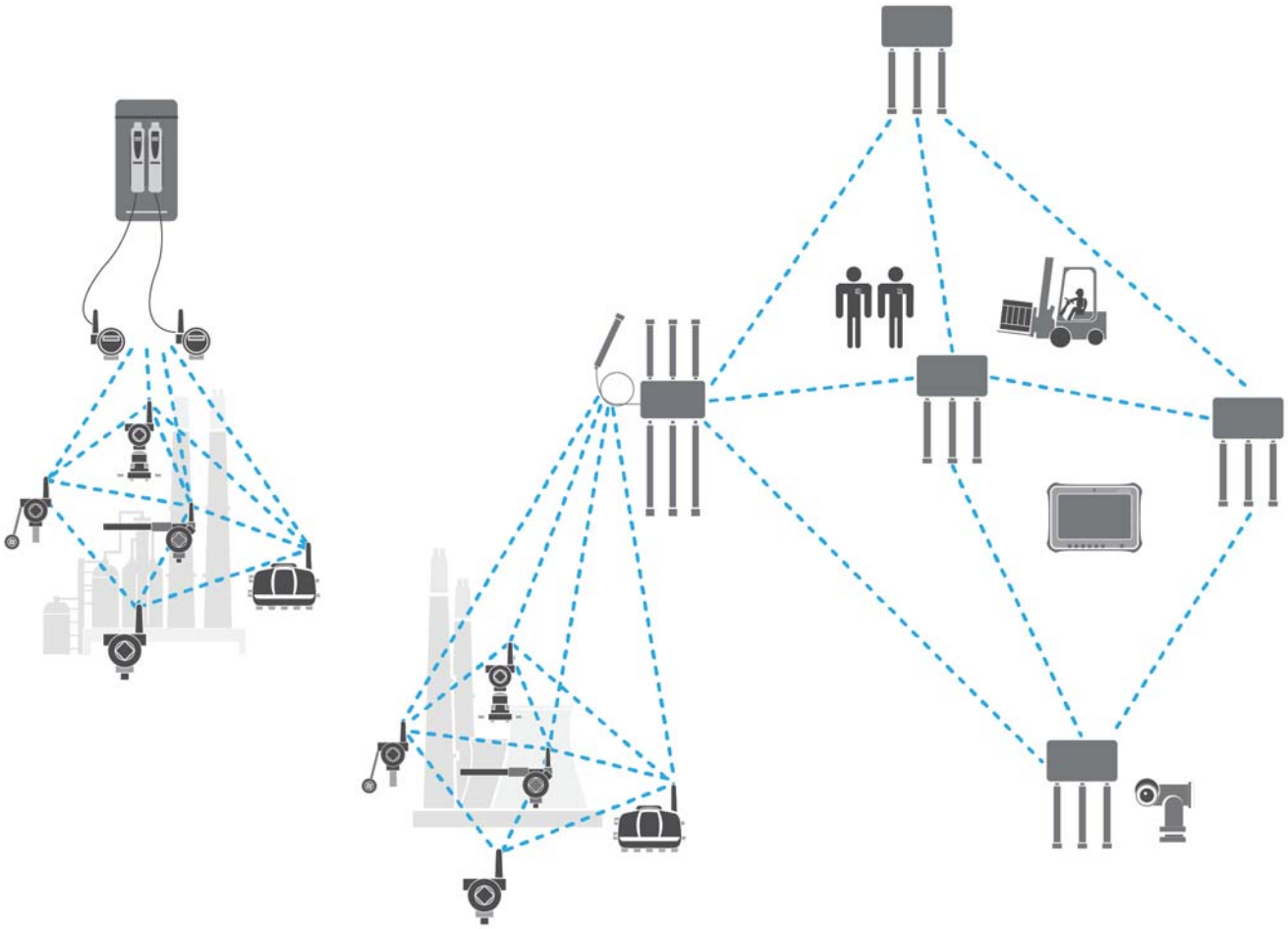
Emerson™ Wireless Security

*Wireless*HART® and Wi-Fi® Security



Wireless security is critical to the successful deployment of both field instrument networks and plant application solutions. This paper demonstrates Emerson's capabilities to deploy secure, reliable and robust wireless solutions for both field instrumentation and plant applications.

EMERSON

1.0 Introduction

This purpose of this document is to fully describe the Emerson Wireless Security Defense in Depth strategy for both IEC 62591 (*Wireless*HART) and Wi-Fi networks. It also describes:

- Emerson Wireless program
- *Wireless*HART standard
- Overall wireless plant network topology
- Application solutions (including how it securely and seamlessly integrates Emerson Wireless field Instruments)

The security features for both the *Wireless*HART field instruments and wireless plant network solutions are described in full.

2.0 Emerson Wireless

Emerson began the development of new wireless field instrumentation solutions several years ago – in partnership with other process industry vendors and customers – which resulted in the release of the *Wireless*HART (HART® 7) standard and ultimately the production of a variety of Emerson Wireless field instrumentation that fully complied with the *Wireless*HART standard.

*Wireless*HART is encapsulated in the HART 7 standard, so all *Wireless*HART devices share the same characteristics and features of wired HART devices – millions of which are installed throughout the world today. For you, it means that all the software, tools, and skills your workforce has today can be used in the commissioning, maintaining, and integration with today's process host systems. The devices do not require any type of Radio Frequency (RF) site survey, and are designed to be easily installed by following a few short best practices.

The *Wireless*HART standard is a single purpose standard. It was designed for devices to take process measurements, communicate those measurements through a mesh network, and easily integrate the measurement data with your existing process host system. The key to the design of the devices and the standard was to limit the power consumed by the devices such that they could be battery powered for 4 to 10 years.

To complement the wireless field instrument solutions, Emerson began offering plant operation solutions that utilized Wi-Fi technology for applications such as:

- Mobile Workforce
- Mobile Voice and Video
- Remote Video Monitoring
- Location Tracking
- Safety Mustering
- Field Data Backhaul
- Control Network Bridging

These "Wireless Plant Network" (WPN) solutions are all based on the IEEE 802.11-2007 family of standards "Wi-Fi" – which are driven by the IT community.

This is an important distinction between these two types of field and plant solutions: *Wireless*HART was created by the process industry for field instruments; Wi-Fi was created by the IT community to support a wide range of applications and solutions. Both standards are broadly adopted with proven solutions installed at customer sites throughout the world.

2.1 *Wireless*HART network communications

*Wireless*HART is a wireless mesh network communications protocol for process automation applications. It adds wireless capabilities to the HART protocol while maintaining compatibility with existing HART devices, commands and tools.

Each *Wireless*HART network includes three main elements:

- Wireless field devices connected to process or plant equipment
- Gateways that enable communication between these devices and host applications connected to a high-speed backbone or other existing plant communications network
- A network manager responsible for:
  - Configuring the network
  - Scheduling communications between devices
  - Managing message routes
  - Monitoring network health

Note
The network manager can be integrated into the gateway, host application or process automation controller.

The network uses the IEEE 802.15.4 radio operating at 2.4 GHz. The radios employ direct-sequence spread spectrum (DSSS) technology and channel hopping for communication security and reliability, as well as time division multiple access (TDMA) to ensure latency-controlled communications between devices on the network.

Each device in the mesh network can serve as a router for messages from other devices. This extends the range of the network and provides redundant communication routes to increase reliability to 99.9%.

