TECHNICAL WHITE PAPER

WIRELESS TECHNOLOGY
*Wireless*HART™

Wireless technology is evolving from the consumer market to industrial applications. Since the requirements for utilization of wireless technology in industrial applications differ greatly from consumer applications, industrial wireless implementation has not been widely used until recently.

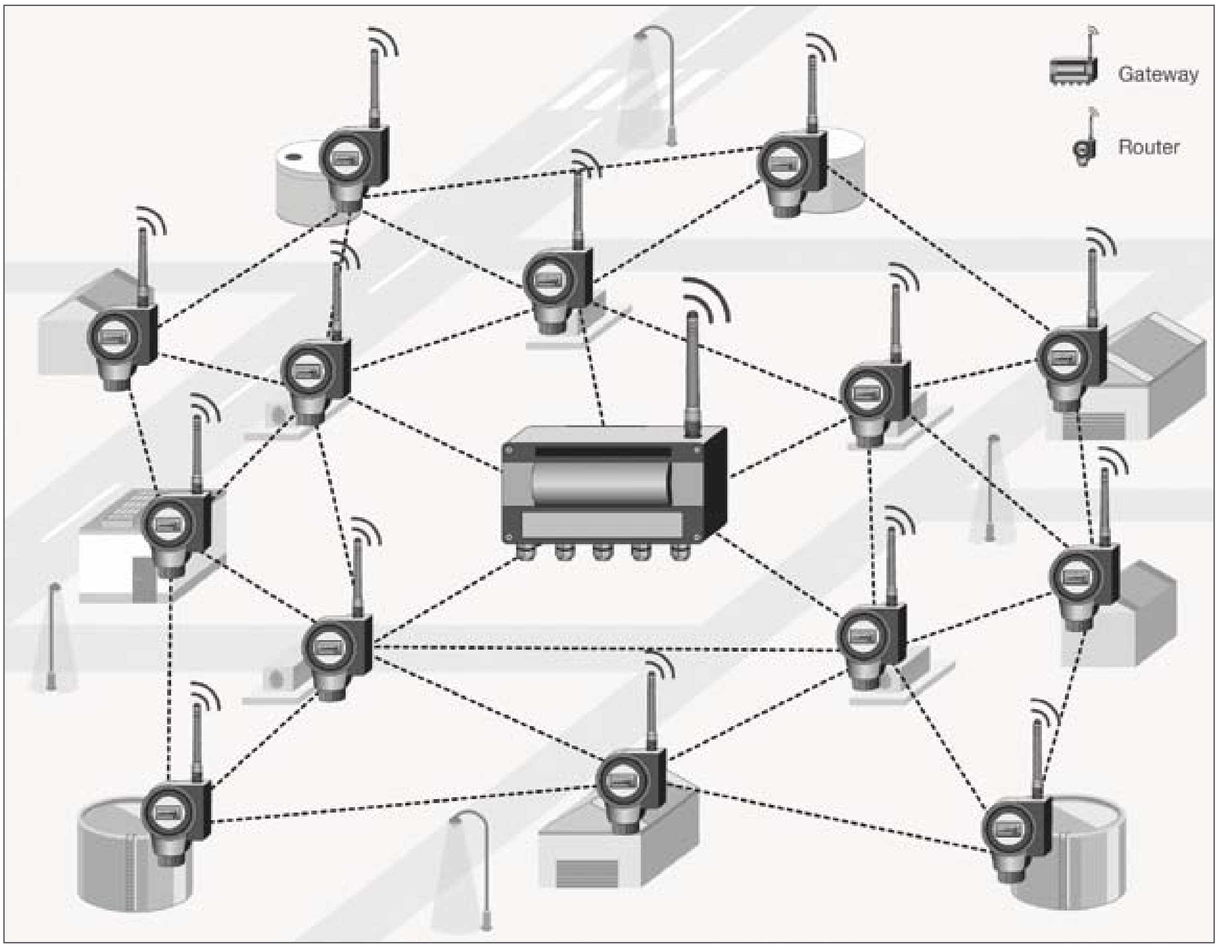
One reason is that no common standard has been developed. Typically, each wireless system installed today is proprietary. Different solutions exist in parallel, which increases planning, maintenance and integration efforts.

This has changed with the introduction of *Wireless*HART. This is the first standard for process automation.

