

## Managing Wireless Networks for Secure Enterprise Control

### **WHAT'S INSIDE:**

---

1. Overview
  2. Managing Business Results
  3. Managing Secure Integration
  4. Managing System Policy
  5. Managing the System Architecture
  6. Managing System Traffic
  7. Managing System Growth
  8. The Invensys/Apprion Solution
-

## 1. OVERVIEW

The radio spectrum available to every enterprise is a communications asset to be carefully exploited. The good news is that the emergence of secure, affordable wireless technology is making it easier to implement wireless solutions every day. Wireless technologies include communications hardware and software such as wireless access points, transmitters, receivers, antenna, protocols, powering options and servers and security technology ranging from intrusion detection devices to data encryption. Making the most effective use of any of these technologies requires resource planning, performance management, and a common wireless systems management platform.

Unlike wired networks, which are virtually as expandable as budget permits, each enterprise is endowed with only a finite amount of radio bandwidth and this must be shared across multiple departments; departments that may have had little need to coordinate activity in the past. Also, unlike wired networks where access can be restricted physically, wireless frequencies are accessible with even the most rudimentary wireless communications devices. This finite, relatively available resource means that today—and for likely many years to come—reaping the many control benefits of wireless communications will be a challenge of technology management much more so than technology performance.

The consequences of unmanaged wireless proliferation are already becoming evident. Anxious to capitalize on the growing interest in wireless networks, vendors are quickly adding wireless products to their portfolio by replacing wires with transceivers. End users are buying these 'point solutions' and, most often, are initially enjoying immediate success. When the first wireless solution from one vendor works well, they buy a different wireless point solution from a different vendor and hope to enjoy the same success. But as this scenario plays out in different departments and in different company locations, the joys of wireless freedom begin to fade. Users may begin experiencing increased interference on the links. Transmission may be interrupted. There may be availability problems, data loss and performance degradation. Furthermore, this ad hoc approach fails to consider the varying criticality and time-sensitive aspects of disparate application data that are contending for use of the spectrum.

These are the symptoms of a wireless infrastructure that has evolved in an ad hoc fashion. The technology that potentially offers a way to improve productivity, and efficiency as well as cut costs, can also add uncertainty, cost and vulnerability if it is not implemented without a focus on systems management.

Although many of the same principles of wired network systems management apply also to wireless networks, the fact that the radio spectrum is both finite and generally publicly accessible adds new and unique challenges to wireless network systems management. Where enterprise-level management has been considered good practice for wired networks, it is increasingly becoming critical for the operation of wireless networks.

Enterprise-level wireless systems management requires attention to the following areas that are described in the detail sections of this paper:

- ♦ Managing business results
- ♦ Managing secure integration
- ♦ Managing system policy
- ♦ Managing the system architecture
- ♦ Managing system traffic
- ♦ Managing system growth

## 2. MANAGING BUSINESS RESULTS

Fundamentally, wireless networks deliver the same basic business benefits as wired networks. They connect data point A to data point B, enabling timely information sharing for a wide range of application and reporting functions. But because of the low cost of wireless sensors, and the minimal cost of running wires, more points can be connected far more cost effectively than in wired networks, raising the possibility of enabling a more detailed measure of process variables, including new strategic measurements that were impossible to achieve previously. Freed from the restrictions of wires, it is possible to set up measures for virtually any point of the enterprise and receive this information in real-time.

Because of the finite amount of radio spectra at a company's disposal, care must be taken up front to determine where the technology will be most beneficial. Following are typical wireless solutions for the process manufacturer that is:

- ♦ Looking to improve equipment availability and reduce maintenance costs through proactive condition monitoring, for example, implementing wireless vibration sensors to indicate system malfunctions
- ♦ Seeking to improve utilization of process equipment through more precise measurements of process variables such as temperature and pressure
- ♦ Seeking to eliminate wiring related costs in upgrading or installing control systems
- ♦ Seeking real-time monitoring of parts and finished goods, across the entire value chain
- ♦ Looking to monitor activity at more checkpoints, throughout the enterprise or in remote locations
- ♦ Addressing proactively the developing requirements for improved plant safety and security through perimeter monitoring, weapons of mass destruction detection, and personnel tracking

---

## TECHNOLOGY UPDATE:

### Managing Wireless Networks

Although it is quite possible that each department will present a strong business case for using wireless networks in its own operation, the finite nature of the bandwidth makes it imperative that these considerations be made at the enterprise level. Whether process, security or logistics needs are more important to the enterprise, is a question that can best be evaluated in the context of the overall enterprise strategy.

