IEC 62591 *Wireless*HART® System Engineering Guide

Revision 2.2

This document provides guidelines for implementing WirelessHART systems in the project process

EMERSON. Process Management

System Engineering Guide for *Wireless*HART

Contents

Preface

This document has been created to support the developing need of *Wireless*HART end users adopting self-organizing mesh networks into the process industry.

This document recognizes *Wireless*HART products available from the HART COMMUNICATIONS FOUNDATION and its members.

This document assumes the reader is proficient with HART instrumentation, therefore the focus of this content will be on the unique aspects of deploying *Wireless*Hart systems. Unless stated otherwise, the reader should assume the project steps are the same for HART and *Wireless*HART instrumentation.

This document is intended to serve as the framework for advanced discussions on the implementation of *Wireless*HART systems.

Authors

A special thanks to the contributors and reviewers of this guide:

Contributor	Company
Daniel Carlson (Editor)	Emerson Process Management
Moazzam Shamsi	Emerson Process Management
Ted Schnaare	Emerson Process Management
Dan Daugherty	Emerson Process Management
Jeff Potter	Emerson Process Management
Mark Nixon	Emerson Process Management

Reviewers

Contributor	Company
Jeremy Fearn	Emerson Process Management
Jeff Jacobson	Emerson Process Management
Lara Kauchak	Emerson Process Management
Rob Train	Emerson Process Management

Revision

Revision Number	Date	Description
2.0	October 2010	Initial Release
2.1	13 November 2010	Added metric references for distance, corrected errors in table of contents
2.2	24 November 2010	Minor editorial corrections.

Disclaimer

This document is informative only and is provided on an "as is" basis only. The document may be subject to future revisions without notice. The authors and contributors will not be responsible for any loss or damage arising out of or resulting from a defect, error or omission in this document or from any users use or reliance on this document.

Feedback

Send feedback to Dan Carlson: Daniel.carlson@emerson.com

- Comments
- Recommendations
- Content Requests

Section 1 Introduction

Purpose

The *Wireless*HART System Engineering Guide is intended to detail how *Wireless*HART devices can be included in capital projects of any size.

Scope

This document includes considerations for *Wireless*HART devices through the capital project cycle as well as the lifecycle of the *Wireless*HART device.

Considerations are given for the differences between HART and *Wireless*HART specifications and *Wireless*HART device types that are unique to the *Wireless*HART standard (IEC 62591).

Exhaustive considerations are not given for minor differences between HART and *Wireless*HART devices; nor features specific to a vendor; nor are exhaustive studies of integration given into various host systems.

Definition

*Wireless*HART is a global IEC-approved standard (62591) that implements a common self-organizing mesh technology in which field devices form wireless networks that dynamically mitigate obstacles in the process environment. This architecture creates a cost-effective automation alternative that does not require wiring and other supporting infrastructure. *Wireless*HART field networks (WFN) communicate data back to host systems with reliability demonstrated in the field in excess of 99% and are capable of both control and monitoring applications.

The similarities between *Wireless*HART and HART allow wireless devices to leverage the training of existing process organizations, minimizing change and extending the benefits of automation to end users who previously could not justify the inclusion in wired capital projects. This opportunity and long-term benefit justifies the addition of new end users including maintenance, safety, environmental, and reliability, in the FEED (Front-End Engineering and Design) of new projects. Additionally, by removing many of the physical constraints of wiring and power, wireless networks provide new flexibility in project execution.

Section 2 Definitions

Terminology	Definition
Gateway	Enables communication between wireless field devices and host applications connected to an Ethernet, Serial, or other existing plant communications network; management of the wireless field network; and management of network security. Conceptually, the gateway is the wireless version of marshalling panels and junction boxes. The gateway functionality may also exist in native *Wireless*Hart I/O cards with field radios
Host System	A system which is typically used for plant control (e.g. DCS or PLC).
Join Key	A four byte numeric field in hexadecimal format used as a security measure by *Wireless*Hart devices to certify that they are valid members of the network. This Join Key may be assigned randomly or specified by the user. The Join Key and Network ID must be identified by both the *Wireless*Hart gateway and device for communication to be established.
Network ID	A integer between 0 and 36863 that specifies the *Wireless*Hart network. Unique gateways and their associated networks should have unique Network IDs. All devices with the same Network ID will operate on the same network and gateway. This Network ID is considered part of the *Wireless*Hart security as it is required to join the network.
Scan Rate	The user specified interval at which a wireless field device will detect a measurement and transmit the measurement to the gateway. The scan rate is the largest impact on battery life due to the powering of the device sensor. Scan rate is independent of radio transmissions required for mesh “hopping” from multiple devices to transmit a measurement

	back to the gateway.
Wireless Adapter	Enables an existing 4-20 mA, HART-enabled field device to become wireless. Adapters allow the existing 4-20 mA signal to operate parallel to the digital wireless signal.
Wireless Field Devices	Field device enabled with a *Wireless*HART radio and software or an existing installed HART-enabled field device with an attached *Wireless*HART adapter.
Wireless Field Network	A self-organized network of wireless field devices that automatically mitigate physical and RF obstacles in the process environment to provide necessary bandwidth for communicating process and device information in a secure and reliable way.
Wireless Repeater	Any wireless field device used to strengthen a wireless field network or expand the distance between wireless measurements.

Acronyms

Abbreviation	Description
FEED	Front-End Engineering and Design

Section 3 Project Concepts

Pre-FEED

During the Pre-FEED phase, consideration must be given to available technologies and an assessment made on the applicability to fulfilling the needs of the project and application. It is during this Pre-FEED phase that *Wireless*Hart should be considered as a candidate technology, along with other protocols including HART, Foundation Fieldbus, and Profibus.

During the Pre-FEED phase, spectrum approvals for the end-user and any intermediary locations should be verified. Refer to Appendix D Wireless Spectrum Governance for more details.

An integrated approach should be used for incorporating wireless into a project. Wireless should be merged with the established procedures for a wired project. The key consideration is to use the right field device technology for the right application and expand consideration for the end users represented in the FEED.

Right Technology for Right Application

*Wireless*HART is designed for both control and monitoring, however most current use cases emphasize monitoring applications due to conservative adoption of technology to meets the needs of a conservative industry.

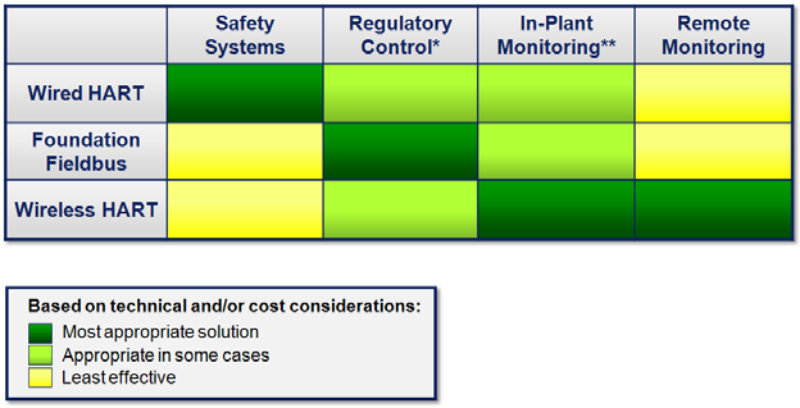


Figure 1. Selecting The Right Protocol

Technology Evaluation

The project should have design rules established to define what measurement points are *Wireless*HART and which are not to enable consistency and efficient engineering for subsequent project phases.

The technical authority will make a decision to use wireless based on the following high level criteria:

- Economic Assessment
- Potential applications
- Potential operational savings
- Potential benefit of new measurements providing additional process insight
- Benefits of adding measurement not previously considered or feasible for inclusion in the automation system due to economics or practicality
- Benefits of flexibility in project execution (e.g. ease of addition of points)

The economics of installing wires has primarily limited the benefits of automation to process control and safety applications with additional points added over the life of the plant to resolve critical problems. Since *Wireless*HART does not require wires, the economics of automation redefine the financial hurdle rate that determines if a point is automated or not. With *Wireless*HART, points that have been traditionally indicated with a gauge, or not at all, can be automated. Additionally, *Wireless*Hart enables diagnostics and other Hart information to be sent to different locations without requiring more infrastructure or impacting the control system and its I/O. With new field information easily available, end users including maintenance, asset protection, health/safety/environment, and reliability should be considered in the FEED and Design Phases.

FEED

Key deliverables exist for wireless in the FEED, for example: cost estimating, design guidelines, and specifications.

Cost Estimation

Vendors of *Wireless*HART field devices may have cost calculators and capital project studies that can be referenced and compared to support the cost justification of wireless into a project or an all wireless project. For a large capital project, wireless can reduce capital costs by switching wired monitoring points to wireless.

Design Engineers should assess and incorporate the following factors in their project cost estimating calculation model:

- Reduced engineering costs (including drawing and documentation, as well as FAT)
- Reduced labor (field installation, commissioning, supervision)
- Reduced materials (terminations, junction boxes, wiring, cable trays/conduit/trunking, power supplies, and control system components)
- I/O capacity management (each *Wireless*Hart gateway essentially provides spare I/O capacity)

Design Guidelines for *Wireless*HART

During the FEED, all project stakeholders should be made aware of the capability and benefits of *Wireless*HART so that design engineers can identify potential candidate applications. The project should develop a wireless design guideline that must be circulated to all project stakeholders.

For example the process design engineer can use a set of criteria such as the simplified table in Figure 2 to identify candidate wireless applications.

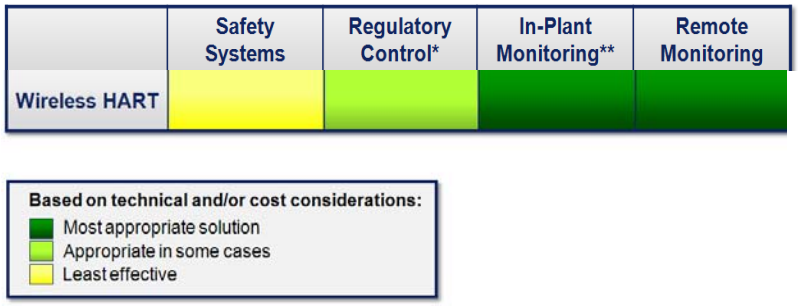


Figure 2. Example Criteria

Candidate *Wireless*HART applications are ideally identified during the early process design phase during FEED. This could be during Process Flow Diagram (PFD) and Piping and Instrument Design (P&ID) Diagram development. However, if an early decision is not taken this should not preclude the use of the technology later in the project.

The basis for design should be shared amongst all stakeholders so that other technical design authorities can identify potential wireless applications and benefit from the installed wireless infrastructure. Furthermore, this process ensures consistent implementation across all design authorities and allows for an efficient decision process to use wireless.

Points to consider when setting guidelines:

- Determine which categories of points are eligible to be wireless: safety, control, monitoring, and local indication.
- Determine if new users are eligible for automation: process efficiency, maintenance, reliability, asset protection, health/safety/environmental.
- Determine percent spares required and necessary spare capacity.
- Factor in distance limitations. Typical clear, line of sight allows for distances of 750 feet (230 meters) between wireless field devices. Best practices manage this constraint.

Specifications

Specifications for *Wireless*HART field devices are 90% the same as wired HART devices. See Appendix B *Wireless*Hart vs. Wired Hart Comparison for examples. Hart instrumentation specifications are the foundation for *Wireless*HART specifications. The fundamental differences with regards to the ISA-20 specifications are output signal, power supply, scan rate, protection type/enclosure. Specifications not included in this short list are either included with the IEC 62591 *Wireless*HART standard, small deviations from HART that require optional attention for the specification process, or are unique to a field device vendor.

Figure 3 is a comparison of fundamental differences in the specification[1]:

Specification Field	Typical HART Specification	Typical *Wireless*HART Specification
Output Signal	4-20 mA HART	IEC 62591 *Wireless*HART
Power Supply	24V DC Loop Powered	Intrinsically Safe Battery[2]
Scan Rate	1 second	1 second to 60 minutes
Protection Type/Housing	Explosion Proof	Intrinsically Safe[2]

Figure 3. Key Differences Between Wired and *Wireless*Hart

IEC 62591 *Wireless*HART is an international standard for wireless process devices. The standard includes advanced provisions for security, protocol, and other features and therefore specification of such attributes covered in the standard are not necessary.

0 provides example specifications for a *Wireless*HART gateway and wireless adapter that can be generically specified as transceivers/receivers.

Detailed Engineering

During the detailed engineering phase of a project, the engineer must account for *Wireless*HART devices per the guidelines established in the FEED, add wireless specific fields to the project database, and conduct wireless field network design procedures to ensure best practices are implemented.

Sort the Points

From the wireless guidelines established in the FEED, the engineer should do a sort of all points in the project data to identify which are eligible to be wireless. For example, if monitoring is deemed to be an eligible category, these points should be sorted from the control and other points. Afterwards, further requirements of the field devices can be applied. For example, some control points may be excluded from wireless eligibility because the required scan rate exceeds either the desired life of the battery or the capability of the field device.

Typical safety and control scan rates may require 1 second or faster. There is a trade-off for wireless devices between scan rate and battery

[1] Values in table are typical and representative, but not comprehensive.
[2] The trend with wireless field device vendors has been intrinsically safe protection, with explosion proof an option. This discrepancy is presented in the best interest of the audience to do thorough due diligence.

life; the faster the scan rate, the lower the battery life will be. The current recommendation is that an application should have a time constant satisfied by a scan rate that supports a battery life of multiple years for reduced maintenance. However, this trade-off favor faster scan rates if the wireless device will be powered externally, through a wireless adapter using power scavenging from the 4-20mA loop, or if battery maintenance is not a concern for that application. Additionally, it is recommended that the scan rate of the measurement be three times faster the process time constant. As an example, measuring temperature changes with a sensor inside a thermowell can be 16 seconds for slow changing temperatures given how long it heat to penetrate the thermowell.

Database Field for Wireless

Each wireless field device must be assigned to a unique gateway that must manage a unique wireless field network. There must be a field that indicates the association of the field devices to the gateway. Without this information, the wireless field device will not be able to receive the proper security provisions to join the wireless field network nor the proper integration into the host system from the gateway. Gateways can have a HART TAG like a HART device, wired or wireless.

Each gateway will manage its own unique wireless field network. Each wireless field network in a plant must have a unique Network ID and Device Join Key to prevent devices from joining the wrong network and insuring proper security; these parameters are akin to a user name and password. Below are examples of a gateway HART TAG, Network ID and Device Join Key.

Parameter	Parameter Options	Example	Technical Details
Gateway HART TAG	Field	UNIT_A_UA_100	32 characters – any in ISO Latin-1 (ISO 8859-1) character set.
Network ID	Number	10145	Integer between 0 and 36863
Device Join Key	4 Fields	23adfe00-0edf000a-000df038-2398dc07	4 four byte numeric fields (in Hexadecimal format). For example - 32 character fields where each character must be a number from 0-9, or a letter from A to F. Randomize for

greatest strength.

Figure 4. Definitions of Network Parameters

For security purposes, the Device Join Key is the most important for implementing security. A user can know the Gateway HART TAG and the Network ID for the network the gateway manages, but without the Device Join Key, a wireless field device cannot join the network. The design engineer should be sensitive to the security policies of the design firm and the security policies of the future owner/operator and, as a minimum, treat the Device Join Key with the same sensitivities as a password for a server to a DCS or database.

Fields should be added to the project database for indication that a field device is wireless and its association with a gateway using the gateway HART TAG or other labeling convention. Parameters required to be managed confidentially should be controlled in a secure means in alignment with established security policies. Staff members with IT security or process security responsibilities are well suited to provide consultation into the handling of sensitive information.

Finally, the design engineer should have awareness into available *Wireless*HART devices. Many come with multiple inputs that can satisfy the total number of points in a project with fewer devices. For example, several vendors have a multiplexed *Wireless*HART temperature device that reduces costs.

Network Design

Once wireless candidate devices have been identified in the instrument database the field network design can begin.

Ideally wireless points should be organized by process unit and by subsection of process unit as typically depicted in a master drawing. This information can be used to determine the number of gateways required. Additional gateways can be added to ensure spare I/O capacity per guidelines or other project requirements. From here, the gateways can be logically distributed throughout the process unit like marshalling panels. Wireless field devices can then be assigned according to which gateway is closest or by which gateway is assigned to the process unit subsection in which the field devices reside. Once this is complete, network design best practices can be checked to ensure the network will be reliable. This will be covered in detail in the Section 7 *Wireless*Hart Field Network Design Guidelines.

Drawings should be created per existing standards. In most instances, a wireless field device is treated identically to a wired HART device. Most drawings do not indicate wires or the type of protocol, thus nothing unique needs to be done for wireless field devices. Section 6 Ancillary Device Requirements documents examples specific to wireless field devices and devices unique to *Wireless*HART such as gateways and wireless adapters. Fundamentally, it will be up to the design engineer to adhere to or provide a consistent convention that means the needs of the contractor and the owner operator as is true for wired HART projects.

Existing HMI (human-machine interface) design guidelines for integration also apply to wireless no change is required.

Factory Acceptance Test

For Factory Acceptance Tests, it will be necessary to establish a connection between the Gateway and the Host Systems. *Wireless*HART gateways have standard output protocols that either directly or indirectly can connect to any host system. The design team should keep a library of these integration options for reference.

Installation

In general, *Wireless*HART device are installed identically to wired HART devices. Emphasis should always be placed on making the best possible process connection for accurate measurement. The self-organizing mesh technology in *Wireless*HART enables wireless field devices to self-route through process environment and reroute when the environment changes. Always consult the manual of the *Wireless*HART device for special considerations. This is covered in detail in Section 7 *Wireless*Hart Field Network Design Guidelines.

*Wireless*HART adapters are typically installed on the existing HART enabled device or somewhere along its 4-20 mA loop. Always consult the manual of the *Wireless*HART adapter for special considerations.

*Wireless*HART gateways are typically placed 6 feet (2 meters) above the process infrastructure (typically above cable trays) and located in the process unit where the maximum number of connections with wireless field devices can be achieved. For small networks, typically less than 10 devices, there is sometimes a need to fortify a wireless network with a repeater. A repeater is any wireless field device used for the sole

purpose of providing additional wireless connectivity. Repeaters are installed like a gateway, but near the location needing additional wireless connectivity.

It is recommended that the gateway is installed first; this allows host system integration and wireless field device installation and commissioning to commence in parallel. Wireless field devices can be completed as soon as process connections are in place. If the wireless device is activated, it will form a network that compensates for the current condition of the process unit and will adapt as the unit is built. The project manager can have wireless device installation occur in parallel with construction to maximize project time buffers or pull in the project completion date.

Commissioning

In general, *Wireless*HART gateways segment the commissioning process. Since gateways connect the wireless field devices to the host system, *Wireless*HART devices can be commissioned to the gateway to ensure proper connectivity. A wireless loop check can confirm connectivity through the gateway to the host system. Interaction with the process and the *Wireless*HART device can confirm the device is operational.

Section 4 Document Requirements

Drawings

Every project will require the establishment of local standards for implementing consistent documentation.

See Section 11 Documenting in Integraph SPI 2009 for a complete treatment of documentation.

