FIELDCOMM GROUP™

Connecting the World of Process Automation

Intrinsically Secure WirelessHART® Field Device Networks and the Industrial Internet of Things (IIoT)

White Paper

Introduction

- With the growing interest in the Internet of Things, as well as growing scrutiny of the security of manufacturing networks, there are ways to put the power of IIoT securely to work in your process plant.
- International standards such as ISA/IEC-62443 provide best practices for developing secure information and operational technology (IT and OT) networks.
- Device connectivity and increased use of wireless naturally increase data management requirements and by association security of that data.
- WirelessHART was designed to be intrinsically secure. It has been vetted through international standardization processes government security audits and – many years of successful usage, with tens of thousands of networks installed.

Table of Contents

Who Should Read this White Paper

This paper will benefit everyone who uses or designs enterprise security as well as those who maintain WirelessHART networks or interested in learning more about WirelessHART security features.

Executive Summary

This paper provides a discussion of security features and use cases for deploying intrinsically safe WirelessHART networks.

The paper is organized into the following sections:

- Introductory information for users who are new to WirelessHART technology
- Standard best practices for users
- Advanced best practices for experienced users and IT professionals
- Glossary

Key Takeaways

- WirelessHART was designed with a priority placed on security from day one
- The WirelessHART specification provides vendors and end users with numerous levels of security
- All WirelessHART communications are required to be encrypted
- Best practices recommend a layered approach to security
- Security considerations for WirelessHART deployments

WirelessHART Basics

WirelessHART (IEC 62591) is a wireless field device communication protocol that is part of the HART (Highway Addressable Remote Transducer) protocol. WirelessHART, a self-organizing mesh network, uses the IEEE 802.15.4 radio standard, which describes low-power wireless communications.

WirelessHART has been designed by industry experts with security in mind. It is an open, multivendor, interoperable protocol that is secure out of the box with security always on and no user configuration needed. This makes WirelessHART a simple, easy to use protocol designed primarily for industrial and other applications.

WirelessHART keeps your data secure by implementing strong encryption using AES 128-bit multiple encryption keys, based on the FIPS-197 standard, a U. S. Government standard for encrypting data. The confidentiality and integrity of your data is ensured as data travels through the network. Even though a field device may route your data, that field device will not have the encryption keys and cannot read the data.

WirelessHART (IEC62591) technology, as designed by leading engineers and scientists from member companies of the FieldComm Group, meets or exceeds process industry security requirements. WirelessHART devices have been successfully used in NERC CIP compliant environments, IEC-62443 environments, as well as having been successfully deployed within the NIST framework.

Major security features of the protocol

- 128-bit message encryption
  - Encryption protects against eavesdropping
- Multiple encryption keys
- Radio security features including:
  - spatial diversity
  - time and frequency diversity
  - power and coding diversity with DSSS (direct sequence, spread spectrum)
- Protections against replay “man in the middle”, “sink hole” and other attacks
- Verifications that messages haven’t been tampered by using integrity codes
- Secure join process with all devices authenticated
  - Prevents against unauthorized devices from joining your network
- Data confidentiality as it’s routed around the network utilizing keys
- Individual sessions with any two WirelessHART entities
- Protection against non-repudiation
- Protection against “denial of service”
- Multi-path mesh networking

Data Security

There are three basic parts to keeping your data secure and usable. First, your data must be available. Next, your data should be confidential, and finally, your data integrity must be assured. Your data must be available or it is useless—you get the data, when and how you need it. Keeping your data confidential means that only authorized people or systems can understand the data and use it. Data integrity means that you can trust that the data hasn’t been harmed or changed.

What is a mesh network?

A mesh is a network topology that allows all the nodes (devices) on the network to communicate with each other. WirelessHART is designed as a self-organizing wireless mesh network in which each node acts as a transmitter and a receiver of data, with a gateway and associated Network Manager and Security Manager. Using algorithms designed into each node or device, the network organizes itself with optimized transmission pathways so that data arrives at the gateway in the most timely manner. The figure below depicts a WirelessHART mesh network.

