A Comparison of WirelessHART™ and ISA100.11a

by

Mark Nixon
Emerson Process Management
1100 W. Louis Henna Blvd., Bldg I
Round Rock, TX, USA 78681-7430
mark.nixon@emerson.com

ABSTRACT

The technology advancements in measurement instruments and final control elements provide greater process insight, reduce engineering costs and contribute to improving the overall operational performance of the plant. These instruments are often collectively referred to as smart devices. These smart devices include advanced diagnostics that can diagnose the health of the device and in many cases, the health of the process that the device is connected to. It is not uncommon for smart devices to include diagnostics that can detect plugged lines, burner flame instability, agitator loss, worn motor bearings, wet gas, orifice wear, leaks and cavitations. These devices tell the user how well they are operating and when they need maintenance. Many customers have reported substantial savings when using smart devices. Getting this technology to the field has often been hampered by the high cost of installation, as well as other factors. To address these needs what has emerged is a whole new line of devices using wireless technology. Although some of these devices contain the same technology as their wired counterparts, newer devices are emerging with innovative low-powered and/or mobile sensors. The most prominent wireless technology to-date uses IEEE 802.15.4-compatible DSSS radios and operates in the 2.4GHz ISM radio band (IEEE 802.15.4 supports multiple bands). Two standards using the IEEE 802.15.4 [2] radio technology are IEC62591-1 (WirelessHART)[1] and ANSI/ISA100.11a-2011 (ISA100.11a)[3]. The international standard, WirelessHART, and the U.S. standard, ISA100.11a, both provide full descriptions of the communication stacks. Although both standards contain many similarities, they also contain differences. This paper provides a brief overview of both standards, presents key differences between the standards and concludes with a discussion on applications and application integration.

1. INTRODUCTION

Protocols such as Foundation Fieldbus, Profibus, and HART are well-established in the industrial process control space. Although the cost of installing and maintaining the wiring for these networks is often quite significant, they continue to dominate installations. Many years of experience with wired technologies and well-established procedures for using them are important to plants. As such, the willingness to replace these networks with something completely new is relatively low. There is also a continued need to improve productivity and safety while at the same time reducing costs. In general, this means more measurements. In many cases, the most effective way to add these measurements is with wireless instruments that use an existing process control application language.

As wireless sensor network installations progress, confidence in the technology is improving. The technology behind these sensor networks includes a combination of device improvements, security, network technology and network management. Network management is key to the operation of the network in that it is used to manage network resources efficiently, schedule communications to meet the requirements of application, and establish routing to meet reliability and performance goals. Network heath reports are used to automatically adapt the network to changing conditions. Network resources are allocated on demand to cover changes in throughput. Security, reliability, ease of use, long battery life and support for large numbers of devices are key requirements that can be met by a manager. Flexibility, especially with respect to the implementation of communications, usually leads to interoperability issues.

Wireless devices can be line-powered or powered by either batteries or energy harvesters. Non-line-powered wireless devices offer the most flexibility for deployment, but low energy consumption is required to make them practical. While these devices may transmit messages at an interval of every second, more typically the average will be in increments of 15 seconds or longer. The most common application is for devices to support periodic communications. It is also possible for devices to support exception reporting, as well as more advanced techniques for increasing reporting rates in response to some condition. Nonetheless, the vast majority of communications carry measurement updates from field devices. These updates usually contain only a few tens of bytes of data per message. Additionally, some devices may transmit stored files or time-series data on a daily or on-demand basis that could be tens of kBs of data. In all of these cases, the on/off ratio is a key to lowering the power required by the non-line-powered device.

Wireless devices are suitable for both large and small plants. In both cases the RF environment may be complicated by interference and obstructions. The establishment and maintenance of the RF network is complicated, and it is therefore important that the network manager be sophisticated enough to hide the complexity from the end user. In the case of a large network, multiple wireless networks may be deployed within the same location with overlapping RF communications where they will be distinct and separate networks with no need for inter-network communication. Since most plant personnel have limited RF background, setting up and maintaining these networks must be easy. It should always be assumed that the wireless environment is always changing and that site surveys have limited value and cannot be relied on for long-term operation. This means that the wireless sensor network must be able to operate and automatically adapt in the presence of interference from other networks, self-interference, radio shadows, multi-path interference and limited single hop range. Although both WirelessHART and ISA100.11a contain capabilities to support coexistence strategies, users need to be aware of limitations that may be implemented by specific suppliers.

Several other papers have been produced that compare WirelessHART and ISA100.11a[16], [17]. Unfortunately the Genyung paper [16] contains many errors and, as such, is only useful by someone with a deep knowledge about both specifications. The Peterson paper [17] is well done and is a good source for those interested in reading further.

The next part of this paper provides an overview of IEC62591-1 (WirelessHART) and ANSI/ISA100.11a-2011 (ISA100.11a).

2. OVERVIEW OF WIRELESSHART AND ISA100.11A

2.1 IEC62591-1 (WirelessHART)

WirelessHART is based on the HART Communication protocol. The HART application layer has been in existence since the late 80s. In its initial release, the HART Field Communications Protocol was superimposed on a 4-20mA signal providing two-way communications with field instruments without compromising the integrity of the analog output. The HART protocol has evolved from a simple 4-20mA-based signal to the current wired- and wireless-based technology with extensive features supporting security, unsolicited data transfers, event notifications, block mode transfers, and advanced diagnostics. Diagnostics now include information about the device, the equipment the device is attached to and, in some cases, the actual process being monitored.

WirelessHART targets sensors and actuators, rotating equipment, such as kiln dryers, and environmental health and safety applications, such as safety showers, condition monitoring and flexible manufacturing in which a portion of the plant can be reconfigured for specific products. WirelessHART also drove extensions to the core HART protocol, ensuring that newer devices, such as vibration monitors, would be fully supported. The standard architecture usually depicted for WirelessHART is shown in Figure 1 [1], [5].

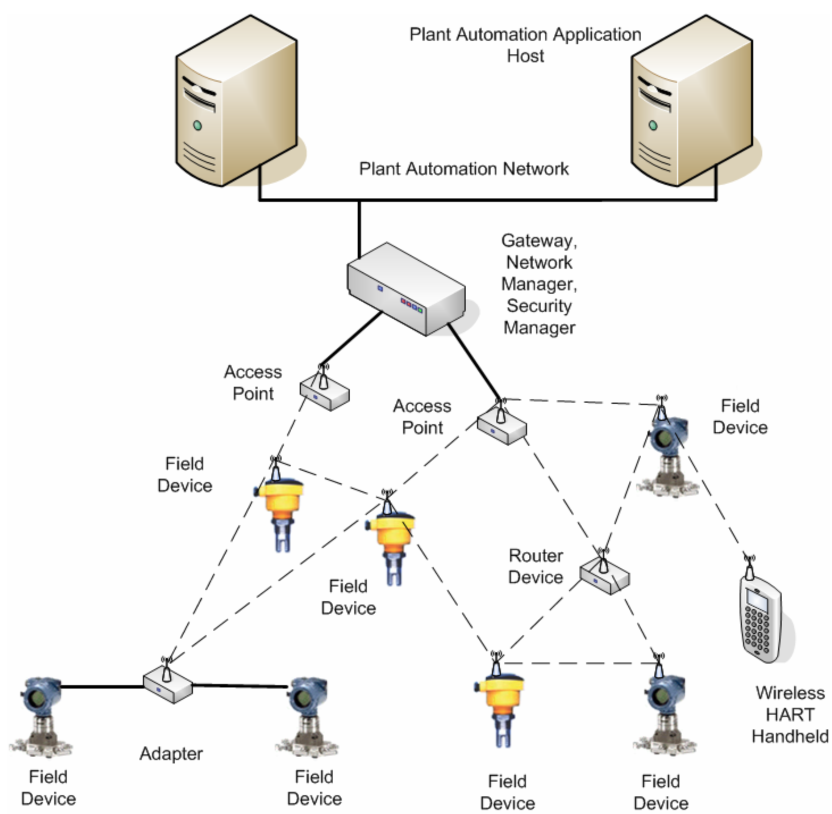

Figure 1 – WirelessHART architecture.

The basic network device types include:

- field devices performing field sensing or actuating functions;
- routers – all devices must have the ability to route packets in the wireless mesh;
- adapters that bind wired HART devices into the wireless mesh;
- hand-held devices carried by mobile users such as plant engineers and service technicians;
- access points that connect wireless mesh to the gateway;
- a simplex or redundant gateway that functions as a bridge to the host applications;
- a single network manager (may be redundant) that may reside in the gateway device or be separate from the gateway;
- a security manager that may reside in the gateway device or separate from the gateway.

In WirelessHART, communications are precisely scheduled based on Time Division Multiple Access (TDMA) and employ a channel-hopping scheme for added system data bandwidth and robustness. The vast majority of communications are directed along graph routes in the wireless mesh network. Graphs are a routing structure that creates a connection between network devices over one or more hops and one or more paths. Scheduling is performed by a centralized network manager that uses overall network routing information in combination with communication requirements that devices and applications have provided. The schedule is translated into transmit and receive slots and transferred from the network manager to individual devices; devices are only provided with information about the slots for which they have to transmit or receive requirements. The network manager continuously adapts the network graphs and network schedules to changes in the network topology and communication demand [5], [12], [18].