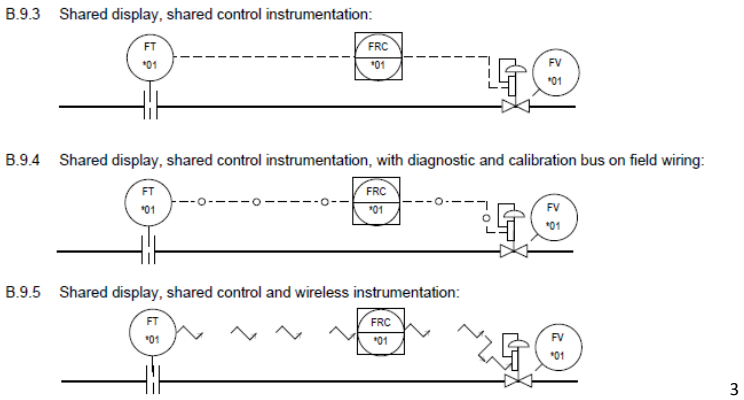
ISA Documentation

The American National Standard document ANSI/ISA-5.1-2009: Instrumentation Symbols and Identification, approved on September 2009, provides basic guidelines for wireless instrumentation and signals.

Key points:

1. There is no difference in the symbol between a HART, FF, and a *Wireless*HART device. An instrument is an instrument.
2. The line style for indicating a wireless signal is a zig zag and not a dash.

   Below is an image from the ISA-5.1 document showing some comparative examples. Please reference ISA-5.1 for complete details.



[3]

Figure 5. ISA 5.1 Wireless Drawing

3. The implementation of *Wireless*HART requires far fewer components, making drawings simpler.

[3] ISA-5.1

Control Narrative

Define in the FEED phase and ensure this is implemented with design guidelines.

Instrument Index/Database

See Section 11 Documenting in Integraph SPI 2009 for recommendations for additional fields not typically included in wired HART specifications.

Instrument Data Sheets

Use standard data sheets created for wired HART devices. Update the following fields to reflect *Wireless*HART:

Specification Field	Typical Value
Scan Rate	1, 2,4, 8, 16, 32, 64+
Power Supply	Intrinsically safe, field replaceable battery
Communication Type	*Wireless*HART

Figure 6. WirelessHart Specifications For Instrument Data Sheets

No special ISA or other specification sheets are required as the same sheets can be used to specify HART, FOUNDATION Fieldbus, or *Wireless*HART. See 0 for a specification sheet example for a *Wireless*HART gateway.

Material Requisitions

Given the need for security and RF emissions, vendors must acquire approvals for importation to the country of end-use for compliance with local spectrum regulation and encryption regulation. The vendor can verify whether importation compliance exists for any given country.

The batteries are commonly made using a high energy compound using Lithium Thionyl Chloride. The Material Safety Data Sheet or equivalent should always be available as well as awareness of any shipping restriction, particularly for passenger aircraft.

Manufacturer Documentation

Every *Wireless*HART device should have the proper documentation, including manual, as would be expected with a wired HART device.

Project Management

Subcontractor Scope Management

Wireless enables simplified sub contractor scope management. Packages can be easily tested and commissioned separately, requiring

only minimal integration and testing to occur. Additionally the sub contractors will also benefit from fewer components and engineering. Tender contracts should be amended to recognize reduced complexity and eliminated work.

Project Scheduling

1. Review schedules to recognize:
   - Limited infrastructure installation and hence reduced material and installation scope
   - Remove some electrical and instrumentation checkout processes
2. Amend contracts to reflect simplified installation handover processes
3. Simplify installation schedule management
4. Reduce material coordination management and simplified construction schedule
   - Eliminated scheduling and expediting associated with marshalling cabinets
5. Schedule should reflect eliminated activities and simplified FAT, SAT and SIT (site integration test) on areas where wireless has been extensively deployed

Responsibility and Skills Matrix

- Amend Roles and Responsibility matrix to reflect reduced/eliminated responsibilities
- Ensure engagement of all project stakeholders/sub-contractor so that wireless can be applied efficiently to improve schedule and material costs

Managing Project Variations

For project change orders and other late design changes, wireless should be considered as the primary solution unless other design considerations exist. Using wireless will result in the fewest changes to the documentation, I/O layout and other detailed design as well as faster commissioning.

Section 5 Field Device Requirements

Support for *Wireless*HART Functionality

All *Wireless*HART devices support methods to allow remote access to device configuration, backwards compatibility with existing field communicators, full implementation of *Wireless*HART security provisions, and *Wireless*HART interoperability.

*Wireless*HART Verification

The literature of the *Wireless*HART device should indicate its compliance to the *Wireless*HART standard. The logos should be present representing *Wireless*HART, a device descriptor (DD) for field communicators, as well as asset management programs.

Device Diagnostics

HART Diagnostics

*Wireless*HART devices contain similar or a subset all of the diagnostics of wired HART devices.. Expect configurable alarms and alerts for both the process and the device. Diagnostics information should be available through HART commands as well as accessible through Device Descriptions (DD) either locally through a field communicator or remotely using asset management software.

Wireless Field Device Network Diagnostics

Every *Wireless*HART field device has diagnostics that indicate if a device is connected to a network or not.

Wireless Field Device Power Diagnostics

Wireless field devices will have one of three power options: battery, energy harvesting (including solar), or line power. Batteries will have a life determined by the scan rate of the wireless field device, network routing for other wireless field devices, and efficiencies of the sensor and electronics. Typically, the primary consumer of power is the wireless field device sensor and electronics; using the *Wireless*HART radio or acting as a repeater/relay for other WirelessHART field devices requires minimal power. Wireless field devices report their battery voltage and have integrated low voltage alarms such that the user can schedule maintenance take corrective action.

Gateway Network Diagnostics

Gateway network diagnostics should indicate whether field devices are connected and functioning properly, and if devices are missing from the network. In order to be connected properly, proper bandwidth must be allocated based on the scan rate of the device. A device connected but with service denied may indicate a device has a scan rate that is too fast for the network capability or the network conditions. With gateways capable of holding 100 devices or more, clear indication of device availability is crucial.

Additionally, gateways should be able to detect, regardless of host system integration, the connectedness of a wireless field device. This information should be continually updated and indicate if a device is not connected for network or device reasons. Simple device states should be made available for integration into the host system regardless of output protocol from the gateway to indicate online/offline status.

Field Device Power

Wireless field devices will have one of three power options: battery, energy harvesting (including solar), or line power and there may be several options with in each category.

Batteries

The most common will be the use of a battery for low power field devices due to ease of deployment. Most vendors will use battery cells incorporating Lithium Thionyl Chloride chemistry since it has the highest energy density that is commercially viable. Although typical cells look like battery cells for consumer electronics, precautions should be taken to ensure batteries are safely introduced into the process environment. Refer to vendor documentation for safe handling practices.

Below are requirements for batteries:

- Batteries cells should be assembled by a manufacturer into a battery module to ensure safety.
- Battery module should prevent a depleted cell being introduced in circuit with a charged cell, which can cause unintended electrical currents and heat.
- Battery module should provide ease of replacement. Battery replacement should take minimal time and training.

- Battery module should be intrinsically safe and not require removal of the wireless field device for replacement.
- Battery module should prevent intended and unintended short-circuiting that could lead to heat or spark.
- Battery module should be designed for the process environment with mechanical properties that provide drop connection and operation over normal process temperatures expected for devices.
- Battery modules should come with necessary Material Safety Data Sheets (or equivalent) and warnings and be disposable per local governmental regulation.
- Battery module should not be capable of connecting to consumer electronics or non-designed applications to prevent a high-capacity supply from being connected to incompatible electrical systems.
- Battery modules should be applicable to several *Wireless*HART field devices to maximize inventory management efficiencies in the local warehouse for spare parts.

The design engineers of the wireless field network and end users should use scan rates that maximize the life of the battery module and minimize maintenance.

Energy Harvesting

Vendors may provide energy harvesting options as alternatives to batteries that may include solar, thermal, vibration, and wind solutions. Current energy conversion techniques for thermal and vibration are relatively inefficient. In many cases, energy harvesting solutions also utilize rechargeable batteries to maintain constant supply. Today's rechargeable batteries have a life expectancy of only several years during which they can maintain a full charge. This life expectancy is often shorter than that of non-rechargeable Lithium Thionyl Chloride batteries. Adoption energy harvesting is likely to increase as vendors reduce the voltage and power consumption of wireless field devices and technical difficulties are removed from harvesting technologies. The current, most viable solution is solar, which has the difficulty of maintaining incidence of light on solar arrays as seasons change along with the tilt of the earth relative to the sun. Additionally, difficulties

have been experienced even in desert environments with an abundance of light due the need to keep the solar panels clean for maximum energy conversion.

Below are requirements for energy harvesters:

- Wireless field device should have a design connection for energy harvesting device.
- Energy harvesting device should have means for providing multiple days of power in the event the energy source is discontinued for several days.
- Energy harvesting device should be mounted such that it is not negatively impacted by changes in the season.
- Energy device should be intrinsically safe and incapable of generating heat or short circuits like the battery module.
- Energy harvester should have the means for the user to know the state of the device.
- Energy harvester should be able to be locked out to prevent uncontrolled energy production.

Line Power

In some ways, a line power option is counter-intuitive for a wireless device. However, some wireless adapters may harvest power off of 4-20 mA loop power devices, and some applications with high power sensors may need to be wireless and require more power than a battery or energy harvester can provide.

Below are the requirements for a line power option:

- Wireless adapters harvesting power from the 4-20 mA loop of the wired device should not affect the control signal during normal operation or failure mode.
- Line powered wireless devices not designed specifically for 4-20 mA loops should not require pristine power supplies. They should be capable of a wide range of voltages and not require filter of noise or special conditioners for proper operation.

Field Device Security

Security is a new consideration that is driven by an increased focus on critical infrastructure security, particularly by governments and other compliance authorities.

Below are the requirements for wireless field device security:

- Wireless devices should be compliant with all *Wireless*HART security provisions including correct usage of Network ID and Device Join Key.
- The user or unintended user should not be able to physically or digitally read the Device Join Key from the wireless device. The Device Join Key should be treated as confidential and subject to the requirements of any local security policy. Although this may be deemed an inconvenience to the intended user, this can be alleviated with work practices that provide an approved method of accessing the necessary security parameter. For example, a technician with low level security clearance could retrieve the Network ID and Join Key from a gateway administrator with proper access to the gateway.
- The wireless device should be receptive to changes to the security provision from the gateway, including Network ID, Device Join Key, and the network, session, and broadcast keys that validate packets sent through the network and prevent tampering and eavesdropping.
- The gateway and any management program connected through the *Wireless*HART network through the gateway should protect all security parameters according to a local security policy.

Approvals

Every *Wireless*HART device must have the appropriate hazardous area approval to meet the conditions of the process environment as well at the appropriate spectrum and encryption approvals. Spectrum and encryption of wireless signals are regulated by government agencies, such as the FCC in the United States. Typically, verifying with the *Wireless*HART device manufacturer that the device has proper approval for importation to the country of usage is sufficient. Spectrum and encryption approval are a procurement issue and do not represent a design parameter like a hazardous area approval.

Accessibility

*Wireless*HART devices are subject to the same mechanical and electrical specifications as wired HART devices as they will operate in the same process environments.

Below are general requirements for *Wireless*HART field devices:

- *Wireless*HART devices shall be locally accessible with HART field communicators that support wired and *Wireless*HART devices.
- *Wireless*HART devices shall be manageable with remote asset management systems that access the *Wireless*HART device via the gateway and through the *Wireless*HART network.
- *Wireless*HART adapters shall extend the benefits of a *Wireless*HART network to wired HART devices that may or may not be operated on a 4-20 mA loop.

Section 6 Ancillary Device Requirements

An ancillary device is defined as any device that does not contain a measuring sensor or output to the process for actuation. These include wireless gateways, local indicators, wireless repeaters and/or *Wireless*HART adapters.

Gateways

The gateway enables communication between wireless field devices and host systems connected to an ethernet, serial, or other existing plant communications network; management of the wireless field network; and management of network security. Conceptually, the gateway is the wireless version of marshalling panels and junction boxes.

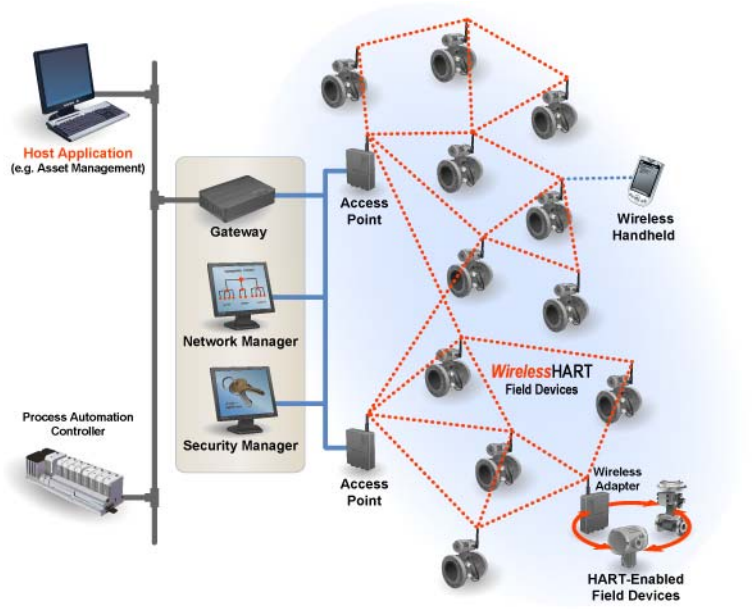


Figure 7. Gateway System Architecture

Below are the requirements for a *Wireless*HART gateway:

- The gateway should provide a manageable solution for enabling gateway, network management, and security management functionality. In this document, the gateway term is used in this context of multiple functions where as other system integration discussions refer to the gateway as just a protocol conversion.
- Gateway shall have controlled access for a security policy. Gateway should have multiple user accounts with differing

access to critical security and configuration parameters such that there can be a sole network administrator.

- Gateway shall have multiple output protocols to ensure integration to a range of host applications. In any given process facility, there can several types of DCS, PLC, and historians requiring unique protocols. Multiple output protocols allow convenient connectivity with a standard gateway.
- The gateway shall support multiple connections and, in effect, act like a server. Typical *Wireless*HART applications require data to be sent to multiple host applications in order to provide data to multiple end users.
- The gateway shall support the secure transfer of all protocols over an Ethernet connection through an encryption process.
- Gateway shall be interoperable and support the network management of *Wireless*HART devices from multiple vendors.

Wireless Repeaters

There are no special requirements for a *Wireless*HART repeater. If a repeater is a *Wireless*HART device with a configurable scan rate, then minimizing the scan rate shall maximize the life of the battery module without impacting the network reliability.

If a vendor chooses to develop a *Wireless*HART device for the specific purpose of acting as a repeater, then that repeating device shall be manageable like any other *Wireless*HART device and subject to all the specifications of a *Wireless*HART device. *Wireless*Hart adapters can be used effectively as repeaters if local power or a wired HART device is available.

*Wireless*HART Adapters

*Wireless*HART adapters connect to wired HART devices that are not inherently wireless and provide parallel output signals through the 4-20 mA loop and the *Wireless*HART field network. There are three main use cases for *Wireless*HART adapters:

- Access HART diagnostics that are not accessible due to limitations of the host system which may prevent the HART signal from passing over the 4-20 mA loop.

- Provide wireless communications for HART devices which are not natively wireless.
- Enable device information to be accessed by multiple users who may not have direct access to the control system. In this scenario, the wired signal is sent to the control room while the wireless signal could be accessed in a separate office by maintenance, reliability, or other personnel.
- Act as a wireless repeater.

Below are the *Wireless*HART Adapter specifications:

- Adapter should not affect the 4-20 mA signals under normal operation.
- Adapter should not affect the 4-20 mA under failure conditions.
- Adapter should operate like any other *Wireless*HART field device in the *Wireless*HART field network.
- Adapter should have a HART Tag.
- Adapter should pass through the wired HART device process variable as well as remote access for configuration and calibration.

Section 7 *Wireless*HART Field Network Design Guidelines

The design of a *Wireless*HART network enables a successful and scalable architecture. Contrary to legacy systems and point-to-point wireless networks, *Wireless*HART is a truly scalable automation technology that gets more robust as more devices are added to an existing network. Design guidelines support the deployment of small networks, less than 10 *Wireless*HART devices, as well as segmenting multiple networks when a process facility requires far larger numbers of *Wireless*HART devices. Additional recommendations are also provided to support the long-term, sustainable adoption of wireless applications including: *Wireless*HART, Wi-Fi, Wi-Max and more.

The best practices for network design are general for networks operating with mix of *Wireless*HART devices with a variety of scan rates from 4 seconds to 3600 seconds (60 minutes). Please see the section Designing for Control for additional considerations when including 1 second scan rates.

A site survey is not normally required or even possible in the case of a Greenfield site. For an overview on spectrum usage refer to Appendix D Wireless Spectrum Governance.

Wireless Project Overview

An extensive overview of the project overview was previously discussed in Section 3 Project Concepts.

Because *Wireless*HART is built upon the HART standard, there are minimum differences between the usages of the devices. The minimal need for wires also means there are fewer engineering details to manage and fewer engineering parameters to introduce. This section provides a thorough discussion of the Project Concepts.

It is the discretion of the user to consider the following discussions which can be applied to small projects requiring a single gateway or a large project requiring several gateways.

WirelessHART Field Network Design

There are three key steps for designing a network:

- Scope – Divide wireless field networks into a single process unit or subsection of a process unit.
- Design – Apply design rules to ensure optimum connectivity.
- Fortify – Fix any potential weaknesses in the network design.

The three basic steps apply for all process environments in all industries, although the context may vary slightly depending on the physical structure of the environment. The basic steps also apply regardless of the vendor of the *Wireless*HART device. Since *Wireless*HART networks become stronger the more devices are added, the Scope step is the most critical for high density applications.

Scoping

The same design rules that govern the segmentation of wired HART networks apply to *Wireless*HART. From a very simple perspective, all process facilities have an architecture that organizes the infrastructure as well as the automation and the people. *Wireless*HART not only self-organizes to the process environment, but also to this inherent organization of the process facility. For example, the process facility below is organized into 7 process units that are separated by roads.

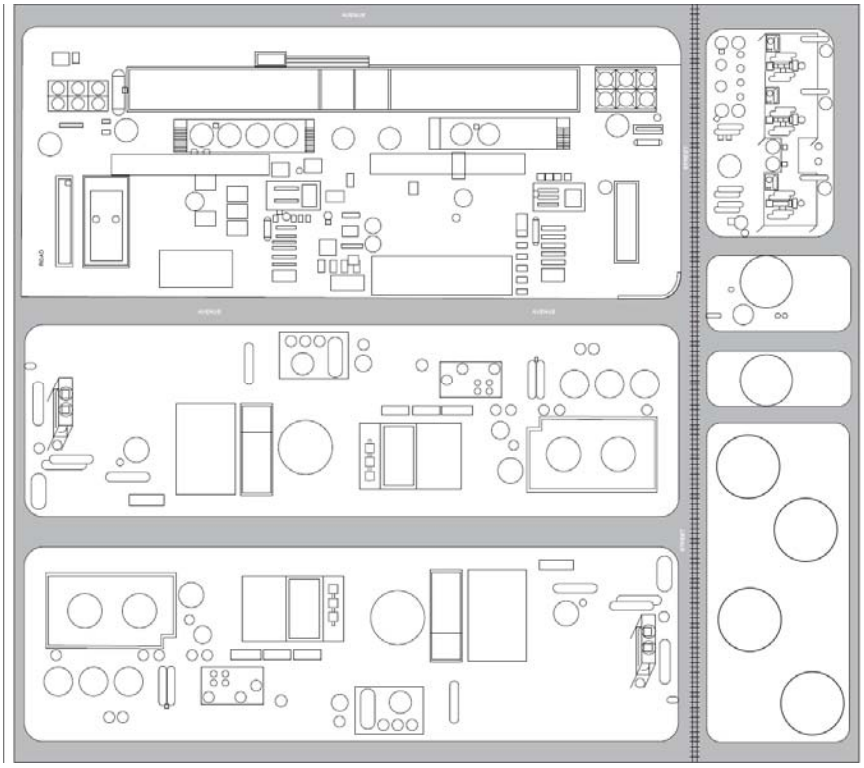


Figure 8. Example Process Facility

If the process facility is not an outdoor production environment, there is still a natural organization that should be used for scoping networks. For example, power plants and biopharmaceutical manufacturing facilities are typically completely enclosed with multiple floors. One option is to scope *Wireless*HART field networks to a floor. If there are 7 floors, then there are several *Wireless*HART networks.

