November/December 2013

System Integration

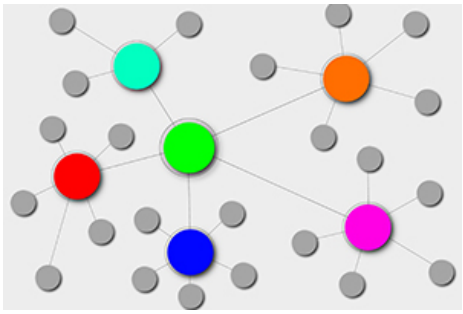
Field wireless networks

ISA-100.11a and other wireless technologies are making inroads into process control and measurement applications

Fast Forward

- Various wireless topologies can be employed to meet the demands of industrial wireless applications, including star, tree, mesh, and cluster.
- Industrial wireless protocols typically provide security features, such as encryption, authentication, and key management, to ensure protected communications.
- Reliability is assured through redundancy, intelligent channel hopping, time synchronization, and other features.

By Amit Ajmeri



Industrial wireless devices and networks are used for measurement and control applications in areas of process plants where it is too difficult or too expensive to hardwire sensors, transmitters, and final control elements. They are also used for temporary applications, such as in research and development and pilot plants. Although most consumer wireless networks are used for convenience, industrial field wireless networks must be much more reliable, and cannot interfere with other wireless applications in the plant. These networks, and their accompanying wireless devices, must also be simple for existing plant personnel to support. Finally, industrial wireless networks and devices must easily integrate with existing wired devices and networks, and the entire wireless system must be flexible and scalable.

Wireless solutions for the process industry

There are three basic areas in which industrial field wireless networks can operate in the process industry: the global canopy, a site backbone, and a field mesh. The *global canopy* is the term used for long-range wireless communication. It can be made up of a site-to-site private network joining locations up to hundreds of miles apart, or it can use public networks, such as the Internet, a satellite, or cellular communications. This type of network is used for data transmission over very long distances.

A *site backbone* is a good solution in cases where data is transmitted from cell-to-cell within a transmission distance of a few miles. Although the distances covered are shorter than with a global canopy, a site backbone network can still be used to transmit data over relatively long distances.

A *field mesh* or wireless sensor network is used for sending and receiving a few kilobytes (kB) of data over a short range up to a few hundred feet. These field wireless networks are comprised of sensors and actuators, field mobile devices, and field end points—and these types of networks will be the focal point of this article.

Frequency bands

Coming Next

Cover Story: Plant Upgrade Strategy

Process Automation: Training Using Simulators

Factory Automation: Discrete Manufacturing Robot Application

System Integration: Safety Systems-Applying Smart Transmitters

Automation IT: Enhanced Operator Interfaces

Special Section: First Robotics

Basics: Temperature Sensor Basics

Ask The Experts

Read questions answered by our experts or join the email list.

Feedback Hub

Training college grads, firewall reliability

Hidden savings

Less theory, more practice and more

ISA Jobs

GENERAL MANAGER â€“ KENTUCKY DIVISION | Confidential

MARKETING/ SALES MANAGER | Ronan Engineering

Instrument Technician | Flint Hills Resources

Communication frequency is one of the most important factors when implementing a field wireless network. The 2.4-gigahertz (GHz) wireless communication frequency band is most commonly used for industrial applications. It is part of the industrial, scientific, and medical (ISM) radio bands that were originally reserved for international use of radio-frequency energy for ISM purposes, as opposed to telecommunications.

The ISM band has become the de facto standard because it is available worldwide and does not require licensing. Within that band, 2.4-GHz communications are used in the following standards:

- IEEE 802.11b/g/n (Wi-Fi) is used for a wireless local area network with communication distances of 300 to 900 feet with a data communication rate of a few megabytes per second.
- IEEE 802.15.1 is used for Bluetooth ® communications that require extremely low power over a short communication range of 3 to 30 feet.
- IEEE 802.15.4 is a self-organizing, self-healing mesh network used in low-power personal area networks. ZigBee, ISA-100.11.a, and WirelessHART use variations of this standard.
- IEEE 802.16e is used for the WiMax communication protocol and covers a 3- to 30-mile range with a data transmission rate of approximately 72 megabytes per second.

Wireless for industrial automation

Figure 1 depicts various types of networks within a plant. Wireless sensors (XC, XX, XV, etc.) are at the bottom of the diagram. The architecture may include a wireless sensor network working at a remote location exchanging data with the process control network using IEEE 802.11 Wi-Fi or IEEE 802.16 WiMax technologies.

