Thinking Through Wireless

Jonas Berge shares some tips & tricks for deploying wireless in process applications.

There are many different types of wireless networks, and not all of them are interoperable. Careful consideration should be taken at the beginning to ensure that you are not left with an antiquated network. So it is advisable to protect your investment with a wireless solution based on an international standard.

And to ensure a wide selection of products, and replacement parts with market-based prices, use a wireless standard adopted by multiple vendors. These should be companies you are already familiar with and use today. The WirelessHart (IEC 62591) standard has been adopted by many instrumentation and controls suppliers.

However, using the same IEEE 802.15.4 radio alone does not ensure interoperability. Therefore make sure all wireless transmitters in the plant also use the same "application protocol", such as Hart. This ensure all transmitters are integrated with the system the same way, are easy to replace, and that they are all setup, calibrated, and diagnosed the same way.

You should also check if the technology has been independently trialed in a multi-vendor plant environment to verify it meets process user requirements. For instance, WirelessHart transmitters from different vendors were independently tested by NAMUR at a BASF plant in Germany. The trial confirmed WirelessHart meets user requirement such as:

- Has high availability/reliability
- Can coexist with other wireless networks
- Cyber security
- Multi-vendor interoperable
- Long battery life

By ensuring that all wireless transmitters are compatible with the same handheld field communicators, laptop software, and documenting calibrators your plant already has and your technicians are familiar with, you can simplify work and avoid specialized software and tools.

The familiar handheld Hart tools also work for WirelessHart.

Network planning

Network planning need not be expensive or time consuming, but is critical to realize for a robust network. Determine what current applications will be wireless, and also consider potential future projects. Your gateway or access point should be located in an area which enables you to meet your current needs and also allows you to meet future needs without unnecessary repeaters or new access points.

Proactive users will consider putting a wireless infrastructure throughout the site so future projects can be more quickly and cost-effectively deployed without additional infrastructure investment.

Don't rely on RF studies of the plant for robust network planning. These studies are often very expensive and only capture the RF environment at that single point in time. Pumps, motors, cars, and the weather can change the RF patterns and will vary unpredictably. Instead, use network planning tools that can account for the total mesh network and varying obstruction density. Mesh networks will adapt more easily to changing RF conditions than other networks. Wireless transmitters are able to communicate 200 m, 600 m, and even 800 m. However steel obstacles in the plant can reduce the maximum range to 100 m or less, depending on density. For this reason, using mesh topology is more important than maximum range. With WirelessHart, messages can be relayed seven or more times between transmitters to circumvent obstacles and sources of noise. Star or point-to point topologies will not be able to maintain network reliability in dense environments where EMI fields change regularly (like all plant environments).

An RF study only captures the operating environment at a single point time; a planning tool that can account for the total mesh network is a much better option.

Deploying wireless instrumentation and Wi-Fi in separate access points will simplify future upgrades, because the IEEE 802.11 standard evolves rapidly with new versions every other year.

Plant performance can be improved, and operations and maintenance cost reduced, by deploying hundreds or thousands of wireless transmitters in applications around the plant. But do not lump all these transmitters onto the same network. Instead, create one smaller dedicated network for each plant area, each gateway associated with that area's DCS controller. This fits nicely with responsibilities divided by plant area.

When wireless transmitters are used for measurements essential to operations, consider use of redundant gateways to increase availability. Remember to include UPS or redundant power supplies and transient protectors (if required). Redundancy doesn't help if the power is lost to both.

The IEEE 802.15.4 radio used in wireless field instruments and the IEEE 802.11 (Wi-Fi) both operate in the 2.4 GHz band but have been designed specifically to not interfere with each other. However, for backbone applications carrying high bandwidth data such as from multiple video cameras, consider using Wi-Fi in the 5 GHz band.

Battery power

By specifying wireless transmitters that use hot-swappable intrinsically safe power modules, battery replacement in the field is made possible. Note that no industrial wireless transmitters use regular carbon-zinc or alkaline batteries. As 10-year battery life is likely with low-power IEEE 802.15.4 radios

found in many devices, large numbers of spare power modules are not required. Consider stocking the same number of spare batteries as a traditional transmitter – typically 10 percent of the total installed.