The benefits of scoping a *Wireless*HART field network to a process unit are:

- Aligns the data flow from the *Wireless*HART device through the gateway to the Host System with existing data architecture.
- Aligns *Wireless*HART tagging convention with wired HART tagging convention.
- Aligns *Wireless*HART documentation practices with the process unit and support device location. If you know device A is on Network A and in process unit A, then one should not look in process unit B.

- Aligns work processes of managing *Wireless*HART device lifecycles with wired HART life cycles including organizational responsibilities.

- Sets reasonable expectations for range between *Wireless*HART devices. Most process units are not more than a few hundred feet (<0.5km) by a few hundred feet (<0.5km).

While scoping, the design engineer should factor in considerations for spare capacity. At a minimum, each process unit should have its own gateway with spare capacity for problem solving in real time. If a project is small and application focused, then typically a single gateway is required if the total number of points is less than the capacity of the gateway. If the project is large with several hundred wireless points, below is the process of determining the total number of gateways and modifying the scope of a network.

1. Filter the points by process unit and determine how many points are in each process unit so that the *Wireless*HART networks can be segmented by process unit. For example, out of 700 points, let's assume process unit A has 154 wireless points requiring 154 *Wireless*HART devices. We need to determine how many gateways are necessary to support. Note that some *Wireless*HART devices support more than 1 wireless point and so there may be instances when fewer devices are required to satisfy the number of measurement points. A key example is *Wireless*HART temperature transmitters where 2 or more temperature elements are used as inputs.

2. Determine the capacity of the gateway for the maximum update rate to be used in the network. Be conservative and assume all devices are operating at the same update rate. Example output: 100 *Wireless*HART device per gateway.

3. Determine and apply any guidelines on spare capacity. If the design rules for the project state I/O components should have 40% spare capacity, then note this value for the following calculation.

4. Use the following calculation to determine the number of gateways needed:

$$\frac{\qquad\qquad}{\qquad\qquad} = 3$$

For the example above, three gateways are needed.

This formula can be entered into Microsoft Excel.

5. Scope the number of required gateways into subsections of the process unit. If more than one gateway is needed per process unit, then the design engineer should segment the networks such that the gateways are distributed in the field like marshalling panels and junction boxes. In Figure 9, the master drawing, the process unit has 16 subsections labeled L-2 through L-17 that should be logically segmented for coverage by gateways. Not every gateway needs to have the same number of wireless points. If redundant gateways are to be used, then double the number of gateways based on the output from the above formula.

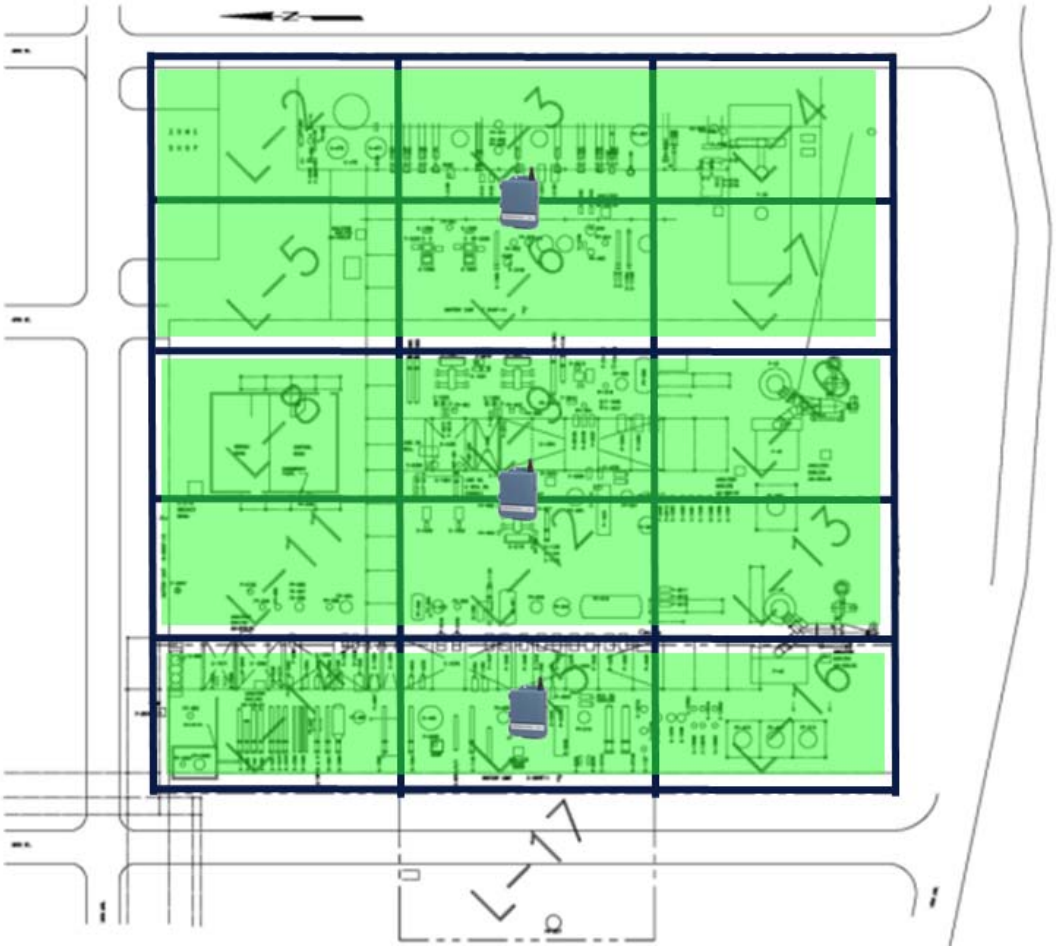


Figure 9. Example Process With Three *Wireless*Hart Networks

This example shows three *Wireless*HART gateways supporting three *Wireless*HART networks in the same process. This is analogous to having three FOUNDATION Fieldbus segments in the same process unit. In this example, the process unit subsections were grouped horizontally instead of vertically to minimize the distance of the process unit. A key consideration is that the gateways, regardless of manufacturer should always be in the process space for which they supply I/O capacity. Below is an image of what not to do:

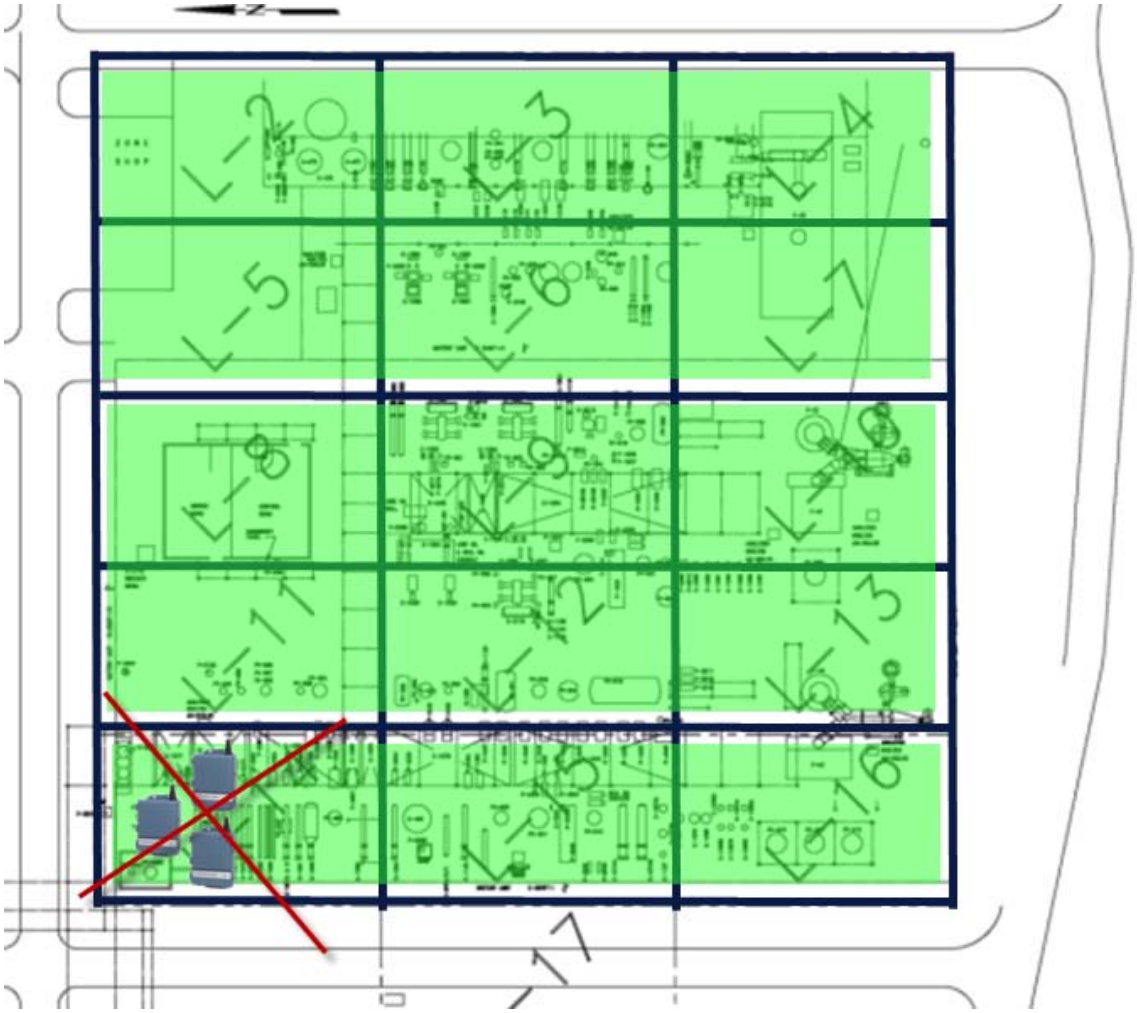


Figure 10. Example Process With Poor Gateway Placement

Do not place all gateways in the same location just because connecting into the host system is convenient. The next section on network design will show this is inefficient and can lead to unreliable networks in the long term. The gateway should be placed in the process space and then the network design around.

When this logic is applied, *Wireless*HART devices logically align with existing documentation.

Key things to remember:

- Scoping is the most important design rule. Use it to ensure wireless capacity, long term scalability, high reliability, and alignment of *Wireless*HART devices and management with existing process facility, organization, and work practices.

- Every *Wireless*HART gateway must have a unique Network ID to properly segment the *Wireless*HART field networks. This is especially true when multiple gateways exist in the same process unit.

- The output from the scoping phase should be a scaled drawing showing the relative locations of assets and process to be automated and potential integration points for the *Wireless*HART gateways.

Designing

The following design rules are intended to be very conservative and are based on real-world deployments of the *Wireless*HART field networks. The effective range of a device is the typical linear distance between *Wireless*HART field devices when in the presence of process infrastructure. Typically, if *Wireless*HART devices have no obstruction between them, have clear line of sight (LOS), and are mounted 6 feet (2 meters) above the ground, then the effective range is 750+ feet (+230m) between two devices. Since the network is a self-organizing mesh, two hops, or communication which gets repeated from 1 device, through another, to get to the gateway, will see an effective range of 1500 feet (462m). Obstructions decrease the effective range. Most process environments have high concentrations of metal that reflect RF signals in a non-predictable manner. The path of an RF signal could easily be 750 feet (230m) even though the neighboring device is only 100 feet (31m) away. Below are three basic classifications for effective range:

- **Heavy Obstruction** – 100 ft. (30 m). This is the typical heavy density plant environment. Cannot drive a truck or equipment through.

- **Medium Obstruction** – 250 ft (76 m). This is the less light process areas, lots of space between equipment and infrastructure.

- **Light Obstruction** – 500 ft (152 m). Typical of tank farms. Despite tanks being big obstructions themselves, lots of space between and above makes for good RF propagation.

- **Line of Sight** – 750 ft (230 m). No obstructions between WirelessHART devices and devices mounted a minimum of 6 feet (2 meter) above ground or obstructions.

These values are practical guidelines and are subject to change in different types of process environments. Conditions that significantly reduce effective range are listed below:

- Mounting field devices close to the ground, below ground, or under water. The RF signal is absorbed and does not propagate.
- Inside or outside of a building relative to the main network. RF signals of any sort do not propagate well through concrete, wood, etc. Typically, if there are wireless devices nearby on the other side of the enclosure, no special design rules are needed. If there is a high volume of *Wireless*HART devices isolated by the network, consider scoping a network inside of the facility. Small, fiberglass instrument and device enclosures often deployed in very dirty or harsh environments show minimal impact on propagation of RF signal and can be used. Large Hoffman-style metal enclosures will prevent RF signals and are not recommended without additional engineering considerations.

The effective range will be used to test the validity of network design.

There are 3 fundamental, recommended design rules.

1. **Rule of 5 minimum** – Every *Wireless*HART network should have a minimum of 5 *Wireless*HART devices within effective range of the gateway. Networks will work properly with less than 5 *WirelessHART* devices but will not benefit from the intrinsic redundancy of a self-organizing mesh network and may require repeaters. In a well formed, well designed network, new *Wireless*HART devices can be added to the interior or perimeter of the network without affecting operation or extensive consideration for design.

2. **Rule of 3** – Every *Wireless*HART device should have a minimum of 3 neighbors with in effective range. This ensures when implemented, there will be at least 2 connections and the potential for connection to change with time.

   Figure 11 is a simple design example. The network has been properly scoped to a process unit and 4 *Wireless*HART devices have been placed with a gateway on a scaled process drawing. The red circle around the gateway represents the effective range of the

gateway. We see in this example, the Rule of 5 Minimum is broken in that there are only 4 devices within effective range of the gateway. This network will likely perform to specification, but it is optimal to fortify for long term scalability and reliability by adding more devices.

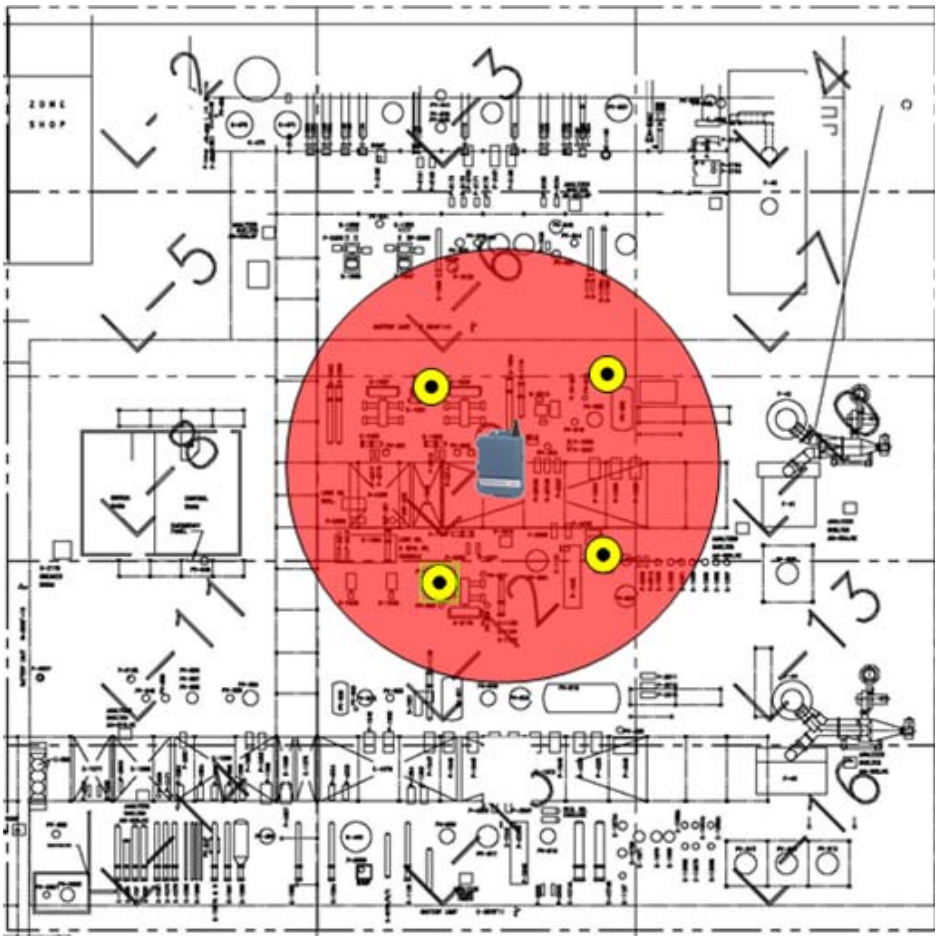


Figure 11. Example Process With Rule of 5 Broken

3. **Rule of 25%** - Every *Wireless*HART network with greater than 5 devices should have a minimum of 25% of devices within effective range of the gateway to ensure proper bandwidth and eliminate pinch points. *Wireless*HART networks can work with as little as 10%, and actual implementation may yield less than 25%, but experience shows this is a practical number. Example, a 100 device network requires 25 within effective range of the gateway.

*Wireless*HART devices are located according to their process connection. Only an approximate location is required for location on the scaled drawing since the self-organizing mesh technology will adapt to

conditions as they exist and change from the point of installation. The design rules ensure a concentration of *Wireless*HART devices for ample paths between the devices. This allows the self-organizing mesh to optimize networking in a dynamic environment.

Continuing on from the previous example, we fortified the network by adding another field device within the effective range of the gateway and added another device as another measurement point. Now the red circle represents the effective range of the *Wireless*HART device that does not have 3 neighbors. For reliability, it is essential for every *Wireless*HART to have 2 paths during operation to ensure a path of redundancy and diversity. The Rule of 3 when designing ensures concentration of devices.

