Smart Wireless Gateway

IEC

WirelessHART

EMERSON
Process Management

Smart Wireless Gateway

NOTICE

Read this manual before working with the product. For personal and system safety, and for optimum product performance, make sure you thoroughly understand the Contents before installing, using, or maintaining this product.

Within the United States, Emerson Process Management has two toll-free assistance numbers:

Global Service Center
Software and Integration Support

1-800-833-8314 (United States)

+63-2-702-1111 (International)

Customer Central
Technical support, quoting, and order-related questions.

1-800-999-9307 (7:00 am to 7:00 pm CST)

North American Response Center
Equipment service needs.

1-800-654-7768 (24 hours—includes Canada)

Outside of the United States, contact your local Emerson Process Management representative.

⚠ WARNING

The products described in this document are NOT designed for nuclear-qualified applications. Using non-nuclear qualified products in applications that require nuclear-qualified hardware or products may cause inaccurate readings.

For information on Rosemount nuclear-qualified products, contact your local Emerson Process Management Sales Representative.

Contents

Appendix B: Product Certifications

Appendix C: DeltaV™ Ready

Appendix D: Redundancy

Section 1 Overview

1.1 Safety messages

Instructions and procedures in this manual may require special precautions to ensure the safety of the personnel performing the operations. Information that potentially raises safety issues is indicated by a warning symbol (⚠). Refer to these safety messages before performing an operation preceded by this symbol.

⚠ WARNING

Failure to follow these installation guidelines could result in death or serious injury.

- Make sure only qualified personnel perform the installation.

Explosions could result in death or serious injury.

- Verify the operating atmosphere of the device is consistent with the appropriate hazardous locations certifications.

Electrical shock could cause death or serious injury.

- Use extreme caution when making contact with the leads and terminals.

1.2 Introduction

The Smart Wireless Gateway connects *Wireless*HART® self-organizing networks with host systems and data applications. Modbus® communications over RS-485 or Ethernet LAN provide universal integration and system interoperability. The optional OPC functionality from the Gateway offers a means to connect to newer systems and applications while providing a richer set of data.

The Smart Wireless Gateway provides industry leading security, scalability, and data reliability. Layered security ensures that the network stays protected. Additional devices can be added at anytime. There is no need to configure communication paths because the Gateway manages the network automatically. This feature also ensures that *Wireless*HART field devices have the most reliable path to send data.

What is included?

The box containing the Smart Wireless Gateway contains several items essential to the complete installation and operation of the Gateway.

- Smart Wireless Gateway
- Quick Start Guide
- Software pack, 2 disk set
- Mounting hardware
- Conduit plugs, 4
- Conduit adapters (optional)

If an optional remote antenna has been ordered, it will be in a separate box containing:

- Remote mount antenna
- Mounting hardware
- Lightning arrestor
- Cable [1 or 2 pieces that total 50 ft, (15,2 m) in length]
- Coaxial sealant

1.3 Manual

This manual will help to install, configure, operate, and maintain the Gateway.

Section 1: Overview

This section introduces the product and describes what components may be found in the box. It also includes details for services and support as well as return and disposal of the product.

Section 2: Initial Connection

This section describes how to connect to the Gateway for the first time and what settings should be configured before placing it on a live control network. It is important to note that some Gateways are used in stand-alone applications and do not reside on a network. In these cases, it is still important to configure the items outlined in this section.

Section 3: Mounting and Connection

This section describes how to properly mount the Gateway and make electrical connections, including electrical wiring, grounding, and host system connections. This section also describes how to mount the optional remote antenna.

Section 4: Software Setup

This section describes the installation and setup of the optional software included with the Smart Wireless Gateway. This software will aid in secure host integration as well as wireless field device configuration.

Section 5: Host Integration

This section describes how to connect the Gateway to a host system and integrate data gathered from the field device network. It covers network architectures, security, and data mapping.

Section 6: Troubleshooting

This section provides troubleshooting tips as well as information to contact technical support over the phone or through email.

Section 7: Glossary

The glossary defines terms used throughout this manual or that appear in the web interface of the Smart Wireless Gateway.

Appendices

The appendices provide additional and more specific information on a variety of subjects including Product Specifications and Product Certifications.

1.4 Service support

Global Service Center
Software and Integration Support

United States 1 800 833 8314
International   63 2 702 1111

Customer Central
Technical Support, quoting, and order related questions

United States 1 800 999 9307 (7:00 a.m. to 7:00 p.m. CST)
Asia Pacific   65 6777 8211
Europe/Middle East/Africa 49 8153 9390

1.5 Return of materials

To expedite the return process outside of North America, contact your Emerson Process Management representative.

Within the United States, call the Emerson Process Management Response Center toll-free number 1 800 654 7768. The center, which is available 24 hours a day, will assist you with any needed information or materials.

The center will ask for product model and serial numbers, and will provide a Return Material Authorization (RMA) number. The center will also ask for the process material to which the product was last exposed.

⚠ WARNING

Individuals who handle products exposed to a hazardous substance can avoid injury if they are informed of, and understand, the hazard. If the product being returned was exposed to a hazardous substance as defined by OSHA, a copy of the required Material Safety Data Sheet (MSDS) for each hazardous substance identified must be included with the returned goods.

1.6 Product recycling/disposal

Recycling of equipment and packaging should be taken into consideration and disposed of in accordance with local and national legislation/regulations.

Section 2 Initial Connection

> ⚠ **WARNING**
>
> **Failure to follow these installation guidelines could result in death or serious injury.**
>
> ■ Only qualified personnel should perform the installation.
>
> **Explosions could result in death or serious injury.**
>
> ■ Verify the operating atmosphere of the transmitter is consistent with the appropriate hazardous locations certifications.
>
> **Electrical shock could cause death or serious injury.**
>
> ■ Use extreme caution when making contact with the leads and terminals.
>
> **This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions:**
>
> ■ This device may not cause harmful interference.
>
> ■ This device must accept any interference received, including interference that may cause undesired operation.
>
> ■ This device must be installed to ensure a minimum antenna separation distance of 20 cm from all persons.

2.1 Overview

This section describes how to connect to the Gateway for the first time and what settings should be configured before placing it on a live control network. It is important to note that some Gateways are used in stand-alone applications and do not reside on a network. In these cases, it is still important to configure the items outlined in this section.

Before the Gateway can be permanently mounted and connected to a live control network, it needs to be configured with an IP address. This is done by forming a private network between the gateway and a PC/laptop. The following items are needed to complete this section:

■ Gateway

■ PC/laptop

■ 24 VDC (nominal) power supply

Note
If the Gateway was ordered with the DeltaV™ *Ready* option, it has been configured to operate on a DeltaV control network, and the Initial Configuration Section does not need to be completed. Only setting the password is required.

2.2 System requirements

The following requirements apply to the PC/laptop used to configure the Gateway. Additional requirements may apply if using the optional Security Setup Utility or AMS® Wireless Configurator. See 00809-0200-4420, Rev HB for more information.

Web browser applications

- Mozilla Firefox® 1.5 or higher
- Microsoft® Internet Explorer® 6.0 or higher

Ethernet

- 10/100BaseTX Ethernet communication protocol

2.3 Initial setup

2.3.1 Prepare PC/laptop

The PC/laptop will need to be configured to form a private network before communicating to the Gateway. The network settings can be found in the control panel of the PC/laptop. To configure these settings:

1. Find and open the Control Panel (Generally found from the Start Menu).

2. Open Network Connections.

3. Select **Local Area Connection**.

4. Right click the mouse and select **Properties** from the list.

5. Select **Internet Protocol (TCP/IP)**, then select **Properties**.

6. From the *General* tab, select **Use the following IP address**.

7. Set the IP Address to "192.168.1.12" and select **Tab**.

8. A Subnet mask of 255.255.255.0 should fill in automatically.

9. Select **OK** to close the *Internet Protocol (TCP/IP)* window.

10. Select **Close** on the *Local Area Connection* window.

Internet proxies will need to be disabled through the PC/laptop's default internet browser.

1. Find and open the default internet browser (typically Microsoft Internet Explorer).

2. Find the *Tools* menu and select **Internet Options**.

3. From the *Connections* tab, select **LAN Settings**.

4. Under *Proxy Server*, verify the boxes for *Automatically Detect Settings* and *Use a proxy server for your LAN* are unchecked.

5.   Select **OK** to close the *Local Area Network (LAN) Settings* window.

6.   Select **OK** to close the *Internet Options* window.

The PC/laptop is now set up to form a private network and to communicate with the Gateway.

Note
Connecting to the Gateway's secondary Ethernet port will require different network settings. Please see Table 2-1 for additional network settings.

Table 2-1. Default IP Addresses

	Gateway	PC/laptop	Subnet
Ethernet 1	192.168.1.10	192.168.1.12	255.255.255.0
Ethernet 2	192.168.2.10	192.168.2.12	255.255.255.0
Ethernet 1 (DeltaV Ready)	10.5.255.254	10.5.255.200	255.254.0.0
Ethernet 2 (DeltaV Ready)	10.9.255.254	10.9.255.200	255.254.0.0

2.3.2   Connections and power

Physically connect the PC/laptop to the Gateway by connecting one end to the Ethernet port on the back of the PC/laptop. Connect the other end to the Ethernet 1 port on the Gateway. Figure 2-1 shows the standard terminal block diagram. Once the Gateway and PC/laptop are connected, wire a 24 VDC (nominal) power supply with a capacity of at least 250 mA to the Gateway power input terminals.

Figure 2-1. Standard Terminal Block
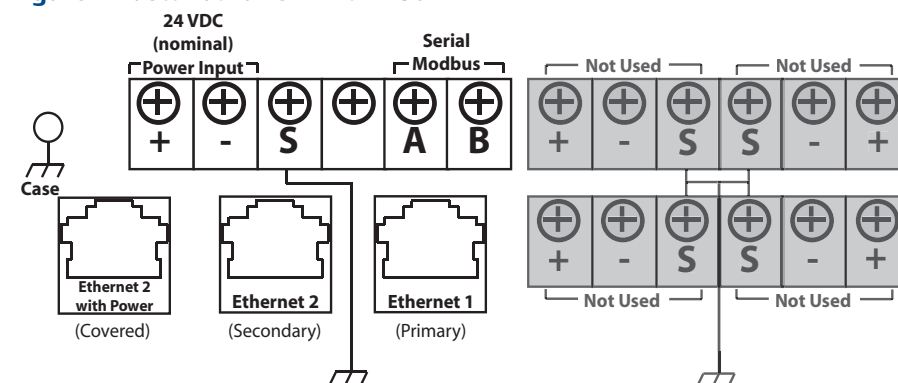
⚠ **WARNING**

When making physical connections to the Gateway it is important to use the electrical conduit entries located on the bottom of the housing. Connecting through the open terminal block cover (the lower cover) may stress the connections and damage the Gateway.

2.3.3   Configure the Gateway

It is now possible to log into the Gateway for the first time and begin configuration for placement on a live control network. The following items need to be configured:

- Security passwords
- Time settings
- TCP/IP network settings

Use the following procedure to log in to the Gateway:

1.   Open a standard web browser (typically Microsoft Internet Explorer).

2.   Enter "*192.168.1.10*" in the address bar.

3.   Acknowledge the security to proceed.

4.   In the *User Name* field, enter "admin".

5.   In the *Password* field, enter "default".

The web browser will now be directed to the Gateway's default home page. There is a navigation menu located on the left hand side with four main areas.

- Diagnostics: view status of communications, client server parameters, and more
- Monitor: screens created by the user to view data from field devices
- Explorer: basic view of values from field devices
- Setup: configure the Gateway for operations, security, and host system integration

Security passwords

There are four-role based user accounts for the gateway with varying levels of access. The table below describes this access.

Table 2-2. Role Based Access User Accounts

Role	User name	Web interface access
Executive	exec	Read-only access
Operator	oper	Read-only access
Maintenance	maint	Configure HART® device settings Configure Modbus® communications Configure Modbus register mapping Configure OPC browse tree Configure Active Advertising
Administrator	admin	Includes all maintenance privileges Configure Ethernet network settings Configure WirelessHART® network settings Set passwords Set time settings Set home page options Configure custom point pages Restart applications

Each of the initial passwords for the user accounts is *default.* It is recommended, for security purposes, that these passwords are changed. The administrator password should be appropriately noted when changed. If it is lost, please contact Emerson Process Management for technical support.

To change the User Accounts Passwords:

1.   Navigate to **System Settings>Users>User accounts**.

2.   Set the new password for each role based user account, and confirm.

3.   Click **Submit**.

Note
It is suggested that the default security settings in **System Settings>Users>User accounts** be changed to the local IT best practices or the *Normal* setting after initial login. Strong or custom settings are available for more robust passwords. For more information on this screen and others please see the User Interface Terminology Guide (document number 00809-0600-4420).

Time settings

The Gateway is the timekeeper for the WirelessHART network, so it is imperative that the Gateway's time is accurate for timestamp data to be meaningful. Time settings can be found by navigating to **System Settings>Time**.

There are three ways to set the Gateway time:

■   Network Time Protocol (recommended)
       This option uses a Network Time Protocol (NTP) server to slowly adjust the Gateway's time in order to match the time of the control network. Enter the IP address for the NTP server and select the packet version (1, 2, 3, or 4).

■   Set with PC Time
       This option will match the Gateway's time to that of the PC/laptop.

■   Manual Entry
       This option allows the user to enter a specific date (MM:DD:YY) and time (HH:MM:SS).

Note
Network Time Protocol (NTP) is recommended for the best network performance because it always adjusts time to match the network time server.

Figure 2-2. Time Settings

TCP/IP network settings

⚠ WARNING

Use caution when making changes to the TCP/IP network settings. If they are lost or improperly configured, it may be impossible to log into the Gateway. Contact the network administrator for information on the proper TCP/IP network settings to apply.

Prior to the gateway being installed and connected to a live control network, it should be configured with an IP address, as well as other TCP/IP network settings.

Request the following configuration items from the network administrator:

- Specify an IP address, or use a DHCP server
- Hostname
- Domain Name
- IP address
- Netmask
- Gateway

Obtaining an IP address from a DHCP server is not recommended, since the Gateway operation will be dependent upon the availability of the DHCP server. For maximum gateway availability it is best practice to specify an IP address.

To change the TCP/IP Network Settings:

1. Navigate to **System Settings>Gateway>Ethernet Communication**.

2. Select Specify an IP address (recommended).

3. Enter the following:

   ■ Hostname
   ■ Domain Name
   ■ IP Address
   ■ Netmask
   ■ Gateway

4. Click **Submit**.

5. When prompted, click **Restart apps**.

6. Click **Yes** to confirm restart.

7. Close the web browser.

Note
Once the IP Address of the Gateway has been changed, communications to the web interface will be lost. Restart the web browser, then log back into the Gateway using the new IP address and other TCP/IP network settings. The PC/laptop TCP/IP network settings may need to be changed.

Figure 2-3. Ethernet Settings

2.3.4 System backup

The Gateway has a System Backup and Restore feature that saves all user-configured data. It is best practice that a System Backup be performed periodically throughout the installation and configuration process.

1. Navigate to **System Settings>Gateway>Backup And Restore>Save Backup**.

2. Click **Save Backup**.

3. The Gateway collects the configuration date and when the file download pop up appears, click **Save**.

4. Enter a save location and file name.

5. Enter **Save**.

6. Click **Return** to form.

Note
System backup contains user passwords and keys used for encrypting communication. Store downloaded system backups in a secure location.

Section 3   Mounting and Connection

> ⚠ **WARNING**
>
> **Explosions could result in death or serious injury.**
>
> - Verify that the operating atmosphere of the device is consistent with the appropriate hazardous locations certifications.
>
> **Electrostatic discharge can damage electronics.**
>
> - Use proper personal grounding before handling electronics or making contact with leads and terminals.
>
> **Electrical shock could cause death or serious injury. If the device is installed in a high-voltage environment and a fault condition or installation error occurs, high voltage may be present on transmitter leads and terminals.**
>
> - Use extreme caution when making contact with the leads and terminals.
>
> **Failure to follow these installation guidelines could result in death or serious injury.**
>
> - Make sure only qualified personnel perform the installation.
>
> **This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions:**
>
> - This device may not cause harmful interference.
> - This device must accept any interference received, including interference that may cause undesired operation.
> - This device must be installed to ensure a minimum antenna separation distance of 20 cm from all persons.

3.1   Overview

This section describes how to properly mount the Gateway and make electrical connections, including electrical wiring, grounding, and host system connections. This section also describes how to mount the optional remote antenna.

