Getting the Most Out of Your WirelessHART® System

A White Paper presented by:
Garrett Schmidt
Wireless Product Manager
Phoenix Contact—Americas Business Unit
P.O. Box 4100
Harrisburg, PA 17111-0100
Phone: 717-944-1300
Fax: 717-944-1625
Website: www.phoenixcontact.com

PHOENIX CONTACT
INSPIRING INNOVATIONS

Getting the Most Out of Your WirelessHART® System

Key concepts:

- HART7, the latest revision of the HART standard, introduced wireless as a physical medium for the protocol
- WIrelessHART will rescue stranded data from inaccessible HART devices
- A WirelessHART gateway with WLAN capability eliminates the need for a cable backhaul, increasing flexibility and reducing costs even further

Introduction

Millions of devices around the world use the HART standard for process measurement applications, but the HART Communications Foundation estimates that as many as 90 percent of these are stranded, making the data inaccessible. WirelessHART is part of HART7, the newest revision of the HART standard. This new technology provides an easy and secure means of accessing this data, without the hassle of running wire and cable.

WirelessHART makes the HART protocol more usable, flexible and cost-effective, but there are still some complications. Larger networks in particular might experience problems, due to increased chatter. Creating a clustered network is one solution. A WirelessHART gateway with WLAN connection can provide a secure wireless backhaul connection, increasing the system's flexibility even more.

History of Process Measurement

Process instrumentation has undergone impressive advancements over the past 70 years, starting with air pressure 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.

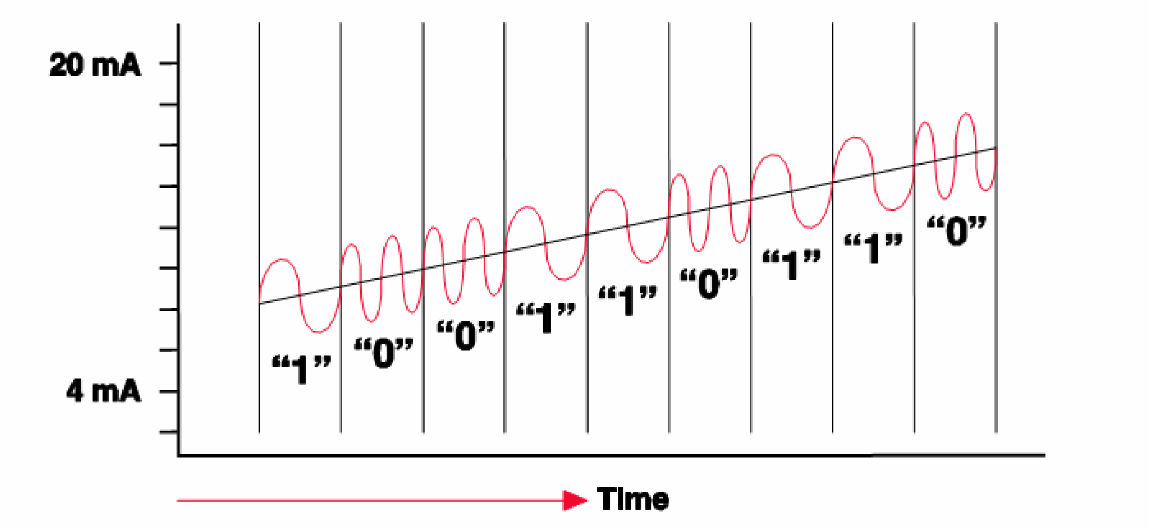
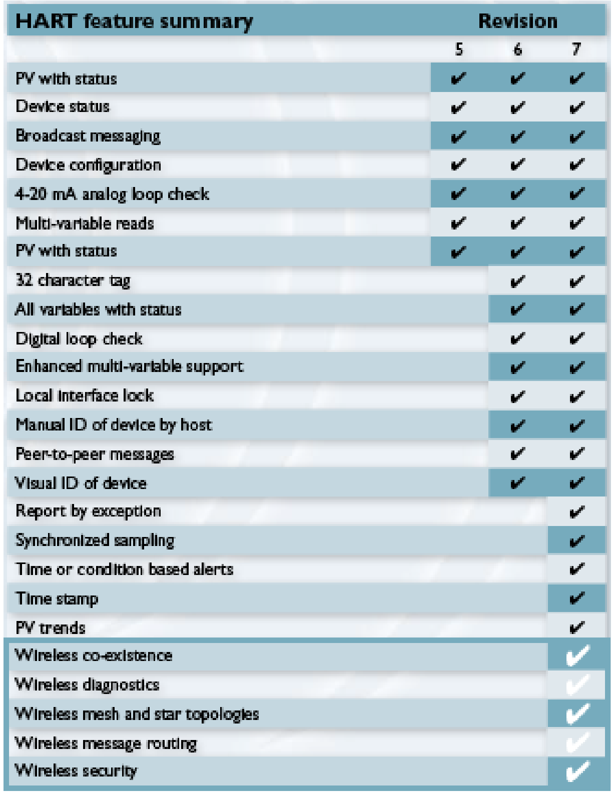


