STIG PETERSEN and SIMON CARLSEN

# WirelessHART Versus ISA100.11a

## *The Format War Hits the Factory Floor*

The first decade of the new millennium has been a stage for the rapid development of wireless communication technologies for low-cost, low-power wireless solutions capable of robust and reliable communication [1]. IEEE Standard 802.15.4 for low-rate wireless personal area networks (WPANs) [2] has been the enabling technology for numerous applications within the field of wireless sensor networks (WSNs) [3], and more recently, wireless instrumentation. Although WSNs quickly found their way into a wide variety of applications, the adoption of wireless technology in the process automation and manufacturing industries has been slow. None of the industrial solutions based on standards such as IEEE 802.11 [4], Bluetooth [5], ZigBee [6], and Internet Protocol version 6 (IPv6) over low-power wireless personal area networks (6LoWPAN) [7] have yet to achieve a breakthrough as

*Digital Object Identifier 10.1109/MIE.2011.943023*
*Date of publication: 9 December 2011*

1932-4529/11/$26.00©2011IEEE

a widely adopted wireless solution for industrial applications. A major reason for this is believed to be the lack of an open, international standard fulfilling the industrial requirements [8]. This changed in September 2007, when the Highway Addressable Remote Transducer (HART) Communication Foundation (HCF) released the HART Field Communication Protocol Specification, Revision 7.0, which included the definition of a wireless interface to field devices, referred to as WirelessHART [9].

Parallel to the HCF's development of WirelessHART, the International Society of Automation (ISA) initiated work on a family of standards defining wireless systems for industrial automation and control applications. The first standard to emerge was ISA100.11a [10], which was ratified as an ISA standard in September 2009. ISA100.11a aims to provide secure and reliable wireless communication for noncritical monitoring and control applications.

As a result, the process automation and manufacturing industries are now faced with two independent and competing standards specifically designed for wireless field instruments, each supported by different industry players. This format war on the factory floor has many similarities to the historical Betamax versus video home system (VHS) struggle of the 1970s, and the more recent battle between the Bluray and high-definition digital versatile disk (HD-DVD) formats. Unfortunately, it is also a continuation of the situation found today with the available standards for wired fieldbuses and industrial Ethernet (a few examples of these standards are Modbus [11], Foundation Fieldbus [11], and Profibus [11]). The process and automation industry as a whole would benefit more from having one global, wireless standard, but with the current situation, this is unlikely to happen in the near future.

The main contribution of this article is the theoretical comparison of WirelessHART and ISA100.11a, both from a technical and a systematical point of view. With two available standards for industrial wireless instrumentation, it is important for the end users to be able to understand the inherent strengths and weaknesses of the two and how these influence their suitability for different applications.

## System Overview

A typical WirelessHART or ISA100.11a installation consists of a group of components, both physical devices and software modules, each capable of fulfilling one or more defined functions.

The following devices and components are associated with a WirelessHART network [9]:

- *Field Device*: A field instrument with integrated wireless communication.
- *Adapter*: A wireless communication module that connects to wired HART field devices, providing them with WirelessHART capabilities.
- *Handheld*: A portable WirelessHART computer used for configuration, diagnostics, and calibration of field devices.
- *Gateway*: A network access point that connects the WirelessHART network to a plant automation network, allowing the data to flow between the two.
- *Network Manager*: An application that manages the WirelessHART network and its devices.
- *Security Manager*: An application that is responsible for generating, storing, and managing join, network, and session keys.

For most WirelessHART implementations, the gateway, network manager, and security manager reside in the same physical, embedded device, usually referred to as either the gateway or network manager by the vendors. However, for scenarios where redundancy or extended coverage is needed, the standard allows for multiple gateways to be managed by a single network manager and security manager. In this article, the definitions will be used according to the WirelessHART specification, as described earlier.

In ISA100.11a, a set of roles are defined to describe the functions and capabilities of a device. An ISA100.11a device shall hold one or more of these roles [10]:

- *Input/Output (I/O)*: A device that provides data (sensor) to or uses data (actuator) from other devices.
- *Router*: A device that is capable of routing data from other devices in the network.
- *Provisioning*: A device that is capable of provisioning other devices, enabling them to join a specific network.
- *Backbone Router*: A device that is capable of routing data to/from a backbone network.
- *Gateway*: A device that provides an interface between the wireless and the plant network or directly to an end application on a plant network.
- *System Manager*: An application that governs the network, network devices, and network communications.
- *Security Manager*: An application that, in conjunction with the system manager, provides a secure system operation.
- *System Time Source*: A device that is responsible for maintaining the master time source for the system.

As can be seen from the definitions of devices and roles in WirelessHART and ISA100.11a, there is a fundamental difference at the field instrument level that influences the possible network topologies in the two standards. In wireless networks, typical network topologies are either star networks, mesh networks, or a combination of the two, called star-mesh networks. The three different network topologies are illustrated in Figure 1.

In WirelessHART, all field devices and adapters are routers capable of forwarding packets to and from other devices in the network, enabling a mesh network topology. Figure 2 shows a typical WirelessHART network and the mesh topology created by the field devices and adapters. In addition, all devices are capable of provisioning other devices to join the network.

For ISA100.11a, the sensor and actuator roles (I/O) are separated from the router role. This enables ISA100.11a field instruments to be defined either as end nodes with no routing capability and/or as router nodes with routing capability. As a result, an ISA100.11a network can employ star, star-mesh, or mesh topologies depending on the roles of the devices present in the network. A typical ISA100.11a network with a star-mesh topology is illustrated in Figure 3. The backbone network represents a wired network connecting the different ISA100.11a devices and components together. For configurations with only one backbone router, the gateway, system manager, security manager, and backbone router can reside in the same physical device. Unlike WirelessHART, the separate definition of the provisioning role means that not all devices in an ISA100.11a network are necessarily capable of provisioning other devices to join the network.

When it comes to network scalability, the technical limit on how many devices can participate in a network is governed by the addressing space, which for both WirelessHART and ISA100.11a is capable of handling thousands of devices. However, the practical limit on the number of devices in a network is a different matter. For large mesh networks, both network latency and individual device power consumption will increase to accommodate all the communication links in the network. Typically, in a mesh network, choke points with high traffic loads will arise at one or more of the devices, which communicate directly with the gateway (such as devices A, B, F, and G in Figures 2 and 3). These devices have to forward packets to the gateway from most of the other devices in the network, and for large networks, this can result in a substantial increase in data traffic, and hence, their power consumption will increase accordingly. Furthermore, the maximum achievable sensor data update rate is proportional to the number of devices in the network, as a high update rate

