Using Emerson™ Process Management Wireless in a NERC CIP Compliant Environment

1.0 Overview

The purpose of this technical note is to provide clear guidance on how Emerson's *Wireless*HART® self-organizing mesh sensor network product line can be integrated into a NERC CIP compliant environment. This document focuses on version 5 of the NERC CIP standards. Although the CIP standards include a group of 11 protection categories (labeled CIP-002 through CIP-011 and CIP-014), this document focuses on CIP-005 and CIP-007 since they are applicable to Emerson's *Wireless*HART products.

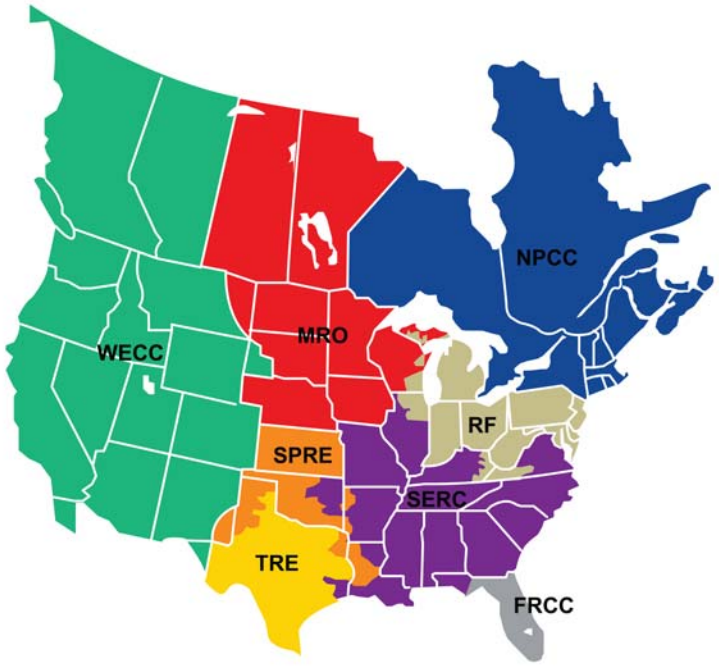
2.0 Scope

This document supplements an existing white paper published by Emerson Process Management entitled “Emerson Wireless Security - *Wireless*HART and Wi-Fi Security” (see references) which discusses general wireless security. This document focuses on how Emerson's *Wireless*HART products can be incorporated into a NERC CIP compliant environment. It is recommended the reader become familiar with this additional information.

3.0 Background

The North American Electric Reliability Corporation (NERC) is a nonprofit, international regulatory corporation in charge of regulating the reliability of the North American bulk power system. This bulk power system provides electricity to 334 million people, covers 211,000 miles of high-voltage transmission lines, and represents more than $1 trillion worth of assets. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico.

Figure 1-1. NERC Regions



The Federal Energy Regulatory Commission (FERC) has certified this corporation as an electric reliability organization and allows users, owners, and operators of the bulk power system in the U.S.A. to be subject to FERC-approved NERC reliability standards.

NERC was originally created to solve an overarching bulk power system problem. In the early 20th century many of the electric power systems were isolated to their own regions and only served customers locally. Connecting all independent systems made power more easily accessible to customers across the country. This in turn created a new risk as these systems began to join together to form larger and larger power systems that could easily be collapsed by a small disturbance.