3.1.1   General considerations

The Smart Wireless Gateway may be mounted in any general purpose location. Be sure the covers are secured tightly to prevent exposure of any electronics to moisture and contamination.

The Gateway should be mounted in a location that allows convenient access to the host system network (process control network) as well as the wireless field device network.

3.1.2   Physical description

For dimensional drawing information refer to 00809-0200-4420, Rev HB. The cast aluminum housing encloses the electronics circuitry of the Gateway. The front of the enclosure has an upper cover and a junction box cover. The upper cover provides access to the electronics and radio. The junction box cover provides access to the terminal block.

To open either cover, use a ¼-in. bladed screwdriver to remove the appropriate screw on the unhinged side of the enclosure.

3.2   Mounting

Find a location where the Gateway has optimal wireless performance. Ideally this will be 15-25 ft. (4,6 - 7,6 m) above the ground or 6 ft. (2 m) above obstructions or major infrastructure. Figure 3-1 shows an example gateway installation.

Figure 3-1. Gateway Installation

A. Control Room
B. Ground
C. Gateway

D. Mast or Pipe
E. Infrastructure
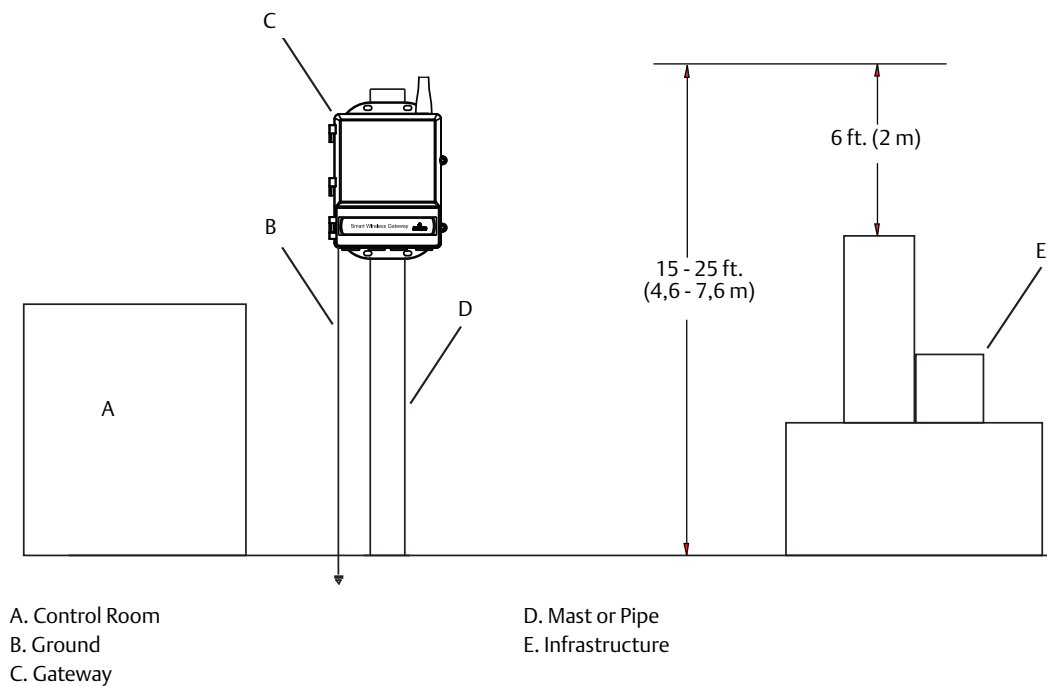
3.2.1   Pipe mount

The following hardware and tools are needed to mount the Gateway to a 2-in. pipe:

- Two $^5/_{16}$-in. u-bolts (supplied with Gateway)
- 2-in. mounting pipe
- ½-in. socket-head wrench

Mount the Gateway using the following procedure:

1. Insert one u-bolt around the pipe, through the top mounting holes of the Gateway enclosure, and through the washer plate.

2. Use a $^1/_2$-in. socket-head wrench to fasten the nuts to the u-bolt.

3. Repeat for the second u-bolt and the lower mounting holes.

Figure 3-2. Pipe Mount
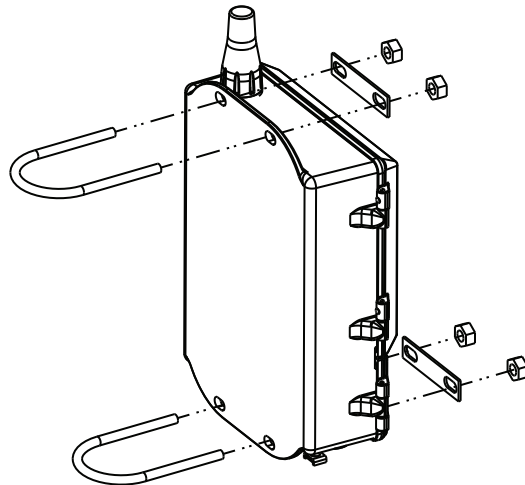
3.2.2   Bracket mount (alternate)

The following hardware and tools are needed to mount the Gateway to a support bracket:

- Four $^{15}/_{16}$-in. bolts
- Mounting support bracket
- $^3/_8$-in. drill
- $^1/_2$ -in. socket-head wrench

Mount the Gateway using the following procedure:

1. Drill four $^3/_8$-in. (9,525 mm) holes spaced 3.06-in. (77 mm) apart horizontally and 11.15-in. (283 mm) apart vertically in the support bracket, corresponding with the holes on the Gateway enclosure.

2. Using a $^1/_2$-in. socket-head wrench, attach the Gateway to the support bracket with four $^{15}/_{16}$-in. bolts.

3.3   Remote antenna (optional)

The remote antenna options provide flexibility for mounting the Gateway based on wireless connectivity, lightning protection, and current work practices.

⚠ WARNING

When installing remote mount antennas for the Smart Wireless Gateway, always use established safety procedures to avoid falling or contact with high-power electrical lines.

Install remote antenna components for the Smart Wireless Gateway in compliance with local and national electrical codes and use best practices for lightning protection.

Before installing consult with the local area electrical inspector, electrical officer, and work area supervisor.

The Smart Wireless Gateway remote antenna option is specifically engineered to provide installation flexibility while optimizing wireless performance and local spectrum approvals. To maintain wireless performance and avoid non-compliance with spectrum regulations, do not change the length of cable or the antenna type.

If the supplied remote mount antenna kit is not installed per these instructions, Emerson Process Management is not responsible for wireless performance or non-compliance with spectrum regulations.

The remote mount antenna kit includes coaxial sealant for the cable connections for the lightning arrestor and antenna.

Find a location where the remote antenna has optimal wireless performance. Ideally this will be 15-25 ft (4,6 - 7,6 m) above the ground or 6 ft (2 m) above obstructions or major infrastructure. To install the remote antenna use one of the following procedures:

Installation of WL2/WN2 option (outdoor applications)

1.   Mount the antenna on a 1.5-2 inch pipe mast using the supplied mounting equipment.

2.   Connect the lightning arrestor directly to the top of the Gateway.

3.   Install the grounding lug, lock washer, and nut on top of the lightning arrestor.

4.   Connect the antenna to the lightning arrestor using the supplied coaxial cable ensuring the drip loop is not closer than 1 foot (0,3 m) from the lightning arrestor.

5.   Use the coaxial sealant to seal each connection between the wireless field device, lightning arrestor, cable, and antenna.

6.   Ensure the mounting mast, lightning arrestor, and Gateway are grounded according to local/national electrical code.

Note
Any spare lengths of coaxial cable should be placed in 12 inch (0,3 m) coils.

Figure 3-3. Installation of WL2/WN2 Option

A. Control Building
B. Remote Antenna
C. Cable
D. Drip Loop

E. Lightning Arrestor
F. Gateway
G. Ground
H. Earth

Installation of WL3/WL4 Option (indoor to outdoor applications)

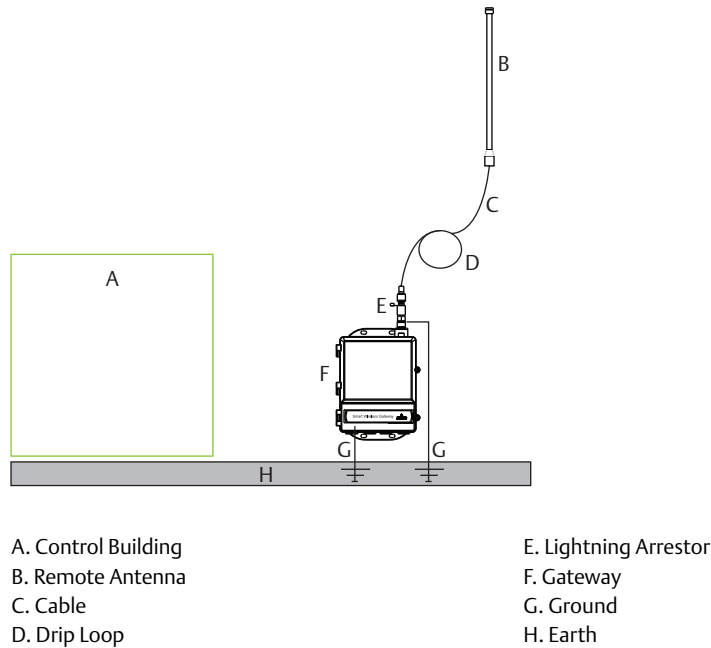1.   Mount the antenna on a 1.5-2 inch pipe mast using the supplied mounting equipment.

2.   Mount the lightning arrestor near the building egress.

3.   Install the grounding lug, lock washer, and nut on top of lightning arrestor.

4.   Connect the antenna to the lightning arrestor using the supplied coaxial cable ensuring the drip loop is not closer than 1 foot (0,3 m) from the lightning arrestor.

5.   Connect the lightning arrestor to the Gateway using the supplied coaxial cable.

6.   Use the coaxial sealant to seal each connection between the Gateway, lightning arrestor, cable, and antenna.

7.   Ensure that the mounting mast, lightning arrestor, and Gateway are grounded according to local/national electrical codes.

Note
Any spare lengths of coaxial cable should be placed in 12 inch (0,3 m) coils.

Figure 3-4. Installation of WL3/WL4 Option
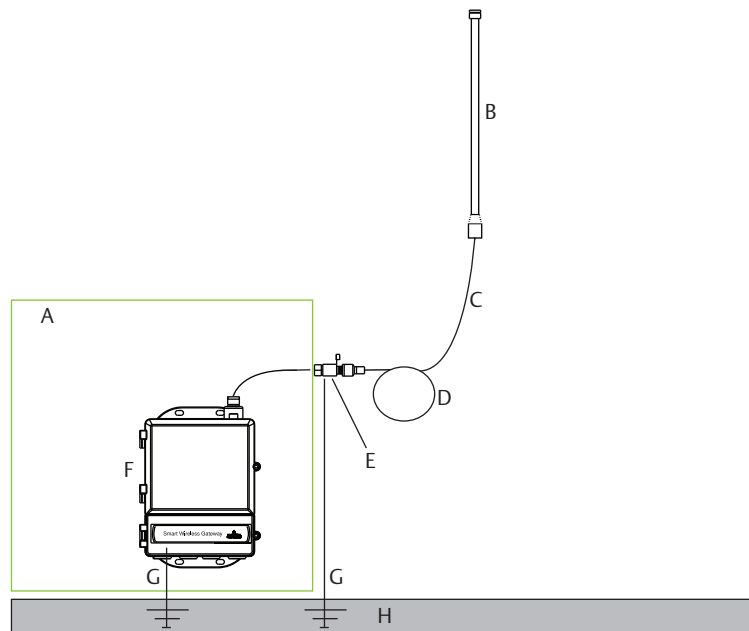
A. Control Building
B. Remote Antenna
C. Cable
D. Drip Loop

E. Lightning Arrestor
F. Gateway
G. Ground
H. Earth

Note: Weather proofing is required!
The remote mount antenna kit includes coaxial sealant for the cable connections for the lightning arrestor, antenna, and Gateway. The coaxial sealant must be applied to guarantee performance of the wireless field network. See Figure 3-5 for details on how to apply weather proofing.

Figure 3-5. Applying Coaxial Sealant to Cable Connections
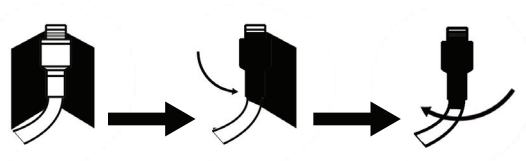
Table 3-1. Remote Antenna Kit Options

Kit option	Antenna	Cable 1	Cable 2	Lightning arrestor
WL2	$^1/_2$ Wavelength Dipole Omni-Directional +6 dB Gain	50 ft. (15,2 m) LMR-400	N/A	Head mount, jack to plug Gas discharge tube 0.5 dB insertion loss
WL3	$^1/_2$ Wavelength Dipole Omni-Directional +6 dB Gain	30 ft. (9,1 m) LMR-400	20 ft. (6,1 m) LMR-400	In-line, jack to jack Gas discharge tube 0.5 dB insertion loss
WL4	$^1/_2$ Wavelength Dipole Omni-Directional +6 dB Gain	40 ft. (12,2 m) LMR-400	10 ft. (3,0 m) LMR-400	In-line, jack to jack Gas discharge tube 0.5 dB insertion loss
WN2	$^1/_2$ Wavelength Dipole Omni-Directional +8 dB Gain	25 ft. (7,6 m) LMR-400	N/A	Head mount, jack to plug Gas discharge tube 0.5 dB insertion loss

3.4 Connecting

All connections to the Gateway can be made at the terminal block, which is located in the lower junction box section of the enclosure. The terminal block label is located on the inside of the lower cover. See Figure 3-6 for the standard terminal block label.

The junction box portion of the enclosure has four conduit entries for power and communications wiring. Do not run communication wiring in conduit or open trays with power wiring, or near heavy electrical equipment.

Install the included conduit plugs in any unused conduit openings. For NEMA® 4X and IP65 requirements, use thread seal (PTFE) tape or paste on male threads to provide a watertight seal.

3.4.1 Grounding

The Gateway enclosure case should always be grounded in accordance with national and local electrical codes. The most effective grounding method is a direct connection to earth ground with minimal impedance. Ground the Gateway by connecting the external grounding lug to earth ground. The connection should be 1 Ω or less. The external ground lug is located below the Gateway enclosure and is identified by the following symbol:

3.4.2 Ethernet

The Gateway is equipped with two 10/100BaseTX Ethernet communications ports (see Figure 3-6). These connections can be used to access the Gateway's web interface and to communicate Modbus TCP and OPC protocols.

The primary Ethernet port (Ethernet 1) is used to connect to the host system or other application systems. The secondary Ethernet port (Ethernet 2) can be used as a back up connection or a maintenance port for local access to the Gateway.

Figure 3-6. Terminal Block Diagram
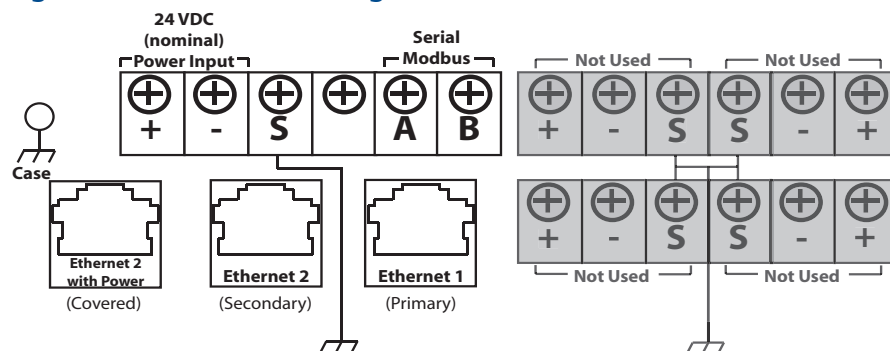
Ethernet connections should use Cat5E shielded cable to connect to an Ethernet hub, switch, or router. The maximum cable length should not exceed 328 ft. (100 m).

Note
Unless dual Ethernet ports were specified at the time of order, the secondary Ethernet port (Ethernet 2) will not be active.

3.4.3 RS-485

The Gateway may be ordered with an optional RS-485 (serial) connection (Figure 3-6). It is referenced by the A and B Serial Modbus terminals. This connection is used to communicate Modbus RTU on an RS-485 data bus.

Use 18 AWG single twisted shielded pair wiring to connect the Gateway to the RS-485 data bus. The total bus length should not exceed 4000 ft. (1220 m). Connect the Tx + (positive, transmit) wire to terminal A and the Rx - (negative, receive) wire to terminal B. The wiring shield should be trimmed close and insulated from touching the Gateway enclosure or other terminations.