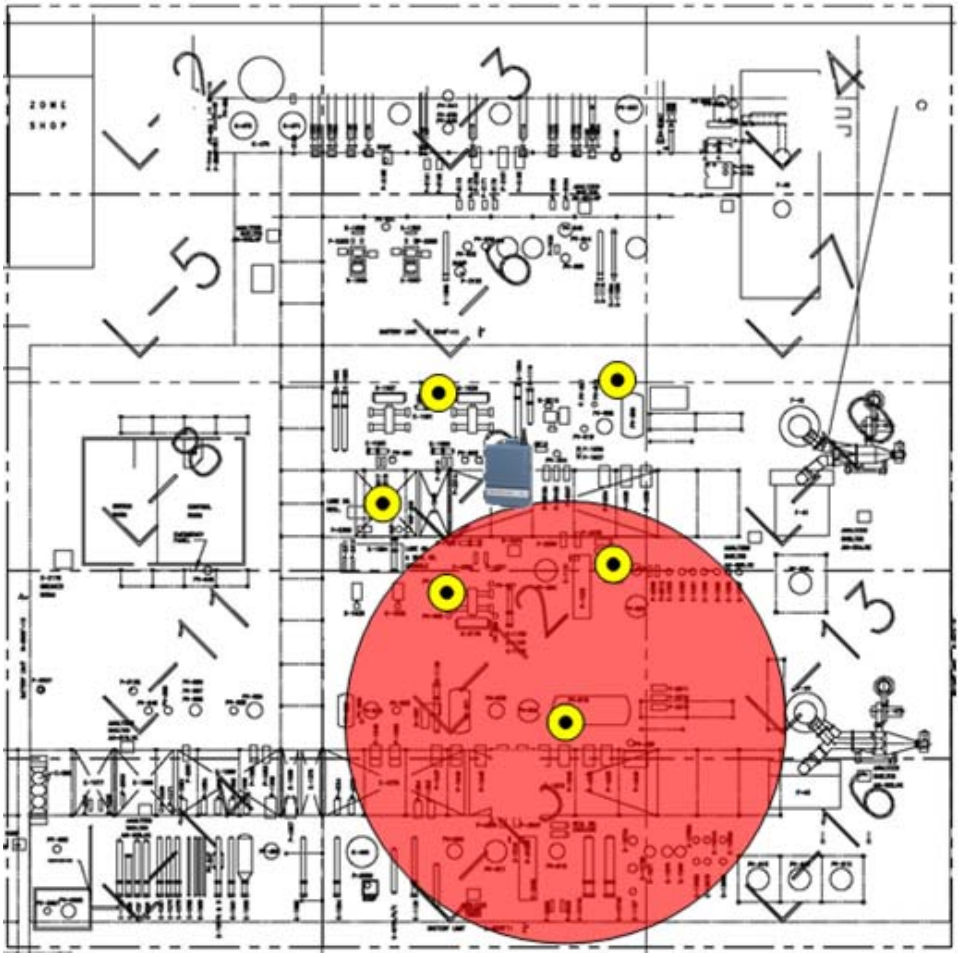


Figure 12. Example Process With Rule of 3 Broken

When the Rule of 3 is broken, it too can be fortified by adding more devices. As networks grow, Rule of 5 minimum and Rule of 3 become

irrelevant as there are many devices in the process space. Rule of 25% becomes dominant for large networks to ensure there is ample bandwidth for all devices in the network. Below is an example of when Rule of 25% is broken.

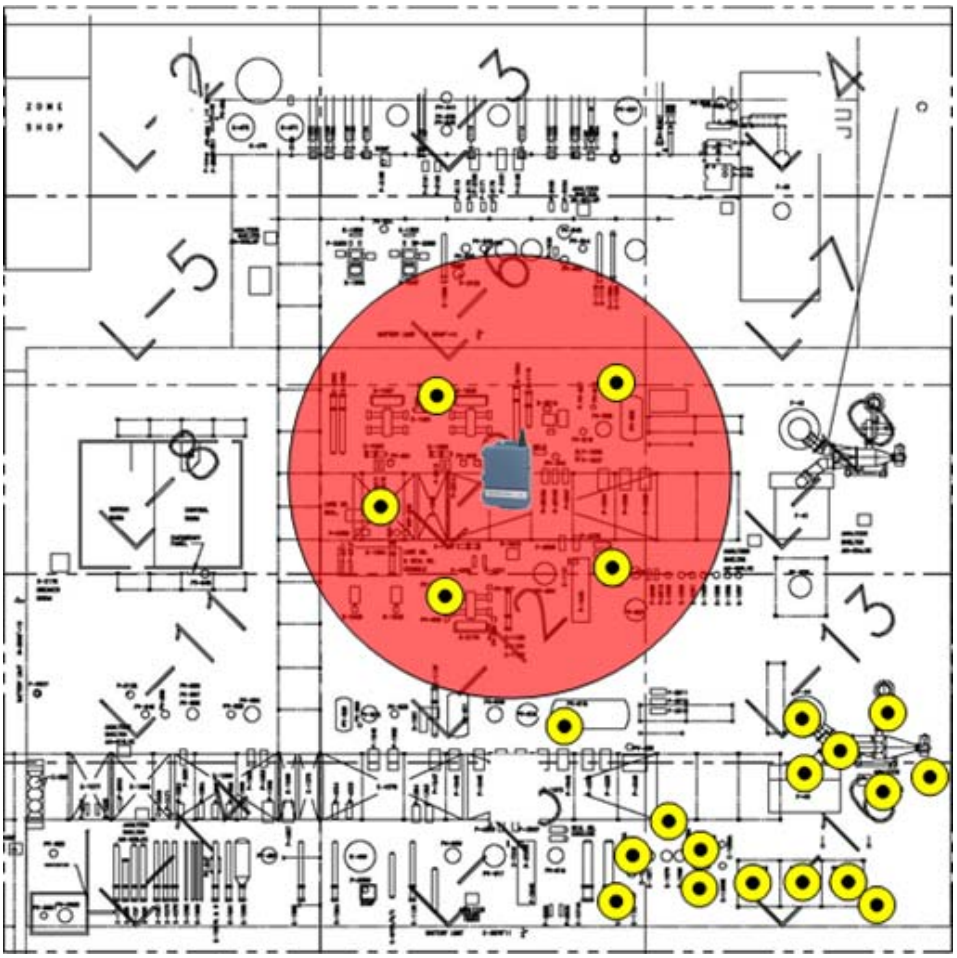


Figure 13. Example Process With Rule of 25% Broken

Rule of 25% can be resolved in several different ways. Below are three options to fortify this network design, each with its own consideration:

1. Add more devices within the effective range of the gateway. While this is a good solution, there may not be more points of value within effective range of the gateway.

2. Move the gateway into a more central location relative to the distribution of *Wireless*HART instrumentation. In this case, there may not be a convenient host system integration point at the center of the network.

3. Add another gateway. This increases overall capacity for the process unit, addresses the needs of that specific concentration of field devices, and ensures long-term, trouble-free scalability. There may still be the issue with convenient host system integration point as with option 2.

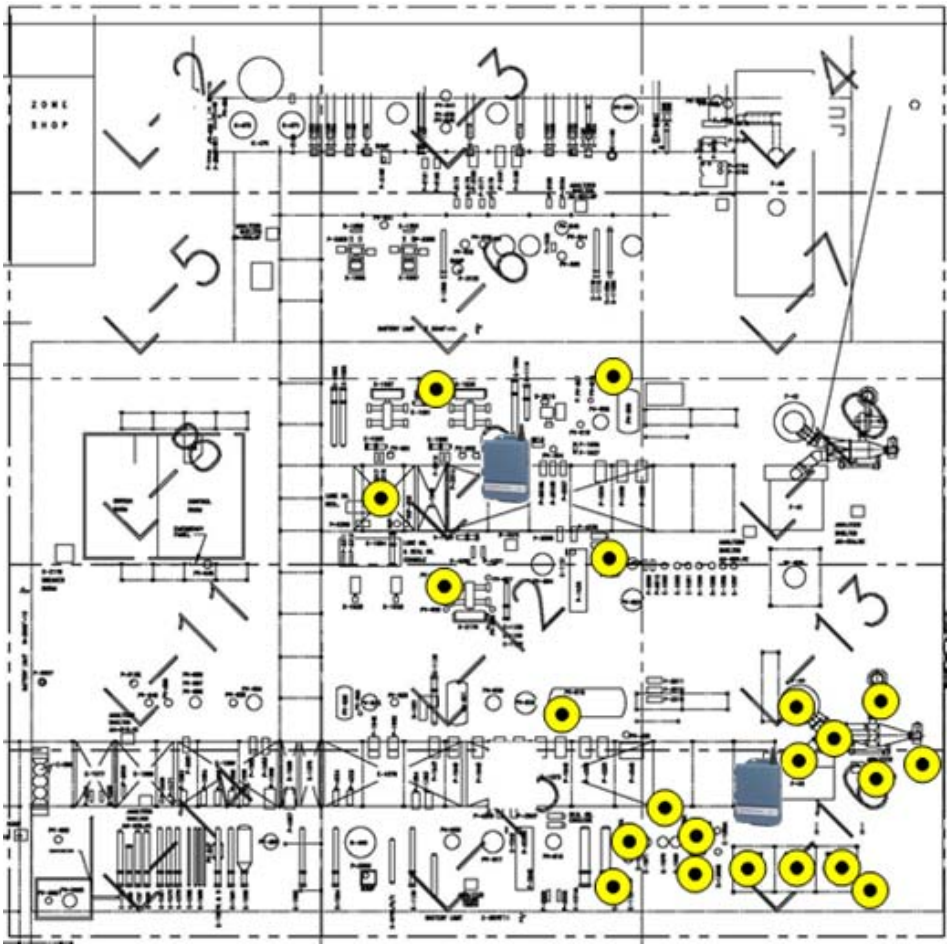


Figure 14. Example Process With Two Gateways

Spare Capacity and Expansion

During a typical project there is often a requirement to provide installed spare hardware (marshalling, I/O cards, terminations) and additional spare space. Typically these figures could vary between 20-30%. The consideration when designing with wireless is different as no cabinetry marshalling, I/O cards, and terminations are required. Additional gateways can be added to the network to increase capacity.

Fortifying

Stress testing the network design by altering the effective range of device is recommended to identify potential weaknesses in the network. To stress test the network, reduce the effective range of the devices in 10% increments. For example, suppose an effective range of 250 feet (76m) was used for initial design. Reducing effective range by increments of 25 feet (8m) (10%) will reveal where the weak spots will exist. At this point it is the discretion of the network designer to what level the network will be stressed; there is a limit of diminishing return.

The example below reveals that one *Wireless*HART device fails the Rule of 3 under a 20% stress test of the effective range. Effective range is set to 250 feet (76m) for the design test on the left and 200 feet (61m) for the design test on the right.

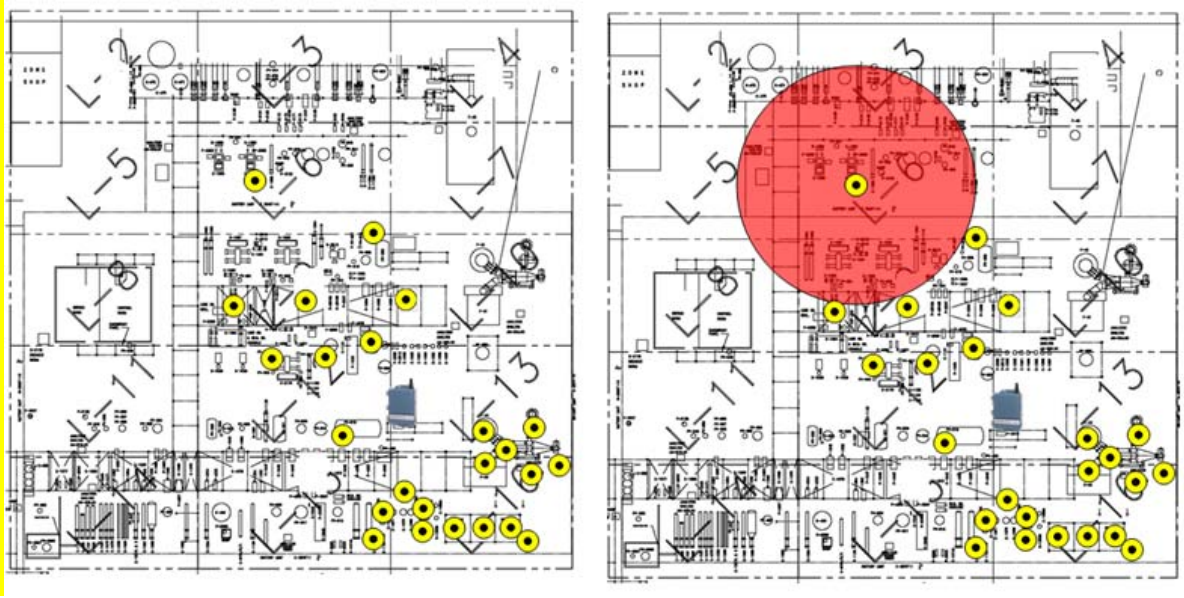


Figure 15. Example Process: Standard Design (Left). Stress-Tested (Right)

The self-organizing mesh technology not only allows for more *Wireless*HART field devices to be added to a network for the purposes of automation, the means for simple design correction also exist. Alternatives include moving the gateway location, adding a new gateway to segment the network, adding more devices or adding repeaters.

Repeaters are also an alternative to support the fortification of a network. Instead of another *Wireless*HART device with a specific measurement purpose, this device is used specifically for the purposes

of providing more connection within the network. Repeaters can be used effectively within dense infrastructure if they are placed above the infrastructure to maximize effective range of devices below. *Wireless*Hart adapters may make cost-effective repeaters if local power is available.

*Wireless*HART Availability and Redundancy

The *Wireless*HART field network is inherently redundant between the wireless field devices and the gateway if the network design recommendations are applied. The user should expect no less than 99% reliability in the flow of data from each *Wireless*HART field device with typical performance approaching 100%.

The following are considerations for maximizing system availability between the host system and the *Wireless*HART Gateway:

1. Apply all field network design recommendation to ensure the field network has inherent redundancy of paths.
2. Always properly ground gateways and field devices per manufacturer recommendations.
3. Always employ proper lightning protection on gateways.
4. Always use an uninterruptible power supply (UPS) to power the gateway. This is the primary source of gateway failure.
5. Deploy redundant gateways for the field network if measurements are critical.
6. Make host systems connections to gateways redundant, especially if redundant gateways are used. This includes physical connections, switches and power supplies.

*Wireless*HART Security

When designing networks, every gateway and every network must have a unique Network ID. Device Join Keys may be configured as either common or individual/unique. If common Device Join Keys are selected as the option, each field device will share the same Device Join Key. If individual Device Join Keys are selected, each field device in the network will have a unique Device Join Key.

Individual Device Join Keys provide stronger security and are recommended.

Network Design for Control

The fundamental concepts of the design rules will not change for control and current recommendations are used for supervisory control. The comments below highlight potential adjustments to fundamental network design that need to be verified in the field through testing to understand and document heuristics unique to designing networks for control where scan rates exceed four seconds and tight tolerances are required for latency.

1. **Rule of Scope** – Ensure all *Wireless*HART measurements forming part of a control loop are hosted on the same gateway/network.

2. **Rule of 5 Maximum** – Minimize the number of hops to the Gateway in order to reduce latency.

3. **Rule of 3** – Possible modifications include increasing the required number of neighbors to four or five to increase the number of potential paths and thus better opportunities for optimizing network performance.

4. **Rule of 25%** - Possible modifications include increasing the percentage of devices within effective range of the gateway to 35%+. This cluster more devices around the gateway and ensure fewer hops and more bandwidth available to *Wireless*HART devices with fast scan rates.

5. **Rule of 1** – New rule. This would ensure key *Wireless*HART devices driving actuators are within effective rage of the gateway to ensure typical hop depth is 1 -2 hops. In this way the advantages of path redundancy and very short transit times can be achieved.

Section 8 Host System Requirements

Use of Standard Protocols

Standard protocols should be used to ensure most cost effective installation. The *Wireless*HART gateway should convert data from the *Wireless*HART field network into the desired protocol and physical layer needed for integration.

Wireless Host System

Data from *Wireless*HART field networks can be integrated into any existing host system. However many wireless automation applications are not for control or process monitoring and may not be required to be accessed by the DCS or PLC system. This information may be useful to non-control room based personnel including reliability engineers, maintenance personnel, and energy engineers. Careful consideration should be observed for determining which information should be place on control operations screens to prevent the dilution of critical information.

For example, suppose a wireless field network is used to replace a manual inspection round where a maintenance technician would manually collect temperature and vibration data from a series of pumps and then manually enter the collected data into a historian for future access. With *Wireless*HART, the gateway can be integrated into the application, in this case a historian, for the automated collection of data.

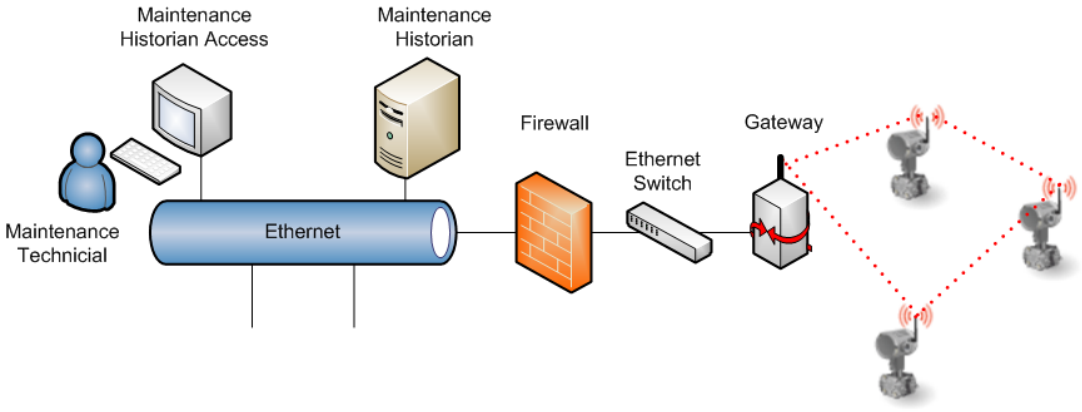


Figure 16. Gateway Integration Into Host System

For *Wireless*HART networks that support users in different roles, the potential exists for each end user to have their own application for

collecting and analyzing data. For users who manually collect data, *Wireless*HART provides the missing piece to their automation.

For long term scalability, where there may be 1000's to 10,000's of *Wireless*HART instruments in a single plant. It will be important to have a coordinated effort to enable end users with different roles and responsibilities to share the I/O capacity of gateways. There is no reason why representatives from maintenance, utilities, operations, health/safety/environmental, and asset management cannot share network resources.

One architecture to consider is a centralized historian and centralized asset management program shown below. In this scenario, multiple gateways are connected on the same Ethernet network and server. Their data to a centralized historian can then be connected to the applications for each of the end users. In this way, host system resources can be shared, all *Wireless*HART instruments can report to the same asset management solution, uniform security policies can be supplied, and end users can see *Wireless*HART data in applications specific to their roles.

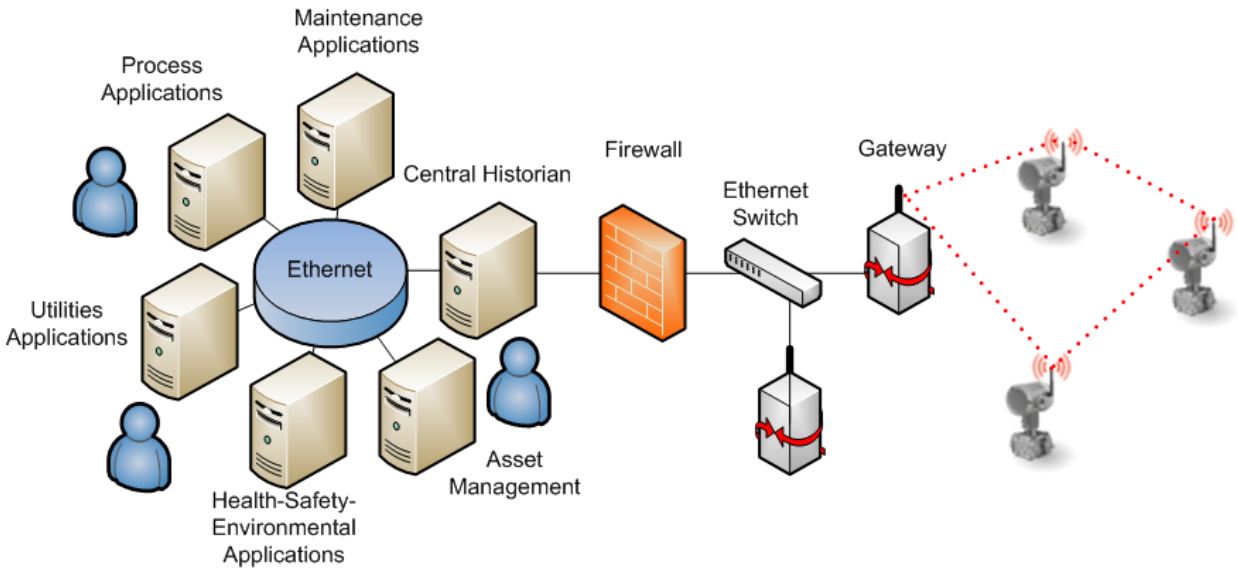


Figure 17. Gateway Information Integrated Into Many Applications

Developing a host system strategy is essential to maximizing return on investment for wireless that is adopted on a large scale. Successful implementation means that data is going to the right people and being turned into information for action. Often times, multiple users will see the same data, but in the context of their applications. This also means

that every time a new *Wireless*HART device is introduced to the plant, host system and integration issues do not need to be solved again and again.

