Prepare Wireless Protocol for the Future

For almost a decade, the ISA100 family of standards has been developing a comprehensive protocol, and it is now ready for the Internet of Things.

By Penny Chen, Yokogawa Corporation of America

Most engineers would say that the International Society of Automation (ISA) 100 standard covers wireless instrumentation in process plants. This is correct, but it overlooks the comprehensive nature of changing wireless standards and best practices that encompass more than just process plants.

The availability of wireless components for process and discrete manufacturing applications is growing, and with broadening adoption of the Internet of Things (IoT), the number of devices and opportunities for building connections in a plant using Internet protocol (IP) networking is increasing. Choosing a wireless protocol that is “future
“proof” is important and was a chief concern throughout the ISA100 development cycle.

SENSORS & INSTRUMENTATION
While many elements make up the larger ISA100 standard (see “The Scope of ISA100” on page 31), one of the first parts completed was ISA100.11a, which covers wireless sensor networks. It was ratified in 2009 and again in 2011 with refinements. In 2011, it was approved by the American National Standards Institute and as IEC62734, it passed as a committee draft for vote in 2013. It will become an International Electrotechnical Commission (IEC) standard.

ISA100.11a is an open-consensus standard. The larger ISA100 committee with 400 members from 250 companies, which represents end users and suppliers in every area of process manufacturing, has been involved at various stages to establish this standard. Creating a standard with a large committee in a deliberative manner ensured the greatest level of participation with the highest possibility of fulfilling the widest range of user cases.

END USER NEEDS
With the development of ISA100.11a, the committee could start with a clean slate to create a wireless networking approach that was not limited by older wired networking protocols. Instead, the committee leveraged more advanced and widely deployed technologies to build a standard that is future-proof. The platform would have to deliver the following:

- **Reliability**—Because the end users cannot see and may not always trust a wireless connection to operate as designed, reliable communications is one of the primary concerns. Process plants often run 24/7 for many years, so high data integrity with low latency and few errors is paramount. ISA100.11a offers robust networking with redundancy where needed. With cyber security becoming more critical, its encryption mechanism maintains safe data and communication channels and protects from outside penetration with sophisticated technologies. Power management techniques that offer highly predictable battery life to minimize maintenance requirements are also considered by providing different field networking topologies that can be mixed and matched as needed. Users can design a flexible network based on application needs, business needs and the character of its sensing devices, among others.

- **Multi-functionality**—While it may begin with instrumentation, ISA100.11a can handle devices with sophisticated data transmission requirements beyond simple sensors. Devices with more complex requirements—such as waveforms or images from analyzers or multi-variable instruments—have no trouble sending larger amounts of data. Where such devices have specialized communication protocols, ISA100.11a can carry that information using tunneling methods to deliver it...
as intended. Therefore, simultaneously incorporating multiple non-Ethernet network protocols (HART, Foundation fieldbus, Modbus, Profinet, etc.) is not an issue. Whether the facility is brownfield or greenfield, ISA100.11a provides a single wireless communication infrastructure to support all application requirements, currently and in the future.

Multiple Ethernet-based network protocols can also be incorporated. Many different types of devices can access the Internet and many types of applications can run on the Internet. The design principle of ISA100.11a follows the same communication methodology, the International Organization for Standardization/Open Systems Interconnection model (ISO/OSI), as the Internet.

- **Scalability**—Users do not want to launch a networking strategy only to find that they are bumping against deployment limits. A full-scale process plant can have tens of thousands of devices spread throughout square miles. The number of allowable devices, the ability to cover the necessary distance and the amount of data throughout all must be flexible to satisfy the variety of applications from condition monitoring to control in the field.

- **Easy deployment**—A wireless networking system that causes implementation or operational headaches will not last. It must be easy to plan, design and implement—and include many options for functions that are not in existence. Network management using drag-and-drop techniques are standard. Like cellular networks with mobile phones, over-the-air (OTA) programming is a state-of-the-art method for installation, provisioning and device management or updates. ISA100.11a has defined OTA capabilities to ensure easy deployment and provisioning, lifetime management and maintenance.

- **Openness and interoperability**—ISA100.11a does not depend on a single vendor or a single protocol, so it can adapt as needed. Simple sensors with limited battery capacity do not have to serve as repeaters. Multi-function smart sensors with fast update rates do not have to serve as routers. Any sensors that play a critical role in the main function in the plant do not have to serve as repeaters. Devices with large data requirements can send information efficiently with low latency. Sensors and network infrastructure hardware from different vendors can work together seamlessly. A flexible standard does not mean it is difficult to use. The ISA100 wireless compliance institute (WCI) is the certifying group to ensure the openness and interoperability of ISA100 standards and devices.

- **Control ready**—A wireless network that cannot deliver data as quickly as the application demands (both a fast update rate and without latency) will not be suited for control applications. Any constraint that reduces the versatility of a network will reduce its usefulness and desirability for deployment. ISA100.11a aims to cover the fastest control loops—up to 10 hertz—with latency of about 100 milliseconds. This performance is not always required, but it can be delivered when the situation demands it. In general, this degree of latency is suitable for most process control applications.

### A STANDARDS-BASED SOLUTION

The complete communication stack for ISA100.11a uses well-recognized and widely used standards. From the physical layer (PHY) to the application, it follows the ISO/OSI model. This means that if one layer of the stack needs to be changed to achieve a different set of operating characteristics, it can be completed without affecting the other layers (see Table 1, page 29).