Like wired HART, *Wireless*HART supports the full range of process monitoring and control applications, including:

- Equipment and process monitoring
- Environmental monitoring, energy management, regulatory compliance
- Asset management, predictive maintenance, advanced diagnostics
- Closed loop control (when appropriate)

Wireless technology will complement rather than replace wired instrumentation, and plants will often have both operating side by side. Virtually every process automation requirement is supported by one or more of the wired HART products available today. *Wireless*HART simply adds another way to communicate with HART devices.[1]

3.0 Wireless plant network overall topology

3.1 Purdue (ISA95) Model

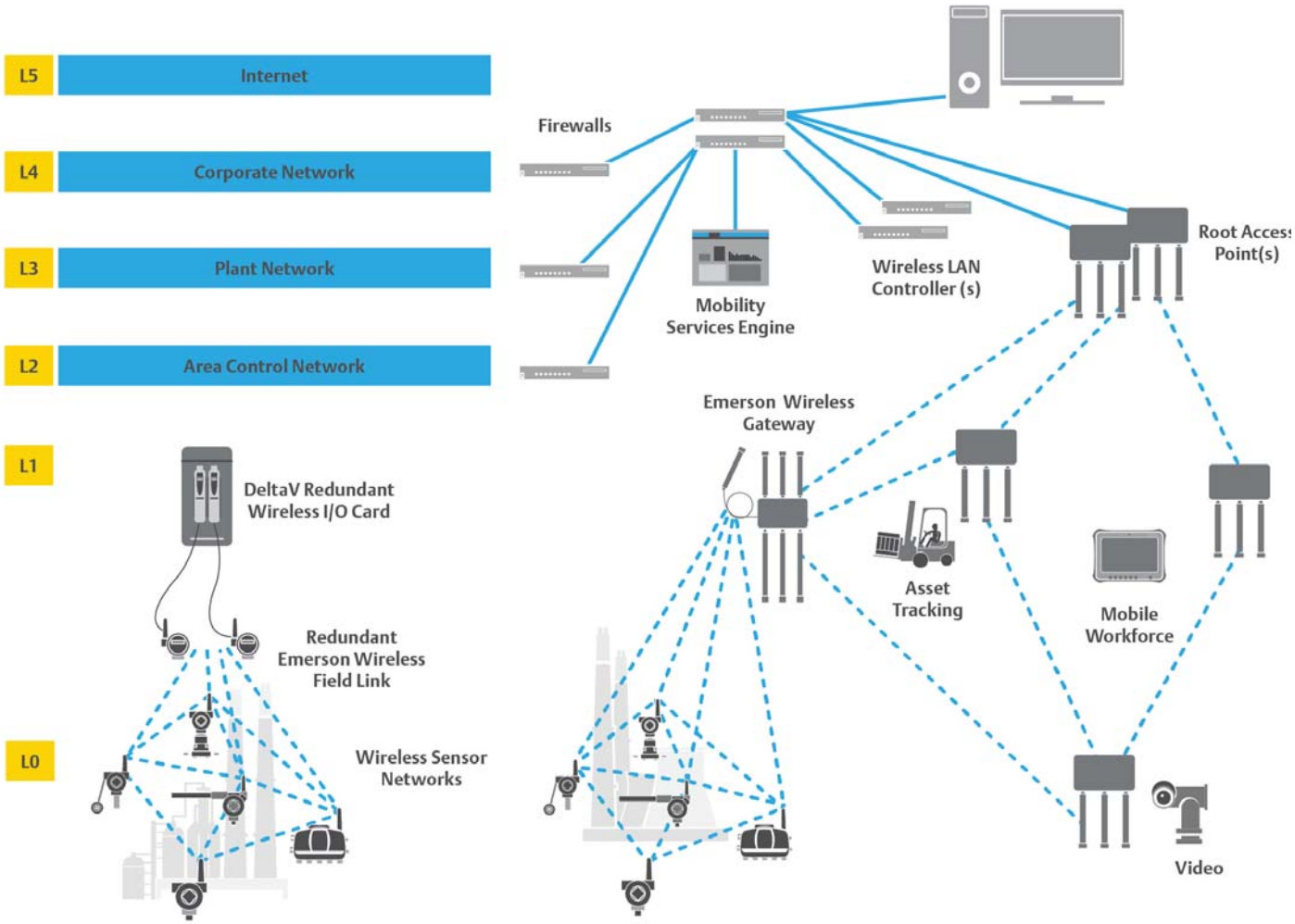
While the *Wireless*HART field instruments are only found at level 0, the wireless plant network must accommodate every other level of the Purdue (ISA95) network model. See accompanying network diagrams. It would be cost prohibitive to install a separate wireless network for each network level, so

1. *HART Communication Foundation, "Why WirelessHART: The Right Standard at the Right Time", October 2007*

each wireless network level is virtualized within the shared wireless hardware. Each secure virtual network is fully isolated in software from the other networks on the common wireless hardware.

Additionally, the wireless plant network supports “Differentiated Services” to establish a bandwidth allotment and priority for each of the virtual networks that must share the bandwidth. This allows the field instrument data (which actually requires very little bandwidth) to be communicated within the WPN at the highest priority.

Figure 1-1. Wireless Plant Network Architecture



Each of the wireless network devices: PDAs, laptops, RFID tags, or field instrument wireless Gateways, has its traffic routed from the device to one of plant network mesh access points. From there the communication travels back through the mesh network until it reaches the root access point. The communication passes directly to the managed switch where the virtual LANs are split in the different physical LANs. The communication is finally routed through a firewall at each network level that serves as "belt and suspenders" to ensure only traffic meant for each network level is routed through. Finally, the communication is routed to the appropriate final network device.

In the case of the wireless instruments, the data is communicated to the Emerson Wireless Gateway, and then routed as described above to a DeltaV™ controller (version 10.3 or later), a Modbus® TCP/IP device, an OPC Server, or AMS Suite.

Video device communications are routed to the Digital Video Recording Server – which can be located at Network Levels 3 or 4. The video camera devices are typically hard-wired into the mesh access points. The video cameras have authentication certificates installed on them to ensure only authorized cameras are installed on the network.

Mobile devices can communicate to any (Purdue model) network level (e.g. 2 through 4), but to only one SSID assigned subnet at a time (in order to prevent cross-over communications). The user of the network device signs on (authenticates) to the SSID where the handheld application will be communicating. There are different legitimate ways of authenticating the user and granting them access to a specific wireless virtual LAN – typically this is done through a RADIUS server which both authenticates and authorizes the user through active directory. The user signs on to the operating system of the device, and using those same credentials requests access to the particular SSID to exchange information with applications residing on the wired network.

Example Level 3 server applications which the client device would be communicating with would be:

- Terminal servers – for remote desktop applications
- DeltaV Remote Access Servers – for devices with DeltaV installed
- Historians
- OPC Servers
- AMS Suite

At Level 4, examples of those server applications would be:

- ERP
- Oil movements and blending applications
- Terminal management systems
- Other custom or proprietary applications

4.0 Field instrumentation integration

The Emerson wireless field instrumentation components integrate with the host control system through the Emerson Wireless Gateway in one of six ways:

1. Native DeltaV node as of version 10.3
2. OPC Server connection
3. Modbus TCP/IP connection
4. AMS HART TCP/IP
5. HART Port
6. EtherNet/IP™ connection
7. Modbus Serial connection

The first six Ethernet methods can all be extended through the WPN seamlessly provided the host system supports the corresponding protocol. Modbus Serial is supported by nearly all legacy control systems, but typically requires a wired connection.

4.1 Emerson Wireless field network integration

The wireless field network consists of several *Wireless*HART devices communicating in a self-organizing mesh network to an Emerson Wireless Gateway. For host systems that do not support *Wireless*HART native integration, there are three different methods to directly connect to the Emerson Wireless Gateway: Modbus Serial, Modbus TCP/IP, EtherNet/IP and OPC DA. These methods offer plenty of flexibility to implement an Emerson Wireless field network solution depending on the process needs.

Figure 1-2. Connecting via Multi-drop with a Modbus Serial Card

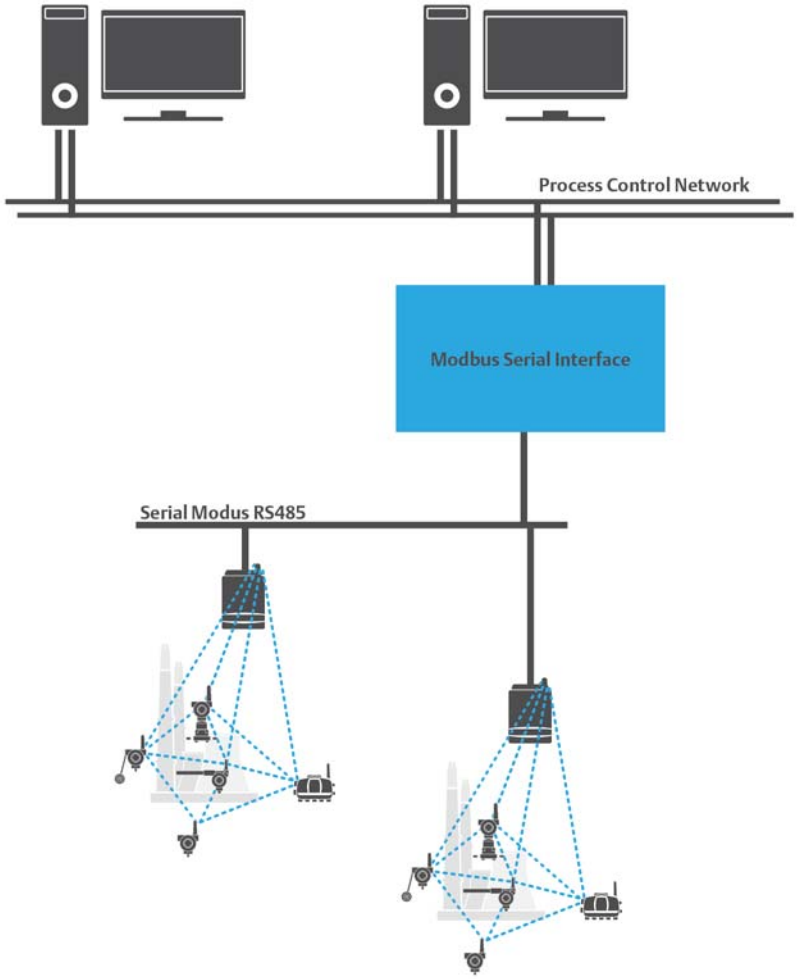


Figure 1-2 shows one of three ways to wire an Emerson Wireless Gateway to a control system and integrate the device data.