*Wireless*HART is truly scalable; *Wireless*HART devices can be added to a network without disrupting operation and more gateways can be added to increase I/O capacity. This ability allows automation to be added, solving problems without large project budgets once wireless network infrastructure is in place. For example, a *Wireless*HART device can be connected in minutes, configured in minutes, and integrated in minutes if a host system strategy is in place.

Host Integration

Integration of data originating from the wireless gateway into a host control system is normally performed in one of two ways - through native connectivity directly to the host system or using standard protocols such as Modbus or OPC.

For native connectivity including vendor specific I/O cards, contact the host vendor.

OPC and Modbus are non-proprietary protocols and use standard data exchange and integration techniques to map data from the gateway into the host control system. Typical data that is mapped to the host are process variables (PV, SV, TV, QV) and overall device status. Diagnostic information is typically passed to an asset management system via ethernet. Check with the gateway vendor for compatible asset management packages.

Often, existing host systems can be a combination of legacy DCS and PLC components and modern data management solutions such as historians. *Wireless*HART gateways should support multiple connections into multiple host systems over multiple protocols. This enables *Wireless*HART networks to support modernization of an existing host system. For example, suppose the existing DCS has no spare capacity and can only receive the 4-20 mA signal from wired HART devices. A *Wireless*HART network could be serially connected to the DCS to bypass the need for more Analog Input Cards to receive more process variables, while in parallel, HART diagnostics flow to an asset management program from existing wired HART devices with *Wireless*HART adapters. This type of modernization project could enable incremental modernization with an older host system and when the

scheduled turnaround occurs to upgrade the DCS, the existing *Wireless*HART networks would transition to the new host system.

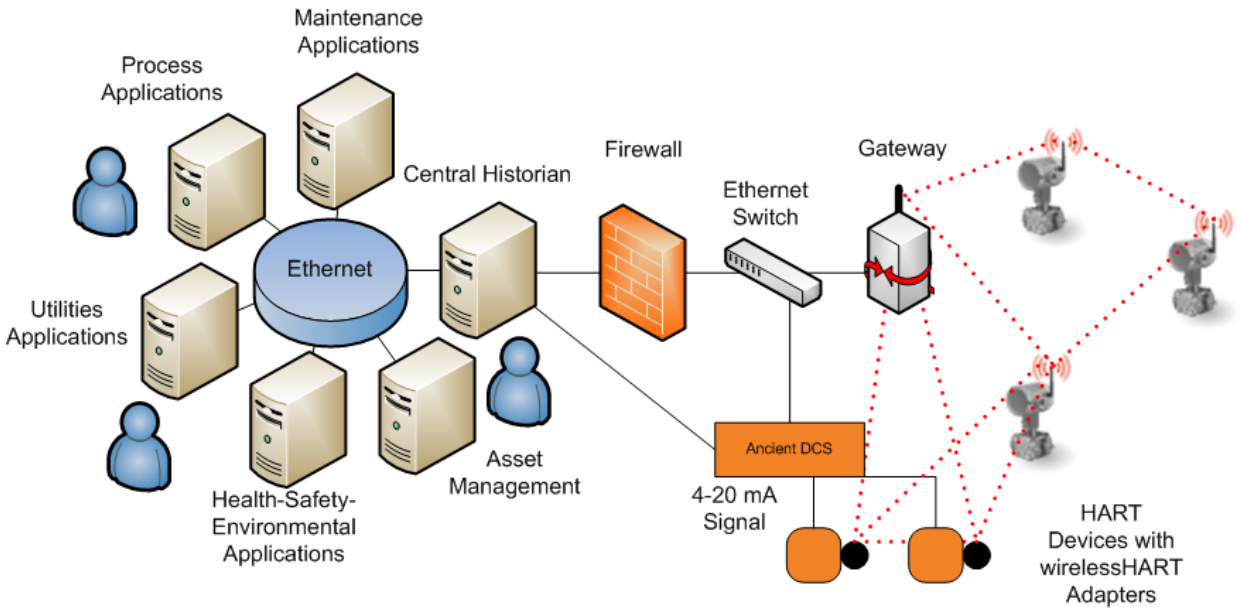


Figure 18. Using WirelessHart Gateway To Bridge Information From Non-Hart Host System

A key output from working with host system administrators is an integration strategy to incorporate a plant-wide wireless infrastructure. If doing a small application, a key output is the physical locations of where to connect the gateways. These will be needed for the network design process.

Key Outputs for Network Design:

- Identifying a host system administrator and system integrator who supports integration of *Wireless*HART data into the host system.
- Potential physical connection points for *Wireless*HART gateways.

Interoperability

Converting *Wireless*HART data from the gateway into standard protocols including Modbus and OPC, ensures interoperability of all *Wireless*HART networks with all host systems. Host systems based on proprietary protocols may have difficulty.

Host System Support for *Wireless*HART Functionality

The *Wireless*HART gateway performs all management of the *Wireless*HART network and manages communications to and from the *Wireless*HART field devices. The host system requires no special software to support the *Wireless*HART field network.

Configuration Tools

*Wireless*HART devices are based on HART. Therefore, existing HART Field Communicators will work for configuration of the field devices. Field Communicators will require the proper device descriptor for configuration, which is no different for any other new HART device, wired or wireless. Host system configuration will be dependent on the host system. HART vendors with asset management software may extend the benefits of remote management from wired to *Wireless*HART devices via the gateway.

Control System Graphics

Not all data collected from the *Wireless*HART field network belongs on the operator screen as part of control system graphics. The risk is that non-pertinent information reaches the operator and becomes a distraction from critical information.

The host system integration should be configured such that data from a *Wireless*HART field network is delivered to the proper end-user even though network resources are shared. To give some examples:

- Data collected on consumption of power from rotating equipment should go to the utilities manager.
- Data collected on vibration spectrums of rotating equipment should go to asset management.
- Data collected on temperature alarms for rotating equipment should go to operators in a non-obtrusive way and the reliability manager.

Properly defining an integration strategy will ensure an efficient collection of data from *Wireless*HART network and dissemination to proper end-users. Many end users not typically receptive of the benefits of automation have application specific databases into which data is manually collected and uploaded. With the ability to integrate *Wireless*HART data on many standard protocols, these existing end-user specific databases can be automatically populated.

Node Addressing and Naming Conventions

A *Wireless*HART device should follow naming conventions of wired HART devices.

Alarms and Alerts

Alarms and alerts should be directed to the appropriate end-user and their associated application and software. Alarm and alert dissemination should be reflective of the end user and their responsibility.

Maintenance Station

*Wireless*HART devices provide internal diagnostics and process and device like any wired HART device. Additional local diagnostics for network connectivity are accessible locally via a HART Field Communicator with the correct Device Descriptor for the *Wireless*HART field device.

The *Wireless*HART gateway will also provide additional diagnostics for network performance. The data from *Wireless*HART devices will not propagate to the host system if the data is deemed questionable from either a HART diagnostic or an extended delay in reception at the gateway from the *Wireless*HART field device. Additionally, the gateway is responsible for *Wireless*HART network management and network diagnostics.

Diagnostics between the gateway and the host system will depend on the host system and the gateway.

Historian

Historic Data collection can be treated the same as any conventional source (e.g. OSIsoft PI or any DCS historian package).

Section 9 Factory Acceptance Testing Requirements

Introduction

The key deliverable of a factory acceptance test (FAT) is the integration of data from *Wireless*HART instruments into the host system via the gateway. The scope of the FAT should be agreed with the end user. Typically only a subset of the field devices and gateways to be installed is used during the FAT.

Factory Staging

The following are basic requirements for factory staging:

- A sample of all applications, gateways and *Wireless*HART devices is present.
- Approved test plan, test procedure and test acceptance criteria.
- HART Field Communicator and user interface to the *Wireless*HART Gateway.

Assumptions

Below are assumptions for the FAT:

- Network topology testing is covered as part of the Site Acceptance Test.
- *Wireless*HART network design does not need to be tested at the factory if network design recommendations are implemented. The conservative nature and ability to fortify the network upon installation with repeaters ensure high confidence of reliable operation.

Factory Acceptance Test (FAT) Requirements

The following are key requirements of a factory acceptance test:

- Physical connection between the gateway and the host system is verified. Can the gateway be accessed from the host system?
- Protocol connection between the gateway and the application that resides on the host system is verified. Can the data seen in the gateway be seen in the application? Can the standard parameters be properly mapped?

- Gateway can support all necessary connections to all required applications.
- Device Descriptor (DD) for all field devices in any asset management solution is tested. This ensures the correct DD is installed and valid. Especially important for *Wireless*HART devices that are new to the market.

FAT Procedure

Since there are no physical IO modules, software testing is performed by simulation of I/O at the processor level. This level of simulation is adequate to verify the application software within the host control system.

As per IEC 62381 standards on factory acceptance testing, general guidance as described for testing of bus interfaces and subsystems shall apply. A subset of instruments (at least one of each type) shall be connected to the gateway as a proof of concept demonstration of integrated system functionality. This test should ideally verify the connectivity of the field device to the gateway and from the gateway to the host system.

Where physical devices will not be tested at the factory, emulation of the interface will be performed if required

Below is a high level procedure for performing a FAT:

1. Power the gateway
2. Add one of each type of *Wireless*HART device to the network and verify proper connectivity. All gateway fields for data from the WirelessHART device should be properly populated.
3. Change Network ID and Join Key of the network and verify all field devices joined to ensure proper network and security management of the network.
4. Create first physical connection to the first required host system application.
5. Verify connectivity between the gateway and the host system application.
6. Integrate necessary data from each sample WirelessHART device into the Host System Application.

a. Optional additional procedure is to change process variables in the *Wireless*HART device through direct stimulation or through simulation. All devices, once properly connected to the gateway, should integrate identically over protocols like Modbus and OPC.

7. Repeat steps 4-6 while adding host system connections to the gateway until all expected connections the gateway are complete.

8. Test integration into an asset management solution if applicable.

    a. Verify each *Wireless*HART device can be properly accessed and configured via the asset management solution.

9. Add any additional procedures for verify control narratives and monitoring narratives.

Section 10 Site Installation Guidelines

Installation follows very closely the installation practices of wired HART instruments. Since there are no wires, *Wireless*HART devices can be installed as soon as the asset or infrastructure is in place and secure.

Network Installations

Always install the gateway first so that integration and field network installation and commissioning can occur in parallel.

Field devices can be commissioned into the gateway and then commissioned into the host system application.

In general, *Wireless*HART devices are installed per the practices of wired HART devices. Always consult the product manual.

*Wireless*HART devices close to the gateway should always be installed and commissioned first to ensure connections for potential devices that cannot directly connect to the gateway. This is the easiest way to establish the self-organizing mesh.

*Wireless*HART devices can be installed in close proximity to each other without causing interference. The self-organizing mesh scheduling of *Wireless*HART ensures devices in close proximity to each other are silent, talking to each other, or talking on different RF channels when other devices are communicating.

If a *Wireless*HART gateway antenna or *Wireless*HART device antenna is to be mounted near a high power antenna of another wireless source, then the antenna should be mounted at least 3 feet (approximately 1 meter) above or below to minimize potential interference.

Lightning Protection

The installation manuals of all *Wireless*HART devices should be consulted prior to installation.

In general, *Wireless*HART devices should not be the tallest feature in the plant to maximize protection against lightning.

Ensure adequate protection is provided between the *Wireless*HART gateways and host system connection as a lightning strike could damage more than just the *Wireless*HART gateway. Redundant gateways should

never be co-located to provide diversity of location in the event a single *Wireless*HART gateway is struck by lightning.

In general, integrated wireless devices may provide better protection of the system than wired, as the energy from a lightning strike will not be able to travel through the wiring and cause potential damage to other components.

Standards such as NFPA 780 provide classification for zones of protection from lightning as well as techniques for proper implementation.

Wireless Connection Test Procedure

Before beginning the wireless connection test procedure, verify the *Wireless*HART device has basic connectivity to the network either through the gateway interface, a local user interface on the device, or a local connection via a HART Field Communicator. If the device is not joining the network, verify the presence of power and the implementation of proper Network ID and Join Key. This assumes the gateway is installed properly, powered and accessible, that the network is designed per best practices, and that there are devices to which the new device being commissioned can connect.

1. Wait a minimum of at least 1 hour from initial powering of the *Wireless*HART device before performing the wireless connection test procedure. This dwell time ensures the device has had time to make several connections for self-organization. Multiple devices can be tested at the same time, and since they rely on each other, it is optimal to have as many on the network as possible for initial connection testing.

2. Verify that network diagnostics indicate the device has proper bandwidth. The gateway should have an indication.

3. Verify each device has a minimum of two neighbors. The gateway should have an indication.

4. Verify device reliability is 99% or greater. Statistics may need to be reset and recertified to remove any anomalies incurred during start up and not indicative of long term performance.

5. Verify sensor configuration per the loop sheet or other form indicating designed configuration.

6. Perform any necessary zero trims for sensors.
7. Repeat for each device in the network.

If a device does not pass the wireless connection test, then follow these basic steps:

1. Wait until entire network is built and operating for 24 hours before considering further action. This will give the gateway time to maximize its self-organization for best communication.
2. For the non-compliant device, verify proper path stability and RSSI values. Path stabilities should be greater than 60% and RSSI should be greater than -75 dBm.
3. Look at the location of the non-compliant device in the network. Verify there is not a broken network design rule or an unexpected installation resulting in poor RF signal propagation.
    a. Add repeaters if necessary to fortify the network if the device is isolated from the network with bad connections.
4. Verify the device has proper power and is working properly as a sensor.
5. Verify the device scan rate is not faster than the fastest allowed by the gateway.
    a. Either reduce the scan rate of the field device or increase the fastest allowed scan rate on the gateway.

Network Checkout Procedure

Below are basic steps for checking out a network:

1. Verify that all devices connected pass the wireless connectivity test. The gateway should have an indication.
2. Verify a minimum of 15% of devices are directly connected to the gateway. The design parameter is 25%; the minimum acceptable is 10%. The gateway should have an indication.

3. Verify overall network reliability is greater than 99%. The gateway should have an indication.

Loop Checkout/Site Integration Tests

Once *Wireless*HART devices are connected to the gateway and the network is checked out, the loop checkout may not be necessary in the traditional sense.

Wireless connection testing verifies each field device has the proper configuration. Since there are no wires to get confused and swapped, there is no need to do the traditional loop check. Alternative loop checks could be to ensure each field devices is reporting to the correct gateway and each gateway is connected into the correct host system. Traditional applications of sensor stimulus can be performed for confidence, but are less valuable in a pure digital architecture if there is complete assurance a field device was commissioned with the correct tag and configuration.

Bench Simulation Testing

Each *Wireless*HART field device is compliant with the HART 7.0+ protocol which has provisions for simulation. Each device can be put into a simulation mode. Bench simulation testing should also verify that all HART Field Communicators have the proper configuration and device descriptors (DDs) for accessing the local user interface of field device when in the field.

Provision of Spares

Below are the recommended spares to have onsite:

- Spare lightning arrestor components for gateways, if lightning protection is used.
- Spare gateways should be kept according to spares policy for host system equipment (e.g. I/O cards). Configurations for gateways should be convenient for rapid replacement if necessary.
- Spare battery modules
- Spare field devices as determined by the policy for wired field devices. Consideration should be given for additional devices to be used as repeaters if necessary.

Removal of Redundant Equipment

Repeaters used temporarily to fortify a network can be removed and reused if the *Wireless*HART network grows to a point where repeaters are no longer needed.

Maintenance Practices

Maintain each *Wireless*HART device per the manual for the device.

The network will self organize and provide alerts for changes requiring intervention. The gateway should have an indication of performance issues in the network or field devices.

Section 11 Documenting in Intergraph SPI 2009

*Wireless*HART devices can be fully documented in Intergraph SPI with minimal customization. Below is an example of how to document *Wireless*HART in a logical, linear order and assumes the reader is skilled in working with Intergraph SPI. This is just an example to illustrate the methodology. Ultimately it is the responsibility of project management to create and reinforce the application of standards and guidelines within the project environment.

User Defined Fields

The first step is to create user defined fields that allow for the accounting of *Wireless*HART engineering parameters that are necessary for defining if a point is wireless and how that point will be connected to a network.

The following global User Defined Fields should be created:

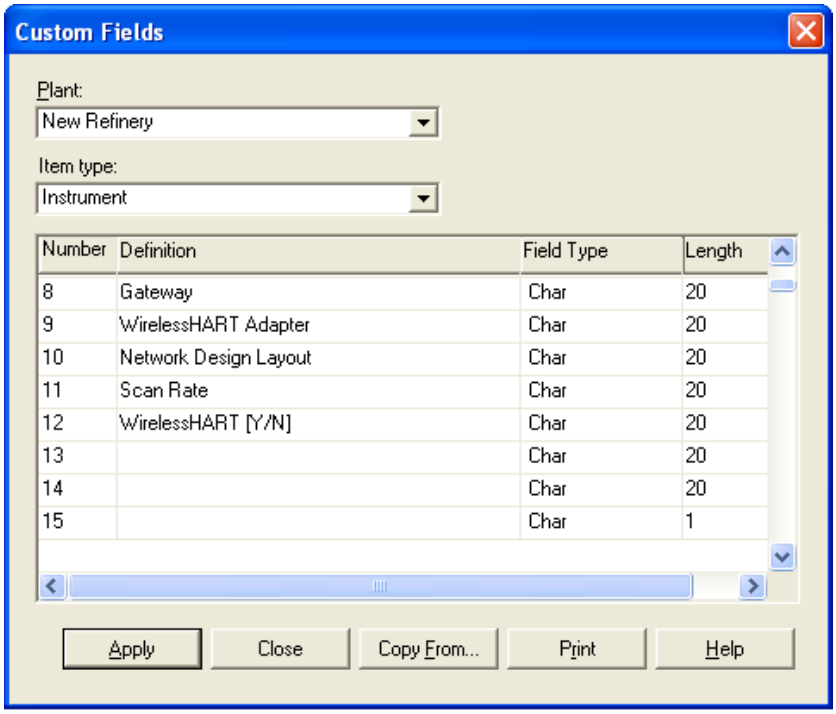


Figure 19. SPI User Defined Fields (UDF) For *Wireless*Hart

Explanation of fields:

User Defined Field (UDF)	**Example**	**Purpose**
WirelessHART (Y/N)	Y	Identify a point as wireless at a high level. Will be used for quickly applying design guidelines to determine what is and what

		is not wireless.
Scan rate	1,2, 4, 8, 16, 32, 64+	*Wireless*HART devices will not all scan at 1 second like wired HART devices. This value will be important for determining what devices may be *Wireless*HART as well as setting configuration parameters.
Gateway	GWY002	Defines which gateway a *Wireless*HART device is to be associated.
WirelessHART adapter	WHA001	Defines which *Wireless*HART adapter a wired HART device is associated with if a device does not have integrated *Wireless*HART capability.
Network Design Layout	A101.DWG	This is a reference field to a drawing or document that was used to validate network design best practices.