A company competing in a mature marketplace on a strategy of being the low-cost provider, for example, might deploy wireless vibration sensors that tell when any asset is not operating optimally, and, subsequently, will see maintenance savings immediately on the bottom line. In contrast, a company competing on fast, reliable delivery might find that adding an RFID product tracking system would improve its competitive position.

### 3. MANAGING SECURE INTEGRATION

The greatest threats to wireless security are not from malicious interference – for example, intruders who might use sophisticated equipment to surreptitiously behave like a temperature transmitter. Instead, the threats are most commonly from otherwise well-intentioned people engaged in sloppy networking practices, such as not changing passwords according to policy, using obvious passwords such as initials, adding or deleting devices improperly, and any number of other lapses. Wireless networks are, of course, subject to interference from non-malicious factors, such as environmental or accidental RF noise, broken RF equipment, dynamic changes in the characterization of the RF site, and the range of non-compatible RF devices generally available. Prevention of these kinds of problems must be engineered into the network from its inception, and must be covered by an enterprise-aware security and management model.

One network user might be taking wireless process measurements from a temperature transmitter. Another person in the same plant might be running a wireless video camera for perimeter security. A third might be running an RFID inventory tracking application. Because they are in different departments and locations and doing different things on different protocols, they might think they are isolated, but, in reality, those radio waves are co-mingling, which creates tremendous potential for performance problems and mismanagement.

Coordination of these diverse needs is critical, but not likely to emerge by consensus. If each department wanting to deploy a wireless solution had to check with every other department to see how their wireless activity would impact them, there would be gridlock. There must be a higher-level framework that respects the tasks that people need to do to

perform their roles and responsibilities, in the context of the business strategy and related job responsibilities. At the same time, users must have assurance that if they do select technologies and practices that conform to company policy, they will enjoy reliable, secure, network operation.

#### 4. MANAGING SYSTEM POLICY

Policies must define all methods for using, sharing and securing the available bandwidth. This has implications for planning, implementation, operation, maintenance and expansion. For these reasons, wireless networks require a very thoughtful level of construction, but just the opposite is happening today.

Policy management also ties into end users' existing IT requirements. Therefore, one company might have IT policies in place that are very different from another in exactly the same industry. The system must be designed to comply with corporate requirements for activities like reporting errors, observing network behaviors, and optimization based on that information. It must cover every aspect of operation, from initial configuration to ongoing optimization.

Performance, availability and utilization are critical parameters that need to be monitored and reported upon within systems management. Monitoring these parameters is required as part of ongoing diagnostic-driving policies, device policies and alarm alert handling... all part of the systems management function.

Policies define how problems will be handled. For example, when the system detects interference, what does it do? Will it reroute traffic, change frequencies, or reconfigure antennas to be active or inactive? Some of the options depend on the capabilities of the technology, but within that framework, policies are necessary to guide choices.

#### 5. MANAGING THE SYSTEM ARCHITECTURE

Optimal execution of any enterprise-wide policy requires a network architecture that can accommodate technology of every possible network vendor, emerging standards and best wireless integration practices. The architecture must be based on a secure model covering authentication and role-based access control. This should provide for common addressing, routing, messaging and device management. It should also provide consistent data structures, storage and reporting, and a common point of configuration for all business rules and workflow.

#### 6. MANAGING SYSTEM TRAFFIC

Unlike wired networks, which can be fairly well isolated, closed by function or protocol and kept independent of other networks, wireless signals cannot be managed physically. Wireless traffic is controlled by agreements and rules, requiring buy-in from everyone who has access to the bandwidth spectrum.

---

## TECHNOLOGY UPDATE:

### Managing Wireless Networks

The data may travel down the same virtual wire or air link, but would not necessarily have to be interspersed with like data. A process packet and an IP packet would not necessarily have to be on the same link. Instead, rules could limit access to process data to users on the process side of the house or transmit data to receivers only on that side. A company has the ability to set policy to determine where the data/signal should go and who has access.

One key to flexible, secure operation is the ability to validate any packet of information moving across the network with a recognized and authorized sender or receiver. This type of identity management can be done in a number of ways including certificates and tokens. Both can authenticate devices with a unique identifier. Management must determine how those certificates are assigned and distributed, how they are evaluated, and what privileges that ID would have as it moves through the system. They must also define exactly how to treat an entity as an object with its own unique properties or attributes. It is a better way of assigning an ID than as an IP or media access MAP address. The token is the unique identifier that then allows you to assign attributes to that object. This is a well-understood technology, but its effectiveness decreases significantly without enterprise-wide coordination of wireless applications.