For many installations, it may not be convenient to pull a wire to the Gateway if it is located far from the main process. In that case, the Gateway can be connected back to central control room via a wireless plant network, or the Emerson 1552WU Wireless Gateway can be used which acts as a mesh access point for the Wi-Fi network and *Wireless*HART Gateway providing a more straightforward and economical manner to deploy pervasive sensing.

For all host systems that support Modbus TCP/IP or OPC, there are two supported methods to integrate the Emerson Wireless field network through the Emerson Wireless plant network as shown in Figure 1-3 and Figure 1-4.

Figure 1-3. Integration of Emerson Wireless Field Network via OPC DA

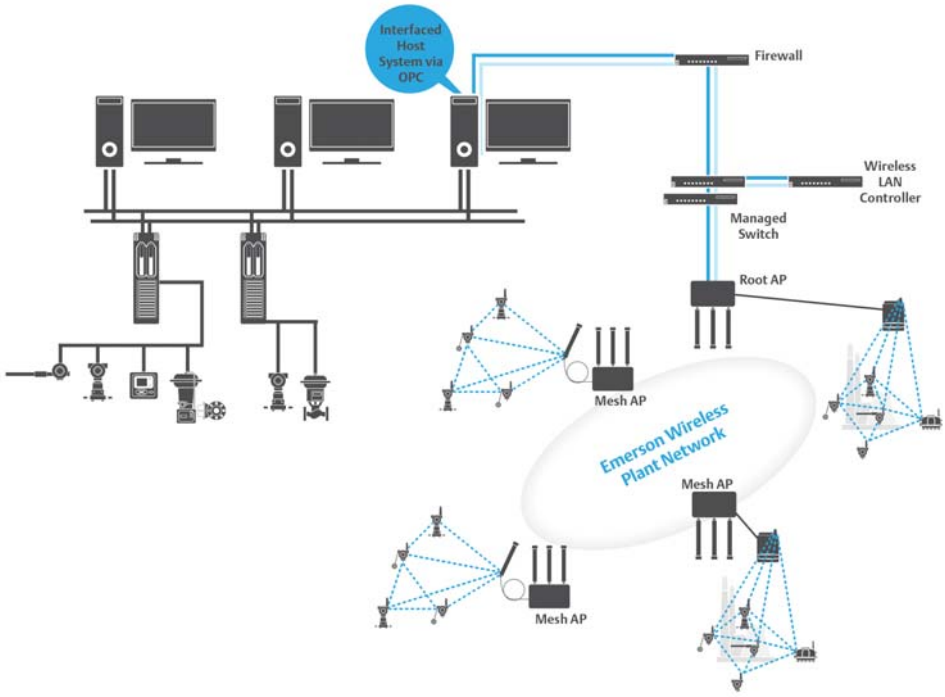
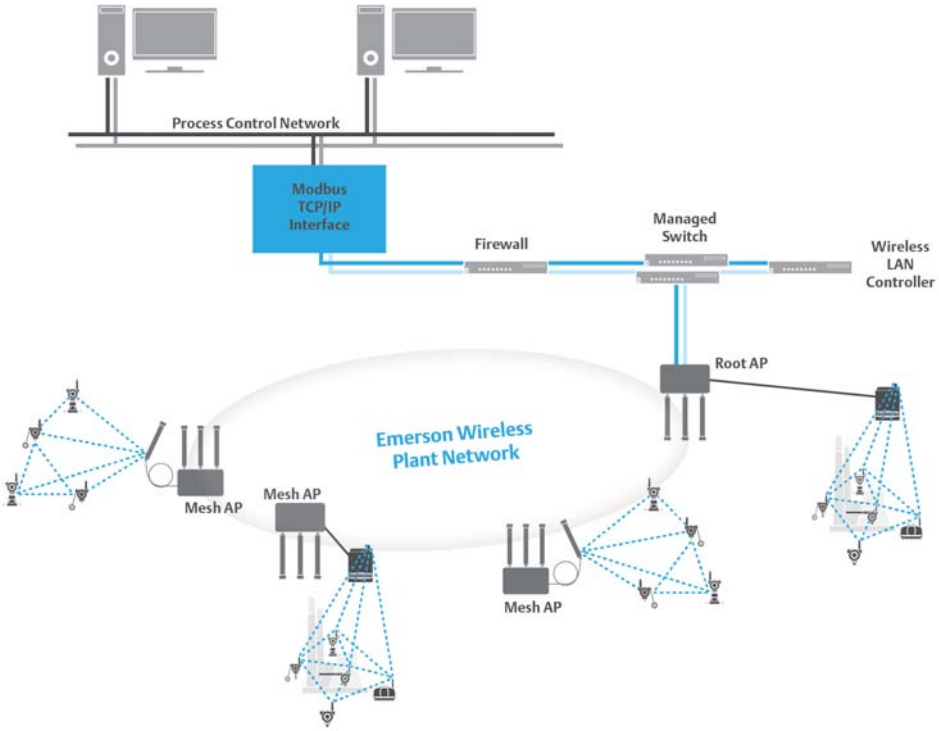


Figure 1-4. Integration of Emerson Wireless Field Network through Modbus TCP/IP Interface



4.2 Wireless plant network

All Emerson wireless plant network application solutions are delivered as turnkey solutions and include a number of services detailed in the previous section as part of the response and include:

- Site assessment and consultancy
- Network system design
- System deployment
- Training
- After project support

The Emerson wireless plant network is built with the following Cisco® network components (see “Wireless Network Architecture” image in Network architecture):

- 1550 series access points
- Wireless LAN (WLAN) controllers
- Prime infrastructure (optional)
- Mobility services engine (MSE) with wireless Intrusion Prevention System (wIPS) (optional)
- Managed switch
- Firewalls

5.0 Plant operation applications

5.1 Wireless field data backhaul

For those wireless field networks (e.g. tank farm) located far away from the central control room, the wireless plant network provides a reliable, scalable and cost-effective wireless mesh backhaul for the wireless field data to communicate with any host control system. The field data can be prioritized using the mesh network's *Class of Service* features to ensure minimal latency. With the wireless plant network, the remote wireless instrument data can be integrated into process control systems economically and quickly.

5.2 Mobile workforce

Mobile workforce applications allow field operators and maintenance workers to do a better job by having the information they need available to them where and when they need it.

Applications for handhelds are generally designed to work one of two ways:

- As a web-enabled client-server application where the main application is running on a server in your wired network and the user connects to it via browser on the handheld. This may be a web-based application that you already have in place.
- A terminal server is installed on the network and the client connects via remote desktop to an individual Windows session that hosts all the software applications the mobile worker needs access to, as in the case of a DeltaV distributed control system.

With the implementation of a wireless plant network, the mobile worker can roam through the plant, but use the Wi-Fi network to stay connected to the process.

Typical examples of connection might be:

- The DeltaV Remote Client, which allows a person to have access to all the capabilities of the DeltaV process automation system on a PDA or laptop. This would give the mobile operator or maintenance person visibility to the alarms and alerts and the ability to monitor the process while they are making their rounds.
- AMS Suite Remote Client provides the mobile user all of the capability of the AMS Suite package, including diagnostics and audit trail, which could be very helpful for troubleshooting a device.

Additionally, with a wireless network connection, the mobile user could access a Computerized Maintenance Management System (CMMS) package or tap into plant drawings or documentation, which could translate into a better, faster, and safer fix compared to doing the work without this information being immediately available.

The mobile workforce has an increasing number of client devices to choose from, with a wide variety of form factors and capabilities. Project-specific requirements would determine which handheld device fits the application being implemented.

