Wireless Process Control Network Architecture Overview

Industrial Wireless Networks Gain Acceptance In Plant Floors

By: Soroush Amidi, Product Manager and Alex Chernoguzov, Wireless Architect
Table of Contents

Multi-Level Network Topology ................................................................................................................................. 1

Wireless Arrival on the Plant Floor........................................................................................................................... 3

How Does a Wireless Network Fit Into The Existing Network Architecture? ............................................................ 4

Network Topology Review .......................................................................................................................................... 5

Recommendations ....................................................................................................................................................... 9

References ................................................................................................................................................................. 10
Multi-Level Network Topology

In recent years, Ethernet has become the network technology of choice on the plant floor as manufacturers strive for more efficient and cost-effective ways to operate their plant. The technology enables manufacturers to unite their company’s administrative, control-level and device-level network into a single system, enabling real-time information flow throughout the company.

Though using the same Ethernet technology for their business applications and process control applications, manufacturing facilities protect their network from external and internal threats using a multi-layered approach by dividing the overall architecture into three segregated networks:

- The **business information network**, also referred to as the Level 4 network in the Purdue Model of Process Control, supports traditional administrative functions such as human resources, accounting and procurement.

- The **control-level network**, also referred to as the Level 2 and Level 3 network, connects control and monitoring devices including controllers, I/O racks, human-machine interfaces, plant historians and advanced control applications.

- The **device-level network**, also referred to as the Level 1 and Level 0 network, links the plant floor’s I/O devices, such as sensors (such as transducers and flowmeters) and other automation equipment.

At each segregated network, switches connect the various devices associated to the same level network. A single interconnection is used to securely exchange information between these networks as illustrated in Figure 1. These single interconnections are composed of a firewall and a router; and quite often the firewall and router are two different hardware devices.

A single interconnection improves the network security by allowing IT managers to monitor a single connection for security threats. It also eliminates a hacker’s ability to address systems not intended to be externally addressable. This security model of isolating networks is also referred to as the ‘air gap model’. Should either network have an issue, the networks may be quickly disconnected to preventing either network from impacting the other, thus creating the air-gap.

---

1 “Security Solutions to Meet NERC-CIP Requirements” Whitepaper, Kevin Staggs, Honeywell Process Solutions
Figure 1: Network Levels in an Experion System
Wireless Arrival on the Plant Floor

The rapid advances and maturation of wireless technology, such as Wi-Fi security, network management, standardization and mesh networking, have captured the attention of corporate and IT managers as they look for new business enablers capable of improving profitability. Companies are now enhancing their wired network by extending it wirelessly.

Wireless networks are being implemented on plant floors to support mobility applications such as laptops, handhelds and other Wi-Fi devices. These Wi-Fi devices are based on the IEEE 802.11 standard which differs from the IEEE 802.3 standard used for Ethernet. The main differences between these two standards are at the physical and MAC layers. Beyond these two differences, the two standards are comparable, allowing a site to deploy the same set of applications on either wired or wireless Ethernet or combination of the two.

Plants are also implementing wireless networks to support their wireless field devices. Most wireless field devices use an IEEE 802.15.4 standard-based radio. The field devices send process data to the control system using a standard such as Zigbee, ISA100, WirelessHART or Bluetooth. The ISA100 standardization effort, which is led by consortium of end-users and suppliers, is encouraging plants to scale up their wireless transmitter footprint and migrate to ISA100-ready transmitters and network.

Figure 2: Access to Drawings in Real-time from the Factory Floor
How Does a Wireless Network Fit Into The Existing Network Architecture?