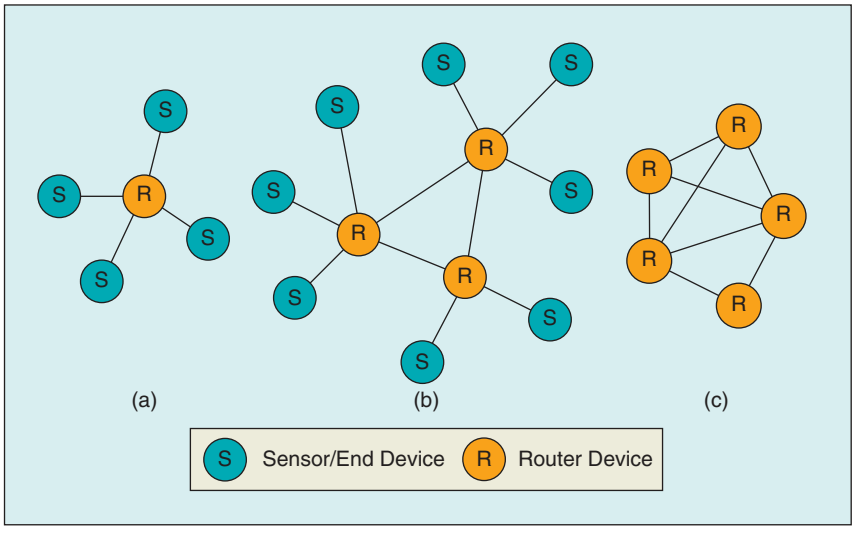


FIGURE 1 – Examples of network topologies: (a) star, (b) star mesh, and (c) mesh.

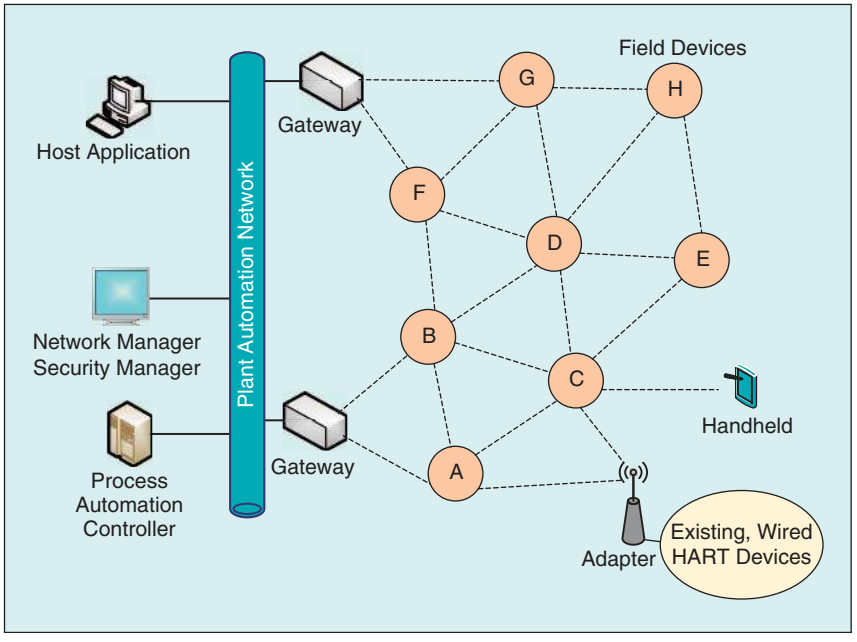


FIGURE 2 – Example of a typical WirelessHART network [9]. (Figure based on Figure 21 of [26].)

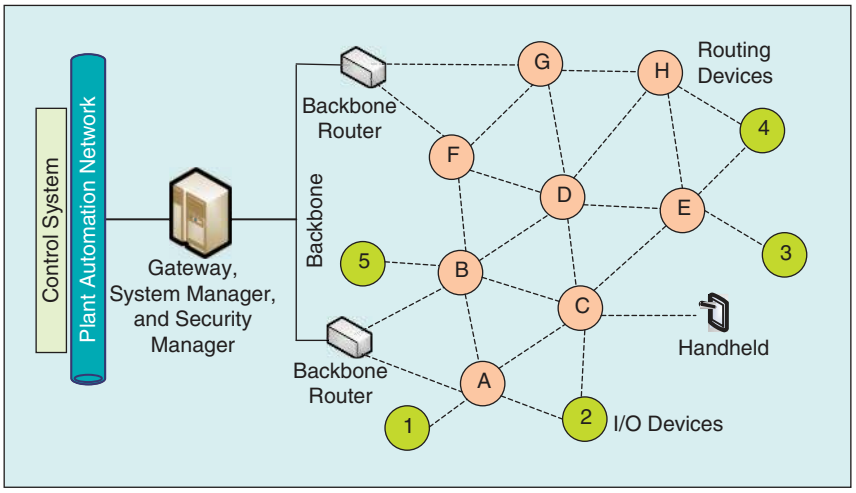


FIGURE 3 – Example of a typical ISA100.11a network. (Figure based on Figure 1 of [10].)

generates more network traffic than a slower update rate.

These potential issues represent one of the reasons why manufacturers of currently available WirelessHART and ISA100.11a equipment have a limit on the number of devices allowed in a network, typically in the order of 50–100.

## Communication Protocols

For communication protocols and standards, stacks are used as a layered and abstract description of the network protocol design. A stack consists of several layers, where each layer is a collection of functions related to the specific task of the layer. A layer is responsible for providing information and services to the layer above it, and it receives information and services from the layer below it. This information and service exchange is performed in a well-defined and standardized message-exchange format.

Both WirelessHART and ISA100.11a use a simplified version of the seven-layered open systems interconnection (OSI) basic reference model [12], as illustrated in Figure 4. The following sections give an introduction to, as well as a comparison of, the protocol layers of WirelessHART and ISA100.11a.

### *Physical Layer*

The physical layer (PHY) handles functions related to the radio frequency (RF) transceiver, and it is the interface to the physical medium where the communication occurs. It is responsible for the transmission and reception of raw data packets and provides control mechanisms for selecting operating channels, performing clear channel assessment (CCA), and RF energy detection. Both WirelessHART and ISA100.11a implement the IEEE Standard 802.15.4 PHY [2], with a few minor modifications.

First of all, for both standards, the operation is defined only in the 2.4-GHz band, using Channels 11–25, as defined by IEEE Standard 802.15.4. Channel 26 is not included in WirelessHART, since it is not legal to use in some countries, while in ISA100.11a, Channel 26 is defined as optional. Each channel uses a bandwidth of 2 MHz, and the channels are spaced 5-MHz apart.

For both WirelessHART and ISA100.11a, a combination of direct sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS) is used as modulation technique. DSSS, which is employed by IEEE Standard 802.15.4, divides the information signal into small fragments that are spread across the available frequency channel. With FHSS, the channel that is selected for data transmission will alternate in a pseudorandom sequence. The channel change happens on a packet level, i.e., the transmission of a packet will take place on one channel, while the next packet transmission will be on another channel. A combination with offset-quadrature phase shift keying (O-QPSK) modulation allows for a raw bit rate of 250 kb/s. The maximum transmitted power is limited to 10 mW (=10 dBm), giving most devices a range of up to 100 m in outdoor conditions with direct line of sight, depending on the sensitivity of the RF receiver.