What is an encryption key?

An encryption key is a random string of bits created explicitly for scrambling and unscrambling data. Encryption keys are designed with algorithms intended to ensure that every key is unpredictable and unique.

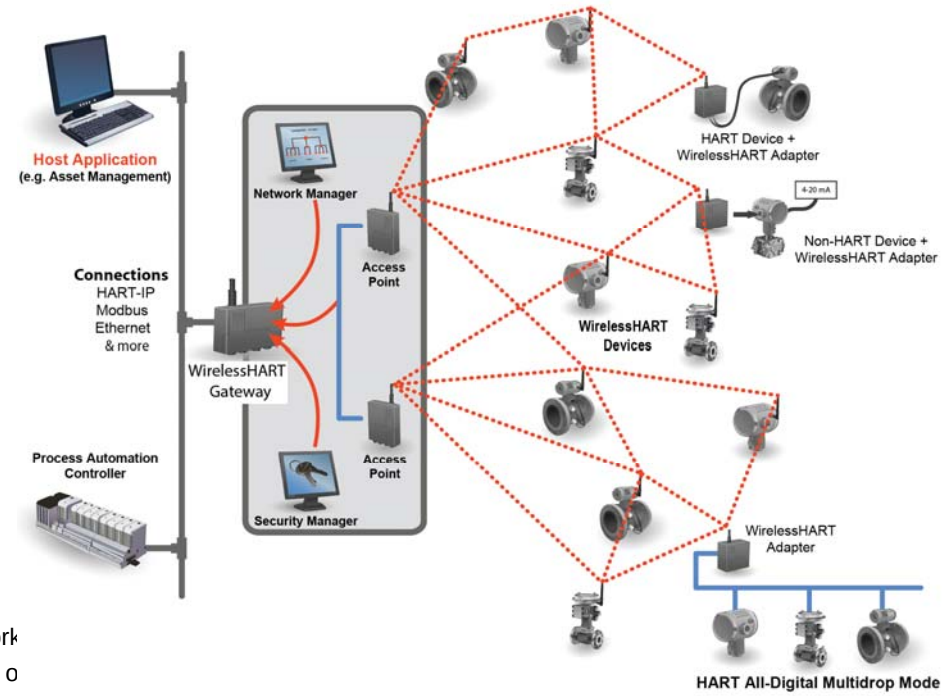
The longer the key built in this manner, the harder it is to crack the encryption code. An encryption key is used to encrypt, decrypt, or carry out both functions, based on the sort of encryption software used

https://www.techopedia.com/definition/25403/encryption-key

Data Availability

Availability is accomplished by specifying IEEE 802.15.4 compliant radios in a wireless mesh network configuration employing frequency, or channel, hopping technology. The protocol provides for multiple tries, re-routing, and the mesh is self-organizing to provide robustness.

WirelessHART instruments automatically use a pseudo-random channel hopping sequence to reduce the chance of interference with other network which o band. Additionally, each network operates on a strict overall timing schedule and each instrument on the network is assigned a time to communicate based on this schedule.



Together, pseudo-random channel hopping and network scheduling act as strong deterrents to security breaches independent of, and in addition to, the cryptographic features of the protocol.

