

Cisco Secure Wireless Plant Solution: Wireless Sensor Networking for Industrial Environments

Today's process industries have increasingly come to rely on information gained from networks of sensors installed at key points through 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 and efficient 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 insight 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, allowing enterprises to improve operations significantly. However, process industries continue to face the immense challenges of global competition. These include the need for:

- Improved resource utilization
- Improved operating efficiency
- Optimized maintenance and plant shutdown
- Improved site safety
- Environmentally responsibility and compliance
- Responsive and dynamic operating environment
- Mobile plant operations and visibility throughout the product cycle
- Extended knowledge management
- Improved asset surveillance and security

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

Cisco® offers the industry's foremost open standards-based Secure Wireless Plant solution for process industry applications. By securely transporting sensor data and transforming it to intelligence throughout the plant, managers can improve safety, compliance, and asset reliability while assuring confidentiality. Using industry-leading Cisco networks, this robust solution unites process-monitoring capabilities with an array of business capabilities including IP-based telephony, asset maintenance and tracking, and video surveillance. Plant and field managers can utilize Cisco solutions to simplify operations while gaining more cost-effective, reliable information gathering that enhances business processes.

Why Wireless for Sensor Networks?

Process industry managers are only too familiar with the complexities of wired sensor networks. They are expensive to install and maintain, requiring special signal wiring, cabling into automation systems, and tracking of multiple sensor readings using multiple software systems. Furthermore, changes to or reconfigurations of the physical environment can require major reworking of sensor systems, at a high cost and with significant impact on the entire site.

Wireless networking, on the other hand, represents a major reduction in capital expenditure, in some cases costing one tenth of wired sensor networks. Wireless sensor systems use self-organizing mesh technology that is tried and tested in the field, and the basis for the WirelessHART standard. Each wireless device in a self-organizing network can act as a router for other nearby devices, passing messages along until they reach their destination.

This capability provides redundant communication paths and better reliability than solutions that require direct, line-of-site communication between each device and its gateway. Whenever there is a change in the network or in conditions that affect communications, the devices and gateways in the self-organizing network work together to find and use the most efficient path for each message – a path that optimizes data reliability while minimizing power consumption.

Another advantage of self-organizing networks is that they are dynamic. As new obstacles are encountered in a plant, such as scaffolding, new equipment, or moving vehicles, the networks can reorganize around them. All of this happens automatically, without any intervention by the user.

These self-organizing networks use IEEE 802.15.4 radios with channel hopping as the physical layer. They are designed and tested to be tolerant to almost all interference and can coexist with other wireless networks in your plant. Robust security is provided through advanced standards-based encryption as well as authentication, verification, key management, and anti-jamming techniques. The networks are also highly scalable and capable of 1-second scanning with low latency.

Wireless devices based on this technology have been proven in use to demonstrate greater than 99.9 percent data reliability.

By being able to install more sensors more easily, enterprises gain a richer understanding of their own processes, as well as additional coverage when primary sensors fail. Based on better information, diagnostics are more reliable and result in more process improvements. Wireless sensors can be temporarily placed and monitored as needed, to assist in troubleshooting or when field operatives need to test or experiment with equipment.

Wireless systems increase efficiency by making it possible to record and take action on previously infeasible measurements, such as monitoring emissions at the tops of high stacks, towers, or tanks; at 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

It may seem natural for some industry managers and executives to believe that a proprietary system must be the best way of assuring 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 – and

this approach has failed. Unfortunately, the customers who purchased these technologies have also lost their investment.

Process industries' need for flexibility, openness, mobility, reliability, and availability assures that the best return on investment is achieved using systems that support the IEEE standards utilized in all major wireless solutions, including 802.11 and 802.16. It is also important to interoperate with the key emerging wireless sensor protocols such as IEEE 802.15.4, a low-data-rate, low-power, low-cost wireless networking protocol 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 months to several years, but does not require data transfer rates as high as those enabled by Bluetooth.