This paper introduces the technical basics and concepts of *Wireless*HART, as well as application examples. It is directed to technical decision makers and technicians who are planning to install a *Wireless*HART system.

Prepared by:
Gerrit Lohmann
Product Portfolio Manager
Pepperl+Fuchs

PEPPERL+FUCHS
PROTECTING YOUR PROCESS



Mesh Network

Pepperl+Fuchs is the proven market leader for communication technology in the process automation market. The product portfolio ranges from conventional interface technology and remote I/O systems to fieldbus components.

Almost all communication in process automation has been realized with a cable. Wireless communication is the latest innovation, which was introduced to provide communication paths between the control room and the field.

As many have come to expect, Pepperl+Fuchs is an early adopter of new technologies, and this will be the case for *Wireless*HART. You can rely on the experience of Pepperl+Fuchs when dealing with new technology and concepts to provide high-quality products that are easy to install, commission and maintain. As a result, you benefit from a great feature that increases the performance of your plant.

Table of Contents

1 Introduction

Wireless technology is evolving from the consumer market to industrial applications. Since the requirements for utilization of wireless technology in industrial applications differ greatly from consumer applications, industrial wireless implementation has not been widely used until recently.

One reason is that no common standard has been developed. Typically, each wireless system installed today is proprietary. Different solutions exist in parallel, which increases planning, maintenance and integration efforts.

This has changed with the introduction of *Wireless*HART. This is the first standard for process automation.

2 From HART to *Wireless*HART

As automation technology was introduced, measurement signals were transformed into current or voltage signals. As a common standard, the 4...20mA loop has been a widely accepted interface. It allows for long communication lines, and the live-zero state allows for failure detection in case of a broken or shorted cable. All of this was able to be done with analog electronic circuitry.

Later, as digital electronics appeared, became smaller and microprocessors became cheap, the desire for more information than just the pure measurement value arose. It was easy to collect the information in the field device itself, but the user wanted to avoid the connection via a dedicated communication line. The idea to modulate the information on the existing 4...20mA loop was born and continues to expand.

The idea is quite simple. Process automation measurement values typically change quite slow; therefore, the 4...20mA current loop can be seen as quasi static. On a static current, it is possible to modulate a sine without changing or affecting the current in the mean value if the frequency of the modulated information is high enough. Since the time of its creation, HART communication has used the Bell Standard with coding a logical “1” into a 2.2 kHz sine and a logical “0” in a 1.2 kHz sine. This kind of modulation is called Frequency Key Shifting (FKS)

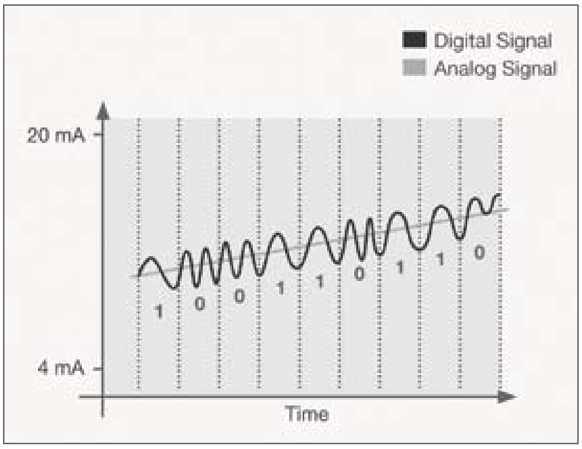


Fig. 1: Conventional HART

With this approach, it was possible to digitally transmit the desired information. Although the concept of superimposing the 1.2/2.2 kHz FKS Signals on the physical layer is sound, it is critical to agree on a common language to understand each other. This language, or more technically protocol, is HART, and it defines the commands and responses to exchange information like status, parameter values, measurement values, and diagnostic data. HART was introduced and has been growing in popularity since the 1980s.

Since then, several revisions of HART have been introduced, each offering more functionality, but all using the same 4...20mA loop as its physical layer. The newest revision of HART, Version 7, has added a wireless network as an alternate physical layer to the conventional 4...20mA loop. When using the wireless network as defined in HART7 for data transmisson, this is called *Wireless*HART.

