These advantages include easier integration, broader choice of suppliers, and greater assurance of long-term support.

Wi-Fi technology is based on the **IEEE 802.11** standards for wireless local area networks (WLANs). Devices marked "Wi-Fi Certified" have also met the interoperability requirements of the **Wi-Fi Alliance** – a group of more than 250 technology and service providers.

IEEE 802.11 is actually a family of related standards. Which ones you use depends primarily on your applications.

- **802.11b** is the most widely used around the world, and, in most cases, the least expensive. Operating at a frequency of 2.4 GHz, radios using 802.11b transmit data at up to 11 Mbps.
- **802.11g** is a more recent version. It operates on the same frequency as 802.11b but at a higher data rate of 54 Mbps.

  802.11g is backward compatible with 802.11b – equipment using the two standards can communicate, but at the slower data rate of 802.11b.
- **802.11a** operates in the 5 GHz frequency band, which is also growing in popularity. It delivers up to 54 Mbps, equal to 802.11g, but at shorter ranges.
- **802.11i**, also known as WPA2, is a security standard for Wi-Fi networks. You'll learn more about it in the "Security" section of this course.

Another related standard, **802.11af**, covers Power over Ethernet (PoE). PoE provides electrical power for a radio or other device over the same cable that carries the data. Although not a wireless technology itself, PoE can be part of an overall solution that combines wired and wireless Ethernet.

Country and regional standards. Although Wi-Fi transmissions don't require a license in most parts of the world, different countries have different restrictions on output power, and some allow different channels within the assigned frequency bands. However, most Wi-Fi radios manufactured today conform to the standards of the country where they are deployed.

Cost-effective

Even the most feature-packed technology is the wrong choice if the benefits don't exceed the costs. Fortunately, Wi-Fi is relatively inexpensive. Broad use has led to mass production that – combined with competition among numerous suppliers – continues to drive down technology costs.

Because Wi-Fi is wireless, installation is also easier and less expensive than for traditional "wired" communications. Using Power over Ethernet (IEEE 802.11af) can further reduce installation costs by eliminating the need for separate line power to Wi-Fi radios in the field.

In harsh environments Wi-Fi radios may require specialty housings and components that can increase costs somewhat, but that's true of almost any communication technology.

Wi-Fi networks are also easy to expand. You can buy what you need now and add more nodes as your needs evolve.

Robust

Wi-Fi has a proven track record for reliability and ease of use over countless hours of operation. Its robustness has enabled use of the technology in applications from residential to commercial to academic and even military.

Now that suppliers have addressed issues related to hazardous-area classifications and operation in harsh environments, process plants around the world are also adopting Wi-Fi technology.

Plant environments can also include many sources of radio-frequency interference. Wi-Fi networks deal with this "noise" by using direct sequence spread-spectrum (DSSS) transmission. DSSS avoids interference problems by spreading the transmission signal across more bandwidth, then concentrating the desired signal – but not the interference – in the receiver.

Secure

Thanks to advances in technology and standards, a Wi-Fi network can be just as secure as a traditional wired network.

Enormous efforts by suppliers, the Wi-Fi Alliance, and the IEEE 802.11 standards committee have led to robust techniques for data encryption, key-distribution, and other security measures. *(For explanations of these and other security concepts, see the Wireless course on* ***Security****.)*

These enhancements were developed after initial Wi-Fi security measures (called "Wired Equivalent Privacy," or WEP) were discovered to be inadequate for applications where robust security is absolutely required.

Two important examples of these enhancements are WPA and WPA2.

WPA (**W**i-Fi **P**rotected **A**ccess) is a powerful, interoperable security technology for Wi-Fi networks. It protects data by using encryption, strong access controls, and user authentication. Replacing an older and less secure technique called WEP, WPA uses 128-bit encryption keys and dynamic session keys to ensure network privacy and enterprise security.

WPA2 takes security a step farther by allowing only authorized users or devices to access the network. Defined by the IEEE 802.11i standard, WPA2 also uses the highly secure Advanced Encryption Standard (AES) for even greater protection.

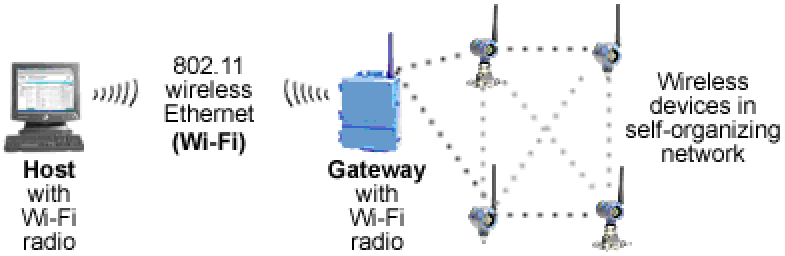
WPA is a practical solution for wireless network security, but WPA2 offers the best long- term solution and is backward compatible with WPA.

Wi-Fi in the plant

Many plants already use Wi-Fi to allow workers to access important applications or send email without physically connecting their PC or laptop to the plant LAN.

Beyond these office-type applications, however, Wi-Fi can also provide access or serve as a "backbone" transport medium for process-related networks.

For example, you might use Wi-Fi to link an isolated area of the plant to a central control room – especially where distance or barriers like rivers or highways make a wired connection too expensive or impractical. Or you could use it to link a self-organizing network of low-power, short-range devices to a host system or wired LAN. *(For more on these applications, see the courses on* ***Near-plant Applications*** *and* ***Self-organizing Networks****.)*



Wi-Fi can provide a secure, robust, affordable link between a host system and a network of field devices.

Why not use Wi-Fi for device-to-device communications as well? Because of its relatively high power consumption, a Wi-Fi-based solution requires either line power or power over Ethernet. The expense of providing these power connections can limit the cost-effective size of the network.

However, Wi-Fi's high power consumption provides much greater range than low-power devices can offer. A 1-watt Wi-Fi radio transmission can reach several kilometers where there are no obstructions or interference, and as much as several hundred meters even in plant environments.

That's why it makes sense to use a local gateway to consolidate data from a network of low-power devices, then connect the gateway to a central host or plant network using Wi-Fi. The gateway can be located to optimize the performance of the wireless device network, and easily moved if the network changes.

Wi-Fi has sufficient bandwidth that one access point can support multiple gateways. It's also easy to integrate with plant LANs and host systems that support wired Ethernet – including many DCSs, PLCs, and PC-based data historians.

Wi-Fi can also give mobile workers access to wireless process control networks. These workers can use Wi-Fi equipped PDAs or tablet PCs to connect with wireless access points throughout the plant – providing access to critical process and asset information, historical data, maintenance systems, and other key functions where and when needed.

Finally, your plant may already have a strong base of Wi-Fi expertise: your IT department, which probably has extensive experience putting this technology to work in office networks. *(For more on this topic, see the course on* ***IT coordination****.)*

Summary

In this course, you’ve learned that….

- Wi-Fi offers the advantages of a technology built on widely supported standards – in this case, the IEEE 802.11 family of standards for wireless Ethernet.
- Its capabilities have been extensively proven – mostly in office and commercial applications, but increasingly in process-industry applications as well.
- The technology is cost-effective, robust, and secure.
- It's a good choice for bridging the gap between device networks or isolated areas of the plant and a central host or plant network.