Benefit by installing reliable, secure wireless communications networks at your plant

By John Blaney, Emerson Process Management

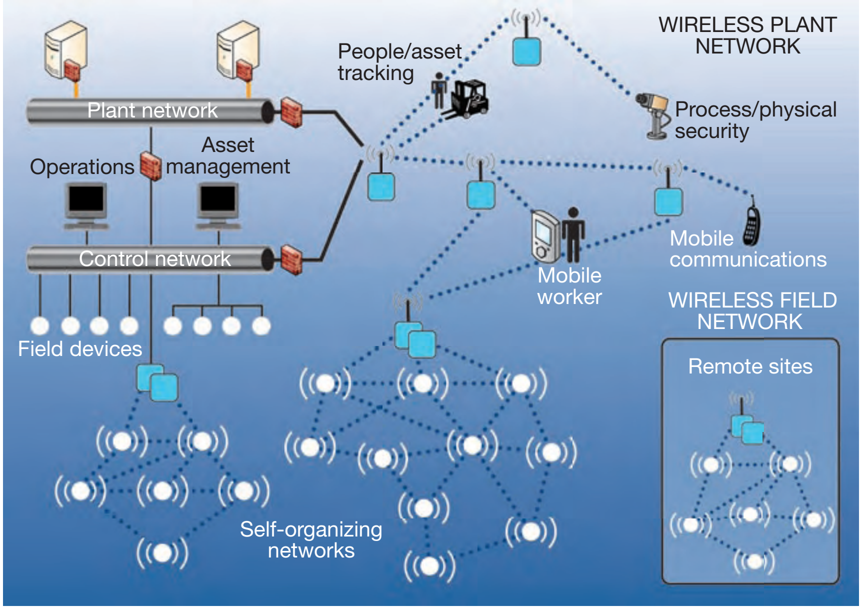
The market for wireless devices and equipment in process and manufacturing plants is on a fast-growth trajectory. A recent study by the ARC Advisory Group (see sidebar) projects sales increasing by 32% per annum to $1.1 billion in 2012. Primary reason for the bullish outlook: An enviable record of successful deployment continuously reaffirms the value of wireless technology; positive experience, in turn, spurs further acceptance.

Flexibility and scalability, coupled with low-cost implementation and ongoing technological advancement, make wireless solutions both practical and economical. Having achieved success in the process world, the technology is migrating to the generation sector of the electric power industry, where it is quickly gaining acceptance.

Understanding how wireless devices can improve powerplant operations and economics requires some background on the basics of the technology. The primer that follows also illustrates wireless solutions and shows how the technology can give you access to information that was generally inaccessible previously. A few short case histories demonstrate the value wireless already is delivering to forward-thinking owners.

Wireless 101: Field networks

Wireless networks can be characterized as either field or plant networks (Fig 1). Each serves different applications and has specific requirements for bandwidth, power, and standards.



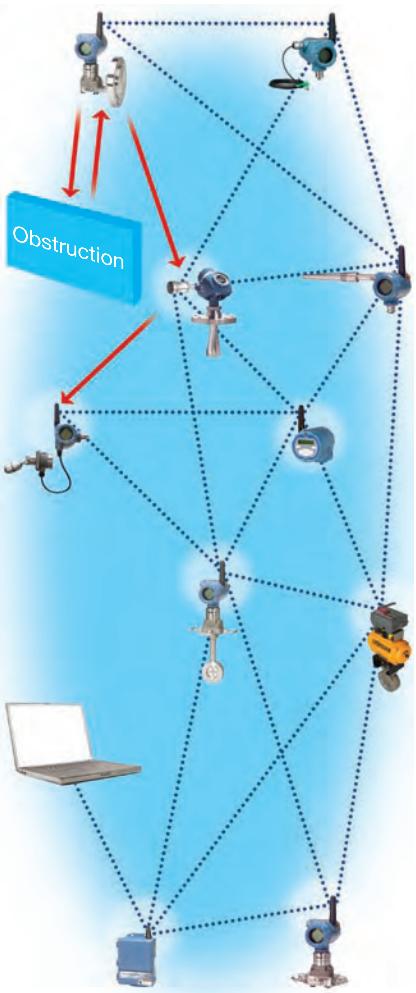
1. **Seamlessly integrating** wireless field and plant networks, and existing wired networks, into a single plant architecture helps optimize applications across the enterprise