Every vendor of wireless devices provides a software package that is used to configure, deploy and manage their devices. While this software works for the vendors devices, it has no ability to manage or coordinate other vendors wireless devices deployed in the enterprise. When there are the inevitable problems of coexistence, this software has limited value. Although each may include a troubleshooting guide, many troubleshooting paths likely point to some unknown device on the network, each of which is likely to point to another unknown device. From both technical and practicable standpoints, you need a single point of access to the whole network of networks, using a common network and a common lexicon.

## 7. MANAGING SYSTEM GROWTH

At some point, from a network management perspective, no one would care if the network is wired or wireless. Your network management center would treat it as another network and the focus would be on managing communications, not technology. But we are far from that point today. In any company, for example, you might find the IT organization managing both the IT network and the telephone, but they are managed as completely different systems. Only recently have we begun to see the two technologies blending in voice over IP systems, have raised the need for integrated management of these technologies. But this has been years in the making and has many growth years yet to come.

Wireless technology is clearly in a transitional phase, but we know there will never be a single wireless protocol and frequency that is exclusively used. Protocols and frequencies will be optimized based on applications. The requirements for power management, distance, site characteristics, bandwidth, cost and security will always result in the need for a wide range of technologies.

What is needed is an integrated yet flexible management strategy that can deliver benefits today, but can be adapted as businesses and technologies change. Following is a check list of the steps that process manufacturers can follow to take full advantage of wireless technology today and tomorrow:

- ♦ Survey your entire company to determine where wireless technologies can best support your business strategy
- ♦ Design architecture that will achieve these goals most effectively
- ♦ Select and purchase hardware and software that is cost-effective, proven, and scalable
- ♦ Implement the solution seamlessly
- ♦ Conduct ongoing maintenance, support and optimization services

Few companies have the resources to maintain staff necessary for all of these steps, especially because demand for specialists with relevant skills is very high. As such, outsourcing to one of the emerging specialist firms is currently the most cost-effective strategy for companies that want to enjoy the benefits of wireless networking most immediately with the least risk.

## 8. THE INVENSYS/APPRION SOLUTION FOR WIRELESS SYSTEM MANAGEMENT

Thanks to standards and innovation, wireless technologies offer a compelling mix of cost and performance that will cause adoption in various areas of the enterprise. In order to move beyond experimentation, toward a future where wireless could be used in control applications, there must be an overarching framework to accommodate and apply multiple wireless technologies. Since there is great heterogeneity to the applications and no “one size fits all” solution with regard to the technology, it is important that the necessary monitoring, management and security span the entire wireless enterprise to ensure the most efficient use of the limited resource while, at the same time, allowing disparate applications to share the spectrum within the context of their importance, time sensitivity and mission criticality.

Like the networks themselves, such a system must be evolving, dynamic and flexible. Since building, and even operating, this type of a management framework is beyond the means of most users, Invensys has undertaken this challenge with its wireless networking initiative. Together with its partner Aprion, Invensys is offering its customers both a wireless infrastructure management platform as well as a technology lifecycle program to

---

## TECHNOLOGY UPDATE:

### Managing Wireless Networks

provide a roadmap and best practices for an iterative expansion of wireless technology throughout a plant, facility or department. Through its unique set of engineering and managed services offerings, Invensys is allowing customers to focus on outcomes and objectives, while providing a cost-effective method for acquiring and integrating the vast array of wireless-enabled products and devices that are increasingly coming to market.

This is a very exciting time for manufacturers looking to implement wireless solutions. We are at the threshold of technology enabling game changing applications that will drive increasing bottom and top line profits and efficiencies. This is not a time to stand on the sidelines and wait for “things to settle down”. They will not settle down for years in wireless, while valuable applications and solutions are available now. The key is managing these point solutions. Expert management of the security, systems, and network requirements will allow these varied technologies to succeed in an industrial environment.

**For more information about Invensys’  
Wireless solutions, contact:**

**Greg Burns**  
**1.978.241.1020 – Office**  
**1.978.350.4051 - Cell**  
**[greg.burns@ips.invensys.com](mailto:greg.burns@ips.invensys.com)**

**Invensys®**