For example, the basic PHY uses the Institute of Electrical and
Electronics Engineers (IEEE) 802.15.4 radio. However, if a specific application would be better served using 802.11 or a more powerful radio to cover a longer distance, it is possible because the network layer protocol is PHY agnostic (see Figure 1, page 29).

If a supplier or user group would prefer using other radio technologies for particular industrial applications, ISA100.11a can adapt it to build a single network infrastructure for easy management. Wired Ethernet protocols are designed to work in applications in which larger data packets are necessary and power management is not as critical. ISA100.11a is designed more for applications in which devices require less bandwidth, and consequently, less networking overhead, but it interfaces seamlessly with existing Ethernet networks.

The ability to change a given layer as necessary helps future-proof ISA100.11a. This is especially important as the IoT will make it practical for industrial applications. ISA100.11a uses the same IPv6 address and leverages the Internet protocol User Datagram Protocol/Internet Protocol (UDP/IP). IPv6 with 6Lo Wireless Personal Area Network (WPAN) will likely be critical for parts of IoT deployments for the foreseeable future, and these work successfully right now with ISA100.11a.

In many respects, the IoT offers the highest potential for creating an overarching communication standard that can bridge many of the fragmented industrial application protocols. Those legacy standards will certainly persist, but it can provide a much higher level of unified networking connectivity using off-the-shelf technology. Those legacy standards will adapt or migrate on the Internet.

Because of growing cyber security threats, some understandably view anything connected to the Internet as a huge security threat. This is a valid concern, but developments resulting from the IoT offer methods that will help secure industrial networks. Because the design principle of ISA100.11a follows the ISO/OSI model, it supports not only hop-to-hop topology with a device-to-device level of...
security, but it also supports IP port-to-port with an application-to-application level of security. To a user, that means it gives flexibility to support different types of security functions based on their applications for today or in the future.

For example, a user may need to set multiple levels of security based on levels of access for operators. When an operator is logged in from the central control room, based on that location, he or she may be granted a high level of access that includes the ability to interact with or modify sensors in the field. When the same operator logs in from remote location, the user may want to reduce the degree of access. If that operator wants to log into the network using a personal iPad or other device allowed under the company’s bring-your-own-device policy, the application may request him or her to answer additional security questions before it grants full access or the system may limit access because it is a personal mobile device.

The cloud allows full control of your applications without the limitations of older technologies. With some sensors getting smarter with new functions, while others are simpler and even disposable, the ability to support security based on applications has become essential for future-proof networks.

One of the characteristics of ISA100.11a is its ability to convey information from other industrial protocols. Foundation fieldbus, Profinet, Modbus, HART, EtherNet/IP, DeviceNet and others can all be used. For example, adding an ISA100.11a wireless adapter to a HART flowmeter can send the process variable and diagnostic data just as if it were wired. The control system receiving the data does not notice the difference (see Figure 2, page 30).

Multiple protocols can be used in different parts of the plant within a single wireless network. When the information from the protocols that are being used reaches the backbone router, it can be sorted and delivered to the control system, just as originally sent. There is no need to convert it to one protocol.

While this capability may sound convenient, it will become far more important as the IoT develops. As many different protocols that are in place now, many more may be available in the future. Therefore, it is imperative that the wireless network can accommodate each of them for plant or enterprise applications.

IS ISA100.11A MORE THAN I NEED?

One of the benefits of ISA100.11a is that it can be as simple or complex as required. Other wireless protocols emphasize their simplicity, but it is simplicity at a cost of limitations because they often have no capabilities beyond their basic deployment strategy.

For example, a user might want to perform a simple installation of 10 or 15 devices in a monitoring application and need to decide between using wireless HART and ISA100.11a. Either approach can complete the job equally well, and appropriate devices are available for either system. So how is the right choice determined?

If it only applies to one type application, either can work. Both networks can be deployed with simple network architecture and a plug-and-play setup. The difference is how it will adapt to future additions and changes. In the future, the user might want to communicate with a network that uses Modbus or another protocol, or the network might grow in device count toward a different networking topology or new applications.

Does the user want to assign resources to manage multiple networks or deploy and manage one network in the field that can handle everything from slow monitoring to fast control functions? For flexibility with minimal management, it is best to select the more flexible network upfront, and that is ISA100.11a.

End users should think through the ways they might want to use a wireless network in the future. It may influence their decision of choosing a more flexible networking strategy that has room to grow.

Penny Chen, PhD, is principal systems architect at Yokogawa Global Strategic Marketing Center where she is responsible for technology standardization and wireless networking technologies for industry applications. She is vice-chair of ISA100 Wireless Compliance Institute (WCI), co-chair of ISA100.15 Wireless Backhaul Networks Working Group along with membership on numerous industry organizations. Her doctorate is in electrical engineering from Northwestern University. Chen may be reached at penny.chen@us.yokogawa.com.
Integrate wired and wireless securely and reliably with Yokogawa’s “Wireless Anywhere” Solution.

Considered best-in-class, Yokogawa’s wireless technology is fully open and interoperable with a flexible architecture to support small or large-scale plants. Use less hardware to cover longer distances, incorporate existing assets, and reduce maintenance costs without compromising transmission speeds or security.

Let us help you save money and improve production efficiency with a wireless solution customized for your needs.

Call 800-888-6400 to arrange a free consultation with a wireless expert.