Field networks, formed by wireless field devices and gateways, are configured for process applications, process control, and diagnostics. Remember that wireless field devices function the same way as traditional wired instrumentation and measure or sense pressure, temperature, flow, level, corrosion, vibration, etc, in critical equipment like turbines, pumps, boilers, generators, etc. Typical field applications include continuous monitoring of (1) pressure relief valves and stacks to avoid environmental excursions and related fines, (2) temperatures at heat-transfer equipment to alert when fouling impacts efficiency and cleaning is necessary, (3) valve position to ensure the process is properly aligned, and (4) vibration—even when the equipment itself is rotating.

Design. Two competing technologies serve wireless field networks: point-to-point and self-organizing mesh. The former relies on direct line-of-sight communication between each device and its gateway. It is less flexible and potentially less reliable than a mesh network because a single obstruction can initiate a communication failure.

By contrast, wireless mesh networks enable each device to act as a router for other nearby devices, passing messages along until they reach their destination (Fig 2). Devices and gateways work together to establish multiple paths of communication. If there is a change in the network or conditions that affect communications, they immediately move to the next available communication path based on signal strength.

Mesh networks deliver data at greater than 99% reliability. As new obstacles are encountered in a plant—such as scaffolding, new equipment, or moving vehicles—these dynamic networks reorganize around them automatically, without



2. Wireless field networks based on mesh technology deliver data at greater than 99% network reliability. As new obstacles are encountered in a plant, these dynamic networks can reorganize around them automatically—without any intervention by the user

any user intervention. Adding and moving of devices also is simplified: As long as a device is within range of at least another in the network, it can communicate. However, best practices for maximum network reliability require that two or more devices be within range.

Because point-to-point networks require direct, line-of-sight communication between each device and its gateway, network set-up often is time-consuming and expensive. A site survey must be conducted to ensure that every node in the system has a line-of-sight path. Such surveys are not required for configuring mesh networks. Another disadvantage of point-to-point networks: They may require as many as five times the number of infrastructure nodes as a self-organizing network.

Operation. Wireless field networks

must be based on open standards to ensure interoperability. Work is ongoing in this area. The Hart Communications Foundation (HCF, www.hartcomm2.org) has ratified WirelessHART™, which adds wireless capabilities to the HART protocol while maintaining compatibility with existing HART devices, commands, and tools. International Engineering Consortium (IEC, www.iec.org), and the International Society of Automation (ISA, www.isa.org) also are developing wireless standards for process control applications.

WirelessHART is the standard that Emerson Process Management and other vendors—including ABB and Siemens—use in manufacturing their wireless intelligent devices. WirelessHART field networks use self-organizing mesh technology and are designed and tested to tolerate almost all interferences; they can coexist with other wireless networks in a plant.

These field networks are designed to the very-low-power IEEE 802.15.4 standard—the same radio technology that also underlies the Bluetooth® and ZigBee wireless communication protocols. The bandwidth characteristics of WirelessHART permit reliable and secure delivery of short, high-priority bursts of data.

In effect, Wireless HART devices only "come to life" when scheduled to do so, maximizing battery life. This intermittent operation and the low power requirement combine to keep batteries in service from five to seven years, depending on the application, update rate, environment, etc. Still longer battery life is predicted for the future.

Security is of top priority when developing wireless solutions. WirelessHART uses a multi-layer approach to assure the highest level of security: frequency-hopping/anti-jamming measures, encryption, authentication, verification, and key management.