The wireless resources the WirelessHART Network Manager controls are:

- RF channels – There are up to 15 RF channels allowed in a WirelessHART system (16 with ISA100.11a in some world areas);
- Time slots – The 10-msec time slots subdivide super frames of configurable sizes;
- Links – Connections to neighbors that specify a channel and time slot in a super frame used for transmission and or reception;
- Graphs – Paths through the mesh network of WirelessHART devices from a source device to and destination device; the paths are designed to be redundant when possible.

Scaling WirelessHART to service large numbers of wireless devices and high network data rates can be accomplished in a number of ways. One way is to use multiple WirelessHART gateways connected to a HART-over-IP backbone. This allows hosts such as DCS systems to connect to multiple gateways. This architecture is ideal for existing DCS systems and has been widely deployed in many different types of plants. Additional techniques for scaling the network are being investigated [13].

Another way that WirelessHART can be scaled up is through the use of multiple access points (AP). Using multiple APs in this way allows for a WirelessHART centralized network management of the wireless communications. This architecture is shown in Figure 2. It has the following advantages:

- Coordinates the wireless resources to prevent islands that overlap in the RF space from interfering;
- Reuses wireless resources in non-overlapping islands to scale the network to large number of devices and higher system throughput;
- Provide multiple backbone access points for higher throughput to the backbone network (each access point has the potential throughput of 100 packets per second);
- Provide access points to connect to backbones that go to different plant organizations and separate plants.

WirelessHART islands also may represent different parts of a plant like separate operations or separate geographic regions.

In this architecture the Network Manager uses the wireless resources to provide services to applications that manage latency, reliability and throughput for the data communications. The Network Manager uses application requirements and network diagnostic data on link availably, device neighbor connectivity and device resource availability to configure super frames and graphs to select links.

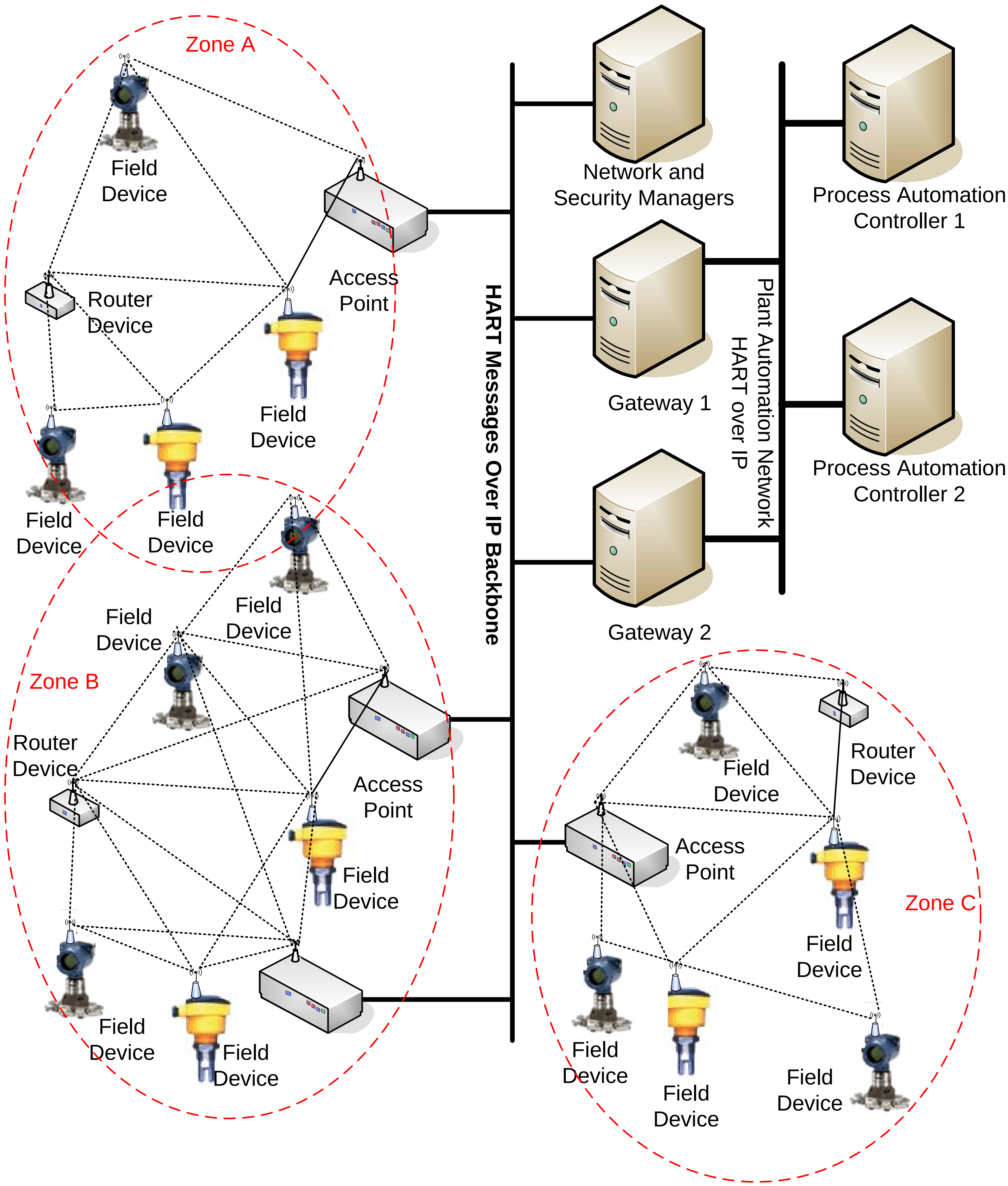

Figure 2 – Using a single backbone to connect multiple access points.

The following sections describe the layers in a WirelessHART network.

The Layers

Figure 3 illustrates the architecture of the WirelessHART protocol stack according to the OSI 7-layer communication model [3]. As shown in this figure, the WirelessHART protocol stack includes five layers: the physical layer, the data link layer, the network layer, the transport layer and the application layer. In addition, a central network manager is responsible for overall network routing communication scheduling.

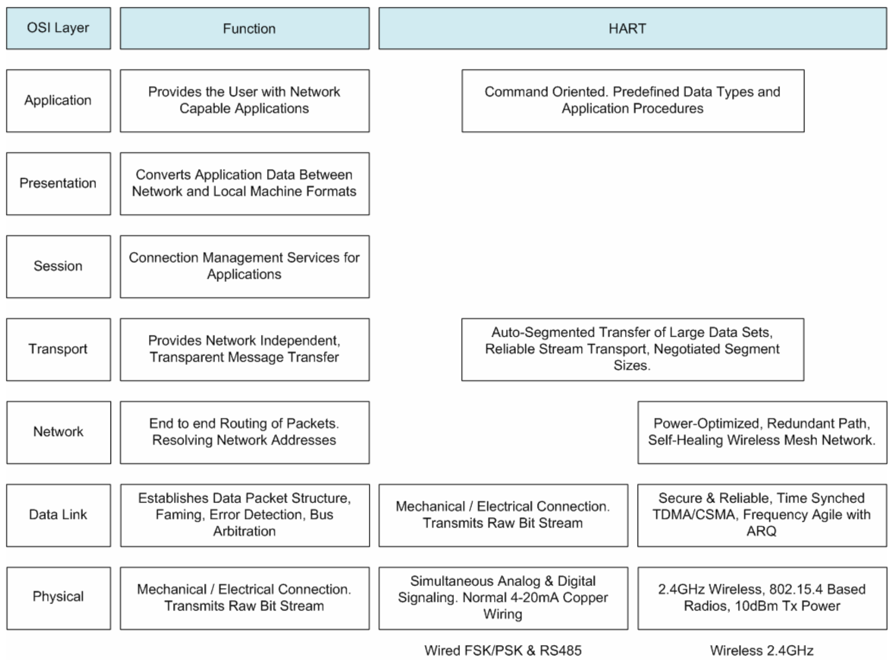

Figure 3 – WirelessHART layers.

Physical Layer

The WirelessHART physical layer is based on the IEEE 802.15.4-2006 2.4GHz DSSS physical layer. WirelessHART fully conforms to IEEE 802.15.4-2006. Additional physical layers can be easily added in the future as radio technology evolves.

Data Link Layer

The WirelessHART Data Link Layer (DLL) is based on a fully compliant IEEE802.15.4-2006 MAC. The WirelessHART DLL extends the functionality of the MAC by defining a fixed 10-ms time slot, synchronized frequency hopping and time division multiple access to provide collision- free and deterministic communications. To manage time slots, the concept of a *super frame* is introduced that groups a sequence of consecutive time slots. A super frame is periodic, with the total length of the member slots as the period. All super frames in a WirelessHART network start from the ASN (absolution slot number) 0, the time when the network is first created. Each super frame then repeats itself along the time based on its period. In WirelessHART, a transaction in a time slot is described by a vector: {frame id, index, type, source address, destination address, channel offset} where frame id identifies the specific super frame; index is the index of the slot in the super frame; type indicates the type of the slot (transmit/receive/idle); source address and destination address are the addresses of the source device and destination device, respectively; channel offset provides the logical channel to be used in the transaction [18]. To fine-tune the channel usage, WirelessHART introduces the idea of channel blacklisting. Channels affected by consistent interferences could be put in the blacklist. In this way, the network administrator can totally disable the use of those channels in the blacklist. To support channel-hopping, each device maintains an active channel table. Due to channel blacklisting, the table may have less than 16 entries.

