blog.isa.org

Analysis of Wireless Industrial Automation Standards: ISA-100.11a and WirelessHART

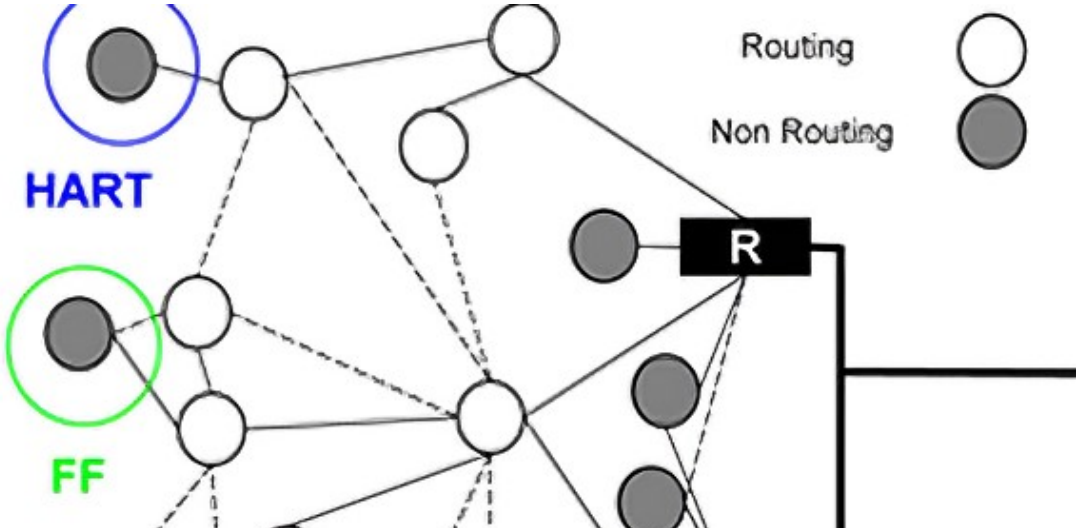
Contributing Authors

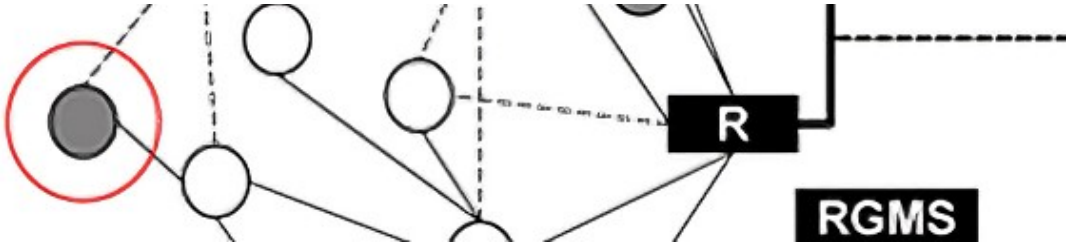
22–28분

This post was authored by Márcio S. Costa and Jorge L. M. Amaral.

The use of wireless transmission is part of everyone's life. Every day, companies develop and update products with wireless capabilities. The benefits of mobility make the use of wireless equipment almost a necessity.

The online life is now possible not only through computer desktops but also through cell phones, tablets, notebooks, and TVs, which makes wireless transmission the first choice of the communication interface.





When one looks to the industrial environment, it is natural to ask if the "wireless wave" will reach industrial applications to be used in automation and instrumentation projects. This question will only be answered in the future. However, when one looks to the near past, very few people could have imagined a scenario in which wireless communication took over the world. So, it is reasonable to assume a similar speed of change will occur within a few years in industrial automation.

The use of wireless networks in industrial automation has increased in the past few years. It can be explained due to several advantages wireless technology presents, such as the reduction of time and cost to install new devices, since there is no need to provide a cabling infrastructure, along with the possibility of installing new devices in hard-to-reach or hazardous areas and the flexibility to alter existing designs.