- Frequency-hopping spread-spectrum radios are used in anti-jamming measures. WirelessHART uses 2.4-GHz frequency for communication, hopping around 16 sub-channels to avoid any interference in the environment—deliberate or not. Spread-spectrum radios are commonly used for security with wireless communication, but should not be considered secure by themselves because they have to run through frequencies and channels on a preset schedule, which can be duplicated.
- Encryption is one of the other mechanisms used by WirelessHART to assure secure communication. It entails taking the HART data packet and scrambling the information so it cannot be used if intercepted. Once received by the intended network, the information is decoded and translated back into usable data.
- Authentication and verification ensure communication is taking place between legitimate, approved parties. Think of them as "handshakes" that allow only known devices in the field network to communicate with each other. For example, authentication on a phone conversation starts with knowing who you are calling, or "prior" identification, and confirming they are who they say they are through voice, accent, and personal information.
- The wireless gateways and devices in the field network maintain a white list of known and joined devices they can communicate with. Any other devices are considered rogues until they join correctly and present the right credentials. Verification uses so-called message integrity codes on top of encryption to ensure the data packets both on an end-to-end and on a per-hop basis are correct.

This prevents rogue devices from being able to mimic a legitimate device and its data, which is akin to the other person on the phone with you providing information only both of you know. If a device is not properly authenticated, other devices will not communicate with it. If a device doesn't verify the data packet correctly, the data will not be used and the device is considered unreliable until it verifies correctly.

- Key management refers to use of passwords to ensure that only authorized devices have access to the data. Without the proper "key," access is denied. Regular key rotation provides an additional measure of security to ensure that keys cannot be duplicated easily.

A gateway interfaces the wireless field network with the wired network world. Most elements of the security components identified above also should be employed on both sides of the gateway. Because the wireless field devices do not use TCP/IP messaging, if an intruder tries to compromise that side of the network, the attempts will be ignored. However, because communication from the gateway to the control system does use TCP/IP messaging, the addition of a firewall or other industry standard technique—such as VPN or HTTPS—is strongly recommended to provide the necessary security.

Wireless 101: Plant networks

Whereas field networks are used to communicate critical process control information, the wireless plant networks serve applications not necessarily central to the basic power-generation process. These include data connectivity, video/perimeter security, voice communication, and people and asset tracking. Some examples include the following:

- A wireless plant network enables mobile operators with suitably equipped wireless laptops to monitor processes anywhere on the plant floor.
- A plant-wide wireless broadband network with Voice over Internet Protocol (VOiP) can replace walkie-talkies. This targets and expands the flexibility of mobile communications, because messages can be broadcast to specific teams based on the IP address of each worker's radio.
- Installing wireless transmitters at eye-wash or shower stations improves health and safety by alerting emergency personnel when activated; assistance can be dispatched, if necessary.

These and other high-bandwidth plant network applications are based on IEEE 802.11, an accepted industry standard commonly referred to as Wi-Fi. Unlike wireless field networks, which are supported by the process industries and organizations serving them, the standards for wireless plant networks are driven by the IT community.

Wireless plant networks also can be based on either point-to-point or mesh technology and they share many of the same security concerns that exist with wireless field networks. Wireless field networks and devices were designed from the start with built-in security features, wireless plant network technology was not. Because plant networks use open IT standards, it has become necessary to add security measures to address evolving concerns. This means it's in your best interest to choose a plant network supplier with the capabilities to address the full range of security concerns to the satisfaction of the IT community.

For example, Emerson Process Management works collaboratively with a leading networking vendor to deliver open-standard wireless plant network applications to the electric power industry. Using that vendor's highly secure wireless architecture, Emerson builds plant networks that offer industrial-class wireless access points, controllers, security and network management software, plus the plant applications that use them. The architecture provides integration within a plant's existing IT infrastructure, thereby eliminating the need for a complex wireless overlay network. Another advantage: Configuration and management of the plant's wireless plant network is centralized, reducing overall cost of ownership.

Case histories

An increasing number of power producers are implementing wireless solutions, using them to cost-effectively extend the capabilities of a digital-bus-based plant architecture to

Key terms in a new language

Communication technologies bring with them a new lexicon that powerplant personnel will have to become familiar with—as if they didn't already have too much to do. Some unfamiliar acronyms are spelled out in the text and web addresses given to facilitate access to additional information. More acronyms and unfamiliar terms are defined succinctly below.

ARC Advisory Group, founded in 1986, is a leading research and advisory firm for manufacturing, energy, and supply-chain solutions. One of its practices guides electric utilities with their strategic planning, supplier selection, and technology assessment needs. Goals include helping clients improve their return on assets, operational performance, shareholder value, etc.

Access www.arcweb.com.