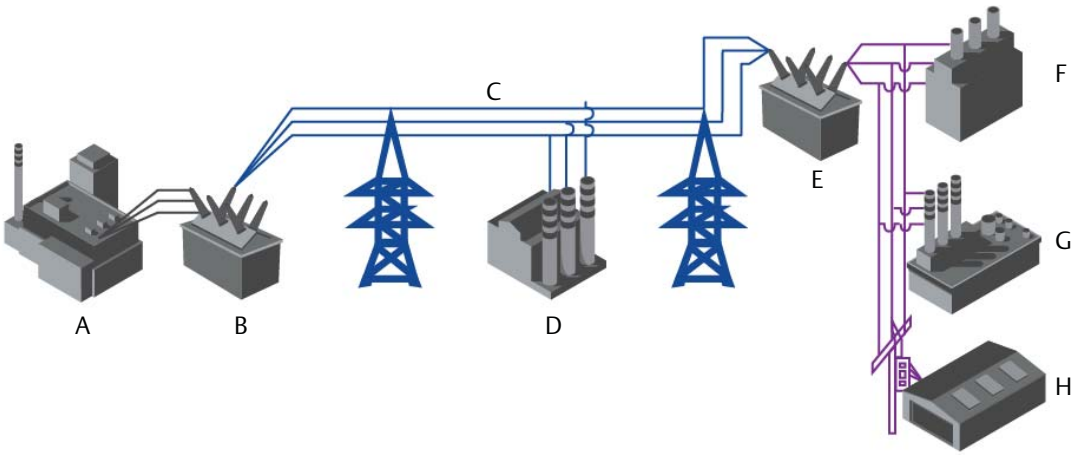
This risk was realized on November 9, 1965 when a power system protection component was not properly configured. A small outage in Queenston, Ontario quickly turned into the largest blackout at that time called the Northeast Blackout of 1965. 30 million customers lost power in the northeastern United States and southeastern Ontario. New York City went dark at about 5:30 p.m. and the entire city's power wasn't returned to normal until nearly 7:00 a.m. the next day. In response to this blackout, both the Federal Power Commission and the proposed Electric Reliability Act of 1967 prompted the formation of a council on power coordination. The National Electric Reliability Council was then established on June 1, 1968, and the name was later changed to the North American Electric Reliability Council since Canada is included in the council's membership.

NERC now oversees many aspects of the North American bulk power system. NERC's four pillars of continued success are reliability, assurance, learning, and risk-based approach. They have created reliability standards that are monitored and enforced with monetary and non-monetary penalties for noncompliance (backed up by the FERC). Reliability excellence is taught through training and education to keep the system operators up to speed with best practices. NERC also analyzes any bulk power systems events or outages for lessons learned to further improve reliability.

4.0 NERC CIP standards

The NERC Critical Infrastructure Protection (CIP) standards apply to the North American electric power industry (see Figure 1-2). They are grouped into protection categories labeled CIP-002 through CIP-0011 and CIP-014 to recognize the differing roles of each entity in the operation of the bulk electric system, the criticality and vulnerability of the assets needed to manage bulk electric system reliability, and the risks to which they are exposed. Each standard should be taken as part of the group of standards.

Figure 1-2. Electric Power Industry



Color Key	A. Generating station	E. Substation step down transformer
Grey: Generation	B. Generating step up transformer	F. Sub-transmission customer 26 kV and 69 kV
Blue: Transmission	C. Transmission lines 756, 500, 345, 230 and 138 kV	G. Primary customer 13 kV and 4 kV
Purple: Distribution	D. Transmission customer 138 kV or 230 kV	H. Secondary customer 120 V and 240 V

The generation and transmission components currently make up the “bulk electric system” however, implementation of SmartGrid technology has raised the issue of whether customer-located technology needs to be regulated as well to protect the overall system.

4.1 NERC CIP summary

Standards CIP-002 through CIP-011 and CIP-014 provide a cybersecurity framework for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system.

- CIP-002 – requires identification and documentation of BES Cyber Systems and their associated BES Cyber Assets
- CIP-003 – requires responsible entities have minimum security management controls in place to establish responsibility and accountability to protect BES Cyber Systems
- CIP-004 – requires personnel having access to the BES Cyber Systems have an appropriate level of personnel risk assessment, training, and security awareness
- CIP-005 – requires identification and protection of the electronic security perimeter(s)
- CIP-006 – intended to ensure the implementation of a physical security program.
- CIP-007 – requires responsible entities to define methods, processes, and procedures for securing the BES Cyber System
- CIP-008 – ensures incident response requirements are in place to mitigate the risk to the reliable operation of the BES resulting from a Cyber Security Incident
- CIP-009 – ensures recovery plan(s) are in place
- CIP-010 – ensures configuration management and vulnerability assessment requirements are in place.
- CIP-011 – ensures information protection requirements are in place
- CIP-014 – ensures physical protection is in place

4.2 *Wireless*HART security overview

Emerson's Wireless Field Network architecture and security is defined in detail in the white paper entitled "Emerson Wireless Security - WirelessHART and Wi-Fi Security". That paper is an excellent resource and it is recommended the reader be familiar with it. This section summarizes the major security architectural features described in that white paper.