If the existing data bus uses a 4 wire Full Duplex configuration, see Figure 3-7 to convert to a 2-wire Half Duplex configuration.
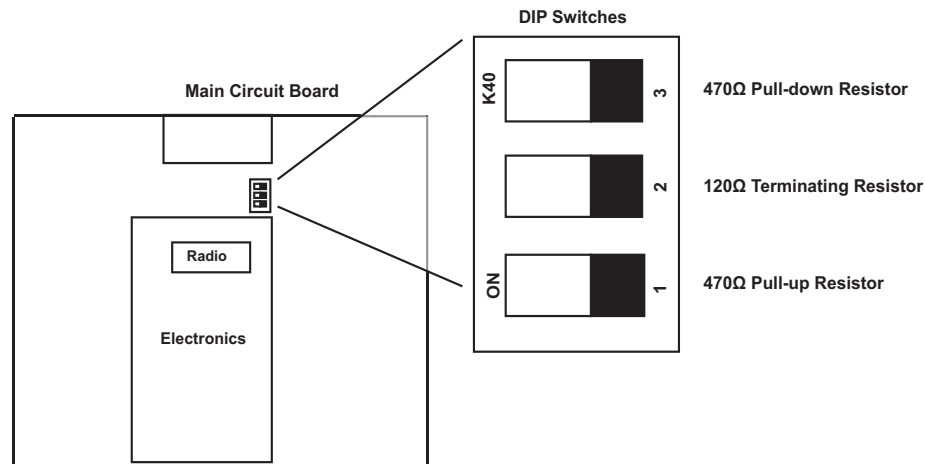
Figure 3-7. Convert from Full to Half Duplex
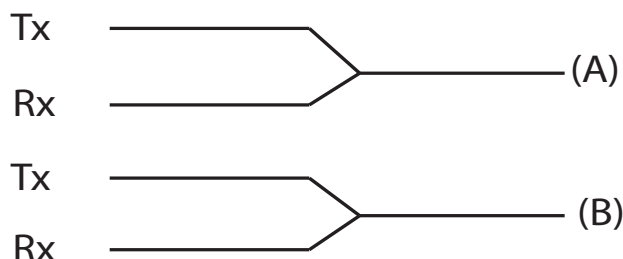
3.4.4   Terminating resistors

Three DIP switches are provided to enable various terminating resistors to the RS-485 data bus. The switches are found inside the electronics housing near the top center of the main circuit board (Figure 3-8).

Figure 3-8. RS-485 Resistor DIP Switches

Switches 1 and 3 are connected to pull-up and pull down resistors. Switch 1 is for the Tx + (A) line and Switch 3 is for the Rx – (B) line. These 470 Ù resistors are used to prevent noise from being interpreted as valid communications during periods when no actual communications are occurring. Only one set of pull-up and pull-down resistors should be active on the RS-485 data bus at time.

Switch 2 is connected to a 120 Ω terminating resistor. This resistor is used to dampen signal reflections on long cable runs. RS-485 specifications indicate that the data bus should be terminated at both ends (Figure 3-9). However termination should only be used with high data rates (above 115 kbps) and long cable runs.

Figure 3-9. Typical Half Duplex (2-wire) Network
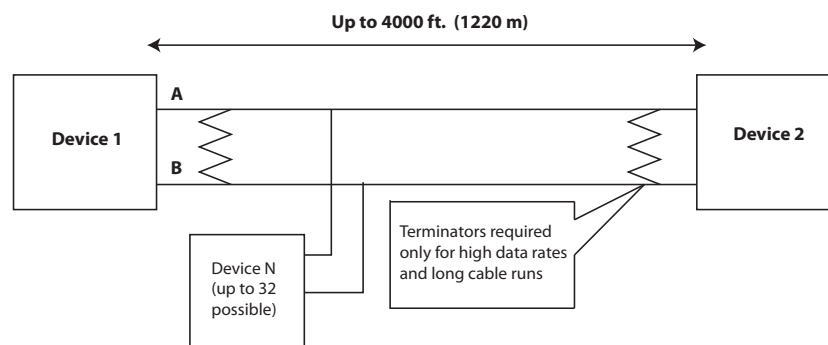
3.4.5 Power

The Gateway is designed to be powered by 24 VDC (nominal) and requires 250 mA of current. The positive and negative connections are found on the left side of the terminal block (Figure 3-6). An additional case ground is found on the left side of the junction box enclosure.

Connect supply power to the positive + and negative – power terminals found on the left side of the terminal block (Figure 3-6). Recommended torque is 7 in-lbs and the gauge is 12 to 22 AWG. An additional internal case ground can be found on the left side of the enclosure. The wiring should include an external power shut-off switch or circuit breaker that is located near the Gateway.

Note
Using an uninterruptible power supply (UPS) is recommended to ensure availability should there be a loss of power.

Section 4 Software Setup

4.1 Overview

This section discusses the installation and setup of the optional software included with the Smart Wireless Gateway. This software is not required for the wireless field network to operate; however, it will aid in secure host integration as well as wireless field device configuration. The following table describes what items are installed and on which disk they can be found.

Table 4-1. Software Applications

Name	Description	Location
Security Setup Utility	This utility allows the setup of SSL enabled communications between the Gateway and host system.	Disk 1
AMS® Wireless Configurator	This application allows complete configuration of wireless field devices and provides added security through drag and drop provisioning.	Disk 2
Network Configuration	This application configures AMS Wireless Configurator to interface to a Wireless Network or a HART® Modem.	Disk 2

Additional system components may be installed depending on the current configuration of the system.

4.2   System requirements

Table 4-2. PC Hardware

Minimum requirements	Recommended requirements
Intel™ Core 2 Duo, 2.0 GHz	Intel Core 2 Quad, 2.0 GHz or greater
1 GB Memory	3 GB Memory or Greater
1.5 GB free hard disk space	2 GB or more of free hard disk space

Note
Additional hard disk space is required for SNAP-ON™ applications. The minimum monitor requirements are 1024 x 768 resolution and 16-bit color.

Table 4-3. Supported Operating Systems

Operating system	Version
Windows™ XP	Professional, Service Pack 3
Windows Server 2003	Standard, Service Pack 2
Windows Server 2003 R2	Standard, Service Pack 2
Windows Server 2008	Standard, Service Pack 2
Windows Server 2008 R2	Standard, Service Pack 1
Windows 7	Professional, Service Pack 1
Windows 7	Enterprise, Service Pack 1

Note
Only 32-bit versions of the operating systems are supported for AMS Wireless Configurator.

4.3 Software installation

The software can be found on the 2 disk pack, included with the Gateway. Depending on the PC system configuration, installation may take 30-35 minutes. Installing both disks in order is recommended. The Security Setup Utility is located on Disk 1. To install the software:

1.   Exit/close all Windows programs, including any running in the background, such as virus scan software.

2.   Insert Disk 1 into the CD/DVD drive of the PC.

3.   Follow the prompts.

AMS Wireless Configurator is located on Disk 2. To install the software:

1.   Exit/close all Windows programs, including any running in the background, such as virus scan software.

2.   Insert Disk 2 into the CD/DVD drive of the PC.

3.   Select **Install** from the menu when the AMS Wireless Configurator setup begins.

4.   Follow the prompts.

5.   Allow AMS Wireless Configurator to reboot PC.

6.   Do not remove the disk from the CD/DVD drive.

7.   Installation will resume automatically after login.

8.   Follow the prompts.

Note
If the autorun function is disabled on the PC, or installation does not begin automatically, double click D:\SETUP.EXE (where D is the CD/DVD drive on the PC) and select OK.

4.4 Security Setup Utility

The Security Setup Utility enables secure communications between the Gateway and host system, asset management software, data historians, or other applications. This is done by encrypting the standard data protocols (AMS Wireless Configurator, Modbus TCP, Ethernet/IP™, and OPC) used by the Gateway and making them available through various proxies within the Security Setup Utility. These proxies can function as a data server for other applications on the control network. The Security Setup Utility can support multiple Gateways at once and each proxy can support multiple client application connects. Figure 4-1 shows a typical system architecture using the Security Setup Utility.

Figure 4-1. Typical Host System Architecture Using Security Setup
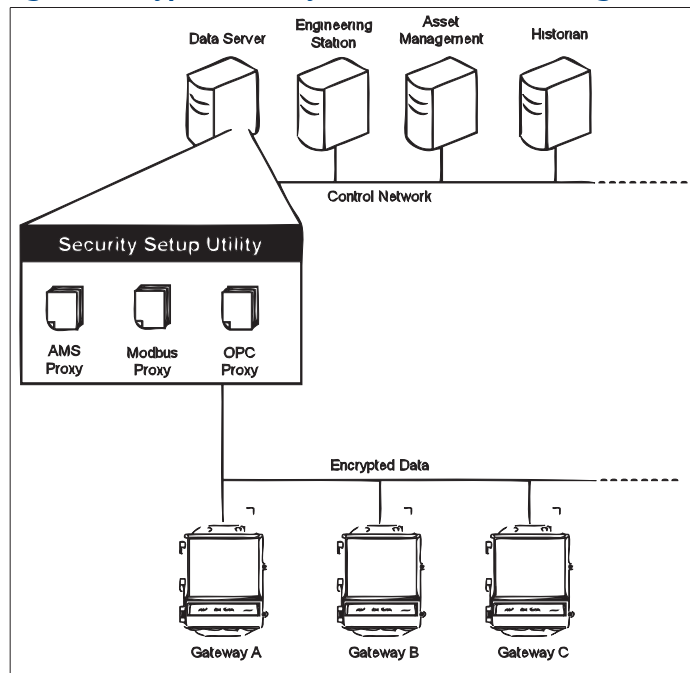
Note
OPC communications requires the use of the Security Setup Utility regardless of whether encryption is required.

4.4.1   Setup

In the Security Setup Utility add a new proxy for each Gateway based on the communication protocol that is being used. For example, add an OPC proxy for each Gateway that is communicating OPC.

Use the following procedure to add a new proxy in the Security Setup Utility:

1.   Open the Security Setup Utility.

2.   Select **EDIT>NEW**, then select the type of new proxy to be added.

3.   Right click on the new proxy entry and select **Properties**.

4.   Enter the target Gateway's Hostname and IP Address.

5.   Select **OK**.

6.   Select **FILE>SAVE**.

7.   When prompted for authentication, enter the admin password for the target Gateway.

8.   Select **OK**.

9.   Repeat Step 2-Step 8 to added additional proxies.

10.   Select **FILE>EXIT** to close the Security Setup Utility.

During this process, the Gateway will exchange security certificates (digital signatures) with the proxy.

Figure 4-2. Security Setup Utility
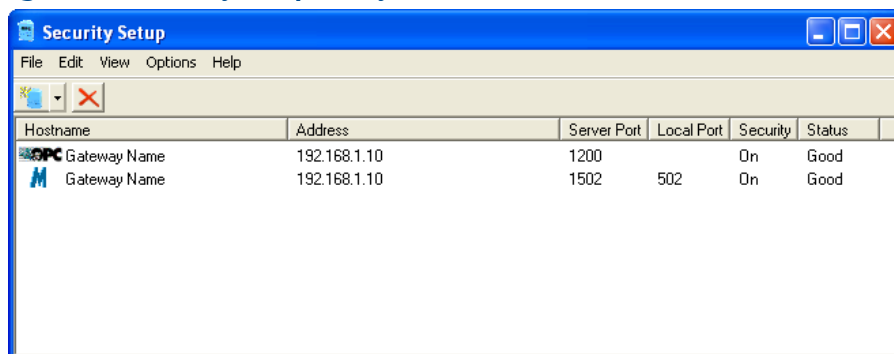
4.5   AMS Wireless Configurator

AMS Wireless Configurator helps deploy and configure wireless field devices. It provides an integrated operating environment that leverages the full capabilities of WirelessHART®, including embedded data trending, charting, and graphical display capabilities provided by enhanced EDDL technology.

- Display and modify device configuration
- View device diagnostics
- View process variables
- Provision a wireless device using the drag-and-drop operation so it can join a Gateway's self-organizing network
- Enhance AMS Wireless Configurator functionality with the AMS Wireless SNAP-ON Application
- Restrict access to AMS Wireless Configurator functions through the use of security permissions

See the release notes for information specific to the current release of AMS Wireless Configurator. To display the release notes, select **START>PROGR>AMS WIRELESS CONFIGURATOR>HELP**.

4.5.1   Setup

AMS Wireless Configurator supports connectivity to a Wireless Network and a HART Modem. Both of these interfaces must be configured through the Network Configuration application. To run this application, select **START>PROGR>DEVICE MANAGER>NETWORK CONFIGURATION**.

Note
Do not have the Security Setup Utility running at the same time as the Network Configuration application or a configuration error might occur.

Use the following procedure to configure a wireless network for AMS Wireless Configurator:

1.   Open the Network Configuration application.

2.   Select **Add.**

3.   Select **Wireless Network** and select **Install.**

4.   Select **Next**.

5.   Enter a name for the wireless network and select **Next**.

6.   Enter the HostName or IP Address for the Gateway and select **Add**.

7.   Repeat Step 6 if multiple Gateways need to be added.

8.   Check the box to *Enable Secure Communications with the Smart Wireless Gateway.*

9.   Select **Finish** to close the configuration window.

10.   Select **Close** to exit the Network Configuration application.

Figure 4-3. Wireless Network in the Network Configuration
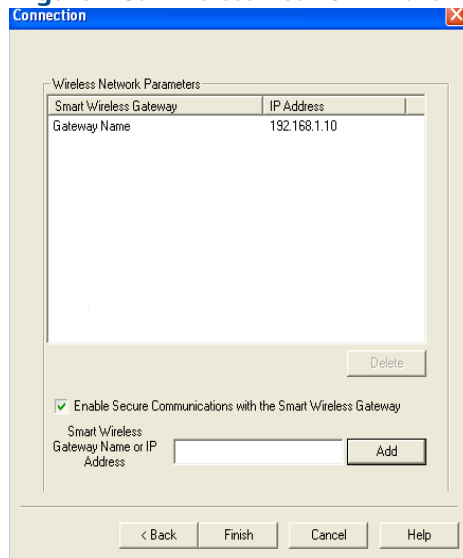
Use the following procedure to configure a HART modem for AMS Wireless Configurator:

1.   Open the Network Configuration application.

2.   Click **Add...**

3.   Select **HART modem** and click **Install...**

4.   Click **Next**.

5.   Enter a name for the HART modem and click **Next**.

6.   Select the *HART master type* (default is AMS Wireless Configurator will be Primary HART master) and click **Next**.

7.   Select the *COM port for the HART modem* and click **Next**.

8.   Check the box to *Check to support Multi Drop* devices.

9.   Check the box to *Include WirelessHART Adapter.*

10.   Click **Finish** to close the configuration window.

11.   Click **Close** to exit the Network Configuration application.

4.6   Licensing and credits

The latest licensing agreements are included on each disk of the software pack.

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

"This product includes software written by Eric Young (eay@cryptsoft.com)"

Section   5   Host Integration

5.1   Overview

This section describes how to connect the Gateway to a host system and integrate data gathered from the field device network. It covers network architectures, security, and data mapping.

In accordance with Emerson *Wireless*HART® security guidelines, the Emerson Gateway should be connected to the host system via a LAN (Local Area Network) and not a WAN (Wide Area Network).

5.2   Network architecture

Physical connection types are important when determining the network architecture and what protocols can be used for integration. Ethernet is the primary physical connection type and RS-485 is available an optional connection type. The following network architecture diagrams will help when integrating data from the Gateway into the host system.

Ethernet

An Ethernet connection supports Modbus® TCP, OPC, AMS® Wireless Configurator, Ethernet/IP™, and HART® TCP protocols. Using this connection type, the Gateway is wired directly to a control network (see Figure 5-1) using a network switch, router, or hub. There are often two networks for redundancy purposes.