Bluetooth™ is defined by Wikipedia as a wireless protocol for exchanging data over short distances from two or more fixed and mobile devices, thereby creating personal area networks. It was originally conceived as a wireless alternative to RS232 data cables.

The Bluetooth Special Interest Group (SIG) is a privately held not-for-profit trade association founded in fall 1998. It does not manufacture or sell Bluetooth-enabled products. Member companies, including leading telecommunications and computing firms, drive technology development and implement and market Bluetooth in their products.

Access www.bluetooth.com.

HTTPS, or Hyper Text Transfer Protocol Secure is a secure version of the Hyper Text Transfer Protocol (http) that you are probably familiar with. It was developed by Netscape Communications to permit secure commerce transactions—such as online banking. The encryption and decryption routines that it runs protect against eavesdropping and man-in-the-middle attacks, according to WhatIs.com.

TCP/IP (Transmission Control Protocol/Internet Protocol) is the network protocol of the Internet because of its ability to connect together networks of different sizes and systems. It originated from research sponsored by the Dept of Defense and provides the functions necessary to deliver a package of bits from a source to a destination over an interconnect system of networks. There are no mechanisms to promote data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols.

Access www.cisco.com.

locations that were inaccessible previously or impractical financially. To illustrate: Millions of installed smart HART-based devices have some level of diagnostics capability but many plants don't have the infrastructure to receive these HART data into an appropriate system.

Since only a small fraction of these devices is monitored digitally, the potential gain from accessing such "stranded" diagnostics is significant. Existing wired HART devices can be upgraded with a wireless adapter to transmit diagnostics information to where it can be used to initiate corrective action as necessary.

The following case studies illustrate the diverse applications to which wireless technology can be applied, as well as the quantifiable benefits.

Case history #1. An electric power producer has two gas turbine/generators and 11 remote pump houses at one site. Each of the pumping stations has a small heater to protect against winter freeze-up. Should a heater fail and water freeze, cost to repair or replace the pump and associated piping could run as much as $20,000—not including the cost of downtime, which could be up to three days.

Wireless temperature transmitters were installed in each of the 11 remote buildings. The devices communicate through a wireless gateway back to the control room, alerting operators to any rapid temperature changes in the remote buildings so they can take corrective action before damage occurs. The alternatives, running trays over the roads or conduit under existing structures, were far too expensive.

Case history #2. A power producer turned to wireless to improve plant performance. It instrumented multiple points to access the data for the performance-improvement effort and then transmitted that information to the plant's existing distributed control system. In sum, nearly 120 wireless devices—mostly pressure and temperature transmitters and wireless gateways—were installed on five turbines. The project would have been cost-prohibitive to implement with a wired solution. Benefits included a reduction in downtime, improved staff efficiency (elimination of operator rounds), and lower maintenance costs.

Case history #3. Laboratorio de Pruebas de Equipos y Materiales (Lapem), the certifying agency for Mexico's Comision Federal de Electricidad (CFE), the national electric utility, is using wireless technology to reduce the time required to calculate the performance of the nation's generating units.

One of Lapem's duties is to evaluate the performance of CFE's 140 combined-cycle, fossil steam, nuclear, hydro, and geothermal plants by measuring pressures, temperatures, flows, and power production.

The laboratory has only five analysis teams to install test instruments at each plant, take measurements, and tear down the setups. Using traditional wired architecture, the Lapem teams could only evaluate about 50 plants annually, short of its goal of reaching every facility biennially.

Wireless was considered a solution for reducing turnaround times. To evaluate its merits, one team was equipped to establish temporary wireless networks in the powerplants it was assigned. This involved installing up to 25 wireless instruments per plant, plus a wireless gateway to receive key flow, pressure, and temperature measurements. Data were routed to a thermal-efficiency model to determine unit heat rate and the efficiency of principal equipment—condensers, cooling towers, boilers, turbines, etc. Results help the analytical team identify problems that must be addressed to improve performance.

Using wireless devices, the Lapem team completed its onsite work in 10 days, five less than the 15 days required when wired instruments are used. The bottom line: The wireless solution enabled the team to improve its productivity and plant coverage by 10%, which translates to an annual revenue increase for the laboratory of $512,000. Also, by covering more plants, the team helped CFE increase its revenue (higher plant output resulting from improved performance) while reducing operating costs.