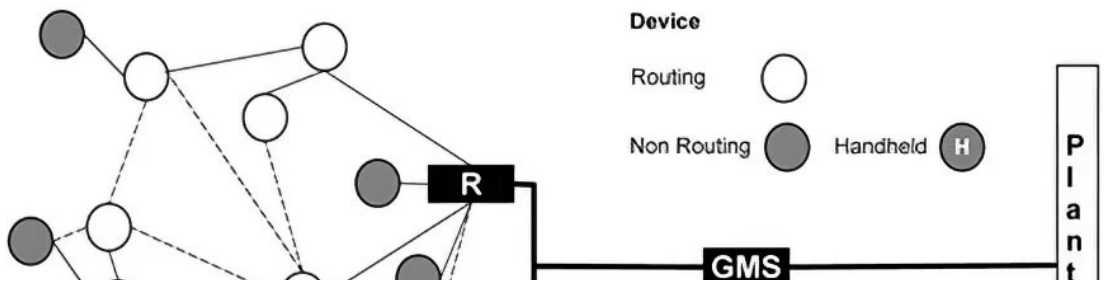
With adopting wireless technology, many important requirements should be considered regarding the solutions presented by the new standards, protocols, methodologies, and support tools. The most important requirements are: reliability, security, robustness, determinism, quality of service (QoS), interoperability, integration with existing systems, networks with large

amount of devices (scalability), and support tools for designing the network layout, process information, and monitoring.

Various solutions (proprietary or not) exist in the market to issues with using wireless transmission in an industrial environment. ISA-100.11a and WirelessHART are two of the most important standards available focused on applications of wireless networks in process automation. This article describes the main features and the solutions adopted, in order to facilitate the comparison between them. The article also briefly discusses some open issues that will have to be addressed in future versions of these standards.

Wireless network standards for process automation

The main purpose of the ISA100 committee is to provide a family of standards for industrial wireless networks, which will address the needs of the whole plant, such as process control, personnel and asset tracking and identification convergence of networks, and long-distance applications. ISA-100.11a is the first standard of the family. It describes a mesh network designed to provide secure wireless communication to process control.



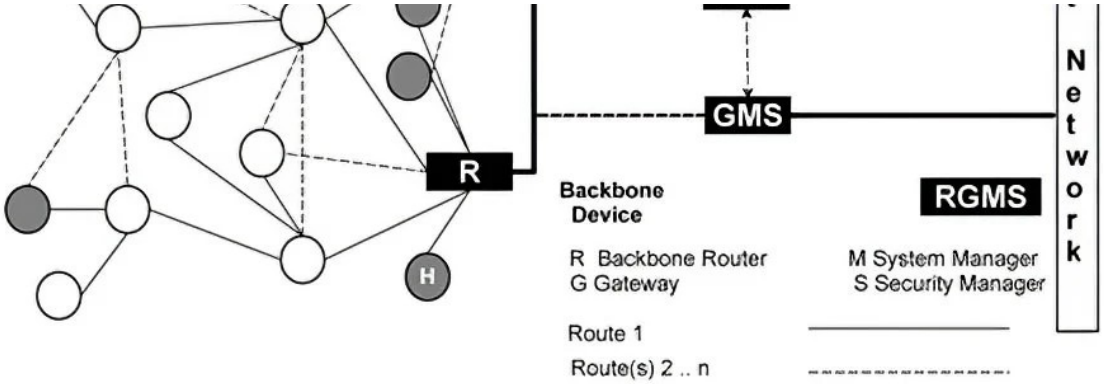


Figure 1. ISA-100.11a network

The ISA-100.11a network can be seen in Figure 1. It presents routing and non-routing field devices, backbone routers, a system manager, a security manager, and gateway. Regarding the field devices, the non-routing ones are the I/O devices (sensor and actuators), while routing devices, besides the routing capability, can also act as I/O devices. It is worth mentioning that routing devices perform an important role in mesh networks. In this topology, data is transmitted from source to the destination through several hops, and the routers are responsible to make sure that the data arrives at the right destination. They can even use alternative paths to improve reliability. The backbone router is responsible to route the data packets from one subnet over the backbone network to its destination, which can be another subnet or the gateway. The *gateway* acts as an interface between the field network and the plant network (and control host applications). The system manager is the administrator of the network and it is responsible for communication configuration (e.g., resource allocation and scheduling), for the device management and network run-time control. The security manager is in charge of the policy security

management of the standard.