5.3 Remote video monitoring

Video surveillance is becoming an indispensable part of process plant safety, security, and operations. Using wireless technology, mission-critical video feeds can now be delivered to the control room, office buildings and other areas in the plant in a highly flexible way that is not possible with a wired solution. The Emerson Wireless Solution for Wireless Video provides a cost-effective and fast approach for process plant security surveillance and operation monitoring. The solution uses high data throughput mesh Wi-Fi technology to transfer video data.

5.4 Safety mustering/location tracking

Wireless technology can track people and assets within a plant which can have many benefits including heightened safety – knowing quickly and accurately who is and isn't accounted for in an emergency. It also provides better visibility of your human and capital resources, so you can use your people and equipment more efficiently or be more responsive when needed. It can also be used to address security issues influenced by the movement of people and assets.

Harsh environments such as refineries and petro-chemical plants require technology that can protect personnel. Providing full visibility to people's locations in case of an emergency is extremely crucial to a safe evacuation or any required rapid reaction to an urgent situation. For example, when the eyewash station is turned on, there is a need to know who is using the eyewash station and who is nearby that can provide help.

5.5 Wireless control network bridge

In some situations, a DeltaV distributed control system needs to be managed remotely; for example, when a highway or water channel separates the control room from the controller, or when an I/O unit needs to be installed in a tank farm or remote site. Installing fiber-optic cable is expensive. Instead, DeltaV units can be connected using wireless technology securely and cost effectively.

As part of the Emerson Wireless offering, Emerson supports DeltaV distributed control systems that have wireless bridges on the area control network. Emerson will work with you to design, install, and perform a FAT/SAT on a wireless control network bridge through an Emerson service contract.

6.0 Wireless plant network security

6.1 Possible attack vectors

With no physical barrier surrounding a wireless plant network's transmissions over the air; it becomes absolutely necessary to have a wireless defense in depth strategy to protect the network against unauthorized access. The following are brief descriptions of some the possible attack vectors.

Rogue access points (APs)

An unsanctioned access point that is connected to the wired network and offers up local wireless service to (un)sanctioned clients. These access points can be "open" or have security employed (to both limit the (un)sanctioned users allowed to connect and help stay off administrators' radars). Rogue APs may offer service to either sanctioned or unsanctioned clients. The rogue AP may be maliciously attached to the network or a rogue AP may be attached by a legitimate employee trying to improve wireless coverage around their cubicle. In this later case, wireless connectivity may be allowed at the facility, but an employee attached a potentially unsecure AP to the network in an attempt to provide "better" wireless signal coverage around his or her cubicle. In the latter case as well, sanctioned clients could connect to the employee installed rogue AP.

Ad-hoc wireless bridges

A subset of the 802.11 protocol allows peer-to-peer connectivity, called ad-hoc networking. The main threat these networks pose is the possibility that machines connected to the wired network may be configured to also participate in such an ad-hoc connection, and the link between the two networks could then be bridged, thereby allowing unsanctioned wireless access to the wired network resources.

Man in the middle (Evil Twin, Honeypot AP, etc.) attacks

There are many types of these attacks, but all are based in the same exploit. An intruder inserts himself in between a legitimate client and the resources that client is attempting to access. This can be done between the client and the legitimate infrastructure, or by getting the client to connect to a rogue access point imitating the legitimate network. The specific exploit used will change over time as new protocol weaknesses are discovered and left unpatched.

Denial of service (DoS) attacks

There are several ways for interlopers to prevent legitimate clients from accessing the wireless network by sending failure messages or fake requests that cause the AP's resources to be consumed by the bad communications and not have sufficient bandwidth to serve a legitimate client that wants to connect and communicate.

Jamming (also considered DoS)

It is possible to cause radio interference on frequencies within the wireless spectrum by aiming a wireless transmitter at a particular area and disrupting communications with "noise."

Reconnaissance and cracking

Many active and passive reconnaissance tools exist to give both administrators and attackers information on network configuration and topology. "Cracking" tools take that a step further and can decipher wireless traffic, either on-the-fly or offline.

6.2 Wireless defense in depth

There are three key areas to a wireless defense in depth model:

1. Control access to the wireless network
2. Protect the wireless network infrastructure
3. Ensure the client integrity.

Most wireless network solutions only take the first step of controlling access to the network which is not sufficient to prevent a breach in the network. Even with all the tools Emerson provides, internal security policy enforcement and periodic log auditing are required to monitor for attackers attempting to breach the network.

Control access to the network

Controlling access to the network requires every user or device to authenticate with a centralized network domain authority. Emerson's solution utilizes an Authentication, Authorization, and Accounting (AAA) server with the RADIUS authentication protocol to coordinate access to the wireless network resources with the existing IT security infrastructure. This allows for centralized control of user's access to the wireless network and can control the user's authorization to access resources on the wired networks. Emerson's solution uses enterprise WPA2 with Extensible Authentication Protocols to authenticate users.

Device certificates can be installed on all approved mobile devices and access to the Wi-Fi network can be restricted to only devices with an approved certificates.

All wireless communications between the client device and the wireless network are encrypted utilizing AES 128-bit encryption preventing unauthorized eavesdropping or data manipulation of any of the communications.

The system monitors and logs network activity (authorized or illegitimate) allowing administrators to follow-up on any attempts to breach the network or attempt to access resources without prior authorization.

Protect the network

Each of the mesh APs on the wireless network is installed with a digital certificate that authenticates it to the wireless controller and allows it to participate in the secure network. This prevents "rogue" or unauthorized access points from mimicking genuine access points.

All communications (where allowed by law) within the wireless network are encrypted utilizing AES 128-bit encryption preventing eavesdropping or packet manipulation. Rogue APs are unable to insert themselves in the middle of the wireless infrastructure or otherwise compromise the network. Emerson also recommends all wireless networks that will have wireless user access to be deployed with a Wireless Intrusion Prevention System – described below.

Ensure client integrity

Even the most secure wired or wireless network can fall victim to a virus or worm from an infected device that connects to it. Emerson wireless solutions include antivirus software installed on wireless client devices to prevent any primary infection of the device. Good security practices should be in force that keep anti-virus software up to date – along with OS security patches. Emerson also strongly

recommends that any device (wired or wireless) that participates in a control solution not have access to e-mail or the Internet as those are the largest sources of infection.

Table 1-1. Plant Wireless Attacks vs. Mitigating Defenses

Attacks	Mitigating defenses					
	w IPS	Authentication	Data integrity	Encryption	Prime infrastructure	Client agent
Denial of service	✓				✓	
MAC spoofing		✓		✓		
Man in the middle	✓	✓	✓	✓		
Ad-hoc wireless bridge			✓		✓	
Rogue APs	✓	✓			✓	
Cracking tools		✓		✓	✓	✓
Non-802.11 attacks				✓	✓	
Client ad-hoc connections	✓	✓				✓
Network reconnaissance	✓			✓	✓	
Authentication and encryption cracking	✓	✓	✓	✓	✓	
Impersonation attempts	✓	✓	✓	✓	✓	

Wireless intrusion prevention system

Lastly, Emerson can deploy a wireless intrusion prevention system that monitors the communications on the wireless plant network. Communications on the network are scanned for unusual patterns and can alert an administrator if suspicious activity is detected. Additionally, the access points scan the airwaves for rogue clients and access points and alerts an administrator if any are found. The wIPS can also be configured to actively attack any rogue access points found within wireless range in order to prevent users from accidentally connecting to one. For jamming, counter measures exist to triangulate the source location in order to shut down the jamming signal and minimize downtime. A wireless intrusion prevention system continually monitors the RF airwaves and communication traffic and will identify and protect the network against the attacks shown in Table 1-1.

7.0 *Wireless*HART field instrument network security features

Note
Cyber-security measures built into version 4 and later of the Emerson Wireless Gateway have been certified by the National Institute of Standards and Technology to meet the requirements of Federal Information Processing Standard 197 (FIPS-197), and by Wurldtech for Achilles Level 1 Certification -- giving customers even greater confidence that their wireless networks are safe and secure.

The *Wireless*HART field network inherent security features for the Emerson Wireless Gateway, the DeltaV Wireless I/O card and Field Link, and devices from any vendor are nearly identical. They include:

- AES-128 encryption (NIST/IEEE compliant) for all communications within the device mesh network and the Gateway
- Individual device session keys to ensure end-to-end message authenticity, data integrity, receipt validation, and secrecy (non-eavesdropping by other devices in the mesh network) through data encryption
- Hop-by-hop CRC and MIC calculations to also ensure message authentication and verification as to source and receiver of communications
- Devices must have a "join key" pre-configured on the device. This can either be a common join key per WFN, or optionally an individual join key per device.

Note
It is important to not use default join keys.

