

**System Redundancy with
*WirelessHART***



HCF_LIT-128

Rev. 1.1

Date of Publication: March 5, 2010

Document Distribution / Maintenance Control / Document Approval

To obtain information concerning document distribution control, maintenance control, and document approval please contact the HART Communication Foundation (HCF) at the address shown below.

Copyright © 2010 (2008) HART Communication Foundation

This document contains copyrighted material and may not be reproduced in any fashion without the written permission of the HART Communication Foundation.

Trademark Information

HART® is a registered trademark of the HART Communication Foundation, Austin, Texas, USA. Any use of the term HART hereafter in this document, or in any document referenced by this document, implies the registered trademark. WirelessHART™ is a trademark of the HART Communication Foundation. All other trademarks used in this or referenced documents are trademarks of their respective companies. For more information contact the HCF Staff at the address below.



Attention: Foundation Director
HART Communication Foundation
9390 Research Boulevard, Suite I-350
Austin, TX 78759, USA
Voice: (512) 794-0369
FAX: (512) 794-3904

<http://www.hartcomm.org>

Intellectual Property Rights

The HCF does not knowingly use or incorporate any information or data into the HART Protocol Standards which the HCF does not own or have lawful rights to use. Should the HCF receive any notification regarding the existence of any conflicting Private IPR, the HCF will review the disclosure and either (a) determine there is no conflict; (b) resolve the conflict with the IPR owner; or (c) modify the standard to remove the conflicting requirement. In no case does the HCF encourage implementers to infringe on any individual's or organization's IPR.

Synopsys:

In process automation, operators make decisions based on the data they have available. When one or more process variables or other types of information are not available, they must make those decisions without a complete picture of what's happening. In fact, they may not even know a decision is needed. The same is true for control systems: without all the necessary input data, the output of a control algorithm may not reflect the best action to keep the process operating smoothly -- or even worse, it could cause a process shutdown.

In process automation, operators make decisions based on the data they have available. When one or more process variables or other types of information are not available, they must make those decisions without a complete picture of what's happening. In fact, they may not even know a decision is needed. The same is true for control systems: without all the necessary input data, the output of a control algorithm may not reflect the best action to keep the process operating smoothly -- or even worse, it could cause a process shutdown.

That's why process operations sometimes use **system redundancy** to minimize the probability of data loss, especially where the process data is operationally critical or where a single component failure could result in the loss of a significant number of process variables.

Redundancy may duplicate any of several types of critical system components – from devices to controllers to communications. For example, a traditional wired system may have two cables carrying the same information.

Wireless systems can also provide redundancy to help prevent data loss. In the case of *WirelessHART*, redundancy is available at all levels of the network system:

- in the wireless sensor network
- at the network access point
- at the gateway / network manager / security manager

This paper examines each of these possibilities.

Redundancy in the wireless sensor network

WirelessHART provides redundancy in the wireless sensor network through several mechanisms. Each communication can have

- Multiple paths between the field device and the gateway (spatial diversity)
- Multiple radio channels (frequency diversity)
- Multiple timing possibilities (time diversity).

Let's use Figure 1 to look at an example. If communication from devices TT101 to the gateway fails on path A-B-C, the device will retry at a slightly different time and channel on a different path – for example, D-E-F. If that fails also, it tries again, perhaps on path D-G-C. The system provides for three retries to get the communication to its destination.

This redundancy is provided in both directions, from the gateway to the device and from the device to the gateway.

The *WirelessHART* standard is the first open wireless communication standard for measurement and control in the process industries. It uses wireless mesh networking between field devices, as well as other innovations, to provide secure, reliable digital communications that can meet the stringent requirements of industrial applications.

This is one of a series of papers helping users recognize the benefits of *WirelessHART*, as well as addressing specific questions about *WirelessHART*.