There is an increasing demand for industrial wireless devices and networks capable of supporting both mobility tools and field devices. Businesses can justify the investment by demonstrating wiring cost savings, real-time access to data previously difficult to collect and employee efficiency with mobile tools. At the device network level, plants need to provide a connection between their wireless transmitters and controllers. They also use wireless technology to connect remote controllers and I/Os. At the control network level, plants need to provide connection for reliability-related transmitters, such as vibration transmitters for rotary equipments, safety wireless devices, tablet PCs, handhelds and wireless cameras for access to real-time data. For instance, Honeywell’s Mobile Station enables field operators to view a control system’s alarm summary and process displays directly in the field. Wireless vibration transmitters are used to monitor the health of previously un-instrumented rotary equipments. Handhelds are used to electronically enter data collected during operator rounds. Safety wireless devices such as wireless gas sensors, personnel location receivers and wireless video improve employee safety. Finally, plants enable their mobility smart devices to have real-time access to business applications local on the business network, such as work orders.

So how can a company design a network infrastructure that will connect the wireless network to the wired network securely and reliably? How many wireless networks are required to support these applications?

The first step is to select the wireless network or networks capable of supporting the various standards used by the many devices existing in or planned for your plant, i.e. 802.3 for Ethernet based devices such as IP cameras, 802.11 for Wi-Fi devices such as handhelds, cameras and finally ISA100, Zigbee, WirelessHART or Bluetooth for wireless transmitters. For control level applications, the wireless gateways connecting the wired network to the wireless network need to support the most common industrial communication protocols such as FOUNDATION Fieldbus, HART, modbus, profibus and OPC. Plants can either implement dedicated wireless networks for each standard or a single universal wireless network capable of supporting all these standards. Honeywell is one of the suppliers that offers a single and universal wireless networks capable of supporting 802.3, 802.11 and ISA100 devices.

The second step is to design a network architecture that securely connects the wireless network or networks to the wired network. In order to design a robust and scalable architecture, the company needs to clearly identify all applications and their users that will leverage the wireless network. Some data needs to go to applications hosted on the business network and others are used by applications hosted on the control-level network. For example, a mobile station providing process data needs to be connected to the control-level network. A handheld used during operator rounds also needs access to the control-level network. But the same handheld might need access to the work-order application which resides on the business network. Wireless transmitters will require access to a device level network.

While collecting all these requirements, the plant needs to also consider the bandwidth requirements. The network architect must be aware of the number of wireless devices connecting to the network and the bandwidth utilization rate for each device type. Can a single wireless network support all business and process control applications? Should the wireless network be segregated into two wireless networks, one for the process control applications and one for business network applications? Or should there be more than two wireless networks, i.e. one for business-level applications, one for control-level applications and one for device-level applications?
Network Topology Review

Let’s review the advantages and disadvantages of the three most commonly considered network topologies.

The first network topology consists of a single wireless network supporting all corporate applications, i.e. business and process control as illustrated below. This option requires implementing wireless virtual LANs (W-VLANs). VLANs are used to separate a single physical infrastructure into multiple logical networks. 802.11q provides a standard for the VLANs. The wireless network is segregated virtually into at least two W-VLANs, one that connects to the business network and another that connects to the process control network.
For this topology to succeed, the company needs to select wireless access points capable of supporting all standards, i.e. 802.3, 802.11 and ISA100. They also need gateways that support both business and industrial protocols such as Modbus, FOUNDATION Fieldbus and HART.

Advantages:

- A single network to manage and maintain
- Low installation and lifecycle cost

Disadvantages:

- The same shared wireless medium is being used for the business and process control logical network which represents a fundamental shift from the multi-level approach used to secure the process control network.
- Wireless network to be managed by either corporate IT team (most common) or site’s system administrator.
- Difficult to balance both corporate and plant’s requests by the corporate IT team responsible for the wireless network.
- The team responsible for the network should be be familiar with the site’s network architecture and have a good understanding of VLANs implemented on both corporate network as well as process control network.
- Availability of the wireless network management at the site level if the wireless network is being managed at the corporate IT level.
The second topology consists of having three separate wireless networks, one for the business-level applications, one for the control-level applications and one for the device-level applications.

**Advantages:**
- This topology allows you to segregate each wireless network. Users will monitor and maintain each network separately.