3 Content and Concept of *Wireless*HART

Contrary to the conventional 4...20mA physical layer, which was easy to specify, the requirements for *Wireless*HART are more complex. First, the scope for *Wireless*HART contains a list of multiple goals which had to be achieved. The following goals have been specified: *Wireless*HART will

- be an open and interoperable standard
- be as easy as using wired HART
- enable wireless access to existing field devices
- use the same configuration, maintenance, diagnostic tools and procedures
- require little additional training
- be usable worldwide
- be usable without a license
- use Standard-Radio-Chipsets which are available commercial, off the shelf (COTS)

The last three goals are the most important. In a globalized world, a standard must be usable worldwide. No license fee or restriction in usage shall apply. The only almost worldwide license-free usable frequency is the 2.4GHz ISM Band. Due to WLAN and Bluetooth using this 2.4GHz ISM Band, there are many radio chips available on the market. These chips contain the RF-circuitry and are implemented easily. This eases development of the final product, such as cell phones with Bluetooth connectivity or laptops with WLAN.

One may think of WLAN and Bluetooth as being similar technologies due to the frequency band, However, WLAN is optimized for a very high through-put with less need for power saving, while Bluetooth is optimized for lower throughput and more power saving.

Looking at process automation plants, the need to transmit measurement data at a very high throughput is not required. In contrary, the sensors are expected to be battery powered, and with respect to the battery lifetime, power saving is important. So, a technology similar to Bluetooth might be the better choice.

Taking a Bluetooth approach would be tied to one condition: the output power is restricted to 10mW, in some countries it is limited to 100mW. This low power causes the distance between sender and receiver to be limited. In the best case, it is limited to 100...200m. In reality, this distance may be suitable for most applications but environmental conditions greatly reduce these limits. For vast process automation facilities, this distance is inadequate. In addition to the limited range for process automation applications, wireless communication is generally not as reliable as wired communication. Several environmental influences like interferences, other radio systems, and the fact that radio waves can get corrupted on their way from the sender to the receiver decrease the reliability.

Both the limited range and the decreased reliability of a wireless network are not acceptable and must be improved to enable applications in process automation.

Taking all these aspects into account, the decision to utilize the IEEE802.15.4 standard was chosen. This standard allows for low power sensor nodes which work in a mesh architectures and are optimized to transfer small amounts of data. Another widely known standard based on IEEE802.15.4 is ZigBee. While ZigBee is optimized for building automation, some other concepts are established in the IEEE standard.

*Wireless*HART uses four different communication concepts, which are interlocked to overcome the disadvantages.

- Flat Mesh Network
- Network Management
- Time Division Multiple Access (TDMA)
- Frequency Hopping

3.1 Flat Mesh Network

The Flat Mesh Network is a concept where all wireless sensors in the field form a network, and a message can be routed through this network. The original sender of the message sends it to its nearest neighbor. This recipient forwards it to the next neighbor and so on until the message reaches the final recipient.

Imagine that all sensors are spread over a certain area and have connection paths between them. It becomes obvious where the name Mesh Network comes from: all wireless sensors are connected and form a mesh.

The mesh has two advantages. First, the area which can be covered is increased. The limitation of the 100...200m range only applies for a link from one wireless sensor to another, while the routing of a message through the mesh makes the covered area and range of this network much larger.

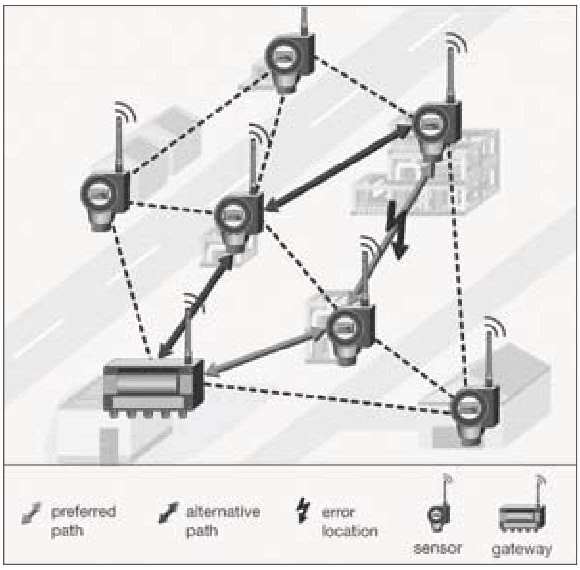


Fig. 2: Mesh Network

Second, if one path fails, there is always an alternative path. If a message gets lost or corrupted, it is first repeated to the same neighbor. If, after a certain amount of retries, the message still is not transmitted, the message will be sent using an alternative path. So, the message will be rerouted. This is called a self-healing network. The chance that a message gets routed through the network has now increased, along with reliability.

