Wireless is More Than Field Devices and WiFi and You Have to Manage the Many Networks Coming Into Your Plant

A Guide to Managing Industrial Wireless Networks

Wireless is More Than Field Devices and WiFi and You Have to Manage the Many Networks Coming Into Your Plant
The last 10 years have seen a major expansion of the use of wireless data technology in every aspect of life, and in every industrial venue. From the ubiquitous cell phone to smart phones, tablets and more, wireless data communications have become an important, perhaps the most important, medium. In the last half dozen years, wireless field devices have begun penetrating the industrial environment, too. IT and plant floor communications managers are faced with a daunting task in coordinating all the uses of wireless in the average 21st century plant.

As more and more wireless devices and applications become an integral part of the industrial arena landscape, concern grows over what layer of the network these wireless devices should be placed. This question concerns everyone since this is sure to impact plant or plant operation in the near future.

We typically see two physical networks. The Process Control Network (PCN) involves Layers 2 and below. The Business Network (BN) involves Layer 4 of the Purdue model. If you are part of a plant team that supports either of these networks, the discussions within this paper have been or will be part of an ongoing discussion for your organization.

We’ve seen a number of major companies make an attempt to stake out where wireless devices will fall and under what level of the network. This paper addresses these types of issues and is intended to provide answers to the many questions that are sure to arise.
Layers 1, 2, and 3 are commonly referred to as the Process Control Network (PCN). It is the PCN where Distribution Control System (DCS), PLC, and field devices reside. This has always been seen as the “Holy of Holies” with access into this layer as sacred, as it should be. The PCN is an extremely time-sensitive network where communication to field devices and control consoles must not be impacted. This is also where other time-critical devices are located.

The PCN layer requires careful planning to ensure that up-to-date patches, firmware, new releases, and comprehensive testing of these changes occur with no outages to the network. This layer usually falls under the Process Safety Management processes and must adhere to strict change control processes that may impact existing systems. The PCN is considered a 24/7 network and no outages are allowed without planning and these are usually rare.

This seems like a logical area where most of the wireless sensor devices would connect to the network. These types of networks are still considered point-to-point solutions since they are normally their own wireless network using protocols such as WirelessHART®, ZigBee®, or other proprietary protocols. They may deploy Mesh network technology but perform a single function and are usually tied back to the PCN via a gateway device. There is very little impact that these devices have on the network as long as the support staff monitors and maintains the devices. However, these devices will require firmware updates as new releases are deployed and as you deploy multi-vendor solutions, additional risks increase and you increase the number of application servers/workstations that are required to monitor and maintain these systems. As you increase the island of point-to-point applications, risks in this physical layer increase.

Now consider the addition of applications such as smartphones, tablets, and handheld communicators running on VoIP technology that allow outside operators and/or maintenance personnel to perform rounds, create work orders, add wireless process video cameras, or implement VoIP communication that can reduce operating costs for your plant. We now move from the point-to-point wireless applications to typical 802.11 (WiFi) and/or 802.16 (WiMax) wireless networks. We just entered the forbidden layer and know that these applications may require Layer 4 or Business System access which imposes risk such as traffic congestion, security risks, and so on to our PCN layers.
The security policy for most PCNs restricts data from outside the PCN firewall, thus restricting the use of the applications listed above. Some companies believe that you should restrict 802.11 from the PCN network due to security risk. However, it is believed that the network physical layers pose just as much risk as a well designed wireless network.

A possible solution being used by some companies is the deployment of two devices at the same location for PCN and BN when deploying 802.11 WiFi devices. This approach allows the separation of the data but increases the complexity of your wireless spectrum, determining rogue devices, clients, and so on. Further, this does not even address the increased maintenance and installation costs.

As corporations implement security policies, deploying and monitoring devices provides a unique challenge if the devices are deployed under the PCN and the same type of monitoring is deployed for Layer 4 devices. A new physical layer may have to be created for the support team in order to monitor both layers of wireless device systems. Most control vendors provide this type of solution under the PCN layers. But what if your knowledgebase for these types of wireless devices are part of your local IT team?

Layer 4 (BN)
This layer is commonly referred to as the Business Network, Plant Network, or the IT Network at industrial facilities. This physical network is either maintained remotely or by a local IT team. Devices attached to this network layer must follow certain security and operating patch policies which require almost constant updates and upgrades to maintain reliability and a secure network.

This layer may contain multiple Virtual Local Area Networks (VLANs) to segment traffic, which provides Quality of Services (QoS) for certain applications. If your corporation has deployed a VoIP PBX, then it’s a safe bet that a VLAN has been deployed to assure no interruption in communications. VLANs allow multiple critical applications to be segmented in order to avoid traffic congestion in well planned networks. A poorly planned, non-monitored network can be the equivalent of a city with a poorly planned highway system. In either case, too much traffic in a given area will cause end-user frustration and impact applications.