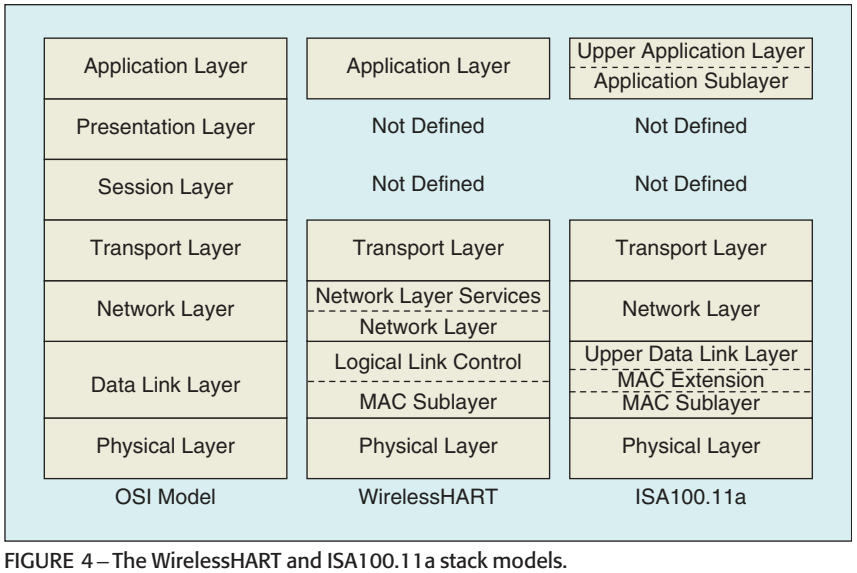


FIGURE 4 – The WirelessHART and ISA100.11a stack models.

### *Data Link Layer*

The data link layer (DLL) traditionally provides access to the radio channel and is responsible for radio synchronization. It handles acknowledgment frames, association/disassociation with other radio devices, and security control. Its main task is to provide a reliable link between the two peer DLL entities.

For WirelessHART, the DLL is divided into a logical link control (LLC) layer and a medium access control (MAC) sublayer. The scope of the WirelessHART DLL is communication on a one-hop level, and any responsibilities to the network beyond the device's neighbors are allocated to the WirelessHART network layer (NL).

ISA100.11a divides the DLL into a MAC sublayer, a MAC extension, and an upper DLL. The MAC sublayer is a subset of IEEE Standard 802.15.4 MAC [2], with the main responsibility of sending and receiving individual data frames. The MAC extension includes additional features not supported by IEEE Standard 802.15.4 MAC, mainly concerning changes to the carrier sense multiple access with collision avoidance (CSMA-CA) mechanisms by including additional spatial, frequency, and time diversity. The upper DLL handles link and mesh aspects above the MAC level, and it is responsible for routing within a DL subnet. Unlike WirelessHART, and contrary to the OSI-model definition of DLLs, this means that the mesh routing is handled by the ISA100.11a DLL. A DL subnet comprises one or more groups of field devices with a shared system manager and a backbone network. The DL subnet stops at the backbone router, but network routing may extend into the backbone and plant network (as illustrated in Figure 3).

Routing beyond the backbone router is handled by the ISA100.11a NL.

Each device participating in an ISA100.11a DL subnet is assigned a short 16-b DL subnet address for local addressing by the system manager. To handle the mesh routing, the standard supports both graph- and source-routing algorithms. A graph route is a list of paths that connect network end points. A single network instance may have multiple, overlapping graphs, and a device may have multiple graphs going through it. An example of graph routing is illustrated in Figure 5. In the figure, device A communicates with device F using Graph 1. To send a packet to device F, device A can transmit it to devices B or C, which in turn will forward it according to their own graph-routing configurations. The following routes from A to F are possible using Graph 1: A–B–D–F, A–C–D–F, or A–C–E–F. Similarly, to communicate with device D, device A sends packets according to Graph 2.

A source route is a single directed route between a source and a destination device, and it defines the specific path a packet must take when traveling from its source to its destination. If a single link in a source route fails, the packet is lost, while in a graph route, each device will have multiple associated neighbors to which they may send packets. This ensures redundancy and enhances reliability compared with source routing. The routes are configured by the system manager based on the periodic reports from devices indicating historical and instantaneous quality of the wireless connectivity to their neighbors.

Time division multiple access (TDMA) combined with frequency hopping is used for channel access in WirelessHART and ISA100.11a. The communication is divided into a two-dimensional matrix consisting of time slots and the 15 available channels (ISA100.11a may have 16 available channels if the optional channel 26 is enabled). A collection of time slots forms a superframe, as illustrated in Figure 6. The superframes repeat in time throughout the entire network

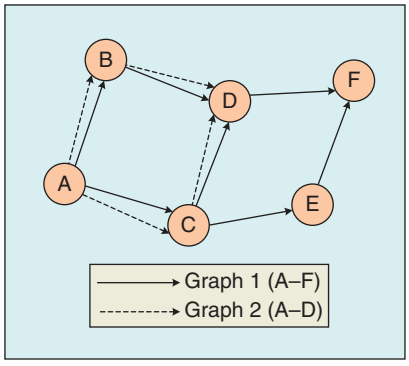


FIGURE 5 – An example of graph routing.

lifetime, and the term frame is used to separate consecutive instances in time of a specific superframe. There is support for superframes of variable lengths, and one superframe must always be enabled. Superframes can be added and removed while the network is operational. The management of the superframes is handled by the network manager/system manager.

In WirelessHART, the duration of a time slot is fixed at 10 ms, while in ISA100.11a it is configurable and set to a specific value by the system manager when a device joins the network.

To supervise the communication within a network, the network manager/system manager typically assigns two devices to a link: one as a source (transmitter) and the other as the destination (receiver). An exception to this is the broadcast messages where multiple receivers are assigned to the same time slot. A link is specified by a superframe, time-slot offset (relative to the first time slot of the superframe), and channel offset. In consecutive superframes, a link will always have the same time-slot offset, while the communication channel will change according to a pseudorandom hop pattern. As an example, for a given link, communication may occur on Channel 14 in time slot $k$ in frame $n$ of superframe A and on Channel 21 in time slot $k$ in frame $n + 1$ of the same superframe. Combining TDMA and frequency hopping allows for multiple devices to transmit data at the same time on different channels, although a single device may only participate in communication on one channel per time slot.

Within the assigned time slot, the source device may transmit a data packet to the destination device. Upon successful reception of a data packet, the destination device transmits an acknowledgment packet (ACK) to the source device (see Figure 7). If the source device fails to receive an ACK, the data packet will be retransmitted in the next available time slot. An ACK is not transmitted upon reception of a broadcast message.

The channel-hopping algorithm described earlier is called slotted channel hopping in ISA100.11a. With slotted channel hopping, the communication channel for a given device switches both between consecutive time slots within a superframe and links in consecutive superframes, as shown in Figure 8(a). In addition to slotted channel hopping, ISA100.11a also defines slow channel hopping and hybrid combinations of slotted

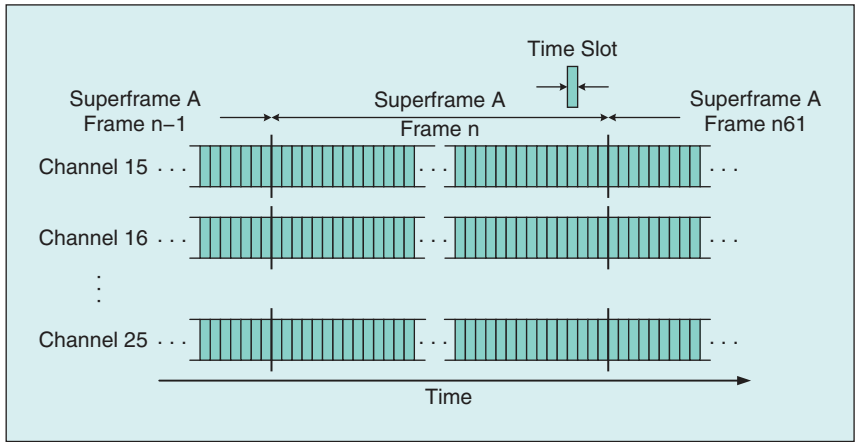


FIGURE 6 – Structure of TDMA channels, time slots, and superframes [9]. (Figure based on information found in [20].)