The ease of use and reliable performance of wireless infrastructure convinced Lapem to equip all five of its analytical teams with wireless instrumentation. Expected result is that 25 more assessments will be conducted annually, generating an additional $1,375,000 in revenue with existing staff. Also, all plants can be tested every two years.

(Wire)less is more

The first step in your wireless journey begins with deciding on the application(s) for which the technology will be used. This, in turn, determines whether the application calls for one or more field networks, a plant network, or both. From there, plant personnel should investigate the options available to them and consider not just the current need, but also think more broadly about how wireless technology might benefit other aspects of the plant.

As part of this assessment, it is important to select an approach based wholly on open standards, which helps ensure that a facility

VoIP, or Voice over Internet Protocol, is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular phone line. VoIP services convert your voice into a digital signal that travels over the Internet. If you are calling a regular phone number, the signal is converted to a regular telephone signal before it reaches the destination.

Access www.fcc.gov/voip.

VPN, or Virtual Private Network, is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network—such as the Internet—instead of by physical wires. A common application is secure company communications through the public Internet to accommodate the needs of remote employees and distant offices.

Access http://computer.howstuffworks.com/vpn.htm.

Wi-Fi is a global standard for high-speed wireless local-area networking. The Wi-Fi Alliance, a non-profit organization with more than 300 members in more than 20 countries, develops tests and certifies wireless devices that implement IEEE 802.11 specifications. To date, the group has certified the interoperability of more than 5000 products.

Access www.wi-fi.org.

ZigBee is a wireless language that connects dramatically different devices and enables them to work together. The ZigBee Alliance is a non-profit association of more than 300 member companies that are driving the development of reliable, cost-effective, low-power, wirelessly networked monitoring and control products based on an open global standard.

Access www.zigbee.org.

is not handcuffed to a specific technology or vendor. It is particularly beneficial to work early on with an established, reputable vendor having a proven track record—one that can manage and advise through all phases of the project.

Also, while wireless is many things, it is important to also remember what wireless is not. At the field level, it is not intended to completely replace wired instrumentation, and—at least now—it is not designed to control boilers, turbines, or other critical power-generation processes. Wireless technology can be used for certain types of control—specifically where the chosen solution can meet latency and update requirements of the application. These typically include open-loop control applications and latency-tolerant non-critical control.

What it can do is cost-effectively extend the full benefits of a digital-bus-based plant architecture to locations that previously were inaccessible or financially impractical. Data from wireless devices can be seamlessly integrated into the control system, offering insight into additional plant and process data for control and asset optimization.

At the plant level, a wireless infrastructure also has implications for workforce productivity—as operators no longer have to make "clipboard rounds"—as well as for plant management, including physical plant security, video monitoring and surveillance, and people and asset tracking.

Seamlessly integrating wireless field and plant networks, and existing wired networks, into a single plant architecture helps optimize applications across the entire enterprise. And it is affordable, with installed costs significantly lower than a wired equivalent—as much as 90% lower in the case of a wireless field network. This is possible because going wireless eliminates the time and expense of drilling through concrete decks, installing conduit and cable trays, and pulling wires.

From an implementation standpoint, wireless is attractive because it is both flexible and scalable. It is not an "all-or-nothing" scenario. Instead, power producers can adopt this approach wherever it makes sense for their plant. By picking an application—even a small one—users can achieve improvements that would not be possible in a traditional plant configuration. They can easily expand their wireless portfolios later, as budget and confidence in the technology grow.

Finally, keep in mind that wired and wireless networks are complementary technologies and as such, operate side-by-side in the plant environment, each serving an important purpose. For power generators looking for a flexible, scalable, and economically feasible solution to optimize plant operations, one thing is clear: When it comes to wireless technology, less really is more. CCJ

John Blaney is Emerson Process Management's PlantWeb® product manager. He has more than 30 years of experience designing, installing, and troubleshooting power-plant control systems. Blaney participates in determining functional requirements for the company's Ovation® products—including intelligent instrumentation, digital fieldbusses, distributed controls, and the management of these smart assets. He can be reached at john.blaney@emerson.com.