INDUSTRIAL WIRELESS NETWORKS

COMPARING THE STANDARDS

PART 2

Glenn Johnson, Editor

In Part 1 of this article, we reviewed the history of wireless sensor networks (WSNs) and defined the common standards used in industrial wireless networks. In this part we compare more closely the two prevalent wireless mesh network standards designed for use in process plants: WirelessHART and ISA100.11a.

Although WirelessHART[1] and ISA100.11a[2] are in many ways the same, being both based on IEEE 802.15.4[3] at the PHY and MAC layers — and designed effectively for the same purpose — there are still some key technical differences between the two standards. Those differences are due to fundamental differences in design philosophy, one opting for ease of deployment and multivendor compatibility, the other choosing flexibility and scalability as key design features.

Network architecture

ISA100.11a uses backbone routers for bridging subnets. Backbone routers limit the throughput into and out of a single subnet to the throughput of one radio, but backbone routers can be used in parallel to create a very large wireless network. Since addressing is based on IPv6, there is really no practical address limitation. WirelessHART uses access points that can be used in parallel to merge subnets into a very large address space. Since the short address used in the WSN is an unsigned integer, however, addresses are limited to 30,000 in a single WirelessHART network.

Frequency hopping

Both WirelessHART and ISA100-11a use the radio interface in the 2.4 GHz ISM band as described in IEEE 802.15.4 — divided into 16 channels, using a 250 Kbps data transmission rate.

The communication reliability is increased through frequency diversity. Channel hopping in WirelessHART is dictated by the standard, meaning that devices from different manufacturers are interoperable by design. In ISA100.11a, there are three different defined channel hopping algorithms, and the user must specify which one is to be used. Users purchasing ISA100.11a devices will need to ensure that the purchased devices support channel-hopping schemes that are compatible with one another.

In both WirelessHART and ISA100.11a, clear channel assessment (CCA) and channel blacklisting are used to combat the influence from other wireless networks. WirelessHART employs manual channel blacklisting, where a network operator must manually configure which channels are available and which channels are blocked. ISA100.11a has an adaptive blacklisting mechanism, where each device in a network may autonomously blacklist channels that suffer from noise or interference. ISA100.11 also defines four different CCA modes, where modes 1-3 are defined by IEEE 802.15.4:

1. **No CCA:** CCA is disabled, and not conducted prior to transmission.
2. **Energy above Threshold:** Reports a busy channel upon detecting energy above a configurable threshold.
3. **Carrier Sense Only:** Reports a busy medium if a signal compliant with IEEE 802.15.4 is detected.
4. **Carrier Sense with Energy above Threshold:** CCA reports a busy medium using a logical combination of Modes 1 and 2.

WirelessHART, on the other hand, has fixed its CCA mechanism to mode 2.

With the correct configuration, ISA100.11a should be better at handling coexistence with Wi-Fi networks, while WirelessHART will only listen for activity from other IEEE 802.15.4 networks.

TDMA

Both WirelessHART and ISA100.11a implement time diversity through TDMA. The main difference is that WirelessHART uses a fixed 10 ms timeslot, whereas in ISA100.11a it is configurable between 10 and

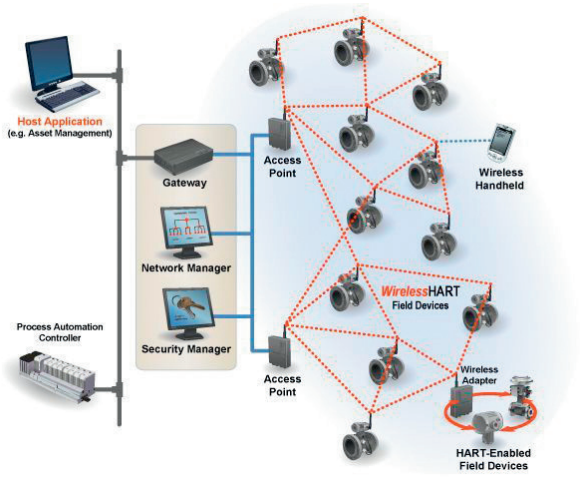

Figure 1: A WirelessHART network: Mesh routing is performed at the network layer by the access points. (Source: FieldComm Group)

14 ms. This means that users will need to ensure that all ISA100.11a devices in a given network support time slot lengths compatible with all other devices in the network.

Addressing and mesh networking

Both WirelessHART and ISA100.11a use an IEEE 802.15.4 mesh network. The routes are configured by the network manager based on information received from the devices so that redundant routes are continually updated based on the spectrum condition. The end-to-end routing and addressing in both cases is performed at the network layer; however, there are some differences in relation to the node-to-node mesh routing.

