PlantWeb University – Wireless 201

Network Components

15 minutes

In this course:

Overview

Selecting the right components for your wireless field network is just as important as selecting the right technology. That's because the components you choose can have a huge impact on the reliability, power consumption, and security of your wireless network.

Any network, whether wired or wireless, requires a transmission source to send a signal, a medium to carry the signal, and a receiver to accept the signal and do something with the information.

In the process automation world, this has traditionally meant field devices sending data over cables to a host system such as a DCS or PLC. Wireless networks use radio waves rather than cables for most data transmission, requiring some changes in network components – like adding radios and antennas.

In this course you'll learn about what to look for when selecting the components of a wireless network:

- **wireless field devices**, which collect and transmit data
- **gateways**, which provide an interface between the wireless devices and the host system
- **host systems**, which receive and manage the information from the wireless network

Because self-organizing networks are the preferred technology for wireless in-plant field networks, we'll focus on how these components are used in that type of network. This course does not cover components such as handheld communicators, PDAs, and tablet PCs used by mobile workers to wirelessly access process control networks..

Hint

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

- What are the components of a wireless field network?
- What should I look for in a wireless field device?
- What is a gateway?
- How will I integrate information from my wireless field network into my existing host?

Wireless devices

Wireless field devices have two parts: a traditional sensor to collect data, and a radio to transmit and receive that data.

Although some wireless devices use line power for the radio and sensor, "truly wireless" devices don't use wires for communications *or* power. Batteries are the most common power source, but some devices can also use energy-harvesting technologies to convert energy in the environment – such as solar, thermal, or vibration energy – into electricity. These significantly reduce reliance on battery power, which in turn reduces long-term maintenance costs associated with replacing batteries. *(For more about power sources, see the course on Power Management.)*

What to look for in a wireless device

- **Built-in router.** Devices in a self-organizing network are not only end-points that transmit measurement data; they also serve as routers that pass along data from other nearby devices. The more such devices in a self-organizing network, the more potential communication paths – providing an even more reliable network.
- **Low-power design.** Choose a device that is designed for low power consumption while providing appropriate signal strength, update rates, and reliability. Devices with integrated electronics for the sensor and radio typically have the lowest overall power consumption.
- **Multiple data types.** In addition to transmitting basic process-variable (PV) information, devices should also be able to communicate HART commands and event-driven notifications such as alarms, alerts, and configuration parameters. Some wireless devices also have built-in diagnostics that can detect or even predict device, radio, and battery problems – reducing the number of trips to the field to check on a device, and increasing your confidence in the network.
- **Low latency.** Measured by the amount of time it takes for data to travel from its source to its destination, excessive network latency can cause messages to arrive too late to be useful in certain types of applications. Make sure devices you choose won't allow latency to exceed the level specified for your application. To aid in network troubleshooting, you should also have on-demand access to information on actual latency.
- **Synchronization and time-stamping.** Choose wireless devices that can synchronize with a network clock and time-stamp all messages.

  Besides ensuring consistent time-stamping, synchronization across the network enables all devices to transmit and receive messages on a predetermined schedule.

Time stamps allow the network to recognize and compensate for latency, and provide a tool for verifying that a message has been successfully transmitted without being altered. They can also aid in record-keeping, such as for regulatory compliance.

- **Flexible communication timing.** Wireless devices should support a variety of measurement sampling and reporting intervals. That's because in a self-organizing network they not only transmit data from their own sensor, but also from other devices on the same network. The ideal wireless device will be able to report at intervals ranging from once every few seconds to once per day.
- **Support for "store-and-forward" data transmission.** In self-organizing networks, every node transmits not only its own data but also data from neighboring devices. With store-and-forward transmission, messages can be temporarily stored and processed at intermediary nodes, then forwarded to their destination at a scheduled communication time. This optional method of delivery reduces power consumption and boosts bandwidth efficiency.
- **Designed-in security.** Devices should offer message authentication, verification, and key management – right out of the box.
- **Support for multiple topologies.** A wireless device should have the built-in intelligence and flexibility to automatically be part of a star, mesh, or cluster-tree topology – or all three – as needed to achieve maximum network efficiency at any given moment.
- **Support for industrial standards.** For smooth integration and compatibility – even as your needs change in the future – look for devices designed to support emerging wireless standards for process automation.
- **Easy installation.** Installing even standard wired instruments can be a complex task. You can reduce installation costs and errors by choosing wireless devices that use the same sensor process connections and procedures as wired instruments.

The Emerson Advantage

Emerson's intelligent field devices – both wired and wireless – combine best-in-class sensor technologies with diagnostics to help you identify and even predict problems before they affect your operation. Our wireless devices are also optimized for low energy consumption and include a full suite of security features to enable a low-risk implementation.

Gateways

In the wireless world, a gateway provides an interface between the wireless field devices and the host system.

The gateway should ensure a seamless integration of data from the wireless network into the systems that use that data, including existing control systems, historians, and other hosts. When it does, you can use existing tools to manage measurement points, collect data, and process information – without having to distinguish between data coming from wired and wireless networks.

What to look for in a gateway

- **Compatibility with existing systems and networks.** Because your gateway may need to integrate data from wireless devices with your DCS, data historian, or some other system, it’s critical that it support a number of connections that can interface with different types of hosts.

The gateway should also function efficiently – without significant effect on power consumption or reliability – if there are other wireless networks in the same area.

- **Designed-in security.** You can reduce potential security risks by choosing a gateway that's designed to support advanced security strategies such as message authentication, verification, and key management.

