CMC Report

Wireless Field Instrumentation

by Dick Caro, CEO CMC Associates

September 16, 2013

Use of new technologies for the process industries does not happen instantaneously, but moves gradually beginning with applications where that technology provides enough benefits to overcome the risk that it will not work or not work reliably. Many users will test the new technology on a few pilot installations, usually for non-critical processes. With success and sufficient economic incentive, the new technology will be specified for new plant construction in locations where vendor support is available. Eventually the new technology will be specified for greenfield new plant construction, major revamps/modernization projects, and become an industry norm. Foundation Fieldbus has followed this pattern with the base technology becoming a standard in 1996, and now (2013) is the industry norm for new plant construction and modernization in the continuous flow process industries such as petroleum refining, petrochemical manufacture, and chemical plants.

Like wired process control communications standards in 2000, today there are directly competing standards for wireless field instrumentation: IEC 62734 (ISA100.11a, ISA100 Wireless™) and IEC 62591 (WirelessHART®.) These two standards appear to be very similar because they are both based on the same IEEE 802.15.4 radio chip, but they are actually not that similar and they are not interoperable. WirelessHART was designed by the HART Communications Foundation specifically to transport HART data over a wireless network as simply as possible, and to be installed and managed with the familiar HART tools and methods. ISA100 Wireless was designed by an open standards organization with technical experts from more than 250 countries to be a wireless internet-based telecommunications protocol for process control data now and for applications not yet invented well into the future. It was designed to efficiently transport HART and practically any fieldbus data objects that use standard IEC 61804 (EDDL.)

One of the problems that is delaying the acceptance of wireless field instrumentation is that most new plant installations and major modernization projects are now using Foundation Fieldbus, a wired all-digital network of very intelligent field instruments. A wireless equivalent or version of Foundation Fieldbus H1 is not available, although both WirelessHART and ISA100 Wireless networks can exchange simple data from either wireless network through a ROM, Remote Operations Manager; a Fieldbus Foundation specified gateway. However, lack of a true wireless Foundation Fieldbus with the same intelligent but wireless field instruments is not available. Not yet tested by the Foundation is Foundation Fieldbus HSE working on Wi-Fi. There is no wireless version of Foundation Fieldbus HSE Linking Device offered or registered by any vendor.

Users are very concerned that there are effectively two competing wireless network standards being supported by the major instrument companies. Of even greater concern is that often that the wireless network standard used by their favorite field instrument supplier is not compatible with the wireless network standard support by their favorite DCS supplier. Users look to their suppliers to solve such problems; vendors must bring solutions to their customers – not problems. Lack of a single wireless network ***norm***, or generally accepted industry practice, has hampered user acceptance of wireless field instrumentation except in a few areas where the benefits of wireless are overwhelming, and applications are not for fast control loops.

Comparing ISA100 Wireless to WirelessHART

What are the features of ISA100 Wireless that make it the best choice as a wireless network for a new application? Remembering that WirelessHART was designed for one application – connecting "stranded HART instruments to a control system" – ISA100 Wireless was designed explicitly for communications with smart process control field instrumentation, and for easy configuration to a specific set of performance requirements. There are many configurable choices possible in the preparation of an ISA100 Wireless device that are specified in the standard. The set of default values for these choices, which appears in the standard, is called the ***Router Profile***, which has been optimized for the secure mesh networking of process control field instrumentation. Therefore, manufacturers of wireless process control field instrumentation do not need to reconfigure any of the options of this standard. Manufacturers of other wireless devices may have specific cost, performance, or security needs may use the ***I/O Profile*** also specified in the standard for low cost devices, or may require adjustments to some other ISA100 Wireless attributes to customize it to their needs. Customized versions of ISA100 Wireless are guaranteed and compliance tested to interoperate with field instruments conforming to the router profile, but adjustment of the ISA100 Wireless profile is not something that users need to worry about.

During the design of ISA100 Wireless the same basic set of requirements were used that were also used in the design of Foundation Fieldbus. Essential to the architecture of both ISA100 Wireless and Foundation Fieldbus is peer-to-peer transfer of data without requiring a host or gateway relay. Both ISA100 Wireless and Foundation Fieldbus devices have a synchronized real-time clock to support the scheduling of objects resident in intelligent network devices. ISA100 Wireless devices have a synchronized real-time clock accurate to ± 1.0 ms. This clock precision is also necessary to support a power industry user requirement for trip sequence analysis.

For example, most process control field instrumentation sampled once per second (1 Hz) is adequate for monitoring and non-critical closed loop control. Both ISA100 Wireless and WirelessHART can deliver this data to a DCS doing such control. However, when flow control that must be faster than once per second is to be configured, only ISA100 Wireless can deliver data with a synchronous response more often than once per second. Typical distillation column flow control requires data to be scanned 2 to 4 times per second. To deliver this type of performance, the data collection times for the flow transmitters should be configured with minimal network meshing to guarantee synchronous sample times. ISA100 Wireless explicitly supports a maximum latency of 100ms and the field backbone routers necessary to enable data to reach the controller in a single hop without the non-deterministic delays of a mesh network.