3.2 Time Division Multiple Access and Frequency Hopping

The Flat Mesh Network is comprised of several senders and receivers. All of them access the same media, the free space. This must be organized to avoid message collision, which could result in data corruption. *Wireless*HART uses the combination of two concepts, TDMA and Frequency Hopping.

TDMA is the abbreviation of “Time Division Multiple Access” and describes clearly that TDMA has an important time component. The TDMA of *Wireless*HART divides a second into 100 slots, 10ms each. The entire network is synchronized in these slots. This enables the wireless sensors to start the communication in a very defined time. If no communication is needed, they go into a sleep mode to save battery power. This also allows other sensors to send data.

The other concept is Frequency Hopping where all 15 defined channels of IEEE802.15.4 standard are used. This means that during one slot, multiple wireless sensors can transmit in one of the available channels in the 2.4GHZ ISM Band. IEEE802.15.4 defines 15 channels which work in parallel. So, 15 wireless sensors in a *Wireless*HART network can send during the same time slot.

Combining 15 communications per time slot by 10ms per time slot results in 1500 communications, which theoretically can go through the entire network.

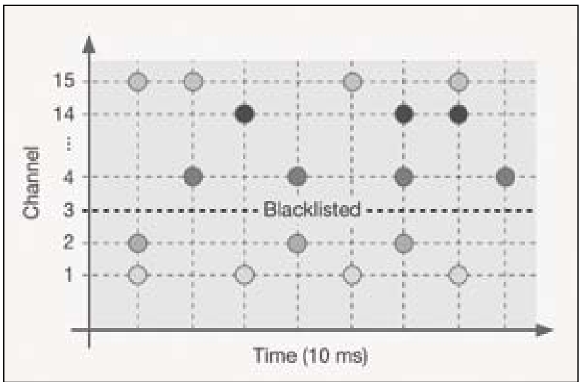


Fig. 3: Time Division Multiple Access

3.3 Network Management

The Mesh Network, with preferred and alternative paths for messages, as well as the TDMA, must be organized. This is done by the Network Manager.

The Network Manager determines the best paths between the single wireless sensors as well as an alternative path. Also, it organizes which sensor is allowed to send a message on which channel. Organized in this manner, the communication in the network is optimized to provide the best performance in terms of speed, throughput, and energy consumption

The Network Manager scans the network continuously and reacts to deviations in the operation. During the conditions when another wireless sensor is added, a sensor failed completely, or a communication path was very unstable, and a better path must be implemented. The Network Manager is responsible to guarantee the best possible operation of the *Wireless*HART network.

3.4 Results of Measures

The results of the described measures overcome the disadvantages of the 2.4GHz band in an elegant way.

- The reliability of the communication has been improved through alternative paths.
- The area which can be covered wirelessly is increased.
- The throughput is maximized by using 15 channels 100 times per second.
- The coexistence is given by allowing free space for other wireless communication systems.
- Due to the low power of IEEE802.15.4, battery powered devices are possible.

The other usability goals of *Wireless*HART are done by the implementation. Above the foundation of IEEE802.15.4, the next protocol stacks are layered. To the outside, the device is still a HART device, only the communication path has been changed. This enables the user to use the same tools and principles as with conventional wired HART. It fulfills the requirements for limited additional training and being an easy-to-use technology.

Since *Wireless*HART is just changing the communication path for the HART protocol from being wired to wireless, one could describe *Wireless* HART as an "add-on" to HART. The protocol extensions are mainly additional commands which had to be implemented to enable control and diagnosis of the wireless network. Nevertheless, a HOST system being connected to conventional HART devices and *Wireless*HART devices does not recognize the difference and treats them both the same.

3.5 Network Forming, Identification and Security

Besides the properties for optimizing the wireless technology for process automation applications, several other properties have to be designed and considered.

The first property is the forming of networks. It must be avoided that any arbitrary sensor can join the network without having control over its inclusion. So, a process for allowing a new sensor had to be found.

