Technical Note
00840-0300-4420, Rev AA
August 2013

Emerson's Smart Wireless and WIB Requirements

EMERSON™
Process Management

1.1 Acronyms

ACL	Access Control List
ACN	Area Control Network
AES	Advanced Encryption Standard
AMS Device Manager	Asset Management System
ANSI	American National Standards Institute
ASD	Automation System Domain
BP	Base Practice
BR	Base Requirement
DCS	Distributed Control System
e.g.	Exempli Gratia (for example)
GHz	Gigahertz
HART	Highway Addressable Remote Transmitter
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IO	Input Output
IPSec	Internet Protocol Security
ISA	International Society of Automation
ISM	Industrial, Scientific and Medical
ISO	International Standards Organization
MIC	Message Integrity Code
NIST	National Institute of Standards and Technology
PA	Process Area
RE	Requirement Enhancement
RF	Radio Frequency
RS	Recommended Standard
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
VPN	Virtual Private Network
WIB	Werkgroep Instrument Beoorderling (International Instrument Users' Association)
Wi-Fi	Wireless Fidelity
WIOC	Wireless Input Output Card
WPA	Wireless Protected Access

1.2 Overview

The purpose of this technical note is to provide clear guidance on how Emerson's Smart Wireless self-organizing mesh sensor network (*Wireless*HART) product line can be integrated into a system which meets the cyber security requirements set forth by the International Instrument Users' Association (WIB) Plant Security Working group. These requirements, defined by the WIB, contain a subset or minimum set of requirements for security policies, standards and specifications. It is possible that end user or national/local regulations exist in which some of the requirements may be more rigorous than the requirements set forth by the WIB. If this is the case, a careful analysis would need to be performed to determine which combination of requirements would be suitable for the given situation.

Note that these WIB requirements are being reconstituted to be part of the more comprehensive IEC 62443 standard (largely being written under the auspices of ISA SP99 in partnership with IEC TC65), and will eventually be the IEC 62443-2-4 standard.

1.3 Scope

This technical note supplements an existing technical note published by Emerson titled Emerson Wireless Security – *Wireless*HART® and Wi-Fi™ Security. Emerson Wireless Security – *Wireless*HART® and Wi-Fi™ Security (see references) discusses wireless security in general while this technical note focuses on how Emerson's WirelessHART field devices can be incorporated into a system that meets the requirements set by the WIB.

1.4 References

1.4.1 Emerson literature

- Emerson Wireless Security *Wireless*HART® and Wi-Fi™ Security, Emerson process Management technical note, November 2011
- Smart Wireless Field Network: Recommendations for Planning, Installation and Commissioning: Technical Note 00840-0400-4180

1.4.2 Industry literature

- Industrial Communication Networks – Wireless Communication Network and Communication Profiles – *Wireless*HART®: IEC 62591
- WIB Requirements: Process Control Domain-security Requirements for Vendors: Report M2784-X-10

1.5 Background

The International Instrument Users' Association (WIB) is an international consortium composed of approximately 80 asset owners which provides process instrumentation evaluation/assessment services for members. Companies that are involved with the manufacturing, marketing or sale of the process instrumentation are excluded from membership. The WIB created a certification program, currently administered by Wurldtech, for its vendors to get them started on a formal standardized security program. This program covers the product, its deployment and maintenance. The program also contains a maturity model to allow improvement to the security offerings over time.

1.5.1 Emerson *Wireless*HART security overview

Emerson Process Management's Wireless Field Network architecture and security is defined in detail in the technical note entitled Emerson Wireless Security - *Wireless*HART® and Wi-Fi™ Security. That technical note is an excellent resource and it is recommended that the reader be familiar with it. This section summarizes the major security architectural features described in that technical note.

Emerson's wireless devices use IEC 62591-compliant (*Wireless*HART) protocols to connect wireless field devices into 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 similar appliance. Both the Gateway and the WIOC ensure that only authorized devices are allowed to participate in the *Wireless*HART network. All communications between devices is 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.

The first stage of *Wireless*HART security is based upon a secure provisioning process using a wired HART connection to field device's the maintenance port. A wireless field device requires two pieces of information to join a WirelessHART 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. Use of a whitelist/ACL of permitted devices is also an option.

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, and includes a set of information about the device to prevent a rogue device from spoofing a legitimate one. If the join request is authenticated by the *Wireless*HART Security Manager, 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 Message Integrity Code (MIC) on a hop-by-hop basis, as well as to encrypt broadcast messages.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 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 *Emerson Wireless Security - WirelessHART® and Wi-Fi™ Security*.