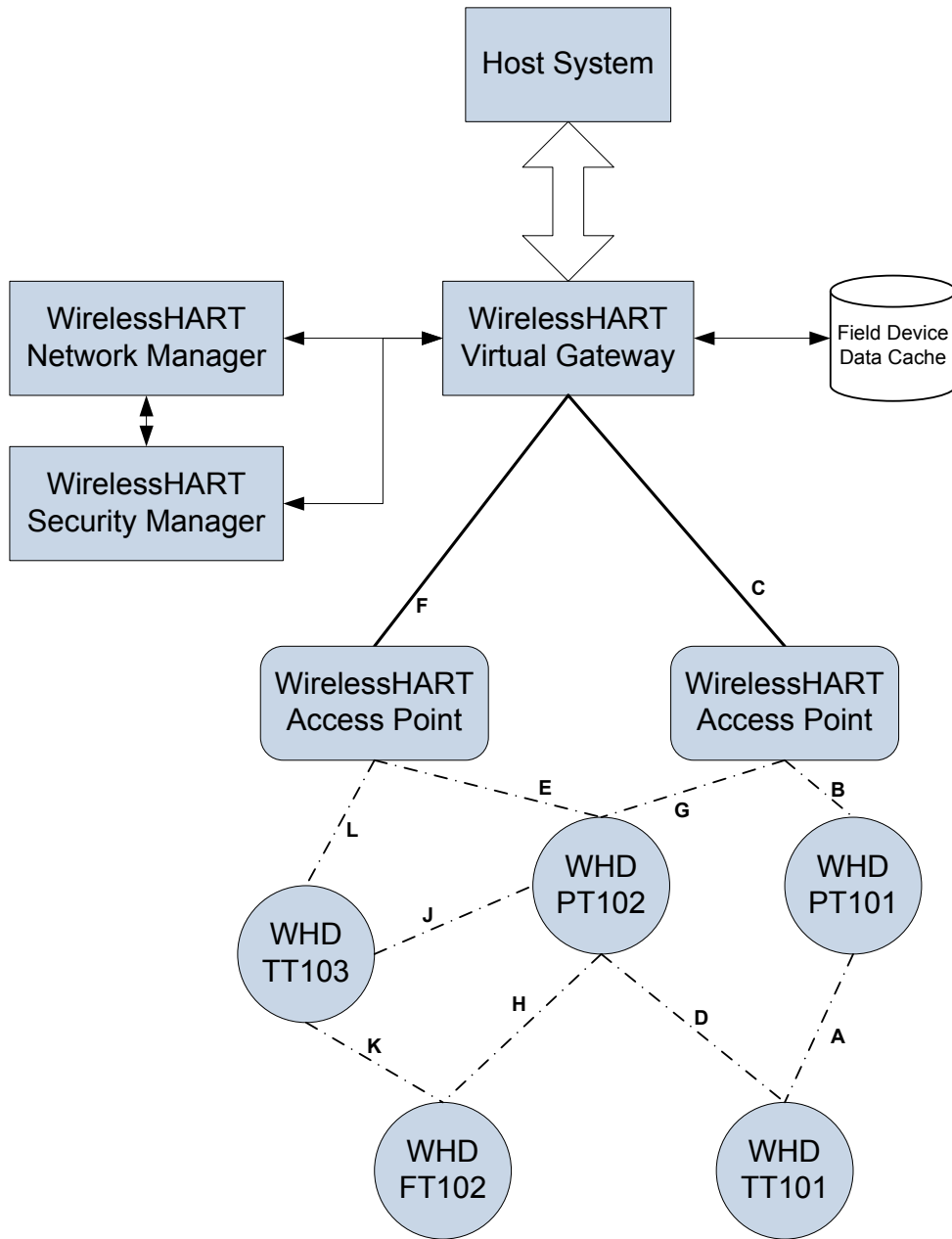


Figure 1 – WirelessHART System Components

Redundancy at the network access point

An access point is simply a specialized *WirelessHART* device with a high bandwidth communication interface to the gateway. It provides an entry and exit point for system communication to and from *WirelessHART* devices.

WirelessHART allows a network to have multiple access points. Besides additional path diversity (as described above), multiple access points also provide additional network bandwidth and redundant communication paths for the gateway and network manager.

Another benefit of multiple access points is that they can provide low-latency access for connection to final control elements. For example, strategically placing an access point near a control valve enables that valve to communicate directly with the access point, providing a low latency path from the gateway to the valve.

There is theoretically no limit to the number of access points a network can have. You simply make the tradeoff between cost, redundancy, and overall network access bandwidth.

Redundancy at the gateway, network manager and security manager

The higher-level components of a *WirelessHART* system are the **gateway**, **network manager**, and **security manager** software functions. Each of these components can also be made redundant.

One way to do this is by putting each function in its own physical execution device and then replicating each of those physical devices. This gives users flexibility to decide which component or components are most critical to their applications. For example, a user might decide the network manager is most critical and make that particular component redundant.

Figure 2 shows another approach: Putting all three components (gateway, network manager and security manager) in one physical gateway device and then simply replicating that device.

In this arrangement, one gateway device is the primary and one is the backup. The two communicate with each other via a redundancy manager to keep the state of the network synchronized. If the primary physical gateway device fails, the secondary recognizes this and takes over the responsibilities from the primary device.