To control this process, a *Wireless*HART network is assigned a unique identifier, called Network ID. The Network ID is fixed by the Network Manager. It only allows sensors to join the network if this particular sensor carries the same Network ID. Sensors not carrying this NetworkID are not allowed to join the network. Also, the concept of the Network ID allows multiple networks to operate in parallel.

To allow a particular sensor to join the network, a sensor has to carry a Join Key which allows the sensor to join the network. If the sensor has the correct Network ID, but a wrong Join Key, it will not be allowed to join the network.

Both the Network ID and Join Key must be parameterized in the devices by the user with a wired connection to avoid interception of this vital data. This connection can either be FSK as conventional HART or as a RS485 connection.

When the device is installed in the field and parameterized with the necessary information of network ID and Join key, it will first listen to advertisement messages which are send out by the existing network to publish it's existence. As soon as such an advertisement message is received, the device synchronizes with the network and then starts sending requests to join the network. This request is transmitted through the existing network to the Network Manager. If the sensor is authorized to join, the Network Manager will include the sensor in the network and send back the necessary data to optimize network flow under consideration of the new sensor.

Besides the necessary network structure related information, the new sensor will receive a 128Bit encryption key. This encryption key is used to encode all HART commands to avoid interception of the network communication. Since *Wireless*HART is not built on TCP/IP as WLAN, it is also not possible to intercept network communication with WLAN standard hardware. To make it even more secure, the encryption key is exchanged in random intervals.

After the encryption key is distributed, it is almost impossible to break into the network, and due to the special MAC layers of WLAN and *Wireless*HART, it is not possible to do this with standard hardware.

4 Possible Network Performance

As described in section 3.2, the combination of TDMA and frequency hopping enables up to 1500 communications in the network per second (100 slots x 15 channels). This is a purely theoretical value, usually the net communication load should not exceed 30%, or approximately 450 communications/second.

Since all communications end up in the Gateway and this can only send one frequency at a time per Access Point, the overall communications from the *Wireless*HART Network to the bus system should not exceed 30 communications per second (100 slots x 30%).

A single *Wireless*HART network can contain up to 250 devices. Taking the rule of 30 communications per second, such a network could update all values about every 8 seconds.

If the Gateway uses multiple Access Points and communicates via multiple channels at one time, this performance increases. Using 2 Access Points, a network with 250 sensors could update approximately every 4 seconds (250 sensors/ (2 Access Points x 30 communications/second)).

If multiple networks or other 2.4GHz systems are installed in parallel, the performance decreases since they all must agree on how to use the available channels. If using two networks, both can use only 7 channel each instead of 15, which reduces their theoretical throughput by 50% (750 communications per second, or a more practical 225 communications/second).

Regardless of these rough values, it is possible to have signal update rates of 1 second or 1 minute. The update rate can be set individually per device. The Network Manager optimizes the data flow through the network to provide each device with thenecessary resources to transmit the data in the desired intervals.

5 Device Types in a *Wireless*HART network

A *Wireless*HART network is built of two main components:

- *Wireless*HART Gateway
- *Wireless*HART Field Device

The *Wireless*HART Field device itself is available in two major types:

- *Wireless*HART Adapter
- *Wireless*HART Field Device

5.1 *Wireless*HART Gateway

The *Wireless*HART Gateway is the core element and the most complex device in a *Wireless*HART network. It contains:

- The radio to access to the network (Access Point)
- The Network Manager
- The Security Manager
- One or multiple Interfaces to the HOST systems, e.g. RS485, Ethernet, PROFIBUS.

Today, all these elements are packed in one enclosure. This makes the *Wireless*HART Gateway compact and easy to use. Of course, a distributed structure is possible and might be available later. For example, multiple Access Points would provide multiple paths within the network which eliminates the single point of failure. The Network Manager and Security Manager could be software running on the network with redundant bus systems providing multiple ways to the HOST systems.

5.2 *Wireless*HART Adapter

The *Wireless*HART Adapter is a device which can be attached directly or with a short cable extension to any conventional wired HART or 4...20mA device. The adapter accesses the data from the conventional field device via HART or changes the 4...20mA current to a digital value and transmits this data to the *Wireless*HART network. This converts the conventional field device into a *Wireless*HART device. This offers the most flexibility.

The *Wireless*HART Adapter can be battery, loop or mains powered. Also, energy harvesting solutions, such as solar cells, are possible.