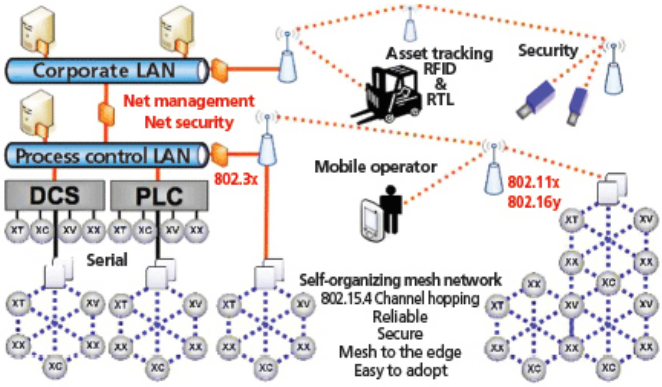


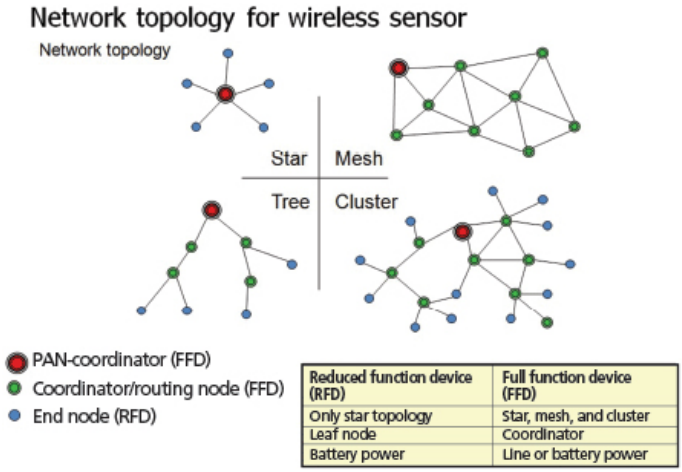
Figure 1. Various wired and wireless network types are often found in a typical manufacturing facility.

Located at the next level up, between the distributed control system and programmable logic controller automation systems and the wireless sensors, are access points or gateways. Gateways are the interface points between the wireless network and the host automation system. The gateway talks to the sensors wirelessly, and communicates with the automation system using wired protocols, such as serial Modbus, Modbus TCP, or Ethernet IEEE 802.3. With most wired protocols distance is a limiting factor, so the gateways are typically located close to the automation system.

In most industrial applications, there are other devices using wireless communications, such as cameras, radio frequency identification (RFID) systems and cell phones—so methods must be devised to reduce interference and ensure reliable communications.

Network topologies

Wireless network topologies can be used, depending on application requirements, including star, tree, mesh, and cluster. The ISA-100.11a protocol supports all these (figure 2).



Reduced function device (RFD)	Full function device (FFD)
Only star topology	Star, mesh, and cluster
Leaf node	Coordinator
Battery power	Line or battery power

Figure 2. Network topologies for wireless networks can be a single star or tree topology or combinations of topologies, such as a mesh or cluster.

The star topology is typically used with reduced function devices that are only powered by batteries. Full function devices that work with batteries or line power are more adaptable for use with other topologies.

The most basic network type is the star topology with one functioning routing or center node that sends and receives information from all the end nodes. Thus, the end nodes only have one function: transmitting data to the center node. As a result, the end nodes consume very little power, because they only send information to the center node, then go back into sleep mode. In addition to reducing the energy needs at end nodes, the star topology prevents any end node failure from affecting the rest of the network, because every end node device is isolated from the larger network by the link that connects it to the center node.

The mesh topology is comprised of nodes that can each route data from neighboring nodes as long as they are in the same radio frequency range. The mesh network system provides reliable, secure data transmissions and is highly scalable. If a path via one node or a set of nodes is not working, a node can route its data to a neighboring node, with the information eventually reaching the destination node via this alternate path.

The tree and cluster topologies are a combination of the star and mesh networks. The tree network has one communication node with star nodes below it, and the cluster network is a combination of star and mesh networks.