Functions provided

Gateway

- One or more interfaces between WirelessHART network and Host System
- Network Time synchronization
- Caching of field device dynamic data
- Interface to the network manager

Network Manager

- Communication scheduling services
- Communication routing services

Security Manager

- Key generation
- Key storage
- Field device authentication services

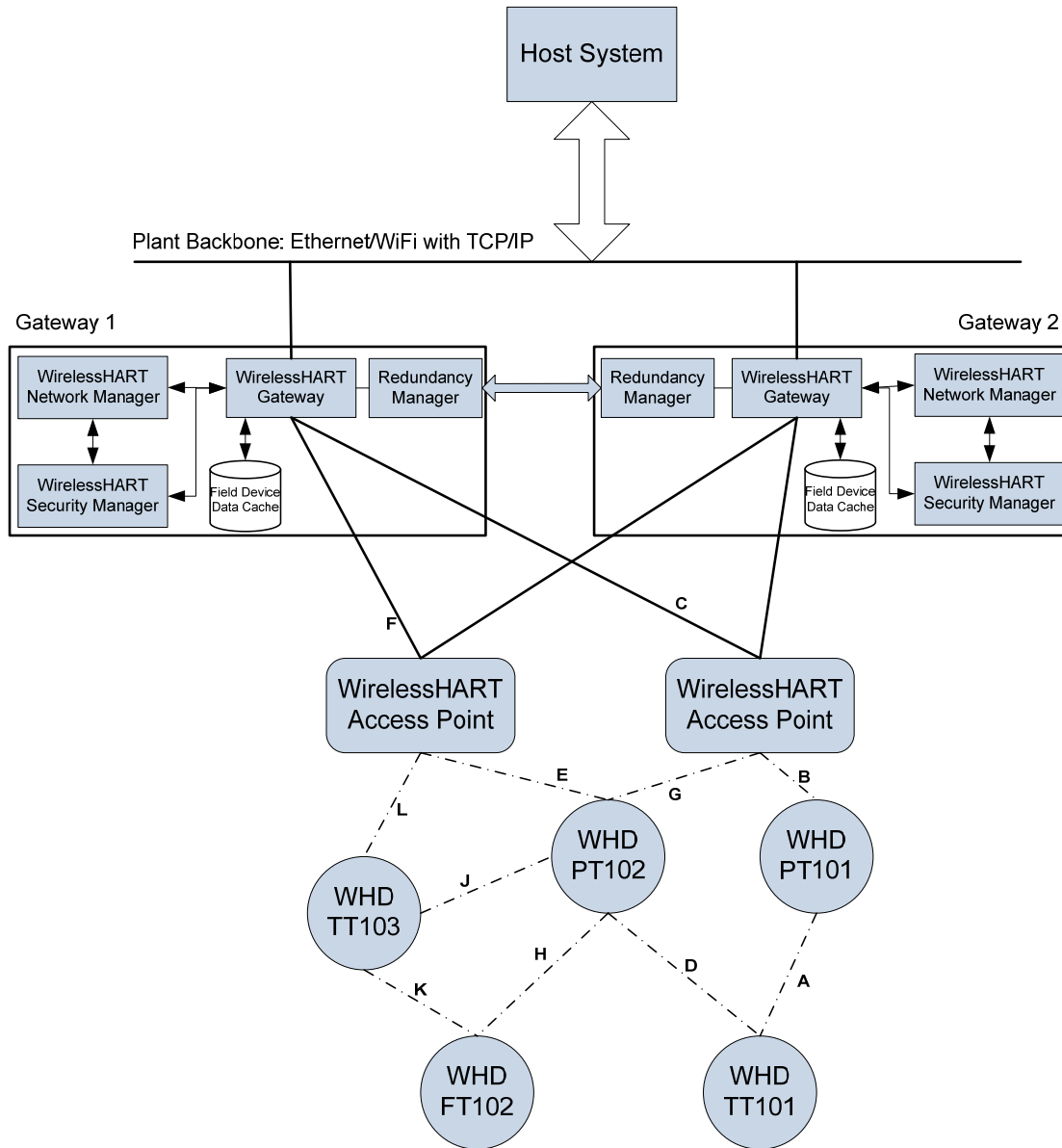


Figure 2 – Example Redundant *WirelessHART* System

Adapters for Redundancy

WirelessHART provides many ways to improve redundancy including the addition of a *WirelessHART* adapter. The *WirelessHART* adapter provides a redundant communication channel to traditional wired HART devices. Devices connected to legacy I/O can have continuous low latency communication to asset management with no change to the control strategy. For more information see the HCF *WirelessHART* Adapter Tech Note.

Conclusion

WirelessHART addresses redundancy at all levels of the network –The examples show that the overall performance of a typical *WirelessHART* network is comparable to that of traditional wired field buses. The *WirelessHART* protocol allows for secure, highly reliable, low latency communication with almost no impact on the bandwidth and process performance. All of this is automatically built into the *WirelessHART* standard – to make it simple, reliable, and secure.