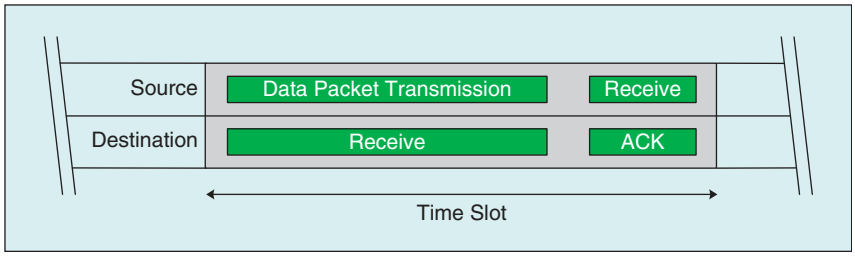


FIGURE 7 – The timing of data transmission within a time slot [9]. (Figure based on information found in [26].)

and slow hopping. In slow channel hopping, a collection of contiguous time slots are grouped on a single channel. One such collection is treated as a single slow-hopping period, and it will be subjected to channel hopping as for slotted channel hopping, but at a slower rate. This is illustrated in Figure 8(b). The duration of a slow-hopping period is configurable. A slow-hopping period is generally shared among a group of devices and used to provide immediate, contention-based channel bandwidth on demand. In other words, transmissions in a slow-hopping period are not driven by a TDMA scheme, but the channel is left open for nondeterministic CSMA-CA-based access. Although the TDMA scheme is not used internally in each slow-hopping period, the devices must still follow the overlaying time-slot synchronization and frequency-hopping patterns of the network. This enables improved support for event-based traffic, where the occurrence of a given event may trigger the need for a device to immediately transmit a data packet or an alarm. With the slotted channel hopping, the device would be forced to wait for the next scheduled time slot where it is assigned as a transmitter, thereby increasing the latency of the event-based data transmission. The drawback of the slow channel-hopping method is that the devices designated as receivers in a slow-hopping period must continuously listen for incoming traffic, which increases their power consumption compared with slotted channel hopping. In a hybrid slotted and slow-hopping configuration, the network will change between periods of slow hopping and periods with slotted hopping. The order in which slotted and slow hopping are combined is flexible.

The WirelessHART specification does not explicitly define the frequency hop pattern, but the assignment of communication links and channel hop patterns is handled by the network manager and distributed to the field devices during the join process. ISA100.11a defines five preprogrammed hopping patterns that shall be supported by all field devices (I/O and routers) [10], and they are

- *Pattern 1:* 19, 12, 20, 24, 16, 23, 18, 25, 14, 21, 11, 15, 22, 17, 13 (, 26)
- *Pattern 2:* pattern 1 in reverse
- *Pattern 3:* 15, 20, 25 (intended for slow-hopping channels)
- *Pattern 4:* pattern 3 in reverse
- *Pattern 5:* 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25 (, 26).

Patterns 3 and 4 are intended for slow-hopping channels, while pattern 5 is intended to facilitate coexistence with WirelessHART. The system manager can configure a device to use any of the five patterns for either slotted, slow, or hybrid hopping.

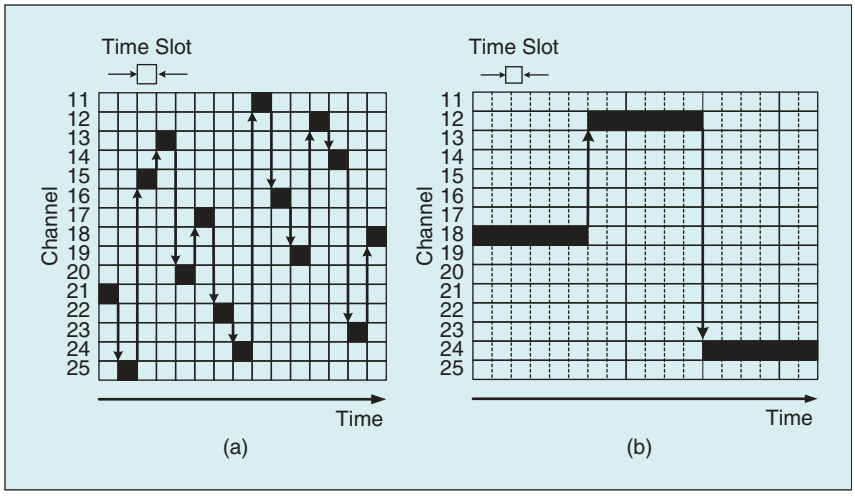


FIGURE 8 – Frequency-hopping patterns: (a) slotted and (b) slow.

### *Network Layer*

The main responsibilities of the NL are routing of packets across the network and to discover and maintain routing tables.

For the HART field communication protocol, NL is the point of convergence for traditional wired HART token-passing networks and WirelessHART TDMA-based networks (see Figure 9). While the WirelessHART DLL specifies the communication of packets between neighboring devices, the NL is responsible for routing packets from the initial source to their final destination. To achieve this, both graph and source routing is defined and must be supported by all devices. All devices in a WirelessHART network maintain a series of routing tables that control the communications performed by the device. The assignment of routing tables is handled by the network manager.

The mesh-level routing within a DL subnet is handled by the ISA100.11a DLL. The DL subnet stops at the backbone router, and network routing beyond the backbone router is the responsibility of the ISA100.11a NL (see Figure 3). As the backbone and plant networks are outside the scope of the ISA100.11a specification, the details of how to route traffic over a backbone or plant network are not specified.

ISA100.11a NL is influenced by the Internet Engineering Task Force (IETF) 6LoWPAN specification [7], with the

goal of facilitating future compatibility. The NL is responsible for determining the appropriate address information, either a 16-b short address for DL subnets or a 128-b long address for application end points and backbone networks. ISA100.11a NL also handles translations between the two address types, and all devices shall maintain an address translation table to facilitate these translations. It is also the task of ISA100.11a NL to fragment and reassemble data packets with a length more than the maximum allowed by the DLL.

### *Transport Layer*

The transport layer (TL) is responsible for end-to-end communication, possibly across several devices, and operates in the communication end points (i.e., not on the routers).

The WirelessHART TL supports both acknowledged and unacknowledged transactions. The acknowledged service allows the devices to send packets and get a confirmation upon delivery, while the unacknowledged services allows devices to send packets without the requirement of end-to-end acknowledgment, thus without any guarantee of successful packet transmission.