Security

Security is a critical factor for industrial wireless systems used in the process industries, so mechanisms for protecting the wireless network must be implemented. The ISA-100.11a standard has several security measures that can keep the network safe, including:

- Encryption: Each ISA-100.11a data communicator has 128-bit encryption.
- Authentication: Only devices authenticated by the system manager and security manager can exchange data.
- Integrity: Each data point uses an end-to-end media access control (MAC) address to ensure data integrity and transport security.
- Key management: All wireless devices must have a join key that acts as a password that the device uses to authenticate it to the network. This is a key differentiator for the ISA-100.11a protocol.

Authentication key management and join-process technology enhance the security of the network by preventing an unauthorized node from joining the network. All node authentications are controlled by the network security manager, which requires any device joining the network to provide all its credentials in an encrypted fashion (join key) to the gateway. Each data packet has a 128-bit encryption. End-to-end basis transport security includes message-level security, such as message encryption, as well as transport-level security, such as Windows.

The network administrator gives all wireless devices a join key and sets the parameters required to access the network. Once the join key is recognized and the device has joined the network, the security manager issues it additional keys (master, session, and private) for further communication. These keys should be periodically updated, because limiting their life spans further protects the network.

The “hop-by-hop” MAC address security requires every data element transmitted between two wireless

nodes to provide the MAC address of the originating node as well as the end node for extra security.

Coexistence strategy

Since many wireless standards use the 2.4-GHz frequency band, it is very important that the various wireless technologies (Wi-Fi, WirelessHART, ZigBee, ultrawide band, and others) can operate together on the band. Among the best methods for establishing coexistence among the various wireless communication devices are spectrum spreading, frequency hopping, and time slotted and scheduled transmissions.

Electronic and electrical noise within an industrial plant can cause disturbances if protective measures are not taken. Lower-power radio technology with a spectrum-spread technique deployed at a 200-kB rate helps overcome the noise problem. Data is distributed among various channels, then collected and reassembled by the receiver. Frequency hopping, in which the data rapidly switches among many frequency channels, helps avoid congestion. These techniques are also a good way to increase security, because both the spectrum-spread code and frequency-hopping patterns are necessary to retrieve the data sent over the network.

Synchronized timing enables multiple access capabilities by assigning each device a particular time slot to avoid collisions. Deterministic transmitting (TDMA) can also save power, because only the sending and receiving devices must be awake during the data transmission. TDMA offers synchronized time sense in which each subnet gets time-synched data from the network protocol server, ensuring that all wireless network data transmissions occur at the proper times.

Other methods for overcoming obstacles are multipath mesh networks and intelligent channel hopping. Wireless mesh networks route traffic toward the Internet gateway (IGW), or from the IGW to the access points. When multiple devices attempt to select the best throughput path toward a gateway, the traffic on these paths can diminish the speed and performance of the network. A multipath mesh network seeks alternative paths during times of congestion.

ISA-100.11a also supports the black listing of channels. For example, suppose a plant uses Wi-Fi channel 3 for ISA-100.11a communications, and channels 21 and 24 for general Wi-Fi communications. The system manager can be configured so channels 21 and 24 are blacklisted for ISA-100.11a communications to avoid performance issues on the network. In this scenario, there are two separate channels: one channel for the Wi-Fi and one for ISA-100.11a communications, enabling the two wireless technologies to coexist in the plant.

Reliability

Reliability is of paramount importance for industrial process control and measurement applications, and the ISA-100.11a standard has numerous techniques for ensuring reliable communications such as redundancy, intelligent channel hopping, duocast technology, and time synchronization.

A mesh network offers redundancy, because it can reroute data from one node to the destination mode, avoiding the obstructed node. For additional reliability, redundancy can also be implemented at the gateway, backbone, security system, and system manager. For example, if one backbone router fails, the other router retrieves the data from the sensors, and then sends the information to the gateway.

Another method to ensure accurate throughput is channel hopping, where clear channel access technology dynamically chooses different channels of operation to avoid interference (figure 3). In addition, frequent retry attempts are made to limit data latency to 100 ms or less.

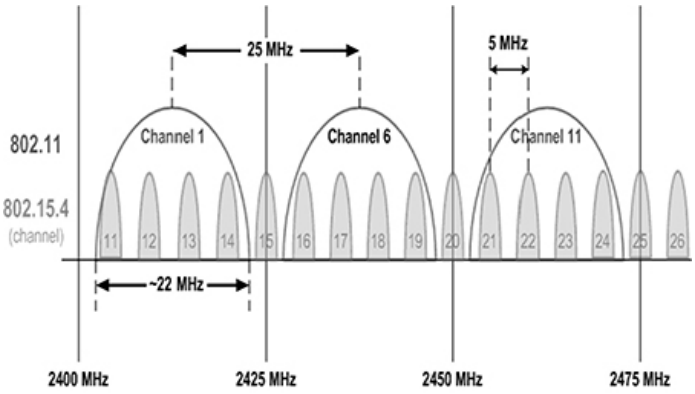


Figure 3. Channel hopping allows wireless devices to dynamically choose different channels of operation to avoid interference.