For addressing, WirelessHART uses an 8-byte local address system defined by the WirelessHART standard and no IP addressing. ISA100.11a, on the other hand, offers 6LoWPAN[4], which specifies IPv6, therefore allowing IP connectivity between devices and allowing 128-bit addresses as an option. For this reason, ISA100.11a offers the possibility of considerably higher mesh network scalability. ISA100.11a also specifies two other addressing schemes, and so users must not only configure this, but also be sure that all devices support the method of choice. Some users may also see IP addressing in the WSN network as being more open to security vulnerabilities.

For WirelessHART, the network layer performs all the routing functions within the mesh network. This layer carries the route tables to route communications through the mesh using graph routes. Interfacing with wired networks is performed at the wireless access point, which acts as a gateway between the wireless mesh and a wired HART-over-IP backbone. The transport layer above provides the network interface to the applications, providing the end-to-end communication, with acknowledgements so the originating device can retransmit any lost packets.

In ISA100.11a, the network layer provides for end-to-end routing using 6LoWPAN. It is possible for server/client pairs to generate IPv6 packets which are then forwarded through 6LoWPAN edge backbone routers to 6LoWPAN-enabled ISA100.11a devices; however, the routing in the mesh (hop-to-hop) happens in the data link layer using graph routing in a process known as 'mesh-under'. The IPv6 packets are fragmented and reassembly is performed in the 6LoWPAN adaptation layer, so IPv6 itself is not actually used in the wireless network.

Routing optional

In the case of WirelessHART, there are no design options — all devices must support routing — although the end user can choose to disable routing on a specific device. For ISA100.11a, routing support is optional, which means that it is feasible that a network could be built with entirely no mesh routing, losing all the advantages. If non-routing devices are to be deployed, considerably more careful site planning and testing must be carried out. This also means that both routing and non-routing versions of a device may need to be stocked as spares.

Application flexibility

WirelessHART and ISA100.11a are inherently different regarding the operational flexibility and configuration possibilities — and this is the fundamental difference in their design philosophies.

WirelessHART is a relatively 'simple' specification with very few optional or configurable parameters. ISA100.11a, on the other hand, is a complex specification with many configurable and optional parameters found in different stack layers. These features can be seen as both strengths and weaknesses depending on the specific application requirements.

Being an extension of the HART Specification[5], designed simply to route HART commands and data to and from wireless devices, WirelessHART has a relatively fixed design approach. The benefit of this is that practically all WirelessHART devices will have identical network behaviour, regardless of the implementation choices made by the equipment vendor, which should easily facilitate interoperability between multiple manufacturers. This naturally comes at the cost of a lack of possibility to adapt and tailor the device and network to specific requirements, or to support other fieldbus technologies. That being said, the ARC Advisory Group in 2012 published data to indicate that of the nearly 75 million field devices installed worldwide, nearly 50% were HART devices — more than all the other fieldbus technologies combined.

ISA100.11a, on the other hand, is a complex specification with many configurable and optional parameters found in different stack layers. The wide range of optional and configurable parameters in ISA100.11a allows for greater flexibility, but it may lead to interoperability issues

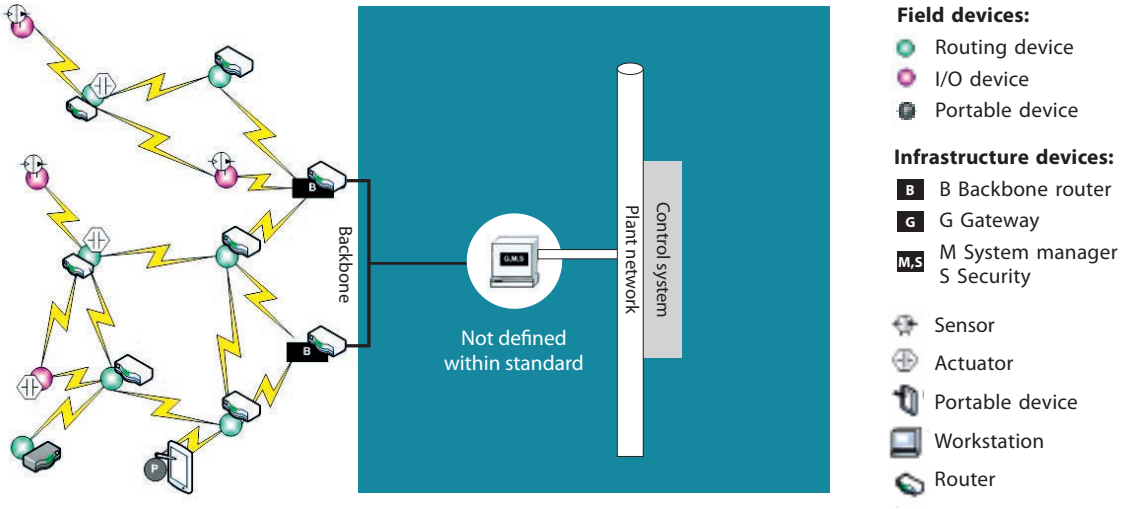

Figure 2: An ISA100.11a network: Mesh routing is performed at the DLL and IPv6 routing must be handled by the backbone routers/gateways. (Source: Yokogawa)

if different vendors choose to implement different features of the standard. ISA100.11a therefore defines application profiles — cross-layer specifications that define which options are mandatory in the different protocol layers.