Figure 5-1. Ethernet LAN Architecture
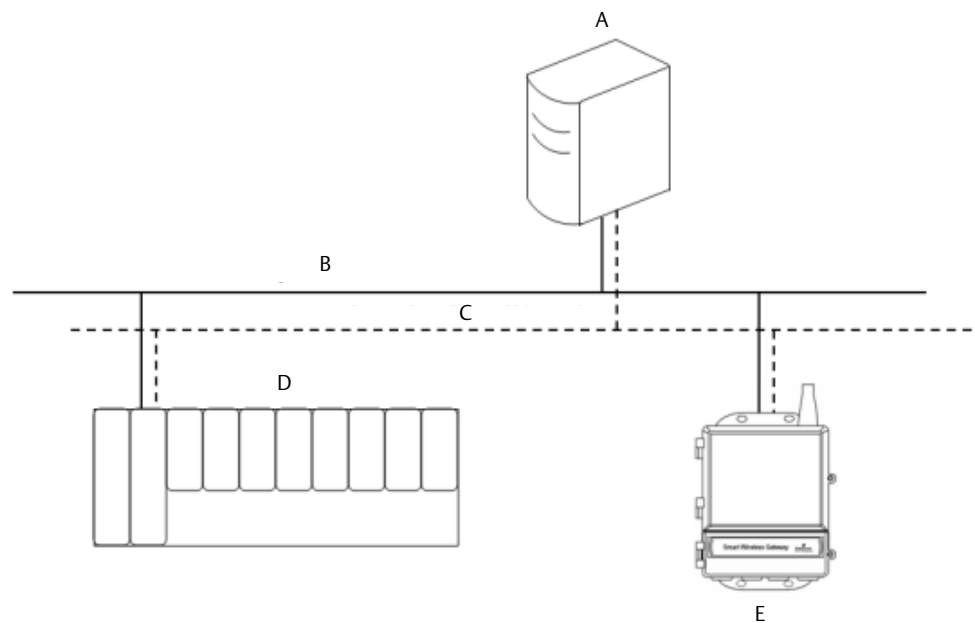
A. Engineering Station
B. Primary Control Network
C. Secondary Control Network

D. Controller and I/O
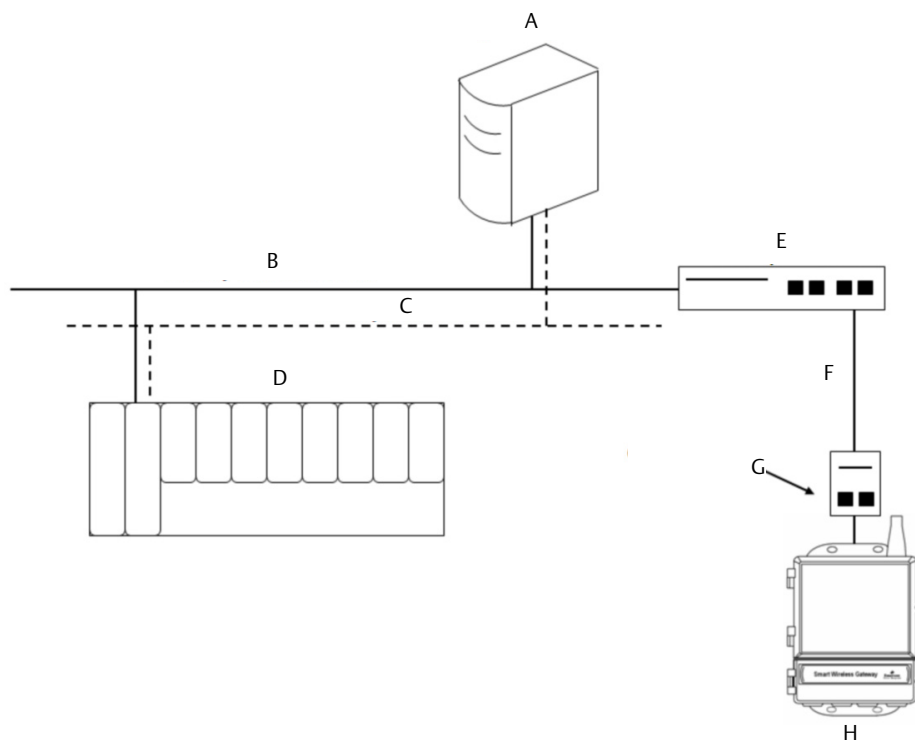E. Smart Wireless Gateway

Fiber optic (optional)

A Fiber optic connection supports Modbus TCP, OPC, AMS Wireless Configurator, and HART TCP protocols. Using this connection type, the Gateway is wired to a fiber optic switch (see Figure 5-2).

Note
A fiber optic connection requires a third party copper Ethernet to fiber optic Ethernet converter.

Figure 5-2. Fiber Optic LAN Architecture

A. Engineering Station	E. Fiber Optic Switch
B. Primary Control Network	F. Fiber Optic
C. Secondary Control Network	G. Copper to Fiber Converter
D. Controller and I/O	H. Smart Wireless Gateway

RS-485 (serial)

An RS-485 connection supports Modbus RTU protocol. Using this connection type, the Gateway is wired to an RS-485 bus which typically leads to a serial I/O card or Modbus I/O card (see Figure 5-3). Up to 31 Gateways can be connected to a single I/O card in this manner.

Figure 5-3. RS-485 LAN Architecture
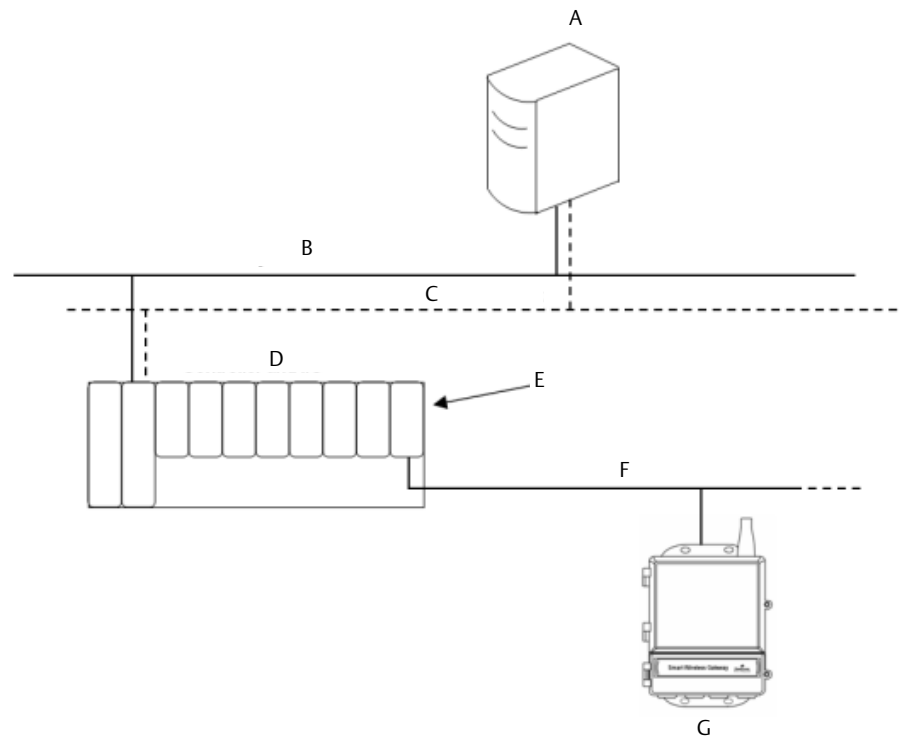
A. Engineering Station
B. Primary Control Network
C. Secondary Control Network
D.Controller and I/O

E Serial I/O Card
F. RS485 Bus
G. Smart Wireless Gateway

5.3 Internal firewall

The Gateway supports an internal firewall that inspects both incoming and outgoing data packets. TCP ports for communication protocols are user configurable, including user specified port numbers and the ability to disable ports.

The Gateway's internal firewall settings can be found by navigating to **System Settings> Protocols>Protocols and Ports**.

Figure 5-4. Security Protocols Page (Internal Firewall)

5.4 Modbus

The Gateway supports both Modbus RTU over the RS-485 serial port and Modbus TCP over Ethernet. It functions as a sub device on the Modbus network and must be polled by a Modbus master or client (host system).

5.4.1 Communication settings

It is import that the Modbus communication settings in the Gateway match the setting in the Modbus master or client. Please refer to host system documentation for more information on how to configure these settings. The Modbus communication settings can be found by navigating to **System Settings>Protocols>Modbus**.

Figure 5-5. Modbus Communications Page

One Modbus Address: When this option is selected, this address is used by the Gateway for Modbus RTU communications.

Multiple Modbus Addresses: When this option is selected, a new column for address will appear on the Modbus mapping page.

Modbus TCP Port: This is the TCP/IP port the Gateway uses for Modbus TCP (Ethernet). To change TCP/IP port settings, see the Internal Firewall section for more details.

Baud Rate: The data rate or speed of serial communications. This setting is only required for Modbus RTU.

Parity: This setting determines parity (none, even, or odd) to use for error checking purposes. This setting is only required for Modbus RTU.

Stop Bits: This setting determines the number (1 or 2) of stop bits to use when ending a message. This setting is only required for Modbus RTU.

Response delay time (ms): This setting determines how long (ms) the Gateway waits before responding to a Modbus request. This setting is only required for Modbus RTU.

Unmapped register read response?: This is the value returned by the Gateway if the Modbus master requests a register with no data assigned to it (empty register). It is recommended this be set to zero fill to prevent errors.

Floating point representation: This setting determines if the Gateway uses floating point values or integer values. There are three options for this setting.

- *Float* uses 32 bit floating point values.
- *Round* rounds the data value to the nearest whole number.
- *Scaled* uses scaled integers to offset negative values or increase decimal point resolution. The equation for scaled integers is:

$$y = Ax - (B - 32768)$$

Where:

y = Scaled integer returned by the Gateway

A = Gain for scaled integer value

x = Measured value from wireless field device

B = Offset for scaled integer value

Use swapped floating point format?: This setting switches which register is sent first for a floating point value. This setting is only used for floating point values.

Incorporate value's associated status as error?: This setting will cause the Gateway to report a predetermined value when a communications or critical diagnostic error is received from the wireless field device. The value is user configurable depending on which floating point representation is chosen. See Value reported for error below.

Value reported for error (floating point): This setting determines what value is reported if the wireless field device reports a failure or stops communicating to the Gateway. This setting is used for floating point values. The choices are NaN (not a number), +Inf (positive infinity), -Inf (negative infinity), or Other (user specified).

Value reported for error (rounded and native integer): This setting determines what value is reported if the wireless field device reports a failure or stops communicating to the Gateway. This setting is used for rounded or scaled integers. The choice is a user specified value between -32768 and 65535.

Scaled floating point maximum integer value: This determines the maximum integer value for the purpose scaling integers. 999-65534

Use global scale gain and offset?: This setting determines if a global gain and offset is applied for scaled integers or if each value has a unique gain and offset. Unique gain and offsets are found on the Modbus Mapping page.

Global scale gain: This value is multiplied to the data values for the purpose of scaling integers. If global scaling is not selected, a gain value will be available for each separate data value on the Modbus Mapping page.

Global scale offset: This value is added to the data values for the purpose of scaling integers. If global scaling is not selected, an offset value will be available for each separate data value on the Modbus Mapping page.

5.4.2 Register mapping

Register Mapping is the process of assigning data points from wireless field devices to Modbus registers. These registers can then be read by a Modbus master or client. Modbus register mapping can be found by navigating to System Settings>Protocols>Modbus.

Figure 5-6. Modbus Register Map Page

To add a new data point to the Modbus register map:

1.   Select **Add New entry**.

2.   Complete all of the table entries for the new data point (note that the entry columns may vary based on the Modbus communications settings).

3.   Repeat for each new data point.

4.   Select **Submit**.

5.   When changes have been accepted, select **Return to form**.

Address: This is the Modbus RTU address used by the Gateway for this data point. It is possible to group data points assigning them the same address (i.e. all data points from the same process unit can have the same address). This column only appears if Multiple Modbus Addresses is selected on the Modbus Communications page.

Register: This is the Modbus register number used for this data value. Modbus registers hold two bytes (16 bits) of information; therefore 32 bit floats and integers require two Modbus registers. Each data point needs a unique Modbus register number, unless they are assigned different addresses. Register numbers 0-19999 are reserved for Boolean (bit, coil, binary, etc…) values. Register numbers 20000+ are reserved for floating point or integer values.

Point Name: This is a two part name for the data point. The first part is the HART Tag of the wireless field device which is producing the data. The second part is the parameter of the wireless field device.

Note
Point Name is entered as *<HART Tag.PARAMETER>*. Point Name can be entered using the list of values (…) or manually entered. The following table gives a list of standard device parameters which may be considered for Modbus register mapping.

Table 5-1. Device Parameters Available

Parameter	Description	Data type
PV	Primary Variable	32-bit float
SV	Secondary Variable	32-bit float
TV	Tertiary Variable	32-bit float
QV	Quaternary Variable	32-bit float
RELIABILITY	A measure of connectivity to the Gateway	32-bit float
ONLINE	Wireless communications status	Boolean
PV_HEALTHY	Health status for PV	Boolean
SV_HEALTHY	Health status for SV	Boolean
TV_HEALTHY	Health status for TV	Boolean
QV_HEALTHY	Health status for QV	Boolean

PV, SV, TV, and QV (dynamic variables) will vary by device type. Please refer to the device's documentation for more information on what value is represented by each dynamic variable.

RELIABILITY and ONLINE relate to wireless communications. RELIABILITY is the percentage of messages received from the wireless field device. ONLINE is a true/false indication of whether the device is communicating on the wireless network.

****_HEALTHY parameters are a true/false indication of the health of a particular variable (**** = dynamic variable – PV, SV, etc…). These parameters incorporate critical diagnostics from the wireless field device as well as communication status.

Note
The **_HEALTHY parameters are a great indication of the health and communications status of the data values.

State (state value): The value of a data point which drives a Modbus output of 1. For example, if a data point is reported as either True or False, a state value of True will report a 1 for True and 0 for False. A state of False will report a 0 for True and a 1 for False. State is only required for register numbers 0-19999 (Boolean, bit, coil, binary, etc...).

Invert: This check box will invert the Modbus output from a 1 to a 0 or a 0 to a 1. Invert is only used for Boolean values using register numbers 0-19999.

Gain: This value is multiplied to the data value for the purpose of scaling integers. Gain is only required if scaled is chosen on the Modbus communications page and globe gain and offset is not chosen.

Offset: This value is added to the data value for the purpose of scaling integers. Offset is only required if scaled is chosen on the Modbus communications page and globe gain and offset is not chosen.

Predefined Modbus registers

In addition to user configurable parameters, the Gateway also supports a list of predefined Modbus registers with diagnostics and test parameters. The following table is a list of the predefined Modbus registers.

Table 5-2. Predefined Modbus Registers

Description	Register	Data type
Current Year (1)	49001	32-bit int
Current Month (1)	49002	32-bit int
Current Day (1)	49003	32-bit int
Current Hour (1)	49004	32-bit int
Current Minute (1)	49005	32-bit int
Current Second (1)	49006	32-bit int
Messages Received	49007	32-bit int
Corrupt Messages Received	49008	32-bit int
Messages Sent With Exception	49009	32-bit int
Messages Sent Count	49010	32-bit int
Valid Messages Ignored	49011	32-bit int
Constant Float 12345.0	49012	32 float
SYSTEM_DIAG.HART_DEVICES	49014	32-bit int
SYSTEM_DIAG.ADDITIONAL_STATUS_0	49015	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_1	49016	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_2	49017	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_3	49018	8-bit unsigned int

Table 5-2. Predefined Modbus Registers

Description	Register	Data type
SYSTEM_DIAG.ADDITIONAL_STATUS_4	49019	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_5	49020	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_6	49021	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_7	49022	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_8	49023	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_9	49024	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_10	49025	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_11	49026	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_12	49027	8-bit unsigned int
SYSTEM_DIAG.UNREACHABLE	49028	32-bit int
SYSTEM_DIAG.UPTIME	49029	32-bit int
SYSTEM_DIAG.TEST_BOOLEAN	49031	Boolean
SYSTEM_DIAG.TEST_BYTE	49032	8-bit int
SYSTEM_DIAG.TEST_UNSIGNED_BYTE	49033	8-bit unsigned int
SYSTEM_DIAG.TEST_SHORT	49034	16-bit int
SYSTEM_DIAG.TEST_UNSIGNED_SHORT	49035	16-bit unsigned int
SYSTEM_DIAG.TEST_INT	49036	32-bit int
SYSTEM_DIAG.TEST_UNSIGNED_INT	49038	32-bit unsigned int
SYSTEM_DIAG.TEST_FLOAT	49040	32-bit float

5.5 Ethernet/IP

Communication settings

It is important that the Ethernet/IP communication settings in the Gateway match the setting in the Ethernet/IP master or client. Please refer to host system documentation for more information on how to configure these settings. Or to the reference manual for Ethernet/IP technical document 00809-0500-4420. The Ethernet/IP communication settings can be found by navigating to System Settings>Protocols>EtherNet/IP. Network architectures should reflect that of a DeltaV system see 00809-0200-4420, Rev HB.