Figure 2 shows the ISA-100.11a protocol stack compared with the OSI reference model and the TCP/IP. It is important to note that the ISA-100.11a protocol stack is built with widely accepted and proven standards; for example, the mesh network is integrated to IPv6. This will allow the ISA-100.11a to provide highly scalable solutions.

The application layer is very flexible and is capable of performing tunneling. This allows users to maintain the compatibility with legacy protocols that are currently in use in their plants.

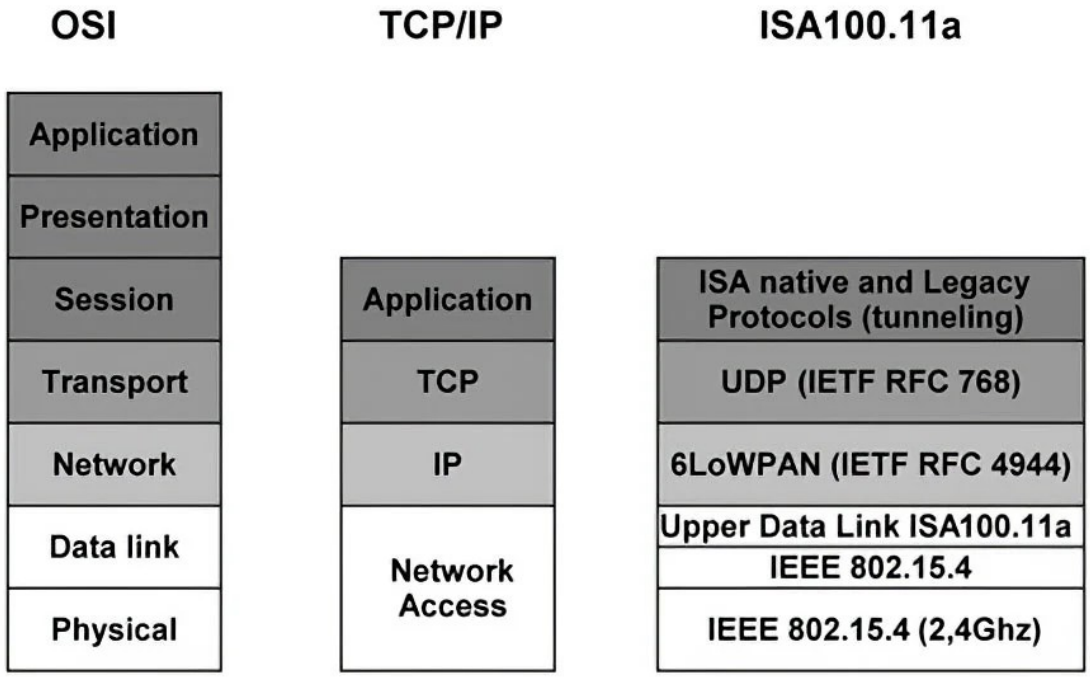


Figure 2. ISA-100.11a protocol stack

WirelessHART was the first standard developed for wireless communication for process control. Officially presented by the HART Communication Foundation in September, 2007, it adds wireless communication capability to the HART protocol, and it is compatible with existing HART devices.

In WirelessHART, each field device may act as a router of other device's data packets. It means that a field device does not have to communicate directly with the gateway; it only needs a neighbor device to transmit its data, which will be responsible for sending the data to another field device until it arrives at the gateway. The mechanism extends the network range and also creates redundant communication paths, which increases the network reliability.

The WirelessHART network supports a wide variety of devices from different manufacturers (Figure 3).

