

Honeywell Process Solutions



IT Perspective On Industrial Wireless Security

Derek Benz
Chief Information Security Officer
Honeywell ACS

Introduction

Despite arguments concerning the use of wireless in the industrial environment, there is little doubt the technology is here to stay. Manufacturers recognize the potential of wireless systems to reduce costs and improve efficiency across their plant and business enterprise.

In order to take advantage of all the benefits wireless technology has to offer, industrial plants must adopt sound policies mitigating risks and ensuring adequate security for processes, people, and the environment. With increased economic pressures, continuing advancement of cost-effective wireless technology, and standardization on the horizon, it's clear we are at the tipping point for wireless to have a real impact in the industrial manufacturing sector.

Today's wireless applications and sensors deliver powerful new capabilities enabling end users to improve plant performance. Wireless solutions not only provide advanced sensing, but also help users make decisions positively impacting their overall business objectives.

The benefits of wireless technology 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.

Background

In some respects, the growth of wireless technology mirrors the environmental movement. Advocates of clean air standards and other "green" initiatives were once labeled a fringe movement. Businesses were reluctant to adopt forward-looking environmental strategies, choosing instead to support the status quo.

However, innovation frequently reflects societal changes and consumer demands—and this was exemplified by the Tesla Roadster, the first car produced by electric car firm Tesla Motors. Tesla claims prototypes have been able to accelerate from 0-60 mph (100 km/h) in about four seconds, and reach a top speed of over 130 mph (210 km/h). Additionally, the car will be able to travel more than 200 miles (322 km) on a single charge of its lithium-ion battery system.

Survival in a wireless world. Like the Tesla roadster, the time for wireless technology has come. It is no longer a question of "if" wireless will find a place in the industrial environment, but rather where and how it will be deployed. Wireless has already revolutionized IT networks in the front office, and the lines between business IT and the industrial world are now blurring.

The advent of industrial wireless networking presents tremendous opportunities, and risks to be considered and addressed, for automation and control suppliers. Process operators are looking for a secure, scalable, multi-functional wireless "cloud" for use in their facilities. They want to implement a universal network infrastructure supporting multiple industrial protocols and applications simultaneously, and providing a single wireless network that is easily managed and operated.

Suppliers who do not recognize the value of wireless for process monitoring and control, and fail to embrace it as part of their product offering, may find their business in jeopardy in the very near future.

Indispensable for modern communications. Over the last 20 years, wireless communications has been employed in a wide range of applications—including everything from satellite television and radio networks, to cell phones, laptop computers, and baby monitors. Wireless is even utilized for the guidance of unmanned aerial vehicles operated by the military, law enforcement, and weather forecasters.

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 or factory floor.

Current Situation

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

Benefits of wireless networks. 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.

In the industrial environment, a new generation of wireless field devices is intended for use in regulatory control loops and high speed monitoring applications. A modern 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 HMIs. Wireless technologies developed for building management and security can also be utilized in process plants to support both asset management and personnel tracking.



Security

The rapid adoption of wireless networks is testimony to the inherent benefits of this technology. Deploying a wireless environment is fundamentally easy, but meeting the requirements of your existing IT security policies, while minimizing business risk, is not. It can be done, but requires planning and a commitment to address a number of architectural, implementation, and operational issues.

Some critics look at the security challenges associated with wireless and believe organizations shouldn't be deploying it yet. These pundits miss the basic fact that organizations *are* deploying the technology anyway. Plus, WLANs are a stealth technology. Most IT departments in large organizations vastly underestimate the number of wireless nodes already installed by enterprising departments as well as individuals.

Reasons to take threats seriously. In the past, pranksters operating out of their basement were responsible for most attacks on networks. Times have changed, and enemy states, terrorist organizations, and even industry competitors now employ professional hackers.

Surprisingly, many large companies fail to recognize the importance of cyber security. Even government agencies such as the FBI, CIA and Department of Homeland Security often receive failing grades for protecting their data.

Without adequate security measures, wireless networks are just another avenue of intrusion for hacker groups seeking to obtain valuable information or do harm to your critical IT networks.

Specific Concerns

With the prevalence of mobile wireless devices and the increasing use of wireless-aware applications, enterprises need to continually track the threats they face and take steps to mitigate them.

Vulnerabilities exist in all networking systems. Threats to wireless networks can include:

- Traffic analysis and eavesdropping
- Rogue access points
- Denial of service
- MAC spoofing and session hijacking
- Remote control

Risks in your own backyard. Understanding the tools hackers use to penetrate security mechanisms is critical when it comes to designing secure wireless networks. Hackers are now beginning to use more sophisticated techniques, which make it harder for an intrusion detection system to detect an attack. Attackers also are increasingly using offline tools, which can reveal passwords quickly, to mount attacks against networks.

With wireless threats constantly evolving, it is mandatory to stay a step ahead to identify and help mitigate security issues before they affect your company.

Although wireless LAN security can seem daunting because of the publicity it has generated, most of the hurdles can be addressed by reasonable security precautions. Network designs will, of course, continue to be affected by the development of new technologies and user demands.

Companies lacking internal expertise in wireless security are advised to seek professional assistance from a qualified and experienced outside organization.