When applications are even more demanding than 4 Hz flow control, it may become necessary for the instrument manufacturer to configure the ISA100 Wireless Data Link Layer to allow processing up to 12 Hz. The advantage of ISA100 Wireless is that the instrument manufacturer has this option available without needing to change the protocol, or to create new function blocks that are not supported by the Fieldbus Foundation interoperability testing.

Applications such as analytical field instrumentation may require transmission of long data sets that cannot fit into the short messages that are necessary with a 10 ms slot time. The network segment that includes the wireless analyzers may use the ISA100 Wireless features to allow longer messages. The application can segment the message such that the data payload is less than about 90 bytes, allowing for the protocol overhead. ISA100 Wireless supports reassembly of segmented long messages. WirelessHART with its fixed 10 ms slot time and simplistic Network Layer is just not suitable for the efficient transfer of long messages, and the responsibility to segment and reassemble messages is left to the application. The issue of leaving it outside the standard and conformance testing is that it will make it more difficult, if not impossible, for multiple manufacturers to develop interoperable products.

One of the features of ISA100 Wireless is tunneling, which gives the ability to transport any data stream across the ISA100 Wireless network, between a field device and the gateway even if the device uses a digital protocol quite different from ISA100 Wireless. As a preferred alternative approach, the object-oriented ISA100 Wireless Application Layer has enabled wireless adapters to form simple valid messages using the ISA100 Wireless object model and services. The device may have ISA100 Wireless built-in or an ISA100 Wireless adapter may be mounted on the device to receive messages in the native format of the device such as Modbus, DeviceNet, ControlNet, EtherNet/IP, PROFIBUS, HART, etc. and encapsulate the message for transport over the ISA100 Wireless network to the gateway. Most applications have used the ISA100 Wireless object model to pass data previously expressed in the above native protocols, and have not needed to use the tunneling features. Software in the gateway can then route the data contained in the original message to an intended receiver. Since the ISA100 Wireless adapter has an IP address, external systems may route messages to the field device at that IP address much as they can interact with any other IP device.

One of the future applications for ISA100 Wireless is to serve as the field network connection for devices hosting web pages. While there are currently no web page hosting applications for field devices, the ISA100 Wireless infrastructure enables such applications. Similarly, a smart device may run the protocol of Foundation Fieldbus HSE which is also UDP/IP-based, and the ISA100 Wireless network will be able to synchronously exchange messages/data with any other device running that same protocol using the publish/subscribe features of ISA100 Wireless that are compatible with those of Foundation Fieldbus.

Users and field instrumentation suppliers have great concerns over security of wireless networks. To meet this need, both ISA100 Wireless and WirelessHART encrypt every message using the built-in AES-128 encryption of the IEEE 802.15.4 radio chip. Security is managed on ISA100 Wireless networks using a rotating encryption key, meaning that the security key is changed on a periodic scheduled basis. During the time it would require for an intruder to hack the network encryption key, a new key is automatically generated and distributed preventing actual intrusions.

WirelessHART protocol limits the encryption and checking of message integrity to only one of the eight possible choices available in the IEEE 802.15.4 standard while ISA100 Wireless makes six possible combinations available. Both standards default to using a 32-bit message integrity code, but ISA100 Wireless also offers a configurable 64-bit or 128-bit message integrity code, providing a higher level of security that is sometimes a requirement by government and quasi-government agencies.

During development of ISA100 Wireless, users declared the need for a secure method to commission or provision a new field device without the need for a specialized handheld device, or physical access to the instrument. ISA100 Wireless has an elegant secure over-the-air method to provision a new device and allow it to seamlessly join into the network using PKI, Public Key Infrastructure. The security is based on two factors: a white-list identifying the devices to be provisioned must be installed in the network prior to provisioning, and the user must have possession of a corresponding 283-bit certificate. The white-list and certificate are installed to the Network Security Manager, using files created by the manufacturer and is supplied to the user on transportable media (CD, DVD, USB flash memory, SD card, etc.) and eliminate the need for a device provisioning operation by the user. When the wireless instrument is installed in the field, it will automatically respond to the network requests to join and then become part of the operating network. The reason this process is secure is the use of a standard 283-bit public/private key method that does not expose any unencrypted joining keys over the air, and does not rely on insecure operational procedures to distribute secret keys to a host system or through a handheld terminal. WirelessHART simply uses a physically attached HART handheld terminal to enter the network address and the security key; a similar interoperable mechanism is also available to ISA100 Wireless users through an infrared port.