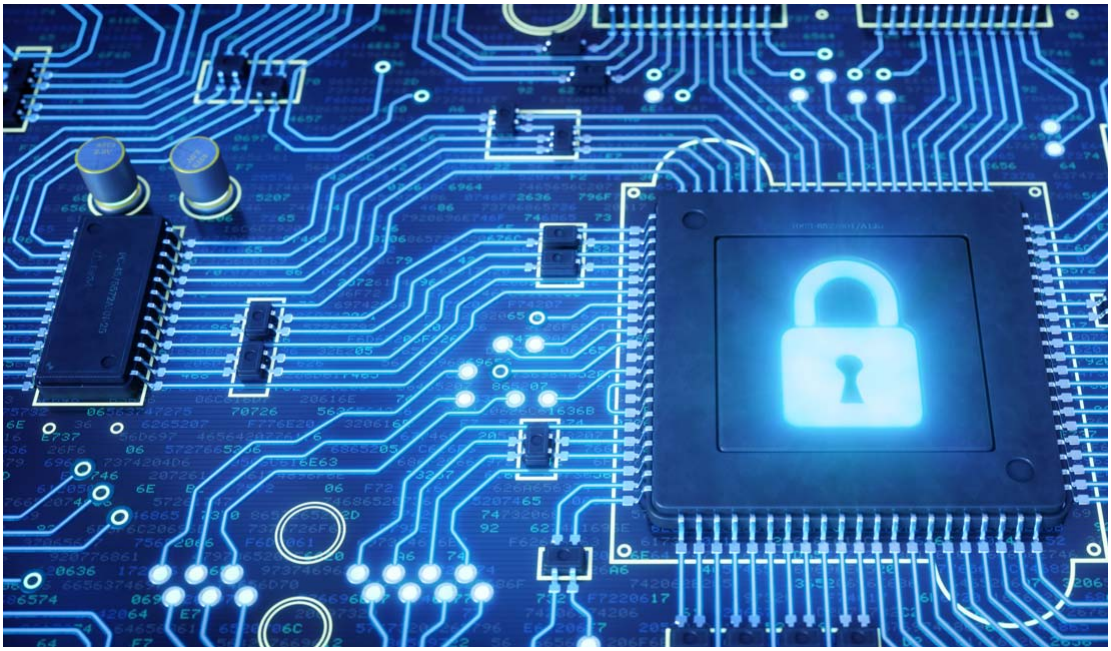
Data Confidentiality

Another integrated and automatic capability of WirelessHART is how confidentiality is maintained by using security features associated with privacy. This prevents eavesdropping by unauthorized devices inside or outside the network. A WirelessHART sensor network provides end-to-end AES-128-bit encryption at the network/transport layer from the data source (e.g. WirelessHART instrument) to the data consumer (e.g WirelessHART Gateway).

Encryption methods include the use of several keys:

1. Individual session encryption keys,
2. A common network encryption key,
3. A separate network join encryption key.

Each key provides security and ensures confidentiality for specific WirelessHART use cases.



Data Integrity and Authentication

Data protection security features associated with integrity and authentication ensure that data sent over the wireless sensor network have come from the correct source and have not been intentionally or unintentionally tampered with or altered.

Keyed message integrity codes (MICs) and cyclic redundancy checks (CRCs) are included in each WirelessHART data packet to ensure integrity. The receiving devices use these codes to confirm that the contents of the packet(s) have not been altered. If the received code doesn't match the calculated code, then the message is discarded.

Data authentication involves verifying that the packet of data has come from the correct source in order to ensure the data can be used and can relied upon. All data communications occur via end-to-end authenticated, secure sessions. The establishment of these secure sessions is discussed later in this white paper.

Strong Key Management

An extremely important part of WirelessHART security involves proper encryption key generation and management. WirelessHART uses multiple keys at multiple layers to ensure security, confidentiality, data integrity and authentication. Join keys, session keys and network keys are used in different ways to protect your data.

Key Management is Crucial for Security

Just as in the IT world, passwords must be kept in a secure fashion. Similarly, for WirelessHART, keys must be stored and distributed securely to ensure their secrecy.

Encryption keys should be randomly generated and must be protected. The use of strong keys rather than default keys, makes it nearly impossible for an attacker to be able to guess a valid key. For this reason, WirelessHART provides the capability to utilize random strong keys. Some systems allow users to choose their own join keys; in these cases, these join keys should be selected and protected carefully. Some other systems may automatically support this entire join key process. All other keys are randomly generated by the WirelessHART network system.