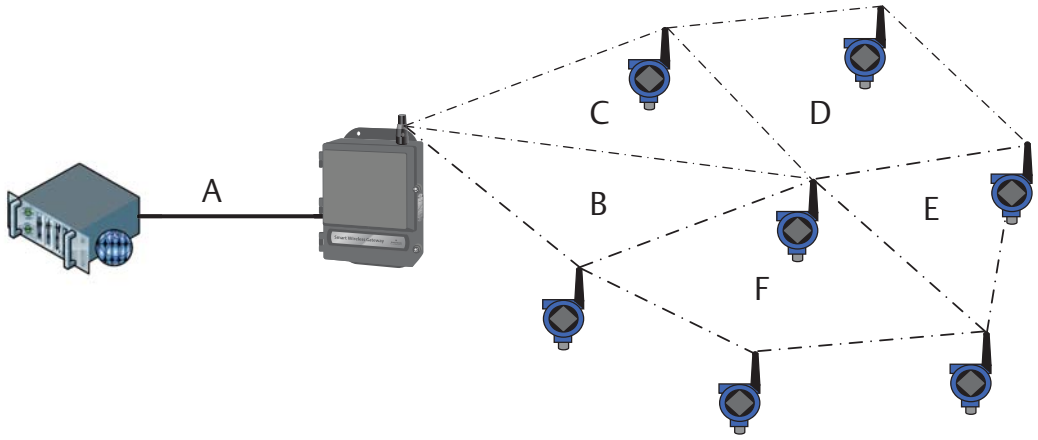
Emerson Process Management's wireless devices use IEC 62591-compliant (*Wireless*HART) protocols to connect wireless field devices to the control system. The IEC 62591 standard provides complete detail on the specifics of *Wireless*HART.

Access is controlled by the *Wireless*HART Network Manager and Security Manager embedded in either the Smart Wireless Gateway or the DeltaV™ Wireless IO Card (WIOC). Both the Gateway and the WIOC ensure that only authorized devices are allowed to participate in the *Wireless*HART network.

Important
All devices on a *Wireless*HART network are authenticated and all *Wireless*HART communications are encrypted.

*Wireless*HART security prevents outsiders from eavesdropping or joining the network, and keeps insiders from monitoring information they do not have the authorization to access. In addition, multiple techniques ensure the availability and integrity of the information transmitted.

Figure 1-3. *Wireless*HART Architecture



A. Multiple secure Ethernet protocols supported
B. *Wireless*HART is non-routable
C. Self healing
D. Robust communication
E. Self forming
F. All wireless communication is encrypted

The first stage of *Wireless*HART security is based upon a secure provisioning process using a wired HART connection to the maintenance port. A wireless field device requires two pieces of information to join a *Wireless*HART network: the desired Network ID and a 128-bit join key. Join keys can be common for all devices that connect to a given network or they can be unique for each device creating a whitelist or Access Control List (ACL).

Once the field device is provisioned, it will issue a join request to the *Wireless*HART network. This request is encrypted with the join key. If the join request is authenticated by the *Wireless*HART Security Manager (embedded in either the Gateway or the WIOC), network resources and 128-bit network and session keys are allocated to the new device. This response is also encrypted.

After joining a network, the field device is given the network key which is randomly generated when the security manager is initialized. The device uses this key to calculate a Message Integrity Code (MIC) on a hop-by-hop basis. The key is shared across the *Wireless*HART network. In addition, various session keys are randomly generated by the security manager when a device joins and transmitted to the device. These session keys are used to encrypt messages on a (potentially) multi-hop basis to provide end-to-end (source to destination) confidentiality and integrity. Only the individual field device and the Gateway and/or WIOC are aware of the relevant session keys. Again, all keys are 128-bit symmetric Advanced Encryption Standard (AES) keys.

The Emerson *Wireless*HART Gateway has an internal firewall that blocks unauthorized in- and out-bound traffic on a port and protocol basis. Documenting and maintaining the Gateway's firewall rules is performed using the *Protocols* page of the Gateway's secure browser application. If desired, an additional external firewall can be used with the system to provide an additional layer of security.

For a more complete discussion on network security, see the "Emerson Wireless Security - *Wireless*HART and Wi-Fi security" white paper.