Network Layer

The network layer is responsible for several functions, the most important of which are routing [19] and security [20] within the mesh network. Whereas the DLL moves packets between devices, the network layer moves packets end-to-end within the wireless network. The network layer also includes other features such as route tables and time tables. Route tables are used to route communications along graphs. Time tables are used to allocate communication bandwidth to specific services such as publishing data and transferring blocks of data.

Network layer security provides end-to-end data integrity and privacy across the wireless network.

Transport Layer

The WirelessHART transport layer provides a reliable, connectionless transport service to the application layer. When selected by the application layer interface, packets sent across the network are acknowledged by the end device so that the originated device can retransmit lost packets.

Application Layer

The application layer is HART. Because of this, access to WirelessHART is readily available by most host systems, hand-helds, and asset management systems. Information on the application layer can be found at [5]. Control over WirelessHART has been widely published [7], [8], [11].

2.2 ANSI/ISA100.11a

ISA100.11a was developed through the International Society of Automation (ISA) [4]. ISA is a U.S.-based, non-profit organization made up of about 20,000 automation professionals. ISA100.11a is intended to be part of a family of standards designed to support a wide range of wireless industrial plant needs, including process automation, factory automation and RFID. The only standard approved thus far is ISA100.11a (note: IEC 62734 is well underway and should pass within the next year). The design criteria for ISA100.11a include:

- flexibility,
- support for multiple protocols,
- use of open standards,
- support for multiple applications,
- reliability (error detection, channel-hopping),
- determinism (TDMA, QOS support),
- security.

ISA100.11a defines the protocol stack, system management and security functions for use over low-power, low-rate wireless networks (currently IEEE 802.15.4). ISA100.11a does **not** specify a process automation protocol application layer or an interface to an existing protocol. It only specifies tools for constructing an interface. The architecture for the ISA100.11a network is shown in Figure 4.

The network and transport layers are based on 6LoWPAN [10], [15], IPv6 and UDP standards [22]. The ISA100.11a data link layer is unique to ISA100.11a and uses a non-compliant form of the IEEE802.15.4 MAC. The data link layer implements graph routing, frequency-hopping and time-slotted time domain multiple access features. The forwarding of messages within the wireless network is performed at the data link layer; i.e. using a link-layer mesh-under design (shown in Figure 5). There is flexibility in how the ISA100.11a data link layer is specified. This flexibility comes from a number of options such as duo-ACKs, configurable time slot size and slow frequency-hopping. Since the slot size and duo-ACKs are not fully specified, it is possible that two ISA100.11a devices may not be able to communicate.

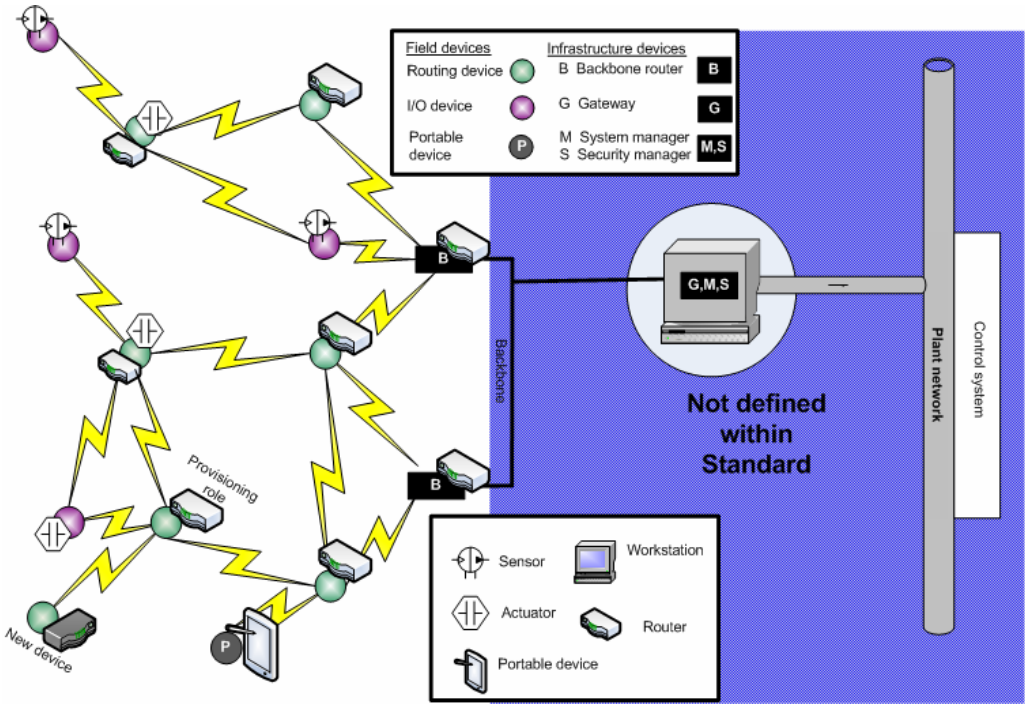

Figure 4 – ISA100.11a architecture.

ISA100.11a leverages IPv6 protocols and addressing for routing-over. All of the nodes connected within a single star or mesh are collectively called a DL subnet (data link subnet). As can be seen in Figure 4 and Figure 5, packets are forwarded between devices at the ISA100.11a data link layer. Until a packet reaches either the destination node within the DL subnet or the border router, it does not get interpreted by the LoWPAN adaptation and IP layers. Messages are forwarded within the DL subnet transparently to the upper layers. As a result, the ISA100.11a data link layer provides an abstraction of a broadcast-type network to the higher layers. The ISA100.11a network (and WirelessHART) support:

- mesh, star-mesh and star topologies (Note: ISA100.11a is limited in the number of hops that can be supported; backbone routers are always required);
- non-routing sensor nodes (through Network Manager configuration in WirelessHART);
- connection to a plant network via a gateway;
- device interoperability;
- data integrity, privacy, authenticity, replay and delay protection;
- coexistence with other wireless networks;
- robustness in the presence of interference.

Routing is a combination of mesh-under and routing-over. As shown in Figure 5, the routing follows the following steps for sending a packet from a wireless field device to a gateway:

1. The network layer of the I/O device passes its own 16-bit data link address as the source address and the 16-bit data link address of the gateway as the final destination address. If the contract table indicates that the ContractID needs to be included in the packet, the contract-enabled header is used; otherwise, the basic header is used if the compression used by the transport allows it.

2. The data link sends the packet to the backbone router. The network layer at the backbone router receives the packet and determines that the packet is not intended for the backbone router, since the final destination address in the received packet is the 16-bit data link address of the gateway. The backbone router translates this 16-bit data link address into the 128-bit IPv6 network address of the desired gateway to determine the next-hop address to reach the gateway using a routing table, and creates a full IPv6 header .

3. The packet with the expanded network header is presented to the backbone interface. The backbone device routes the packet towards its final destination. In this example, the next hop is the final destination of the gateway.

4. The packet arrives at the IPv6 network layer of the gateway over the backbone. The network layer at the gateway determines that the final destination address is equal to the address of the gateway itself and passes the packet to the transport layer.

The gateway then follows its application process and communicates with the control system. Depending on the protocol, this may involve translating data and states.

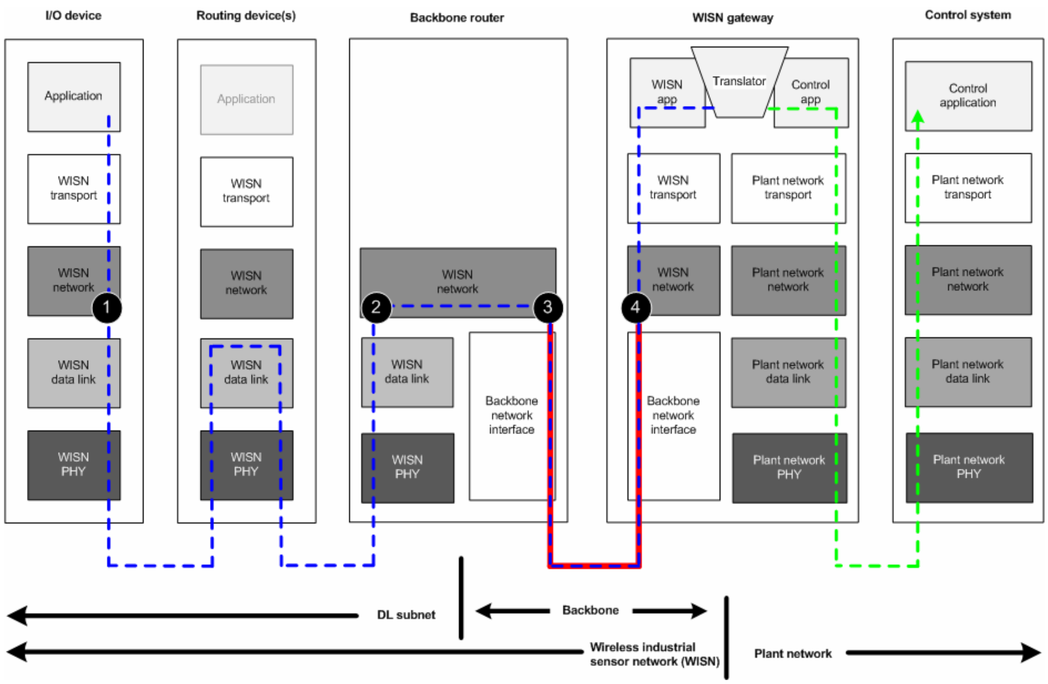

Figure 5 – ISA100.11a routing.

