# Whitepaper

## Getting the Most Out of Your *Wireless*HART System

Author:
Garrett Schmidt
Wireless Product Manager
Phoenix Contact—Americas Business Unit
gschmidt@phoenixcontact.com

ION05-15.000.PR5

Table of contents

## Introduction

Standardized nearly 30 years ago, HART (Highway Addressable Remote Transducer) is the most broadly supported protocol in the world for the process industry with over 40 million devices installed. HART was originally developed as a way to make analog process measurement devices "smarter" by superimposing digital data on a 4…20 mA signal loop; however, it is estimated that less than 10% of the installed devices are connected to a HART capable control system.

Today, more methods of accessing HART data are regularly being introduced – including wireless and Ethernet. Backwards compatibility and manufacturer interoperability means you face no danger of getting locked into vendor-specific or regional solutions.

## History of Process Measurement

Process instrumentation has made several evolutionary advancements over the past 70 years, starting with pneumatics in the 1940s, to magnetic-based electronics generating 10-50 mA in the 1950s and 60s, to the currently used 4…20 mA signal. The advent of the "smart" instrument in the mid-1980s revolutionized the industry, allowing users to get much more than just a 4…20 mA signal, which represents the process variable, from their devices. Rich diagnostics, identification and preventative maintenance data permitted process optimization. The proprietary technology behind smart instrumentation was quickly released as an open standard, known as the Highway Addressable Remote Transducer protocol, or HART for short.

The HART protocol uses the Bell 202 modem's Frequency Shift Keying (FSK) modulation to superimpose digital communication signals at a low level on top of the 4…20 mA analog signal.

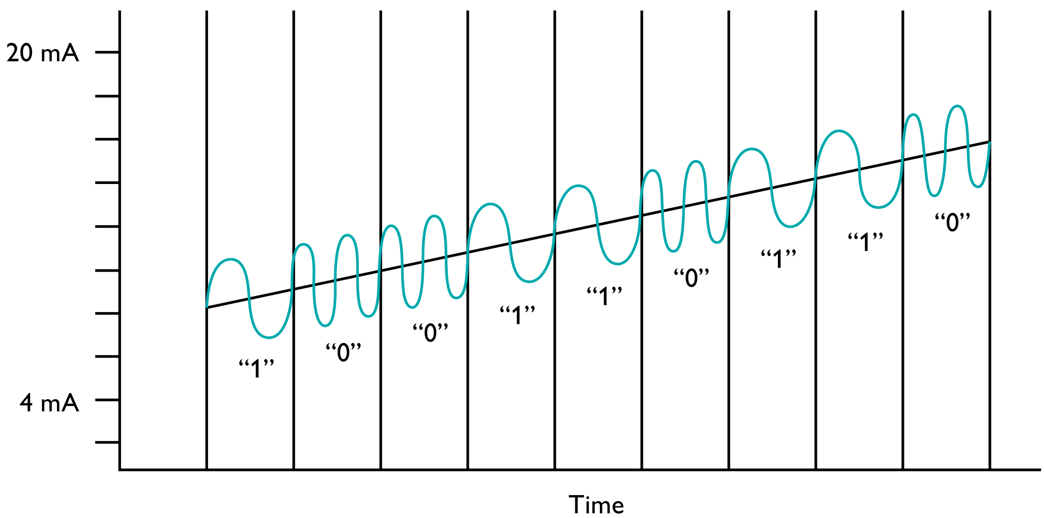


***Figure 1***
*HART data superimposed on a standard 4…20 mA signal*

## The Value of HART

The most basic use of HART allows users to configure their devices, setting the zero, span, and engineering units, calibrating the 4…20 mA loop, and selecting the sensor type. Most HART devices are multivariable, meaning that they can provide multiple measurement values, although only the primary variable is represented by the 4…20 mA signal.

Expanded use of HART-capable devices enables users to perform specialty operations, such as partial-stroke testing, data logging, and asset management using the information specific to each device type. These predictive maintenance operations help to increase plant availability and reduce operating costs.

## Why Go Wireless?

*Wireless*HART meets the critical wireless requirements of industrial plant environments, including reliability, noise immunity and latency, while still using the same maintenance and diagnostic tools as traditional wired HART devices. The technical advantages and cost benefits of *Wireless*HART provide many new opportunities for process automation in various situations.