Figure 20. Definitions for *Wireless*Hart SPI User Defined Fields

If the user chooses, SPI rules can be created such that these custom fields only appear for points that are HART or checked to be *Wireless*HART. This minimizes exposure to non-pertinent information for non-*Wireless*HART devices.

Filtered Views

A custom view of the Instrument Index will be useful for applying design guidelines for selecting what instruments are to be wireless as well as seeing the organization of networks. Below is a sample view leveraging the User Defined Fields shown in the previous section.

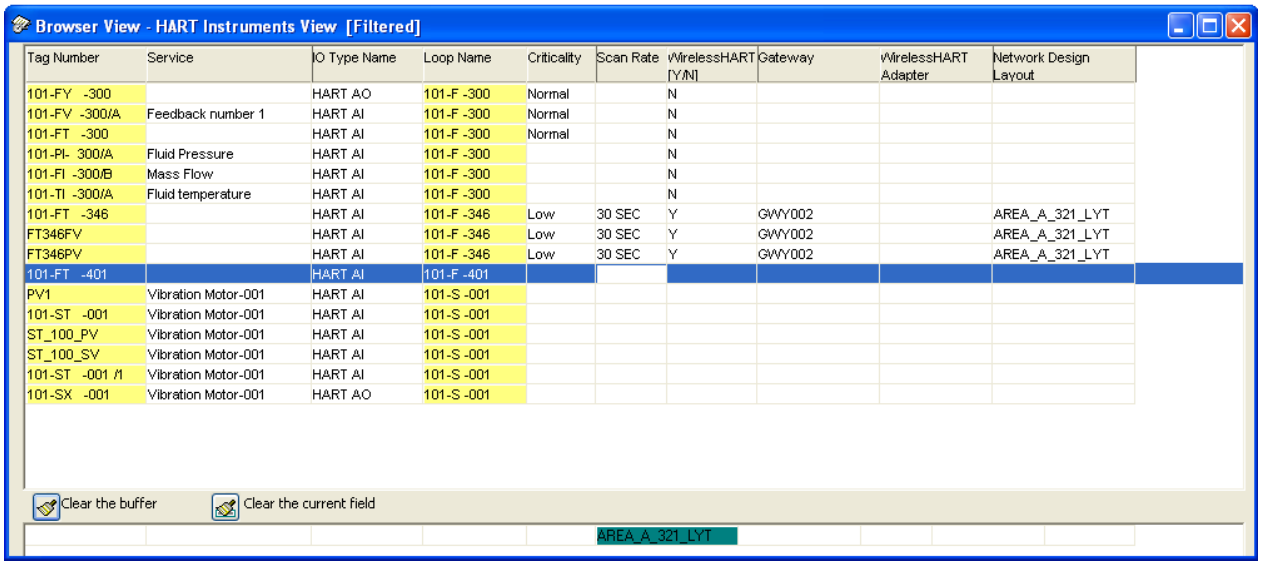


Figure 21. Custom View Of SPI's *Wireless*Hart User Defined Fields

The “Criticality” and “Scan Rate” should be foundations for any engineering guidelines that determine whether a device is *Wireless*HART. Some low criticality loops may have scan rates faster than 4 seconds, and should be included with the design guidelines. Because *Wireless*HART devices primarily run on batteries, WirelessHART may not be suited for all fast scan rate applications.

At a high level, using the “Criticality” and “Scan Rate”, engineers can determine whether a device should be *Wireless*HART. If wireless, the device will need to be associated with a gateway. If a device can only be specified as a wired HART device and requires a *Wireless*HART adapter, then the “*Wireless*Hart Adapter” tag information should be defined.

Every *Wireless*HART field network should be validated against network design best practices. “Network Design Layout” provides a reference field to link to the drawing on which network design best practices were checked.

Creating Instrument Types

Early in the process, symbols and instrument types should be defined and a *Wireless*HART instrument library should be developed. Below the basic modifications to a HART device to create a *Wireless*HART instrument type is illustrated.

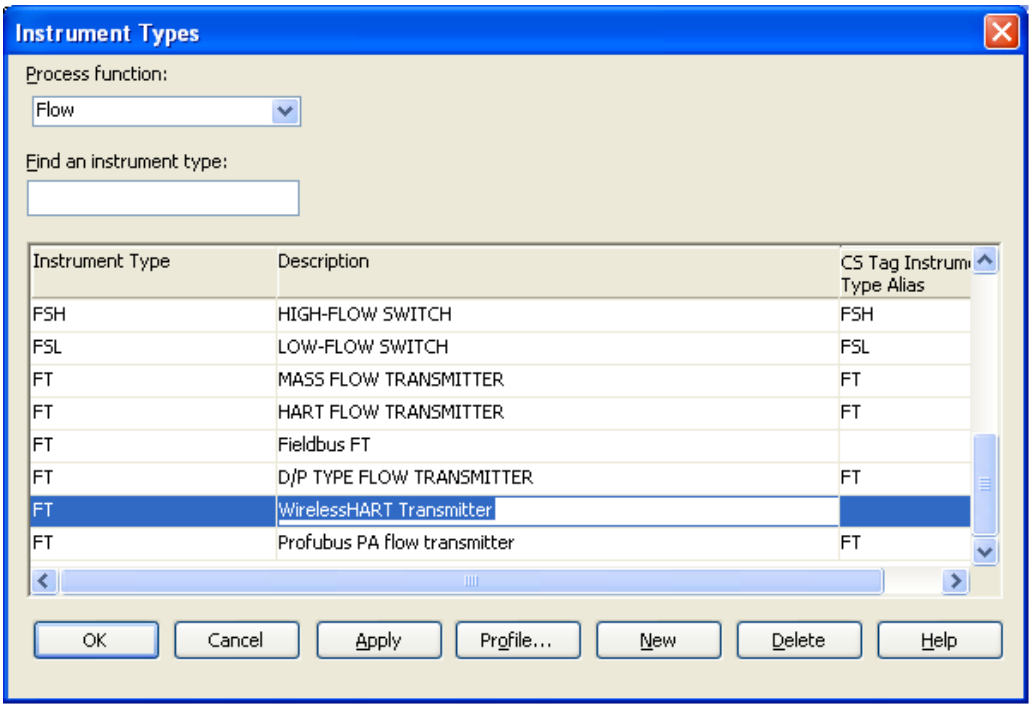


Figure 22. Defining *Wireless*Hart Instrument Type In SPI

The first step is to create a new device with a new description. In this example, we have created a *Wireless*HART flow transmitter. Please note that if the device will be specified as a wired HART device with a *Wireless*HART adapter, no new instrument types are necessary.

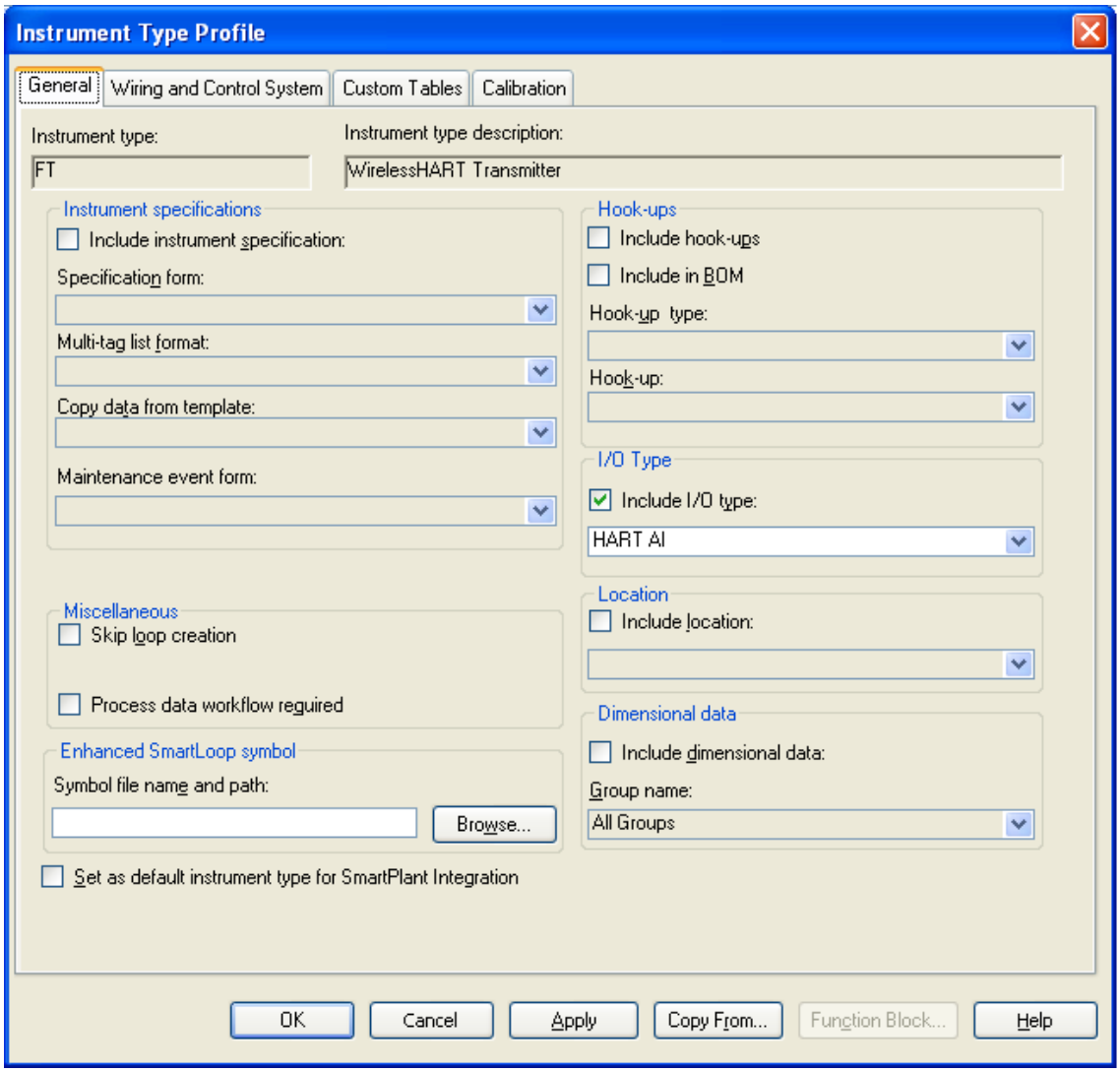


Figure 23. Defining A New *Wireless*Hart Instrument In SPI

Nothing needs to change on the general tab. Be sure to leverage that the device is a HART AI or a HART AO so that all of the basic parameters of HART apply. Manage the wiring, or lack of wiring separately. The fact that *Wireless*HART is based on HART allows leverage these pre-defined variables.

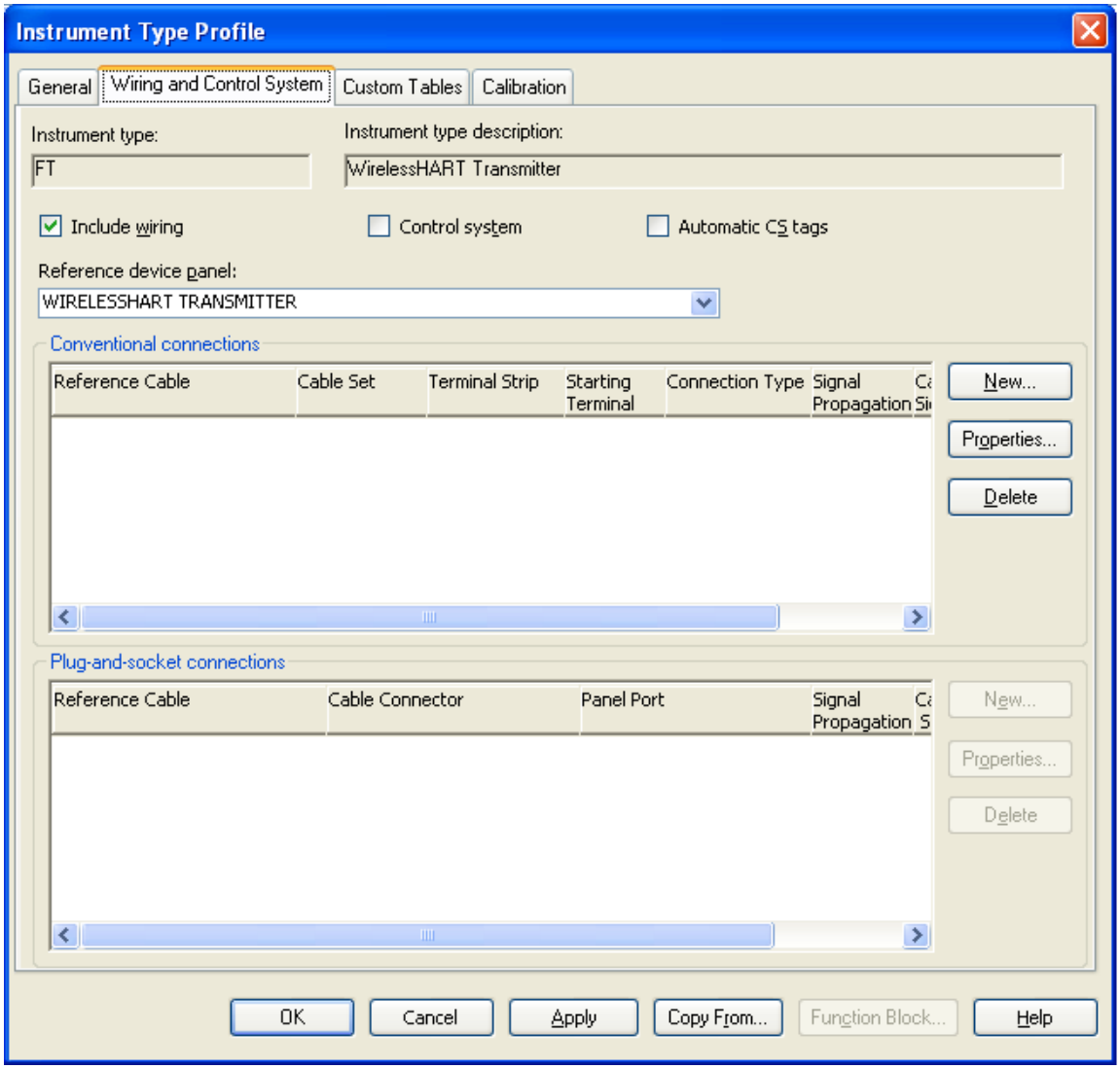


Figure 24. Defining Wiring Types In SPI

Check the box to include the wiring. If this box is not checked when SPI generates loop drawings, the device cannot be added to loop drawings. This also allows for flexibility for different wiring configurations, to be defined elsewhere. Examples include wiring *Wireless*HART adapters in series with the loop and line power for *Wireless*HART devices. This process should be repeated for each unique *Wireless*HART instrument type.

There are only two instrument types that are unique to *Wireless*HART and could be considered ancillary - the *Wireless*HART gateway and the *Wireless*HART adapter. To create these instrument types, it is recommended to use the symbols YG for a *Wireless*HART gateway and YO for a *Wireless*HART adapter.

Once the instrument type is defined, the device panel properties can be modified to include reference symbols. It is recommended to assign symbols for both the Enhanced SmartLoop and the Cable Block Drawing.

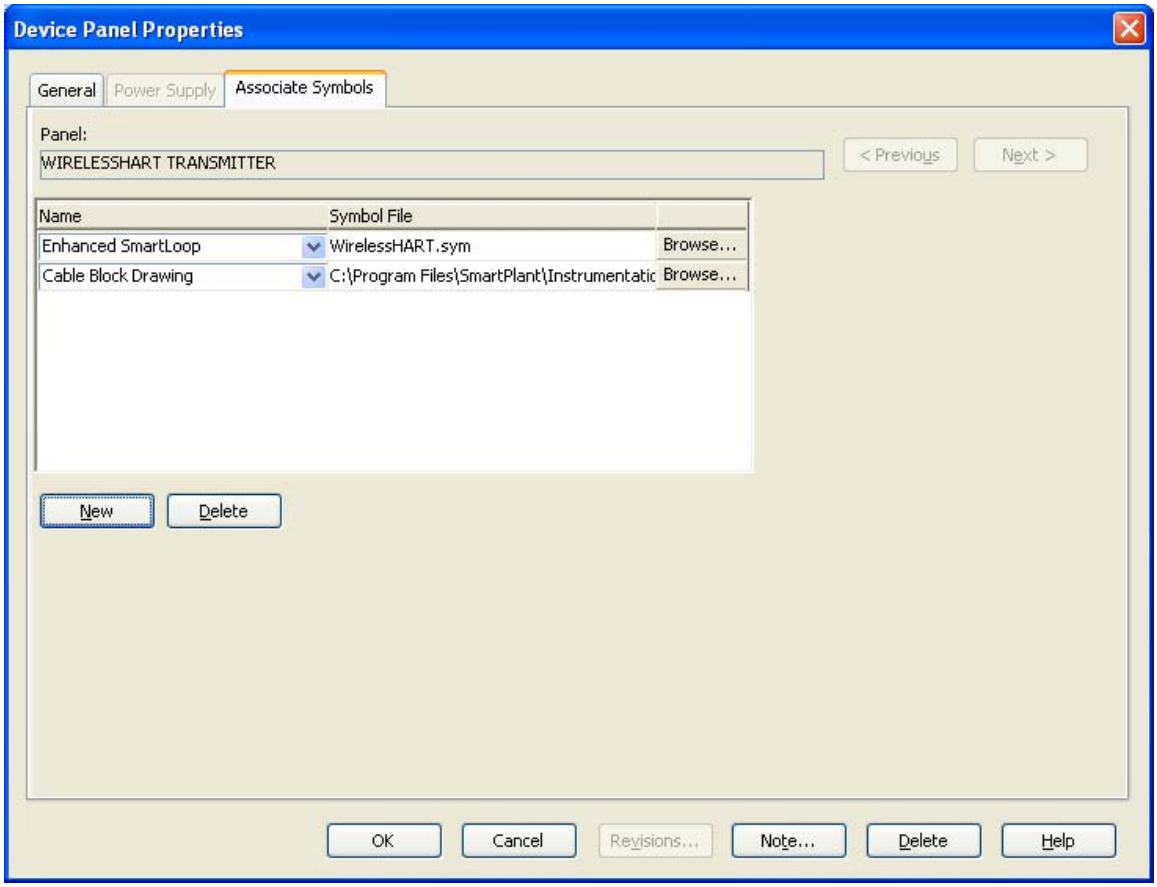
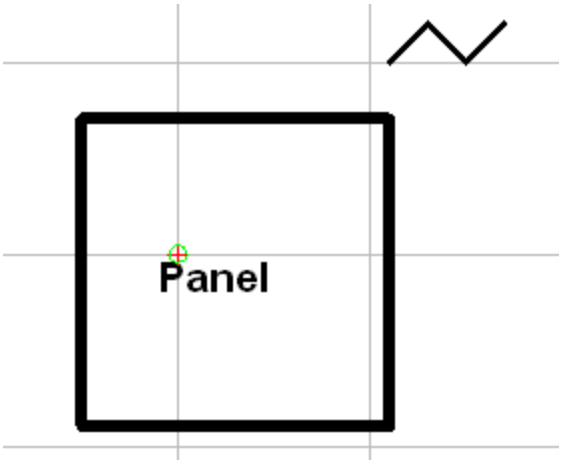


Figure 25. Assigning Symbols In SPI

Basic symbols can be created in SPI using the editing tools. Below are examples for *Wireless*HART field devices and a *Wireless*HART gateway. The zig-zig symbol shown below is defined by ISA. For more documentation, nothing special is required since signaling is typically not well indicated. For auto-generated documents, it may be useful to include the scan rate by referencing the User Defined Field, although this is not an absolute requirement. Most importantly, the project management team decides on a symbol convention and remains consistent throughout the project.