4.3 Routable versus non-routable protocols

As defined by the NERC guideline "Identifying Critical Cyber Assets, Version 1.0," routable protocols use addresses having at least two parts: a network address and a device address. Routable protocols allow devices to communicate between two different networks by forwarding packets between the two networks. Non-routable protocols only use a device address and do not allow messages to be sent from one network to another, thus allowing communications to take place only on a single network. Since *Wireless*HART packets only have device addressing and do not contain any network addressing portion, *Wireless*HART is considered a non-routable protocol. Data on a *Wireless*HART network will only be routed within a single network and cannot be routed to other networks. The fact that *Wireless*HART uses a non-routable protocol gives end users significant flexibility in network configurations while still being compliant with the NERC CIPs.

4.4 CIP-005-5 – Electronics Security Perimeter(s)

The purpose of this CIP is to manage electronic access to BES Cyber Systems by specifying a controlled electronic security perimeter to protect against compromise. Emerson's *Wireless*HART systems can be fully compliant and provide significant flexibility.

CIP-005: Requirement 1

"Each responsible entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter*."

Compliance guidance

NERC CIP-005 Requirement 1.1: "All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP."

Since *Wireless*HART is not a routable protocol; the wireless field devices do not need to reside in a defined ESP.

The *Wireless*HART Gateway communicates with the rest of the control system via a wired Ethernet or Modbus® over a wired serial RS-485 interface. Serial Modbus is not a routable interface since each packet only contains a device address. If only serial Modbus is used, the Gateway would not be required to reside within a defined ESP. The other Ethernet protocols (e.g. EtherNet/IP, Modbus TCP, HART-IP™, OPC) would be considered a routable protocol, so if the Gateway is considered an applicable Cyber Asset, it would need to reside within a defined ESP.

The Gateway is configured using the web interface. This communication uses a web browser to connect to the Gateway using the Secure Hypertext Transfer Protocol (HTTPS). So even if the end user is using serial Modbus, the HTTPS protocol used to configure the Gateway is a routable protocol. If the Gateway does not reside within an ESP, configuration would need to be done from outside the ESP or pass through an access point. This should be considered when deciding whether or not the Gateway will reside within an ESP.

NERC CIP-005 Requirement 1.2: "All External Routable Connectivity must be through an identified Electronic Access Point (EAP)."

Since *Wireless*HART is not a routable protocol, *Wireless*HART traffic does not need to be routed through an EAP even if the wireless Gateway is inside an ESP and the wireless field devices are outside the ESP.

Depending on how the Gateway is being used, communication may or may not need to be routed through an EAP. As mentioned earlier, serial Modbus is not a routable protocol and does not need to be routed through an EAP. Ethernet traffic (e.g. HTTPS, Modbus TCP, HART-IP, OPC, Ethernet/IP) is routable traffic so if it is crossing an ESP boundary, it must be routed through an EAP.

NERC CIP-005 Requirements 1.3: "Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default."

All *Wireless*HART field devices are authenticated before being granted access to join the network. In other words, access to the *Wireless*HART network is restricted and denied by default. A device is only allowed to join if it has the correct network ID and join key.

The wireless Gateway incorporates a port and protocol firewall and the user has complete control over which ports and protocols are enabled. All unused protocols and ports can be disabled.

NERC CIP-005 Requirements 1.4: "Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets."

This requirement is not applicable to Emerson's *Wireless*HART systems since they do not support dial-up access.

NERC CIP-005 Requirements 1.5: "Have one or more methods for detecting known or suspected malicious communication for both inbound and outbound communications."

As mentioned earlier, the Gateway incorporates a port and protocol firewall and the user has complete control over which ports and protocols are enabled. The Gateway also supports internal logging as well as support for a syslog server. Many events, including join failures and MIC failures, will be logged; those logs can be reviewed for suspicious activity.

CIP-005: Requirement 2

"Each responsible entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*."

Compliance guidance

NERC CIP-005 Requirements 2.1: "Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset."

NERC CIP-005 Requirements 2.2: "For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System."

NERC CIP-005 Requirements 2.3: "Require multi-factor authentication for all Interactive Remote Access sessions."

Requirement 2.1, 2.2, and 2.3 relate to remote access and the use of intermediate systems. The Gateway supports multiple secure, encrypted wired Ethernet protocols to interface with the host system. At the time this document was published, the Gateway does not support multi-factor authentication but this feature may be added in the future.

4.5 CIP-007-5 – Cyber Security – Systems Security Management

The purpose of this CIP is to manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

CIP-007: Requirement 1

"Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services*."