1.5.2 WIB defined security requirements

The WIB requirements are organized into four Process Areas (PA's) domains. These PA's consist of Base Practices and Requirement Enhancements (RE's). This table contains a column defining the PA and BP from which the requirement is derived. The actual requirement text is listed along with a response on how Emerson's Smart Wireless solution is compliant with the requirement.

The WIB requirements listed in this document are not a complete list of requirements, rather a subset of WIB requirements that are applicable to Emerson's Smart Wireless solutions. See WIB documentation for a complete list of requirements.

*Wireless*HART segments

Description

Process area category	Base practice	Requirements	Compliance
PA12: Connect wirelessly	BP.12.01: Approved standards	BR: Where wireless devices are appropriate, the Vendor's system shall provide the capability to use wireless devices that comply with approved international wireless standards (e.g., IEEE, ISA, and IEC).	Emerson's wireless devices comply with the approved IEC62591 standard -*Wireless*HART
PA12: Connect wirelessly	BP.12.01: Approved standards	RE(1): The use of proprietary and non-standard protocols shall not be used unless approved by the Principal.	Emerson's wireless devices comply with the approved IEC62591 standard -*Wireless*HART
PA12: Connect wirelessly	BP.12.01: Approved standards	RE(2): Industrial wireless field devices should be based on ISA 100 or WirelessHART. The use of other techniques shall not be used unless approved by the Principal.	Emerson's wireless devices employ the use of *Wireless*HART
PA12: Connect wirelessly	BP.12.01: Approved standards	RE(3): Wireless devices and systems (including infrared and non-RF) shall comply with approved international standards (e.g., NIST, ANSI, IEEE, IEC, ISO) or with regulatory requirements governing licensing of frequency bands.	Emerson's *Wireless*HART devices operate in the 2.4 GHz ISM band using IEEE 802.15.4 standard radios. The devices meet all applicable regulatory requirements.

PA15: Protect data	BP.15.03: Encryption	RE(1): The Vendor's system shall provide the capability to use strong encryption (WPA2 or AES-256) or use VPN tunnels secured with IPSec or SSL for wireless bridges used for point-to-point backbone connectivity.	Emerson's *Wireless*HART devices use strong encryption. All *Wireless*HART keys are 128-bit symmetric Advanced Encryption Standard (AES) keys. In addition to all *Wireless*HART communication being encrypted, the gateway provides several secure host protocols which are encrypted. All unencrypted protocols can be disabled by the user.
PA17: Harden the system	BP.17.02: Firewall use	RE(1): During system testing and commissioning the Vendor's system should verify that the point of connection within the control system network between wired and wireless networks is firewalled with documented and maintained firewall rules. *Note*: Responsibility for maintaining up-to- date firewall rules and documentation may have been transferred to the Principal prior to system turnover. If this is the case, the Vendor role is, if required, to support verification that the firewall rules are up-to-date.	Emerson's Smart Wireless Gateway supports an internal firewall that inspects both incoming and outgoing data packets. TCP ports for communication protocols are user configurable, including user specified port numbers and the ability to disable ports. Further, an optional external firewall can be used if desired.
PA23: Connect wirelessly	BP.23.04: Secure accounts	RE(1): During system testing and commissioning, the Vendor's system shall verify that unused ports provided on wireless devices, such as a RS232 interface for configuration, should be made physically secure or disabled where possible.	The internal firewall allows user to enable/disable specified port numbers. Changing the *Wireless*HART join key via the wired HART port is disabled on the wireless field devices when the device is connected to a network.

