WirelessHART® networks: 7 myths that cloud their consideration for process control

Misinformation about WirelessHART® networks prevails among many instrument engineers in the process industries. This article attempts to set the record straight by debunking 7 myths about these networks.
1. **WirelessHART is unsafe**

False. WirelessHART is safe. But why? A variety of tools make this so.

**Encryption**—A WirelessHART network always encrypts communications. The network uses a 128-bit AES encryption system (Advanced Encryption Standard)—a standard in several fields of wired communication. The encryption cannot be disabled.

The security manager in the WirelessHART gateway administers three parameters. The parameters include:

- Network ID,
- Join key and
- Session key.

Integrating a WirelessHART transmitter into a network requires a network ID and join key. After these are entered, the transmitter first searches for the network with the right ID. If it finds such a network, it sends a "Join Request" message with the key configured. The WirelessHART gateway checks the join key of the transmitter. If correct, the network accepts the transmitter. A session key encrypts the communication. Every network subscriber gets a separate session key. So it is possible only to be accepted into a network with the join key, but this does not decrypt the encrypted communication of the other subscribers.

**Access list**—After completing commissioning, the acceptance of new network subscribers can be disabled. In this way, no new network subscriber can be integrated into the network even if the network ID and the join key are correct. To integrate a new subscriber, this function can either be disabled or the UID (Unique Identifier = unique device serial number) of the network subscriber can be entered manually into the gateway. A network subscriber that does not appear in the subscriber list of the gateway is also ignored by the other network subscribers when messages are forwarded.

**Join counter**—If a WirelessHART transmitter is integrated into a network, it records this information in the so-called join counter. If the device is restarted and if it joins the same network, its join counter is increased. Both the network subscriber and the gateway have a join counter. They cannot be read out. If a device now tries to integrate into a network with a join counter that does not match the gateway, the gateway declines it. As a result, it is not possible to substitute one device with another without this being noticed, even if both have the same UID.

**Nonce counter**—Each transmitted message has a nonce counter. This is composed, among others, of the UID and the number of messages sent by the transmitter so far. Each message is marked uniquely with this mechanism. If a message gets intercepted to resend it again later,
it will be identified as outdated and thus rejected. This technique obstructs any manipulation in the communication.

**Modifying the network parameters**—The network parameters, network ID and join key can only be changed by the gateway itself or at a WirelessHART transmitter locally via a service interface or the display. No network subscriber or hacker in the network can modify this information.

**2. WirelessHART networks are too expensive**

Yes, WirelessHART devices are more expensive than wired HART devices. But, more importantly, how do costs for the overall communication investment compare?

WirelessHART devices are more expensive because:

- they contain ultra low power electronics to get long battery life
- they require measures to achieve explosion protection
- they use high frequency components.

But the whole solution must be considered, not just the devices. The solution involves engineering hours, labor hours and material.

**Infrastructure for wired devices**—The measurement signal of a new wired device usually must be connected to a PLC or DCS to use the data. This is either done by system's local I/O, a remote I/O system or a fieldbus connection. While this is easy during a new installation (greenfield), this could rise to a challenge for an existing installation (brownfield). To add the new component, spare capacity must exist (free slots, channels, terminals). Another issue concerns bringing the wires from the measurement to the I/O, requiring routing and protection of the device cabling, junction boxes, cable trays and glands, and all of their accessories. All this infrastructure must be ordered, prepared and installed. Also an accessible location must be found. Otherwise this access must be gained by other means, such as by setting up a scaffold tower.

**Engineering and labor costs**—Before all this, engineers must develop a plan involving where cables can run, which I/O makes sense, and how this work can be executed. The documentation must be continuously updated to track the location of wires.