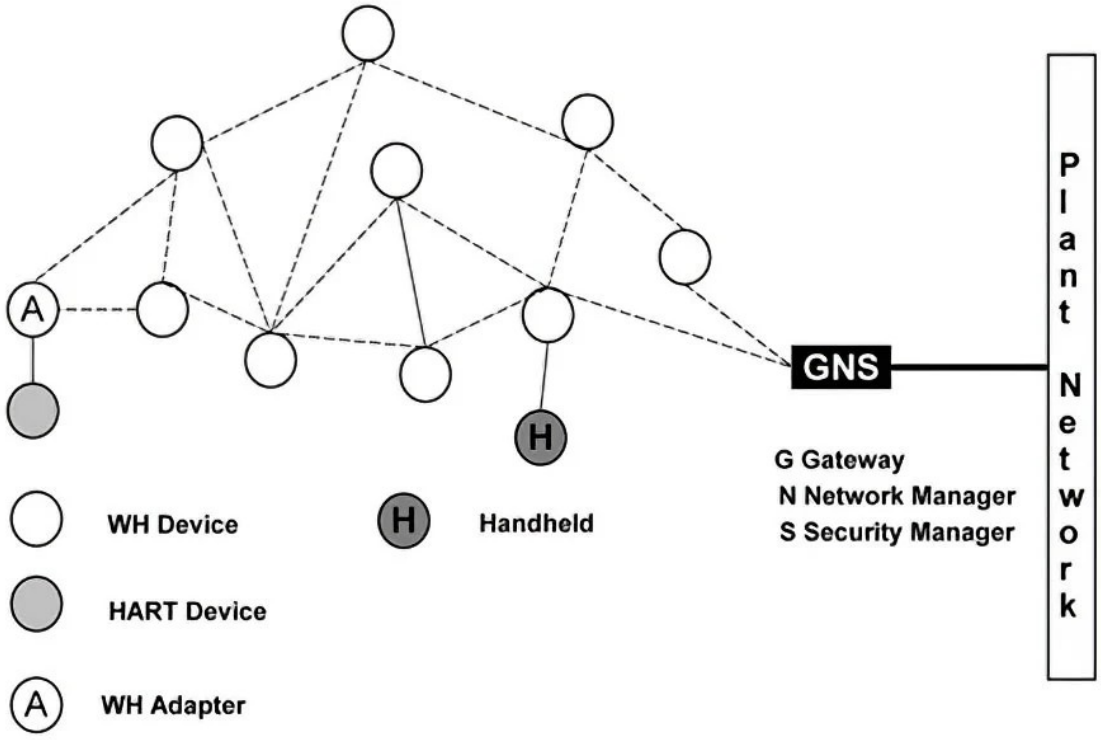


Figure 3. WirelessHART network

A WirelessHART network presents the following components:

- Field devices-they can measure process variables and also retransmit data packets received from other devices;
- Adapters-they connect a wired HART device to a

WirelessHART network;

- Gateway-it connects the field network to the plant network. It allows the control host applications to access the data from the field network;
- Handheld-a portable computer used to configure (provisioning), perform diagnostics and calibration of field devices;
- Network manager-it is responsible for network configuration, management of the network device communication (graph route tables), and monitoring the state of the field devices. It can be implemented in the gateway;
- Security Manager-it can also be implemented with the gateway and is responsible for generation, storage, management, and distribution of the keys used in the device authentication and data cryptography.

The WirelessHART protocol stack is shown in Figure 4.