Figure 1: HART data superimposed on a standard 4-20 mA signal

The Advantages of the HART Protocol

One of the great advantages of the HART protocol lies in the wiring connections. The HART data shares the same wire as the commonly used 4-20 mA signal, thus simplifying the wiring methods and reducing the number of conductors required to gather all the data. Since a standard 4-20 mA signal is also used, HART devices are easily backwards-compatible to host systems that don't have HART capability. In fact, nearly 90 percent of the approximately 26 million installed HART devices are connected to legacy host systems that cannot utilize the HART data. However, using HART devices offers an additional benefit of a common programming tool for configuration. This makes the price premium over traditional analog instrumentation attractive to most end users.

Even still, the development of the HART protocol has been very organic over the years. The HART Communication Foundation, formed in 1993, continuously gathers feedback from users. The Foundation integrates innovative concepts from suppliers to improve the protocol. Several revisions of HART have been released over the last decade. The most recent revision, HART7 in 2007, introduced the next step in the evolution of the protocol by adding a new physical medium—wireless.



HART feature summary	Revision		
	5	6	7
PV with status	✓	✓	✓
Device status	✓	✓	✓
Broadcast messaging	✓	✓	✓
Device configuration	✓	✓	✓
4-20 mA analog loop check	✓	✓	✓
Multi-variable reads	✓	✓	✓
PV with status	✓	✓	✓
32 character tag		✓	✓
All variables with status		✓	✓
Digital loop check		✓	✓
Enhanced multi-variable support		✓	✓
Local interface lock		✓	✓
Manual ID of device by host		✓	✓
Peer-to-peer messages		✓	✓
Visual ID of device		✓	✓
Report by exception			✓
Synchronized sampling			✓
Time or condition based alerts			✓
Time stamp			✓
PV trends			✓
Wireless co-existence			✓
Wireless diagnostics			✓
Wireless mesh and star topologies			✓
Wireless message routing			✓
Wireless security			✓

Figure 2: HART Protocol Revision Features

Why Go Wireless?

The technical advantages and cost benefits of WirelessHART provide many new opportunities for process monitoring 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.

The primary reason for creating a wireless capability within the protocol was to enable facilities to gather previously unreachable additional diagnostic information. WirelessHART 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 technology behind WirelessHART 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, WirelessHART is a globally available standard with a 10 mW radio transceiver. The 802.15.4 radio is frequently used for low power radio networks, including Zigbee.

The true strength of WirelessHART 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
- and 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 small battery.

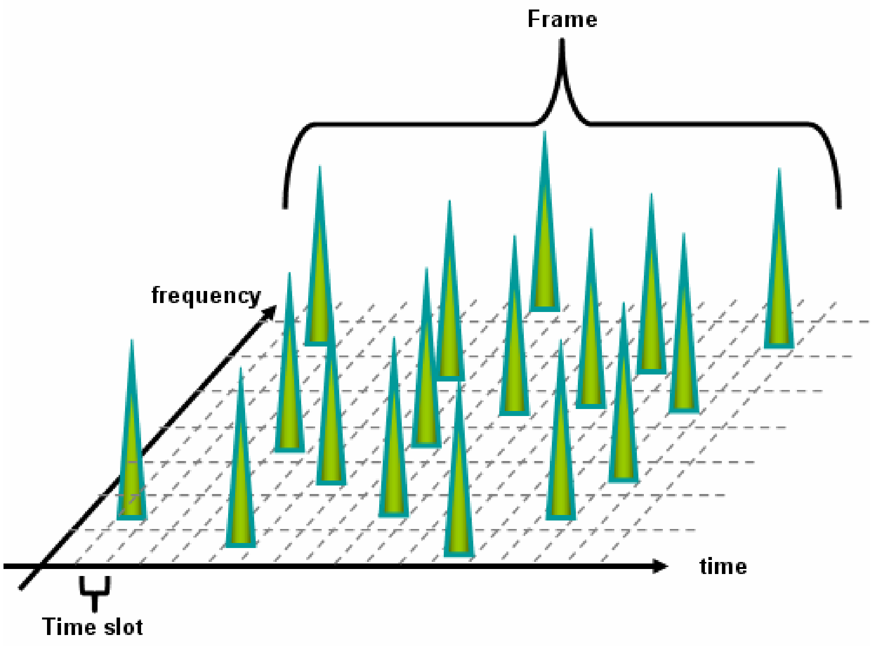


Figure 3: WirelessHART is diverse in frequency and time

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.