**Hazardous areas**—These areas further increase the difficulty and efforts compared with general purpose areas. Engineers must consider local conditions and technical issues. An expert in explosion protection must verify the planned installation, including a secure power supply and zone separation.
**Wireless device break-even points**—Of course, some planning and installation is also necessary for a WirelessHART network. The chief difference involves the effort since only the WirelessHART gateway requires a powered installation. Local conditions will determine affordability. The WirelessHART devices can be installed in whatever way optimizes the measurement. And separation of explosion zones happens by default since no physical connection exists between the zones apart from the mechanics (e.g. a thermowell).

But how much could be saved? The wireless solution gains a breakeven point for the first installation of three or four WirelessHART devices plus one gateway. For example, consider take a well-known device, a monitored heat-exchanger having two inputs and two outputs. The heat exchanger will need four temperature transmitters. So assume:

- 4 temperature transmitters,
- a distance of 100 meters between control room and the scheduled junction box and
- 10 meters of cables between the junction box and each transmitter.

Realizing this solution will account about USD20,000, where just 20% represents the cost of the temperature transmitters.

In the case of wireless, assume:

- 4 temperature transmitters and
- a distance of 10 meters between control room and the WirelessHART gateway.

Realizing this solution will cost about USD15,000, where 80% represents the cost of the WirelessHART devices and the gateway.

So the wireless solution saves 25% compared the wired one. And it will save even more in time. In fact, this solution could be available in a quarter of time. And the next heat exchanger?
Wired, it will cost an additional USD20,000. Wireless, it will just add the cost of the new WirelessHART devices since the gateway is already available.

While you could get three wireless solutions for the price of two wired solutions, you could get four wireless solutions in the same time as one wired solution!

### 3. WirelessHART networks are unreliable

A communication link for process control or even monitoring must be reliable and available as needed. Everyone knows examples of communication failures just when needed. So can a wireless communication ever be reliable? Surprisingly it can be more reliable than cable. This is achieved by using a time-synchronized, frequency hopping, meshed network.

**Meshed network**—As mentioned earlier, every network has a gateway that transforms the wireless data into wired data ready for a DCS or PLC. Most wireless communication has a star architecture, meaning all network participants connect only to the star center or head. WLAN and mobile phone communication are prominent examples for a star topology. WirelessHART has a mesh, rather than a star, architecture. Within a meshed network the participants are communicating with the gateway and additionally among one another. Furthermore, the wireless devices tell the gateway which other participants they can communicate with.
Other wireless participants in range are called neighbors. The gateway analyzes information about neighbors and creates a routing table. This table contains the information about which network participant has which neighbors. As participants can reach each other, they can also route the data packets from and to their neighbors. In this way, the gateway can create redundant communication paths for each network participant. Should one communication path fail, the sender will automatically switch to a redundant path. Since each transmitted packet must be acknowledged by its receiver, it's easy to recognize a broken link.

**RSSI and path stability**—The radio signal strength indicator (RSSI) indicates the quality of a communication link to the gateway. Knowing this, the gateway can determine if enough reserve strength is available or if the signal level is already too low. Since the gateway gets the RSSI of each single communication link, it can readily distinguish between high and low level signals. Additionally, the gateway counts the data packets lost during transmission for each link. By comparing the total number of transmitted packets within a network, the gateway can recognize paths with high losses and retransmissions. It uses both kinds of information to identify good or bad paths in a network. So the gateway now can pick the good paths that the network participants should use to communicate.

**FHSS and DSSS**—To ensure reliability, WirelessHART makes use two techniques: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). WirelessHART is a frequency hopper in its 2.4 GHz band. After each transmission between two network participants, the radio channel changes. Hopping across multiple frequencies is a proven way to sidestep interference and overcome RF challenges. Should a transmission be blocked, the next transmission will be to an alternate participant on a different frequency. The result is simple but extremely resilient in the face of typical RF interference.

DSSS transmits more information than necessary. It sends eight bits for each single information bit. Every bit is encrypted in such a way that the main bit is restored even if less than half of the eight bits are received. This makes the communication more robust against short disturbances and data does not need to be re-transmitted, which saves time, bandwidth and energy.