A battery powered adapter can supply energy to the *Wireless*HART Adapter and the field device. This configuration enables autonomous measurements. The *Wireless*HART Adapter is continuously powered to act as the router in the mesh network. When a measurement must be taken, the adapter powers the field device for a certain time, which is necessary to obtain the measurement value and then shuts down the device again. Unfortunately, the field devices are not designed to be low power. Also, they typically require a minimum 12V to start up, while some require more voltage. Stepping up the battery voltage and converting it to a useable value is not very effective. Still, depending on the power consumption of the field device, the time and voltage needed for start up, and the cycle and interval between the measurements, the battery can last for years.

The loop powered type of *Wireless*HART Adapters can be connected to an existing 4...20mA loop and accesses power from the loop. The Adapter uses the HART signal on the loop and sends it via the wireless network, providing a second communication path besides the 4...20mA loop. Of course, the Adapter causes a voltage drop in the loop. Since some loops do not have much reserve in terms of voltage, this option might not be suitable for some application. The adapter might only gain enough power from the loop to send at certain intervals. Between the intervals, the Adapter regains some power and stores it for the next message.

If power is available in the field, a mains powered Adapter Version can be installed. No power management is necessary with this version. The *Wireless*HART Adapter and field device can be powered all the time and can send uninterrupted messages at a fast rate.

5.3 *Wireless*HART Field Device

Another option for a field device is one that contains only *Wireless*HART devices. The devices have no 4...20mA interface. Instead, they have just an antenna. Several powering options are possible. When designing such a device from scratch, it is possible to optimize the power consumption. Also, the battery voltage is not required to be stepped up or converted. This makes these devices much more efficient than the combination of a *Wireless* HART Adapter with a conventional field device.

5.4 HOST Integration

A *Wireless*HART Network of course has to fullfill a certain task; therefore, the data obtained by the network must be submitted to a processing system. Depending on the application, this can be a DCS, a PLC, an Asset Management System or any other controlling or monitoring system. The goal is to interface to any of those systems as seamless as possible.

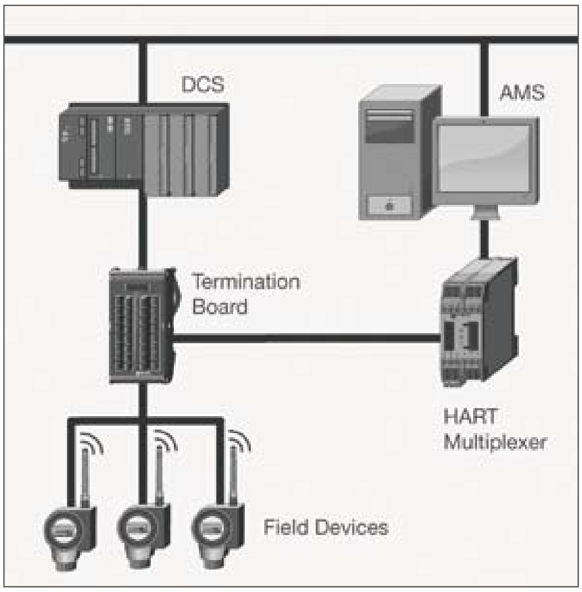


Fig. 4: Structure of Conventional HART infrastructure

In the process automation environment, there are two major software configuration concepts: DTM and DD based. One can explain the concept of DTM or DD as a driver for the device, running in a frame application. In the end, the DTM and DD are files which describe the properties and parameters of the device. These are common concepts and all HART devices come with a DD. Most instruments are also available with a DTM.

This same concept is also used by *Wireless* HART. Every *Wireless*HART device will have a driver in DTM and DD format. As a result, the use of *Wireless*HART devices is no different from the use of the regular wired HART devices.