The time to engineer and develop the expansion or construction of a process unit can be drastically reduced by installing wireless systems to replace both infrastructure and signal cabling. The up-front cost of a wireless network is often immediately lower than cabling and conduit costs, and the savings in labor and permits are enormous. A signal that previously took days to bring online using traditional wiring can now be commissioned within hours. This time savings and flexibility allows maintenance crews to deploy wireless nodes for temporary troubleshooting or to add "stranded" measurement points for safety or improved efficiency.

One of the primary reasons for the development of *Wireless*HART was to provide a method to access the HART data from devices that were previously installed. Plant asset management (PAM) provides an enhanced look into the efficiency of the process and health of the equipment—something that's only possible with the use of HART data.

## Types of *Wireless*HART Devices

The core technology behind *Wireless*HART has been hardened over many years of development and continues to improve. That technology has been integral in defining the features and functions of a *Wireless*HART network, as well as the device types themselves. Essentially, all *Wireless*HART devices can be classified as one of three types: an adapter, end device, or gateway.

The *Wireless*HART adapter connects an existing wired HART device into a *Wireless*HART network. The adapter connects to the 4…20 mA wiring to gather the HART signal while the 4…20 mA signal remains intact and functional. One *Wireless*HART adapter can collect HART signals from multiple devices, resulting in a lower installation cost. It can be powered from an existing analog loop, line powered from local DC power, or battery powered. The primary application for an adapter is to gather HART data from a previously installed HART device connected to a host with no HART capability. Alternatively, it can be used to add a second layer of automation.

A *Wireless*HART device (also called a wireless instrument) contains a radio integrated with measurement or monitoring capabilities. This allows easy expansion of an existing plant or a rapid deployment in a new installation. Measurement points previously inaccessible due to cabling costs or environmental restrictions can now be captured with ease. Many different sources can power these devices including solar, line, loop or battery.

A *Wireless*HART gateway actually consists of three pieces, according to the HART standard.

- The radio that connects to the remote field devices is known as the access point radio.
- The network manager is the software that acts as the "brain" for the mesh network, controlling the mesh links and managing the security and authentication of the field devices.
- Finally, the gateway is the portal between the plant network or host system and the *Wireless*HART network.

These three pieces may be co-located in one package, or split in any combination; however, the gateway interface defines the overall performance and capability of the mesh network to the user.

## *Wireless*HART Technology

The technology behind *Wireless*HART gives the standard its robustness and dependability. Built on an IEEE 802.15.4 radio platform operating in the license-free 2.4 GHz ISM band, *Wireless*HART is a globally available standard with a 10 mW radio transceiver. The IEEE 802.15.4 radio is frequently used for low power radio networks, including Zigbee.

The true strength of *Wireless*HART lies in the Time Synchronized Mesh Protocol (TSMP) that provides redundancy and fail-over in time, frequency and space to ensure very high reliability even in the most challenging radio environments. TSMP also provides the intelligence required for self-organizing, self-healing mesh routing. The result is a short-range (50-100 m in-plant) wireless network that installs easily with no specialized expertise, automatically adapts to changing environments, and can be expanded as needed.

There are five key components of TSMP that contribute to end-to-end network reliability, simple installation and power efficiency:

- Time synchronized communication
- Channel hopping
- Automatic node joining and network formation
- Fully redundant mesh routing
- Secure message transfer

By utilizing time-synchronized communications, each device in a network maintains a precise sense of time and thus remains synchronized with neighboring devices. All device-to-device communication occurs in a pre-scheduled time window (10 ms in length) for collision-free, power-efficient and scalable communication. In addition to scheduling transmissions over time, TSMP also schedules each transmission to occur on a different frequency. This provides a tremendous increase in effective bandwidth. It also dramatically reduces power consumption of the devices so that they can run for several years on a relatively small battery (depending on the update frequency).