**Redundancy**—Because each WirelessHART device can route data for other devices, it is possible to set up a network topology with redundant paths for each network participant. Having at least three independent and good communication paths ensures a reliable communication with the gateway. The gateway can determine all information concerning topology, network traffic, and quality of the communication paths.

4. The range of WirelessHART networks is too short
A common question concerns the maximum distance that can be covered by WirelessHART. Answers relating to surroundings and obstructions sometimes confuse the issue. What range does a WirelessHART device actually need to achieve? The practical answer revolves around the network setup, bandwidth, and repeaters.

**Network setup**—The ultimate aim of the network is to get the wireless data to a gateway that transforms it into wired data ready for a DCS or PLC. A properly setup WirelessHART network has at least three devices within range of each other, including the gateway. This ensures a reliable connection to the gateway. In addition, the gateway should be located towards the middle of the network. Otherwise devices near the gateway become pinch points that shorten battery life and risk network failure.

Following these recommendations for network setup should provide coverage of nearly 200 feet, even in a highly obstructed area. In reality coverage will often expand to 300 feet. Large installations will include installing more measuring points. This automatically expands the network coverage as every new WirelessHART device will route the communication for other devices.

**Frequency spectrum and bandwidth**—To minimize power consumption, reduce the number of device transmissions to whatever is necessary to serve an application. It’s important to keep the number of re-transmissions as low as possible, too. To avoid collisions, WirelessHART uses time-division multiple access. This means each link has its unique time slot to communicate. If this link fails for some reason, transmission passes to another link.

WirelessHART uses the license-free 2.4GHz ISM band. This band can be used by any other application as well (Industrial, Scientific and Medical Band). So WirelessHART must share its bandwidth with all other technologies working in the same band. And this will cause collisions and re-transmissions for each device within the network since these different networks are not synchronized to each other (WLAN, Bluetooth etc.).

To keep the network reliable and stable, time slots for re-transmissions must be reserved even if rarely needed. Faster update rates of a device require more time slots, and the total available network bandwidth decreases. In fact, having an update rate of 1 second could easily result in a maximum amount of 12 devices within one gateway. As an alternative, operating two WirelessHART networks in parallel is possible, but this will also lead to collisions, reducing the bandwidth of both networks. As opposed to one long range network, having two short-range networks covering different areas with only a small overlapping areas will increase their stability and device battery lifetime.
**Repeater or routing device**—Sometimes a measuring point is too far away from a network to connect. This can be corrected by installing additional routing devices. Any WirelessHART device will do, but the best fit is a device that is small, requires minimum effort to install, and provides an easily replaceable battery.

5. **WirelessHART devices constantly need new batteries**

What would a wireless device be that requires a power cord—not completely wireless of course. So an independent and reliable power supply is mandatory. Batteries can fulfill this requirement, but with the disadvantage of their finite energy. For sure, dead batteries must be replaced to get a battery powered device running again. But how big is this disadvantage really?

ABB’s WirelessHART devices use an industrial-standard D-size primary cell. This cell was especially designed for extended operating life over a wide temperature range of -55°C to +85°C to fulfill the requirements of process industries. But how much lifetime is achievable? It depends. Battery life is not predictable as a hard fact. Rather it behaves like the fuel consumption of a car. Some need more, some need less, depending on acceleration and speed, vehicle weight, and traffic.

To maximize battery life, ABB electronics have an ultra-low power design—less by a factor of 20 compared to a conventional 4-20 mA HART device. All components have been chosen by their functionality and their current consumption. The design goal is to consume the minimum energy possible, including software. For example, sub-circuits power down if not needed. So the sensor itself powers down between two measurements as well as the display. If the update rate is slow enough, the device will fall into a "deep-sleep mode" between two measurements as often as possible.