Note
Ethernet/IP can be integrated with any approved Ethernet/IP ODVA member. Other protocols such as HARTIP are still functional within the Gateway. See the Product Data Sheet (document number 00813-0200-4420) for ordering options.

Figure 5-7. Ethernet/IP Communications Page

Table 5-3. System Settings>Protocols>EtherNet/IP

Terms	Description
Assembly Object Type	Ethernet/IP use Static assembly object.
Ethernet/IP TCP Port	The TCP Port used to access Ethernet/IP TCP data directly from the Gateway.
Ethernet/IP UDP Ports	The UDP Ports used to access Ethernet/IP UDP data directly from the Gateway.
Incorporate value's associated status as error?	If the HART variable status indicates a critical failure or if there is a loss of communications, it will be reported through the Ethernet/IP member.
Value reported for error (floating point)	Chooses what value is reported if the value's associated status indicates a critical failure. Only used if the Gateway is using float representation
NaN	Not a number is reported if the value's associated status indicates a critical failure.
+Inf	Positive infinity is reported if the value's associated status indicates a critical failure.
-Inf	Negative infinity is reported if the value's associated status indicates a critical failure.
Other	User defined value is reported if the value's associated status indicates a critical failure.
Value reported for error (native integer)	User defined value is reported if the value's associated status indicates a critical failure. Only used if the Gateway is using integer representation.

Unmapped parameter read response?: This is the value returned by the Gateway if the Ethernet/IP master requests a register with no data assigned to it (empty register). It is recommended this be set to zero fill to prevent errors.

Parameter mapping

Register Mapping is the process of assigning data points from wireless field devices to Ethernet/IP registers. These registers can then be read by a Ethernet/IP master or client. Ethernet/IP register mapping can be found by navigating to System Settings>Protocols> EtherNet/IP>EtherNet/IP Member Map.

Figure 5-8. Ethernet/IP Register Map Page

Table 5-4. Summary of Terms Used for the Ethernet/IP Mapping Page

Terms	Description
Input Instance	Ethernet/IP Input Static Assembly Instance - 496 bytes
Output Instance	Ethernet/IP Output Static Assembly Instance - 496 bytes
Member	Ethernet/IP Instance Member in which data will get produced or consumed
Point Name	Assigned data point in the format HARTtag.parameter
New entry	Creates a new entry in this table
<<First	Navigates to the first page of this table
<<Previous	Navigates to the previous page of this table
Search	Finds the next occurrence of the characters entered into this field

Table 5-4. Summary of Terms Used for the Ethernet/IP Mapping Page

Terms	Description
Next>>	Navigates to the next page of this table
Last>>	Navigates to the last page of this table
Delete Selected	Removes the selected entry from this table
Select All	Selects all table entries
Select None	De-selects all table entries
Select Errors	Selects all table entries that have an error message
Submit	Accepts all changes (highlighted in yellow)

To add a new data point to the Ethernet/IP register map:

1.   Select New entry.

2.   Complete all of the table entries for the new data point (note that the entry columns may vary based on the Ethernet/IP communications settings).

3.   Repeat for each new data point.

4.   Select Submit.

5.   When changes have been accepted, select Return to form.

See Table 5-1 on page 39 for options of parameters that can be mapped.

Section 6 Troubleshooting

Note
For more information see the user interface terminology guide (document number 00809-0600-4420).

This section provides basic troubleshooting tips for the Smart Wireless Field Network. To receive technical support by phone:

Global Service Center
Software and Integration Support

United States 1 800 833 8314
International   63 2 702 1111

Customer Central
Technical Support, quoting, and order related questions

United States 1 800 999 9307 (7:00 a.m. to 7:00 p.m. CST)
Asia Pacific   65 6777 8211
Europe/Middle East/Africa 49 8153 9390

Or email the wireless specialists at: *Specialists-Wireless.EPM-RTC@EmersonProcess.com*

Table 6-1. Troubleshooting Initial Connection

Issue	Troubleshooting steps
Web browser returns page not found	1. Connect the Gateway and PC/laptop 2. Verify the Gateway is properly powered, 24 VDC (nominal) and 250 mA. Open the upper cover and verify if any indicator lights are on. 3. Verify which Ethernet port is being used on the Gateway. 4. Verify the IP address for the Gateway (default primary port is 192.168.1.10, default secondary port is 192.168.2.10 or for DeltaV Ready Gateway's default primary port is 10.5.255.254, default secondary port is 10.9.255.254). 5. Verify the IP address of the PC/laptop is in the same subnet range as the Gateway (i.e. If the Gateway IP is 155.177.0.xxx, then the PC/Lap IP address should be 155.177.0.yyy). 6. Disable internet browser proxy settings.
Can not find Gateway after changing IP address	1. Verify the IP address of the PC/laptop is in the same subnet range as the Gateway (i.e. If the Gateway IP is 155.177.0.xxx, then the PC/Lap IP address should be 155.177.0.yyy).
Can not find Gateway using Secondary Ethernet Port	1. Verify which Ethernet port is being used on the Gateway. 2. Verify the IP address for the Gateway (default primary port is 192.168.1.10, default secondary port is 192.168.2.10). 3. Verify the IP address of the PC/laptop is in the same subnet range as the Gateway (i.e. If the Gateway IP is 155.177.0.xxx, then the PC/Lap IP address should be 155.177.0.yyy).
Can not log into the Gateway	1. Verify the user name and password. The administrator user name is admin and the default password is default. See Table 2-1.

Table 6-2. Troubleshooting AMS® Wireless Configurator

Issue	Troubleshooting steps
Gateway does not appear in AMS Wireless Configurator	1. Verify the Security Setup Utility is installed on the same PC as AMS Wireless Configurator. 2. Setup a wireless network interface using the Network Configuration application. See Section 4: Software Setup. 3. Verify if the wireless network interface is configured for Secure Gateway Communications. 4. Verify secure/unsecure AMS Wireless Configurator protocol settings in the Gateway. Log on to the Gateway and navigate to SETUP > SECURITY > PROTOCOLS. 5. Restart AMS Wireless Configurator data server. Right click on AMS Wireless Configurator server icon in the Windows system tray (lower right corner) and select stop server.
Wireless devices do not appear under the Gateway	1. Verify wireless devices are connected to the Gateway. Log on to the Gateway and navigate to EXPLORER. 2. Right click on wireless network and select rebuild hierarchy.
Wireless device appears with red HART® symbol	1. Install latest device support files from AMS Wireless Configurator. Go to www.emersonprocess.com > BRANDS > AMS SUITE > AMS DEVICE MANAGER > DEVICE DESCRIPTION (DDs).
Device configuration items are grayed out	1. Verify whether current or historical information is being displayed. This setting is displayed at the bottom of each device configuration screen. Configuration requires the Current setting. 2. For security purposes a configuration timeout is applied to sessions that have been idle for more than 30 minutes. Log back into AMS Wireless Configurator.

Table 6-3. Troubleshooting Wireless Field Devices

Issue	Troubleshooting steps
Wireless device does not appear on the network	1. Verify the device has power. 2. Verify the device is within effect communications range. 3. Verify the proper Network ID has been entered into the device.
Wireless device appears in the join failure list	1. Re-enter the Network ID and Join Key into the device.
Wireless device appears with service denied	1. Verify the total number of devices on the network (100 max). 2. Go to SETUP > NETWORK > BANDWIDTH and click analyze bandwidth (Note: any changes will require the network to reform) 3. Reduce the update rate for the device.

Table 6-4. Troubleshooting Modbus Communications

Issue	Troubleshooting steps
Can not communicate using Modbus RTU	1. Verify the use of RS-485. 2. Verify wiring connections. See Section 3: Mounting and Connection. 3. Verify if termination is required. 4. Verify that Modbus serial communications setting in the Gateway match the Modbus Host settings. Log on to the Gateway and navigate to SETUP > MODBUS > COMMUNICATIONS. 5. Verify the Modbus address for the Gateway. 6. Verify Modbus register mapping in the Gateway. Log on to the Gateway and navigate to SETUP > MODBUS > MAPPING.
Can not communicate using Modbus TCP	1. Verify secure / unsecure Modbus protocol settings in the Gateway. Log on to the Gateway and navigate to SETUP > SECURITY > PROTOCOLS. 2. Verify the Modbus TCP communications settings in the Gateway. Log on to the Gateway and navigate to SETUP > MODBUS > COMMUNICATIONS. 3. Verify Modbus register mapping in the Gateway. Log on to the Gateway and navigate to SETUP > MODBUS > MAPPING.
Can not communicate using secure Modbus TCP	1. Verify the Security Setup Utility has been installed. 2. Configure a Secure Modbus Proxy for the Gateway. See Section 4: Software Setup. 3. Verify secure / unsecure Modbus protocol settings in the Gateway. Log on to the Gateway and navigate to SETUP > SECURITY > PROTOCOLS. 4. Verify the Modbus TCP communications settings in the Gateway. Log on to the Gateway and navigate to SETUP > MODBUS > COMMUNICATIONS. 5. Verify Modbus register mapping in the Gateway. Log on to the Gateway and navigate to SETUP > MODBUS > MAPPING.

Table 6-5. Troubleshooting OPC Communications

Issue	Troubleshooting steps
OPC application can not find a Gateway OPC server	1. Verify the Security Setup Utility has been installed on the same PC as the OPC application. 2. Configure an OPC proxy for the Gateway. See Section 4: Software Setup.
Gateway OPC server does not show any Gateways	1. Configure an OPC proxy for the Gateway. See Section 4: Software Setup.
Gateway OPC server does not show any data tags	1. Configure the Gateway OPC Browse Tree. Log on to the Gateway and navigate to SETUP > OPC > OPC BROWSE TREE. 2. Verify the connection status for the OPC proxy in the Security Setup Utility. 3. Verify if the OPC proxy is configured for secure or unsecure communications. 4. Verify secure / unsecure OPC protocol settings in the Gateway. Log on to the Gateway and navigate to SETUP > SECURITY > PROTOCOLS. 5. Verify network firewall and port settings.

Table 6-6. Troubleshooting Ethernet/IP

Issue	Troubleshooting steps
The Gateway is not publishing the parameters	1. Verify connection is established with Ethernet/IP. Navigate to SETUP > SECURITY > PROTOCOLS 2. Reference technical document 00809-0500-4420: Installation manual to connect to an Allen Bradley system.

Section 7 Glossary

This glossary defines terms used throughout this manual or that appear in the web interface of the Smart Wireless Gateway.

Term	Definition
Access Control List	A list of all devices that are approved to join the network. Each device will also have a unique join key. Also referred to as a white list.
Active Advertising	An operational state of the network manager that causes the entire wireless field network to send messages looking for new or unreachable devices to join the network.
Baud Rate	Communication speed for Modbus® RTU.
Burst Rate	The interval in which a wireless field device transmits measurement and status data to the Gateway. Same as Update Rate.
Certificate	A digital signature used to authenticate a client/server while using encrypted communications.
Connectivity	Typically refers to a combination of communication statistics and link reliability of a wireless field device. May also refer to the connection between the Gateway and the Host System.
Device ID	A hexidecimal number that provides unique device identification.
DHCP	Dynamic Host Configuration Protocol: Used to automatically configure the TCP/IP parameters of a device.
Domain	A unique designator on the internet comprised of symbols separated by dots such as: this.domain.com
Gateway	Refers to the Smart Wireless Gateway.
HART Tag	The device's electronic tag that the Gateway uses for all host integration mapping. Refers to the HART® long tag (32 characters, used for HART 6 or 7 devices) or the HART message (32 characters, only used for HART 5 wired devices connected via a WirelessHART adapter)
Host Name	A unique designator in a domain associated with the IP address of a device such as: device.this.domain.com. In that example the hostname is device.
HTML	Hyper Text Markup Language: The file format used to define pages viewed with a web browser.
HTTP	Hyper Text Transfer Protocol: The protocol that defines how a web server sends and receives data to and from a web browser.
HTTPS	HTTP over an encrypted Secure Sockets Layer (SSL)
Join Failure	When a wireless field device fails to join the WirelessHART® network. Most join failures are due to security reasons (missing or incorrect join key, not on access control list, etc.)
Join Key	Hexadecimal security code that allows wireless field devices to join the wireless field network. This code must be identical in the device and the Gateway.
Latency	The time from when a message leaves a wireless field device until it reaches the Gateway.
Netmask	A string of 1's and 0's that mask out or hide the network portion of an IP address leaving only the host component.

Term	Definition
Network I.D.	Numeric code that associates wireless field devices to the Gateway. This code must be identical in the device and the gateway.
Network Manager	Operational function within the Smart Wireless Gateway that automatically handles all device connections and scheduling of wireless data.
NTP	Network Time Protocol. Used to keep the system time synchronized with a network time server.
Path	A wireless connection between two devices in a wireless network. Also referred to as a hop.
Path Stability	A measure of connectivity between two devices in the wireless network. Calculated as the ratio of the number of received messages over the number of expected messages.
Primary Interface	Ethernet 1 or Fiber Optic port that is used for primary host communications.
Private Network/LAN	A local connection between a Smart Wireless Gateway and a PC/laptop. This network is used for commissioning and configuration of the Gateway.
Reliability	A measure of connectivity between the Gateway and a wireless field device. Calculated as the ratio of the number of received messages over the number of expected messages. Takes into account all paths.
RSSI	Received signal strength indication (dBm) for the wireless field device.
Secondary Interface	Ethernet 2 port that is used for backup connection or a maintenance port for local access.
Security Setup Utility	A software application that enables secure communications between the Gateway and host system, asset management software, data historians, or other applications.
Self-Organizing Network	Mesh network technology in which a network manager automatically handles all device connections and scheduling of wireless data.
Service Denied	The device has been denied bandwidth and can not publish its regular updates.
TCP/IP	Transmission Control Protocol/Internet Protocol. The protocol that specifies how data is transmitted over Ethernet.
Update Rate	The interval in which a wireless field device transmits measurement and status data to the Gateway. Same as Burst Rate.
Wireless Field Device(s)	WirelessHART field devices that are a part of the wireless field network.
Wireless Field Network	WirelessHART network, consisting of Smart Wireless Gateway and multiple wireless field devices.
Wireless Plant Network	Industrial Wi-Fi network, used to integrate the Wireless Field Network into the control network.

Appendix A　　Product Specifications

A.1　　Functional specifications

Input voltage

10.5-30 VDC

Current draw

Operating Current Draw is based on 3.6 Watts power consumption.

Momentary startup Current Draw up to twice operating Current Draw.
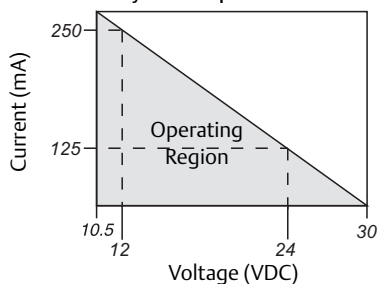
Radio frequency power output from antenna

Maximum of 10 mW (10 dBm) EIRP

Maximum of 40 mW (16 dBm) EIRP for WN2 High Gain option

Environmental

Operating Temperature Range:
-40 to 158 °F (-40 to 70 °C)

Operating Humidity Range:
10-90% relative humidity

EMC performance

Complies with EN61326-1:2006.

Antenna options

Integrated Omni-directional Antenna
Optional remote mount Omni-directional Antenna

A.2 Physical specifications

Weight

10 lb. (4,54 kg)

Material of construction

Housing

Low-copper aluminum, NEMA® 4X

Paint

Polyurethane

Cover gasket

Silicone Rubber

Antenna

Integrated Antenna: PBT/PC

Remote Antenna: Fiber Glass

Certifications

Class I Division 2 (U.S.)

Equivalent Worldwide

A.3 Communication specifications

Isolated RS485

2-wire communication link for Modbus® RTU multidrop connections

Baud rate: 57600, 38400, 19200, or 9600

Protocol: Modbus RTU

Wiring: Single twisted shielded pair, 18 AWG. Wiring distance is approximately 4000 ft. (1,524 m)

Ethernet

10/100base-TX Ethernet communication port
Protocols: Modbus TCP, OPC, EtherNet/IP™, HART®-IP, https (for Web Interface)
Wiring: Cat5E shielded cable. Wiring distance 328 ft. (100 m).

Modbus

Supports Modbus RTU and Modbus TCP with 32-bit floating point values, integers, and scaled integers.
Modbus Registers are user-specified.