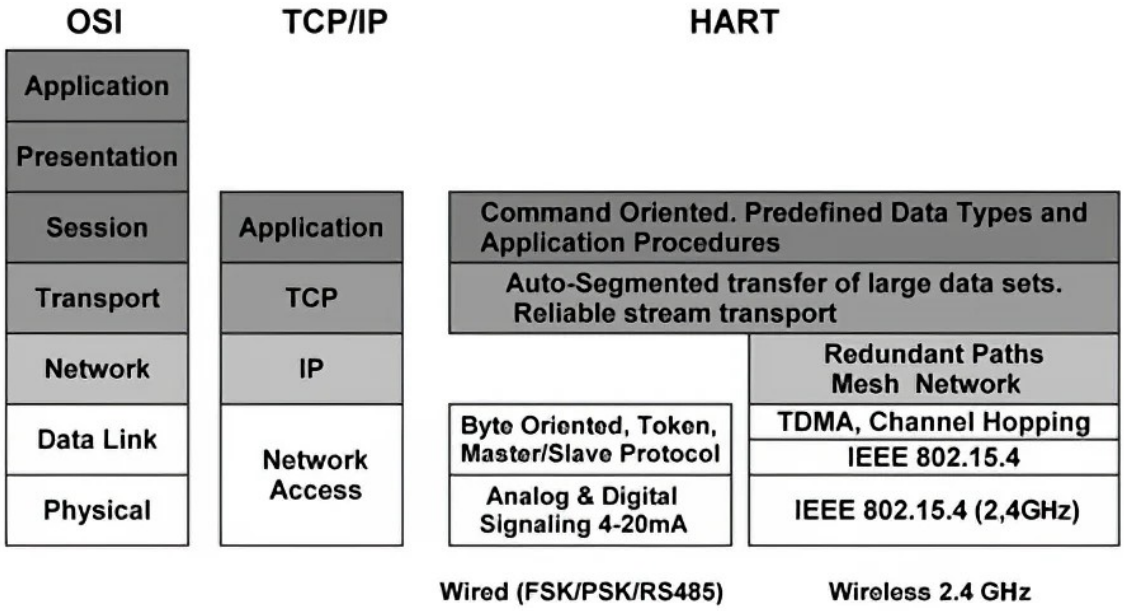


Figure 4. HART protocol stack

It can be seen that the new layers were included in order to make the HART protocol work in a wireless network.

Protocol stack comparison

The physical layer defines the mechanical and electrical interfaces and the procedures to establish and disestablish the physical connection to transmit the information coded in bits. ISA-100.11a and WirelessHART use the radio interface described in IEEE 802.15.4. These radios operate in 2.4-GHz unlicensed band (ISM-industrial, scientific, and medical). This band is divided in 16 channels, uses DSSS (direct sequence spread spectrum) and 250-Kbps raw data transmission rate.

In ISA-100.11a, the physical layer and the lower data link layer use the IEEE 802.15.4, while the upper data link layer implements TDMA (time division multiple access). It is a medium access control method that provides time diversity (i.e., the communication between devices can only occur in a specific time slot). The duration of the time slot can be configured (10 to 14 ms) to better accommodate the application needs. All the time slots needed to allow the network communication form what it is called a *superframe*. Depending on the communication type, the time slots can be dedicated-only one source device (to guarantee timing requirements), shared-multiple devices access the medium using CSMA/CA (carrier sense multiple access/collision avoidance) to accommodate busy traffic and alarms.

In order to provide better support applications with strict time requirements, besides the use of TDMA, there is a flow control method with priority assignment. Messages can be given two different levels of priorities.

The communication reliability is increased through frequency diversity. ISA-100.11a presents three different schemes of channel hopping. In channel hopping, the communication between devices uses a different channel on every transmission. The choice of channel follows a pseudo-random sequence of the available channels (hop sequence). It increases data communication reliability, because it increases immunity against interferences. Another strategy used to improve reliability is the ARQ (automatic repeat request). The transmitted messages need to be acknowledged by the destination device. If it does not happen, then the message is retransmitted automatically in another channel.

In favor of minimizing possible interferences caused by other wireless networks (WirelessHART, ZigBee, IEEE 802.11, Bluetooth, microwaves, etc.), ISA-100.11a uses spectrum management techniques, such as *channel blacklisting*and *adaptive hopping*.

Based on the data received from the field device, regarding the RF spectrum, the system manager can interdict (prohibit) the use of one or more channels for a certain period of time. These forbidden channels go to a "*channel blacklist*" and they are not used in the hop sequence. The *adaptive hopping* is similar to *channel*

blacklisting, with the exception that the decision is taken by the field device based on the statistical data of some wireless parameters.

The traditional HART protocol uses *token-passing* as medium access control. When the WirelessHART was added to the HART specification, the protocol stack was altered to accommodate wireless transmission. As stated before, the WirelessHART radio interface is taken from the IEEE 802.15.4 standard. The medium access control is also TDMA to assure temporal determinism and to optimize the use of the device battery. The duration of the time slot is fixed (10 ms), and the time slots are organized in a superframe, which are periodically repeated to accommodate different types of traffic.

The slot can be dedicated-in order to obtain minimum latency-or can be shared to allow better use of the bandwidth.

The protocol is able to support several types of messages, such as one-way publishing of process and control values; spontaneous notification by exception; ad-hoc request/ response; and auto-segmented block transfers of large data sets.