WirelessHART 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 WirelessHART radios) of hearing the next transmission.

Types of WirelessHART Devices

The core technology behind WirelessHART has been hardened over many years of development and continues to improve. Its flexibility and adaptive capabilities make it well suited for harsh industrial environments. That technology has been integral in defining the features and functions of a WirelessHART network, as well as the device types themselves. Essentially, all WirelessHART devices can be classified as one of three types: an adapter, end device, or gateway.

The WirelessHART adapter connects an existing wired HART device into a WirelessHART 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 WirelessHART adapter can collect HART signals from multiple devices, resulting in a lower installation cost. It can be loop, line, 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.

A WirelessHART 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.

What is now commonly becoming known as a WirelessHART 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 WirelessHART 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.

Networking with WirelessHART

The concept of large-scale wireless mesh networks will only be as good as how all the information is presented.

Implementing a WirelessHART 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. As the number of hops increases, so does latency.

Large networks will 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.

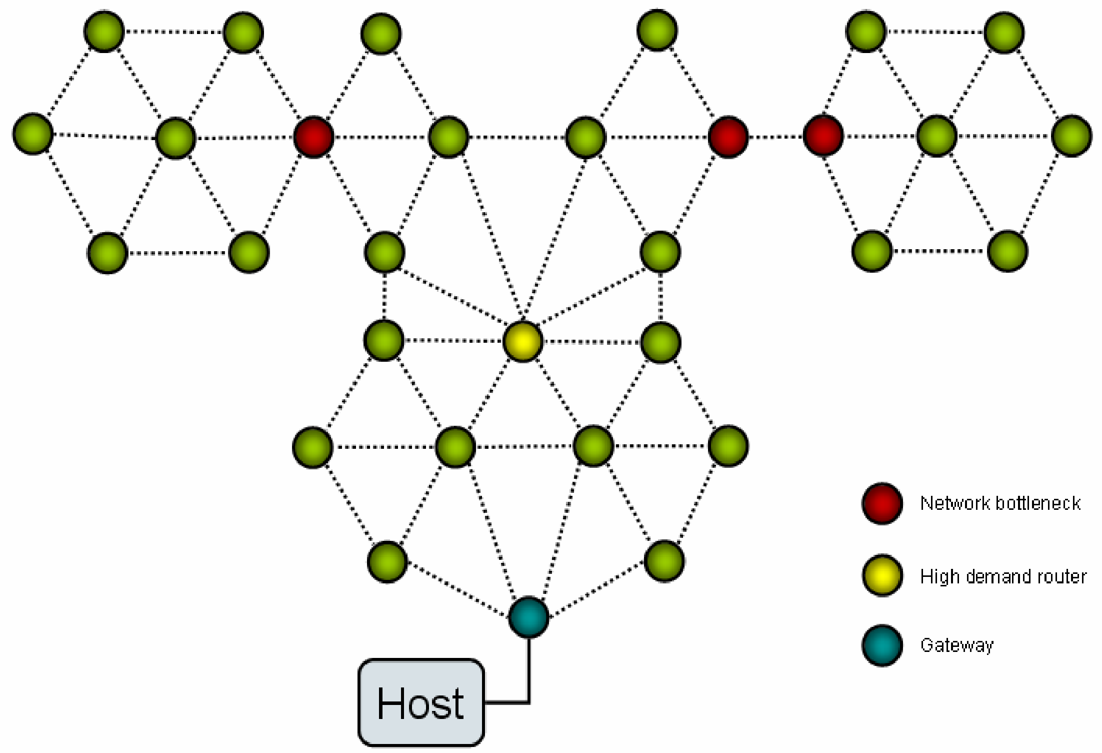


Figure 4: Large WirelessHART network topology

Breaking the large network into several smaller ones, or clusters, has several advantages. Clustering reduces overall network latency 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.