OPC

OPC server supports OPC DA v2, v3

EtherNet/IP

Supports EtherNet/IP protocol with 32-bit Floating Point values and Integers. EtherNet/IP Assembly Input-Output instances are user configurable. EtherNet/IP specifications are managed and distributed by ODVA.

A.4 Self-organizing network specifications

Protocol

IEC 62591(*Wireless*HART®), 2.4 - 2.5 GHz DSSS.

Maximum network size

100 wireless devices @ 8 sec.
50 wireless devices @ 4 sec.
25 wireless devices @ 2 sec.
12 wireless devices @ 1 sec.

Supported device update rates

1, 2, 4, 8, 16, 32 seconds or 1 - 60 minutes

Network size/latency

100 Devices: less than 10 sec.
50 Devices: less than 5 sec.

Data reliability

>99%

A.5   System security specifications

Ethernet

Secure Sockets Layer (SSL) enabled (default) TCP/IP communications

Smart Wireless Gateway access

Role-based Access Control (RBAC) including Administrator, Maintenance, Operator, and Executive. Administrator has complete control of the Gateway and connections to host systems and the self-organizing network.

Self-organizing network

AES-128 Encrypted *Wireless*HART, including individual session keys. Drag and Drop device provisioning, including unique join keys and white listing.

Internal firewall

User Configurable TCP ports for communications protocols, including Enable/Disable and user specified port numbers. Inspects both incoming and outgoing packets.
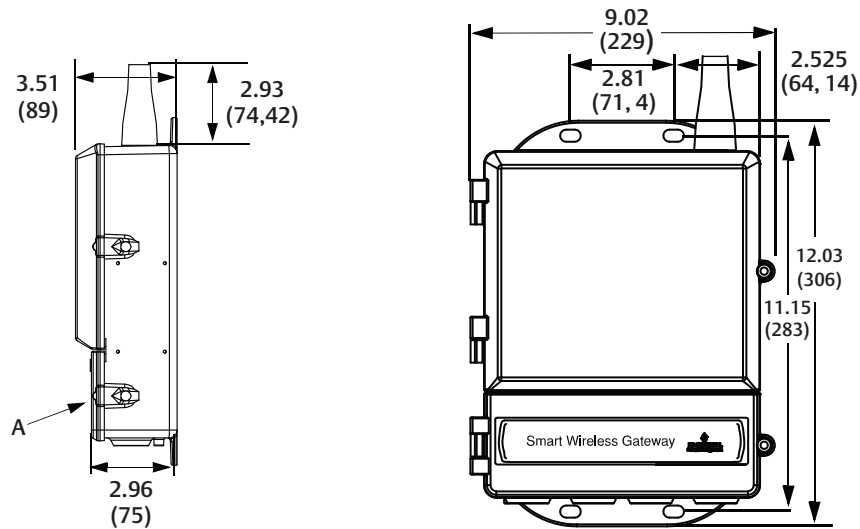
Third party certification

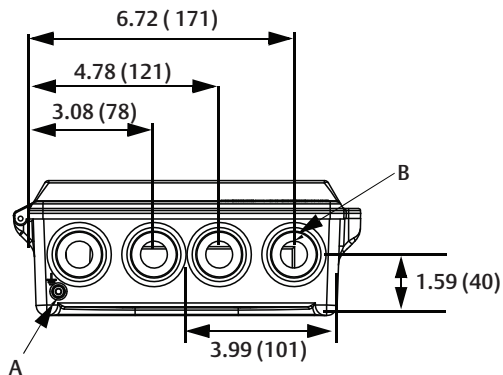Wurldtech: Achilles Level 1 certified for network resiliency

National Institute of Standards and Technology (NIST): Advanced Encryption Standard (AES) Algorithm conforming to Federal Information Processing Standard Publication 197 (FIPS-197).

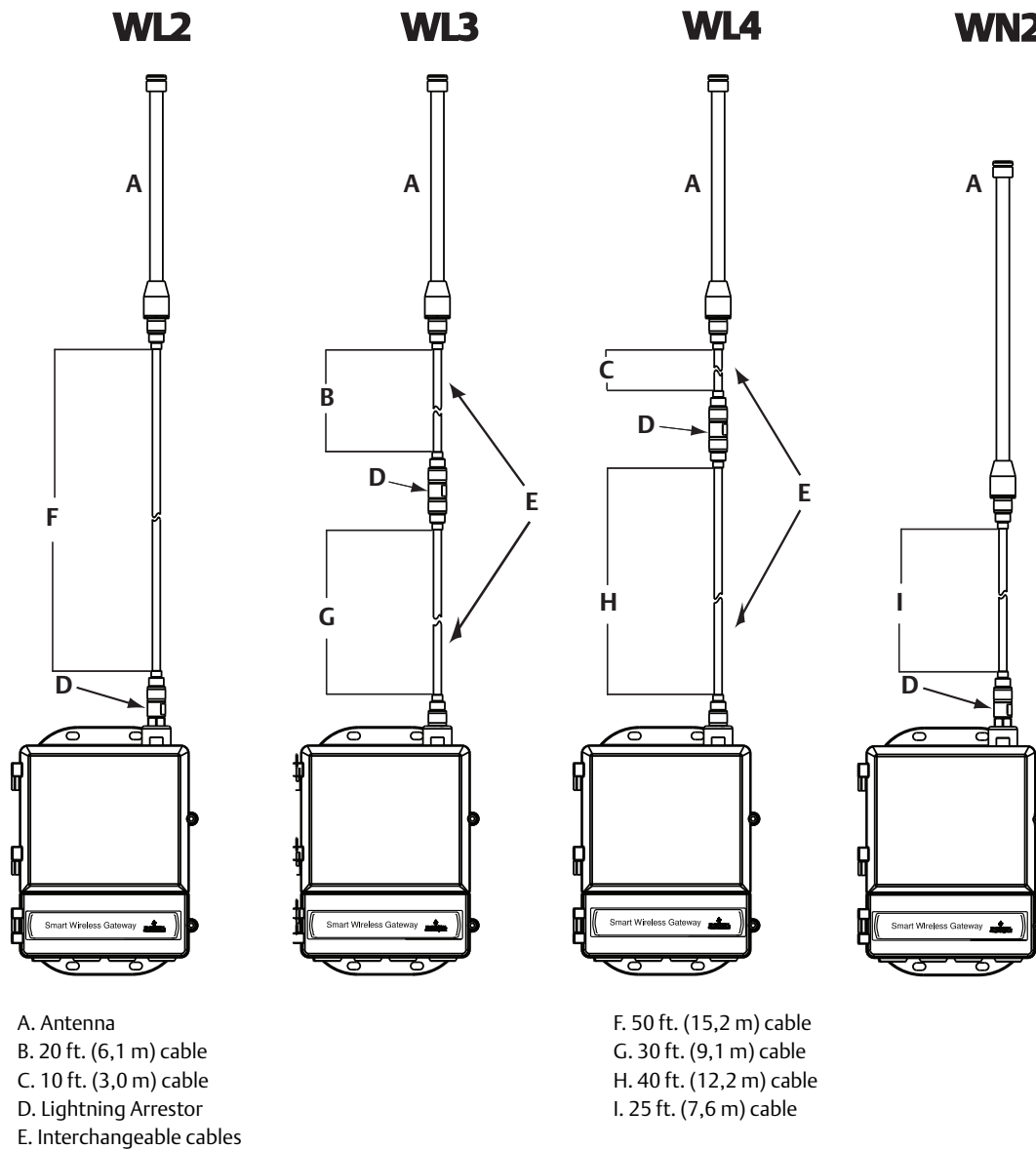# A.6 Dimensional drawings

Figure A-1. Smart Wireless Gateway

A. Lower Cover (remove for electrical connections)

A. Ground Lug
B. $^1/_2$ inch NPT Conduit Connection (4 Places)

Dimensions are in inches (millimeters).

WL2   **WL3**   **WL4**   **WN2**

A. Antenna
B. 20 ft. (6,1 m) cable
C. 10 ft. (3,0 m) cable
D. Lightning Arrestor
E. Interchangeable cables

F. 50 ft. (15,2 m) cable
G. 30 ft. (9,1 m) cable
H. 40 ft. (12,2 m) cable
I. 25 ft. (7,6 m) cable

Remote omni-antenna kit

The Remote Omni-Antenna kit includes sealant tape for remote antenna connection, as well as mounting brackets for the antenna, Lightning Arrestor, and the Smart Wireless Gateway.

Lightning protection is included on all the options. WL3 and WL4 provide lightning protection along with the ability to have the gateway mounted indoors, the antenna mounted outdoors, and the lightning arrestor mounted at the building egress.

Note
The coaxial cables on the remote antenna options WL3 and WL4 are interchangeable for installation convenience.

A.7 Ordering information

Table A-1. Smart Wireless Gateway Ordering Information

★ The Standard offering represents the most common options. The starred options (★) should be selected for best delivery.
  The Expanded offering is subject to additional delivery lead time.

Model	Product description	
1420	Smart Wireless Gateway	
Power input		
A	24 VDC Nominal (10.5-30 VDC)	★
Ethernet communications - physical connection		
1[(1)(2)]	Ethernet	★
2[(3)(4)]	Dual Ethernet	★
Wireless update rate, operating frequency, and protocol		
A3	User Configurable Update Rate, 2.4 GHz DSSS, *Wireless*HART	★
Serial communication		
N	None	★
A[(5)]	Modbus RTU via RS485	★
Ethernet communication - data protocols		
2	Webserver, Modbus TCP/IP, AMS Ready, HART-IP	★
4	Webserver, Modbus TCP/IP, AMS Ready, HART-IP, OPC	★
5[(6)]	DeltaV Ready	★
6[(6)]	Ovation Ready	★
8	Webserver, EtherNet/IP, AMS Ready, HART-IP	★
9	Webserver, EtherNet/IP, Modbus TCP/IP, AMS Ready, HART-IP	★
Options (include with selected model number)		
Product certifications		
N5	FM Division 2, Non-incendive	★
N6	CSA Division 2, Non-incendive	★
N1	ATEX Type n	★
ND	ATEX Dust	★
N7	IECEx Type n	★
NF	IECEx Dust	★
KD	FM & CSA Division 2, Non-incendive and ATEX Type n	★
N3	China Type n	★
N4	TIIS Type n	★
Redundancy options		
RD[(7)(8)(9)]	Gateway Redundancy	★

Table A-1. Smart Wireless Gateway Ordering Information
★ The Standard offering represents the most common options. The starred options (★) should be selected for best delivery.
The Expanded offering is subject to additional delivery lead time.

Adapters		
J1	CM 20 Conduit Adapters	★
J2	PG 13.5 Conduit Adapters	★
J3	³/₄ NPT Conduit Adapters	★
Antenna options[10]		
WL2	Remote Antenna Kit, 50 ft. (15.2 m) cable, Lightning Arrestor	★
WL3	Remote Antenna Kit, 20 ft. (6.1 m) and 30 ft. (9.1 m) cables, Lightning Arrestor	★
WL4	Remote Antenna Kit, 10 ft. (3.0 m) and 40 ft. (12.2 m) cables, Lightning Arrestor	★
WN2[11]	High-Gain, Remote Antenna Kit, 25 ft. (7.6m) cable, Lightning Arrestor	
Typical model number: 1420 A 2 A3 A 2 N5		

(1) Single active 10/100 baseT Ethernet port with RJ45 connector.
(2) Additional ports disabled.
(3) Dual active 10/100 baseT Ethernet ports with RJ45 connectors.
(4) Multiple active ports have separate IP addresses, firewall isolation, and no packet forwarding.
(5) Convertible to RS232 via adaptor, not included with Gateway.
(6) Includes Webserver, Modbus TCP, AMS Ready, HART-IP, and OPC.
(7) Requires the selection of Dual Ethernet option code 2.
(8) Not available with DeltaV Ready option code 5.
(9) Not available with EtherNet/IP option codes 8 and 9
(10) The WL2, WL3, WL4, and WN2 options require minor assembly.
(11) Not available in all countries.

A.8 Accessories and spare parts

Table A-2. Accessories

Item description	Part number
AMS Wireless SNAP-ON™, 1 Gateway License	01420-1644-0001
AMS Wireless SNAP-ON, 5 Gateway Licenses	01420-1644-0002
AMS Wireless SNAP-ON, 10 Gateway Licenses	01420-1644-0003
AMS Wireless SNAP-ON, 5-10 Upgrade Licenses	01420-1644-0004
Serial Port HART Modem and Cables only	03095-5105-0001
USB Port HART Modem and Cables only	03095-5105-0002

Table A-3. Spare Parts

Item description	Part number
Spare Kit, WL2 Replacement[1], Remote Antenna, 50 ft. (15,2 m) Cable, and Lightning Arrestor	01420-1615-0302
Spare Kit, WL3 Replacement[1], Remote Antenna, 20/30 ft. (6,1/9,1 m) Cables, and Lightning Arrestor	01420-1615-0303
Spare Kit, WL4 Replacement[1], Remote Antenna, 10/40 ft. (3,0/12,2 m) Cables, and Lightning Arrestor	01420-1615-0304
Spare Kit, WN2 Replacement[1], High Gain, Remote Antenna, 25 ft. (7.6 m) Cable, and Lightning Arrestor[2]	01420-1615-0402

(1) Can not upgrade from integral to remote antenna.
(2) Not available in all countries.

Appendix B   Product Certifications

B.1   Approved manufacturing locations

Rosemount Inc. – Chanhassen, Minnesota, USA
Emerson Process Management GmbH & Co. - Karlstein, Germany
Emerson Process Management Asia Pacific Private Limited - Singapore
Beijing Rosemount Far East Instrument Co., Limited - Beijing, China

B.2   Telecommunication compliance

All wireless devices require certification to ensure that they adhere to regulations regarding the use of the RF spectrum. Nearly every country requires this type of product certification. Emerson is working with governmental agencies around the world to supply fully compliant products and remove the risk of violating country directives or laws governing wireless device usage.

B.3   FCC and IC

This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions. This device may not cause harmful interference. This device must accept any interference received, including interference that may cause undesired operation. This device must be installed to ensure a minimum antenna separation distance of 20 cm from all persons.

B.4   Ordinary Location Certification for FM

As standard, the Gateway has been examined and tested to determine that the design meets basic electrical, mechanical, and fire protection requirements by FM, a nationally recognized testing laboratory (NRTL) as accredited by the Federal Occupational Safety and Health Administration (OSHA).

North America

N5 FM Division 2, Non-Incendive
Certificate: 3028321

Nonincendive for Class I, Division 2, Groups A, B, C, and D.
Suitable for Class II, III, Division 2, Groups E, F, and G.
Enclosure Type 4X
Temperature Code: T4 (-40 °C $\leq T_a \leq$ 60 °C)

Canadian Standards Association (CSA)

N6 CSA Division 2
Certificate: 1849337
Suitable for Class I, Division 2, Groups A, B, C, and D.
Install per Rosemount drawing 01420-1011.
Temperature Code: T4 (-40 °C $\leq T_a \leq$ 60 °C)
CSA Enclosure Type 4X

B.5 European Union Directive Information

The EC declaration of conformity for all applicable European directives for this product can be found on the Rosemount website at www.rosemount.com. A hard copy may be obtained by contacting your local sales representative.

ATEX Directive (94/9/EC)

Emerson Process Management complies with the ATEX Directive.

Electro Magnetic Compatibility (EMC) (2004/108/EC)

Emerson Process Management complies with the EMC Directive.

Radio and Telecommunications Terminal Equipment Directive (R&TTE)(1999/5/EC)

Emerson Process Management complies with the R&TTE Directive

$C\epsilon$

Europe

N1 ATEX Type n
Certificate: Baseefa 07ATEX0056X
ATEX Marking: ⬡ II 3 G
Ex nA nL IIC T4 (-40 °C $\leq T_a \leq$ 60 °C)

Special Conditions for Safe Use (X):

1. The surface resistivity of the antenna is greater than one gigaohm. To avoid electrostatic charge build-up, it must not be rubbed or cleaned with solvents or a dry cloth.

2. The Apparatus is not capable of withstanding the 500V insulation test required by Clause 9.4 of EN 60079-15: 2005. This must be taken into account when installing the apparatus.

ND ATEX Dust
Certificate: Baseefa 07ATEX0057X
ATEX Marking: ⟨Ex⟩ II 3 D
Ex tD A 22 IP66 T135 (-40 °C ≤ T_a ≤ 60 °C)
Maximum working voltage = 28 V

Special Condition for Safe Use (X):

1. The surface resistivity of the antenna is greater than 1GΩ. To avoid electrostatic charge build-up, it must not be rubbed with a dry cloth or cleaned with solvents.