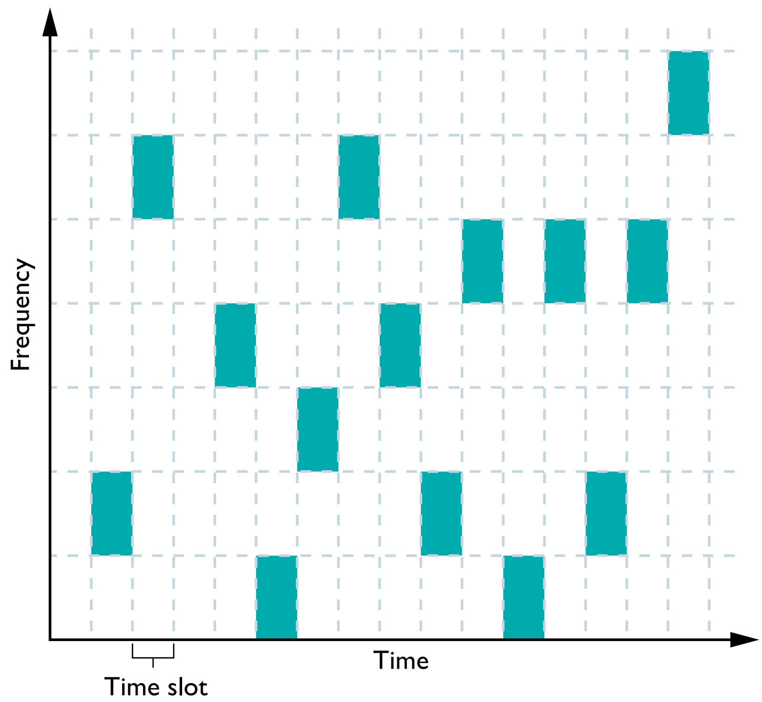


***Figure 2***
*Wireless*HART *is diverse in frequency and time*

## Transmitting the Data

The frequency-hopping spread spectrum (FHSS) is a well-known wireless transmission method. The FHSS method automatically changes the channel in a pseudo-random pattern for every data transmission. The goal is to tolerate interference in the band while still moving data from location to location. Each "hop" is essentially a narrowband transmission that takes a few milliseconds before moving on to another channel to transmit another packet of data. Because of this, the entire spectrum would have to be clogged with interference before the radio link will fail. FHSS is a very robust technology for interference-rich process applications.

Direct Sequence Spread Spectrum (DSSS) is another transmission method used in the license-free Industrial, Scientific, and Medical (ISM) bands. A DSSS radio mixes some application data with a special "spreading" code to spread the RF transmission across a wider portion of the spectrum. At the receiver, the code is removed to restore the user data. If any interference was received, the logic function to de-spread the data will suppress the damaged data. The resultant effect is known as coding gain. The wider channel used for transmission translates to higher data rates than frequency hopping allows, but radio failure will occur much sooner with DSSS.

*Wireless*HART uses a combination of FHSS and DSSS to provide both interference rejection (FHSS) and the coding gain (DSSS). This creates a very robust interference handling mechanism.

## Mesh Networking and Security

A key attribute of a TSMP network is its ability to self-organize. “Full-mesh” topology is implemented, so that every device has multiple redundant communication paths. There are no reduced function or non-routing nodes. A full-mesh topology with self-organizing and self-healing characteristics lets the network maintain long-term, hands-off reliability and predictability in spite of changing environments.

Every device has the intelligence to discover neighbors, measure RF signal strength, acquire synchronization and frequency hopping information, and then form or break links with neighbors. The network is defined by a unique ID that binds nodes together into a network. This allows multiple networks to coexist without sharing data or misrouting messages.

Three Pillars of Security provide mechanisms for encryption, authentication and integrity:

- 128-bit AES encryption guarantees that other parties cannot read information.
- Authentication verifies the sender’s validity through the use of packet source addresses protected by 32-bit Message Integrity Codes (MIC).
- Integrity ensures that the message is delivered unaltered via the same MIC.

Additionally, frequency hopping provides some level of security because of the pseudo-random hopping sequence. If an unauthorized receiver does capture one transmission, then it only has a 1 in 15 chance (for *Wireless*HART radios) of hearing the next transmission.

## Networking with *Wireless*HART

The concept of large-scale wireless mesh networks will only be as good as how all the information is presented. Implementing a *Wireless*HART network is not a difficult task. The finite types of devices and self-forming mesh capabilities take much of the guesswork out of the execution, but the technology has some limitations as the network grows. Larger networks will logically have devices that need more “hops” through the mesh to get data back to the host.