Compliance guidance

NERC CIP-007 Requirement 1.1: "Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed."

NERC CIP-007 Requirement 1.2: "Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media."

Requirement 1.1 and 1.2 involve network accessibility. Using the secure web interface, the user can disable all unused ports and leave only required ports and protocols open and enabled. The user has complete control. The Gateway has two wired Ethernet ports and a serial Modbus port accessible to the user. There are no user accessible console commands or removable media.

CIP-007: Requirement 2

"Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management*."

Compliance guidance

NERC CIP-007 Requirement 2.1: "A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists."

NERC CIP-007 Requirement 2.2: "At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1."

NERC CIP-007 Requirement 2.3: "For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:

- **Apply the applicable patches; or**
- **Create a dated mitigation plan;**

or

- **Revise an existing mitigation plan.**

Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations."

NERC CIP-007 Requirement 2.4: "For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate."

CIP-007 requirements 2.1 through 2.4 discuss patch management. Emerson periodically releases firmware upgrades for the Gateway. A user can be notified when new Gateway firmware is available by visiting EmersonProcess.com/Wireless and registering their wireless Gateway. The firmware upgrade can also be downloaded by navigating to the same address. Once the user has downloaded the new firmware, it is uploaded using the secure web interface following the instructions in the wireless Gateway manual.

CIP-007: Requirement 3

"Each responsible entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention*."

Compliance guidance

NERC CIP-007 Requirement 3.1: "Deploy method(s) to deter, detect, or prevent malicious code."

NERC CIP-007 Requirement 3.2: "Mitigate the threat of detected malicious code."

NERC CIP-007 Requirement 3.3: "For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns."

Requirements 3.1 to 3.3 relate to malicious code. The Gateway incorporates a bi-directional port and protocol firewall and the user has complete control over which ports are open and which protocols are enabled. The Gateway also uses a hardened Linux® OS to prevent malicious software execution. All Gateway firmware updates are cryptographically signed to prevent inadvertent or intentional tampering and contain the latest security updates which will prevent malicious code from executing. The Gateway also supports logging. Events are logged and viewable via the Gateway's secure web interface. The Gateway also supports the use of a syslog server for longer log retention. These log files may be useful if anomalous behavior is detected.

CIP-007: Requirement 4

"Each responsible entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring*."

Compliance guidance

NERC CIP-007 Requirement 4.1: "Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

- **4.1.1. Detected successful login attempts;**
- **4.1.2. Detected failed access attempts and failed login attempts;**
- **4.1.3. Detected malicious code.**

NERC CIP-007 Requirement 4.2: "Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):

- **4.2.1. Detected malicious code from Part 4.1; and**
- **4.2.2. Detected failure of Part 4.1 event logging.**

NERC CIP-007 Requirement 4.3: "Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances."

NERC CIP-007 Requirement 4.4: "Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents."

Requirements 4.1 through 4.4 involve logging. The Gateway supports logging. Events are logged and viewable via the Gateway's secure web interface. The Gateway also supports the use of a syslog server to allow users more flexibility with longer log retention. The Gateway logs many events, including successful and failed login attempts. Configuration of the logging functionality is performed via the secure web interface.

CIP-007: Requirement 5

"Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R5 – System Access Controls*."

Compliance guidance

NERC CIP-007 Requirement 5.1: "Have a method(s) to enforce authentication of interactive user access, where technically feasible."

The Gateway supports authentication of interactive users. When using the secure web interface, users will be prompted for their username and password. The Gateway also supports role based accounts. Different users with different access levels can be created and customized via the secure web interface.

NERC CIP-007 Requirement 5.2: "Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s)."

All users with access to the Gateway can be viewed using the Gateway's secure web interface. The account list shown in the secure web interface includes all accounts; there are no hidden or backdoor accounts present in the Gateway.

NERC CIP-007 Requirement 5.3: "Identify individuals who have authorized access to shared accounts."

All users with access to the Gateway can be viewed using the Gateway's secure web interface. The account list shown in the secure web interface includes all accounts; there are no hidden or backdoor accounts present in the Gateway.

NERC CIP-007 Requirement 5.4: "Change known default passwords, per Cyber Asset capability"

All user passwords can be changed via the secure web interface.