The following sections describe the layers in an ISA100.11a network.

The Layers

Figure 5 illustrates the layers within the ISA100.11a network and a typical path through the layers. The protocol stack also follows an interpretation of the OSI 7-layer communication model[3]. As shown in this figure, ISA100.11a protocol stack includes five layers: the physical layer, the data link layer, the network layer, the transport layer and the application layer. In addition, a central system manager is responsible for overall network routing communication scheduling.

Physical Layer

The ISA100.11a physical layer is based on the IEEE 802.15.4-2006 2.4GHz DSSS physical layer.

Data Link Layer

The ISA100.11a data link layer provides support for the creation, maintenance and packet forwarding – functions required for the wireless sensors. In the OSI model, the data link layer sits between the physical layer and the network layer. It establishes data packet structure, framing, error detection and bus arbitration. The data link layer also includes the medium access control (MAC) functions. In ISA100.11a the data link layer was extended to include the following functions:

- link-local addressing,
- message forwarding,
- PHY management,
- adaptive channel-hopping,
- message addressing, timing and integrity checks,
- detection and recovery of message loss,
- clock synchronization.

Messages are communicated in time slots (typically 10-millisecond time-synchronized slots, but they are configurable). Time synchronization provides accurate time stamping, and the adaptive channel-hopping increases reliability by avoiding occupied channels. In addition, the time-synchronized slots and channel-hopping reduce the utilization of any single channel, thereby improving ISA100.11a's coexistence with other RF networks in the same spectrum.

The data link layer creates and uses graph routing. Graph routing provides for a number of different data paths for different types of network traffic within the data link subnet. Multiple graphs are used by different devices to transmit different types of data. For example, a node will use one graph route to send periodic sensor data to the plant network and another graph route to send large blocks of data. While all of the routes of the graphs are generally anchored at the same point, within the data link subnet, the path of the messages from any single node may vary , depending on the traffic type, bandwidth required and other factors. These various graphs are created by the System Manager. The System Manager takes input from the system/network designer as to the specific requirements for data throughput and transmissions, and information provided by the sensor nodes about the RF environment. Based on this, the System Manager calculates and creates a set of graphs and assigns contract IDs to the graphs. The applications on the sensor nodes then use these contract IDs to notify the nodes on the route to the plant network as to the requirements for the transmission and forwarding of that particular message. The graphs are instantiated based on specific traffic characteristics. ISA100.11a supports periodic data, event data, client-server communications and bulk data transfers.

The System Manager uses these different traffic types along with the requirements for the amount of data and requirements for frequency and latency to calculate graphs for the specific traffic. The System Manager also takes into account the performance of the various channels between pairs of nodes, as well as the power constraints of each node that the traffic will pass through. At the end of the calculations, contract IDs are assigned to each of the graphs. These contract IDs are carried within the data link layer header, and each node on the forwarding graph examines the contract ID and graph ID to determine the "next hop" for the message.

In this way, the ISA100.11a data link layer provides a network topology upon which to build higher layer network functionality. It supports low-power and high-availability operations even in the presence of non-intentional interferers and supports data transmission characteristics for the different types of network traffic required in an industrial process control or factory automation application.

Network Layer

The network layer in ISA100.11a uses 6LoWPAN [15]. IPv6 addressing is used for end-to-end routing. In an ISA100.11a network it is possible for server/client pairs to generate IPv6 packets which are then forwarded through 6LoWPAN edge routers to 6LoWPAN-enabled ISA100.11a devices. The edge router performs the adaptation from IPv6 format to a 6LoWPAN format that can be understood by ISA100.11a devices. The ISA100.11a mesh forwards the IP-based packets to the destination according to routing information configured in the DLL header. This is referred to as mesh-under. The IPv6 packets are fragmented and reassembly is performed in the 6LoWPAN adaptation layer. In this way, IPv6 itself does not play a role in the wireless network. Interestingly enough, to send packets through a ISA100.11a network requires intimate knowledge of ISA100.11a APIs, as explained in transport layer row of Table 2.

Transport Layer

The ISA100.11a transport layer supports a connectionless service based on UDP with an enhanced message integrity check and end-to-end security.

Application Layer

Currently no process control application layer is specified by ISA100 to work with the ISA100.11a communication protocol stack.

ISA100.11a specifies only a set of services for user applications and not a process automation application. Only the System Management application is specified.

3. COMPARING COMMUNICATION PROTOCOLS

3.1 Similarities

Each of the technologies uses the IEEE 802.15.4 standard for low-rate wireless personal area networks (L-R WPAN) to define the radio. WirelessHART also uses the IEEE802.15.4-2006 MAC. ISA100.11a uses a modified, non-compliant version of the same MAC. Both have similar mechanisms for forming the wireless network and transporting data to and from the gateway. These networks are very low power, enabling the use of long-life batteries instead of power taps or solar panels for power. The radio spectrum used in each is in the 2.4 GHz ISM (Instrumentation, Scientific and Medical) band and does not require licensing. The radio technology uses a combination of channel-hopping and direct-sequence, spread spectrum (DSSS) to achieve coexistence with other users of the same spectrum. Networks can occupy the same physical space and radio spectrum without blocking one another.

Both specifications use similar graph routing, source routing, security and centralized network management functions.

3.2 Differences

The major differences between WirelessHART (IEC62591-1) and ANSI/ISA100.11a-2011 can be directly traced to the differences in the goals of each standard. Whereas WirelessHART is designed to address key end-user concerns (reliability, security, appropriate fit for purpose in industrial environments, strict interoperability and support for Application Classes 1 through 5), ISA100.11a is designed to provide flexibility (by providing a variety of build options to the manufacturer and run-time options for customizing the operation of the system). ISA100.11a devices implementing non-compatible options will not interoperate. This flexibility can be a source of confusion for end users. Differences in the stacks are summarized in Table 1. Other differences are summarized in Table 2.

Table 1 – WirelessHART and ISA10011a Stack Comparison

Layer	IEC 62591-1 (WirelessHART)	ANSI/ISA100.11a

Layer		IEC 62591-1 (WirelessHART)	ANSI/ISA100.11a
Physical (PHY)		IEEE 802.15.4 2.4GHz DSSS radio	IEEE 802.15.4 2.4GHz DSSS radio
Media Access Layer (MAC)		Complies with the 802.15.4-2006 MAC and MAC services	Based on a modified, non-compliant version of the IEEE 802.15.4-2006 MAC
Data Link Layer (DLL)		Time-slotted Channel-hopping Secure acknowledgements Clock propagation Security: hop-by-hop data integrity	Time-slotted Channel-hopping Secure acknowledgements Clock propagation Security: hop-by-hop data integrity and encryption Graph and source routing Joining Options* for: Slow hopping and hybrid slow/fast hopping Dual acknowledgement Configuration based time slot sizes Explicit congestion notification
Network Layer		Graph and source routing. Graph routes include the “1 through n access points,” allowing redundant/multiple connections to the backbone networks. This enables a single network to support very high throughput. Joining Security: end-to-end encryption and data integrity	IETF IPv6 and 6LoWPAN Fragmentation and reassembly at backbone router. Note: If fragmentation and reassembly is used, then graph route must terminate and reassemble messages at a single backbone router, introducing a single point of failure.
Transport Layer		Connectionless service Reliable delivery with an acknowledgement service	Connectionless UDP service Security: end-to-end encryption and data integrity
Application Layer	Process Control	HART 7	No process and control application layer

Layer		IEC 62591-1 (WirelessHART)	ANSI/ISA100.11a
	Management	Diagnostics Centralized network configuration of super frames links and routes Joining	Diagnostics Centralized network configuration of super frames links and routes Joining Options* for: Distributed network configuration
	Security	Key management	Key management
	Application Sub Layer	Command and response structure Data encoding Security: Encryption and data integrity	Object and method services structure Data encoding

* Not all the options are full specified in ISA100.11a and are proprietary implementations if used.

Table 2 – WirelessHART and ISA10011a Differences

	IEC 62591 (WirelessHART)	ANSI/ISA100.11a	Comments

	IEC 62591 (WirelessHART)	ANSI/ISA100.11a	Comments
Device Types and Roles	WirelessHART defines device which includes field device, access point, gateway, network manager, security manager, adapter and hand-held	ISA100.11a defines roles which I/O, router, provisioning, backbone router, gateway, system manager, security manager and system time source	There is a fundamental difference at the field instrument level; ISA100.11a devices are not required to support the router role. For this reason it will be very likely to see ISA100.11a networks that are star-only vs. WirelessHART networks which are inherently mesh.
Provisioning	All field devices and access points must support join requests	ISA100.11a defines a specific provisioning role, which means that not all devices will be capable of provisioning other devices to join the network.	The choice of ISA100.11a devices will have a significant influence on the topology that can be deployed. If the user is forced into using a star topology, then it also quite likely that they will require site surveys to ensure the network will form.
Address space	WirelessHART is limited to about 30K devices per WirelessHART network	ISA100.11a uses IPv6 and, as such, has much larger address space.	The practical limit on the number devices per access point and gateway is a few hundred and a few thousand. Since DCSs are fully capable of connecting to many gateways this address space limitation is interesting, but not limiting.
Scaling a single mesh (choke points)	WirelessHART supports multiple access points per local area network. For increased I/O data rates additional access points can be added. For large plants more than one gateway may be used.	ISA100.11a supports 1 or more backbone routers per local area network. If a local area exceeds the bandwidth of one radio, then additional backbone routers are added.	This is a fundamental difference between the architecture of two networks.
Fragmentation and Reassembly	WirelessHART supports fragmentation and reassembly at the application layer. A specific function-block data transfer is defined for this purpose.	ISA100.11a supports fragmentation and reassembly at the network level. This capability is inherently provided by 6LoWPAN.	Although ISA100.11a supports fragmentation and reassembly, what is not defined is how multiple backbone routers coordinate the reassembly of packets Without this function, a graph must terminate on one backbone router, which introduces a single point of failure.