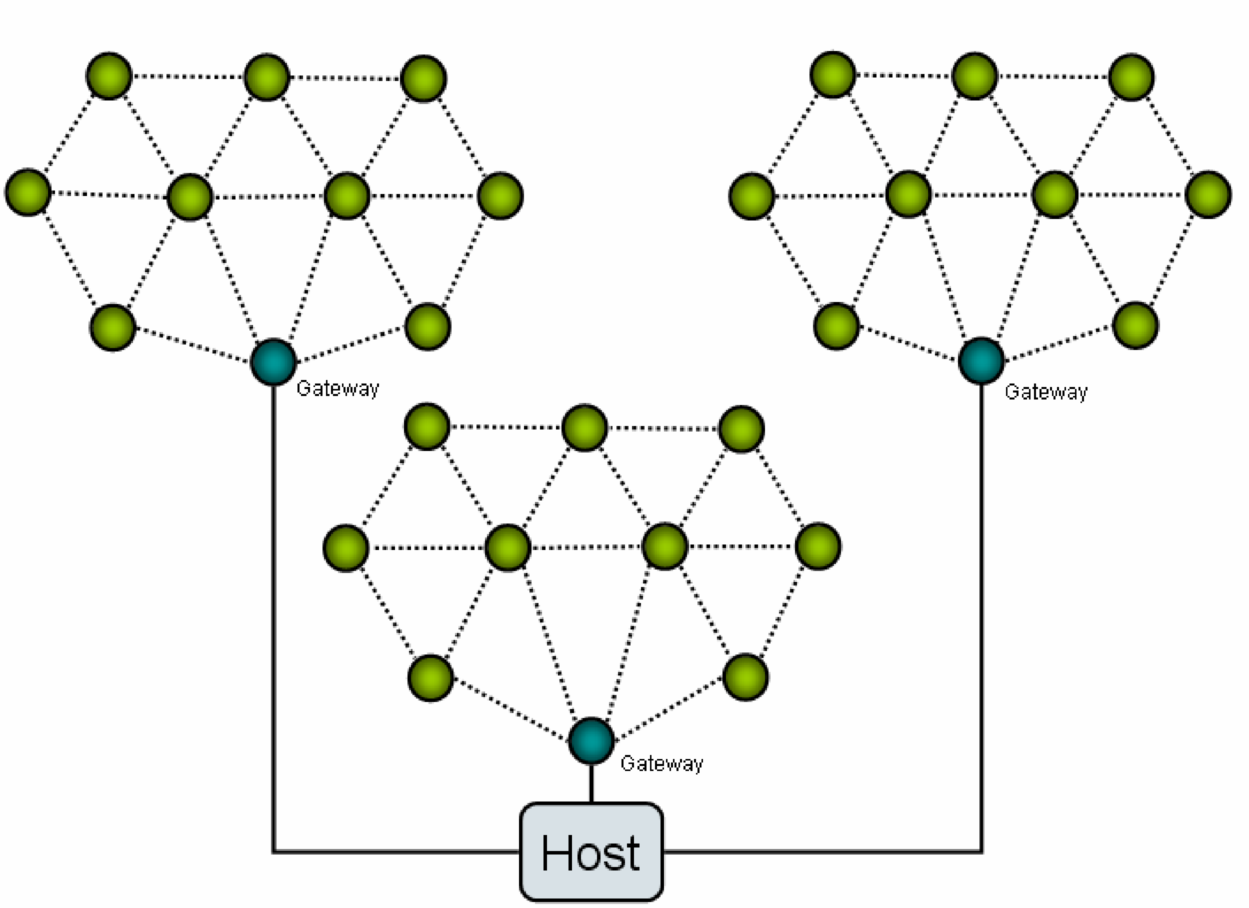


Figure 5: WirelessHART using clustering

Using the clustering method shifts the focus toward the gateway's capabilities. Because of the range of WirelessHART, 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. If a copper or fiber-optic connection must be made to the gateway in the field, then much of the cost savings associated with WirelessHART may be cancelled out, thus eliminating the backhaul cable, resulting in even more cost savings and flexibility. One solution to this problem is a WirelessHART 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 WirelessHART access point radio, network manager, and gateway interface in conjunction with a WLAN client. The gateway connects up to 250 WirelessHART field devices and converts HART data to Modbus TCP or HART UDP for easy integration into almost any host 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. The RAD-WHG/WLAN-XD can also be programmed using a HART handheld programmer.

