Table of Contents teaser:
Industrial wireless has specific requirements in terms of performance, reliability and security. Various wireless technologies including the ISA 100.11a protocol are employed to meet these requirements in areas such as topology, security and customization.

Fast Forward Bullet Points:

- 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.

Resource Box:
1. Analysis of Wireless Industrial Automation Standards: ISA-100.11a and WirelessHART; http://www.isa.org/InTechTemplate.cfm?Section=Article_Index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=93257
2. A Real Mesh; http://www.isa.org/InTechTemplate.cfm?Section=Article_Index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=79947
3. Opportunities for Smart Wireless Ph, Conductivity Measurements; http://www.isa.org/InTechTemplate.cfm?Section=Article_Index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=80886

Field Wireless Networks

ISA100.11a and other wireless technologies are making inroads into process control and measurement applications

By Amit Ajmeri, Consultant for Wireless and Field Network Technology at Yokogawa Corporation of America.

Mr. Ajmeri has been with Yokogawa for over ten years. Prior to joining Yokogawa, he spent 12 years with Emerson Process Management promoting Foundation Fieldbus technology and interoperability. He currently represents Yokogawa on various committees for ISA, FDT Organization, HART and Foundation Fieldbus. His email address is amit.ajmeri@us.yokogawa.com.

Industrial wireless devices and networks are used for measurement and control applications in areas in process plants where it’s 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.
While 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 to support with existing plant personnel.

Finally, industrial wireless networks and devices must easily integrate with existing wired devices and networks, and the entire wireless system must be very 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, 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**

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’s part of the industrial, scientific and medical (ISM) radio bands that were originally reserved for international use of RF 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:

- IEEE802.11b/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.

- IEEE802.15.1 is used for Bluetooth communications that require extremely low power over a very short communication range of 3 to 30 feet.

- IEEE802.15.4 is a self-organizing, self-healing mesh network used in low power personal area networks. ZigBee, ISA100.11.a and WirelessHART use variations of this standard.
IEEE802.16e is used for the WiMax communication protocol and covers a 3- to 30-mile range with a data transmission rate of approximately 72 megabytes (MB) per second.

**Wireless for Industrial Automation**

Figure 1 depicts various types of networks within a plant. Wireless sensors (XC, XX, XV, etc.) are located 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 802.11 Wi-Fi or 802.16 WiMax technologies.

Located at the next level up, between the DCS and PLC automation systems and the wireless sensors, are access points or gateways. Gateways are the interface point 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, RFID systems and cell phones—so methods must be devised to reduce interference and ensure reliable communications.

**Network Topologies**

There are a variety of wireless network topologies that can be used depending on application requirements including star, tree, mesh and cluster. The ISA 100.11a protocol supports all of these topologies (Figure 2).

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 of 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 set of nodes isn’t 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 ISA100.11a standard has several security measures that can be applied to keep the network safe including:

- **Encryption:** Each ISA100.11a 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 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 ISA100.11a protocol.

Authenticate 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.

All wireless devices are given a join key by the network administrator who 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 key, session key, private key) for further communication. These keys should be periodically updated as limiting their life spans further protects the network.

The “hop by hop” Media Access Control (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's very important that the various wireless technologies (Wi-Fi, WirelessHART, ZigBee, UWB 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 aren’t taken. Lower power radio technology with a spectrum spread technique deployed at a 200 kB rate helps overcome the noise problem, as 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 provide effective power savings 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 the entire wireless network data transmissions occur at the proper times.

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

ISA100.11a also supports the black listing of channels. For example, a plant uses Wi-Fi channel 3 for ISA100.11a communications, and channels 21 and 24 for general Wi-Fi communications. The System Manager can be configured so the channels 21 and 24 are blacklisted for ISA100.11a communications to avoid performance issues on the network. In this scenario, there are two separate channels: one channel for the Wi-Fi and another for ISA100.11a 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 ISA100.11a standard has numerous techniques for ensuring reliable communications such as redundancy, intelligent channel hopping, Duo Cast 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 in which clear channel access technology dynamically chooses different channels of operation to avoid interference. In addition, frequent retry attempts are made to limit data latency to 100 milliseconds or less (Figure 3).

ISA100.11a also supports Duo Cast 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 Duo Cast, 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 very limited time to capture the data packet and decipher the information, which provides very secure communication.

**Scalability and Flexibility**

Each ISA100.11a 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 ISA100.11a protocol has many features to provide 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 multi-functionality of the ISA100.11a architecture.

For fast firmware downloads and increased staff mobility, ISA100.11a supports the slow hopping mode using Carrier Sense Multiple Access. This enables a channel to be locked for a specific period of time, instead of hopping every 10 milliseconds. 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 the use of a handheld device for calibration checks, and for configuring a specific device.