ISA100.11a TL provides connectionless services, which extends User Datagram Protocol (UDP) [13] over IPv6 [14] with optional compression as defined by the IETF 6LoWPAN specification [7]. The extension includes better data integrity checks and additional authentication and encryption mechanisms. ISA100.11a TL does not support acknowledged transactions.

### *Application Layer*

The application layer (AL) provides services to user-defined application processes, and it defines the necessary communication services to enable object-to-object communication between distributed applications. WirelessHART inherits its AL from the wired HART AL. HART AL defines the commands, responses, data types, and status reporting supported by the HART field communication protocol specification. All communication between devices on AL level is through a set of defined commands and is divided into the following four groups.

- *Universal Commands*: They are defined in the International Electrotechnical Commission (IEC) Standards IEC 61158-5-20 [15] and IEC 61158-6-20 [16] and state the minimum AL support required for all HART-compatible devices, including WirelessHART devices. All commands shall be implemented exactly as described within the two IEC standards.
- *Common Practice Commands*: They are a set of standardized, device-independent commands used to enhance interoperability between devices from different manufacturers. The commands are optional, and some, all, or none may be implemented by a field device.
- *Device Families Commands*: They are a set of commands for field devices based on the type of process connection they support (e.g., temperature, pressure, flow, and vibration). They are used to further extend interoperability.
- *Device-Specific Commands*: They are the commands developed by manufacturers that are outside the scope of the HART communication protocol. However, the commands must comply with the requirements of the specification.

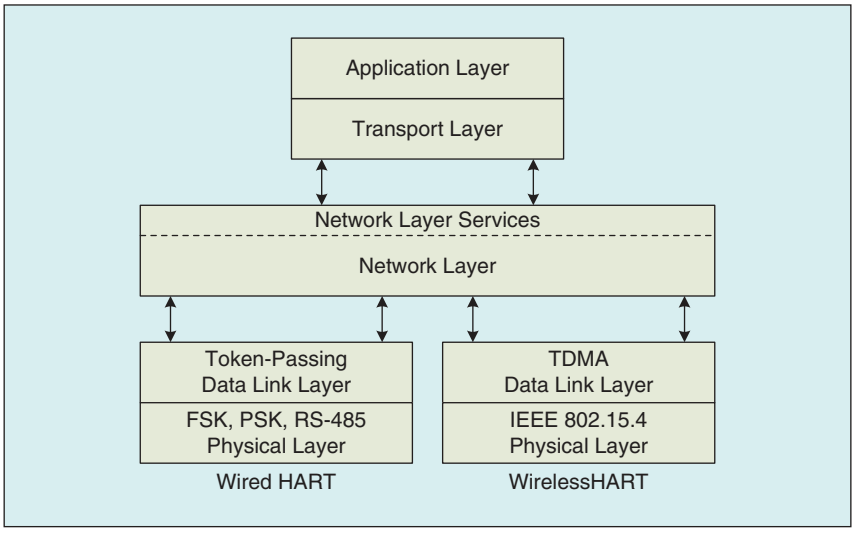


FIGURE 9 – The HART Field Communication Protocol Specification 7.0 protocol layers. (Figure based on Figure 1 of [9].)

ISA100.11a AL defines software objects to model real-world objects. It is divided into two sublayers: the upper AL (UAL) and the application sublayer (ASL). The UAL contains the application processes for the device and may be used to handle input and/or output hardware, support protocol tunneling, or perform a computational function. The ASL provides the services needed for the UAL to perform its functions, such as object-oriented communication and routing to objects within a user-application process (UAP) across the network.

## Security

While the introduction of wireless technology in process automation and manufacturing industries has many potential benefits, it is important to remember that wireless networks are potentially susceptible to cyber attacks. To ensure data confidentiality, authenticity, and integrity, wireless protocols must implement sufficient security mechanisms and algorithms. However, with limited resources such as computation capability and memory, traditional security solutions cannot guarantee security requirements and communications overhead in industrial wireless networks [17]. The following list illustrates the security issues that wireless networks are susceptible to [18]:

- *Accidental Association*: An unintentional access to a wireless network by a foreign computer or device.
- *Malicious Association*: Access to a wireless network is obtained by hackers to steal user information, passwords, or data, or to launch other attacks and install malicious software.
- *Identity Theft*: The hacker is able to impersonate an authorized device or user by listening to credential traffic.
- *Man-in-the-Middle Attacks*: The hackers gain access to a network with malicious association and transparently monitor network traffic and/or provide false information and data to other network users.
- *Denial of Service*: A target device or gateway is flooded with bogus protocol messages and data in an attempt to reduce or suspend its responsiveness and ability to perform regular functions—intentional jamming of a wireless communication channel falls under this category.
- *Network Injection*: Access access points/gateways to introduce bogus network configuration commands that may affect routers, switches, and intelligent hubs. The network devices may crash, shutdown, restart, or even require reprogramming.
- *Byzantine Attack*: An attack where an intruder reprograms a collection of compromised sensors, where they send fictitious sensor readings to the control room
- *Radio Interference*: The interference from other wireless networks operating in the same frequency bands.

The main tasks of the security mechanisms are to provide protection against the attacks mentioned earlier by ensuring secure communication between devices and to provide message authenticity and data confidentiality.

### Payload Encryption and Message Authentication

WirelessHART and ISA100.11a apply security protection through payload encryption and message authentication for both single-hop (hop-by-hop) messages and end-to-end messages. For both standards, the single-hop protection takes place on the DLL, while end-to-end message protection is handled by the NL in WirelessHART and TL in ISA100.11a. The DLL security defends against attackers who are outside the system, while NL/TL security defends against attackers who may be on the network path between the source and destination.

WirelessHART and ISA100.11a supports counter with cipher block chaining message authentication code (CCM) mode in conjunction with Advanced Encryption Standard (AES)-128 (standard with 128-b block size) block cipher using symmetric keys for message authentication and encryption [19]. This authenticated encryption algorithm is designed to provide both data authentication and privacy.

### Keying Models

Both WirelessHART and ISA100.11a define a set of security keys that are used to ensure secure communication. Symmetric cryptography relies on both communication end points using the same key when communicating securely. Attackers that do not share the keys cannot modify messages without being detected and cannot decrypt the encrypted payload information. Common to both standards is that a new device is provisioned with a join key before it attempts to join a network. The join key is used to authenticate the device for a specific network. Once the device has successfully joined the network, the security manager will provide it with keys for further communication. The use of the join key is optional in ISA100.11a. A global key, a well-known key with no security guarantees, may also be used in the join process for devices not supporting symmetric keys.

In addition to the join key, WirelessHART defines session and network keys. The session key is used by the NL to authenticate end-to-end communication between the two devices. Different session keys are used for each pairwise communication. The network key is used by the DLL to authenticate messages on a one-hop basis. Network keys are rotated based on the security procedures of the process automation plant. The key generation and key management is handled by the security manager and distributed to the field devices by the network manager.