ISA-100.11a also supports duocast for redundant connectivity in which one device sends information to two neighboring nodes simultaneously. The two receiving nodes send a confirmation from both end

devices in the same time slot. Without duocast, if one communication path fails, a retry attempt is used before going to a neighboring channel to transmit the data, which can slow communications.

Time synchronization is highly accurate, because each data packet is time stamped using International Atomic Time. All data has a time slot allocation, and the data must reach its end destination and receive a confirmation from each node within that time slot. There is a limited time to capture the data packet and decipher the information, which provides secure communication.

Scalability and flexibility

Each ISA-100.11a end device uses Internet Protocol version 6 (IPv6), the newest Internet technology. This helps “future proof” the network by enabling access from a field wireless node using the latest IP technologies. The ISA-100.11a protocol has many features for scalability in terms of the number of nodes that can be added, as well as how much area can be covered. To expand the network and add more nodes, an additional backbone router can be added to create a subnet. Multiple subnets, slow-hopping mode, protocol mapping, and tunneling and backbone routing are all examples of the multiple functions of the ISA-100.11a architecture.

For fast firmware downloads and increased staff mobility, ISA-100.11a supports the slow-hopping mode using carrier sense multiple access. This enables a channel to be locked for a specific period, instead of hopping every 10 ms. The slow-hopping mode is particularly beneficial when performing a firmware download to upgrade a radio or sensor electronics for a wireless node. It also facilitates using a handheld device for calibration checks, and for configuring a specific device.

Protocol mapping and tunneling reduce infrastructure costs by supporting legacy protocols and combined wired and wireless integrations. The ISA-100.11a architecture supports many existing protocols, including Foundation Fieldbus, HART, Profibus, Modbus, and CIP. The ISA-100.11a stack includes provisions for protocol mapping and tunneling to enable Foundation Fieldbus, HART, and Profibus to use the ISA-100.11a stack for wireless communications. ISA-100.11a is targeted for measurement and control applications that can function with a 1-second data rate, and it also supports peer-to-peer communications for proportional, integral, derivative loop scheduling.

A HART device can transmit data by putting an ISA-100.11a wrapper on top of the HART data, and then sending the data through the wireless network router (figure 4). When the data is received at the gateway, the ISA-100.11a wrapper is removed, and the HART data is sent to the network.

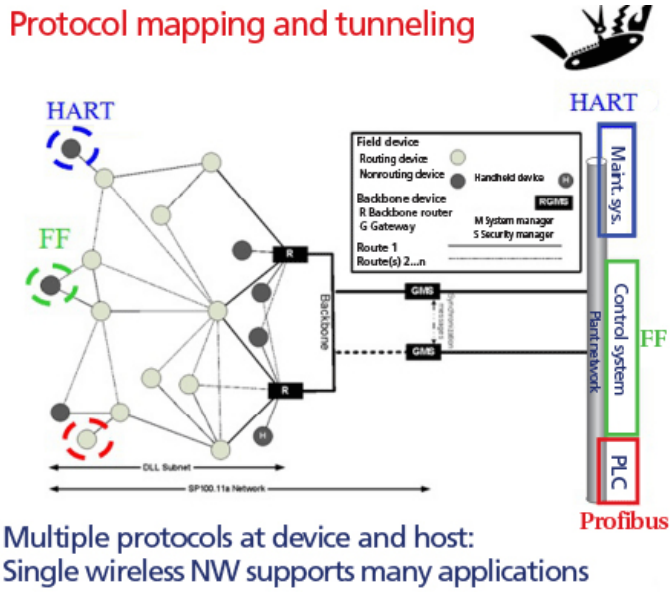


Figure 4. The ISA-100.11a standard can support multiple protocols simultaneously on a single network.

Customizable network performance

To support control applications, a subnet can be created with a 1-second data update rate via direct communications to the backbone router. This enables a 1-second transmission speed from the node to the automation system.