	IEC 62591 (WirelessHART)	ANSI/ISA100.11a	Comments
Redundancy	WirelessHART is a mesh network; by design all paths should be defined to be redundant. At the backbone, multiple access points can be used.	ISA100.11a is defined to optionally support mesh technology. Backbone routers may be designed to support DUO-CAST.	The ISA100.11a DUO-CAST is a very capable technology, but it is not fully specified, leading to proprietary implementations. Both schemes should work well in real plant environments.
Data-link layer	WirelessHART uses a 10-ms slot time. A single algorithm for channel-hopping is defined. MIC codes are always 4 bytes. Networks are coordinated by their absolute slot time (AST).	ISA100.11a supports a configurable time slot size. 10 is just one slot size that may be supported. The System Manager configures the slot time when a device joins the network. Three channel-hopping sequences and five hopping patterns are defined. The channel-hopping patterns are provided to the system manager when the device joins the network. MIC codes may be 4 to 16 bytes. Networks are coordinated by TAI time. ISA100.11a also supports routing at the DLL.	The ISA100.11a standard support of configurable slot sizes and channel-hopping patterns is very flexible. The drawback of their slow hopping pattern is that the receiver must remain on for much longer periods of time, which increases power usage. Contrary to the OSI model definition of DLL, this means that mesh networking routing is done at the DLL level vs. the network layer. All of the ISA100.11a options mean not all ISA100.11a devices will interoperate.
Network Layer	WirelessHART supports routing, joining and encryption/decryption at the network layer.	ISA100.11a supports IETF IPv6 and 6LoWPAN at the network layer.	The network layers in the two standards are very different. Whereas WirelessHART uses the network layer to support routing over the mesh network, ISA100.11a uses the network layer to support routing across the backbone. Since routing across the backbone uses IPv6, the network layer also implements 6LoWPAN. Included as part of 6LoWPAN is support for fragmentation and reassembly and IPv6 header compression.

	IEC 62591 (WirelessHART)	ANSI/ISA100.11a	Comments
Backbone routing	WirelessHART does not mandate a backbone technology. HART-Over-IP can be used for the backbone.	ISA100.11a uses IPv6 for the backbone to route packets between subnets	Backbone routing is designed for scaling networks. WirelessHART achieves this by adding additional access points and gateways. ISA100.11a uses IPv6 which may or may not be available in a plant network.
Transport Layer	WirelessHART supports both acknowledged and unacknowledged services. The acknowledged service allows devices to send packets and get a confirmation upon delivery, while the unacknowledged services allows devices to send packets without the requirement of endto-end acknowledgment, thus without any guarantee of successful packet transmission.	ISA100.11a TL provides connectionless services through User Datagram Protocol (UDP) over IPv6 with optional compression as defined by the IETF 6LoWPAN specification. The extension includes better data integrity checks than is available using the UDP checksum and additional authentication and encryption mechanisms. ISA100.11a TL does not support acknowledged transactions.	In ISA 100.11a, the network layer uses IETF IPv6 and 6LoWPAN formats, and the transport layer provides connectionless UDP IPv6 service with compressed or uncompressed source and destination ports. ISA 100.11a packets can travel around the Internet and are transparent to the routing nodes. However, the security header, the application payload and the MIC form the message payload of the UDP, so any Internet end node that sends and/or receives such messages MUST understand these three components. In other words, it must follow the ISA100.11a security protocol. It must know how to set up the ISA100.11a security with its peer and how to use it. This means that Internet-based applications must be designed to be ISA100.11a-compliant – things are not as open as they are made out to be. In contrast, WirelessHART is designed to work with existing HART applications that were designed before WirelessHART was specified.

	IEC 62591 (WirelessHART)	ANSI/ISA100.11a	Comments
Application Layer	WirelessHART uses the HART AL. The AL, as defined and supported by the HART Communication Foundation (HCF), is extensive. The AL includes Universal Commands (defined by IEC 61158-5-20 and IEC 61158-6-20). Universal Commands define the minimum support that must be implemented by a device. The AL also includes common practice commands. These commands enhance the overall operation of the device. The AL also includes device family commands, which further extend the functionality of devices (e.g., temperature, pressure, flow, vibration, discrete). The final groups of commands supported by the AL are device-specific commands. These commands are used by manufactures to provide functionality above and beyond what is defined by the other groups of commands. WirelessHART devices are defined using EDDL and fully supported by existing handhelds.	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-based communication and routing to objects within a user-application process (UAP) across the network.	This is the most significant difference between the two standards. While WirelessHART fully supports HART, ISA100.11a takes a more open approach and allows for, but does not define, application protocols.

	IEC 62591 (WirelessHART)	**ANSI/ISA100.11a**	**Comments**
Security	WirelessHART supports join keys, network keys and session keys. Session keys are allocated for device-to-device communications. All devices must use a join key. All communications must be encrypted using session keys. Join keys are provisioned using a hand-held device. Symmetric AES-128 keys are supported. Keys may be rotated.	ISA100.11a supports join keys, network keys and session keys. Session keys are allocated for device-to-device communications. Join keys are optional, as are session keys. Join keys are provisioned using over the air provisioning. Symmetric AES-128 keys are supported. ISA100.11a also optionally defines asymmetric keys for the join process. Keys may be rotated.	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. ISA100.11a allows for optionally encrypting messages. ISA100.11a OTAP in combination with asymmetric keys is useful for scaling up networks. WirelessHART does not allow security to be optional, which prevents mistakes that can compromise the system.

	IEC 62591 (WirelessHART)	ANSI/ISA100.11a	Comments
Security Manager	Role of Security Manager is defined. Commands and API for Security Manager are not defined.	ISA100.11a provides a specification for the Security Manager.	Since the Security Manager functionality tends to be provided in conjunction with the Network Manager, for small-to-medium-sized networks, there is little to be gained by describing the security manager in-detail. For larger networks, a case can be made for a more completely defined security manager.
Network/System Manager	WirelessHART contains an extensive description and set of commands for the Network Manager.	ISA100.11a contains an extensive description and set of services for the System Manager.	There are many differences between the Network Manager and the System Manager. The differences begin to show up when looking at the details for diagnostics, configuration and activation of super frames and links, routes and contracts and time tables. The ISA100.11a System Manager must also keep track of the roles that specific devices support, and it must be able to correctly provision and manage those devices. This makes the System Manager more complicated to use.
International Standard	IEC 62591-1 as of March 2010 HART7 as of 2007	ANSI/ISA100.11a-2011	WirelessHART is an international standard since March 2010-. ISA100.11a is in the progress of making its way towards international standard (IEC 62734).
Interoperability (ability of devices and gateways built by different manufacturers to work together)	Interoperability between WirelessHART devices is required by the HCF. The HCF performs interoperability testing with multiple manufacturers' WirelessHART devices and gateways for both the communication stack and the HART7 application.	Stack conformance testing is performed by the WCI. The focus of ISA100.11a is on the flexibility of the specification, which leads to options some of which are not fully defined. The ISA100.11a options are not defined so that when implemented they interoperated with devices that don't use them.	ISA100.11a devices can pass WCI testing and yet not work together – depends on how options were used There is no process automation interoperability testing for ISA100.11a devices.

	IEC 62591 (WirelessHART)	ANSI/ISA100.11a	Comments
Co-existence	Yes	Yes	Feature of Physical Layer, channel-hopping and TDMA
Number of manufacturers currently supplying products	Emerson, Siemens, ABB, Endress+Hauser, Pepperl+Fuchs, MACTek and others (about 13 suppliers support WirelessHART, many others of the 240 HCF member companies are working on products).	Honeywell and Yokogawa support ISA100.11a	The number of suppliers supporting WirelessHART and the number of WirelessHART products shipping far exceed their counterparts for ISA100.11a. WirelessHART has a two-year head start, supports a fully defined application layer, has much more extensive set of suppliers and has a significant number of deployed networks worldwide.
Physical Layer and Communications Stack	IEEE 802.15.4 – 2006. Communications stacks include Linear Technology, WiTECK, Nivis and AwiaTech.	IEEE 802.15.4 – 2006. Communications stacks include Nivis.	
Base packet protocol	HART7	ISA100.11a	ISA100 should be able to tunnel HART7 through its base protocol, but methods required for interoperability have not been standardized yet.
HART adapters that enable wired HART devices to connect to wireless network.	Yes, currently being supplied by a large number of manufacturers.	Possible, but not yet available.	Adapters are key part of WirelessHART. They enable older HART 5 and 6 devices to communicate over a WirelessHART network.