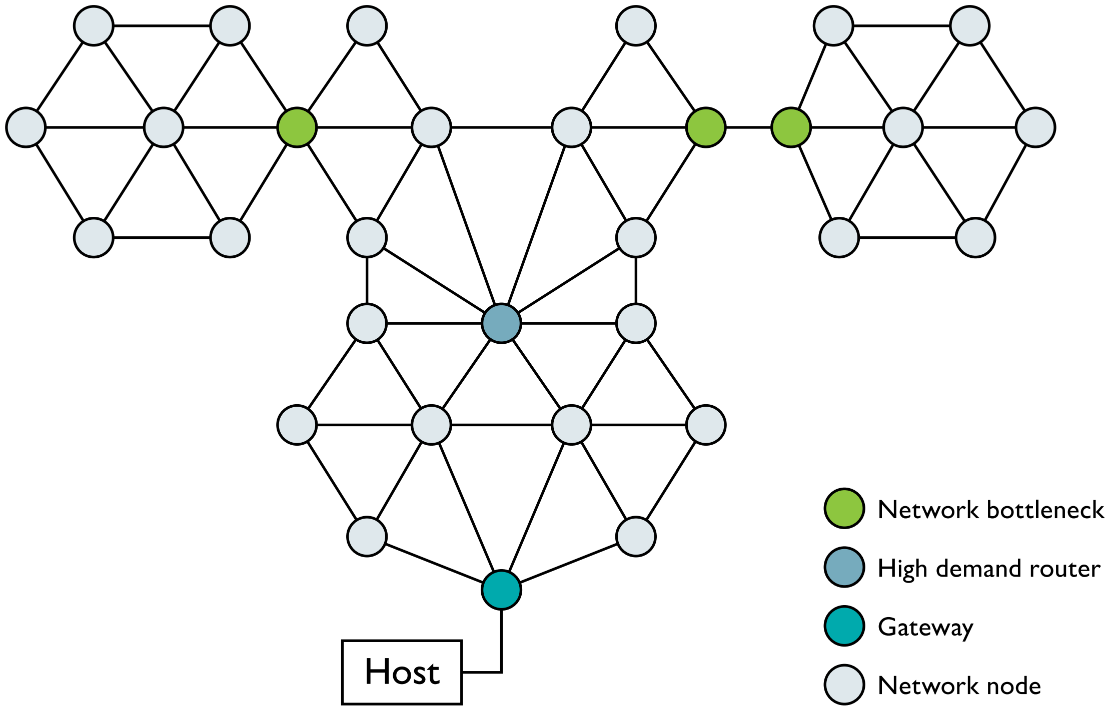


***Figure 3***
*Large Wireless*HART *Network Topology*

Larger networks of one hundred or more devices may also be harder to manage; the relatively short RF range of the radio will likely necessitate the installation of additional devices to act as repeaters. Bottlenecks in the mesh become more likely, and a failure there can bring down a large portion of the network.

Breaking the large network into several smaller ones has several advantages. Small networks reduce the overall network complexity because nodes have to travel through fewer hops to get to the gateway and then to the host. These simpler networks drastically reduce the probability of needing repeaters. This creates a more reliable (and potentially stable) network with no bottlenecks. By eliminating bottlenecks and high demand routers, the demand on battery-powered devices is also reduced, resulting in less maintenance.