Supported industrial protocols

Since, as stated above, WirelessHART is a wireless extension of the wired HART specification, all information and data in a WirelessHART network must be transmitted in the shape of HART Commands. At the OSI Application Layer, well-known HART features are readily available, supporting all the many control systems, configuration and management tools that are well established in the marketplace.

The ISA100.11a application layer is object oriented and implements tunnelling features that allow devices to encapsulate foreign protocols and transport them through the network. However, no specific functions are published, and only the system management interface is specified. Vendors must define their own application profiles to support their products over the network. As a result, most ISA100-11a implementations would involve single-vendor systems — that is, the software and all hardware devices would be supplied by a single vendor to ensure interoperability.

Security

When assessing security mechanisms, the criteria that must be considered are the confidentiality of information, the integrity of that information, the authentication of communication devices and the availability of information.

Confidentiality

Ensuring confidentiality involves making sure that only authorised members of the network can have access to the information. Both WirelessHART and ISA100-11a utilise AES-128 encryption with different key mechanisms at both the data link layer (hop-to-hop) and the transport layer (end-to-end). That is, each hop through the network is encrypted with a key, and the overall communication payload between end nodes is encrypted with a separate key.

Integrity

The integrity of the transmissions is based on mechanisms inherent to the IEEE 802.15.4 standard. At the data link layer each message includes a message integrity code (MIC) that is added to the data, which ensures the integrity of the entire MAC frame including the payload. An algorithm at the receiving node uses the MIC to determine if the data has been corrupted or altered by an attacker.

The ISA100-11a standard adds additional security to protect the integrity of the communication by using a timestamp for each communication and using it to construct a 'nounce' — a one-time arbitrary number to sign the end-to-end communication. The receiving node checks the nounce, and if the packet was created outside a valid time interval the packet will be discarded, this adding an extra level of protection against injection and impersonation.

Authentication of devices

Devices that are to join the network must create a join request, which is sent to the network manager and security manager devices, that will verify the credentials of the request, forwarding a join response to the router that the device is attempting to connect with. Both protocols use this mechanism; however, WirelessHART additionally uses a separate join key to authenticate the new device.

Since both standards use a separate node to be responsible for keeping track of the devices in the network, the chance of a successful node replication attack is low.

Availability

Availability can be threatened by wireless interference. As mentioned previously, both WirelessHART and ISA100.11a use channel hopping and channel blacklisting to mitigate the effect of continuous or intermittent interference. However, neither protocol at this time provides a mechanism to avoid deliberate denial of service through collision attacks or join request flooding, although warning may be received by mechanisms to detect excessive retransmissions.

Both WirelessHART and ISA100.11a rely on a centralised security manager for the authentication of new devices and the generation and management of security keys throughout the lifetime of the network. This means that the loss of the security manager will cause the loss of security mechanisms in the network, and so can be seen as a single point of failure. Newer releases of WirelessHART and ISA100.11a networks are offering redundant network and security manager solutions with automatic and transparent handover from the primary to the secondary system in case of failure.

Security configuration differences

While for the most part WirelessHART and ISA100-11a use the same security protection mechanisms as described above, there is one

