

Honeywell Process Solutions



Wireless Technology Delivers Value to the Power Industry

Cindy Bloodgood, Honeywell Process Solutions

Table of Contents

Introduction 3

Background 3

 Today's Environment 3

Applications for the Power Industry 4

 Related Developments 5

Selecting the Right Network..... 6

 Choosing a Wireless Supplier..... 8

Conclusion..... 9

Table of Figures

A wireless mesh network has multiple paths between access points, or nodes, to establish a redundant infrastructure. 6

Introduction

Wireless technology offers benefits beyond just wiring cost savings. With a multi-functional, plant-wide wireless network, utility and power generation facilities can improve safety, reliability and efficiency through optimized employees, equipment and processes.

This paper is intended to assist power industry companies in exploring the endless possibilities of wireless in plant automation. It will help end users understand what to look for in selecting the right wireless network for their requirements, and then learn how to get started with this innovative technology.

Background

Wireless technology has revolutionized network connectivity in the IT world, as well as the commercial and consumer markets. Substantial growth in wireless solutions is driven by standardization, industry investment and R&D. Modern wireless applications and sensors deliver powerful new capabilities enabling end users to improve operational performance. Wireless systems not only provide advanced sensing, but also help users make decisions positively impacting their overall business objectives.

Despite arguments concerning the use of wireless in power plants, there is little doubt the technology is here to stay. The path forward still has question marks, but a growing number of electric power facilities recognize the potential of wireless systems to reduce costs and improve efficiency across their plant and business enterprise.

The benefits of wireless go far beyond saving on installation and wiring costs. Wireless helps plant operators gather field data more easily, increase asset life through continuous monitoring, and improve the safety of their most important assets—their people. Wireless also enables improved plant availability, reduced downtime, and increased productivity.

As wireless technology gains greater acceptance, the wired world is slowly fading into the background. Protocols such as Wi-Fi represent the future—not only for traditional wired IT network requirements, but also for monitoring and control applications across the plant floor.

In order to take advantage of all the benefits wireless technology has to offer, power plants must adopt sound policies mitigating risks and ensuring adequate security for processes, people, and the environment.

Today's Environment

Power plants implementing wireless systems do so for the same reason as the designers of the first telegraph system—cost savings. Utilities look to wireless to add real business value, both in terms of installation costs and optimized operations from increased data availability.

Just as Marconi's technology eliminated the need to erect poles for wired communication, modern wireless solutions simplify installation requirements when compared to conventional wired networking, while also improving reliability and productivity.

An ultra-secure and ultra-reliable wireless field infrastructure supports not just wireless instruments, but also IEEE 802.11 WLAN applications and mobile clients such as hand-held computers and mobile Human-Machine Interfaces (HMIs). A single wireless network, supporting multiple wireless technologies and classes of service, can handle diverse tasks ranging from communicating sensor information back to a host system, to closed-loop control, information, HMI, video, communication, and enterprise applications. Wireless technologies developed for building management and security can also be utilized in process plants to support both asset management and personnel tracking.

Modern wireless networks are formed with a series of wireless access points, or radio nodes, placed strategically in the facility. Many networks support a 'mesh' infrastructure where each radio node communicates to at least one other in range, providing backup

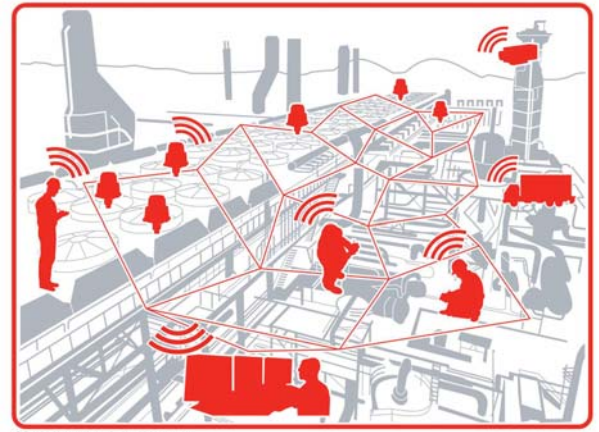
communication should communication from one be interrupted. The coverage area of the radio nodes working as a single network becomes a mesh “cloud.”