N7 IECEx Type n
Certificate: IECEx BAS 07.0012X
Ex nA nL IIC T4 (-40 °C ≤ T_a ≤ 60 °C)
Maximum working voltage = 28 V

Special Conditions for Safe Use (X):

1. The apparatus is not capable of withstanding the 500V electrical strength test as defined in Clause 6.8.1 of IEC 60079-15: 2005. This must be taken into account during installation.

2. The surface resistivity of the antenna is greater than one gigaohm. To avoid electrostatic charge build-up, it must not be rubbed or cleaned with solvents or a dry cloth.

NF IECEx Dust
Certification : IECEx BAS 07.0013
Ex tD A22 IP66 T135 (-40 °C ≤ T_a ≤ 60 °C)
Maximum working voltage = 28 V

Combinations

KD Combination of N5, N6, and N1.

Appendix C　　DeltaV™ Ready

C.1　　Overview

Native integration with DeltaV enables the Smart Wireless Gateway to be autosensed and easily commissioned for seamless integration with all DeltaV applications: Explorer, Diagnostics, and Control Studio. WirelessHART® devices can be easily added to the wireless field network and then reconciled through DeltaV Explorer and assigned to analog channels through drag and drop assignment.

C.2　　Latency considerations in control logic design and operation

Since the DeltaV wireless I/O scanner software requests updates for 1/5 of the devices each second, DeltaV receives updates on a particular field device once every 5 seconds. That is not necessarily synchronized with the update rate of the field device. Also, there is some latency between when the field device takes a process sample and when it is permitted to pass its value onto the wireless network. Status update responses can also increase latency in some instances. So for example, if a device updates once every 8 seconds, and wireless network latency is 2 seconds, the amount of time that could pass between when an event occurred in the field and before it is available to the DeltaV I/O bus is between zero and 15 (8+2+5) seconds. The update period of the DeltaV control module should be added to that total to determine the range of latencies before an event in the field can be acted upon by the control system.

Operators should be made aware that the update rate of wireless measurements on operator screens are somewhat slower than those from wired devices. For example, if the operator initiates a valve movement, it can be 5-15 seconds before confirming feedback appears on the operator screen. Any control logic designed along the same principles should also take the update rates and latencies into account as well.

C.3　　Requirements

DeltaV

Version 10.3 or newer.

Smart Wireless Gateway

DeltaV Ready option (Data Protocol option 5). See "Ordering information" on page 57.

C.4   Mounting and connecting

Mount the DeltaV Ready Gateway in the same manner as a standard Gateway. ("Mounting" on page 16). The Gateway should be mounted in a location that allows convenient access to the DeltaV control network as well as the wireless field network.

Connect the Gateway's primary Ethernet port (Ethernet 1) into the DeltaV primary control network. If the dual Ethernet option (Physical Connection code 2) was ordered with the Gateway, connect the secondary Ethernet port (Ethernet 2) into the DeltaV secondary control network.

Figure C-1. Delta V Control Network Architecture

A. Pro+ Engineering Station   D. Controller and I/O
B. Primary Control Network   E. Smart Wireless Gateway
C. Secondary Control Network
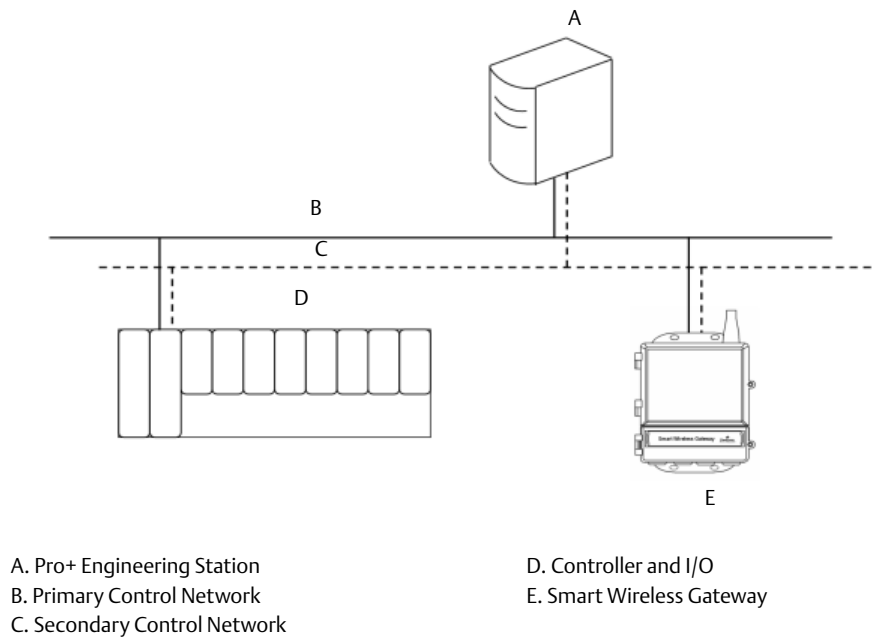
C.5   Setup

Out of the box the Smart Wireless Gateway is pre-configured for use on the DeltaV control network. In the DeltaV Explore application, the Gateway will automatically appear in the Decommissioned Nodes folder.

To setup a wireless network will require 3 steps:

1.   Commission the Gateway.

2.   Assign wireless device tags.

3.   Assign Gateway to controller and download.

**Figure C-2. Decommissioned Nodes Folder within DeltaV Explorer**
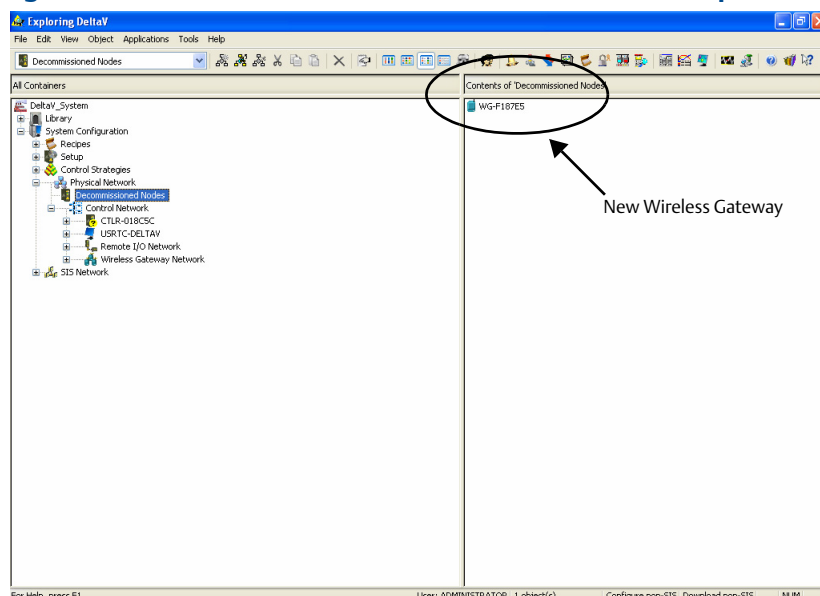
Commission the Gateway using the following procedure:

1.   Select **START**>**PROGRAMS**>**DELTAV**>**ENGINEERING**> **DELTAV EXPLORE** to launch the DeltaV Explorer application.

2.   Expand the folder **SYSTEM CONFIGURATION** >**PHYSICAL NETWORK**>**DECOMMISSIONED NODES**.

3.   Right click on the *Smart Wireless Gateway* and select **Commission**.

4.   Enter a name for the Gateway and select **OK**.

5.   Select **YES** when prompted to *Auto-Sense Wireless Gateway*.

At this time the *Reconcile I/O* window will appear. The purpose of this screen is to assign WirelessHART devices to DeltaV I/O channel. This allows the wireless device to be referenced in other DeltaV applications like Control Studio.

**Figure C-3. Assign WirelessHART Devices to DeltaV I/O Channel**
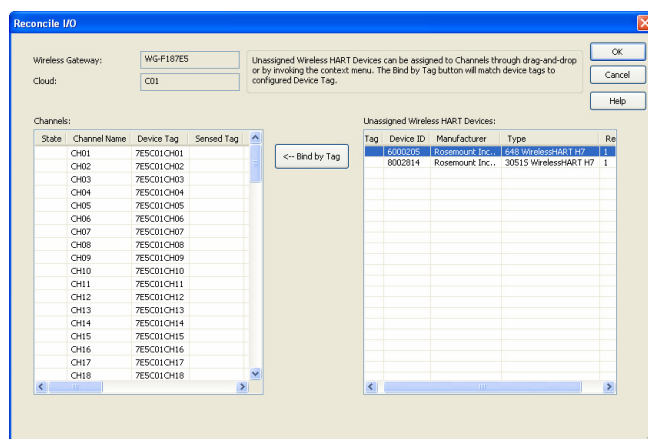
Assign wireless device tags using the following procedure:

1.   Drag and drop WirelessHART device from the *Unassigned Wireless HART Devices:* list to the *Channels:* list.

2.   Repeat this process for each wireless device until all have been assigned.

3.   Select **OK** to continue.

Next the Gateway will need to be assigned to a DeltaV Controller and download all. Assign and download the Gateway using the following procedure:

1.   Right click on the Gateway and select **Assign...**

2.   Use the browse window and select the desired controller.

3.   Select **OK** to close the assignment window.

4.   Right click on the Gateway and select **Download**.

5.   Follow the download dialog.

6.   Select **OK** to close the download window.

Figure C-4. Gateway Context Menu (Right Click)
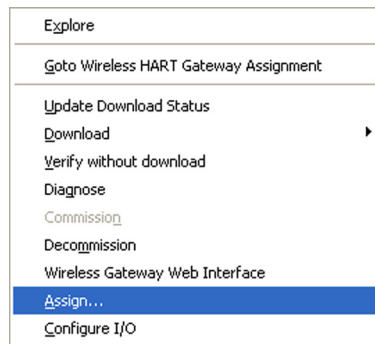
Now the Gateway and wireless devices are fully commissioned and available to use in other DeltaV applications. When new devices are added to the wireless network, they will need to be assigned to DeltaV channels through the reconcile process (right click on Gateway and select configure IO).

Note
Logging in to the Gateway is not possible using the default TCP/IP network setting. If the Gateway is decommissioned, use an IP address 10.5.255.254. If the Gateway is commissioned, right click on the Gateway in DeltaV Explore and select Wireless Gateway Web Interface.

Appendix D   Redundancy

D.1   Overview

Redundancy for the Smart Wireless Gateway increases the availability of the wireless field network by providing two sets of physical hardware which operate as a single Gateway system. This section covers setup and installation of a redundant Gateway system. It also covers diagnostics and integration to help monitor the health of the redundant Gateway system.

- Where to mount the respective antennas

- Illustration of maximum redundancy including dual switch and UPS

- Understanding how the fail over works and experience to expect

- How to leverage the multimaster capability for Modbus® integrations

D.2   Requirements

Smart Wireless Gateway

Firmware Version 4.3.19 or greater is recommended

RD option for Gateway Redundancy

Static IP Address

Must have matching output protocols (e.g. Modbus or OPC) on each Gateway.

Host system

Ethernet connection for Modbus TCP or OPC DA communications

Serial (RS-485) connection for Modbus RTU communications

D.3   Setup

When configuring redundant Smart Wireless Gateways, it is only necessary to configure one system. The other Gateway will be configured automatically when it is paired with the first Gateway.

Choose one Gateway as the starter Gateway. For the purposes of this document, it will be referred to as Gateway A. The other Gateway will be referred to as Gateway B.

To configure redundancy system settings:

1.   Connect a PC/laptop to the Ethernet 1 port on Gateway A.

2.   Log in using the admin user account.

3.   Navigate to System **Settings>Gateway>Redundancy**.

4.   Gateway A's factory serial number will be assigned to Gateway A.

5.   Gateway B's factory serial number will be assigned to Gateway B.

The Gateway names will be used in diagnostic messages and host system integration to help identify each Gateway. It is recommended that these names be marked on each physical Gateway, in addition to the configuration settings.

Selecting left or right for Gateway A is for visualization purposes only. It has no effect on performance or functionality.

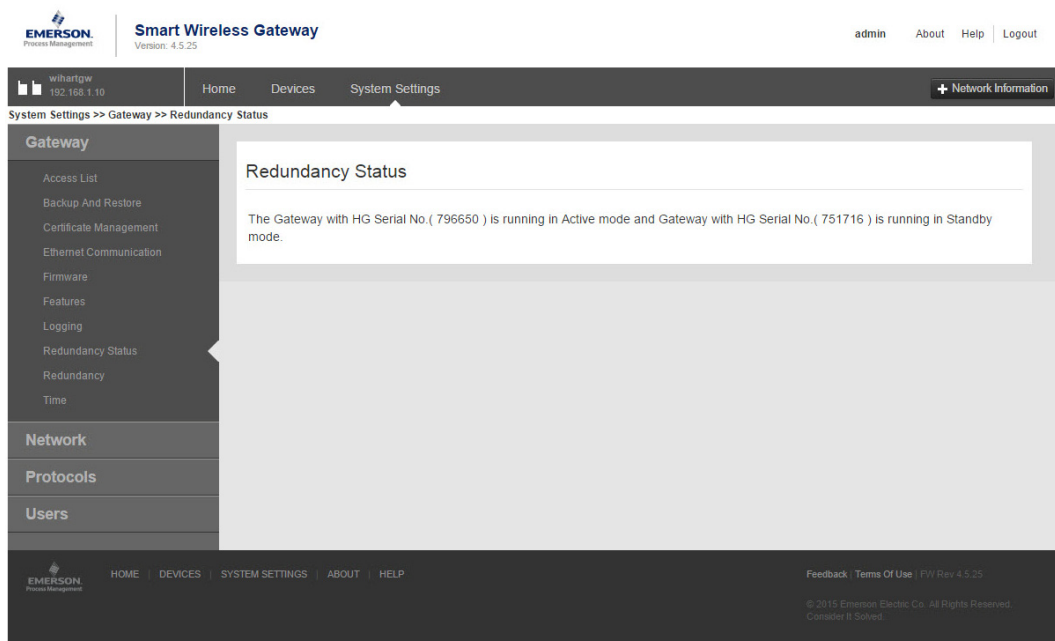**Figure D-1. System Settings>Gateway>Redundancy**
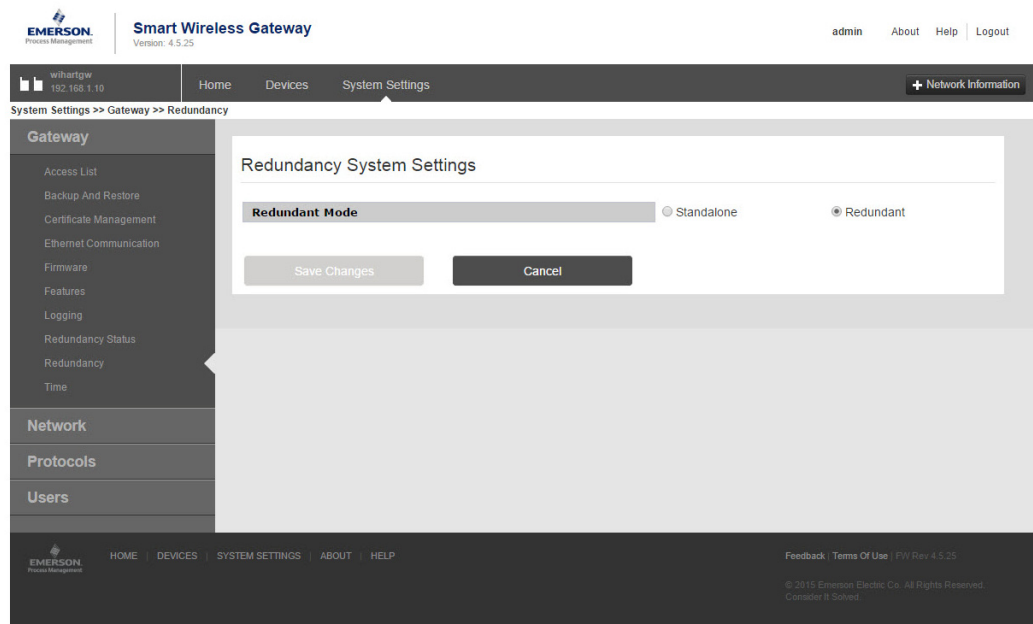
Figure D-2. Redundancy Status

After the redundancy system settings have been configured, the two Gateways must be connected and undergo a pairing process.