In ISA100.11a, devices are issued a master key, DL key, and session key upon joining a network (if the device supports these security features). The master key is used for communication between the security manager and the device, the DL key is used by the DLL to compute the message integrity code (MIC), and the session key is an optional key used to encrypt and/or authenticate TL messages. The keys are limited in time and need to be periodically updated. In addition to these symmetric keys, ISA100.11a also supports optional asymmetrical keys. In asymmetric cryptography, different keys are used to encrypt and decrypt a message. Each device has a pair of keys: a public and a private key. The private key is kept secret, while the public key may be freely and openly distributed. Messages encrypted with the public key can be decrypted only with the private key. Unlike symmetric cryptography, this does not require a secure initial exchange of one or more secret keys to the transmitter and receiver. ISA100.11a defines two asymmetrical keys: CA_root and Cert-A. CA_root is the public key of a certificate authority that signed a device's asymmetric-key certificate. It is used to assist in verifying the true identity of the device communicating the certificate. Cert-A is the asymmetric-key certificate of device A, used to evidence the true identity of the device during execution of an authenticated asymmetric-key establishment protocol.

When joining a network, an ISA100.11a device shall use either symmetric keys, public keys, or no security. The no-security option uses the global key, and the MIC will

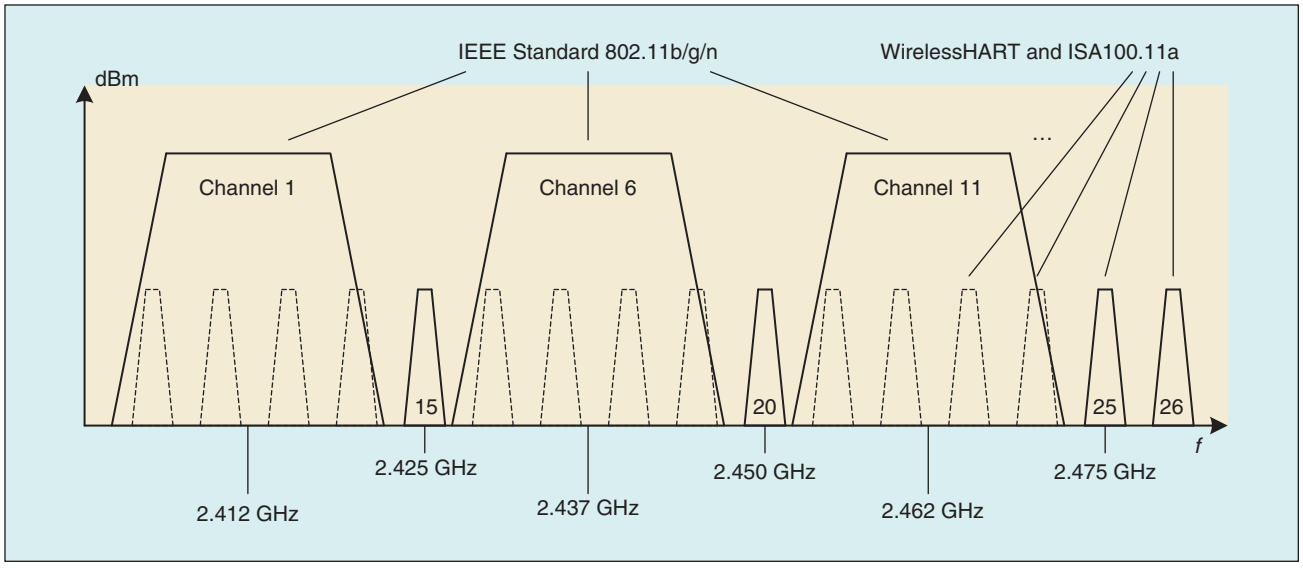


FIGURE 10 – Distribution of IEEE Standards 802.11 and 802.15.4 channels in the 2.4-GHz band.

be the equivalent of a cyclic redundancy check (CRC) with no security guarantees. For these devices, no end-to-end secure transmissions are allowed.

## Coexistence

For the successful adoption of WirelessHART and ISA100.11a in the process automation and manufacturing industries, it is imperative that the technologies are capable of friendly coexistence with other wireless systems that operate in the 2.4-GHz band. Examples of such systems are IEEE Standard 802.11-based wireless local area networks (WLANs) [4], Bluetooth, and cordless telephones.

### *IEEE Standards 802.15.4 and 802.11 for Frequency and Channel Configurations*

In an industrial setting, it is natural to expect WLAN to be a strong contender for the available frequency spectrum. The widespread deployment of WLANs has reached the process and manufacturing plants, and it is expected that most WirelessHART and ISA100.11a deployments will be in an area that is under influence from a nearby WLAN.

IEEE Standard 802.11 defines a total of 14 channels in the 2.4-GHz band. Channel 14 is only available in Japan, while Channels 12 and 13 are prohibited in North America and some Central and South American countries. Each channel is 22-MHz wide, and they are spaced 5-MHz apart, which means that neighboring channels overlap in frequency. To ensure maximum utilization of the frequency band, it has become common in industrial deployments to configure WLAN access points to use the nonoverlapping Channels 1, 6, and 11. The frequency distribution of these three channels along with the WirelessHART and ISA100.11a channels is illustrated in Figure 10. As can be seen, relative interference-free operation for WirelessHART and ISA100.11a can only be achieved in Channels 15, 20, and 25 (and in the optional Channel 26 for ISA100.11a).

### *Spectrum Management*

To better cope with coexistence and interference issues, both WirelessHART and ISA100.11a employ various spectrum-management techniques. A CCA is performed before data transmission to ensure that the RF channel is free to use. IEEE Standard 802.15.4 [2] defines three CCA modes.

1) *Energy Above Threshold*: CCA reports a busy medium upon detecting any energy above a configurable threshold.
2) *Carrier Sense Only*: CCA reports a busy medium if a signal compliant with IEEE Standard 802.15.4 PHY modulation and spreading characteristics is detected.
3) *Carrier Sense with Energy Above Threshold*: CCA reports a busy medium using a logical AND/OR combination of Modes 1 and 2.

For WirelessHART, CCA is fixed to Mode 2. ISA100.11a specifies CCA, as described in IEEE Standard 802.15.4, with the addition of the possibility of completely disabling CCA, defined as CCA Mode 0.

To avoid the use of channels with high levels of noise and/or interference, channel blacklisting may be used. If one or more channels are blacklisted, the device will change its hop pattern to not include the blacklisted channels. For WirelessHART, the blacklisting of specific channels is an optional feature, and it must be manually performed by the network administrator. ISA100.11a employs adaptive blacklisting, giving each device the capability of autonomously blacklisting problematic channels. However, the system manager may disable the adaptive blacklisting feature of any devices in the network.