Most importantly, wireless networks can be designed to support multiple communications protocols, as well as existing applications and standard TCP/IP communications, so that legacy investments do not have to be discarded.

Applications for the Power Industry

Modern wireless solutions improve productivity by enabling the right people to be at the right place at the right time. Process and asset information can be extracted, viewed, and processed where the data resides to enable more accurate and timely decisions. Access to the right process data can significantly enhance operational efficiency and extend access to critical process information beyond the control room.

A wireless system can include anything from a network of transmitters monitoring a single, specific application, to a full-scale wireless network deployed across an entire site to handle multiple applications including monitoring and supervisory control.



In the evolution of wireless technology, the first generation of products was sensor specific and not designed to cover entire plants, which resulted in smaller implementations. Today’s generation of products is more appropriate for wider plant deployment.

For example, wireless mobility tools provide a fully functional PC environment that personnel can interact with directly from a handheld device while performing maintenance rounds, data collection and inspections. These solutions are optimized for specific end user applications, ranging from read-only access over the Intranet by multiple casual users, to secure system access for mobile operators. This wireless collaboration can improve decision-making, production uptime and process monitoring, and incident avoidance.

Handheld access to process data allows technicians in the field to view the latest plant information to help identify failures and causes that may previously have gone unrecorded, and can open the door for further investigation of a system’s reliability. Users can integrate field data with data from multiple other sources, including production, control, and work management systems. They also provide mechanical and engineering data and support calibration of instrument databases. On-site computing helps management improve the tracking and reporting of inspections, tests, and repairs for pumps, actuators, valves, vents, pipes and other plant process equipment.

The new breed of wireless transmitters enables employees to obtain data and create information from remote and hazardous locations without the need to run wires, where running wire is cost prohibitive or the measurement is in a hazardous location.

There are countless remote applications in power plants that can benefit from wireless technology. For example, one Nebraska power plant is using wireless technology to monitor their remote oil tanks. In addition, they are now able to efficiently monitor water run-off where electricity is not available. Their battery-powered transmitters transmit over long distances back to a powered node.

Other plants are considering applications such as:

- Supervisory control and data acquisition
- Emissions monitoring
- Flame sensing with transmitters or even a remote wireless video
- Control applications, such as turbine control, boiler control, or motor control
- Monitoring the health of rotating assets

Another specific example comes from a power plant in Bulgaria that used wireless temperature transmitters to measure steam used for heavy oil burners. These were entirely new measurements that were not available previously. They replaced a wired solution that would have taken two months just to procure, with a wireless solution that took just two days. Now that this network is in place, they will expand to detect gas at their water treatment plant with wireless detectors and send the signal 300-400 meters to their system.



Another remote example applies to large areas such as wind farms. Many have ineffective or no means to determine wind speed or kilowatt/megawatt power production. Battery-operated wireless devices provide the opportunity to gather data and effectively calculate production.

Furthermore, wireless multiplexers provide a simple and reliable means of implementing a wireless solution for applications with high-density I/O concentrations, providing the lowest cost per wireless measurement point that enables new applications that save millions of dollars on wiring costs. This can help with substation monitoring and communicating information back to a central monitoring station.

Wireless technology also offers an innovative, cost-effective alternative for measuring the health of water or corrosion from fluid in tanks and pipes. For example, remote analytical PH readings provide the ability to monitor water quality. And, with a wireless corrosion monitoring system, online and real-time corrosion monitoring now becomes cost-effective. A wireless solution can carry process and maintenance data over the same network. Correlation with maintenance and operator tasks is possible by enabling mobile workers with wireless technology, eliminating sifting through maintenance logs and matching tasks with corrosion data. It can all be integrated into one set of data.