Process Management organizations can now utilize 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 disparate islands of sensory data and manages them as a complete network, while providing a platform for a wide variety of other business capabilities, including:

- Enhance worker MRO processes and workflow automation
- Extend communications
- Integrate process automation (condition monitoring, sensing, and control)
- Integrate industrial wireless and emerging wireless sensor networks
- Track and trace human and capitalized assets
- Manage, monitor, and alert on environmental operating conditions in real time
- Improve HSE management (using real-time telemetry and location services)
- Secure assets (using integrated video surveillance and video intelligence)
- Enable knowledge centers for excellence for remote diagnostic and inspection services
- Collaborate across boundaries and extend operating expertise virtually anywhere, anytime

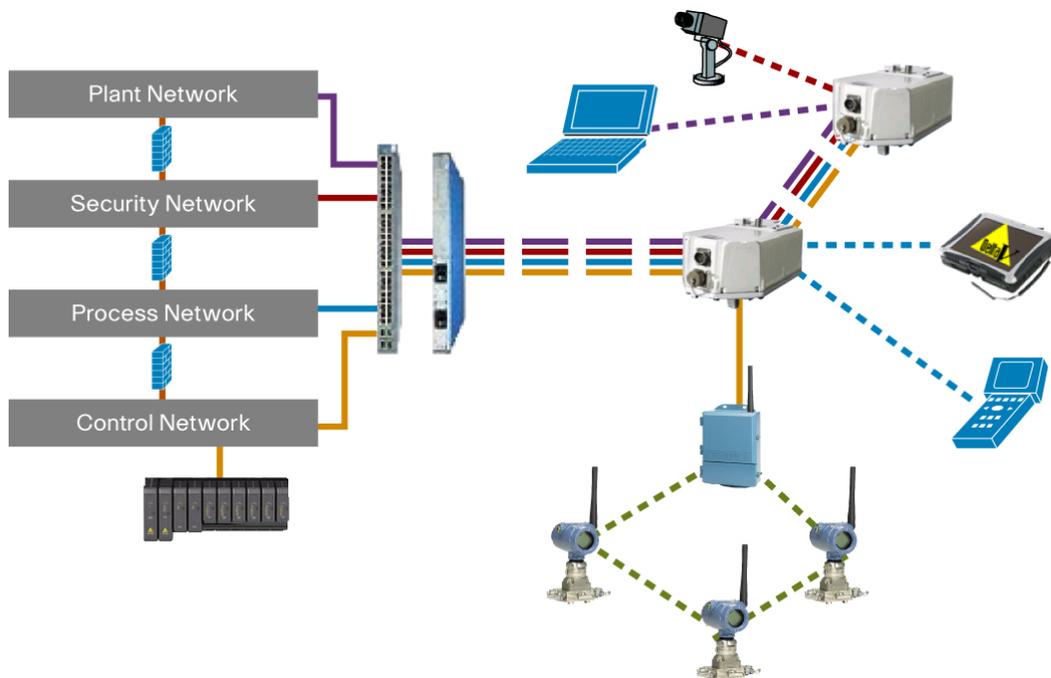
By relying on converged Cisco networks, major organizations across a variety of industries have experienced significant cost savings and improved productivity based on this pervasive network technology. The Secure Wireless Plant solution is founded upon the proven Cisco Unified Wireless Network, which combines wireless and wired networking to deliver secure, scalable, wireless LANs with a low total cost of ownership. (See Figure 1.)

Sensor data is sent to the network using the Cisco Aironet® 1520 Series Outdoor Mesh Access Points, which are Class I, Div. 2, certified and 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 access points dynamically respond to varying use 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 pre-tested and

validated backhaul technologies, including Wi-Fi bridging, WiMAX, and satellite connectivity, are also available.

Figure 1. The Cisco Sensor Network Architecture



The network is managed by the Cisco Wireless Control System (WCS) software, supported by Cisco Secure Services for network security. Cisco WCS is the industry's leading platform for wireless LAN (WLAN) planning, configuration, management, and mobility services. It enables administrators to 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 as well as the 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 achieve regulatory compliance, provide end users with freedom and mobility, and ensure the integrity of corporate information and systems. Cisco's industrial wireless solution is based on its 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

Process industry managers can rest assured that with the Cisco Secure Wireless Plant solution, 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 led the networking field 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 key offering to its suite of technologies designed for process industry organizations.

By relying on this solution, managers optimize plant productivity while achieving regulatory and industrial compliance and enhancing asset reliability – all while lowering costs. Cisco sensor networks can be used where wired connections are infeasible, not only matching but 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, enabling a new level of information-gathering and analysis to improve production processes.

As a result, a wide variety of applications can be enabled within the business operation. Automated data gathering through sensors replaces manual rounds to collect data from devices, resulting in more accurate 24-hour monitoring of equipment, conditions, and devices. Workers 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 are tracked at all times to maintain their safety and to prevent loss. Physical security is improved with networked surveillance systems that not only patrol the facility, but product processing as well.

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 insight 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, elevating your company to new levels of productivity and achieving greater competitiveness. To learn more about this solution, please visit <http://www.cisco.com/web/strategy/manufacturing/secure-wireless-plant.html> or contact your Cisco representative.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)