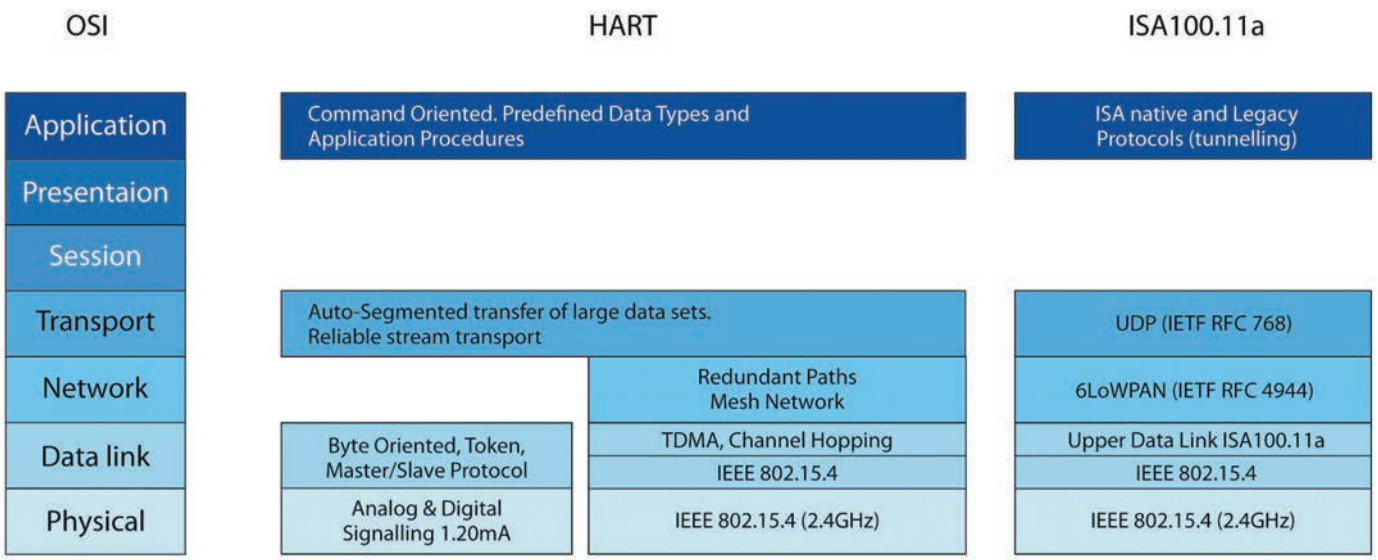

Figure 3: Industrial wireless protocol stacks.

major difference in how they are implemented: WirelessHART devices from all manufacturers are forced to be compatible by the standard, whereas many security features are optional for ISA100-11a, in keeping with its flexible design principles.

Because security algorithms require additional processing time, memory and power, making them mandatory means that devices that may not require strict security policies cannot disable them in WirelessHART to achieve benefits such as extended battery life. However, users implementing ISA100-11a must be aware that different vendors may choose to not implement all the security options, potentially introducing undesired security risks.

Conclusion

This two-part article has covered most of the architectural differences and standards involved with industrial wireless networks, focusing mainly on architecture considerations. Other additional features of these protocols — for example, quality of service (QoS) or their support for larger data transfers such as device firmware updates — have not been described for the sake of brevity, but information on these can be found in the standards or from wireless device vendors.

The two significant standards for industrial wireless networks are WirelessHART and ISA100.11a. While ZigBee (or more specifically ZigBee Pro) has been put forward as the industrial wireless standard, it lacks some of the resilience and protocol support that the main contenders offer, and as a result has not been a serious contender for use in larger industrial process systems, such as those found in the oil and gas industry.

WirelessHART and ISA100.11a, while both being based on the same basic wireless sensor network (WSN) technology of IEEE 802.15.4, have fundamental differences in design philosophy, one opting for ease of deployment and multivendor compatibility, the other choosing flexibility and scalability as key design features. Both provide network resilience for harsh industrial environments and both provide extensive security features — as much as can be provided for currently in wireless systems. However, WirelessHART enjoys the greatest market share for two main reasons:

- The extensive existing deployment of HART-compatible devices (around 50% of all field devices) and therefore direct legacy compatibility with existing systems.
- The inherent fixed capabilities, with few options, that ensure device compatibility between different vendors.

These benefits come at the cost of scalability, flexibility and support for non-HART protocols.

With ISA100.11a, the designers have opted to develop a standard that allows potentially any fieldbus network to be operated over a resilient mesh wireless network but have not provided the direct support for these protocols in the standard. This leaves it up to vendors to build their own software and hardware to support whatever they require. Utilising IPv6 as an addressing scheme supports greater mesh network scalability than WirelessHART, and extensive deployment options and feature choices make it far more flexible, but these same benefits introduce potentially greater deployment costs, because the network must be designed far more carefully, and choices of vendors may be affected by interoperability considerations. ISA100.11a, in its current form, is more suited to a single-vendor deployment.

References

1. International Electrotechnical Commission (IEC), 2010, *Industrial Communication Networks – Wireless Communication Network and Communication Profiles – WirelessHART*, IEC 62591.
2. International Society of Automation, 2009, *Wireless Systems for Industrial Automation: Process Control and Related Applications*, ISA100.11a-2009.
3. Institution of Electrical and Electronics Engineers, 2006, *IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and Metropolitan networks – Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Computer Society.
4. Internet Engineering Task Force (IETF), 2007, *Request For Comments (RFC) 4911 – IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals.*
5. HART Communication Foundation, 2007, *HART Field Communication Protocol Specification, Revision 7.0.*