The most common wireless devices and applications using this layer are 802.11

As wireless systems were deployed, the need for the separation of wireless networks into a Third Physical Network or Third Network was developed. The Third Network - The Plant Network - has different domains, different requirements, and different applications.

Layer 3.5 (DMZ)
Layer 3.5 is commonly referred to as the DMZ of the PCN. This allows communication to and from systems such as Plant Historian to PCN layers and the same firewall that allows communication from the BN to Plant Historian and other devices that are collecting data from PCN layers.

A firewall provides protection to the PCN and restricts access to layers 3 and 2. The firewall may fall under the support of the Plant IT/Corporate IT department or the Plant Control System Group. Regardless of who supports these firewalls, there are usually strict policies on the type of traffic that can and should flow outbound and inbound within the PCN layers. This will be discussed later in this paper since this is what we refer to as the Third Physical Wireless Network Layer, also known as the Wireless Network Layer.
(WiFi) devices that provide wireless access in conference, VoIP, wireless handhelds, and 802.16 (WiMAX) that allows you to backhaul or replace fiber at hard to get locations such as contractor trailers and turnaround trailers that may require temporary access to the network.

Layer 4 is typically connected via a Wide Area Network (WAN) to other plant sites that include corporate and international business units for large corporations. Corporate IT personnel usually maintain these network connections and maintain access into and out of the organization via a firewall or by an outsourcer provider. Remote or traveling employees may have the ability to access the network remotely via different access levels such as VPN or remote access providers. With this type of access, very few, if any, have access below Layer 4 devices remotely.

The 3rd Network – The Plant Network

Different domains, different requirements, and different applications warrant consideration of a third, related and interconnected, but separate network.

Regardless of what layer is best for your site, it is important to understand your future wireless needs and the applications your site may deploy. Decisions are often based on current cost versus the cost of the decision in tomorrow dollars. What if you had to move or add applications that impacted a maintenance team application deployed a year ago? Will your investment today be re-usable for additional applications in the future and what is the best layer to place these applications? What are the corporation’s future wireless plans and what will the impact be on the project or future application costs?

As wireless systems were deployed, the need for the separation of wireless networks into a Third Physical Network or Third Network was developed. The need was not that wireless is less secure than wired networks, but it was evident that implementing wireless sensors, gateways, handhelds, VoIP devices, process and security video, coupled with monitoring and support impacted both the BN and the PCN. As discussed earlier, the ability to handle multiple wireless devices and maintain different security requirements for different applications was placing a strain on existing infrastructures and posed implementation risks including outages.

One example is that some companies have not implemented VLANs or may have limited use on certain switches. Therefore, deploying VLANs across all plant switches may be considered too risky for existing infrastructures. This usually requires that all switches be at the same firmware level and that access to all the switches is available. There may be a mix of different managed switches from different vendors and some unmanaged switches that do not allow VLANs or segmented data unless unmanaged switches are replaced.

Creating a Third Network layer allows us to implement a solution that allows locations to access the PCN layer via the DMZ layer or the 3.5 layer and allows access to the BN or layer 4 for applications such as handheld devices that require access to the ERP system or Plant System in order to access Standard Operating Procedures (SOPs). This physical layer allows us to create VLANs for additional applications and some customers have added a firewall between the Third Network and the DMZ layers.

Companies that deploy this type of access are able to leverage remote monitoring and maintenance of the wired devices and network.
without compromising performance or risk to the PCN or BN layers. This increases Return on Investment (ROI) on additional applications deployed on this layer.

**The Growth of Industrial Field Device Wireless Networks**

Level 1, 2 and 3, the PCN has been expanded by the use of wireless field devices to measure (and control) both basic measurements like flow, level, temperature and pressure and also new measurements like vibration, and the like that are of more interest to the asset management system.

Communication managers find the situation complicated by the existence of multiple wireless standards, as well as proprietary solutions throughout the industrial world. The four basic wireless field device standards found in plants are IEC 62591 WirelessHART, ISA100.11a, WIA-PA (a Chinese standard being submitted to IEC) and Zigbee. In many plants, Bluetooth networks exist to connect short range communications on the plant floor. This multiplicity of standards, and proprietary offerings has meant that it is extremely difficult for a communication strategy to be developed that will not have the significant chance of having to be ripped and replaced as something better comes along.

At least the big four mentioned above are basically open standards, and well on the way to becoming IEC global standards. Convergence efforts have failed, so we are left with the need to provide a network that can handle a variety of open standard networks.

This discussion will focus on IEC62591 WirelessHART and ISA100.11a, as the most common open standards currently being used.