3.3 Discussion of Differences

The following are key points about the differences between WirelessHART and ISA100.11a.

1. Although WirelessHART and ISA100.11a contain many similarities, architecturally they are quite different. Whereas WirelessHART extends HART by introducing device types, ISA100.11a introduces the concept of roles and allows these roles to be applied in various combinations. ISA100.11a includes backbone routers for bridging subnets vs. WirelessHART, which uses access points. Backbone routers limit the throughput into and out of a single subnet to the throughput of one radio. That said, 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. In contrast, WirelessHART access

points can be used in parallel to merge subnets into a very large address space. Since the short address is an unsigned integer, addresses are limited to 30K in a single WirelessHART network. In both ISA100.11a and WirelessHART DCS's can connect to many gateways.

2. WirelessHART directly uses the HART protocol, greatly simplifying implementation for the end user. WirelessHART devices are configured with existing asset management tools and interface with control systems and applications in exactly the same way wired HART devices are configured and interfaced. In contrast, ISA100.11a provides a number of options that must be specified or configured by the end user. For example, in order to provide flexibility, ISA100.11a avoids requiring a specific application protocol, which leads to an interoperability issue. Until an ISA100.11a HART profile is defined, users will not be able to access HART diagnostics or configuration and will only be able to access process data through a mapping mechanism (such as Modbus) supported by their PAS. The ISA100.11a HART profile will not be as efficient as the native HART implementation provided as part of WirelessHART.

3. Channel-hopping in WirelessHART is dictated by the standard, such that devices from different manufacturers are interoperable by design. In ISA100.11a, there are several defined channel-hopping algorithms. 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.

4. WirelessHART specifies that all devices must support routing, although the end user has the option to choose that routing not be used on any given device. ISA100.11a specifies that device support for routing is optional, meaning it is possible for a network to have devices for which routing is not an option. Networks comprised completely of such non-routable devices are not able to adapt to changing conditions and will require site surveys to ensure antenna placement results in sufficient signal strength along designed signal paths. Mesh networks of routable devices are inherently adaptable and do not require extensive site surveys. Users deploying ISA100.11a must plan their network, select the network topology, determine where to deploy routing and non-routing devices and then purchase the different devices required. This also means that the end user must stock spare parts that are routing and non-routing. This is true even if the physical measurement is the same. For example, the end user must stock both a routing and non-routing pressure transmitter and know which one to use as a replacement. This leads to increased cost to deploy and maintain a network.

5. WirelessHART specifies that all communication must be encrypted. ISA100.11a allows for communications to not be encrypted. Users concerned about security will need to ensure ISA100.11a devices can support secure communications and must be careful to ensure that security is maintained.

6. WirelessHART specifies that time slots must be 10 ms. ISA100.11a does not specify fixed time slot lengths. 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. Since

ISA100.11a does not specify timing parameters for non-10-ms time slots, networks using them will be proprietary.

7. WirelessHART defines only one network header – with *no* IP addressing. ISA100.11a defines several network layer header formats supporting IPv6, as well as several compressed header formats. Users need to ensure that all ISA100.11a devices in a network support compatible network header formats, and are compatibly configured prior to use. Some users are concerned about the use of IP headers in general because of the perceived security risk of IP-based security breaches.

8. WirelessHART supports message fragmentation/reassembly at the application level (meaning inside each device or backbone router). Backbone routers may coordinate the reassembly of fragments. Although this is a useful feature within ISA100.11a, it is not yet defined. Without specifying how fragments are reassembled between backbone routers, this feature is only usable in networks with single-sourced suppliers. For this reason, ISA100.11a users will need to make sure they only purchase one brand of backbone router.

9. WirelessHART uses HART as its application layer. ISA100.11a does not specify an application layer nor does it specify interfaces to standard process control protocols.

10. ISA100.11a fully defines a backbone. This backbone works well with large networks. WirelessHART is compatible with the use of HART-over-IP for the backbone.

11. ISA100.11a partially defines Over the Air Provisioning (OTAP) using both symmetric and asymmetric keys. OTAP works well for large to very large networks. HART 7 supports a block transfer function, but it does not specify an over-the-air transfer firmware image application. This is left to the individual device manufactures.

3.4 Interoperability

The HART Foundation rigorously enforces device interoperability for both WirelessHART and HART, and it certifies this with device testing.

The ISA100.11a promotes proprietary, non-interoperable designs in the specification with it implementation options and options that are not fully specified:

- Non-10-ms times slots do not have templates that specify the required timing parameters;
- DUO-CAST ACK do not have a mechanism for coordinated ACK responses;
- Backbone routers do not have a mechanism for reassembling fragments received across devices;
- There is no application or application interface specified for a process control protocol;
- The distributed System Manager option does not specify how network resources are coordinated.

3.5 Packet Sizes

3.5.1 WirelessHART

WirelessHART employs two architectural patterns: a service-oriented pattern and a message bus pattern. A message bus supports message-oriented communications. With message-oriented communications, all communication between application layers is based on messages that use well-known descriptions. With this style, it is not necessary for applications to know specific details about each other. Interaction between applications is accomplished by passing messages over a common bus. A service-oriented approach allows application functionality to be provided as a set of services. The network services that a specific device supports are summarized in the device's EDDL description. Services are accessed through interfaces that are defined as part of the WirelessHART standards. Since services are invoked through message-based interactions, the locations of the service requester and service provider can be separated (and distributed).

Combining the two approaches provide several benefits. First, applications can be run in different environments (for example, one side of the application may be running on a Windows-based host and the other end in an embedded device, such as a Rosemount 3051S pressure transmitter). Second, not all devices need to support all services. Third, services allow higher level applications to be implemented independently of the actual bus protocol. And fourth, the commands exchanged as part of the message bus can be highly compressed and very efficient. This interaction is illustrated in Figure 6.

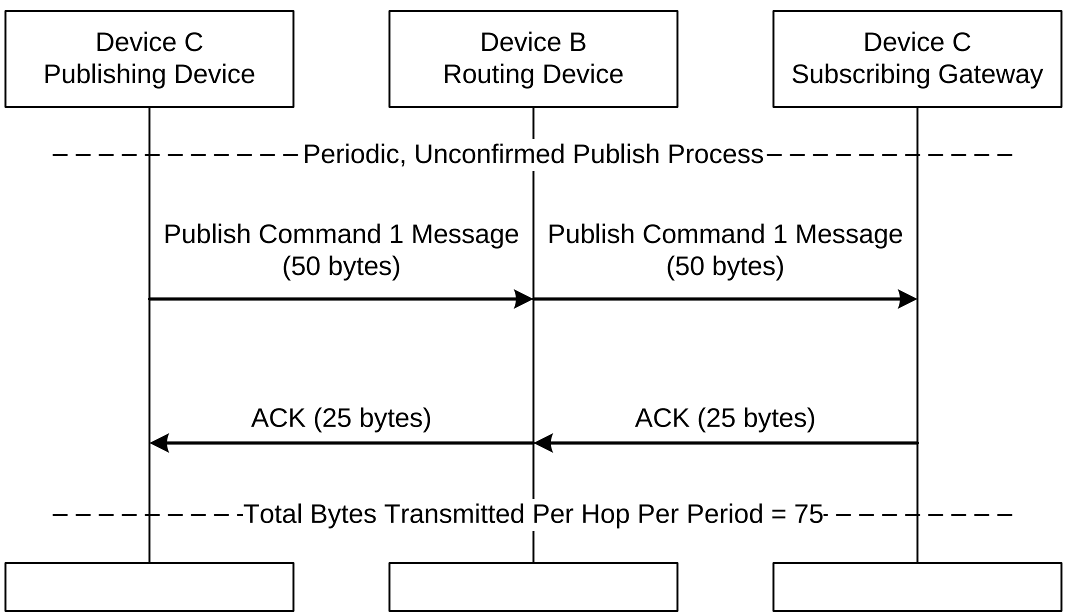

Figure 6 – WirelessHART Packets

As shown in Figure 6 the total size of a packet for Command 1 is 50 bytes for transmission and 25 bytes for the acknowledgement.

3.5.2 ISA100.11a

ISA100.11a employs an object-index mechanism for referencing and transferring data. The advantage of this approach is that it is largely self-describing while at the same time is relatively efficient. This same technique has been successfully used by Foundation fieldbus for many years. The packet exchange and byte counts are shown in Figure 7.