- "White listing" (ACL) – If individual join keys are used, devices are explicitly given permission to join the network via the Gateway/network manager via an ACL entry which also includes their globally unique HART address. White listing is the recommended mode of operation for the wireless Gateway. White listing is not supported in the DeltaV WIOC.

All of these security features combine to produce an extremely robust communications system yet remains easy to use/manage. While the WirelessHART standard fully encrypts field communication and ensures only authenticated devices can communicate on the network, this is not entirely sufficient to secure the device network solution. It also requires the connectivity from the field network Gateway device to the host system to be secured.

The connectivity from the Emerson Wireless Gateway to the host system is secured by:

- An internal firewall which is easily configured to permit only the protocols and ports required for the field solution to be enabled for communication
- Ethernet-based protocols (Modbus, OPC, EtherNet/IP, AMS, HART Port, https) all support SSL-protected communications
- The Gateway's internal bi-directional firewall is implemented with the default to "reject all," with user-defined protocols and ports opened utilizing a *Setup-Security-Protocols* screen
- The firewall does not require active management

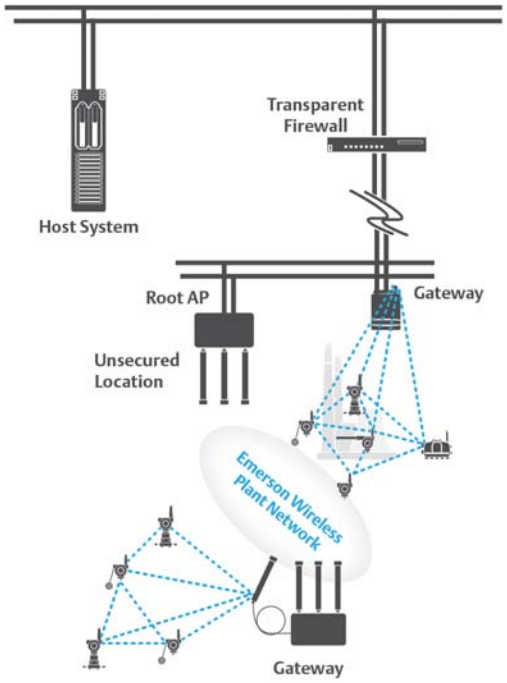
Table 1-2. Field Wireless Attacks vs. Mitigating Defenses

Attacks	Mitigating defenses				
	Anti-jamming	Authentication	Verification	Encryption	Key management
Denial of service	✓				✓
Spoofing		✓		✓	
Man in the middle		✓	✓	✓	
Replay			✓		✓
HELLO floods	✓	✓	✓		✓
Sinkholes		✓		✓	✓
Eavesdropping				✓	✓

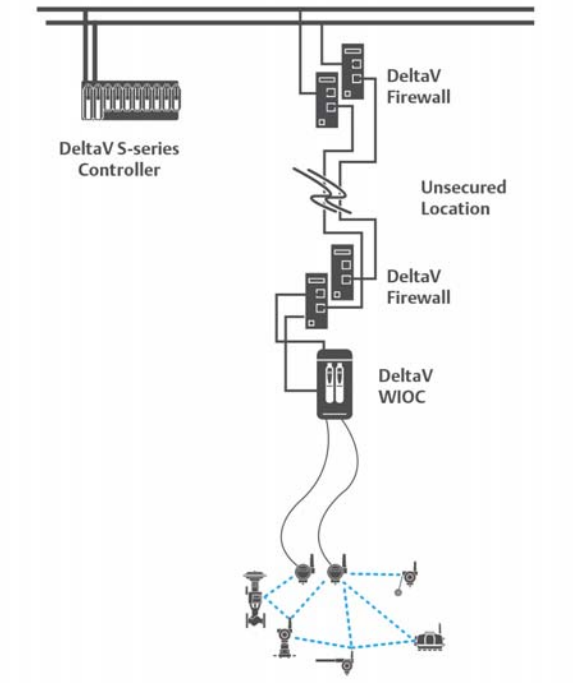
To protect against intruders attempting to break into the plant network via the Ethernet connection between the Gateway and the plant – particularly when the Gateway is not in a secured location – a firewall can be installed on the plant side of the wire in a secure location.

Figure 1-5. Firewalls

Transparent firewall installed between Gateway and host system



DeltaV Firewall between the WIOC and DeltaV system



DeltaV wireless I/O card

In addition to the Emerson Wireless Gateway, Emerson also has a DeltaV redundant wireless I/O card (WIOC) and Rosemount Field Link 781 for native integration to version 11 and later DeltaV systems.

The connectivity from the Emerson DeltaV WIOC to the DeltaV controller is secured by:

- An external DeltaV firewall configured to only permit DeltaV protocols and ports to be enabled for communication
- The WIOC itself rejects any communications that do not conform to the DeltaV proprietary protocol
- The WIOC is configured and managed by the DeltaV application software

8.0 Requirements for wireless security

The following section addresses well known security issues with the technology of the day. While the issues still exist, the solutions to mitigate these security concerns continue to evolve.

8.1 Emerson Wireless field instruments

Since the Gateway for the Emerson Wireless field instrument network has an Ethernet connection in the process area, many customers will want a separate firewall to be installed where the Gateway connects to the process IP network. It is understood that the reasoning for this is to prevent potential vulnerabilities between the Gateway and the process control network. Emerson has addressed this requirement by

designing the Gateway as both a field instrument wireless access point and dedicated firewall in order to eliminate the management and associated costs of an additional network device.

The Gateway's firewall is easy to configure, requires no active management afterwards, and limits all communications to just those ports required for the chosen protocols by which the process data is communicated and the Gateway's configuration is managed.

In order to protect the plant or DCS network from intrusion, Emerson can supply a separate firewall that limits communications and access to those ports required by the Gateway and the DCS.

The following sections describe how the Emerson Wireless network defends against the various attack vectors.

Jamming

*Wireless*HART uses IEEE 802.15.4 radios (2.4 GHz) with channel hopping on top of the standard Direct-Sequence Spread Spectrum. This combination has proven highly resistant to interference in numerous harsh real-world applications. The *Wireless*HART network is a self-forming, self-healing mesh network which allows devices to route their communications through other devices to the Gateway along multiple routes – increasing the reliability of the communications of the network to over 99.9%.

Emerson has performed numerous coexistence tests which show *Wireless*HART can coexist with Wi-Fi without channel blacklisting, without either communication protocol incurring significant degradation.

Eavesdropping

Each device has its own session key with the Gateway that enables encrypted communications between each device and the Gateway that cannot be deciphered – not even by other *Wireless*HART devices that are forwarding the message on behalf of the originating device.

Detection

Even though devices within the *Wireless*HART network are transmitting at a much lower power than 802.11 devices, detection of those communications is still possible. This is why the *Wireless*HART security measures utilize many techniques such that all an unauthorized user would be able to do is detect that some type of wireless communications were occurring but would not be able to gain access, eavesdrop, or otherwise disrupt the network.

Replay (or Delay) attacks

The *Wireless*HART Gateway manages the security for the device network. After each device joins the network, it receives the network key and an individual session key for encrypting all communications between it and the Gateway. There is no need to change the network or session keys because within each message is a Cryptographic nonce (number used once) which will essentially never roll over. Use of a nonce combined with a robust crypto algorithm and sufficient key length ensures that even repetitive messages will result in unique encrypted message strings.

The Data Link layer nonce consists of the 8 octet source address plus the full 5 octet ASN (time counter at 10ms increments). At one second sampling the ASN doesn't roll over for at least 300 years (i.e. the Data Link nonce will never be reused) thus preventing replay attacks. Since the nonce includes time, delay attacks are also thwarted. The network link layer nonce used for managing the *Wireless*HART network is shared by all the devices. *Wireless*HART again uses the 8 octet source address plus a 4 octet counter plus a 1 octet 0 pad. At one second sampling, the nonce will not roll over for 136 years.

Man in the middle (backdoor)

Devices are protected against man in the middle attacks by the data link layer nonce and message integrity code calculations which occur on a device hop-by-hop basis. While the *Wireless*HART standard fully encrypts field communication and ensures only authenticated devices can communicate on the

network, this is not entirely sufficient to secure the device network solution. It is also important to note that *Wireless*HART intentionally does not implement "IP to the edge", thus eliminating the risk of numerous pre-existing attack malware being utilized against the WFN. However, to fully secure communications end-to-end from the field device to the data consumer, the connectivity from the field network Gateway device to the host system must also be secured.