**Integrating Field Devices into the “Third Network”**

These open standards-based wireless applications networks are secure, reliable, and scalable and allow plants to choose precisely the right wireless applications, devices and technologies for ‘plug and play’ interoperability. Open industrial wireless networks require wireless networking appliances that seamlessly integrate wireless sensor network gateways based on either ISA100.11a or WirelessHART® standards with 802.11 (WiFi) radios to support other industrial wireless applications such as mobility, location, video, and communications and to enable efficient backhaul of sensor data wirelessly. By supporting devices with both these standards, industrial facilities will be equipped with the easiest, most cost-effective way to gather accurate and timely information to improve safety, product quality and productivity plant-wide.

**Benefits of an Open Industrial Wireless Application Network**

An open, standards-based industrial networking appliance and devices offer processing manufacturers the option to choose either ISA100.11a or WirelessHART® standards with 802.11 (WiFi) radios. Wireless sensor networks can enable better, more timely data into your control system, predictive maintenance or asset management application.

The new generation of wireless network technology and standards offer a tremendous opportunity to realize significant improvements in the overall efficiency of your plant.

Condition monitoring based on an open, standards-based wireless application network enables cost-effective, reliable, and safe instrumentation for critical facility measurements needed to optimize plant efficiency.

Wireless instruments based on ISA100.11a or WirelessHART® deliver data to the full range of maintenance, safety, and security applications.

Reliable, long-range, high bandwidth wireless broadband technologies like WiMAX (IEEE 802.16) have been ruggedized for industrial environments and applications. These industrial broadband networks are designed to deliver improved reliability and wireless capacity.

An open, integrated wireless application network enables plants to use many “best of
breed” applications for increased ROI and lower total investment costs, which can be sustained for many years.

**Wireless Technologies at Work**
One doesn’t have to look far to see that major automation vendors are increasingly integrating wireless technologies into their products. Going wireless is seen as a way to cost effectively add more process monitoring capabilities, enhance workforce mobility, improve safety and security, and drive greater utilization of assets, raw materials and energy. However, for wireless to work in manufacturing environments the technologies must deliver reliable performance, security, and ease of use.

Although wireless is heralded as the next big thing in automation, it certainly isn’t new. The move to use wireless technology to reduce costs and improve efficiency has been underway for some time in manufacturing organizations. What has changed is the emergence of products, applications and standards to address the specific challenges for using wireless in large manufacturing facilities. By extending the range and lowering the costs of plant and process network communications, this new generation of wireless network technology offers a tremendous opportunity to realize significant improvements in the overall efficiency of the plant.

Wireless sensor networks can enable better, more timely data into your control system, predictive maintenance or asset management application. Operators in the field are now able to see the control system and review standard operating conditions, procedures, and corrective actions in real-time as they make field adjustments. Security departments are using wireless as a means to improve security and achieve timely compliance with increasing regulations by wirelessly adding video monitoring, along with improved access control and intrusion detection. Other technologies and applications such as voice communications and asset tracking use wireless to enable productivity gains that have already been realized in other industries such as healthcare and transportation.

**Benefits, Yes, But Too Costly to Run Wires**
In some cases these benefits were simply too costly to achieve by running wires, while in others they simply couldn’t be done without wireless networks. Going forward the challenge is to insure that the best of breed industrial wireless solutions are secure, reliable, scalable and simple to operate. Overcoming that challenge requires a clear understanding of the alternative technologies and to best apply them.

**Choosing the Right Wireless Technology**
As the list of wireless applications grows, so do the number of wireless devices and systems that support these applications. This application growth adds complexity from using multiple wireless technologies to address each application’s specific requirements for coverage, latency and throughput.

There is not a “one-size-fits-all” wireless networking technology that adequately supports the diverse and demanding requirements of the many different kinds of industrial applications and environments.

Most wireless systems have been designed to use public frequencies, which are shared across the different technologies and applications. The frequency sharing is made easier by the emergence of robust standards for communications, but standards alone are not enough. Standards assure the proper function of the systems with a given set of cost/performance characteristics, and a basis for interoperability - but no single wireless technology or standard is capable of being the single solution for every application.

This diversity of cost/performance trade-offs among the dozens of available industrialized wireless networking technologies dictates that users choose the most effective technology and devices for a specific application. There is not a “one-size-fits-all” wireless networking technology that adequately supports the diverse and demanding requirements of the many different kinds of industrial applications and environments.

Standards-based technologies like WiFi (IEEE 802.11) have been hardened for mobile workers to take ruggedized tablet PCs and PDAs into the plant. Other radios like those based on IEEE 802.15.4 have been optimized to support...
wireless sensor networks for industrial instrumentation via the ISA100.11a and WirelessHART® standards. Standards for wireless instrumentation and condition monitoring ISA100.11a and WirelessHART® enable the creation of scalable, integrated applications based on wireless sensor networks. Wireless sensor networks based on ISA100.11a or WirelessHART® deliver data to the full range of maintenance, safety, and security applications.