## Discussion

As mentioned earlier, WirelessHART and ISA100.11a are competitors in the quest of becoming the de facto global standard for wireless instrumentation for factory and process

**WirelessHART and ISA100.11a are competitors in the quest of becoming the de facto global standard for wireless instrumentation for factory and process automation.**

automation. Although both specifications are ratified as standards within the context of their respective organizations (HCF and ISA), they also aim to be approved by other national and international standardization organizations. The WirelessHART specification was approved by the IEC as international standard IEC 62591 Ed. 1.0 for wireless communication in process automation [20] in March 2010, which is believed to strengthen its position in the market. In January 2010, ISA100.11a suffered a setback when the American National Standards Institute (ANSI) failed to approve the new ISA standard. ANSI's main concerns with approving ISA100.11a is reportedly not of a technical or scientific degree but related to the ISA 100 committee's handling of at least one of the appeals against the approval (ratification) of the standard in September 2009. It has been suggested that one of the appeals was rejected without consideration, on the grounds that the appeal was submitted after the deadline for submissions. However, it had been the committee's own delays in responding to the decision to appeal that had been responsible for the deadline being missed in the first place [21]. As ANSI is the official U.S. representative to IEC, it is unlikely that ISA100.11a will be accepted as an IEC standard as long as the relevant national body has reservations.

Despite the ongoing struggle for market position, the HCF and ISA have agreed on a collaborative effort to develop a common standard for monitoring and control applications. The ISA100 committee has created the ISA100.12 working group with the goal of investigating the possible long-term convergence of the two standards. Current ongoing work of the ISA100.12 include the preparation of a recommended practice for WirelessHART and ISA100.11a coexistence in overlapping radio space and a recommended practice for a single wireless device that can be provisioned or configured to run either WirelessHART or ISA100.11a.

When it comes to the technical properties of WirelessHART and ISA100.11a, there are some key differences between the two. In the following sections, a breakdown of some of the most prominent features that separate the two standards are presented.

### *Flexibility*

WirelessHART and ISA100.11a are quite different when it comes to the operational flexibility that the specifications allow for. Although WirelessHART is a rather straightforward specification with very few optional parameters, ISA100.11a is a complex specification with many optional parameters found in different stack layers. These features are both strengths and weaknesses depending on specific needs and usage scenarios.

The strict approach of WirelessHART ensures that all devices will have the same behavior, and it should easily facilitate interoperability between vendors, as basically, all implementations adhering to the standard will be equal. This comes at the cost of a lack of flexibility to adapt and tailor the behavior of the network to specific application requirements.

For ISA100.11a, the wide range of available optional parameters allows for great flexibility when it comes to adapting to various application requirements. However, it can lead to interoperability issues, as different vendors might choose to implement different features of the standard. To combat this, ISA100.11a has defined application profiles. A profile is a cross-layer specification defining which options in each protocol layer are mandatory for that profile. Although the profile definitions should help with the possible interoperability issues, experiences from other wireless specifications such as Bluetooth and ZigBee have shown that it is initially challenging to achieve full vendor interoperability.

### *Protocol Support*

WirelessHART is the wireless extension of the wired HART field communication specification [9], which naturally confines WirelessHART to using the HART protocol.

ISA100.11a implements a tunneling protocol that allows devices to encapsulate foreign protocols and transport them through the network. Although the successful application of tunneling depends upon how well the technical requirements of the foreign protocol are met by the ISA100.11a network, this opens up the possibility of transferring a multitude of wired protocols over an ISA100.11a network.

ISA100.11a also incorporates support for IPv6 traffic through its inclusion of the connectionless services, which extends UDP [13] over IPv6 [14] with optional compression as defined by the IETF 6LoWPAN specification [7].

### *Coexistence with the IEEE 802.11-Based Networks*

Practical experiments have shown that the performance of a WirelessHART network will be degraded when coexisting with IEEE 802.11 networks [22], [23]. The packet loss rate of WirelessHART will increase with increasing network traffic load on IEEE 802.11 networks, and the conclusion is that careful deployment considerations should be made before deploying a WirelessHART network in

an area already occupied by IEEE 802.11 networks.

Similar experiments are not yet available for ISA100.11a, but with the addition of adaptive channel blacklisting and the possibility to employ CCA Mode 1 or 3, it is expected that ISA100.11a is somewhat better equipped to handle coexistence with IEEE 802.11 networks. By using CCA Modes 1 or 3, a transmitting ISA100.11a device will report a busy medium if any energy above a threshold is detected. This means that if a nearby IEEE 802.11 access point or client is transmitting, an ISA100.11a device will back off and delay its transmission to the next available time slot. Although this will result in an identical increase in latency, no power is wasted trying to transmit a packet that will probably not be received correctly by the recipient. In addition, ISA100.11a's capability of blacklisting channels can remove this problem completely by not using the channels that are shared with IEEE 802.11 networks. However, this mechanism will result in a decrease in network throughput of up to 75%, as ISA100.11a network might in a worse-case scenario ending up having to share four channels (15, 20, 25, and 26) instead of the original 16.

### *Security*

Although both WirelessHART and ISA100.11a implement a number of security mechanisms to ensure the integrity of the network, some possible security weaknesses have been identified.

For WirelessHART, all security features are mandatory, while in ISA100.11a, many security features are defined as optional. Considering that security schemes consume additional processor time, memory, and power, having mandatory security features in WirelessHART means that devices that may not require strict security policies cannot disable them to achieve benefits such as extended battery life. However, the added flexibility of the optional security features in ISA100.11a might be a security threat in itself and an issue when it comes to interoperability. Vendors might not choose to implement the full-security suite, and different vendors might choose to implement different parts of the security features. Also, signals from one of the ISA100.11a vendors indicate that their first generation of ISA100.11a devices will not implement any of the optional security features.

**The packet loss rate of WirelessHART will increase with increasing network traffic load on IEEE 802.11 networks.**

Both WirelessHART and ISA100.11a rely on a security manager for the generation and management of the security keys and the authentication of new devices. This means that the loss of the security manager will cause the loss of security mechanisms in the network.

For WirelessHART, the standard does not provide detailed specifications or design guidelines for the security manager, and the security specifications in the standard are not well organized and are dispersed throughout the standard. This lack of design guidelines and ambiguous security specifications impede the implementation of the standard as it requires the developers to have a detailed knowledge of all the core specifications [24].

In addition, experiences from a practical effort to build a WirelessHART protocol stack have shown that performing AES calculations in software on embedded platforms is too time consuming to meet the 10-ms time-slot requirements of WirelessHART [25]. To fulfill the requirements, it is suggested to use an AES hardware accelerator. It is expected that this issue will be encountered in ISA100.11a implementations as well, especially if using a variable time-slot duration of 10 ms or less.

## Conclusions

In this article, a theoretical comparison of the WirelessHART and ISA100.11a specifications has been presented. Although there are some differences between the two standards, most features regarding the fundamental wireless communication parameters are the same. Both standards operate with 2-MHz wide channels in the 2.4-GHz band, using DSSS and FHSS combined with O-QPSK modulation techniques, giving a maximum raw data rate of 250 kb/s. Furthermore, the maximum transmitted power is regulated by governing bodies and limited to 10 mW, allowing a transmission range of up to 100 m. Finally, TDMA with frequency hopping is used for channel access, and they both employ self-configuring, self-healing mesh networks with redundant paths and ACK-based packet retransmissions. With these qualities, both standards should be capable of robust and reliable communication in harsh industrial environments. As a result, predicting which of the two standards will emerge as the de facto standard for wireless field devices on the factory floor is nearly impossible. As ISA100.11a has recently been ratified and the first generations of products are just being shipped, the current market situation is naturally in favor of WirelessHART. Emerson is the current leading supplier of WirelessHART instruments, and they are reporting an increasing demand for the products from their wireless portfolio. Other companies supplying WirelessHART are Siemens, ABB, Endress + Hauser, and Pepperl + Fuchs, while the main supporters of ISA100.11a are Honeywell and Yokogawa.