NERC CIP-007 Requirement 5.5: "For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:

- **Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and**
- **Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset."**

The Gateway supports fully customizable password rules that comply with these requirements. Users can customize the password length, number of required uppercase and lowercase characters as well as required number of digits and symbols. Users can also set account session timeout and password lifetime settings. Actions taken when a user enters a wrong password as well as the login message are also customizable via the secure web interface. These settings can only be changed by a user with *Admin* level access.

NERC CIP-007 Requirement 5.6: "Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months."

As discussed in the response for requirement 5.5, a user with *Admin* level access can customize the password expiration time via the secure web interface.

NERC CIP-007 Requirement 5.7: "Where technically feasible, either:

- **Limit the number of unsuccessful authentication attempts; or**
- **Generate alerts after a threshold of unsuccessful authentication attempts."**

As mentioned in the response to requirement 5.5, a user with *Admin* level access can limit the number of unsuccessful authentication attempts. The Gateway also logs unsuccessful login attempts. The Gateway can also be configured to communicate with a syslog server. If a syslog server is used, a message will be sent when an unsuccessful authentication attempt is made.

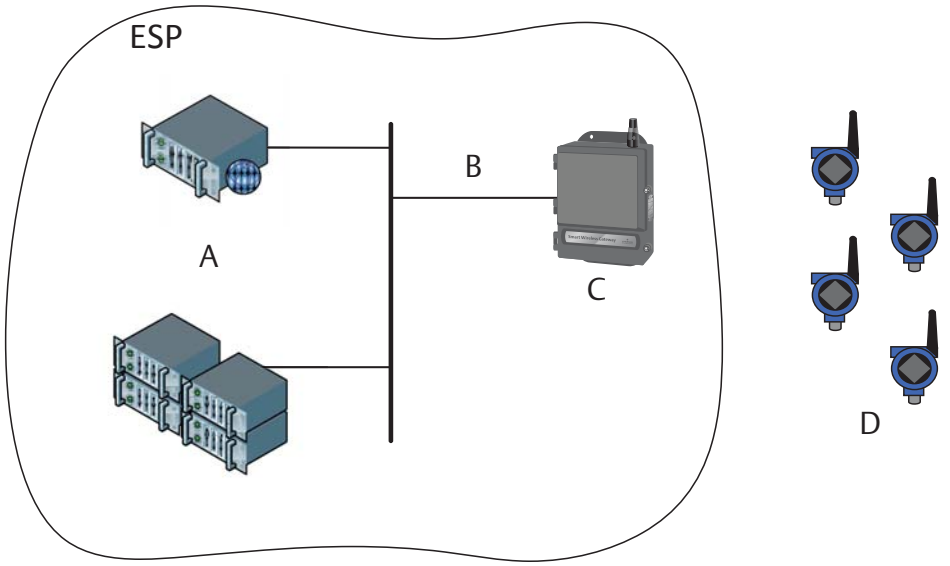
5.0 Network architecture examples

As already mentioned, the fact that *Wireless*HART is not a routable protocol provides significant flexibility for *Wireless*HART users. This section discusses several network architectures that end users can consider when implementing *Wireless*HART systems.

5.1 Example 1

Figure 1-4 shows the Gateway is inside of an ESP while the *Wireless*HART field devices are outside the ESP. In this example, the Gateway can communicate with the rest of the control system using a routable Ethernet protocol or a non-routable protocol, such as serial Modbus. Since the Gateway is inside the ESP, no access point is needed for communication back to the rest of the control system. Additionally, an access point is not required for wireless communication between the field devices and the Gateway since *Wireless*HART is not a routable protocol.