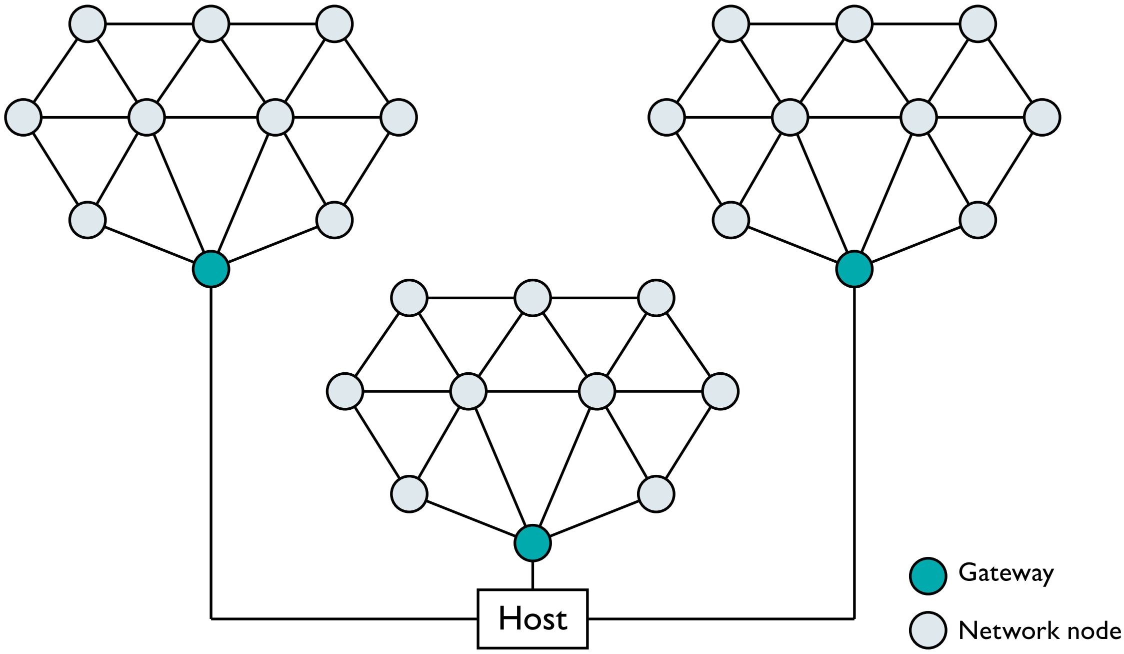


***Figure 4***
*Multiple Wireless*HART *networks*

Using the clustering method shifts the focus toward the gateway's capabilities. Because of the range of *Wireless*HART, this method demands that the gateways be moved closer to the devices in the field, so the physical connection to the host comes into question. One solution to this problem is a *Wireless*HART gateway featuring an integrated WLAN transceiver, such as the gateway developed by Phoenix Contact.

The 45 mm wide rail-mount RAD-WHG/WLAN-XD contains the *Wireless*HART access point radio, network manager, and gateway interface in conjunction with a WLAN client. The gateway connects up to 250 *Wireless*HART field devices and converts HART data to Modbus TCP or HART IP for easy integration into almost any control or PAM system.

To maintain a secure backhaul connection, gateway uses the 802.11i (WPA) standard with 128-bit AES encryption to protect the WLAN data. The WLAN transceiver can also be disabled, and the host connection can be made via the wired Ethernet port. All programming and diagnostics can be accessed via an embedded web server.


***Figure 5***
*RAD-WHG/WLAN-XD*


***Figure 6***
*RAD-WHA-1/2NPT*

The RAD-WHA-1/2NPT *Wireless*HART adapter brings further flexibility to a *Wireless*HART installation by supporting up to 4 HART devices. The multidrop feature is ideal for adding new measurement points or accessing diagnostic data cost effectively. The RAD-WHA-… can be line powered with 24 VDC, and supply loop power to the HART devices. The loop power is galvanically isolated from the supply voltage, making it a robust solution for installations which have "dirty" or noisy power, including pulse width modulated (PWM) solar charge controllers.

Many *Wireless*HART installations are in-plant, where line of sight is limited and there are many obstructions present. Further, most process measurement devices are installed low to the ground and very close to tanks, pipes, and other obstructions, making it difficult to achieve a quality RF signal. Therefore, the RAD-WHA features a patented removable antenna, making it a simple matter to connect a coaxial extension cable and remotely mount the antenna in an unobstructed location.

## Conclusion

Millions of HART devices are installed in process applications around the world, but the vast majority of these devices and their data are "stranded" due to the high cost of installing cable. *Wireless*HART, part of the HART7 standard, provides an easy-to-install, reliable and cost-effective way to connect these devices back to the host system.

## PHOENIX CONTACT

Phoenix Contact is a worldwide market leader for components, systems, and solutions in the fields of electrical engineering, electronics, and automation.

Our extensive manufacturing capability means that it is not just screws and plastic and metal parts that are produced in-house, but also highly automated assembly machines. The product range consists of components and system solutions for energy supply including wind and solar energy, device manufacturing and machine building, as well as control cabinet manufacturing.

With a wide range of terminal blocks and special terminal blocks, PCB terminal blocks and connectors, cable connection technology, and installation accessories, we offer innovative components. Electronic interfaces and power supplies, automation systems based on Ethernet and wireless, safety solutions for people, machines, and data, surge protection systems, as well as software programs and tools provide comprehensive systems for installers and operators of systems as well as device manufacturers.

Markets within the automotive industry, renewable energy, and infrastructure are supported by means of consistent solution concepts, ranging from engineering and maintenance to training services, in line with specific needs. Product innovations and specific solutions for individual customer requirements are created in the development facilities at our sites in Germany, China, and the USA. Numerous patents emphasize the fact that many developments from Phoenix Contact are unique. Working closely with universities and scientific institutes, technologies of the future such as E-Mobility and environmental technologies are researched and transformed into marketable products, systems, and solutions.



PHOENIX CONTACT GmbH & Co. KG
32825 Blomberg, Germany
Phone: + 49 5235 3-00
Fax: + 49 5235 3-41200
phoenixcontact.com