*Wireless*HART Gateway symbol:



*Wireless*HART Device Symbol:

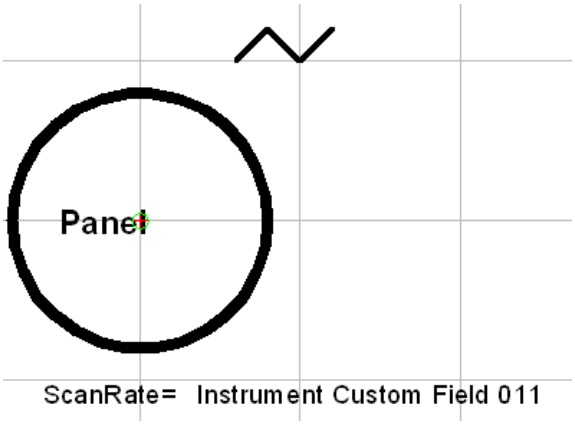


Figure 26. *Wireless*Hart Symbols

*Wireless*HART devices can be connected to a *Wireless*HART gateway using the User Defined Field. This type of drawing does not show the path through the *Wireless*HART network, but does show the relationship of the *Wireless*HART device and the *Wireless*HART gateway: Below is an example from the ISA-5.1 document, page 118.

B.9.5 Shared display, shared control and wireless instrumentation:

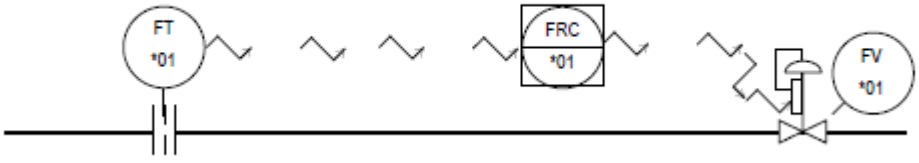


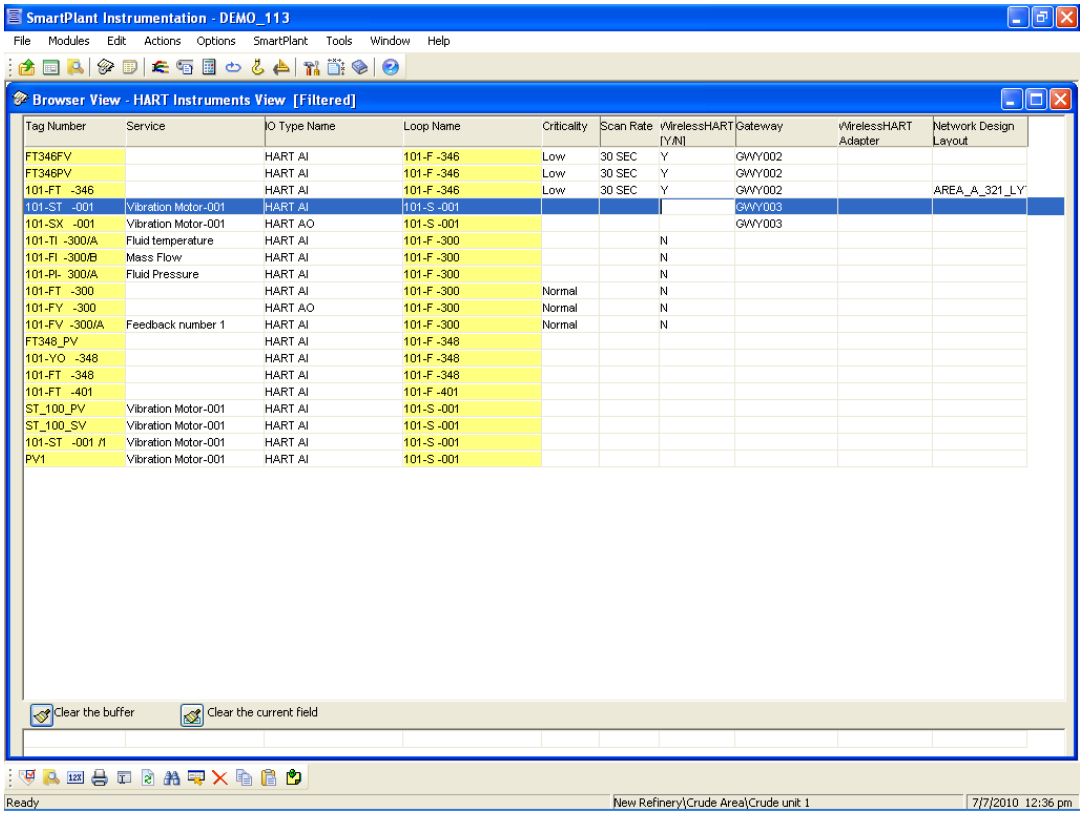
Figure 27. ISA 5.1 Drawing Example

Please note that inclusion of scan rates and the wireless signal symbol are optional. The authors of this document found the practice of including such information supportive of adopting and managing the unique attributes of *Wireless*HART.

Loop Drawings

Given that *Wireless*HART field devices do not require signal cabling, the documentation of the equivalent of wireless loop drawing is very simple to create.

The key information is to relate each wireless field device to the respective gateway. It is recommended that a basic wireless loop drawing show the traditional tag information as well as the *Wireless*HART User Defined Fields. This way, it is very clear to see which wireless devices are associated to which *Wireless*HART gateway. Currently, Intergraph SPI 2009 does not have the means to implement this in a specific drawing, thus it is recommended to use the Instrumentation Index showing the *Wireless*HART User Defined Fields. In the image below, a comprehensive list of *Wireless*HART devices are shown associated to different gateways.



Tag Number	Service	IO Type Name	Loop Name	Criticality	Scan Rate	WirelessHART [Y/N]	Gateway	WirelessHART Adapter	Network Design Layout
FT346FV		HART AI	101-F -346	Low	30 SEC	Y	GWY002		
FT346PV		HART AI	101-F -346	Low	30 SEC	Y	GWY002		
101-FT -346		HART AI	101-F -346	Low	30 SEC	Y	GWY002		AREA_A_321_LY
101-ST -001	Vibration Motor-001	HART AI	101-S -001				GWY003		
101-SX -001	Vibration Motor-001	HART AO	101-S -001				GWY003		
101-TI -300/A	Fluid temperature	HART AI	101-F -300			N			
101-FI -300/B	Mass Flow	HART AI	101-F -300			N			
101-PI- 300/A	Fluid Pressure	HART AI	101-F -300			N			
101-FT -300		HART AI	101-F -300	Normal		N			
101-FY -300		HART AO	101-F -300	Normal		N			
101-FV -300/A	Feedback number 1	HART AI	101-F -300	Normal		N			
FT348_PV		HART AI	101-F -348						
101-YO -348		HART AI	101-F -348						
101-FT -348		HART AI	101-F -348						
101-FT -401		HART AI	101-F -401						
ST_100_PV	Vibration Motor-001	HART AI	101-S -001						
ST_100_SV	Vibration Motor-001	HART AI	101-S -001						
101-ST -001 /1	Vibration Motor-001	HART AI	101-S -001						
PV1	Vibration Motor-001	HART AI	101-S -001						

Figure 28. Filtered View Of *Wireless*Hart Tags

This list can then be filtered and printed by gateway. A key piece of information is the link to a drawing verifying that best practices have been verified which can also include physical instrument location.

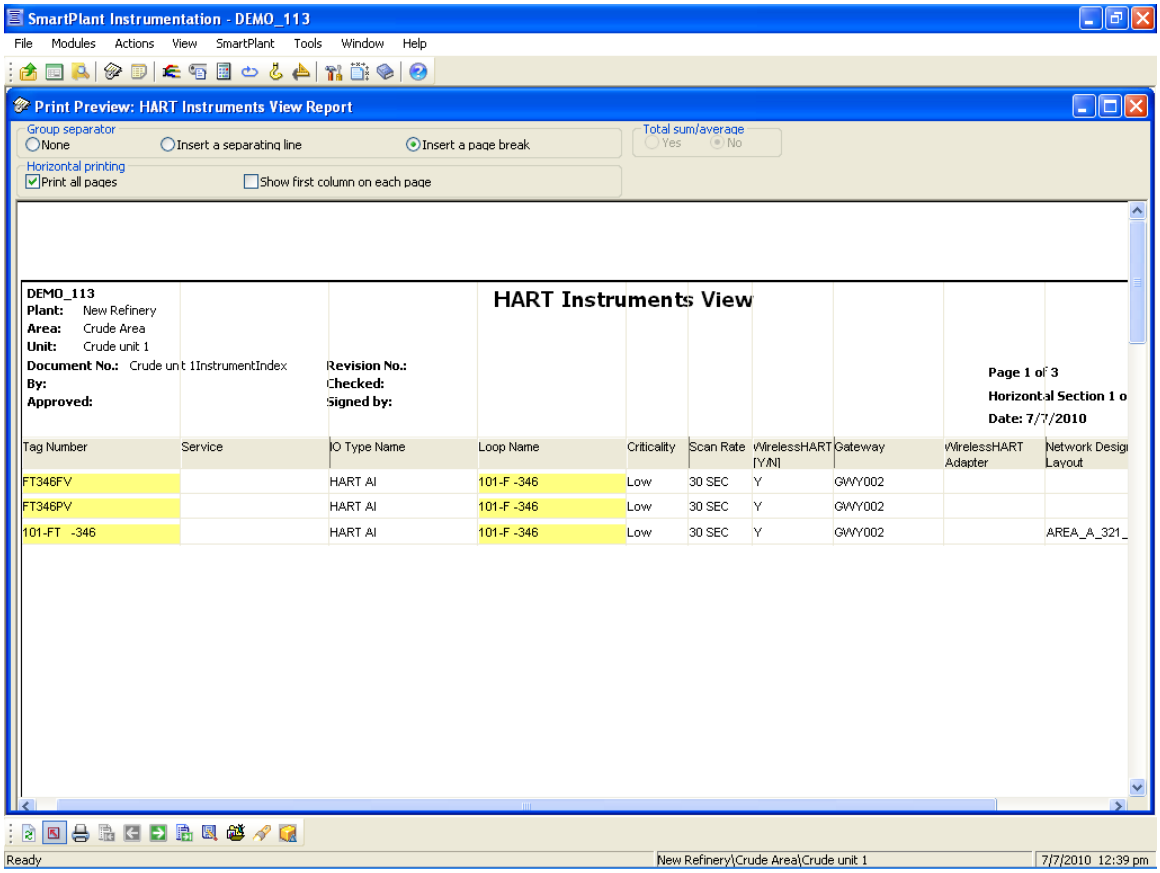


Figure 29. Tag View Filtered By Gateway

Loop Drawings for *Wireless*HART Adapters

A *Wireless*HART adapter is an accessory to a loop and should be treated as loop accessory like a multiplexor or transient protection. Loop accessories are traditionally not indicated on the loop drawing and are installed on site. It is recommended for simplicity that there are no modifications for the loop drawing of a wired HART device to reflect the presence of a *Wireless*HART adapter.

The *Wireless*HART adapter would be properly documented and accounted for on the Wireless Loop Drawing that shows the gateway and all associated *Wireless*HART devices.

Gateway Cable Block Drawings

A useful drawing to create is a Gateway Cable Block Drawing showing the gateway power and communication connections. All *Wireless*HART gateways, regardless of vendor, should have uninterruptable power supplies to maximize system reliability.

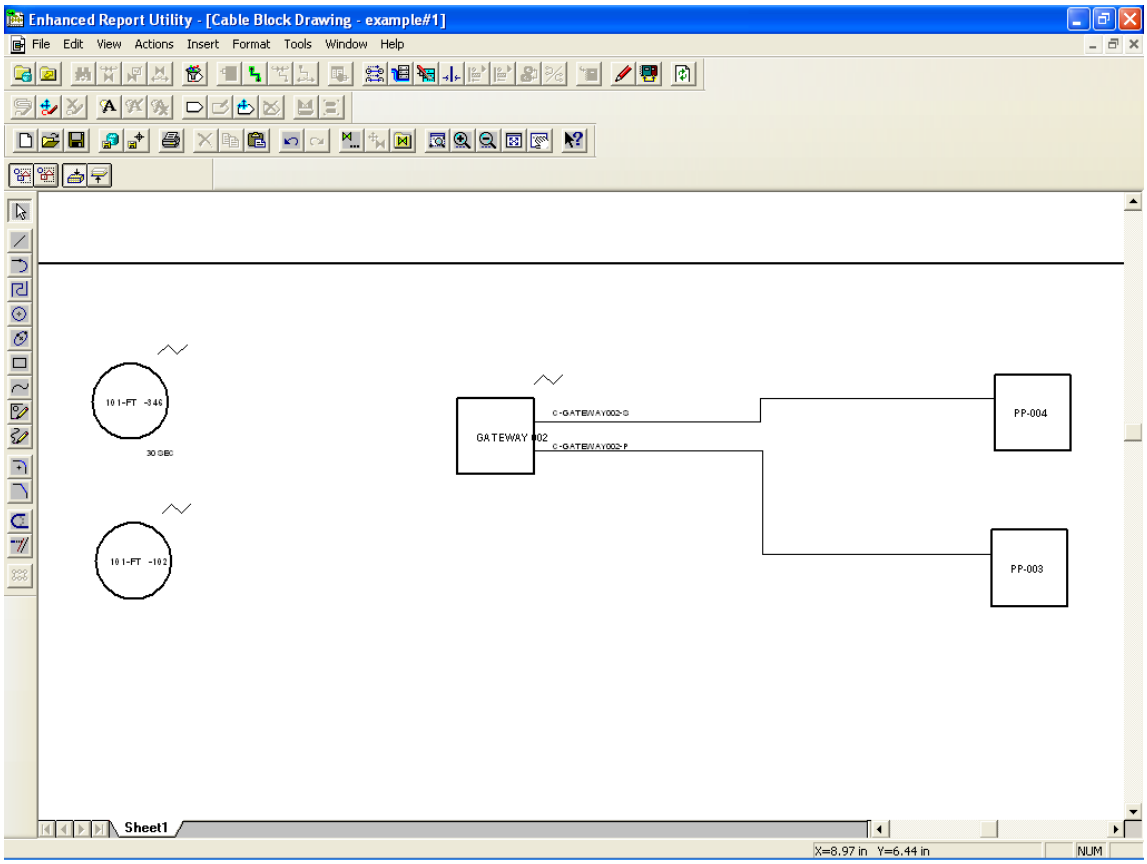


Figure 30. Gateway Cable Block Diagram

An additional drawing to consider, possible with a Cable Block Diagram, would be to show all gateways assigned to an area on the same document for convenience.

SPI Specification Sheets

Existing specification sheets can be used to indicate *Wireless*HART devices. Key fields to change are listed in the table below:

Specification Field	**Typical Value**
Scan Rate	4, 8, 16, 32, 64+
Power Supply	Intrinsically safe, field replaceable battery

Communication Type WirelessHART

Since *Wireless*HART is derived from wired HART, other specification fields should be completed as if it is a wired HART device.

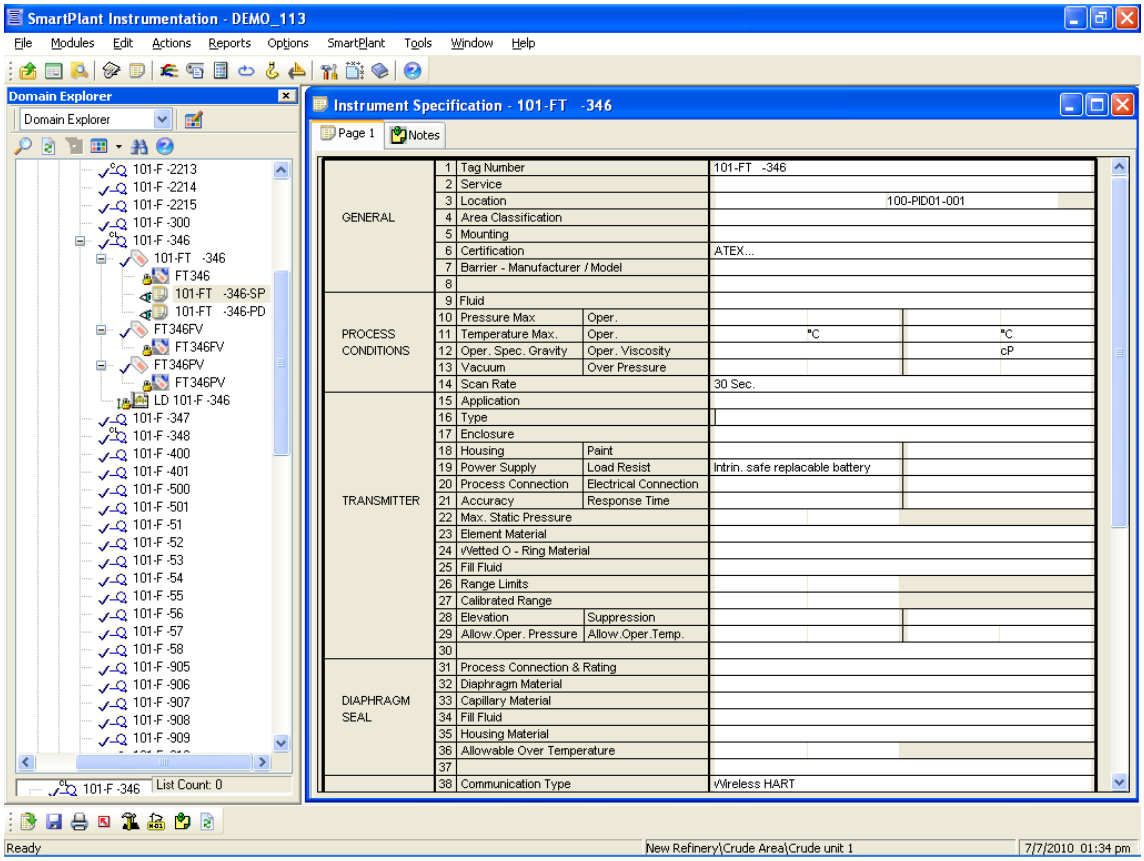


Figure 31. *Wireless*Hart Instrument Specification Sheet

Drawings in SPL – Smart Plant Layout

*Wireless*HART devices should be installed as their wired HART counterparts. Therefore, all *Wireless*HART devices can be indicated in drawings without deviation from the practices used for wired HART devices.

*Wireless*HART gateways should be located like junction boxes and reflect the installation guidelines from the network design.

Documenting Security Information

The *Wireless*HART security parameters of Network ID and Device Join Key should not be a part of a wireless loop drawing or in the SPI design environment. These are security parameters used to protect the

network and should be managed per a local security policy implemented by the Owner/Operator. The Network ID and Device Join Key are not required for the design. The wireless loop drawing associates the *Wireless*HART device with the *Wireless*HART gateway tags. Separately, secure documents containing *Wireless*HART security provisioning including the *Wireless*HART gateway tag can be used to cross reference the Network ID and Join Key. Remember, all Network ID and Device Join Keys should be unique for every gateway and every *Wireless*HART field network. This type of security management is similar to the management of security information for control systems and servers.

Appendix A. Example ISA Specifications

Below is a sample specification for a *Wireless*HART gateway.

RECEIVER INSTRUMENTS (Wireless Gateway)

NO	BY	DATE	REVISION

SHEET ____ OF ____ | SPEC. NO. | REV. | CONTRACT | DATE | REQ. P.O. | BY | CHK'D | APPR.