Figure 1-4. Architecture Example 1

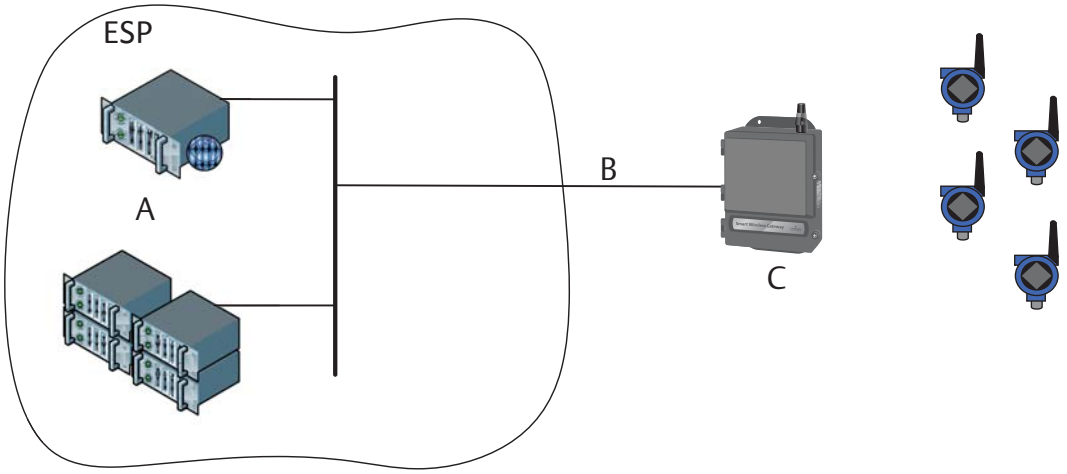


A. Control network
B. Routable or non-routable
C. Gateway inside the ESP - No access point since *Wireless*HART is not a routable protocol
D. Sensor outside the ESP - *Wireless*HART is not a routable protocol

5.2 Example 2

Figure 1-5 shows the Gateway and field devices outside the ESP. In this case, serial Modbus, a non-routable protocol, is used to communicate with the rest of the control system. Since a non-routable protocol is used to communicate back to the rest of the control system, data does not need to pass through an access point. One note is that the Gateway uses a secure web interface (HTTPS) for configuration. HTTPS is a routable protocol so configuration would need to be done from outside the ESP or pass through an access point.

Figure 1-5. Architecture Example 2

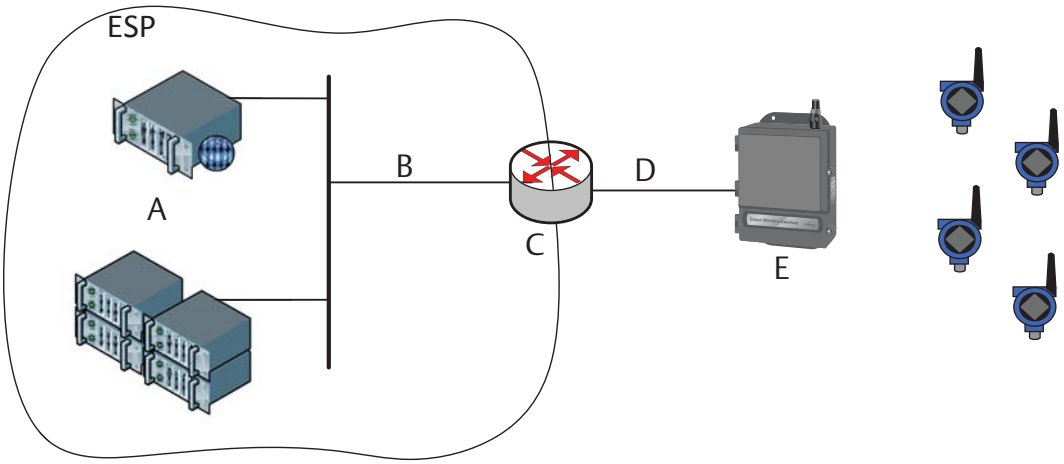


A. Control network
B. Non-routable (i.e. Modbus)
C. Sensors and Gateway are outside the ESP; both Gateway and devices communicate using a non-routable protocol.
Note: Gateway management via web interface would need to be done outside the ESP.

5.3 Example 3

Figure 1-6 shows the Gateway and field device outside the ESP and is similar to the second example. The difference between network architecture example 2 and this example is the protocol used by the Gateway to communicate back to the rest of the control system. In this example, an Ethernet protocol, (e.g. Modbus TCP, OPC, HART-IP) is used. Since these Ethernet protocols are routable, the data from the Gateway that passes through the ESP must pass through an Access Point. Since an Access Point is used, configuration of the Gateway using the secure web interface (HTTPS) can be done from inside the ESP.