If a common join key is being utilized, it should be changed periodically to increase the overall integrity of the system. Note: if the network is configured to use unique join keys, (also known as an access control list), rotation or changing is

Simplifying security for end users

Security is not an option with WirelessHART. But with numerous features and methods to implement security practices simple, robust, and functional product design is the responsibility of suppliers. Many security best practices are automatically managed by implementers of the specification, making them invisible to users and greatly simplifying procedures.

Never Use Default Keys or Passwords

In line with the security best practices, default keys are not as safe or as strong as a randomly generated key. It is strongly recommended that randomly generated keys be used.

not required, since each key is generated for that device. Ensuring all devices are on the network when the join key is changed will make sure devices aren't orphaned. Some implementations of WirelessHART support automatic changing of keys.

The Security Manager, a part of the WirelessHART system, is usually embedded within the WirelessHART Gateway and automatically handles all keys except for the join key. As a user, this leaves only one type of key to control. In some cases, the security manager can also automatically manage this type of key as well. Implementations which hide all keys from view reduce the chance of inadvertent exposure.

Advanced best practices for experienced users and IT professionals

WirelessHART has built in security. For tips, recommendations and best practices for your specific system, consult your vendor for additional information. The IEC 62591 WirelessHART Engineering Systems Guide (link here) is also an excellent resource for additional good design and installation practices.

Device Access Control Lists Using Unique Join Keys

When designing networks, every network must have a unique network ID and a join key before a device can join the network. This join key can be common for each device on the network or it can be unique to each device, creating an Access Control List (ACL). The resulting ACL identifies devices which are permitted to join the network, also known as a whitelist. By using such a device access control list, you can block unknown nodes from joining and/or monitoring your network.

Physical Security

Physical security adds important protection to any security program and helps protect systems and information. Restricting physical access by unauthorized personnel helps to protect end user assets. This is true not only for WirelessHART systems, but all systems used within the facility. Unauthorized personnel can intentionally or unintentionally cause significant damage to equipment. Access to control system equipment should only be granted to authorized personnel.

Conclusion

The WirelessHART protocol has been specifically designed to provide the highest level of data security to users of field devices in the process industries. Combining the designed-in security features of WirelessHART with both Operational Technology (OT) and Information Technology (IT) network best practices will produce a high performance wireless field device network that maximizes data availability, confidentiality, and integrity, while dependably delivering process data in the industrial industry.

Work with your vendor to better understand specifics.

Glossary

AES 128-bit encryption: Advanced Encryption Standard using a 128-bit block.

Encryption Key: a security measure that turns data into an unreadable cipher.

Field Device: Valve, Transmitter or other device with WirelessHART enabled.

FieldComm Group: the organization that owns the HART and WirelessHART, Foundation Fieldbus and FDI specifications.

Gateway: the connection from the WirelessHART field devices to the control system.

HART: Highway Addressable Remote Transducer protocol for wired and wireless communication between field devices and a control system

IEEE 802.11 b/g: WiFi

IEEE 802.15.4 mesh network standard for wireless devices

IT: Information Technology (as opposed to OT)

MIC: Message Integrity Check, a field in the data designed to indicate that the data hasn't been tampered with or changed.

Mesh Network: A network composed of nodes that can communicate with every node on the network. A wireless mesh network can be self-organizing and provide optimization for communication from each node.

Network Manager: software that controls the mesh network

OT: Operations Technology, IT for the plant floor (as opposed to IT)

Security Manager: software that provides the security features of a WirelessHART network

Whitelist: a list of all the trusted devices on the network.

FieldComm Group is a global standards-based non-profit member organization consisting of leading process end users, manufacturers, universities and research organizations that work together to direct the development, incorporation and implementation of communication technologies for the process industries.

FIELDCOMM GROUP™
Connecting the World of Process Automation

For More Information, contact:

FieldComm Group
9430 Research Blvd., Suite 1-120 Austin, TX
78759 US
Tel: 512.792.2300
www.fieldcommgroup.org

June 2017