Also, it still remains to be seen how the differences between WirelessHART and ISA100.11a will affect their operative performance. WirelessHART offers a HART-based plug and play technology that should be easy to install and get operative, while ISA100.11a might have the

potential to provide an increased performance for many applications, given that the network is optimally configured. However, as the ISA100.11a standard has just been ratified, devices with a full-scale implementation is not to be expected from the first generation of products. To hit the market fast, the networks will probably be configured to a fixed set of operational parameters, leaving many of the nonmandatory options for the next generation.

As both standards are relatively new, there are many topics that require further research. For ISA100.11a, practical experiments and pilots in industrial settings are needed to investigate aspects such as general network performance and coexistence with other wireless technologies, specifically IEEE 802.11 networks.

To further clarify the relative strengths and weaknesses of WirelessHART and ISA100.11a, performing comparative experiments in controlled environments is recommended. A suggestion is to compare the various optional features of ISA100.11a with WirelessHART for different sets of application requirements.

Also, given the difference in freedom of choice for configuring network parameters between WirelessHART and ISA100.11a, testing vendor interoperability for the two standards should be of interest—especially to observe how ISA100.11a handles application profiles.

## Acknowledgments

The authors acknowledge the support of the real-time wireless communication for process control (WiCon) project, which is funded by the Research Council of Norway (grant 201376/S10).

## Biographies

***Stig Petersen*** (stig.petersen@sintef.no) received his M.Sc. degree in electrical engineering from Norwegian University of Science and Technology (NTNU), Trondheim, Norway, in 2000. He has been a research scientist at the Department of Communication Systems, SINTEF Information and Communication Technology (ICT), Trondheim, Norway, since 2002. He is currently the project manager of the WiCon project funded by the Research Council of Norway, addressing the use of wireless communication for process control. His research interest includes industrial WSNs. He is a member of the IEEE Industrial Electronic Society's Technical Committee on Industrial Informatics.

***Simon Carlsen*** received his M.Sc. degree in telecommunications from NTNU, Trondheim, Norway, in 2002. He has worked within audio and video technology in the technical department of the Norwegian Broadcasting Corporation. He has experience with computer networking and infrastructure. He has also been working as an acoustics consult for the development of equipment for building acoustics measurements. Since 2005, he has been employed as a principal analyst in the industrial ICT department in Statoil, where he is engaged within R&D on wireless communication and wireless instrumentation for the oil and gas industry. He is a Member of the IEEE.

## References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] *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 802.15.4, 2006.

[3] Q. Yu, J. Xing, and Y. Zhou, "Performance research of the IEEE 802.15.4 protocol in wireless sensor networks," in *Proc. of the 2nd IEEE/ASME Int. Conf. Mechatronic and Embedded Systems and Applications*, Aug. 2006, pp. 1–4.

[4] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Networks—Specific Requirements—Part 11: Wireless Local Area Network Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE 802.11, 2007.

[5] *Bluetooth SIG—Bluetooth Specification Version 4.0*, Dec. 2009.

[6] *ZigBee PRO Specification*, ZigBee Alliance, Oct. 2007.

[7] *Request for Comments (RFC) 4944—Transmission of IPv6 Packets over IEEE 802.15.4 Networks*, Internet Engineering Task Force (IETF), 2007.

[8] N. Kim, F. Hekland, S. Petersen, and P. Doyle, "When HART goes wireless: Understanding and implementing the WirelessHART standard," in *Proc. IEEE Int. Conf. Emerging Trends and Factory Automation*, Sept. 2008, pp. 899–907.

[9] *HART Field Communication Protocol Specification, Revision 7.0*, HART Communication Foundation, Sept. 2007.

[10] *Wireless Systems for Industrial Automation: Process Control and Related Applications*, ISA-100.11a-2009 Standard, 2009.

[11] *Industrial Communication Networks—Fieldbus Specifications*, International Electrotechnical Commission (IEC) 61158, 2007.

[12] *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*, ITU-T X.200 (07/94), 1994.

[13] *Request for Comments (RFC) 768—User Datagram Protocol*, Internet Engineering Task Force (IETF), 1980.

[14] *Request for Comments (RFC) 2460—Internet Protocol, Version 6 (IPv6) Specification*, Internet Engineering Task Force (IETF), 1998.

[15] *Industrial Communication Networks—Fieldbus Specifications—Part 5–20: Application Layer Service Definition—Type 20 Elements*, International Electrotechnical Commission (IEC) 61158, 2007.

[16] *Industrial Communication Networks—Fieldbus Specifications—Part 6–20: Application Layer Protocol Specification—Type 20 Elements*, International Electrotechnical Commission (IEC), IEC 61158, 2007.

[17] X. Zhang, M. Wei, P. Wang, and Y. Kim, "Research and implementation of security mechanism in ISA100.11a networks," in *Proc. 9th Int. Conf. Electronic Measurement and Instruments*, Aug. 2009, pp. 4-716–4-721.

[18] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, "Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries," in *Proc. 24th IEEE Int. Conf. Advanced Information Networking and Application*, Apr. 2010, pp. 949–957.

[19] T. Lennvall, S. Svensson, and F. Hekland, "A comparison of WirelessHART and ZigBee for industrial applications," in *Proc. IEEE Int. Workshop Factory Communication Systems*, May 2008, pp. 85–88.

[20] *Industrial Communication Networks—Wireless Communication Network and Communication Profiles—WirelessHART*, International Electrotechnical Commission (IEC) 62591, 2010.

[21] A. Bond. (2010, Jan. 8). ANSI ISA100.11a Approval Stalled, Control Global [Online]. Available: http://www.controlglobal.com/industrynews/2010/015.html

[22] L. Angrisani, M. Bertocco, D. Fortin, and A. Sona, "Experimental study of coexistence issues between IEEE 802.11b and IEEE 802.15.4 wireless networks," *IEEE Trans. Instrum. Meas.*, vol. 53, no. 8, pp. 1514–1523, Aug 2008.

[23] S. Petersen and S. Carlsen, "Performance evaluation of WirelessHART for factory automation," in *Proc. IEEE Int. Conf. Emerging Trends and Factory Automation*, Sept. 2009, pp. 479–487.

[24] S. Raza, T. Voigt, A. Slabbert, and K. Landernäs, "Design and implementation of a security manager for WirelessHART networks," in *Proc. 5th IEEE Int. Workshop Wireless and Sensor Networks Security*, Oct. 2009, pp. 995–1004.

[25] J. Song, S. Han, A. K. Mok, D. Chen, M. Lucas, and M. Nixon, "WirelessHART: Applying wireless technology in real-time industrial process control," in *Proc. Real-Time and Embedded Technology and Applications Symp.*, June 2008, pp. 377–386.

[26] *Industrial Communication Network—Fieldbus Specifications—WirelessHART Communication Network and Communication Profile, Edition 1.0*, IEC/PAS 62591, 2009–01.