Both WirelessHART and ISA100 Wireless support mesh networking, which is an excellent method to extend the distance the network can cover, to access devices that are shielded by buildings from direct line of sight, and to provide a resilient path for data transfer to increase reliability. However, when meshing is used in a synchronous control loop, only ISA100 Wireless can limit the depth of the mesh and simultaneously provide a fully resilient data path using ***duocast*** technology. Limiting the depth of the network requires the location of field routers reachable in a single hop since multilevel meshing can cause indeterminate delays in signals reaching their intended destination. Reliable networking by using resiliency requires that the information sent on the resilient data paths be identical. The ISA100 Wireless feature that assures that the data sent on resilient data paths are identical is the ***duocast*** feature built into ISA100 Wireless technology. WirelessHART has the ability to send data to multiple routes on its mesh, but not in the same slot time.

In configurations where a device needs to access data from a neighbor in a mesh network, long latencies can be involved in transmitting data through the mesh to and from a DCS. To address this, ISA100 Wireless supports direct communication between devices in proximity to each other. This peer-to-peer relationship involves direct wireless communication, operating in conjunction with an application object model that can execute control-in-the-field (CiF) logic remotely without DCS involvement, similar to the operation of CiF in Foundation Fieldbus.

Manufacturer's Dilemma

Manufacturers of process control field instrumentation face a dilemma in choosing which wireless network to support. Their choices are the following:

1. Do not support wireless field instrumentation,
2. Only support ISA100 Wireless,
3. Only support WirelessHART,
4. Build two product lines one supporting ISA100 Wireless and the other supporting WirelessHART,
5. Build dual-boot devices that can be configured at installation to support either standard, or
6. Support another standard such as WIA-PA, ZigBee, Bluetooth, or a proprietary network.

Analysis

1. and 6. Not offering a wireless network field instrumentation, supporting another standard, or building a proprietary network is against the interests of *all* of their potential customers who want the benefits of *standard* wireless field instrumentation. Both WirelessHART and ISA100 Wireless have field-proven strong security needed to assure users of both privacy and intrusion protection.

4. and 5. Supporting both ISA100 Wireless and WirelessHART with two product lines would meet the needs of their potential wireless customers, but at much higher development, maintenance, and product cost. Building a "dual-boot" device that contains both protocols or can be initialized with either protocol also meets some of the needs of potential wireless customers, but with much greater complexity during installation and maintenance.

2. and 3. Supporting either standard alone could greatly reduce their potential market size if the network chosen does not become the wireless network norm.

Answering the Dilemma and Developing the Network Norm

While instrumentation suppliers might be drawn to supporting both networks via the dual-boot method (option 5), this does not achieve the long term establishment of an industry norm, which has been at the root of requests by all end users. ISA100 Wireless can be the core of future wireless industrial networking technology in much the same way as Ethernet TCP/IP and Wi-Fi have become the network norms for IT (Information Technology) networks. ISA100 Wireless is totally built upon well-established network standards. This means that ISA100 Wireless is an application-independent internet-based telecommunications network designed for the critical and non-critical industrial automation environment, just like Ethernet TCP/IP and Wi-Fi are application-independent internet-based telecommunications for business networks. As long as the applications are built to use common network standards based on IP protocol, they can be transported across any standard network, such as ISA100 Wireless, with adequate bandwidth for the task, and suitably adapted to the particular needs of the automation industry.

Also, like Ethernet TCP/IP, use of ISA100 Wireless is independent of the network hardware. As microprocessors and communications semiconductors evolve, and frequency assignments change, ISA100 Wireless will be able to make these transitions without requiring any changes in the applications that are carried on this network technology. If the past is a good predictor of future development, future wireless network technology is destined to get less expensive and much faster. ISA100 Wireless will naturally be able to fit right onto the new wave of wireless network technology as it becomes commercially available.

Manufacturers of process control equipment are concerned primarily with meeting customer needs and in reducing product cost to enable competitive pricing. Part of the customer needs are to solve short term problems, but they also would like to develop a long term architecture for their process automation needs. WirelessHART has been, due to its earlier product introduction, available to solve the short term needs, but several end user organizations are now recognizing the fact that ISA100 Wireless alone meets the needs of a long term wireless architecture.

Conclusions

Early users of wireless process control instrumentation had application requirements that centered only on obtaining process data from locations that were either too costly or impossible to wire. Most of these applications can be satisfied with either WirelessHART or ISA100 Wireless, and have now been field-proven and accomplished their goals.

Users that decide to use WirelessHART as their plant wireless network are committing themselves to a control system architecture in which there is little intelligence in the field devices. Their DCS must do all the work of signal processing and closed loop control. ISA100 Wireless can certainly connect to those same HART field devices, but its open architecture allows synchronous two-way wireless data transfer with full function (intelligent) field devices when they are ready, *without changes in the basic network*. And we know that there is a strong trend toward Foundation Fieldbus with its intelligent field devices and highly synchronous data transfers.

While the early efforts have now resulted in two widely used standards, users still want to establish a single wireless network norm suitable for a wide range of applications well beyond acquisition of remote data points. Leading users have recognized that the wireless network norm must not only be an international standard, but must be suitable for demanding applications such as wireless Foundation Fieldbus and Internet web servers in field instrumentation. Only a highly secure IP-based protocol can do these, and only ISA100 Wireless can meet these needs.