To avoid interferences, disturbances, and collisions with other communication systems, WirelessHART also uses channel hopping, but only one scheme was defined. Regarding spectrum management, channel blacklisting is also used.

Mesh network and addressing

Both WirelessHART and ISA-100.11a use a mesh network. In this topology, a field device can be used to route the messages from the other devices to its final destiny. It increases the network range and also creates redundant paths (routes), mitigates problems with interferences and obstacles without user intervention, and helps increase network reliability.

The routes are configured by the manager of the network based on the information received from the devices. Hence, the redundant routes are continually updated based on the spectrum condition.

In WirelessHART and in ISA-100.11a, the network layer is in charge of routing and addressing. However, in WirelessHART, the addressing is done at a local level using an 8-byte address (EUI-64) or a 2-byte address (nickname), similar to what happens at a subnet level in ISA-100.11a. Regarding ISA-100.11a, the addressing and routing is done on a subnet level and also at backbone level. Its network layer is based on IETF RFC 4944 (6LoWPAN), which specifies the transmission of IPv6 packets over an IEEE 802.15.4 network, allowing the IP connectivity within field devices. The address scheme supports EUI-64 (64 bits), IPv6 (128 bits), and IEEE 802.15.4 (16 bits). It means that ISA-100.11a can take advantage of IPv6 to build highly scalable networks with a large amount of devices.

Security

The security mechanisms must be evaluated using the following criteria: conﬁdentiality of information, integrity of information, authentication of communication devices, and availability of information.

The confidentiality of information guarantees that only the authorized network members will have access to the information. In ISA-100.11a, the confidentiality is established through the use of state-of-the-art encryption based on AES-128, along with different keys in the data link layer (hop-to-hop security) and in the transport layer (end-to-end security). These keys have an expiration time and can be updated.

The integrity of the information is ensured through the inherited mechanisms from 802.15.4.

The MIC (message integrity code) is added to the data that will be transmitted. It allows the receptor to verify if data were corrupted or altered by an attacker. Additionally, the MIC and symmetric keys can be used to authenticate data packets transmitted between the network nodes.

Devices that are willing to join the network listen to and capture advertisement messages from routers. These advertisements contain the required information about the network to allow the device to assemble a *join request*. This request is sent to the system manager to ask permission to become a member of the network. The system manager processes this request with the security

manager, which is responsible for verifying whether the new device presents all the security credentials. Once the request is approved, the system manager sends a response to the router and admits the new device in the network.

The ISA-100.11a standard presents additional features to improve security. For example, the ISA-100.11a network is protected against several attacks, such as replay attacks, because all communication receives a time stamp, which is used to construct the *nounce*-an arbitrary number used only once to sign a cryptographic communication. The transport layer uses the *nounce* to indicate when the data packet was created. When the final destination attempts to authenticate the data packet, it can check if it was created outside of the valid time interval and it will discard the packet.

The join process can also make use of asymmetric keys, which does not require a secure initial exchange with a joining device.

WirelessHART also uses the AES-128-based encryption and an MIC to authenticate and verify the integrity of information in different layers with dynamic keys (i.e., a network key and session key). The joining process is similar to the one described previously. The device that is willing to join the network sends a *join request*, and if all goes well, it receives a *join response* from the network manager. However, WirelessHART uses a separate *join key* to authenticate the device in the joining process.

Since in both standards there is a central entity responsible for keeping a record of the devices belonging to the network, the probability that successful node replication attacks occur is very low.

The availability of the information can be threatened by interference (continuous or intermittent) in the communication channels. In the case of continuous interference in several channels, the channel blacklisting provides an efficient solution. If the interference is intermittent, then the channel hopping is an adequate solution. In addition, to avoid these types of problems, the transmission spectrum is continuously monitored.
None of the standards presents a mechanism to avoid collision attacks or against large number of joining requests. However, field devices report statistical data regarding the wireless communication, such as the number of attempted retransmissions and the number of unacknowledged transmissions that could be used to detect anomalies.

Application

In ISA-100.11a, the application layer is object-oriented and derived from Foundation Fieldbus, HART, and Profibus. Devices can report values and status (they even use the same units as Fieldbus). It also allows the creation of contracts between the system manager and the device, which will guarantee the quality of service (QoS) required by the application.