Most importantly, wireless technology enables safety. With new opportunities for integrating asset tracking, people location data or real-time data and supervisory control, wireless technology can provide:

A real-time location system throughout the facility to monitor employee locations and ensure safe procedural operations

- Safety shower monitoring
- An infrastructure that supports emergency responders
- Wireless leak detection and repair support
- Integration with existing control and safety systems
- Continuous wireless monitoring of equipment and field devices for diagnostic equipment health assessments
- Voiceover IP for communicating

Related Developments

A recent report from Venture Development Corp. (Natick, Mass.) forecasts that the global market for wireless infrastructure networking products use in facilities will expand at a 34 percent compound annual growth rate over the next several years, rising from shipments of \$261.9 million in 2006 to more than \$1.1 billion in 2011.

New developments in wireless technology promise to open up a wide range of plant floor applications where cabling is either difficult to install or prohibitively expensive. Wireless also offers the key advantage of integration of multiple devices, such as sensors, mobile PCs, and security systems.

To keep up with wireless development activity and help process industry end users find the best solution for their unique application, several organizations are drafting recommendations or wireless standards as well as offering open solutions. Standards provide freedom of choice. If an end-user chooses not to pursue a turn-key contract, choosing strands-based devices will let them choose

For example, the Instrumentation, Systems and Automation Society's (ISA) ISA100 initiative, chartered in early 2005, is intended to create a roadmap for implementing wireless systems in the automation and control environment through defining and publishing a set of standards, recommended practices, and technical groups.

The objective of the ISA100 Committee is to assure the confidence in, and integrity of, digital wireless communications used in the manufacturing and power generation environment. The committee has developed criteria for the procurement and implementation of wireless solutions throughout the control system marketplace.

ISA100 compliance will ensure supplier specifications are consistent and easy to interpret; user requirements are succinct, relevant and easy to understand; technology options are clear and easily differentiable; and probable outcomes are quantitatively evaluated against alternative wireless solutions.

The power industry is currently represented on the ISA100 committee by companies such as TXU Power and Consolidated Edison. All end-users are welcome to participate. More information is available at:

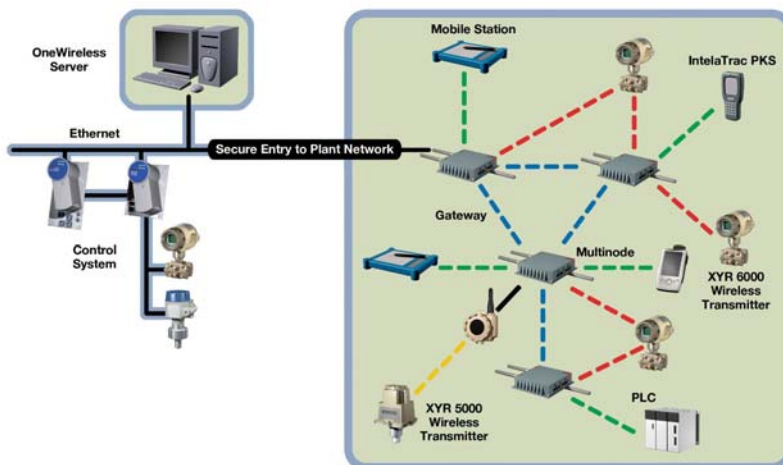
<http://www.isa.org/MSTemplate.cfm?MicrositeID=1134&CommitteeID=6891>

Emerging standards represent one criterion from which to make the wireless technology choice. However, with various solutions currently on the market and on the horizon, an opportunity exists today to start taking advantage of the benefits available with wireless-enabled applications.

Selecting the Right Network

Power companies and other end users considering the implementation of wireless technology have identified a number of key wireless system requirements. These include: high security, reliable communication, good power management, open platforms, multi-speed monitoring, multi-function capabilities, scalability, global usage, high quality of service, multi-protocol support, and control readiness.

According to wireless technology experts, the emerging wireless infrastructure will be based on a universal mesh network supporting multiple wireless-enabled applications and devices within a single environment. With just one network required to support multiple applications, deployment, network maintenance, and security management are simplified.