Future Outlook

Technological progress may soon relegate to the ashbin of history the bundles of cables that characterize plant floor machinery. Advancements in industrial wireless technology promise to open up a range of applications where cabling is either difficult to install, such as on offshore rigs, or prohibitively expensive. Wireless also offers the key advantage of integration of multiple devices, such as sensors, mobile PCs, and security systems

Among the first areas to benefit from industrial wireless technology were sensors and I/O. The idea: Get rid of the bulky network cables and wiring now needed to route sensor signals back to process controllers. Use instead modern wireless transmitters enabling automated monitoring in areas where hard-wired transmitters are too costly, difficult, or time-consuming to implement.

To keep up with wireless development activity and help users find the best solution for their unique application, several organizations are drafting recommendations or wireless standards as well as offering open solutions.

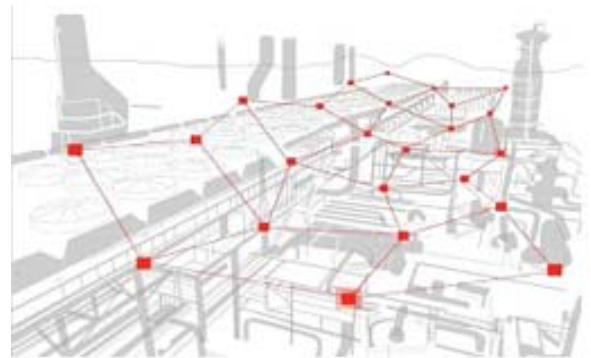
For example, the Instrumentation, Systems and Automation Society's (ISA) SP100 initiative, chartered in early 2005, is intended to create a roadmap for implementing wireless systems in the automation and control environment through defining and publishing a set of standards, recommended practices, and technical groups.

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

Universal, simple and efficient. For industrial end users, the wireless network must be universal (one network supporting multiple applications, using multiple protocols simultaneously, to serve the needs of multiple departments in the plant), simple (one system to learn, operate and maintain) and efficient (one platform enabling many applications with optimum bandwidth utilization and scalability).

The emerging industrial 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.

Mesh networks use a self-propagating, self-healing network of nodes to achieve blanket coverage of an area. Each node can communicate with any other node, so if one fails, the network can re-route data and connectivity is not lost.



Advanced wireless network solutions will also optimize performance with efficient use of ISM bandwidth and prioritizing messages so critical information is received first. Thanks to a high-speed and self-organizing mesh network, users achieve flexible channel allocation and a robust architecture with latency control and redundancy for safe wireless control. In addition, wireless signal interference can be avoided 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.

Best Practices

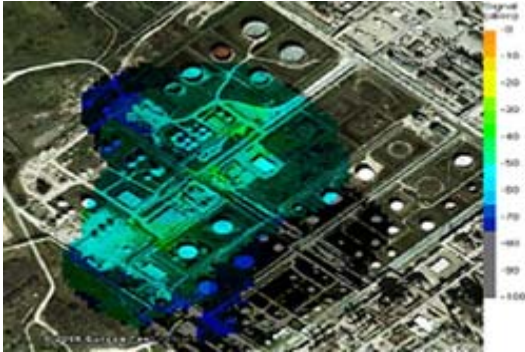
Today's proprietary, wireless-enabled solutions tactically solve many industrial business needs, but may not meet your requirements for the future. Furthermore, proprietary solutions often suffer from single-vendor dependence, unproven security measurements, limited device availability, and interference with other wireless systems such as 802.11.

When implementing a wireless strategy, key implementation issues that must be addressed include:

- Handling multiple types of devices, from just a few to thousands
- Operating in noisy radio frequency environments
- Sending data reliably and when needed
- Ensuring predictable power management and security

Learn the lay of the land. While there are inherent security challenges with the IEC 802.11 technology, there are also many straightforward measures that can be taken to mitigate them. As with many new technologies, the best way to get started is to recognize the problems and make a commitment to address the ones that can reasonably be solved in your environment.

No matter what type of wireless system is used, it is important to carefully assess your site requirements and to design the network with current and future needs in mind. A wireless assessment & design study is recommended for any wireless installation. Each plant has different needs and limitations, and deployment of wireless technology should consider the unique way in which you operate.



The wireless assessment & design study provides a comprehensive plan for implementing a fully scalable wireless infrastructure supporting multiple applications within your enterprise. The study answers the following questions:

- Will network performance be impacted when scaling?
- Is the network secure?
- Will interference be an issue?
- How much infrastructure do we really need?

Do your homework before forging ahead. Typically, businesses need a strong economic justification before embarking on a wireless installation. Wireless projects will gain management support if there is a clear demonstration of opportunities to reduce costs, increase efficiencies, manage risks, and ensure safety.

Additional advice for process operators installing wireless systems:

- Work with your IT department from the start of a wireless project
- Don't choose a wireless solution and "throw it in the laps" of your IT personnel.
- Close cooperation with your IT department will help ensure a successful outcome.

Choosing A Supplier

Rarely can a single supplier meet both plant and office IT requirements. Instead, select a supplier with proven expertise in wireless applications found in the industrial environment, and offers a broad product portfolio and user support capability.

Your supplier-of-choice must have the experience necessary to adequately address wireless 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.

Supplier selection checklist. Key factors to consider when choosing a wireless technology supplier include:

- Comprehensive and end-to-end industrial 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 you 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 industrial wireless network to the company's business IT network?

Conclusion

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 the risks—and rewards—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-mealed” 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.

More Information

For more information on 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: +1-602-313-6665 or 877-466-3993

www.honeywell.com/ps

WP-08-12-ENG

May 2008

© 2008 Honeywell International Inc.

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