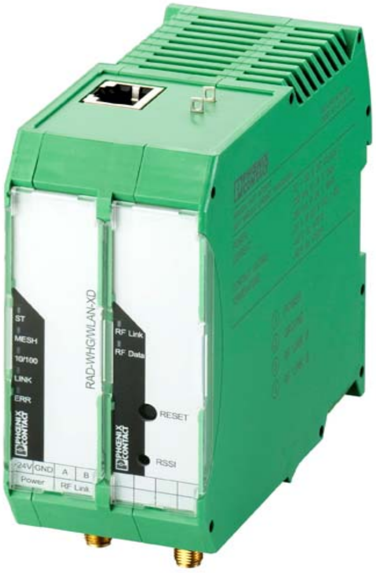


Figure 6: Wireless gateway with WLAN transceiver

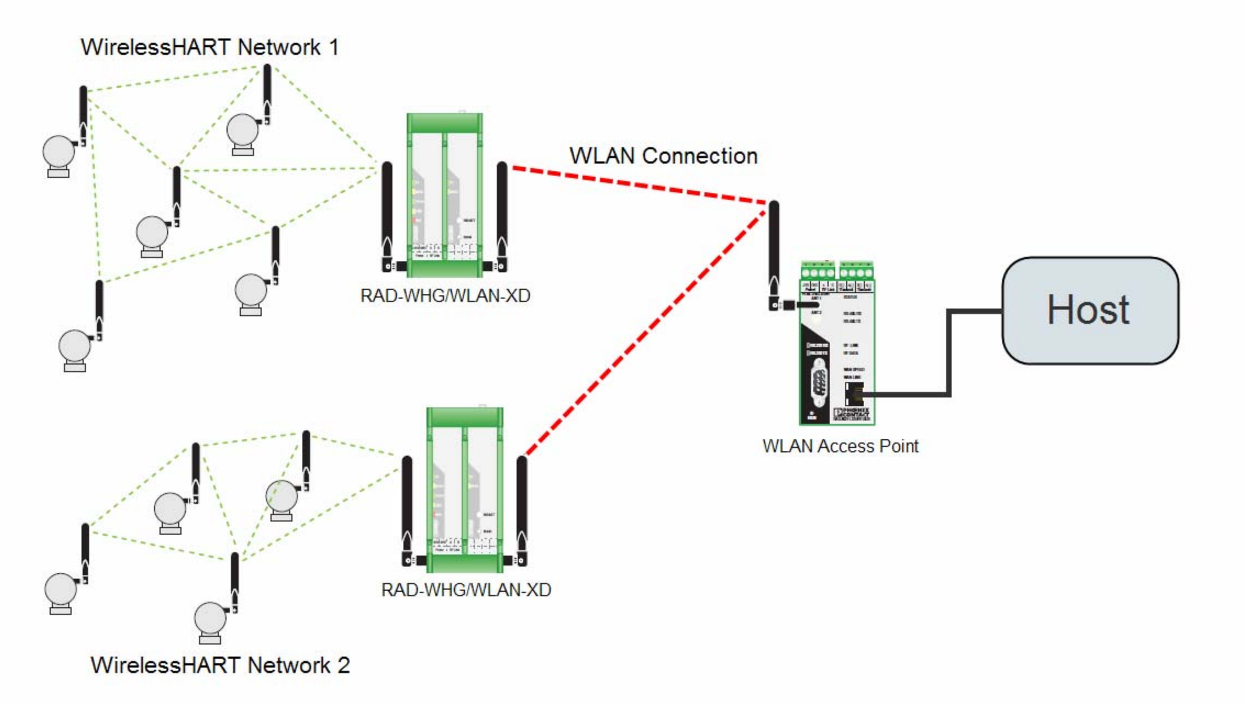


Figure 7: RAD-WHG/WLAN-XD Application Exam

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. WirelessHART, part of the HART7 standard, provides an easy-to-install, reliable and cost-effective way to connect these devices back to the host system. A WirelessHART gateway with integrated WLAN can further increase the flexibility and reliability of a WirelessHART network.

About Phoenix Contact

Phoenix Contact is a leading developer of industrial electrical and electronic technology. The company's diverse product range includes components and system solutions for industrial and device connection, automation, electronic interface and surge protection. Phoenix Contact GmbH & Co. KG, Blomberg, Germany, operates 47 international subsidiaries, including Phoenix Contact USA in Middletown, Pa. Global sales exceed more than1 billion euro annually. Phoenix Contact's formal Integrated Management System is registered to ISO quality, environmental and safety standards (ISO 9001:2008,14001:2004 and 18001:2007).