The application layer presents end-to-end communication, and it can support different communication modes such as publish/subscribe and client/server.

This object-oriented layer presents different types of objects that optimize the channel use, such as concentrator objects that collect the data from other objects and transmit them in one data packet, and the alarm-reporting objects that manage the transmission of alarms. The *upload* and *download* objects can be used to send large blocks of data, which allows the user to perform firmware upgrades and read waveforms from sensors. Finally, there are also generic functional blocks, such as analog in, analog out, binary in, and binary out to perform these more common I/O functions. The tunneling allows commands, and services from other networks (e.g., HART, DeviceNet, and Foundation Fieldbus) can be transmitted over the wireless ISA-100.11a. It ensures that the legacy protocols already used in the plant will be supported.

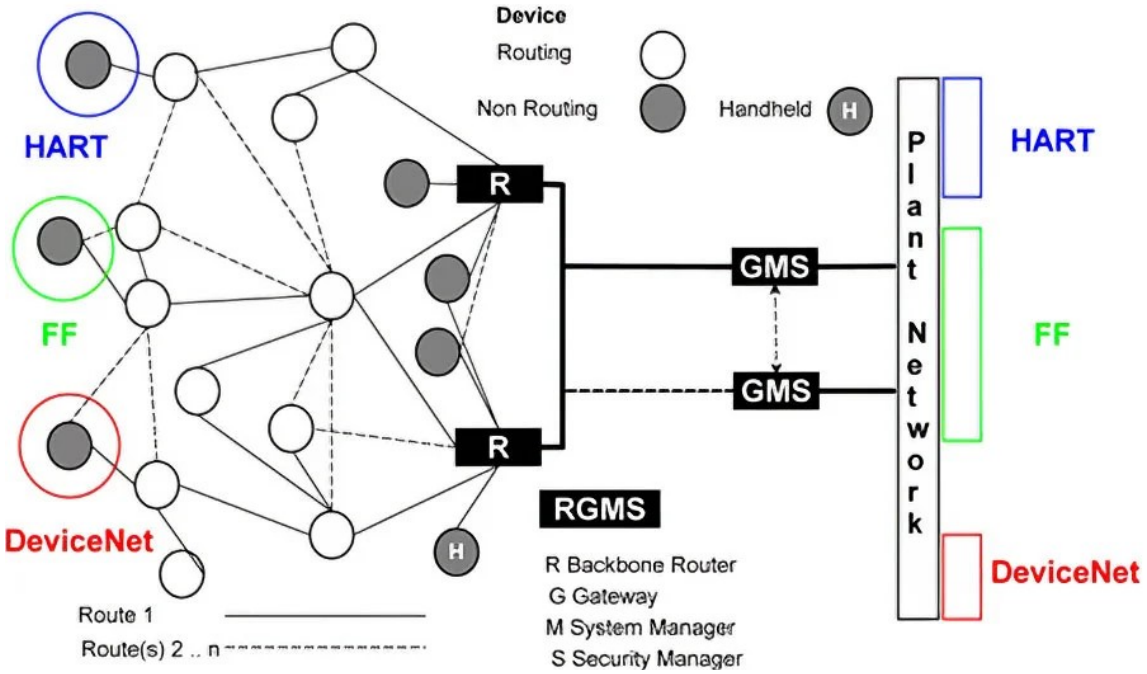


Figure 5. Tunneling

In WirelessHART, process data and setpoints can be periodically published in the network when there is a significant change in the values or if one of them crosses a critical threshold. Notification messages are automatically sent to the applications when the process variables or their statuses are altered.

In WirelessHART, the communication between the gateway and the field devices is done using commands and responses. Several types of commands and responses defined as well as their data type and the status indication required. The application layer is in charge of parsing the message and identifies the command number. Once it is done, it executes the command and provides the appropriate response.

Conclusion and comparison table

After this brief description of the standards, one can see they present several common features. However, the definition of the most appropriate standard for the user application will always be a difficult choice to make, since both standards are based on widely accepted and proven concepts.