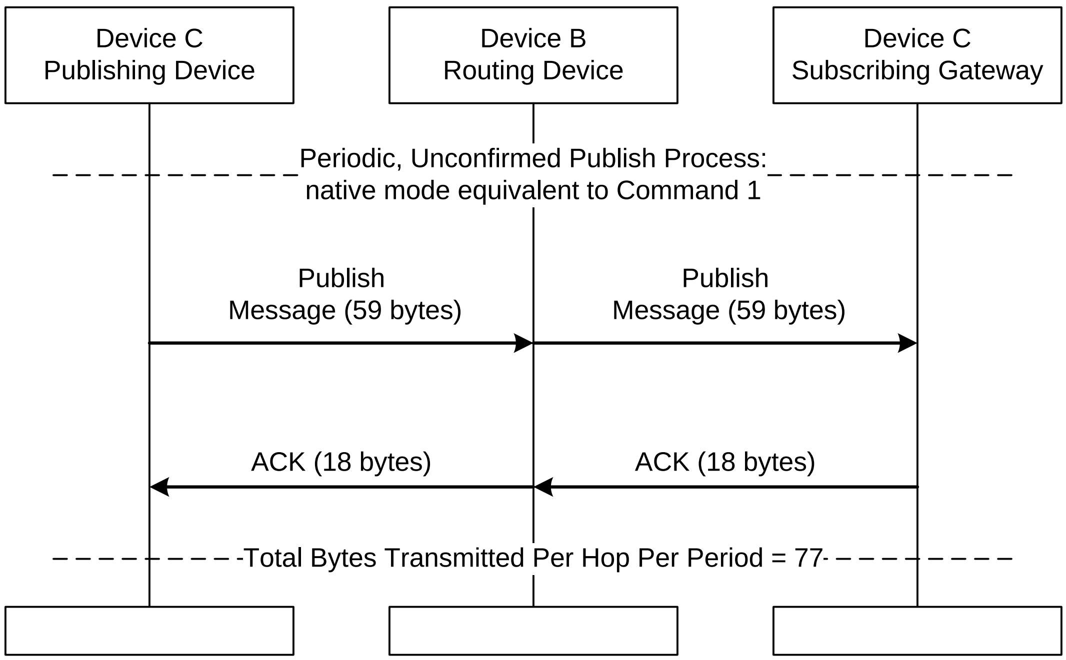

Figure 7 – ISA100.11a packets.

As shown in Figure 7, the total size of a packet for communicating a single parameter (equivalent of Command 1) is 59 bytes for the transmit and 17 bytes for the acknowledgement.

3.5.3 Discussion of Packet Sizes

What is not shown in the discussion above is the effect of increasing the payloads, for example using HART commands 3 or 9. WirelessHART's application layer is structured around messages that are identified by a two-byte ID that implies the data structure that follows. This is a low-overhead method for transmitting data inside a frame. The ISA100.11a application layer incurs overhead for each object in the payload and each data attribute in the object. More complicated HART messages that concatenate multiple commands will drive up the ISA100.11a application layer overhead. WirelessHART is more efficient for communicating device measurements with multiple sensors, alarm and other information.

3.6 Practical Considerations

WirelessHART (IEC 62591) is specifically designed for monitoring and control applications. The basic premise is that it should be easy for users to understand and use. It should make maximum use of existing tools and procedures. Reliability, robustness and secure operation are essential.

ISA100.11a is designed to support a broader range of applications. Although that additional flexibility in ISA100.11a is important in certain non-traditional applications, it introduces unnecessary complexity for the many users.

WirelessHART (IEC 62591) has a clear advantage in purchasing availability (wide variety of device types available now), with multiple manufacturers providing gateways (Emerson Process Management, P+F, Phoenix Contact, so far), guaranteed interoperability (HART Communications Foundation requirement) between devices and also between devices and gateways, use of a single established protocol (HART) that is already in wide use and acceptance. In all cases, the WirelessHART gateways can connect to virtually any PAS/AMS by a variety of means (Modbus and OPC), and in some cases (Emerson) can establish the field device as a native I/O point without requiring mapping.

There is nothing in ISA100.11a that precludes tunneling HART through its data packets, or even interoperability, but without a strict governing body such as HCF, it appears interoperability between manufacturers is unlikely to occur (Walt Boyes of *Control* magazine [www.controlglobal.com] reported that some manufacturers have stated having no interest in being interoperable with other manufacturers, essentially nullifying the value of having a standard by deploying the product line as proprietary).

Unlike WirelessHART (IEC 62591), there is nothing in ISA100.11a that requires all field devices to have routing capability. Without routing capability, devices are limited to being within one hop of a device that does have it, or within one hop of the gateway, and limits the adaptability of the network to re-route when connections deteriorate due to changes or movements in the plant. Lack of routing capability forces the issue of careful site surveys to measure radio strengths and antenna placement, greatly increasing installation costs and difficulty. It is perfectly understandable that end users will want to deselect routing capability for a few designated devices, but it is much easier to maintain if the device has the option. Once a device with no routing option is installed, the only way to ever enable routing at that location is to replace the device or add one that has the option.

3.7 Convergence Discussions through ISA100.12

A Request for Proposals (RFP) to achieve convergence between ANSI/ISA100.11a-2011 and IEC 62591-1 was issued on Nov. 8, 2010. The proposals were *solely* evaluated against the Convergence User Requirements Task (CURT) requirements developed jointly by WG8 and SC12. After several meetings and extensive reviews the final outcome of that report was the following:

Three RFP responses were submitted. These three can be characterized as follows:

- Use ISA100.11a as the basis of a “converged” solution;

- Use WirelessHART as the basis of a “converged” solution;
- Converge above field device communication stack level in a gateway – both device stacks continue without modification

The three proposals were evaluated at length. The outcome of the effort was the following; there is no clear reason to select one proposal over the other. All three proposals are able to meet the CURT requirements. The wording in the final work product is still being evaluated.

3.8 Comparing WirelessHART with Zigbee

In [21], Lennvall et al. present WirelessHART and compare it with Zigbee [6] regarding issues such as robustness, coexistence and security. They concluded that WirelessHART outweighs Zigbee in many aspects for the industrial applications. Details of that evaluation can be found in the referenced paper.

3.9 Coexistence

Many papers have been published looking at the effects of interference and radio strength [14]. This topic is not discussed in this paper.

4. APPLICATIONS

In these sections we describe how the integration between smart devices, control systems and hand-helds is supported by both WirelessHART and ISA100.11a.

4.1 Improved measurement and control

There has been much written about monitoring versus control applications. Looking at this discussion from a slightly different angle, the real question is, “How are measurements being used?” In many cases the measurements are used by operators to monitor tank levels, emission levels, water quality, equipment health and a wide range of other things. These measurements are often used to generate reports for the FDA, EPA and other agencies. These measurements are used by plant personnel to make decisions about the operation of the process, plan maintenance activities and to schedule production runs. These measurements are often directly or indirectly used to validate that the quality of the finished product has been met. These measurements are often also directly or indirectly tied into feed-forward and feedback control strategies.

On the control side of the discussion, there are many kinds of control elements including valves, agitators, blowers, conveyors, etc. These control elements take a value and perform some action. In the case of an on-off valve, the valve will attempt to open or close. In the case of a regulating valve, the read-back of the actual valve position is important in order to determine if there are problems with the final control element itself that are impacting control performance. In the case of an agitator, it’s important to know if the agitator is moving. More examples related to control elements are provided in the section on improved operations.

In many cases devices support the use of more than one measurement. In the case of a level or pressure device, a high level or high pressure indication is often provided. In these cases the device is really a multi-variable device.

So how do WirelessHART and ISA100.11a support improved measurement and control? It is critical to know the measurement quality (level of goodness), whether the device making the measurement is healthy, and the timeliness of the measurement. WirelessHART fully uses HART. As part of the HART standard, status is defined for and provided on all measurements. In addition, conditions detected by the field device that would impact the validity of the measurement are made available as the status of the digital value. Taking advantage of this capability, devices perform checks on hardware and software associated with the input or output and in-turn report this status. The status of an output parameter is calculated to give an explicit indication of the quality of the value; good, poor, bad or fixed. A good signal may be used for control. A poor value is suspect and may not reflect the true measurement or calculated value. A bad value means that the parameter value does not reflect the true measurement, calculation, or control value. Fixed means that the parameter value is constant and not being updated in a periodic fashion. ISA100.11a does not define status. Until profiles are defined, it will be difficult to compare WirelessHART and ISA100.11a.

WirelessHART uses HART's Extended Device Status. The Device Status value includes field device malfunction, configuration changed, cold start, loop current fixed, loop current saturated, non-primary variable out of limits, primary variable out of limits, and other information. The Extended Device Status value provides information on whether the device has malfunctioned (maintenance required), a device variable is in an alarm or warning state (Device Variable Alert), or when power is critically low (Critical Power Failure). Both Device Status and Extended Device Status are included with cyclic command 9. There is no equivalent in ISA100.11a.

Another feature set that is now available as part of the WirelessHART standard is discrete capability. The recent ballot of the HART 7.3 standard includes discrete functionality. WirelessHART devices support both sensors and actuators have already been released.

4.2 Improved Operations

Improved operations is an important topic which includes the operators' ability to monitor and adjust the process, interact with equipment, respond to process conditions and monitor and adjust control operations. Operators are responsible for starting up and shutting down equipment, adjusting the plant to meet production schedules, and responding to unplanned situations such as equipment failures, power changes, etc. When things aren't working correctly, they are often the first to try to troubleshoot the problem.

Consider the following scenario in which the pH measurement of a liquid in a tank is oscillating around setpoint. As a first step in investigating this problem, the operator would likely put the valve target, the actual valve position and the pH reading and its setpoint on a trend. After reviewing the trended oscillations the operator decides to adjust the controller gain. The operator notes that the oscillations remain the same regardless of whether he or she increases or decreases the controller gain. The operator also notes that the read-back value of actual valve position indicates that the minimum change in valve position is 0.5% and notes that a step in an actual valve position change always precedes the pH change. The operator suspects that the oscillation is being caused by the resolution (stick-slip) of the control valve. To follow-through on this idea, the operator requests a valve signature from the valve and compares what she is seeing with the actual process.