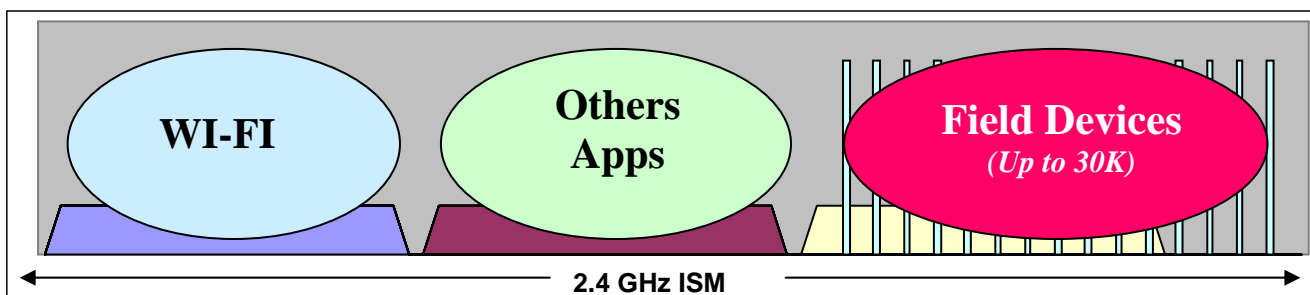
A wireless mesh network has multiple paths between access points, or nodes, to establish a redundant infrastructure.

A wireless network must be secure to ensure the entire facility is safe, offering one comprehensive and end-to-end integrated security system from the control or host system all the way down to the sensor. This means there's only one wireless security system to manage. A layered approach to security means protecting the network from multiple risks:

- A 'passive listener' can sit outside the facility just reading and accessing data. The response is to include confidentiality in the system with encrypted messaging.
- An 'active listener' can take good messages and resends bad ones, alters a real message, or replays old messages. They may only change one bit at a time – like turning on or off an alarm, event, or switch. To avoid this, networks need incorporated message integrity and replay protection, including time stamping, cyclic redundancy checks, and other message markers.
- A "rogue device" is an active attacker who takes the place of a good sensor and actively sends bad messages to the system. To avoid this, a network needs source authentication.
- A "DNS attacker" tries to flood the system with bad messages so that good messages can not get through, basically shutting down all wireless communications through a wireless access point. A secure network incorporates resistance to denial-of-service attacks through a combination of authentication, mesh network, redundant paths, and a performance designed architecture that minimizes affects on the mesh network.
- Another important feature includes a key management system that conveniently provides keys to sensors and nodes within the system, easily providing authentication easily.

Mesh networks use a self-propagating, self-healing network of nodes to achieve blanket coverage of an area. A node can send and receive messages, and in a mesh network, a node also functions as a router and can relay messages for its neighbors. If one node fails for any reason (including the introduction of strong RF interference), the network can re-route data and connectivity is not lost. With point-to-point signaling, the power consumption (and battery life) of each field device becomes accurately predictable. This efficiency helps extend the life of batteries to reach their standard shelf life, some up to 10 years, minimizing the time between changing batteries. Changes in latency caused by routing changes to the network also are eliminated.

Wireless mesh networks optimize performance with efficient use of industrial, scientific and medical (ISM) radio bandwidth and prioritizing messages so critical information is received first. Because communication devices using the ISM bands must tolerate any interference from ISM equipment, these bands are typically given over to uses intended for unlicensed operation. Unlicensed operation typically needs to be tolerant of interference from other devices. In the United States of America, ISM band usage is governed by FCC rules.



Efficient wireless mesh networks mitigate signal interference in these limited ISM bands by employing a frequency-hopping spread spectrum (FHSS). This technique modulates the data signal with a carrier signal that periodically "hops" from frequency to frequency across a wide band. Through the relaying process, a packet of wireless data will find its way to its destination, passing through intermediate nodes with reliable communication links.

Installing a wireless network at a power plant can pose some unique considerations to avoid the risk of electromagnetic field and RFI interference. Usually this can be easily mitigated with proper placement and antenna choices.

