HART COMMUNICATION FOUNDATION

TECH NOTE

*Wireless*HART Security Overview

HCF_LIT-114

Rev. 1.0

Date of Publication: March 4, 2010

Contributors: Jim Cobb, Emerson Process Management
Eric Rotvold, Emerson Process Management
Jeff Potter, Emerson Process Management

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.

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:

The WirelessHART technology was designed to enable secure industrial wireless sensor network communications while ensuring ease-of-use is not compromised. Security is built in and cannot be disabled. It is implemented with end-to-end sessions utilizing AES-128 bit encryption. These sessions ensure that messages are enciphered such that only the final destination can decipher and utilize the payload created by a source device

Introduction

The *Wireless*HART technology was designed to enable secure industrial wireless sensor network communications while ensuring ease-of-use is not compromised. Security is built in and cannot be disabled. It is implemented with end-to-end sessions utilizing AES-128 bit encryption. These sessions ensure that messages are enciphered such that only the final destination can decipher and utilize the payload created by a source device.

Risk Assessment / Reduction

To be a credible threat, an attacker must possess access, knowledge, and motivation. *Wireless*HART's security architecture helps owner/operators address all three of these areas:

- Minimize, control, and audit access.
- Require high levels of technical expertise to subvert.
- Reduce the consequences (span and duration) of any individual security breach.

Wireless sensor network security can be broken down into two main categories which can be termed Data Protection and Network Protection. Data Protection, or Confidentiality, deals with maintaining the Privacy and Integrity of the information being passed over the network, while Network Protection, or Availability, deals with maintaining the functionality of the network in the face of internal and/or external attacks (intentional or unintentional).

Data Protection

Security features associated with privacy aim to prevent eavesdropping by unauthorized devices inside or outside the network. A WirelessHART sensor network provides end-to-end CCM* mode AES-128 bit encryption[1] at the network/transport layer from the data source to the data consumer. In addition to individual session keys, a common network encryption key is shared among all devices on a network to facilitate broadcast activity as needed. Encryption keys can be rotated as dictated by plant security policy to provide an even higher level of protection.

A separate 128 bit join encryption key is used to keep data sent and received during the joining process private. The join key also serves as authentication to the security manager that the device belongs to this network. The join key is treated separately from the other keys to enhance security. Join keys can either be unique to each device, or be common to a given WirelessHART network based on the user security policies.

Data Protection security features associated with Integrity ensures that data sent over the wireless sensor network has not been tampered with or falsified. WirelessHART computes an encrypted message integrity check field that is added to each packet. The receiving device uses this message integrity check field along with the protected data to confirm the contents of the packet have not been altered. The message integrity check field also protects the network routing information as well. This prevents attacks that attempt to change the packet's network/transport layer information.

Data Integrity also involves verifying that the packet has come from the correct source. The network/transport layer message integrity check field, the information used to generate the check field, and the sender/receiver unique session key that codes/decodes the data are tools that can be used to verify the source.

Network Protection

A wireless sensor network also needs tools to protect it against attacks. These attacks HART can attempt to compromise the network by inserting Trojan horse devices, impersonating networks to get sensitive data from legitimate devices, and disrupting the network to deny service. Attacks can be launched from outside or inside the company by external people or employees. Network security depends upon techniques to support Authentication, Authorization, and Attack Detection.

A *Wireless*HART gateway and the wireless sensors joining the network must be configured to control which devices are allowed to access the network. The network will only be secure if all the devices in the wireless network maintain security. A *Wireless*HART gateway therefore has a secure authentication process which it uses to negotiate with all joining devices to ensure they are legitimate. As with all other network communications, all join negotiation traffic is encrypted end-to-end.

Denial of service attacks are aimed at impairing the proper operation of the system by interfering with communications within the wireless sensor network. These attacks may try to jam the radio or they may try to overload a process like packet acknowledgments. WirelessHART devices can report anomalous conditions that might signal a denial of service attack, such as traffic counters, retransmissions, etc. Other attacks may be indicated by failed access attempts, message integrity check failures, authentication failures, etc.

Device Roles

Devices are network routers as well as data sources. Devices are not authorized to be network key servers or wireless network managers. An important note: A WirelessHART sensor network does NOT implement the TCP/IP communications stack, and thus is explicitly safe from many typical hacker attacks.

Security Manager

As discussed, Join, Network and Session Keys must be provided to the WirelessHART Network Manager and Join keys must be provided to Network Devices. These keys are used for device authentication and encryption of data in the network. The WirelessHART Security Manager is responsible for the generation, storage, and management of these keys.

There is one Security Manager associated with each WirelessHART Network. The Security Manager may be a centralized function in some plant automation networks, servicing more than just one WirelessHART Network and in some cases other networks and applications.

Transitional WirelessHART Device States

- **Idle -** The device is quiescent and its wireless transceiver is not active. It has no knowledge of the WirelessHART network.

- **Joining -** The device is listening for the network, attempting to acquire an advertisement and requesting admission to the network.

- **Quarantined -** The device has successfully joined the network but only has a security clearance to talk with the Network Manager. It is not available or allowed to perform data acquisition or control functions or otherwise communicate with the Gateway.

- **Operational -** The device can be accessed by Host Applications via the Gateway. It is integrated in the system's operation.

  Note: A device may also be **Suspended** or enter a **Re-synching** state after joining.

Summary

Security is a core element of the WirelessHART design and has been addressed with the encryption, validation and other techniques described above. There are also other aspects of the WirelessHART design which make it difficult to intercept