In order to support this scenario several key things are required. First, the sampling and reporting must be fast enough not to miss the oscillations. Second, the actual valve position and signal status must be reported along with the target position. Third, the control valve needs a standard way to report more complex information such as the valve signature. In HART 7 several features were added and enhanced to support these scenarios. First, instead of polling the device for values, cyclic data reporting must be used (polling is likely to miss some of the key information). To enhance the cyclical publishing of "burst" messages, HART 7 added exception-based reporting with an adjustable reporting period; the reporting period is based on the signal value. To ensure that the measurement is being periodically reported, command 9 was enhanced to include the time stamp. Multi-variable digital values with status on each value was described in the previous section; cyclic command 9 needs to be used to report these values. As discussed earlier, WirelessHART, which fully supports the HART application layer, picks up these capabilities.

ISA100.11a also includes strong support for published communications. As part of the standard, there is a comprehensive description for contracts as part of contracts burst-mode type communications. Since there is no application layer defined, access to the information required by the above scenario is not available in a standard way.

The last part of this scenario, accessing the valve signature, requires a different kind of feature – large data transfers. In HART 7 block data transfer was greatly enhanced. The block data transfer mechanism is best classified as a Transport Layer service. The data transfer mechanism is like a pipeline. It establishes a "connection" between the host and the slave device and guarantees the transfer of a stream of data. The mechanism is designed to maximize the use of the HART communication bandwidth while performing the transfer. In this scenario the valve signature would be transferred using block data transfer.

ISA100.11a also supports large data transfers. In the case of ISA100.11a packet fragmentation and reassembly would happen at the Network Layer. For very large data transfers, such as for a vibration monitor, a specialized application layer implementation would also need to be defined.

Operators are responsible for a large number of loops, many pieces of equipment and, often, different processes and utility areas. In order to cover all of these things, they rely very heavily on a well-engineered alarm and alert system. In an ideal world, equipment and devices would analyze themselves, report their health on an on-going basis, and tell the operations staff when plant equipment and devices should be scheduled for maintenance (many smart devices and control elements today have exactly these capabilities). More advance devices also have the ability to provide additional information about the process they are inserted into; for example, they can detect plugged lines, burner flame instability, agitator loss, wet gas, orifice wear, leaks, bubbles in the line and cavitations. So how do devices and equipment report this information, and how does HART 7 support these requirements? The answer is event notifications.

Event notification publishes changes in the device's status, independently from data publishing supported in other burst mode commands. For events. the status included in the Device Status byte, Extended Device Status byte and Command 48 can be used. It is possible to specify a limited set of bits that will trigger event notification. To prevent spurious event notifications a de-bounce interval is configured. This defines the amount of time that a condition must persist before the event notification is time-stamped and sent out. Once an event has been latched, it is transmitted repeatedly at the rate indicated by the retry period until the event has been acknowledged. Event notifications have a low priority, but require a time stamp in order to indicate the first time when a notification occurred. Event notification requires and is built upon burst mode operation.

4.3 Reduced Configuration, Installation and Checkout

Configuration is a rather large and somewhat involved topic. When discussing the topic of configuration, both the configuration of the device and the configuration of the control strategy must be considered. Let’s start with devices. Devices are designed to work in a wide number of processes. The actual process that the device is inserted into requires the device to be configured. As part of this configuration the device is given a tag, scaled (instrument scaling includes high scale value, low scale value, engineering units and decimal places), and signal conditioning is applied. (In the case of a valve, it is important to know which direction the valve goes when the signal valve is increased.) Field devices may be commissioned and calibrated in the factory or on site in the instrumentation shop or once the device is installed. The set of parameters that a device supports and the methods available to the device are described by the EDD files written in EDDL. Customers usually have standard parameter value templates for different types of devices and use these templates to customize devices for use in their plants. Many have tools that use EDD files such as the 475 field communicator to calibrate and configure their field devices. In this way devices can be completely defined off-line and configured at the factory, in the shop, or prior to start-up by downloading the off-line configuration into the device. All that is required is to associate the unique device identifier in the configuration system and then use this as a key for the device. WirelessHART leverages EDDL, which is fully defined and supported by the HCF. ISA100.11a does not specify this level of detail.

Configuring the control system requires a different set of information. In the case of the control system what is important are measurements that the device supports and the signal information that is to be associated with those measurements. Signal information includes information such as signal tag (since devices can be multivariable, they can have many signal tags associated with them), scaling information, alarm information, linearization, description and “other.” Control system configuration usually bulk configures all of this information and downloads the information into the control system at various points in the configuration cycle. Again, this information is provided as part of HART, and WirelessHART picks up all of this by supporting the HART application layer.

4.4 Improved Asset Management and Maintenance

HART from the beginning has always been specified with features to support both operators and maintenance personnel. Features such as process variables plus status give operators far better visibility of the instrumentation health. Features such as event detection and reporting give them a chance to respond to problems before they occur. For maintenance personnel, features such as the ability to validate a device setup, audit trail, calibration and diagnostics give them the ability to validate that the device has been properly configured, calibrated, and is performing well.

WirelessHART which fully supports the HART application layer gets all of these features. ISA100.11a defines none of these things.

5. CONCLUSION

In this paper we provide an overview of WirelessHART and ISA100.11a. We also discuss key differences, as well as applications. WirelessHART (IEC 62591) is designed to be simple to apply, using established tools and an established protocol (HART), and is governed by the HART Communication Foundation to assure interoperability between manufacturers required at the device level. ISA100.11a has many options for users to carefully specify to ensure compatibility, and this is likely to lead to networks consisting of only a single source of manufacturer in order to guarantee compatibility between devices in the network and the network infrastructure. ISA100.11a assures communication stack conformance, but does not test devices for interoperability at the application layer.

WirelessHART (IEC 62591) is a field-proven technology, with more than four years of installed base, over 100,000 devices, over 8000 networks and currently growing at a rate greater than 30% per year. It has been an international standard (IEC 62591-1) since March 2010. A wide variety of devices types are available from more than 13 manufacturers (so far).

ISA100.11a recently became a U.S. standard. The increased flexibility of ISA100.11a will be ideal for some applications. Increased flexibility and the lack of an application layer have slowed down the adoption of ISA100.11a.

6. REFERENCES

1 IEC 62591 Ed. 1.0 b:2010, “Industrial Communication Networks—Wireless Communication Network and Communication Profiles—WirelessHART™,” 2010.

2 IEEE Std 802.15.4TM -2006: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), October 2006.

3 ISO 7498-1 Information Processing Systems—OSI Reference Model—The Basic Model

4 “ISA,” www.isa.org.

5 “HART Communication,” www.hartcomm.org.

6 “ZigBee Alliance,” www.zigbee.org.

7 F. Seibert and T. Blevins, “WirelessHART Successfully Handles Control,” *Chemical Processing*, 2011, www.chemicalprocessing.com/articles/2011/WirelessHART-successfully-handles-control.html?page=1

8 Broadley, S., Karschnia, R., Nixon, M. and Blevins, T., "Using Wireless Transmitters in Single-Use Disposable Bioreactor Control," IFPAC Conf., Baltimore, Md. (Jan. 2009).

9 Constrained Application Protocol (CoAP), http://tools.ietf.org/html/draft-ietf-core-coap-09

10 IPv6 over Low-Power WPAN (6lowpan), tools.ietf.org/wg/6lowpan/

11 Song, J., S. Han, A. K. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt, “WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control,” in RTAS, 2008.

12 Fiore, Gabriella, Valeria Ercoli, Alf J. Isaksson, Krister Landern, and Maria Domenica Di Benedetto, “Multi-Hop Multi-Channel Scheduling for Wireless Control in WirelessHART Networks,” in ETFA, 2009.

13 Chen, D., M. Nixon, T. Lin, S. Han, X. Zhu, A. Mok, R. Xu, J. Deng, and A. Liu, “Over the Air Provisioning of Industrial Wireless Devices Using Elliptic Curve Cryptography,” CSAE, 2011.

14 Elnahrawy, Eiman, Xiaoyan Li, Richard Martin, “The Limits of Localization Using Signal Strength: A Comparative Study,” IEEE SECON, October 2004.

15 Shelby, Zach, Carsten Bormann, *6LoWPAN: The Wireless Embedded Internet,* Willey, 2009.

16 Wang, Gengyun, “Comparison and Evaluation of Industrial Wireless Sensor Network Standards ISA100.11a and WirelessHART,” CHARMERS Master’s thesis, 2011.

17 Petersen, Stig, Simon Carlsen, “WirelessHART Versus ISA100.11a”, IEEE Industrial Electronics, December 2011.

18 Deji Chen, Mark Nixon, Aloysius Mok, *WirelessHART Real-Time Network for Industrial Automation*, Springer, 2010.

19 Han, Song, Xiuming Zhu, Deji Chen, Aloysius K. Mok, Mark Nixon, "Reliable and Real-time Communication in Industrial Wireless Mesh Networks" in RTAS, 2011.

20 Raza, Shahid, Adriaan Slabbert, Thiemo Voigt, and Krister Landern¨, “Security Considerations for the WirelessHART Protocol,” in ETFA, 2009.

21 Lennvall, T., S. Svensson, and F. Hekland, “A Comparison of WirelessHART and Zigbee for Industrial Applications,” WFCS, 2008.

22 IETC RFCs, http://tools.ietf.org/html/rfc2894