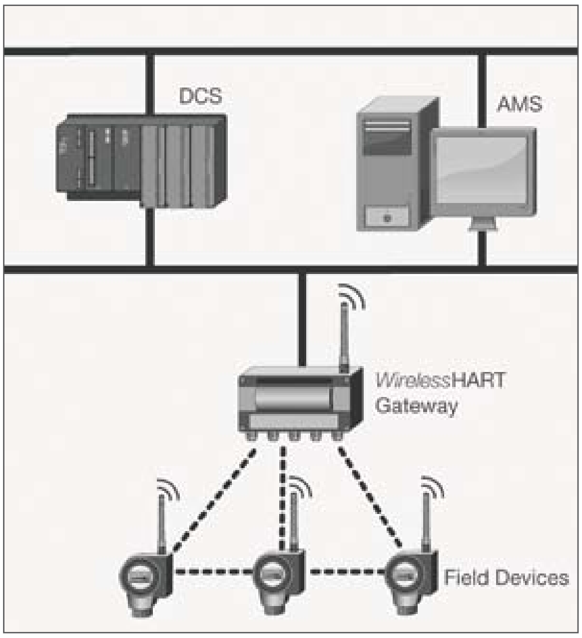


Fig. 5: Structure new *Wireless*HART infrastructure

The configuration options for a *Wireless*HART do not stop there. The *Wireless*HART Gateway can have multiple interfaces (see 4.1). For example, a *Wireless*HART Gateway with a PROFIBUS interface will be provided with a GSD file for PROFIBUS integration. A version with Modbus can be connected to the controller in the regular manner and act as a wireless Remote I/O. An Ethernet version gateway can be fitted with an OPC server to publish the desired values in the Network and be attached to ERM Systems.

By providing all the interface and integration possibilities, the implementation of *Wireless*HART is easy and seamless into almost all existing communication structures.

6 Applications

Even if the concepts of *Wireless*HART improve the transmission reliability, it is still a wireless technology, and may never be as reliable as a wired network. The first wireless applications will concentrate on preventive maintenance, environmental monitoring, asset management and non-critical open-loop control. Applications with a very high demand on reliability, such as safety functions and time-critical, closed-loop control are not the target applications for *Wireless*HART.

Nevertheless, there are many applications providing valuable benefits.

Since asset management is no longer restricted to the field devices itself, it will be extended to all equipment in the field. Typically, it is acceptable to run a power cable to a pump, but it is not acceptable to run an additional wire for pump diagnosis. Pump diagnosis can be important. If the pump does not function in the optimal working point, this will cause major damage after a short time. A broken pump can cause a production shutdown for days, depending on its size and location. A diagnosis of the pump will help to reduce the danger of unplanned shut downs.

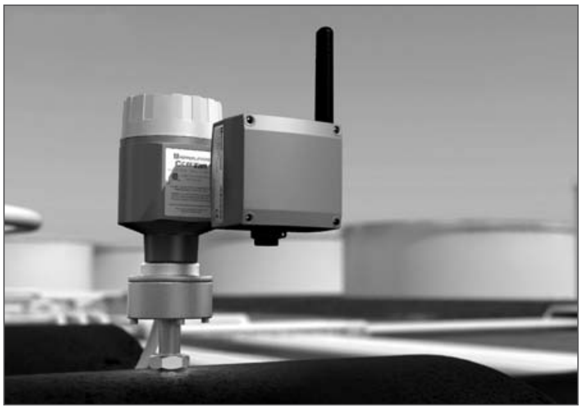


Fig. 6: Wireless Corrosion Monitoring with *Wireless*HART Adapter

The same principle is valid for bearings, or motor temperatures, or grease levels of floating bearings. Many valves have abrasion detection via HART, which can be monitored easily with a wireless link Also, corrosion monitoring can be simplified with a wireless network. A corrosion sensor must be applied to spots in the pipeline or the tank where corrosion is the greatest. This depends on the structure of the pipe or tank, as well as the flow within it. The location of the corrosion sensor does not normally offer a convenient location to wire a HART connection. A wireless corrosion sensor can be mounted where required without the need to run cables in a complex and expensive way.

An often cited application for any wireless system is monitoring the levels of tank farms. The slow changing levels of storage tanks can ideally be monitored with *Wireless*HART networks. There are many tanks with no installed level measurement technology. The content of these tanks are checked manually. A level sensor, upgraded with a *Wireless*HART Adapter will improve this operation.

Semi-finished goods, which are not needed in vast amounts, are manufactured in small installations. After the required amount of this material has been manufactured, the installation will be used for another semi-finished product and must be retrofitted to be enabled for this new production. Using *Wireless*HART, the majority of the sensor wiring can be eliminated.