To pair both Gateways and form a redundant system:

1.   Connect a PC/laptop to the primary Ethernet port on Gateway A.

2.   Log in using the admin user account.

3.   Navigate to **Diagnostics>Advanced>Redundancy Status**.

4.   Connect the secondary Ethernet port on Gateway A to the secondary Ethernet port on Gateway B (see Figure D-3 on page 70, Redundancy Setup Connections).

5.   A dialog will appear on the page; select **Form redundant pair**.

6.   Wait for the Pairing to redundant peer status to turn green.

7.   Select **Return to page**.

Figure D-3. Redundancy Setup Connections

A. Gateway A
B. Gateway B
C. PC / Laptop

E. Primary Ethernet
F. Secondary Ethernet
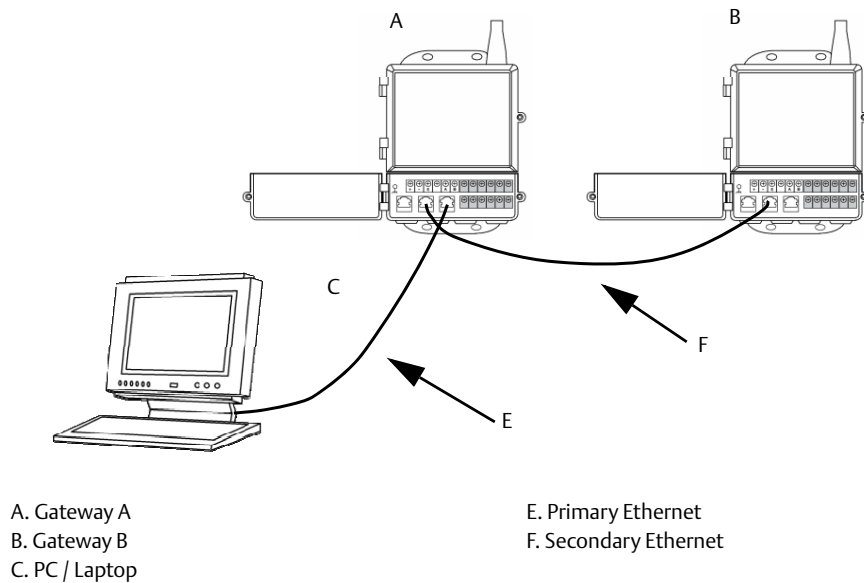
Once the Gateways have finished the pairing process, Gateway A will appear as the current active Gateway on the left hand side and Gateway B will be the standby Gateway on the right (note that left/right hand appearance can be changed on the Redundancy System Settings page). If significant configuration changes need to be downloaded to the standby Gateway, it may temporarily go offline shortly after the pair process is complete. This is expected behavior and does not represent instability in the system.

D.4 Mounting and connections

Redundant Gateways follow similar mounting and connection practices as a standalone Gateway. Please refer to Section 3: Mounting and Connection for more information. In addition to the standard practices, the following considerations should be taken when installing redundant Gateways.

Mounting

The redundant Gateways should be mounted in a location that allows convenient access to the process control network as well and provides good coverage for the wireless field network.

The redundant Gateway antennas should be mounted at the same height and be spaced between 3 ft to 9 ft (1m to 3m) horizontally. This is to ensure that they provide identical coverage for the wireless field network and to help eliminate coverage gap in the event of a switch over.

Ethernet

An Ethernet connection to the host system will support Modbus TCP, OPC, AMS® Wireless Configurator, and HART IP protocols. When using this architecture, connect the secondary

Ethernet port on Gateway A directly to the secondary Ethernet port on Gateway B. Then connect the primary Ethernet ports for both Gateways to a process control network using separate/redundant network switches. See Figure D-4 Ethernet Connection Architecture.
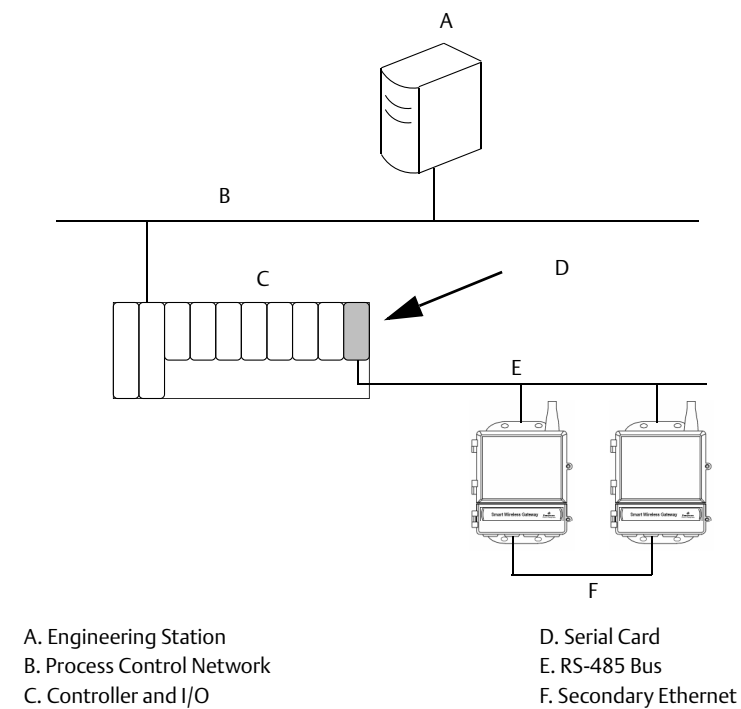
Figure D-4. Ethernet Connection Architecture

A. Engineering Station
B. Process Control Network
C. Gateway A
D. Primary Ethernet

E. Secondary Ethernet
F. Gateway B
G. Primary Ethernet
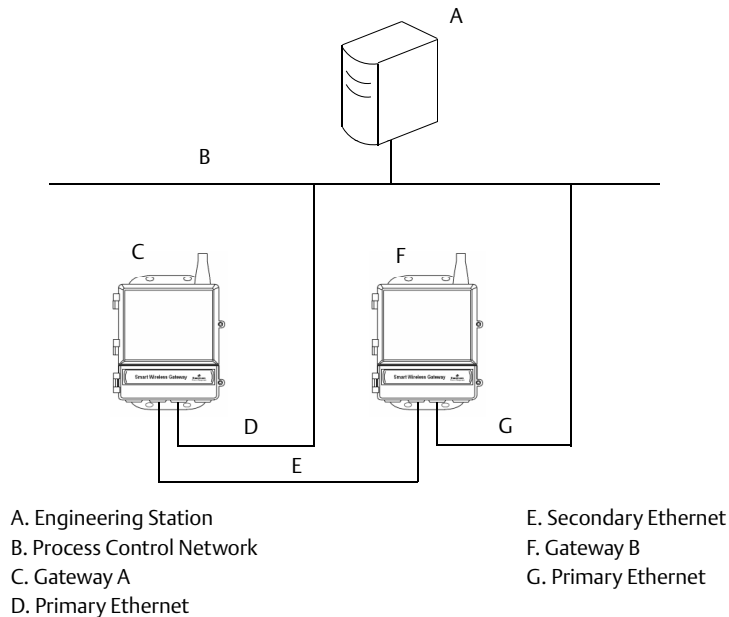
Note
The primary Ethernet port for each Gateway should be connected to separate network switches on the same process control network. Consult a control system administrator for more details about available redundant network switches.

Simplex RS-485

A simplex RS-485 host connection supports Modbus RTU protocol. When using this architecture, connect the secondary Ethernet port on Gateway A directly to the secondary Ethernet port on Gateway B. Then wire the RS-485 ports for both Gateways in parallel to a single serial card at the host system. See Figure D-5 Simplex RS-485 Architecture.

Figure D-5. Simplex RS-485 Architecture

A. Engineering Station
B. Process Control Network
C. Controller and I/O

D. Serial Card
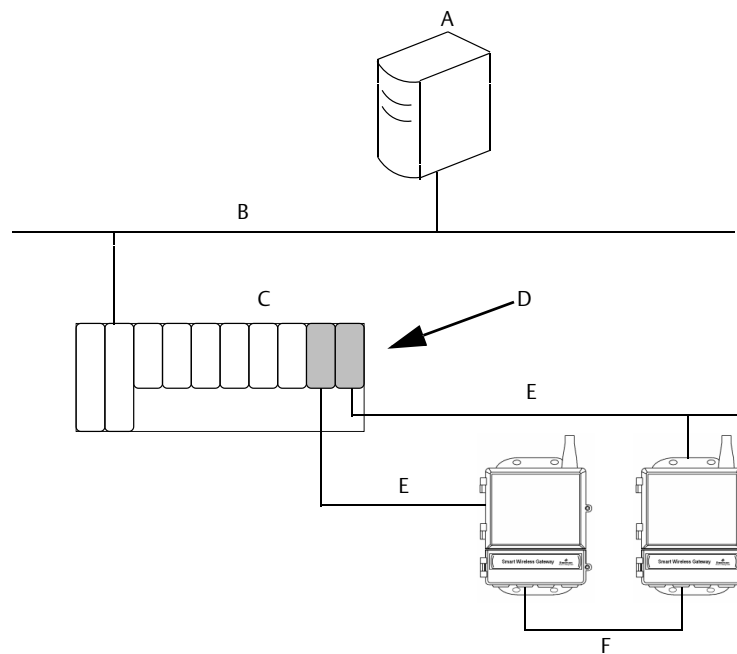E. RS-485 Bus
F. Secondary Ethernet

Note
In either a simplex or dual RS-485 architecture, the primary Ethernet ports can be connected to an asset management network to provide connectivity to AMS Device Manager or AMS Wireless Configurator.

Dual RS-485

A Dual RS-485 host connection support Modbus RTU protocol. When using this architecture, connect the secondary Ethernet port on Gateway A directly to the secondary Ethernet port on Gateway B. Then wire the RS-485 ports for both Gateways separately to dual serial cards at the host system. See Figure D-6 Dual RS-485 Architecture.

Figure D-6. Dual RS-485 Architecture

A. Engineering Station
B. Process Control Network
C. Controller and I/O

D. Dual Serial Card
E. RS-485 Bus
F. Secondary Ethernet

Note
By default, only the active Gateway in a redundant system will respond to Modbus polling requests. If simultaneous polling is desired, login to the Gateway web interface, navigate to Setup>Modbus>Communications and set "Respond when running as redundant standby?" to Yes. Only use this setting in a dual RS-485 architecture.

Power

Power for the redundant Gateways should be applied after all primary and secondary Ethernet and RS-485 connections have been made. Using separate uninterruptable power supplies (UPS) is recommended to ensure availability of the redundant Gateway system.

D.5 Diagnostics

The redundant system will perform many diagnostic checks to verify the health and connectivity of the system.

Figure D-7. Redundancy Status (Diagnostics>Advanced>Redundancy Status)
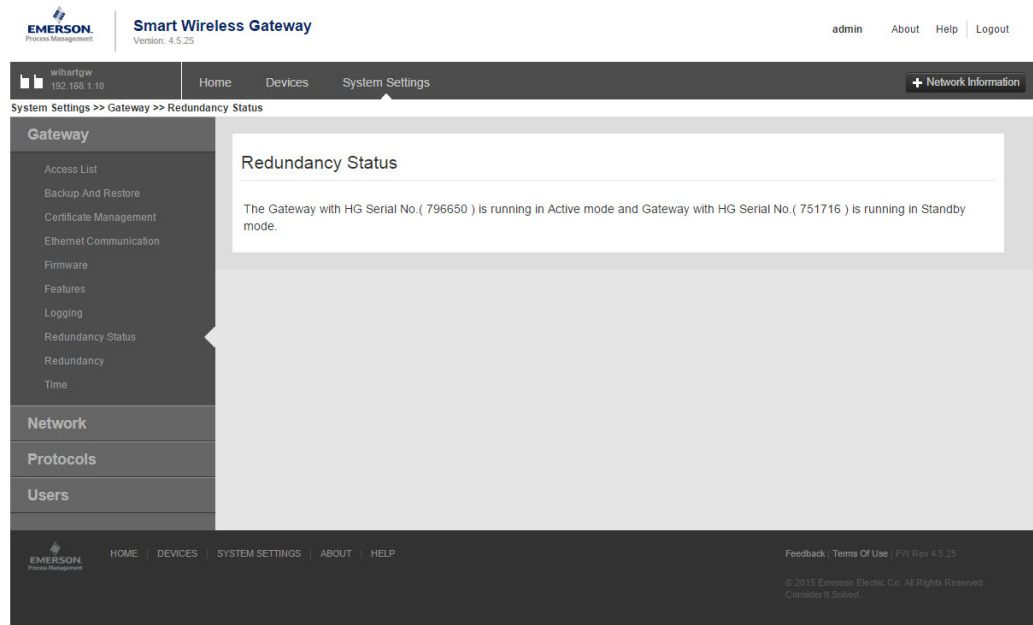
These diagnostics can also be mapped to Modbus registers or OPC tags. The following table covers what diagnostics are included on the Redundancy Status page as well as how they can be mapped as parameters in Modbus or OPC.

Table D-1. Redundancy Diagnostics

Parameter	Description	Data type
REDUNDANT_HEALTHY	Overall redundancy status indicating the system is ready for a switch-over	Boolean
RF_COVERAGE_FAILURE	Check to verify that both Gateways have the same RF coverage of the wireless field network	Boolean
REDUNDANT_A_ONLINE	Operational status of Gateway A	Boolean
REDUNDANT_A_MASTER	Indication if Gateway A is the active system	Boolean
REDUNDANT_A_PING	Indication if Gateway A is able to ping designated host IP address	Boolean
REDUNDANT_A_ETH0	Electrical connection status of the primary Ethernet port for Gateway A	8-bit unsigned int
REDUNDANT_B_ONLINE	Operational status of Gateway B	Boolean
REDUNDANT_B_MASTER	Indication if Gateway B is the active system	Boolean
REDUNDANT_B_PING	Indication if Gateway B is able to ping designated host IP address	Boolean
REDUNDANT_B_ETH0	Electrical connection status of the primary Ethernet port for Gateway A	8-bit unsigned int

In addition to the redundancy diagnostics, an additional check may be configured to test network connectivity to a host system or other application. The redundant system will use this check to determine the best connectivity option and which Gateway should be set to the active Gateway.

To configure network connectivity check:

1.   Navigate to **System Settings>Gateway>Ethernet Communication**.

2.   Enter the host system IP address in the *Check Network Connectivity IP Address* field.

3.   Select **Save Changes**.

**Figure D-8. Network Connectivity Check
(System Settings>Gateway>Ethernet Communication)**

D.6   Gateway replacement

When replacing or reintroducing a Gateway in a redundant system, always connect both the primary and secondary Ethernet connections before powering the standby Gateway. If the Gateway is being reintroduced (i.e. it was a part of the original redundant system), it will automatically rejoin the redundant system. If the Gateway is new or has been set to default configuration, it will need to be paired to the current active Gateway. Navigate to **System Settings>Gateway>Redundancy** and follow the recommended actions on that page or follow the procedure above to pair Gateways and form a redundant system.

Rosemount World Headquarters

Emerson Process Management

6021 Innovation Blvd

Shakopee, MN 55379, USA

- +1 800 999 9307 or +1 952 906 8888
- +1 952 949 7001
- RFQ.RMD-RCC@EmersonProcess.com

North America Regional Office

Emerson Process Management

8200 Market Blvd.

Chanhassen, MN 55317, USA

- +1 800 999 9307 or +1 952 906 8888
- +1 952 949 7001
- RMT-NA.RCCRFQ@Emerson.com

Latin America Regional Office

Emerson Process Management

1300 Concord Terrace, Suite 400

Sunrise, Florida, 33323, USA

- +1 954 846 5030
- +1 954 846 5121
- RFQ.RMD-RCC@EmersonProcess.com

Europe Regional Office

Emerson Process Management Europe GmbH

Neuhofstrasse 19a P.O. Box 1046

CH 6340 Baar

Switzerland

- +41 (0) 41 768 6111
- +41 (0) 41 768 6300
- RFQ.RMD-RCC@EmersonProcess.com

Asia Pacific Regional Office

Emerson Process Management Asia Pacific Pte Ltd

1 Pandan Crescent

Singapore 128461

- +65 6777 8211
- +65 6777 0947
- Enquiries@AP.EmersonProcess.com

Middle East and Africa Regional Office

Emerson Process Management

Emerson FZE P.O. Box 17033,

Jebel Ali Free Zone - South 2

Dubai, United Arab Emirates

- +971 4 8118100
- +971 4 8865465
- RFQ.RMTMEA@Emerson.com

EMERSON.
Process Management