Cisco Secure Wireless Plant Solution: Wi-Fi-Based Sensor Networking for Industrial Environments

Today’s process industries rely increasingly on information gained from networks of sensors installed at essential points throughout the factory or field site. Measurement of air pressure, electrical current, weight load, fuel levels, temperature, corrosion, pipe flow, seismic activity, such readings are critical to the effective, efficient, and safe operation of oil pipelines and refineries, pharmaceutical and chemical companies, food and beverage manufacturers, and power plants.

The evolution of sensor technologies has enabled managers and administrators to gain more visibility into complex processes. For example, the introduction of microprocessors and digital communications led to distributed control systems (DCSs) and the migration of intelligence into field devices, which allowed enterprises to improve operations significantly. However, process industries continue to face the immense challenges of global competition. These include:

- Improving resource use
- Increasing operating efficiency
- Optimizing maintenance and plant shutdown
- Improving site safety
- Increasing environmental responsibility and compliance
- Creating a responsive and dynamic operating environment
- Managing mobile plant operations and maintaining visibility throughout the product cycle
- Extending knowledge management
- Improving asset surveillance and security

To meet these challenges and to boost performance, process industries are increasingly adopting the proven technology of wireless networks, or Wi-Fi. The use of Wi-Fi for Internet connectivity has become very familiar in business enterprises, educational institutions, and cities: campus-wide networking, municipal wireless mesh networks, Wi-Fi–based telephony, and the use of mobile information-gathering devices and applications are commonplace. Process companies are now using this secure, powerful technology to network multiple plant and field sensors and to support the ability to examine, analyze, and act on real-time sensor information.

Cisco® offers the industry’s first open standards-based Secure Wireless Plant Solution for process industry applications. By integrating sensor data into a highly secure network and transforming it to intelligence throughout the plant, managers can improve safety, compliance, and asset reliability while helping to ensure confidentiality. Using Cisco’s industry-leading networks, this robust solution unites process-monitoring capabilities, developed with partner Emerson Process Management, with an array of business capabilities, including IP-based telephony, asset maintenance and tracking, and video surveillance. Plant and field managers can use Cisco solutions to streamline operations while they gain more cost-effective, reliable information gathering to enhance business processes.
Why Rely on Wireless?

Process industry managers are only too familiar with the complexities of wired sensor networks. They are expensive to install and maintain, and they require special signal wiring, cabling into automation systems, and tracking of multiple sensor readings using separate software systems. What’s more, changing or reconfiguring the physical plant can require managers to do major reworking of sensor systems, at a high cost and with significant impact on the entire site.

Wireless networking, however, represents a major reduction in capital expenditure, in some cases costing only one-tenth of the cost of wired networks. Wireless systems rely on meshes of access points, small, unobtrusive ceiling- or wall-mounted transmitting/receiving stations, that can be moved easily to accommodate changing physical environments. With a wireless network, companies don’t need signal wiring or conduit installations. If plant systems are reconfigured or new pipes or equipment is installed, the wireless sensor network can be scaled to the new needs quickly and easily, at a minimal cost compared to the redeployment of wired sensors.

By being able to install more sensors more easily, enterprises gain a richer understanding of their processes, as well as additional coverage if primary sensors fail. With better information, personnel can make more reliable diagnostics and improve processes. Wireless sensors can even be placed temporarily and monitored on an ad hoc basis to assist in troubleshooting or when field operatives need to test or experiment with equipment.

Wireless systems increase efficiency another way: They make it possible to record and respond to measurements that were previously infeasible to obtain, such as the emissions at the tops of high stacks, towers, or tanks; or conditions over long distances such as from platforms or pump houses; in areas with large common-mode voltage differences; over water; on operating machinery; or in extreme environmental conditions.

Investing in Open-Standard Wireless Networking

Some industry managers and executives believe that a proprietary system is the best way to ensure wireless reliability and security. Indeed, due to the rapid rate of development, they may find themselves confronted with a proliferation of proprietary wireless sensor solutions. However, the road to today’s ubiquitous wireless technology is littered with the remains of companies that have tried to develop and rely on proprietary standards. The proprietary approach has failed, and the customers who purchased those technologies have lost their investment.

Process industries have a need for flexibility, openness, mobility, reliability, and availability. As such, they can achieve the best return on their investment by implementing systems that support the IEEE standards used in all major wireless solutions, including 802.11 and 802.16. It is also important that systems interoperate with the primary emerging wireless sensor protocols, such as IEEE 802.15.4 (sold under the commercial name ZigBee). A low-data rate, low-power, low-cost wireless networking protocol, ZigBee is targeted toward automation and remote sensor I/O control applications. It is expected to provide low-cost and low-power connectivity for equipment that needs battery life for as long as several years, but does not require data transfer rates as high as those enabled by Bluetooth.
ZigBee can also be implemented in large mesh networks (such as the Cisco® Unified Wireless Network and Cisco Outdoor Wireless Network solutions). ZigBee-compliant wireless devices can transmit from 10 to 75 meters, depending on the environment and the power output consumption required for a given application, and they operate in the unlicensed RF worldwide (2.4 GHz global, 915 MHz Americas, or 868 MHz Europe). The data rate is 250 kbps at 2.4 GHz, 40 kbps at 915 MHz, and 20 kbps at 868 MHz.