The update rate is the user-defined interval at which a wireless device initiates a measurement and transmits the data to the gateway. The update rate has the largest impact on battery life—the faster the update rate, the lower the battery life. This means the update rate must be as slow as possible, but still meet the needs of the application. Depending on the time constant of the process variable, the update rate should be 3 to 4 times faster for monitoring open loop control applications and 4 to 10 times faster for regulatory closed loop control and some types of supervisory control.

A special attention should be spent for update rates faster than four seconds. These faster rates will prevent the device from going into the deep-sleep mode. They will consume much more power as well, impacting the total number of devices that can be handled by one gateway.
**Burst command setup**—All WirelessHART devices are able to burst up to three independent HART commands. Of course, the update rate of each command could be setup separately. But as described before, the device tries to fall into deep-sleep mode as much as possible. By default, the update rates are set up as multiples of each other, giving the device the best conditions to save as much energy as possible.

**Network topology**—Mesh-functionality can also influence the battery life since each device has routing capability. If one device acts as a parent for another device and both devices are setup with the same burst configuration, the parent must transmit data twice as often as its child. The most power saving network topology has all devices within effective range of the gateway. While this is rarely possible, it’s more important to think about this before placing the gateway. To extend battery life, the gateway should be placed more or less in the middle of a planned network. In this way, the devices acting as parents would be equally distributed—not relying on only a few devices to route data.

Knowing all this about battery life, what can be expected? Taking all these energy saving recommendations into account and assuming the following:

- bursting one command
- having a direct communication path to the gateway
- having three child devices with the same update rate and
- using the device at 21°C.

Under these conditions the battery life could last up to

- 5 years with an update rate of 8 seconds
- 8 years with an update rate of 16 seconds and
- 10 years with an update rate of 32 seconds.

If a faster update rate is favored or if the device has a key position for routing within the network, ABB’s Energy Harvester option would reliably relieve the battery.

And last—but not least—ABB’s WirelessHART transmitters use standard batteries, making them easy to procure. This will not save battery life, but will save money.

**6. WirelessHART networks require specialists to set up**

A lot of engineers think that setting up a wireless network can be an arduous and annoying job. Getting everything running, ensuring safe communication and including all desired network participants can take much time. But is this true? What do we really need to do to get a WirelessHART network running?

The wireless elements of a WirelessHART network include:

- field devices connected to the process or plant equipment. Of course, they all be WirelessHART capable.
- a gateway that enables communication between host applications and the field devices in the WirelessHART network.

- a set of network parameters: Network ID and Join Key.

That's it. Now you can set up your network in a few steps:

**Input of network parameter**—To get the gateway into proper operation you must input the network parameter. This could be done easily via the integrated web browser of the WirelessHART gateway. Most gateways provide this comfortable way of configuration. Now the network participants can join the network. They also need the network parameters. Here's the easiest way: order them with the desired network parameters. Otherwise you must input parameters manually.

Since all WirelessHART devices provide a maintenance port, you can use the tools already available for wired HART devices; this avoids the need for additional equipment. And they can be operated just like the wired HART devices. Additionally, ABB WirelessHART devices can be brought into operation just by using their HMI. Again, you need not concern yourself with security because it's built-in.

**Update rate**—All WirelessHART devices burst their measurement values. By default, all ABB WirelessHART devices burst HART command 9 every 16 seconds. This includes the dynamic variables PV, SV, TV, QV (for devices with multiple outputs) with the status of each and the remaining battery lifetime. They burst HART command 48 every 32 seconds—the additional device status information. So typically, you needn't deal with the burst configuration. Nevertheless the commands or the update rates can be changed as needed.

**Placement of field devices and gateway**—Start with the gateway installation first. Find a suitable place for it and power it up. As it is the connection between host application and the WirelessHART network it will need a power supply and wired connection to the DCS. After the WirelessHART devices have been prepared they now can be installed in the field.

Installation can be done in the same way as well-known for wired HART devices. But WirelessHART devices require less effort because they have no wires. This is especially true in hazardous areas where nothing will cross the zones and no output device needs to be checked with its ex parameters against an input device. After the devices are powered up they will appear in the network automatically. Everything else is handled by the gateway; a user does not need to take care of meshing the net or which device communicates with which.