Sybil attack

In a Sybil attack the attacker subverts the reputation system of a peer-to-peer network by creating a large number of identities, using them to gain a disproportionately large influence. First of all, all devices on a *Wireless*HART network must be authenticated so rogue devices will never be allowed to join the network. Using a unique Join key for each device creates an access control list (ACL) back at the wireless Gateway. Each device has its own unique identity which is controlled and maintained by the Gateway and visible to the user. ACLs are specified in the *Wireless*HART specification (IEC-62591) and they ensure that only one device could represent one identity. The *Wireless*HART specification also provides either on demand or automatic key rotation. Key rotation is managed via the Gateway web interface for Emerson *Wireless*HART systems or available as a function within DeltaV Explorer for the DeltaV wireless I/O Card.

Emerson Wireless network management

Securing the network requires a few best practices by the user, but the network does most of the heavy lifting as described below.

Join key management

The Gateway administrator can configure the join key to be a single key for all devices in the network, or unique per device. A common join key is only visible to the administrator on the Gateway. Individual join keys are invisible to everyone, at all times. Only the administrator can change the join key(s).

The common (or each individual device) join key can be changed in the Emerson Wireless Gateway at any time. This change is securely propagated through the *Wireless*HART mesh network – rendering the old join key(s) obsolete. When using a 375 or 475 handheld to configure device join keys, this allows for a large deployment of devices to be completed and afterwards change the join key – protecting the network from a malicious or careless insider.

For tighter security that is easier to use, device technicians can use the AMS Device Manager application and a HART modem to configure the WirelessHART devices before they are installed and joined to the *Wireless*HART network. When using the AMS Device Manager's graphical interface, the join key is assigned to the device without the user seeing the hexadecimal representation of the key.

No frequency planning required

There is no frequency planning required for *Wireless*HART networks. By design, the protocol utilizes every channel in the 2.4 GHz range by channel hopping during the course of normal communications. A separate white paper is available from Emerson on coexistence testing performed between *Wireless*HART and Wi-Fi devices. As long as the Wi-Fi devices and *Wireless*HART instruments are kept one meter apart, there are no coexistence issues with the network communications.

Unauthorized access prevention

The Gateway's password strength is controlled locally. Factory accounts can no longer be activated by a local administrator **without** having a factory-supplied firmware option key. This key is signed and is unique to a specific Gateway. The administrator can then revoke this option later.

No location sensing is available at the instrument level at this time. The Gateway's internal functions are protected through role-based access control internally on the Gateway. Users must be assigned roles and provided the appropriate passwords based on their required privileges to have access.

Good processes/procedures for password control for the Gateway user interface are expected and will prevent any tampering with the Gateway settings.

Physical access

Physical security is an important part of any security program and fundamental to protecting your system. Restrict physical access by unauthorized personnel to protect end users' assets. This is true not only for *Wireless*HART systems but all systems used within the facility. Unauthorized personnel can potentially cause significant damage to end users' equipment. This could be intentional or unintentional and needs to be protected against.

Role-based security

The Gateway has role-based security to enable four levels of access to the features the end user can configure.

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 custom trends
Administrator	admin	Includes all maintenance privileges Configure Ethernet network settings Configure *Wireless*HART network settings Set passwords Set time settings Set home page options Configure customer point pages Restart applications

The DeltaV and AMS software has permission based security to determine the level of access that a user can have to wireless devices and the WIOC.

Permission "key"	Control system access
Configure or Device Write	Commission a WIOC Assign a wireless device to a channel Modify device settings
Operate	Read-only access
Diagnostics	WIOC switchover to standby device

8.2 Mobile workforce and Wi-Fi/WLAN 802.11

The Emerson Wireless Solutions are delivered using Cisco's Wi-Fi Mesh technology – which is based on the 802.11-2007 family of standards.

The standardization of Wi-Fi use and commercial availability of equipment is regarded by Emerson as having tremendous value – by allowing you to choose from a wide variety of products and applications that easily communicate and integrate for new applications and solutions.

The concerns raised in this section are correct with respect to the 802.11 standard as being a security risk because the wireless signals transmitted can be received by any commercially available 802.11 compliant device.

These risks can be overcome, but they require solutions based on these standards to exercise multiple mitigating techniques in order to secure them from the many types of security risks and attacks that are known to have occurred in the public domain.

At a minimum, by authenticating users before allowing them to access the wireless network, most attackers can be kept off of the network. Additionally, the Emerson-deployed solution encrypts all wireless data that is transmitted within the Wi-Fi mesh network and between the Wi-Fi mesh network and all client devices, to prevent unauthorized users from eavesdropping on any communications or from manipulating any information transmitted wirelessly.

The following sections describe how the wireless plant network defends against the various attack vectors.

Jamming

The Emerson wireless plant network solutions are delivered as a controller-based mesh access point system rather than through a simple set of autonomous access points.

Autonomous APs are configured to communicate on a single channel and must be manually changed by the user if it is discovered that interference is occurring nearby.

There are many advantages to the Emerson controller-based solution:

- Mesh APs within the system monitor the airwaves and the signals from the other mesh APs and dynamically adjust both their signal strength and the channel they are communicating on in order minimize interference from both outside the mesh network and within it.
- While each mesh AP is capable of transmitting on a different channel, the client device is seamlessly handed off from one mesh AP to another without the user having to do anything with respect to channel management.
- When combined with a wireless Intrusion prevention system, the mesh network will simultaneously monitor the airwaves for signals that are attempting to jam the mesh, alert the administrator of the issue, and triangulate on the source of the jamming signal.

Rogue access points

Rogue access points (or laptops) are prevented from joining the mesh network infrastructure though device authentication. Each mesh AP has a unique signed X.509 digital certificate. This digital certificate authenticates the AP to the entire mesh network. Access points attempting to join the network or mimic the network are flagged by the intrusion prevention system.

One or more additional Wi-Fi APs are installed within the plant that listen on the frequencies utilized by the plant. Anomalous communications are flagged for attention by the wIPS on the prime infrastructure.

Site assessment

As part of the Emerson Wireless services for plant Wi-Fi applications, a site assessment is performed throughout the facility to detect internal RF signals and potential interference from neighboring areas. The wireless engineer will design the network such that the mesh AP placement and antenna type will minimize potential interference. For Field *Wireless*HART only installations, a site assessment is unnecessary.

The mesh network uses 802.11b/g/n for the client access and 802.11a/n for wireless backhaul of the client communications to the wired network. The network deploys the Class of Service standard which allows several Virtual LANs to be configured to be available to client devices on a single wireless mesh network. This allows office domain users to share the same physical mesh network as the process control domain users, but they are completely isolated from one another. This eliminates the concern of having multiple Wi-Fi networks. There would be only one shared wireless mesh network in the plant.

Detection

Emerson recommends that customers always broadcast the SSID. Disabling or hiding the SSID does not offer any meaningful security and actually hinders roaming. The SSID is transmitted in probe request and association request frames. These frames are not encrypted and sent in clear text so the SSID is easily discovered even when not broadcast.

Eavesdropping

The Emerson WPN deploys WPA2 (AES 128 bit) security encryption where permitted.

The WPN includes integration with an Authentication, Authorization, and Accounting Server utilizing the RADIUS protocol to securely authenticate users with their standard network credentials which allows for dynamic key management and eliminates it as a security concern for the user when a resilient EAP method is chosen.

Wireless network isolation

The WPN supports many virtual wireless LANs which eventually must be connected to one or more wired networks. This is achieved through a managed switch. While the managed switch is sufficient to isolate each virtual LAN to communicate **only** with its wired network, Emerson supports firewalls to further ensure traffic is routed properly as a "belt and suspenders" approach to prevent network crossover.

Emerson supports user configurable addressing to have DHCP turned off and only use static IP addressing if desired.

8.3 Manageability/maintainability

Training

Because Emerson Wi-Fi solutions are relatively complex when compared with wireless field instruments, Emerson will work together with you to specify a training curriculum that meets your specific needs and can include but is not limited to training on wireless:

- Network management
  - Control of equipment and configuration
  - Location and installation specific information
  - Management of the shared wireless access for corporate and plant networks
- Security management
  - User access and authorization
  - Password management through normal IT control
  - Security risks/threats
- Specific applications delivered as part of the solution

The training is intended to have you be as self-sufficient as desired.

Support

Emerson provides a comprehensive support structure to help you resolve issues in your day-to-day operations. The WPN support is delivered under a local service agreement. Those agreements are tailored using the SureService™ portfolio to your needs and interests. Service delivery is provided through a combination of Emerson expert technical support and local support. Consistent with DeltaV, WPN customers may contact the global service center for expert technical support.