From the user's point of view, there are several advantages to using a wireless network for industrial automation. Conversely, the user must be confident in adopting such innovative solution, and the existence of

two different standards does not help. It would be beneficial for the end user if both standards committees were to join together to develop one single wireless network standard for industrial automation and process control, without losing the investments already made.

In this sense, the subcommittee ISA100.12 is working on the convergence of the two standards. In addition to the operational and financial benefits, this would allow a joined effort to provide a solution to some of the open issues.

The first is that neither of the standards is able to meet hard, real-time requirements (latency in 1 to 10 ms range). This would require development of new technologies to be used in the physical layer.

Another important issue is QoS in heterogeneous networks. Although the subcommittees ISA100.12 and ISA100.15 are working to make ISA-100.11a more compatible with WirelessHART and Zigbee, and the ISA-100.11a tunneling capability makes it compatible with legacy protocols, such compatibility requires protocol translation, which can increase the latency and decrease the performance since some protocol features may have to be disabled.

The third issue is related to the QoS in mesh networks. In this topology, the data packets transmitted between the same peers can use different paths, which means that they may present different delays. Both standards do not describe the necessary mechanisms to guarantee QoS in

this situation.

Regarding security, new procedures to deal with collision and joining requests flooding attacks will have to be developed.

Finally, new tools still have to be developed to help the engineers to plan and design the deployment of these wireless networks to make sure they will meet the necessary requirements, such as latency, throughput, and fault tolerance. Also, it is important to develop new methodologies to monitor the network to prevent attacks and deal with the huge amount of information available to diagnose the equipments and the plant.

The comparison table summarizes some of the features of the two standards.

	WirelessHART	**ISA 100 Wireless**
Architecture	*Access pointsField devices (I/O and router, router)*	*Backbone routerField devices (I/O only, router, router and I/O) Multiple subnets*
Physical layer	*IEEE 802.15.4*	*IEEE 802.15.4*
Data link layer	*IEEE 802.15.4 + (TDMA, Channel hopping (1), mesh topology)Fixed*	*IEEE 802.15.4 + (TDMA, Channel hopping (3), mesh topology)Configurable*

	time slotPriority levels (4)	*time slots Priority levels (2) subnets*
Network layer	*Based on HART 16- and 64-bits addressing*	*Based on IPv66LoWPAN (IETF RFC4944) 16-, 64- and 128-bits addressing*
Transport layer	*Auto-segmented transfer of large data sets, reliable stream transport*	*Connectionless service UDP (IETF RFC768) 6LoWPAN compatibility*
Application layer	*Command-oriented, Predefined data types, Support HART protocol*	*Object-oriented, Support legacy protocol (tunneling), QoS contracts*
Real-time support	*TDMA Priority levels (4)*	*TDMA Priority levels (2) QoS contracts*
Reliability	*Mesh topology Channel hopping (1)*	*Mesh topology Channel hopping(3) Adaptive hopping*

	Channel blacklisting ARQ	*Channel blacklisting ARQ*
Security	*AES-128 encryption Security mechanisms in different layers Keys have an expiration time Interference protection (blacklist, channel hopping)*	*AES-128 encryption Security mechanisms in different layers Keys have an expiration time Interference protection (blacklist, channel hopping)*
Join process	*Symmetric method*	*Symmetric and asymmetric methods*
Provisioning	*Cable connection to the maintenance port using handheld*	*Provisioning device OTA configuration (over the air)*

About the Author

Márcio S. Costa, M.Sc, a senior engineer, has worked as a leader of automation and instrumentation projects for more than 20 years. Currently, he works as a consultant at Petrobras-BR, is a collaborator researcher in networks for industrial automation at Rio de Janeiro State University (UERJ), occupies the Education Chair in a working group

of the ISA-RJ, and is a professor of industrial networks and protocols at Brazilian Institute of Petroleum (IBP).

Connect with Marcio

About the Author

Jorge L. M. Amaral, D.Sc., is an associate professor of the Department of Electronics and Telecommunications Engineering-Rio de Janeiro State University (UERJ) and researcher at The Industrial Networks and Automation Systems Laboratory (LARISA-UERJ). His main research interests are computational intelligence, machine learning, electronic instrumentation, and wireless networks for industrial automation.

Connect with Jorge

A version of this article also was published at InTech magazine.