7. WirelessHART is too slow
When asked for the required speed to cover an application, a user will often answer: as fast as possible. The update rate for WirelessHART devices within a network can be configured individually between once per second and once per hour. Is that fast enough for everything? Let’s look at a few considerations before answering too quickly.

**Usage**—At first, examine the uses for which a WirelessHART network is actually intended: condition monitoring and process supervision. Remember, the wireless sample/update rate should be:

- 3 to 4 times faster than the process time constant for condition monitoring and open loop control applications
- 4 to 10 times faster for regulatory closed loop control.

For measurements in the process industries today, more than 60% simply monitor conditions—not for control applications. So a WirelessHART update rate that's greater or equal to one second may fit many of these applications. Of course other factors may apply too.

**Timing**—For wired devices, update rates and timing aren’t often considered. Engineers and operators assume the values in the DCS are the real time values from the process, achieved by oversampling. In fact, signals often are converted and scaled from the initial sensor element before reaching the DCS. So in a traditional wired installation, the measurement values also have latencies. Instrument engineers are rarely aware of these, but just assume these values are timely enough. In the world of WirelessHART, the data packets have time stamps that spell out how old a measurement value is. This indicator lets engineers assess latencies and properly react to them.

**Thinking differently**—Instrument engineers must know how fast a process value can change for both control applications and condition monitoring. No additional knowledge is needed for WirelessHART. For wired installations, this knowledge affects a DCS or PLC. For WirelessHART, it affects the planning of the network. Because the bandwidth is a limited resource, engineers must consider how fast the update rate needs to be rather than how fast it could be.

**Comparing speeds**—The traditional FSK-HART loop provides a speed of 1200 bits per second. In practice, HART on RS-485 cable is limited to 38,400 bits per second. WirelessHART provides a speed of 250,000 bits per second. This means WirelessHART is more than 200 times faster than wired HART and even six times faster than HART over RS-485 cable. By allocating the "Fast Pipe" to a network participant, the wireless gateway provides a high-bandwidth connection that is four times faster than normal. This is ideal for transmitting a large amount of data, such as up- and downloading a complete configuration.
**Terminology**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>A Network Device containing at least one host interface (such as serial or Ethernet), acting as ingress or an egress point.</td>
</tr>
<tr>
<td>Hop</td>
<td>A term used to describe the data being passed from one device to another as a means to lengthen the transmit distance. Also used to denote the function of changing channels.</td>
</tr>
<tr>
<td>Join</td>
<td>Process by which a Network Device is authenticated and allowed to participate in the network. A device is considered Joined when it has the Network Key, a Network Manager Session and a normal (not join) superframe and links.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>Adjacent nodes in the network.</td>
</tr>
<tr>
<td>Nonce</td>
<td>A number constructed so as to be unique to the current packet to ensure that old communications cannot be reused in replay attacks</td>
</tr>
<tr>
<td>Security Manager</td>
<td>An application that manages the Network Devices security resources and monitors the status of the network security.</td>
</tr>
<tr>
<td>DCS</td>
<td>Distributed Control System</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>UID</td>
<td>Unique Identifier</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency Hopping Spread Spectrum</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>Child</td>
<td>A device that receives time information from another mote is its child. A child forwards data through its parent and has no direct communication path to the gateway.</td>
</tr>
<tr>
<td>Parent (or time parent)</td>
<td>A device that serves as a source of time synchronization. A mote's parent is one hop closer to the gateway and forwards a child's data towards this.</td>
</tr>
<tr>
<td>Node (or device)</td>
<td>An addressable logical or physical device attached to the WirelessHART network.</td>
</tr>
<tr>
<td>Link</td>
<td>Communication path between two network devices</td>
</tr>
</tbody>
</table>

**Related links**