A complete Emerson Wireless solution – after project support portfolio was developed covering:

- Expert technical support
- Emergency on-site services
- Spares management programs
- Scheduled on-site maintenance – software updates
- Application support/life cycle management

Unauthorized access prevention

The Emerson solution specifies an AAA server which can be located within the network and configured to work with your site's IT security systems to maintain individual user single sign-on credentials for either or both the office domain and process domain. This prevents users from having to maintain separate credentials for the wireless, plant, and corporate networks. IT can manage the wireless network access as it does the wired network. This is achieved through the use of RADIUS servers that can be located on the different networks to authenticate users authorized to access that specific network (plant or office).

The WPN supports granting administrative rights and privileges to specific users and groups of users in order to limit access to sensitive network configuration management.

The WPN supports WPA2 enterprise key management in order to eliminate the need to manage keys per user. Network level certificates (keys) are will protected within the WPN management software so that only authorized users have access in order to extend the network or change the keys.

Wireless user session keys (used to encrypt communications between the client device and the access point) are renewed each time a client device associates with a mesh access point, so there is no need to manage session key rotation.

Two-factor authentication compatible with Microsoft® Windows™ CryptoAPI can be used for authentication with the device, connecting to the wireless network, and logging onto applications/servers on the plant and office network.

8.4 Wireless – an engineered solution

Emerson WPN solutions are delivered as a specified turnkey solution that includes:

Site assessment and application consultation

Emerson wireless engineers will meet with your plant's wireless stakeholders to develop an overall plan for your current and long terms needs. Based on the specific application Emerson is asked to deploy, the engineers will conduct an RF study at the site and collect other on-site information used to determine the number and location of the mesh access points.

System architecture and network design and planning

Based on the site survey result and the applications being deployed to meet your business requirements, engineers design the overall system architecture, including the network infrastructure, security measures, and the applications. The network design and planning process creates a detailed network infrastructure that can be reviewed with your site's process and IT personnel to ensure all requirements are correctly designed and planned.

Physical network installation management and system commissioning

Emerson delivers the detailed instructions for the location and how each mesh access point is to be installed in the process plant. Emerson can install the wireless equipment or you can elect to install with other resources. After the network components are installed, Emerson will configure network components and commission the entire network.

Application implementation

Based on your specified application requirements, engineers design and implement the applications into the wireless solution and install them onsite.

9.0 Wireless bridging links

The Emerson wireless bridging solutions have available all the security features detailed in the previous section – the most important feature is full encryption of all wireless communications between the Wi-Fi bridged devices. Emerson recommends these additional installation guidelines:

- Install managed switches in the installation in order to enable the wireless network and the interconnecting wired network to be monitored.
- Utilize the 5 GHz band if possible (depends on world area) as the 2.4 GHz band can be overcrowded.
- Monitor the nodes in the path of the wireless communication network with a Simple Network Management Protocol (SNMP) monitoring application. WhatsUp® Gold is an example of one application that can be used to monitor and troubleshoot communication issues should they arise.
- Configure the SNMP monitoring to periodically check to ensure the wireless communications have not degraded over time due to changes in the surrounding environment.

9.1 Jamming

See "Jamming" on page 18.

9.2 Detection

Networks that are bridged wirelessly are typically configured without client access (i.e. there is no advertised network access for rogue clients to detect).

9.3 Eavesdropping

The bridge solution is fully encrypted utilizing AES private certificates. Access to these private keys are limited to a specified few individuals.

10.0 Approvals

If your site has its own specific security requirements for wireless applications, Emerson can work with you to address all of your security concerns and requirements.

11.0 Network architecture

The following pages identify the components of a wireless plant network solution as shown in Figure 1-6 on page 26. While the applications provided by Emerson all share the wireless plant infrastructure equipment, their communications are all securely isolated from one another. All critical components in the wireless plant network solution can have a redundant partner.

A. Emerson Wireless Gateway

Configuration management of the wireless field network is achieved through version 10 or later of either the DeltaV system or AMS Intelligent Device Manager applications. The Gateway is autosensed when it is plugged into the DeltaV Control Network. Drag and drop the unassigned Gateway to the wireless I/O subsystem and it is automatically configured with an IP address. Wireless transmitters that are joined to the Gateway's network auto populate the database. The user simply has to drag and drop the new wireless transmitter to a channel assignment. From a configuration perspective the wireless transmitter now looks like any other wired device. I/O from the Gateway can be assigned to one controller. The Gateway and all its communications are managed through the DeltaV control system and its associated

applications. The Emerson 1420 and 1552WU are both wireless Gateways that can be integrated to DeltaV, whereas the Emerson 1552WU also includes Wi-Fi connectivity.

B. Wireless I/O card

In version 11 of DeltaV the redundant wireless I/O Card (WIOC) was introduced and allows for a fully redundant plug and play solution for DeltaV. The *Wireless*HART device network is managed by the WIOC through the radio located within the Rosemount 781 Field Link device. The *Wireless*HART network and security management of the wireless devices is performed by the WIOC in the same manner as it is for the Emerson Wireless Gateway.

The WIOC is autosensed when it is plugged into the DeltaV Control Network. Drag and drop the unassigned WIOC to the wireless I/O subsystem and it is automatically configured with an IP address. Wireless transmitters that are joined to the WIOC's network auto populate the database. The user simply has to drag and drop the new wireless transmitter to a channel assignment. From a configuration perspective the wireless transmitter now looks like any other wired device. I/O from the WIOC can be assigned to up to four controllers. The WIOC and all its communications are managed through the DeltaV control system and its associated applications.

C. Wireless DMZ

The wireless DMZ further isolates the applications on the wireless network from the plant and corporate networks by isolating the application server communications behind a firewall on a separate network IP address range and controlling access from all sides. Security is enforced within the domain, but management of the wireless DMZ is possible from different networks.

D. Distribution layer switch

This is the managed switch at the center of the wireless and wired communications. The virtual LANs of the shared wireless network are configured and connected to each of the respective wired networks. The components of the wireless DMZ are all connected to the wireless network at the switch. This switch has basic firewall capability, but an additional firewall can be added for better performance if required.

E. Wireless LAN Controller

The controller is the component that automatically and actively manages the mesh APs of the wireless plant network. Security of the communications within the network itself is managed by the controller as well as ensuring only authorized mesh APs can join the network. The wireless LAN controller is the device that is responsible for network-wide wireless functions such as security policies, intrusion detection, RF management, Quality of Service (QoS), and mobility. Communications from Wi-Fi clients pass through the wireless LAN controller in a CAPWAP tunnel – after which they land on the wired network. Devices that are hardwired into a mesh AP do not pass through the wireless LAN controller – they land on the wired network right at the root AP.

F. Prime infrastructure

The prime infrastructure is the graphical tool that allows the administrator to easily configure and manage the entire wireless network by allowing network managers to design, control, and monitor enterprise wireless networks from a single location, simplifying operations. It oversees a series of WLAN controllers. This software provides network management including diagnostics and troubleshooting tools to keep the network running smooth.

G. Prime infrastructure with wireless intrusion prevention system (wIPS)

The wIPS adds another layer to wireless defense in depth protection against potential wireless attacks. Beyond just controlling access to the network, wIPS protects the wireless network from attackers, and ensures the integrity of all wireless clients that access the network. A Cisco 3600-Series Access Point is configured to monitor the RF Spectrum and communicate anomalies to the prime infrastructure with wIPS.

H. Mobility services engine (MSE)

The MSE is required for wIPS and for location tracking solutions. It performs all the mathematics and works in conjunction with the Prime Infrastructure to report anomalies detected by the wireless network.

I. DeltaV firewall

A DeltaV firewall is a transparent firewall (i.e. it is configured to have the same subnet on both sides of the firewall) yet constrain the communications to be between only DeltaV devices by restricting access to only those ports required by DeltaV to communicate between the WIOC and the area control network through the wireless plant network.

J. Emerson Wireless Gateway OPC Server

The Gateway can communicate data to OPC clients (e.g. OPC Mirror) through the Gateway's OPC Server installed on a PC on the wired network. The Gateway's OPC Server application communicates to the Gateway via an SSL secured communication link. The OPC DA standard versions 2 and 3 are fully supported. The OPC server is utilized when a native *Wireless*HART interface on the host DCS does not exist.

K. DeltaV OPC Server

The easiest way to link the Gateway with a DeltaV version 9 or earlier system is through the DeltaV OPC Server which can be licensed on a DeltaV application or base station.

L. Mesh access point

Mesh access points provide the connection to roaming Wi-Fi enabled handheld devices used by the mobile worker, or fixed Wi-Fi resources (e.g. video cameras). Additionally, fixed assets such as the wireless field Gateway can have a wired connection to the mesh access point which provides a wireless backhaul to the root AP and on to the wired network – connecting the Gateway to the host control system. The Emerson 1552WU Wireless Gateway is also a mesh access point for the Wi-Fi network.