Multiple subnets can work in the same physical space and share a single wireless network with flexible customization for optimal network performance. In addition to sharing a single network, ISA-100.11a also allows networks with different communication speeds to operate in the same physical space. For example, one subnet can be comprised of low-speed sensors, while another provides a 1-second update rate for control applications.

ISA-100.11a supports peer-to-peer control communications, so the data from a measuring device does not need to go to the gateway, but can instead be transmitted directly to the final end control element. These peer-to-peer communications enable data exchange from one wireless node to another within a high-speed subnet for 1-second updates.

An ISA-100.11a wireless network can be deployed and reconfigured through device installation and software configuration and changes—instead of requiring burdensome wiring, addition of I/O modules, programming, and possible upgrades to the automation system. Many of the ISA-100.11a system components, such as the backbone routers and the system manager, are designed as function modules that can be added or removed depending on system requirements.

ISA-100.11a provides reliability, scalability, high performance, and the ability to simultaneously support numerous devices and protocols. Several companies are supporting the ISA-100.11a standard with field instrumentation, automation systems, and software to support the latest wireless technologies from temperature and pressure sensors, gateways, and more.

Interoperability testing and certification from the ISA100 Wireless Compliance Institute (www.isa100wci.org) ensures all manufacturers' wireless devices can communicate with the backbone router and gateway without problems in a plug-and-play manner.

ABOUT THE AUTHOR

Amit Ajmeri (amit.ajmeri@us.yokogawa.com) is a consultant for wireless and field network technology at Yokogawa Corporation of America. Ajmeri has been with Yokogawa for more than ten years. He currently represents Yokogawa on various committees for ISA, FDT Organization, HART, and Fieldbus Foundation.

Understanding the ISA100 series of standards

ISA100 is a multi-national, multi-industry standards development initiative of ISA, an accredited member organization of the American National Standards Institute. The ISA100 program was launched to create a reliable and universal family of wireless standards and guidelines for industrial automation applications. It is a market-driven (not vendor-driven) standards development program created by a committee that includes end users. The end users actively participate and vote on decisions regarding the standards and on requirements for wireless plantwide communications.

The ISA100 committee is organized into several working groups (WG), including:

- WG14, Trustworthy Wireless, to improve the reliability and security of wireless, as well as to simplify configuration and usage in a plant environment
- WG15, Wireless Backhaul Network, focusing on middle-range cell communications within the plant environment
- WG16, Factory Automation, to cover a completely separate requirement for data latency compared with that of the process industries
- WG18, Power Sources, to improve battery standardization
- WG20, Common Network Management (CNM), to present a CNM framework to monitor and provide actionable information to various and disparate wireless networks commonly found in wireless network environments for industrial automation and control systems. The framework will be scalable to address various network sizes and device populations and extensible to adapt to changing technologies, applications, and user requirements.

ISA-100.11a-2011 was approved as an ISA and American National Standard in 2011, and is currently nearing final approval by the International Electrotechnical Commission as IEC 62734.

Other documents developed by ISA100 include:

- ISA-TR100.15.01-2012 – Backhaul Architecture Model: Secured Connectivity over Untrusted or Trusted Networks
- ISA-TR100.14.01-Part I-2011 – Trustworthiness in Wireless Industrial Automation: Part 1, Information for End Users and Regulators
- ISA-TR100.00.03-2011 – Wireless User Requirements for Factory Automation
- ISA-TR100.00.02-2009 – The Automation Engineer's Guide to Wireless Technology: Part 2 – A Review of Technologies for Industrial Asset Tracking
- ISA-TR100.00.01-2006 – The Automation Engineer's Guide to Wireless Technology Part 1: The Physics of Radio, a Tutorial

For more information, visit www.isa.org/findstandards and select "100" from the drop-down list.

Resources

"Analysis of Wireless Industrial Automation Standards: ISA-100.11a and WirelessHART"
www.isa.org/link/analysisofwireless

"A real mesh"
www.isa.org/link/arealmesh

"Opportunities for smart wireless pH, conductivity measurements"
www.isa.org/link/smartwireless

Wireless Networks for Industrial Automation
www.isa.org/wirelessnetworks

Post a Comment

Jean-Pierre
2013-12-14 04:58:09

Congratulations. This is one of the best articles I have ever read about ISA-10.11a. I just have one question : you mention the possibility of having multiple subnets in the same physical space. I assume each of them has its one backbone r ...more

Related Files
System Integration image