Protocol mapping and tunneling reduces infrastructure costs by supporting legacy protocols and combined wire and wireless integrations. The ISA 100.11a architecture supports many existing protocols including but not limited to Foundation Fieldbus, HART, Profibus, Modbus and CIP.

The ISA100.11a stack includes provisions for protocol mapping and tunneling to enable Foundation Fieldbus, HART and Profibus to use the SP100.11a stack for wireless communications. ISA100.11a is targeted for measurement and control applications that can function with one-second data rate, and it also supports peer-to-peer communications for PID loop scheduling (Figure 4).
As pictured in Diagram 4, a HART device can transmit data by putting an ISA100.11a wrapper on top of the HART data, and then sending the data through the wireless network router. When the data is received at the gateway the ISA wrapper is removed, and the HART data is then provided to the network.

**Customizable Network Performance**
To provide support for control applications, a subnet can be created with a one-second data update rate via direct communications to the backbone router. This enables a one-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, ISA100.11a 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 one-second update rate for control applications.

ISA100.11a 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 wireless node within a high-speed subnet for one-second updates.

**Conclusion**
Interoperability testing and certification from the ISA100 Wireless Compliance Institute ensures all manufacturers’ wireless devices can communicate with the backbone router and gateway without problems in a plug-and-play manner.

An ISA100.11a 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. Moreover, many of the ISA100.11a 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.

ISA100.11a provides reliability, scalability, high performance, and the ability to simultaneously support numerous devices and protocols. Yokogawa has been an innovator in developing field instrumentation, automation systems and software to support the latest wireless technologies, from temperature and pressure sensors to gateways and more. To learn more about Yokogawa’s wireless products, please visit [http://www.yokogawa.com/tpc/ourbusinesses/tpc-businesses-en.htm](http://www.yokogawa.com/tpc/ourbusinesses/tpc-businesses-en.htm)
## Table 1: ISA100.11a Wireless Network Architecture Components

<table>
<thead>
<tr>
<th>Role</th>
<th>Role Definition and Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input/Output</td>
<td>Sources or consumes data. Does not route.</td>
</tr>
<tr>
<td>Router</td>
<td>Routes messages for other devices operating in the wireless subnet.</td>
</tr>
<tr>
<td>Backbone Router</td>
<td>Routes data via the backbone. Mitigates among devices operating in the wireless subnet and devices operating on the backbone.</td>
</tr>
<tr>
<td>System Manager</td>
<td>The “brains” of the network. Manages all network devices through policy-controlled configurations based on desired performance parameters.</td>
</tr>
<tr>
<td>Security Manager</td>
<td>Enables, controls and supervises the secure operation of all devices present in the network.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Provides an application interface between the wireless network and the plant network.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Provisions devices with configurations required for operation within the network.</td>
</tr>
<tr>
<td>System Time Source</td>
<td>Responsible for maintaining the master time source of the network.</td>
</tr>
</tbody>
</table>
SIDEBAR: Understanding the ISA100 Family of Standards

The International Society of Automation (ISA) was founded in 1945 as a global, non-profit organization to set automation standards. The ISA100 standard was developed with funding from the U.S. Department of Energy for the purpose of creating a reliable and universal family of wireless standards for industrial automation applications. It’s a market-driven (not vendor-driven) standard created by a committee primarily comprised of end users who vote on decisions regarding the standards and on requirements for wireless plant-wide communications.

The ISA100 is a family of standards, including:

- Working Group 15 which makes decisions for the Wireless Backhaul Network. This comprises middle range cell communication within the plant environment.
- Working Group 14 for Trustworthy Wireless whose goal is to improve the reliability and security of wireless, as well as simplifying configuration and usage in a plant environment.
- Working Group 18 for Power Harvesting that works to improve battery standardization.
- Working Group 21 for ISA100.21 Asset Tracking using RFID and Real-Time Locating System technologies.
- ISA 100.12 WirelessHART and ISA100.11a Converged Network Applications to create a single global standard instead of two competing standards
- Working Group 16 for Factory Automation, which has a totally separate requirement for data latency as compared to the process industry (Figure 5)

The Process Applications (ISA100.11a) specification for wireless sensing networks is already completed and released. The Wireless Backhaul Network (ISA100.15) standard has preliminary specifications ready for a vote.

Other standards are less developed. Trustworthy Wireless (ISA100.14) is still in progress, as well as the WirelessHART and ISA100.11a for Converged Network Applications (ISA100.12) standard. Preliminary specifications are in place for the People and Asset Tracking Standard (ISA100.21).
Figure 1: Various wired and wireless network types are often found in a typical manufacturing facility.

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.

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

Figure 4: The ISA100.11a standard can support multiple protocols simultaneously on a single network.

Figure 5: This diagram depicts the ISA100 timeline for the several groups developing specifications for the family of standards.