Even with a high degree of plant automation, there are still a lot of manually operated elements, like ball valves, which are not monitored. Occasionally, an operator checks the position of these valves, but in the end, there is no overview of their status. The position of the ball valve could be detected with small proximity switches and be transferred directly to the control room. Also, the position of automatically operated valves gives no feedback, now it can be detected and transmitted. Last but not least, *Wireless*HART allows the full use of today's multivariable field devices. Most field devices do not just measure the primary value which is represented by the 4...20mA loop, but secondary and tertiary values as well. For example, ultrasonic level devices measure the temperature for compensation. This second value now can be obtained and transmitted to the HOST system.

*Wireless*HART can also be used to check the device calibration. If the 4...20mA value differs from what is digitally transmitted from the HART variables, the current output may be degraded. So, the reliability of the conventional measurement can be checked and measures can be taken before significant deviations occur.

None of these application examples are primarily aimed for control of the process; rather, these examples result in better monitoring of the process and the assets involved. The improved information on the plant status results in early recognition of unusual parameters and helps save money due to predictive and preventive maintenance.

7 Summary and Outlook

*Wireless*HART is an enabling technology to bring wireless communication to process automation plants. It is built upon the known and proven HART protocol and combines this technology with mechanism to increase the reliability and range of wireless communication.

Contrary to other wireless networks available today, *Wireless*HART is supported by multiple suppliers as a common, interoperable standard. Customers do not need to rely on a single source and are able to select the best devices for their needs. In the near future, a wide variety of *Wireless*HART devices will be available to increase the number of applications.

The easy implementation of *Wireless*HART products and the HOST integration in the same manner as wired HART makes it easy for the customers to set up, operate, and maintain *Wireless*HART networks.

*Wireless*HART will redefine the definition of asset management, preventive maintenance, and plant monitoring; therefore, it will help to plan services and maintenance tasks. This reduces down time of plants and helps to keep them competitive.

For your notes

PROCESS AUTOMATION – PROTECTING YOUR PROCESS

For over a half century, Pepperl+Fuchs has been continually providing new concepts for the world of process automation. Our company sets standards in quality and innovative technology. We develop, produce and distribute electronic interface modules, Human-Machine Interfaces and hazardous location protection equipment on a global scale, meeting the most demanding needs of industry. Resulting from our world-wide presence and our high flexibility in production and customer service, we are able to individually offer complete solutions – wherever and whenever you need us. We are the recognized experts in our technologies – Pepperl+Fuchs has earned a strong reputation by supplying the world's largest process industry companies with the broadest line of proven components for a diverse range of applications.

1 **Worldwide/German Headquarters**
Pepperl+Fuchs GmbH
Mannheim · Germany
Tel. +49 621 776 2222
E-Mail: pa-info@de.pepperl-fuchs.com

2 **Asia Pacific Headquarters**
Pepperl+Fuchs PTE Ltd.
Singapore
Company Registration No. 199003130E
Tel. +65 6779 9091
E-Mail: pa-info@sg.pepperl-fuchs.com

3 **Western Europe & Africa Headquarters**
Pepperl+Fuchs N.V.
Schoten/Antwerp · Belgium
Tel. +32 3 6442500
E-Mail: pa-info@be.pepperl-fuchs.com

4 **Middle East/India Headquarters**
Pepperl+Fuchs M.E (FZE)
Dubai · UAE
Tel. +971 4 883 8378
E-mail: pa-info@ae.pepperl-fuchs.com

5 **North/Central America Headquarters**
Pepperl+Fuchs Inc.
Twinsburg · Ohio · USA
Tel. +1 330 486 0002
E-Mail: pa-info@us.pepperl-fuchs.com

6 **Northern Europe Headquarters**
Pepperl+Fuchs GB Ltd.
Oldham · England
Tel. +44 161 6336431
E-Mail: pa-info@gb.pepperl-fuchs.com

7 **Southern/Eastern Europe Headquarters**
Pepperl+Fuchs Elcon srl
Sulbiate · Italy
Tel. +39 039 62921
E-Mail: pa-info@it.pepperl-fuchs.com

8 **Southern America Headquarters**
Pepperl+Fuchs Ltda.
São Bernardo do Campo · SP · Brazil
Tel. +55 11 4341 8448
E-Mail: pa-info@br.pepperl-fuchs.com

www.pepperl-fuchs.com

PEPPERL+FUCHS
PROTECTING YOUR PROCESS