Fortunately, wireless communication is not line of sight technology, it can reflect and bounce off metal in a facility. There are three main ways to mitigate the risk from interference:

- Spatial diversity – every device sends to two nodes in different locations to diversify the communication
- Temporal diversity – a device sends data and if the data is not received by either node, it will retry two more times, and as quick as the next millisecond
- Frequency diversity – every transmission is performed at a different frequency. Typical EMI interference is short with scattered bursts, making it relatively easy to navigate around it.

Matching multi-hop, wireless mesh communications with distributed control facilitates a new dimension of interactions between sensors or sensor clusters. Sensors can now communicate directly with other devices on the network. Plus, monitoring equipment can take readings from sensors without having to directly access them via wired connections. This is useful in calibration and troubleshooting.

By utilizing a single, universal, wireless mesh cloud, end users have access to one integrated platform supporting multiple field protocols and applications. With a high-speed and self-organizing mesh configuration, network users achieve flexible channel allocation and a robust architecture with latency control and redundancy for safe wireless control. They also have one scalable network that conserves power and spectrum. Best of all, plant personnel only have one system to learn, operate and maintain.

Choosing a Wireless Supplier

Since most power companies are unwilling to act as system or platform integrators for their future plants, they look to their automation supplier to perform this function. This includes not just providing equipment and support services, but also managing the platform over the long term so that rapidly developing new technologies and applications such as wireless can be quickly and inexpensively added.

Plant operators also look to their automation supplier to manage embedded technology, so that process control systems remain up to date and skirt around technological dead ends without causing unnecessary cost and downtime.

Rarely can a single supplier meet both plant and office IT requirements. Instead, utilities should select a supplier with proven expertise in wireless applications and offering a broad product portfolio and user support capability.

Your wireless supplier-of-choice must have the experience necessary to adequately address security concerns at all levels of the plant enterprise. Robust security measures should be “built-in” to their wireless solution—not provided as an after-thought or add-on.

Key factors to consider when choosing a wireless technology supplier include:

- Comprehensive and end-to-end security measures
- Documented best practices for a secure wireless system configuration
- A secure wireless network architecture
- A keen focus and process providing users with the latest security fixes
- Qualification of anti-virus software
- Policies focused on high security
- Established services to help assess, design, implement and manage a secure wireless environment

Your supplier selection checklist should also ask:

- Does the supplier tightly integrate process control with physical and cyber security?
- Do they provide a dedicated security response team to monitor and advise upon emerging security threats?
- Do they offer a security design service providing a detailed design of the security infrastructure connecting your wireless network to the company's business IT network?

Conclusion

Power industry operations can now benefit from a wireless solution that satisfies the multiple conflicting demands of redundancy, distributed communications, flexibility, and reliability. Furthermore, self-configuring, self-healing wireless mesh networks are inherently less expensive to install and maintain as radios and microprocessors become cheaper. A significant barrier to low-cost connectivity has been removed.

To get started with wireless, and unlock the possibilities of this innovative technology, it is important to view your wireless implementation as a partnership between the plant operator, company IT department, and wireless supplier. Each party has a share in determining the outcome of this effort.

Also, it is best to manage your infrastructure as a single network. Think strategically about your wireless deployment and select a universal network meeting all of your needs. Experience has shown how a “piece-meal” system is a nightmare to manage.

Finally, always consider safety first. If you can't install wireless safely, it's better not to do it at all. Fortunately, with the right technology and support, you can enjoy all of the advantages of wireless while protecting your plant information and ensuring safe operations.

For More Information

To learn more about Honeywell's wireless solutions, visit our website www.honeywell.com/ps/wireless or contact your Honeywell account manager.

Automation & Control Solutions

Process Solutions

Honeywell

2500 W. Union Hills Dr.

Phoenix, AZ 85027

Tel: 877.466.3993 or 602.313.6665

www.honeywell.com/ps

WP-08-23-ENG
July 2008
© 2008 Honeywell International Inc.

The Honeywell logo, consisting of the word "Honeywell" in a bold, red, sans-serif font.