  If the gateway offers wireless Ethernet output, it should also support security standards such as HTTPS (a secure web interface), SSH (a secure shell), and VPN (a secure link).

  To secure the network even more, a “controlled access” gateway can limit user access, as well as the kinds of tasks they can perform.

- **Self-healing capabilities.** Devices in self-organizing wireless networks can "heal" communication disruptions by automatically changing transmission frequencies or paths. The gateway should be able accommodate both methods.

- **Support for multiple topologies.** Like other nodes in a self-organizing network, gateways should be able to automatically become part of a star, mesh, or cluster-tree topology as needed.

- **Scalability.** Choose a gateway that allows you to **easily** add devices to the network at any time.

- **Diagnostic information.** The gateway should also provide network statistics and diagnostic data to help with installation, troubleshooting, and maintenance of the network. Information that should be easily accessible includes

  - Which devices are "alive"
  - Path statistics for each channel
  - End-to-end message reliability
  - Radio signal strength indication (RSSI)
  - Link Quality Index for individual segments of each communication path

The Emerson Advantage

Emerson's 1420 Smart Wireless gateway is designed specifically to meet the rigorous requirements of process automation applications – with added intelligence to help you make the most of a self-organizing wireless network. Capabilities include

- Easy-to-use security features, including automated key rotation and support for both wired and wireless Ethernet authentication methods

- Support for a wide variety of communication protocols to simplify integration into legacy host systems, including

  - Modbus/RTU and Modbus/TCP for DCSs and PLCs
  - OPC for data historians and human-machine interfaces (HMIs)
  - Ethernet for asset-management systems and other applications on the plant LAN
  - HTTP for web interfaces used in configuration and simple monitoring
  - XML and CSV for bulk data transfer

- Field-device diagnostic data, such as battery voltage and alarm indications, as well as network statistics

- Embedded web server for browser-based configuration, diagnostics, device operational information, and key management tools

- Support for self-organizing networks, including self-healing and self-organizing capabilities, and easy network expansion without rebooting or reconfiguration

- Seamless integration, with no requirements for proprietary software or nonstandard host-side hardware modifications.

Host systems

A host system is where most users will access and use the information from wireless networks. It could be a DCS, PLC, SCADA system, asset management application, data historian, or web interface.

In a well-integrated system, data will look the same regardless of whether it comes from a wired or wireless source. In addition, a host system should be able to easily integrate incremental data that will come from wireless devices. It should also allow you to configure wireless devices, and access network and device diagnostics, as you do for wired devices and networks today.

Some wireless networks may even provide data to multiple host systems. The type of host will determine how the gateway and host are connected.

For example, many modern control systems and process control networks communicate using Ethernet – enabling easy integration with gateways that also support Ethernet. This gateway-to-host connection can be either wireless or wired (including optical fiber).

Integrating data into a legacy DCS or PLC that does not support Ethernet, OPC or Modbus TCP will require a Modbus RTU connection. RTU is based on serial communication and is the most common of the Modbus protocols. Modbus RTU can also support HMI (Human-Machine Interface) applications.

Data historians and many other applications can be connected using OPC (Object linking and embedding for Process Control) – a widely used industry standard for real-time data interchange. Such applications can provide information to users in operations, maintenance, and engineering while avoiding sending data not critical for control or safety to the DCS.

The Emerson Advantage

Emerson's DeltaV process automation system was the first digital automation system in the industry to embrace standard platforms and open protocols as an inherent aspect of the automation architecture. For years this has allowed us to support and easily connect customers using a wide variety of wireless solutions.

Data management

Wireless networks can provide the data needed to gain a better understanding of what's happening in your operation. Trending, data historians, and other forms of data management can provide the information to help you reveal more efficient ways to run your plant and manage your assets.

All data-management applications should be able to accept data from wireless sources. For example, asset-management software should allow you to access device diagnostics that are transmitted wirelessly just as if they were collected through a wired network.

The Emerson Advantage

Our industry leading AMS Suite applications allows seamless integration of wireless data and allows users to capture and utilize 'stranded' diagnostics from installed HART devices. Linking the 1420 Smart Wireless gateway to the AMS Suite: Intelligent Device Manager application provides access to a full complement of capabilities for device diagnostics, configuration management, calibration management, and maintenance documentation.

New applications may also appear that leverage the ease and cost-effectiveness of accessing data wirelessly. Possibilities include logging activation of remote pressure-relief valves for regulatory compliance, and monitoring use of safety showers to speed emergency response.

Vendor selection

It’s best to work with a supplier who has the process and automation know-how to understand your objectives – not just for your wireless network, but for the operation it supports – and provide the appropriate technologies and services.

The vendor you choose must be committed to open standards and interoperability. That way, you can be confident that your network components will continue to work even if you expand or change your network (or even switch vendors) in the future.

The Emerson Advantage

All components in Emerson's Smart Wireless solutions have been designed and proven to solve real-world process automation problems. Emerson can deliver complete solutions for implementation of highly reliable wireless networks, and our commitment to open standards provides assurance of smooth integration and future compatibility as your needs evolve.

Summary

In this course you learned that…

- The primary components of a wireless field network are wireless devices that collect and transmit data, gateways that provide an interface between the devices and host systems, and host systems that allow users to access and manage their data.
- Important capabilities in a wireless field device include a low-power design, and support for self-organizing network capabilities and diagnostics.
- Gateways should provide compatibility with a wide range of host systems, as well as security, scalability, and self-organizing network capabilities.
- Potential host systems range from distributed control systems to data-historian and asset-management applications, with a variety of network-connection and data-management methods.