Figure 1-6. Architecture Example 3

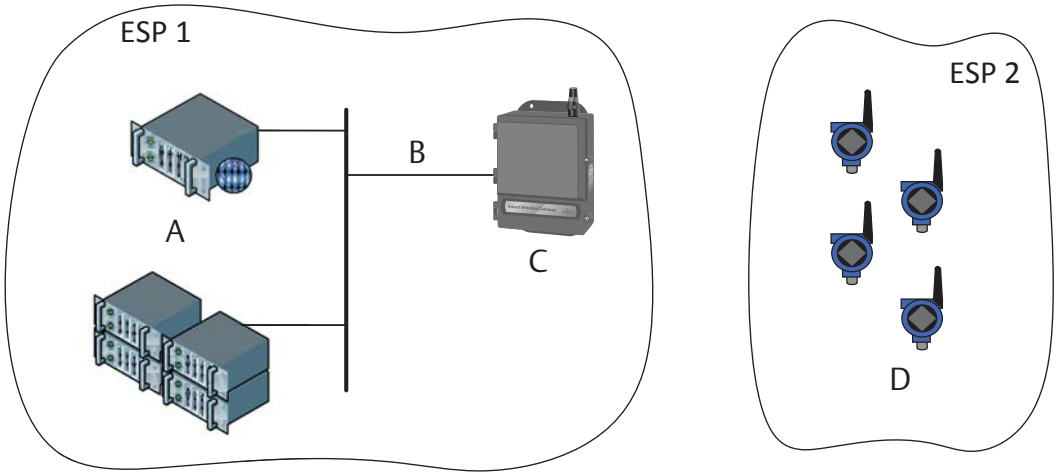


A. Control network
B. Routable or non-routable
C. Access point
D. Routable (i.e. Modbus TCP)
E. Sensors and Gateway are outside the ESP; Gateway uses a routable protocol through an access point to communicate with the rest of the control system.

5.4 Example 4

Figure 1-7 shows the Gateway in one ESP and the *Wireless*HART field devices in a second ESP. Since the *Wireless*HART protocol is non-routable, it can pass through both ESPs without the need of an access point.

Figure 1-7. Architecture Example 4



A. Control network
B. Routable or non-routable
C. Gateway inside the ESP – no access point required to communicate with sensors in a different ESP - *Wireless*HART is not a routable protocol.
D. Sensors inside a different ESP – no access point required to communicate with Gateway - *Wireless*HART is not a routable protocol.

6.0 Conclusion

Emerson's self-organizing wireless mesh networks were designed with security in mind, not as an afterthought. Emerson's wireless technology has proven reliability and can be used in a NERC CIP-compliant environment. Emerson's wireless field network provides a secure, flexible solution and there are many examples of end users using Emerson's wireless solutions in a NERC CIP-compliant environment.

7.0 References

- Emerson Wireless Security *Wireless*HART and Wi-Fi Security, Emerson Process Management White paper
  EmersonProcess.com/siteadmincenter/PM%20Central%20Web%20Documents/Emerson%20Wireless%20Security.pdf
- System Engineering Guidelines, IEC 62591 *Wireless*HART, Emerson Process Management, September 2015
  EmersonProcess.com/siteadmincenter/PM%20Central%20Web%20Documents/EMR_WirelessHART_SysEngGuide.pdf
- Smart Wireless Field Network: Recommendations for Planning, Installation and Commissioning: Technical Note 00840-0400-4180
  EmersonProcess.com/siteadmincenter/PM%20Rosemount%20Documents/00840-0400-4180.pdf
- Gateway Manuals: 00809-0200-4420 (for the 1420)
  EmersonProcess.com/siteadmincenter/PM%20Rosemount%20Documents/00809-0200-4420.pdf

  and 00809-0200-4410 (for the 1410)
  EmersonProcess.com/siteadmincenter/PM%20Rosemount%20Documents/00809-0200-4410.pdf
- NERC guideline "Identifying Critical Cyber Assets," Version 1.0
  http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf

7.1 Industry literature

- Industrial Communication Networks - Wireless Communication Network and Communication Profiles - *Wireless*HART: IEC 62591
- NERC CIP Standards Version 5 (CIP-002 through CIP-0011 and CIP-014)

7.2 Resource

Smart Wireless Gateway
EmersonProcess.com/en-US/brands/Rosemount/Wireless/Wireless-Gateways

For inquiries, contact Emerson Process Management Wireless at:
SmartWireless@Emerson.com

Global 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, FL 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

Linkedin.com/company/Emerson-Process-Management

Twitter.com/Rosemount_News

Facebook.com/Rosemount

Youtube.com/user/RosemountMeasurement

Google.com/+RosemountMeasurement

ROSEMOUNT

EMERSON
Process Management