	1	Tag No.	Service
GENERAL	2	Function	Record ☐ Indicate ☐ Control ☐ Blind ☐ Integ ☐ Deviation ☐ Other IEC 62591 wirelessHART Network Administration/Setup
	3	Case	MFR STD ☒ Nom Size 229mmX283mm Color: MFR STD ☒ Other Blue
	4	Mounting	Flush ☐ Surface ☐ Rack ☐ Multi-Case ☐ Other Field mounted with or without remote antenna. For Multiple Case, See Spec. Sheet
	5	Enclosure Class	General Purpose ☐ Weather Proof ☒ Explosion-Proof ☐ Class Class I Div II For Use in Intrinsically Safe System. ☐ Other IEC 62591 wirelessHART field Network
	6	Power Supply	117 V 60Hz ☐ Other ac ____ dc ☒ 24 Volts
	7	Chart	____ Strip ☐ ____ Roll ☐ ____ Fold ☐ Circular ____ Time Marks ____ Range ____ Number ____
	8	Chart Drive	Speed ____ Power ____
	9	Scales	Type ____ Range 1 ____ 2 ____ 3 ____ 4 ____
CONTROLLER	10	Control Modes	P = Prop (Gain), I = Integral (Auto Reset), D = Derivative (Rate), Sub: s = Slow, f = Fast P ☐ PI ☐ PD ☐ PID ☐ I_f ☐ D_f ☐ I_s ☐ D_s ☐ Other ____
	11	Action	On Meas. Increase Output: Increases ☒ Decreases ☐
	12	Auto-Man Switch	None ☐ MFR STD ☐ Other ____
	13	Set Point Adj.	Manual ☐ External ☐ Remote ☐ Other ____
	14	Manual Reg	None ☒ MFR STD ☐ Other ____
	15	Output	4-20 mA ☐ 10-50 mA ☐ 21-103 kPa (3-15 psig) ☒ Other OPC, Modbus RTU, Modbus TCP, HART, HTML
INPUTS	16	Input Signals	4-20 mA ☐ 10-50 mA ☐ 21-103 kPa (3-15 psig) ☐ Other IEC 62591 wirelessHART
	17	No. of Inputs	1 ☐ 2 ☐ 3 ☐ 4 ☐ X 100 devices
	18	Power for XMTRS	External ☒ This Inst ☐ No. of Independent Supplies ____ For Transmitters, See Spec Sheet. ____
ALARMS	19	Alarm Switches	Quantity ____ Form ____ Rating ____
	20	Function	Meas. Var. ☐ Deviation ☐ Contacts To ____ On Meas ____ Other ____
	21	Options	Filter-Reg ☐ Supply Gage ☐ Charts ☐ Int. Illumination ☐ Other Multiple Ethernet connections, remote mount antenna, additional output protocols, additional hazardous area approvals
	22	MFR & Model No.	____

Notes:
1. Support device burst (scan) rates from 4 seconds to 60 minutes.

ISA Form S20.1a

Figure 32. ISA Sample Wireless Gateway Specification Sheet

Appendix B. *Wireless*HART vs. HART Comparison

Below is a comprehensive list of all differences of end user significance in a *Wireless*HART device relative to a wired HART device. Not all features are implemented in every wireless field device by every vendor.

wirelessHART Parameter	Parameter Options	Example	Technical Details	Notes
Long Tag	field	UNIT_A_TT-101	32 Characters - characters can be any in ISO Latin-1 (ISO 8859-1) character set.	Not unique to wirelessHART - wired HART6 and 7 devices also have Long Tag. Additional field to the HART short tag with 8 characters. Devices can have a long and short tag.
Network ID	Number	10145	An integer number between 0 and 36863	Every gateway must have a unique ID - and field devices must have the matching ID to a specific gateway that it is to join with.
Network Join Key	4 fields	23adfe00-0edf000a-000df038-2398dc07	4 four byte numeric fields (in Hexadecimal format). For example - 4 8 character fields where each character must be a number from 0-9, or a letter from A to F.	Randomize for greatest strength
Broadcast Message	One or more Enumerated choices	Device Status & All Process Variables	Choices include: 1- Primary variable only 2 -Primary variable in percent of range and mA 3 -All dynamic variables in engineering units 9 - Selectable process variables/status in engineering units 33 -Selectable process variables in engineering units 48 -Device status number between 0 and 65535 - Custom command	Not unique to wirelessHART - wired HART devices can also broadcast (burst) commands on the wired loop. Field devices have more than 1 broadcast message available. All wirelssHART devices must support a minimum of 3 messages - but can support up to 250 if they choose. The most optimal configuration to preserve power is to have as few of these broadcast messages configured as possible. We attempt to simplify this by asking the user to choose between 2 options which dictate the complete set of Broadcast messages and Broadcast modes. These 2 options are "Emerson Optimized" or "Generic". Some products (e.g. the THUM Adapter) may have special situations where a simple choice between these 2 global modes are not adequate - and thus multiple broadcast messages should be specified.
Broadcast Variables	One or more sets of 8 Enumerated choices	PV, SV, TV, QV, Variable 0, Variable 1, Variable 2, and Variable 3	Choices include: 243 - Battery Life 244 - Percent of range 245 - Loop Current 246 - PV 247 - SV 248 - TV 249 - QV 250 - Disabled 0 thru 249 specific to each device User-friendly choice names from 0 to 249 are device specific. Might just have to specify numbers	Not unique to wirelessHART - wired HART devices can also broadcast (burst) commands on the wired loop. Field devices have 1 set of broadcast variables for each broadcast message. Broadcast variables are only applicable when the corresponding broadcast message is Selectable process variables / status (up to 8 can be chosen), or Selectable process variables (up to 4 can be chosen).
Triggered Broadcast Rate	One or more Numbers	60	In seconds - must be 1, 2, 4, 8, 16, 32, or any number between and including 60 to 3600 seconds)	Not unique to wirelessHART - wired HART 7 devices can also broadcast (burst) commands on the wired loop. Field devices have 1 broadcast rate for each broadcast message. We attempt to simplify this by asking for ony 1 broadcast rate, and setting all available broadcast messages to the same rate. Some products (e.g. the THUM Adapter) may have special situations where multiple rates should be specified.
Broadcast Mode	One or more Enumerated choices	Continuous	Choices include: Disabled Continuous Report by Exception On Change	Not unique to wirelessHART - wired HART 7 devices can also broadcast (burst) commands on the wired loop. Field devices have 1 Broadcast Mode for each broadcast message. Most products only support Disabled or Continuous. Future revisions of products will offer the remaining 2 modes.
Maximum Broadcast Rate	One or more Numbers	60	In seconds - must be 1, 2, 4, 8, 16, 32, or any number between and including 60 to 3600 seconds) Must be larger than Triggered Broadcast rate.	Not unique to wirelessHART - wired HART 7 devices can also broadcast (burst) commands on the wired loop. Field devices have 1 Maximum broadcast rate for each broadcast message. This parameter is only applicable when the corresponding Broadcast mode is set to "Report by Exception" or "On Change".
Broadcast Trigger Threshold	One or more Number	345.2	IEEE-754 single precision floating point value	Not unique to wirelessHART - wired HART 7 devices can also broadcast (burst) commands on the wired loop. Field devices have 1 Burst Trigger Threshold for each broadcast message. This parameter is only applicable when the corresponding Broadcast mode is set to "Report by Exception".
Broadcast Trigger Units	One or more Fields	PSI	Choices include all units available in the HART Common Tables Specification.	Not unique to wirelessHART - wired HART 7 devices can also broadcast (burst) commands on the wired loop. Field devices have 1 Burst Trigger Units for each broadcast message. This parameter is only applicable when the corresponding Broadcast mode is set to "Report by Exception".
Event Notification Control	One or more enumerated choices	Disabled	Choices include: Enabled Disabled	Not unique to wirelessHART - wired HART 7 devices can also broadcast (burst) events on the wired loop. Field devices have 1 Event Notification Mode for each event. All WirelessHART devices must support at least 1 event - but can suport up to 250 events if they choose.
Event Notification Retry Rate	One or more Numbers	60	In seconds - must be 1, 2, 4, 8, 16, 32, or any number between and including 60 to 3600 seconds)	Not unique to wirelessHART - wired HART 7 devices can also broadcast (burst) events on the wired loop. Field devices have 1 Event Notification Retry Rate for each event.
Event Notification Default Rate	One or more Numbers		In seconds - must be 1, 2, 4, 8, 16, 32, or any number between and including 60 to 3600 seconds) Must be greater than Event Notification Retry Rate	Not unique to wirelessHART - wired HART 7 devices can also broadcast (burst) events on the wired loop. Field devices have 1 Event Notification Default Rate for each event.
Event Notification Debounce Rate	One or more Numbers		In seconds - must be 1, 2, 4, 8, 16, 32, or any number between and including 60 to 3600 seconds) Must be less than Event Notification Retry Rate	Not unique to wirelessHART - wired HART 7 devices can also broadcast (burst) events on the wired loop. Field devices have 1 Event Notification Debounce Rate for each event. All WirelessHART devices must support at least 1 event - but can suport up to 250 events if they choose.
Event Notification Event Mask	One or more sets of 13 integers	0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF		Not unique to wirelessHART - wired HART 7 devices can also broadcast (burst) events on the wired loop. Field devices have 1 set of Event Notification Masks for each event. All WirelessHART devices must support at least 1 event - but can suport up to 250 events if they choose.
Power Source	Field	Battery	Choices include: Battery Energy Scavenging Line Power	Most devices only support Battery as a choice. Future products may allow one or more of the other choices.
Radio Output Power	Field	+10dBm	A signed integer between +10 and -10.	Whole wirelessHART network should be set to same value. Most wireless products to dat support either +10 or 0 dBM only.

Appendix C. AMS Wireless Snap-On Application

All design parameters discussed in the previous section are automated in the AMS Wireless Snap-On Application from the Asset Optimization Division of Emerson Process Management. Networks can be design and files saved to support the engineering process. The design features of the application require no additional software.

AMS Snap-On documentation is available on-line:

http://www.documentation.emersonprocess.com/groups/public_assetoptprodlit/documents/data_sheets/idm_allds0508e_wirelesssnapon.pdf

Appendix D. Wireless Spectrum Governance

Wireless applications have been deployed in the process industry for over 40 years. In any process facility, many applications using RF signals including personnel communications, RF ID systems, ad hoc systems, cell phones may exist. The essential ingredients to making wireless automation feasible were solving the problems of power to enable devices to operate on batteries for multiple years; self-mitigating all obstacles in the process environment so advanced wireless knowledge was not a requirement for adoption; and coexisting with other sources of wireless energy.

*Wireless*HART operates in the 2.4 GHz Industrial, Scientific, and Medical (ISM) radio band that typically operates from 2.400-2.500 GHz. The exact frequency limitations and RF output power levels may be slightly different country by country. *Wireless*HART employs limitations that allow for universal operation in almost all countries with exceptions being noted for specific products by device manufactures. The ISM radio bands are license-free, but do require approval from governmental regulating agencies. These approvals are typically obtained by the *Wireless*Hart vendor. Since vendors for multiple applications can use the same spectrum, *WirelessHart* must be able to successfully coexist.

*Wireless*HART uses multiple techniques to coexist with other wireless applications:

- Network segmentation – allows thousands of *Wireless*HART devices to exist in the same physical space, provided each network has a unique Network ID.
- Spectrum isolation – wireless applications in different portions of the spectrum do not “see” each other and thus do not interfere with each other.
- Low power – *Wireless*HART devices are very low power relative to handheld personnel communicators, Wi-Fi, and RFID readers. This prevents WirelessHART interference with these high power applications.

- Spacial hopping – self-organizing mesh networks can hop on different paths that may be exposed to different RF conditions. The *Wireless*HART devices self-organize paths through the process environment that mitigate RF obstacles the same way as physical obstacles.

- Channel hopping – *Wireless*HART devices use 15 channels within the 2.4 GHz spectrum. Rotation of channel usage ensures that interference on one or several channels does not prevent reliable communications.

- DSSS coding – allows transmissions to be modulated with unique encoding for the purposes of encryption as well as filter. DSSS Coding extends radio receive sensitivity through digital processing.

- Time Synchronized Meshed Protocol (TSMP) – allows for multiple retries within the specified scan rate on different network paths and on different frequencies.

Despite these coexistence features, it is still beneficial to have some form of wireless governance. *Wireless*HART can be interfered with, but only under conditions that likely disrupt all wireless applications operating in the 2.4 GHz spectrum.

A key example is broadband interference. Many legacy wireless systems are very high power. As an example, consider a personnel communication system using high power two-way radios operating in the 800 MHz frequency range. Although the system is legal and operating according to specifications, it can emit broadband interference that spans several GHz in the spectrum. This broadband interference then affects all applications in other spectrums by minimizing the signal-to-noise ratio. The simple solution is to place a band pass filter on all systems such that they only emit RF energy in the spectrum licensed for usage. See the illustrative diagram below showing broadband interference before and after the implementation of a low pass filter.

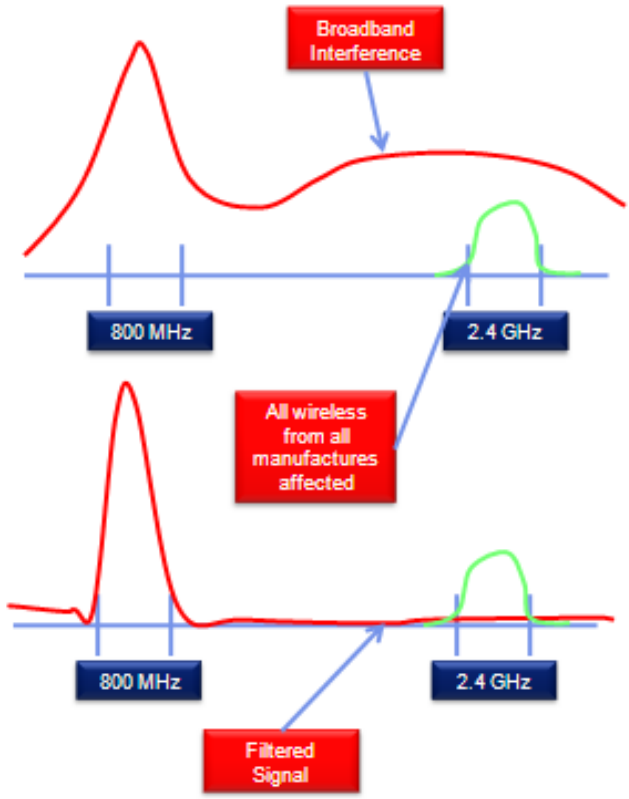


Figure 33. Installing A Low-Pass Filter

Most government agencies make the license of high power radios public information since there is the potential to interfere with private and public entities other than the licensee. In the United States, the federal government makes all licensed radios searchable at http://wireless2.fcc.gov/UlsApp/UlsSearch/searchLicense.jsp. If a facility has licensed radios, efforts should be made to verify low-pass filters are in place. The regulations were created before the advent of low-power systems, including Wi-Fi, and future consideration was not given to coexistence of low power with high power systems. Other countries are also likely have a similar type of database.

Installing low pass filters is straight forward and typically only requires insertion of the unit in series with existing RF cabling and proper resealing of RF connections.

The emerging 802.11N Wi-Fi standard may emit broadband interference if operating a non-802.11N application in the 2.4 GHz ISM radio band. Relative to 802.11B or 802.11 G which use a single channel, typically 1,

6, or 11, 802.11N will use multiple adjacent channels to enable increased bandwidth for demanding applications such as bulk data transfer, security cameras, and streaming video. 802.11N can be operated in either the 2.4GHz ISM band or the 5.8 GHz ISM band. Operation in the 5.8 GHz band applies the principle of spectrum isolation and comes with the additional advantage that 5.8 GHz RF signals can transfer information much faster than 2.4 GHz RF signals due to the much faster modulation.

Another emerging standard is Wi-Max, which operates in the 2.3 GHz, 2.5 GHz, or 3.5 GHz radio bands. Although these spectrums do not overlap the 2.4 GHz spectrum, there are no provisions in the Wi-Max standard to adopt or enforce the usage of low-pass filters in either clients or Access Points. The high power of Wi-Max has the potential to interfere with all wireless applications specifically designed for operation in the 2.4 GHz spectrum. Wi-Max clients should have limited deployment in the process facility and Wi-Max systems should be deployed in the 3.5 GHz spectrum to minimize risk of broadband interference.

Aside from managing potential broadband interference sources, wireless governance a basic process. Below is a summary of key considerations for wireless governance:

- A local wireless governance policy should serve the purpose of documenting all wireless sources in a plant and enforcing best practices for wireless coexistence.
- Enforce proper installation and compliance with regulation for all wireless applications with regards to power levels, spectrum usage, and encryption in accordance with government regulation.
- Provide guidelines for wireless applications spectrum usage.
    - Limit 802.11N Applications to 5.8 GHz ISM radio band.
    - Limit Wi-Max deployment to the 3.5 GHz spectrum.
    - Put high bandwidth wireless applications such as security cameras in the 5.8 GHz radio band.
- Support proper segmentation of *Wireless*HART networks.

- Every network in the process facility should have a unique Network ID and Device Join Key to prevent *Wireless*HART devices from joining the wrong network and ensure a maximum level of security.

Appendix E. References

Topic	Reference
***Wireless*HART**	1. **HART Communication Foundation** http://www.hartcomm.org/protocol/wihart/wireless_technology.html - Protocol Specifications, Overview, Member Companies. 2. ***Wireless*HART: Real-Time Mesh Network for Industrial Automation** http://www.amazon.com/gp/product/1441960465?ie=UTF8&tag=easydeltavcom-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=1441960465, Comprehensive resource on *Wireless*HART.
Security	1. **ANSI/ISA-TR99.00.01-2007** – "Security Technologies for Industrial Automation and Control Systems" (ISA Technical Report provides a relatively current "assessment of various cyber security tools, mitigation counter-measures, and technologies…") http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=9665 2. **DHS –** Main Control Systems Security Program (CSSP) website: http://www.us-cert.gov/control_systems (An actively supported government resource for Industrial Control System security information, many links to other resources) 3. **DHS** – Recommended Practice for Patch Management of Control Systems http://csrp.inl.gov/Documents/PatchManagementRecommendedPractice_Final.pdf (an example of the Recommended Practices documents available) 4. **DOE** – "21 Steps to Improve Cyber Security of SCADA Networks" (an oldie but a goodie) http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf 5. **Emerson** – "DeltaV System Cyber-Security" http://www.easydeltav.com/pd/WP_DeltaVSystemSecurity.pdf 6. **NISCC/BCIT** – "Firewall Deployment for SCADA and Process Control Networks" (from 2005, but still a great reference) http://www.cpni.gov.uk/docs/re-20050223-00157.pdf 7. **CPNI** – "Deployment Guidance for Intrusion Detection Systems" (lots of good stuff from UK's Centre for the Protection of National Infrastructure) http://www.niscc.gov.uk/Docs/re-20031119-00730.pdf?lang=en 8. **NIST** – SP 800-53, Revision 3 "Recommended Security Controls for Federal Information Systems and Organizations" (this latest version includes Appendix I: Industrial Control Systems, Security Controls, Enhancements, and Supplemental Guidance, basis for SP99, TG4 Foundational Requirements work) http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

9. **NSA** – "Defense in Depth" (excellent whitepaper on this important security concept) http://www.nsa.gov/ia/_files/support/defenseindepth.pdf
10. **NSA** – "The 60 Minute Network Security Guide (First Steps Towards a Secure Network Environment)" (The NSA's Information Assurance website has a lot of useful information) http://www.nsa.gov/ia/_files/support/I33-011R-2006.pdf
11. **SANS** – "20 Critical Security Controls – Version 2.0, Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines" (note link to printer friendly version) http://www.sans.org/cag/