M. Video cameras

A large variety of cameras are available for use in a remote video monitoring solution including fixed, pan-tilt-zoom (PTZ), wireless, and thermal imaging. Most of the cameras are wired into the mesh access points for backhaul communications.

N. Video server

All video images are centrally recorded, stored and served to other workstation and applications from the digital video recording server. Users can remotely view or store video from a variety of IP cameras, review stored video and snapshots, and click-to-point control of PTZ cameras though an Internet browser interface. All video images are centrally recorded, stored and served to other workstation and applications from the digital video recording server which can be located within the wireless DMZ.

O. Video client

The video client provides a configurable interface to the network cameras. A client of the video server, the video client can manage multiple cameras from multiple video servers. The user can define how to use screen real estate in with an unlimited number of multi-up, multi-function views. From these views users can view live and stored video, control PTZ cameras, schedule camera tours, and manage alarms.

P. RFID Wi-Fi asset tag

The RFID tags communicate their location through the Wi-Fi mesh network. A variety of tags are available including those that have call buttons to signal an emergency for the wearer.

Q. Location server

The location server is where all the rules for location alerts are executed, and configuration of user and asset data is stored.

R. Location client

This web-based application allows any user to visually see the locations of assets and personnel on a display map. Specific personnel movements can be tracked in real-time on the graphical display. Operators have ready access to contact information for field personnel or physical characteristics of physical assets simply by clicking on the asset's onscreen icon.

S. Redundant bridged access points

There are several models of wireless access points available for deployment as a wireless bridge depending on network needs. There are indoor and outdoor models as well as Class I, Div 2 or ATEX Zone 2 certified equipment. The radio utilized can be based on IEEE 802.11a/b/g/n standards following the local regulations and the specific requirements of the solution.

T. Handheld devices

While Emerson promotes the Panasonic® Toughbook® CF-19 and CF-31, and the Panasonic Toughpad® FZ-G1: rugged tablet capable of running Emerson's Plantweb™ applications with a wireless connection to the process; Emerson also supports other wireless laptops and PDAs as specified and requested by the user. Emerson can provide custom program solutions as an engineered solution upon request.

U. Remote access service (RAS)

Mobile DeltaV operated devices connect to the DeltaV Application Server (which hosts the remote access service) that sits inside the wireless DMZ. All DeltaV process information is indirectly routed from the RAS located on the control/plant network, through the wireless DMZ to the RAS located inside the wireless DMZ. This enables an even greater amount of secure communication isolation.

V. Terminal server

Alternatively, a terminal server solution can be implemented for other legacy control systems – provided those systems support Microsoft's or some other vendor's terminal server solution. Emerson can work with you to determine the viability and requirements for such a solution.

W. RADIUS server

This is a RADIUS server that authenticates and authorizes users to access the wireless network and the specific SSIDs (VLANs). This allows for ease of maintenance of user access through the configuration of local group policies.

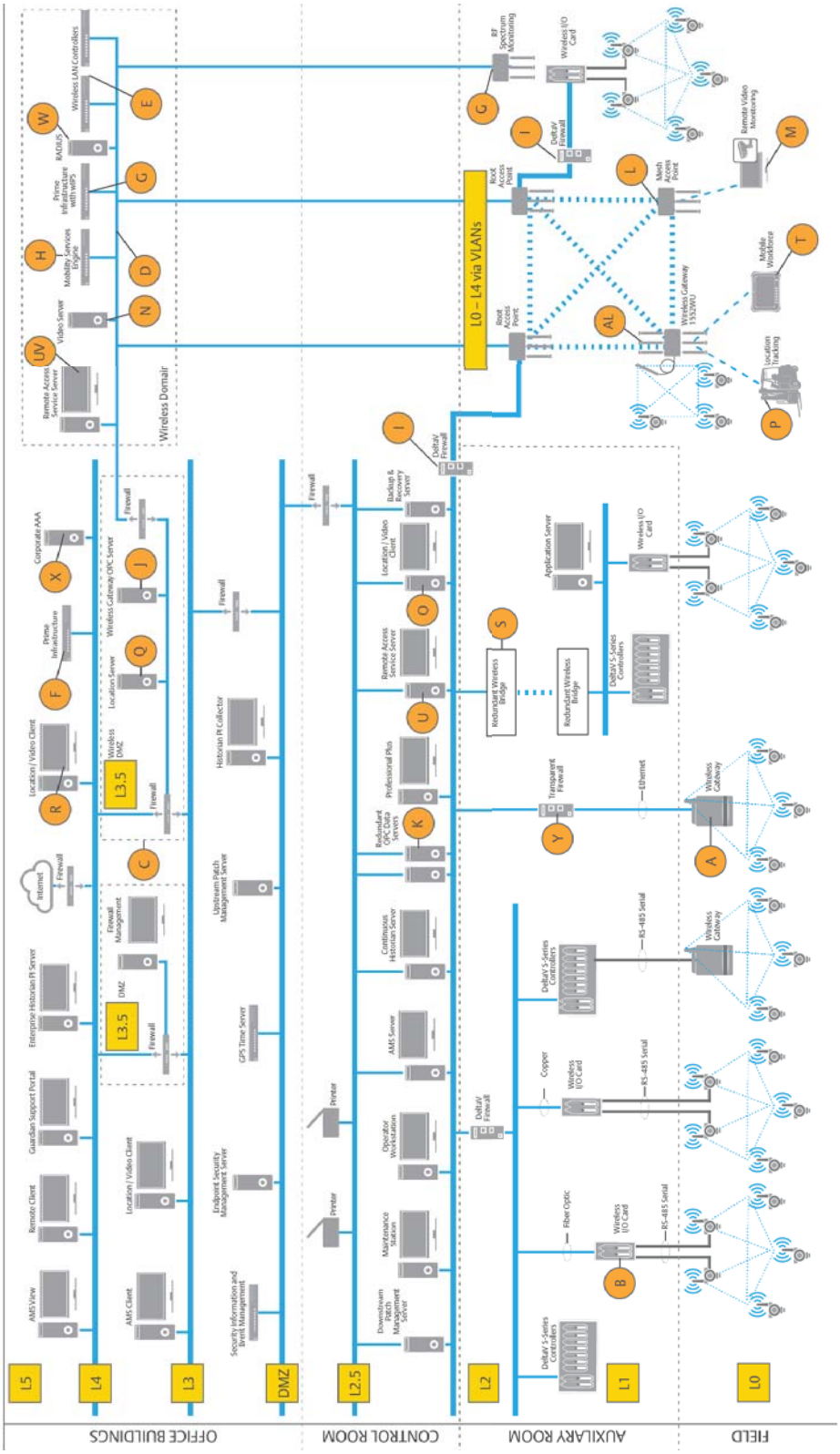
X. Enterprise domain controller (AAA)

The RADIUS server is configured to authenticate users with your site's existing enterprise authentication, authorization, and accounting server. User credentials are maintained here rather than local to the wireless DMZ.

Y. Transparent firewall

A transparent firewall can be configured to have the same subnet on both sides of the firewall, yet constrain the communications to be between only certain device IP addresses and restrict access to only those ports required by DeltaV or AMS to communicate between the Gateway (or WIOC) and the area control network.

Figure 1-6. Network Architecture



12.0 Conclusion

Wireless security is critical to the successful deployment of both field instrument networks and plant application solutions. This document demonstrates Emerson capabilities to deploy secure, reliable and robust wireless solutions for both field instrumentation and plant applications.

Emerson is knowledgeable in all of these security technologies and can work with you to apply them to improve process monitoring, increase workforce productivity, and to lower operating costs.

Emerson has proven wireless expertise to provide you turnkey solutions for both Emerson Wireless field instrumentation and wireless plant application solutions.

Technical Note
00840-0200-6129, Rev AA
September 2017

Systems and Solutions Headquarters
Emerson Automation Solutions
1100 W Louis Henna Blvd., Building One
Round Rock, TX 78681, USA

Emerson Wireless Headquarters
Emerson Automation Solutions
6021 Innovation Blvd.
Shakopee, MN 55379, USA
+1 800 999 9307 or +1 952 906 8888
+1 952 949 7001
RFQ.RMD-RCC@Emerson.com
Emerson.com/Wireless

Linkedin.com/company/Emerson-Automation-Solutions

Twitter.com/EMR_Automation

Facebook.com/Emerson-Automation-Solutions

Google.com/+Emerson-Automation-Solutions

EMERSON