PlantWeb University – Wireless 402

IT Coordination

15 minutes

In this course:

Overview

In the past, process automation and office automation had little in common. As a result, process operations have often functioned independently of Information Technology (IT) departments, and IT policies haven't always filtered into the process world.

That's changing as process automation uses more technologies that originated in the IT world – from Ethernet to Microsoft Windows – and as process networks are linked to IT-controlled business networks and even the Internet.

Introducing wireless technology for process applications can raise concerns in your IT department. They may simply be unfamiliar with how it will work in the plant environment or have specific concerns about technology, security, and support.

On the other hand, IT may also have valuable experience and resources to help you plan a wireless network, get it up and running, and keep it that way.

This course shows how you can address common IT concerns about wireless technology for plant automation, and work with them to maximize the return on your wireless investment.

Hint

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

- What are likely IT concerns about using wireless networks in process applications?
- How can you reduce concerns about technology risk and compatibility?
- How can IT input help in project planning for wireless networks?
- What network-support tasks might benefit from IT involvement?

IT Concerns

Although wireless networks are becoming more common in office environments, your IT group may not be as familiar with them as with wired networks – especially when it comes to wireless technologies designed for industrial applications.

They’re also likely to be concerned about anything that may represent a risk to the security of assets they have been charged with protecting, including both information and infrastructure.

And they may be concerned about how a wireless-networking project will affect their workload – especially for ongoing maintenance and support.

In the following sections we'll look more closely at these concerns about **technology**, **security**, and **support** – and how to deal with them.

Technology

Your IT group may have concerns about **technology risk** (whether the wireless solution will work, and keep working) and **compatibility** (how it will work with other technologies and existing IT infrastructure).

You can relieve those concerns by sticking to solutions based on **appropriate**, **proven**, **standards-based** technologies – and making sure IT understands that's what you're doing.

Start by clarifying which wireless technology you're planning to use. For example, the primary technology for in-plant applications may be a **self-organizing network** based on the **IEEE 802.15.4** physical standard. Your IT group may be less familiar with this technology than the **802.11 Wi-Fi** networks used in offices, but the fact that it is based on an IEEE standard should reduce their concerns about risk and compatibility.

Wi-Fi *may* be a component of some solutions – for example, to provide a wireless link between a **gateway** (which collects data from several wireless devices) and the control room or to provide mobile workers access to the plant control network. If so, you may be able to take advantage of existing IT experience with this technology.

*(For more on these topics, see the courses on **Self-organizing Networks** and **Wi-Fi Networks**.)*

Compatibility concerns may focus on the gateway itself, since it is the point where self-organizing networks integrate with other plant networks. You can overcome IT objections by selecting a gateway that will "play by the rules" – for example, by supporting standard network scanning, discovery, and vulnerability tools.

The Emerson Advantage

Emerson's **Smart Wireless** solutions are designed from the ground up to meet expectations for robustness and compatibility. For example, our **1420** gateway supports not only IEEE 802.15.4 for collecting information from the field devices, but also SSH, VPN, SNTP, SMTP (send only), DHCP, and other protocols that your IT group will appreciate for easier and secure integration. Emerson's active participation in the development of emerging open standards for wireless industrial applications – including **Wireless HART** and **SP-100** – also helps ensure that our products will meet your immediate and future needs.

Security

It's a common misconception that wireless devices are not as secure as wired networks. In fact, wired and wireless networks are both vulnerable – and a well designed, properly implemented wireless network can be more secure than a typical wired one.

Show your IT group that most of today's wireless solutions for industrial applications – unlike older office and automation networks – are designed with security in mind. Encryption, authentication and verification, key management, and anti-jamming measures all help prevent unauthorized access to network data. You can work with IT and your wireless supplier to identify the techniques that make the most sense in your application.

Adding a wireless component to your existing plant environment may also prompt a more comprehensive review of plant information security in general – from firewalls and virtual private networks (VPNs) to passwords and anti-virus software. That’s a good thing! In fact, system audits and reviews of security procedures and policies should be done on a periodic basis, regardless of specific networking decisions.

*(To learn more about securing your wireless network, see the Wireless course on **Security**.)*

The Emerson Advantage

Emerson Smart Wireless solutions also have security designed in from the start. For example, our 1420 wireless gateway offers built-in key-management capabilities, including automated key rotation. The 1420 gateway also supports a wide range of standard authentication protocols on the Ethernet side (wired or wireless), including EAP, Radius, 802.1x, LDAP, and Kerberos. Those are capabilities your IT group will understand and appreciate.

Support

Just like the other parts of your plant, your wireless system may need periodic maintenance, upgrades, and other support.

Timely implementation of patches, as well as anti-virus software, will help to ensure that the gateway and devices are updated in a consistent manner, and may prevent a costly shutdown of plant operations.

Your IT group can be a great resource for best practices on handling patches and upgrades, as well as network troubleshooting if needed. They may even be willing to do it for you.

Regardless of who does it, the work will be easier – and your IT department will be less concerned – if your supplier has a record of making reliable products and an efficient system for managing patches and upgrades.

The Emerson Advantage

Emerson has a longstanding reputation for making reliable products that help minimize maintenance costs. When patches or upgrades are appropriate, we will provide tools, training, and services to ensure network instruments, gateways, and software are updated correctly and consistently – in many cases without process downtime.

How IT can help

The preceding sections of this course focused on how to relieve potential IT concerns about wireless technology in process applications. But do you need to involve them at all?

Possibly not. If you are connecting a self-organizing wireless network to an existing process-automation network, especially through a wired gateway device, you may not need to involve IT. The process and equipment information collected from wireless instruments is the same as that from wired devices, and it will be used in the same way – all within the process-automation world.

If you include IT in your planning, however, you may benefit from their networking expertise, tools, and resources. For example,

- If you're using Wi-Fi, much of what they've learned about applying this technology in office environments will also be relevant in process-related applications.
- Their experience evaluating network suppliers and conducting IT-security audits can be useful as you do the same for your wireless network.
- They can be invaluable in determining the best way to make the data available to other plant and business systems.

Finally, if you expect your IT group to provide ongoing maintenance for your network, it's a ***very*** good idea to get them in the loop early and make sure it's implemented in a way they will support.

Summary

In this course you’ve learned that:

- Typical IT concerns about wireless networking in process-automation include technology risk and compatibility, security, and ongoing support.
- Using standards like IEEE 802.11 and/or 802.15.4 can reduce concerns about technology risks.
- Wireless networks can actually be more secure than typical wired networks – if they're well designed and correctly implemented – but a thorough review of *all* plant information security is a good idea.
- Planning for a wireless network should include processes and responsibilities for patches, upgrades, and other support.
- Even if a wireless networking project doesn't require IT involvement, their experience and expertise can be helpful.