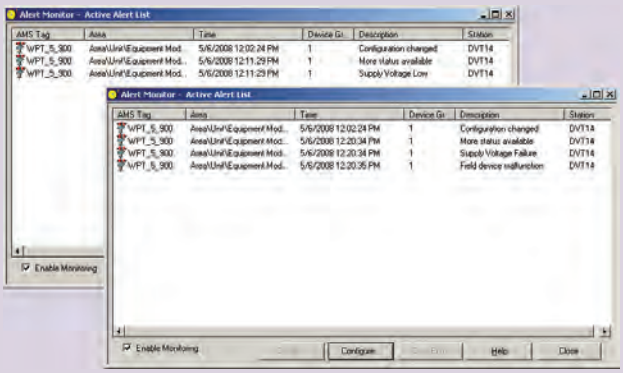
Use a wireless technology based on the low-power IEEE 802.15.4 radio technology to ensure long battery life. Note that 10-year battery life is possible with mesh topology because the routing function only turns on the radio, not the sensor, measurement electronics or display, all of which consume the most power.

While one second update periods are available in networks today, do not default all transmitters to this setting. The biggest impact on battery life is measurement updates, since the sensor must be powered. Although the radios in a mesh network may be powered more frequently to enable mesh routing, this has minimal impact on battery life. Take a moment to decide what update rate is really required. Depending on the application, a temperature check once every minute is often sufficient, and vibration checks every half-hour are appropriate.

The biggest impact on battery life is measurement updates, since the sensor must be powered.

To optimize battery replacement, use an intelligent device management software to monitor all wireless transmitters for low battery warnings. WirelessHart transmitters provide escalating battery warning before and near battery end of life.

In fact, intelligent device management software should be used to monitor overall device health for predictive maintenance. WirelessHart adaptors support pass-through of full diagnostics for even the most advanced devices such as valve positioners. Overall health is reported in every process value update. Technicians can then zoom into increasing depth of detail.



Intelligent device management software provides early and escalating battery warning.

Security issues

Make sure the wireless technology supports the security mechanisms to protect against various cyber attack threats. The minimum required protection measures are:

- Encryption
- Authentication
- Verification
- Anti-Jamming
- Key Rotation
- Sequence Number

Most importantly, verify that it is not possible to purposely or inadvertently turn security off. For WirelessHart the security cannot be disabled. Look for third party security certification of your wireless networks including Achilles testing.

You should also let the gateway periodically rotate (change) the encryption keys automatically to make hacking more difficult. And to avoid the security risk of "sticky notes" with passwords written down, consider using intelligent device management software which can automatically generate the network join key (password) and automatically transfer it into the wireless transmitter using a wire modem. This way the join key is not revealed to any user, and there will be no issue of typing it in incorrectly.

For ease of use, share a common join key for all transmitters on the wireless network. If a higher level of security is required, use individual join keys for each transmitter, but do so only with intelligent device management software which can automatically generate, assign, and track all these join keys. Exposed IP addresses present a security risk as hackers can "spoof" the network and take it down or insert unauthorized traffic. Therefore use wireless instrumentation which does not rely on IP addressing. WirelessHart meets this requirement which means the I&C department can freely deploy WirelessHart transmitters without IT involvement.

Wireless networks can do control, but fast-update requirements need careful planning and you should discuss with your vendor.

How about control?

While monitoring has been the main application for wireless thus far, wireless networks are ready for control applications today and have been used successfully by end users.

Several types of "control" are often referenced with regards to wireless. For slow or open loop control, most networks are quite capable of this, with >99 percent data reliability. When it comes to fast updates, some networks claim to be able to support one second updates for fast wireless control. Mesh and star/point-to-point topologies are capable of this, but both will require some careful planning. Make sure to ask the vendor for any practices or limitations that will need to be followed to assure >99 percent data reliability. For PID control, although no network currently has a wireless valve positioner, highly reliable wireless networks can be used for measurement input into PID loops. And for discrete output, some networks, including WirelessHart, do support devices with discrete output capabilities. These can be used with reliable networks for latency tolerant control applications like level control, or mixing applications. **CEA**

Jonas Berge, is Director of PlantWeb Consulting, Emerson Process Management (www.emersonprocess.com).