In addition, reliable, long-range, high bandwidth wireless technologies like WiMAX (IEEE 802.16) have been ruggedized for industrial environments and applications. These industrial broadband networks are designed to deliver improved reliability and wireless capacity.

This diversity of cost/performance trade-offs among these and the dozens of other available industrialized wireless networking technologies dictates that users choose the most effective technology and devices for a given application. There is not a “one-size-fits-all” wireless network-ting technology that adequately supports the diverse and demanding requirements of industrial applications and environments. The laws of physics dictate that it is extremely unlikely that there will be such a powerfully flexible wireless technology anytime in our future.

Managing Your Most Important Wireless Asset
There is an extremely important asset that you own and control. However, if you don’t manage this asset effectively, it could turn into your greatest liability. This asset is your airwaves – the radio-frequency spectrum that is available to you in and around your facility. Imagine two to three years from now when you have hundreds or even thousands of wireless devices in your plant from dozens of vendors. Just like your wired networks today, without the right tools for managing the secure, effective coexistence of your airwaves, the wireless networks will become unreliable, slow, and potentially create unintended security vulnerabilities. In addition, the choices you make today, may limit your options in the future as new wireless technologies become available. How do you both avoid this looming wireless logjam and future-proof your wireless networks? There are three basic choices a plant can make in implementing wireless networks:

**Choice #1:**
Select a Single Vendor
Choosing all of your wireless networking applications from a single vendor gives you the advantage of an engineered system that is designed to integrate various wireless technologies into a single seamless system. Unfortunately, this choice locks you into a limited set of lowest-common-denominator proprietary “standards” that will leave you vulnerable to being held hostage by that single vendor. As new applications emerge and wireless technologies evolve, your dependence on that single vendor will limit your options, lock you into the preferences of a single vendor, and hold you back while your competitors move forward.

**Choice #2:**
Select Best-of-Breed for Each Application Need
The second option is to review the unique needs of your operations, facilities, and desired applications and choose the best wireless technology for the specific applications. This best-of-breed approach will have a better chance of delivering the performance and reliability for that one specific solution. But each best-of-breed point solution you deploy will demand its own infrastructure and management system – requiring an investment in technology and manpower. Each point-solution, wireless technology and application will also require its own wireless infrastructure, network management, and security approach. There will be no reuse of a common infrastructure. Each additional

Open standards-based wireless networks are secure, reliable, and scalable. A truly open wireless infrastructure will allow plants to choose precisely the right wireless devices and applications for ‘plug and play’ interoperability.
wireless application will be much more expensive to deploy and manage – making it difficult to establish a positive return on your investment in any single wireless technology or application.

**Choice #3:**
**Select an Open, Scalable Wireless Network**

It is obvious that wireless technologies are not standing still. There will be new wireless technologies, tools, devices and applications becoming available over the next decade. Locking yourself into a single vendor or an inflexible, dedicated network and point solution wireless system won’t let you easily take advantage of new technologies as they become available.

The answer is to have a single shared wireless application network that allows “plug and play” interoperability, management, and security of any wireless devices and applications – regardless of their radio frequency, protocol, or application. A truly open wireless application network will allow you to choose exactly the right wireless device and application for your plant. This wireless application network also delivers greater application flexibility and cost certainty with an engineered approach that creates a network of systems and integrated applications based on open standards, best practices and vendor neutrality across all your wireless applications.

An open, integrated wireless application network enables plants to use “best of breed” applications for increased ROI and lower total investment costs.

Open standards-based wireless networks are secure, reliable, and scalable. A truly open wireless infrastructure will allow plants to choose precisely the right wireless devices and applications for ‘plug and play’ interoperability. Plants that select an open, integrated wireless application network benefit from being able to use many “best of breed” applications. This comprehensive and open wireless network delivers increased ROI and lower total investment costs, which can be sustained for many years.

An open, standards-based wireless application network enables process manufacturers to cost-effectively deploy the best possible wireless applications for their plant. This vendor-neutral approach to industrial application implementation insures that plant operations managers are able to cost effectively deploy the best wireless solution for any given application.

The choice should be easy. The financial and operations benefits of industrial wireless are most effectively realized with an open solution architecture capable of utilizing the best technologies and applications available – from any vendor. The Apprion ION System is a vendor-neutral approach to industrial application implementation that insures that plant operations managers are able to cost effectively deploy the best wireless solution for any given application.

The financial and operations benefits of industrial wireless are most effectively realized with an open solution architecture capable of utilizing the best technologies and applications available – from any vendor. The Apprion ION System is a vendor-neutral approach to industrial application implementation that insures that plant operations managers are able to cost effectively deploy the best wireless solution for any given application.