**Disadvantages:**
- Additional infrastructure cost
- Different type of infrastructure, which require a security manager and network manager at each level
- On-site system team needs to manage two different wireless networks.
- Sensor network has a slower update rate.
- High implementation and lifecycle costs
The third topology is to have two segregated wireless networks, one for business-level applications and one for the process control application. The process control network and business network are connected to each other through the wired network which is air-gapped. In this topology, the process control wireless network supports both control-level applications as well as device-level applications, capable of communicating with wireless transmitters and Wi-Fi devices. The process control wireless network is basically an extension of the process control network. The topology will rely on W-VLAN technology to create a logical network for L2 and L3 applications such as L2-based HMI process displays and L3 electronic operator round applications.

Advantages:
- Segregated wireless business and process control networks.
- Corporate IT is responsible for the business wireless network while plant IT is responsible for the wireless control network.
A single wireless network to maintain and monitor at the plant level.

Wireless devices leverage the wireless backhaul which is a faster network. This reduces the latency between field devices and controller and increase the battery life time of the wireless devices.

Disadvantages:

Two wireless infrastructures to maintain at the corporate level, one for the business applications and one for the process control applications.

Recommendations

There is no “one size fits all” network infrastructure. Each site needs to select the most convenient infrastructure based upon their needs and risk tolerance. However, the current trend is for plants to choose either the one wireless network model with the local site controlling and monitoring the wireless network or the two segregated wireless network model (third topology above) since they are the most efficient and cost effective solutions.

Sites extend their process control network through an industrial wireless network capable of supporting the various wireless standards and field devices protocol. They also extend their business network with a wireless network capable of supporting their Wi-Fi devices and business applications.

Honeywell has been helping plants implement industrial wireless networks with the multifunctional OneWireless network. The network consists of industrial access points called Multinodes which are capable of self-discovering each other and forming a mesh network. Unlike the access points used in a business environment, these industrial access points do not need to be physically connected to the wired network and communicate with each other wirelessly. To reduce implementation and lifecycle cost, Honeywell an industrial access point that is equipped with three antennas, one used to communicate with Wi-Fi devices (handhelds, laptops, Wi-Fi based sensors), one used to communicate with ISA100-ready transmitters and one used to communicate with other access points. The wireless network is connected to the wired network through a node acting as a wireless bridge at the Level 2 and/or Level 3 network. The Level 2 node, referred to as a Wireless System Gateway supports all field protocols and standards required to support process control applications. The field protocols and standards include Modbus, HART and OPC. Additional field protocols will be offered with the next gateway release.

Benefits of the OneWireless network include:

- Supports most common wireless standards: IEEE 802.3, IEEE 802.11 a/b/g, IEEE 802.11q, ISA100-ready
- Supports most common industrial protocols: Modbus, HART, OPC, upcoming ISA100 standard
- Lower installation and maintenance cost as it is capable of communicating with Wi-Fi based applications as well as wireless field I/Os.
- Tight integration with the Honeywell Experion PKS control system
- Transmitter battery life reaches 10 years.
- Transmitter publication is individually configurable up to a 1 second update rate.
- No separate LAN controllers are needed to configure the access points.
- If a single Multinode becomes inoperable, only that Multinode and its associated coverage area are affected.
• The Multinode is powered by 24 VDC power which is typically found in operating areas of industrial manufacturing facilities. The Multinode can also be powered by an external AC/DC power supply. The power supply can be replaced without disassembling the Multinode.

• The Multinode wireless backbone mesh network is very scalable and flexible with the ability to mesh at either 2.4 or 5.8 GHz as well as the ability to fine-tune the mesh based on signal strength or even disable individual mesh links.

• A single network management application used to monitor and maintain the wireless networks and field devices associated to it.

References

• Kevin Staggs, Honeywell Process Solution White Paper, Security Solutions to Meet NERC-CIP Requirements

• ANSI/ISA-TR99.00.01-2007, Security Technologies for Industrial Automation and Control Systems