Connecting only the process systems within a company provides benefits up to a point. But capitalizing on open standards can propel innovation and create alliances that allow businesses to take advantage of new opportunities and become truly competitive in today’s global business environment. Industry organizations can now use wireless systems that not only monitor and report on sensor networks, but also provide a solid foundation of networking capabilities combined with security, scalability, resiliency, and manageability throughout the company.

The Cisco Secure Wireless Plant Solution

The Cisco Secure Wireless Plant solution integrates isolated systems of sensory data and manages them as a converged network, while providing a platform for a wide variety of other business capabilities, including:

- Enhanced worker MRO processes and workflow automation
- Extended communications
- Integrated process automation (supervisory control and data acquisition, DCS, PLC, condition monitoring, sensing, and control)
- Integrated industrial wireless and emerging wireless sensor networks
- Personnel and asset tracking and tracing
- Real-time management, monitoring, and alerts on environmental operating conditions
- Improved HSE management (via real-time telemetry and location services)
- Increased asset security (via integrated video surveillance and video intelligence)
- Drive knowledge centers for excellence for remote diagnostic and inspection services
- Collaboration across boundaries and the extension of operating expertise virtually anywhere, anytime

By relying on Cisco’s converged networks, major organizations in a variety of industries have experienced significant cost savings and improved productivity. The Secure Wireless Plant solution is founded upon the proven Cisco Unified Wireless Network, which combines wireless and wired networking to deliver highly secure, scalable WLANs with a low total cost of ownership (see Figure 1).

The network receives sensor data via Cisco Aironet® 1520 Series Lightweight Outdoor Mesh Access Points, which support dual-band radios compliant with IEEE 802.11a and 802.11b/g standards. Simple to deploy and operate, this solution is based on intelligent wireless routing technology and a powerful, self-organizing, self-healing, and self-configuring architecture. Once implemented, the solution dynamically responds to varying conditions, providing optimal route selection in the event of failures and environmental changes.
Because the access points are based on open standards and protocols, they provide a universal infrastructure for all the wireless applications in the plant or field area, including security, personnel and asset tracking, and mobile worker productivity solutions. A combination of pretested and validated backhaul technologies, including Wi-Fi bridging, WiMAX, and satellite connectivity, are also available.

**Figure 1.** The Cisco Sensor Network Architecture
The Cisco Wireless Control System (WCS) software manages the network, supported by Cisco Secure Services for network security. WCS is the industry's leading platform for wireless LAN planning, configuration, management, and mobility services. With it, administrators can manage routing, segregation, and prioritization of wireless data, as well as the security infrastructure for data transmission and access. This provides a cohesive wireless communications platform across the physical and functional areas of plant operations, so that the shared network can support diverse applications with the necessary security, policy, and performance management.

Network managers need to provide end users with freedom and mobility while they help to ensure the integrity of corporate information and systems, and achieve regulatory compliance. The solution is based on the Cisco Self-Defending Network, which provides a business-ready, standards-based architecture, including:

- Consistent, reliable, and secure mobile networking
- Mitigation of sophisticated passive and active WLAN attacks
- Wireless device host intrusion prevention and an integrated authentication framework
- Interoperability with a wide range of client devices
- Reliable, scalable, centralized security management
- Support for Wi-Fi Protected Access (WPA) and WPA2 security standards for robust authentication and data encryption

Using the Cisco Secure Wireless Plant solution, process industry managers can be confident that sensor data is reliably and consistently collected, managed, and integrated with corporate data and functionalities without loss of information, confidentiality, or performance.

Understanding the Benefits of the Cisco Secure Wireless Plant Solution

Cisco has been the industry leader in networking solutions for the past 20 years, offering powerful, award-winning solutions across a variety of industries. With the Cisco Secure Wireless Plant solution, Cisco has added another essential offering to its suite of technologies designed for process industry organizations.

By relying on this solution, managers can optimize plant productivity, achieve regulatory and industrial compliance, and enhance asset reliability, all while they decrease costs. Cisco wireless sensor networks can be used where wired connections are infeasible, not just matching but actually improving sensor coverage. This allows timely and appropriate response to threats and incidents, which increases safety for personnel and the surrounding environment. Real-time sensor information is also extended securely to corporate staff supervising the production environment, facilitating a new level of information gathering and analysis to improve production processes.

As a result, businesses can implement a wide variety of applications within their operations. Automated data gathering through sensors can replace “clipboard rounds,” resulting in more accurate 24-hour monitoring of equipment, conditions, and devices. Workers can access desktop applications and perform tasks from wherever they happen to be, including viewing and responding to alarms from the field. Equipment and human assets can be tracked at all times to help ensure their safety and to prevent loss. Physical security can be improved with networked surveillance systems that patrol not only the fence line, but also product processing.
Many of these applications are possible today without wireless technologies, but wiring costs and technical limitations have made them impractical. Cost-effective and easy-to-integrate wireless technology overcomes these barriers, providing better visibility into the plant and making the workforce more productive.

**To Learn More**

The Cisco Secure Wireless Plant solution provides a powerful networking capability for process industries. By working with Cisco, your firm can take advantage of these powerful functionalities, helping your company to reach new levels of productivity and achieve greater competitiveness. To learn more about this solution, go to [http://www.cisco.com/go/manufacturing](http://www.cisco.com/go/manufacturing) or contact your Cisco representative.