PA23: Connect wirelessly	BP.23.06: Architecture documentation	BR: Prior to system testing and commissioning the system Vendor shall verify that its system architecture documentation describing wireless systems is up-to-date in its description of the following. a. Data exchange between Layer 1 and wireless instrumentation. b. Data exchange between Layer 2 and Layer 3 through a secure wireless link c. Bridge connecting the Layer 3 network using a secure wireless link d. Security mechanisms that prevents an intruder from gaining access to the ASD systems using the wireless system. e. Security mechanisms that restrict access within the ASD by workers with handheld wireless devices f. Where required, security mechanisms that provides remote management of wireless systems.	See Emerson Wireless Security *Wireless*HART® and Wi-Fi™ Security. This paper contains discussion regarding the recommended architecture of Emerson wireless solutions. This paper also describes the security mechanisms which restrict or prevent access to various parts of the system.
PA23: Connect wirelessly	BP.23.06: Architecture documentation	RE(1): During system testing and commissioning the system Vendor shall verify that its system plan for the use of frequencies in wireless infrastructures, addressing non-interference and co-existence is up-to-date and approved by the Principal.	Emerson's *Wireless*HART devices operate in the 2.4 GHz ISM band using IEEE 802.15.4 standard radios and have been proven to coexist with other systems which operate in the same frequency range.
PA25: Protect data	BP.25.03: Encryption	RE(1): During system testing and commissioning the Vendor's system shall verify that for wireless connections, the highest feasible level of WPA, WPA2 or AES security and encryption is used.	All keys are 128-bit symmetric Advanced Encryption Standard (AES) keys.
PA25: Protect data	BP.25.03: Encryption	RE(2): During system testing and commissioning the Vendor's system shall verify that encryption or a secure tunnel between wireless devices are used where possible.	All keys are 128-bit symmetric Advanced Encryption Standard (AES) keys.

PA27: Harden the system	BP.27.02: Firewall use	RE(1): During scheduled maintenance testing the Vendor's system should verify that the point of connection within the control system network between wired and wireless networks is firewalled with documented and maintained firewall rules. Note: Responsibility for maintaining up-to-date firewall rules and documentation may have been transferred to the Principal at system turnover. If this is the case, the Vendor role is, if required, to support verification that the firewall rules are up-to-date.	Emerson's Smart Wireless Gateway supports an internal firewall that inspects both incoming and outgoing data packets. TCP ports for communication protocols are user configurable, including user specified port numbers and the ability to disable ports. Further, an optional external firewall can be used if desired.
PA33: Connect wirelessly	BP.33.06: Architecture demonstration	RE(1): Prior to scheduled maintenance, the system Vendor shall re-verify that its system plan for the use of frequencies in wireless infrastructures, addressing non-interference and co-existence is up-to-date and approved by the Principal.	Emerson's *Wireless*HART devices operate in the 2.4 GHz ISM band using IEEE 802.15.4 standard radios.
PA35 Protect data	BP.35.03: Encryption	BR: During scheduled maintenance testing the Vendor's system shall re-verify that encryption or a secure tunnel between wireless devices are used where possible.	All keys are 128-bit symmetric Advanced Encryption Standard (AES) keys.
PA35 Protect data	BP.35.03: Encryption	RE(1): During scheduled maintenance testing the Vendor's system shall re-verify that for wireless connections, the highest feasible level of WPA, WPA2 or AES security and encryption is used.	All keys are 128-bit symmetric Advanced Encryption Standard (AES) keys.

Separation of maintenance workstations and wireless devices

All maintenance and engineering of wireless devices connected through the Area Control Network (ACN) should be performed on or routed through an ACN workstation. Access to wireless devices that bypass the ACN workstations is not permitted.

Wireless devices can also be connected to ACN systems, but only for instrumentation purposes, not for control. Maintenance and engineering of these remotely connected wireless devices must be performed from an ACN workstation that is protected by the ACN firewall.

The recommended architecture outlined in Emerson's technical note titled "Wireless Security *Wireless*HART® and Wi-Fi™ Security" is fully compliant with the WIB requirements detailed in this section.

Process area category	Base practice	Requirements	Compliance
PA23: Connect wirelessly	BP.23.02: Wireless device maintenance	BR: During system testing and commissioning the Vendor's system shall, where applicable, verify that maintenance and engineering of wireless devices connected to Layer 1 or Layer 2 are routed through the control system management workstation. Note: Direct access to these devices using wireless connections which bypass the DCS is not allowed.	See Emerson Wireless Security *Wireless*HART® and Wi-Fi™ Security. This paper contains discussion regarding the recommended architecture of Emerson's wireless solutions. This paper also describes the security mechanisms which restrict or prevent access to various parts of the system.
PA23: Connect wirelessly	BP.23.02: Wireless device maintenance	RE(1): During system testing and commissioning the Vendor's system shall verify that remote maintenance and remote engineering of wireless devices connected to Layer 3 is only possible via wired connections through the ASD firewall. Note: Direct access to these devices using wireless connections is not allowed.	See Emerson Wireless Security *Wireless*HART® and Wi-Fi™ Security. This paper contains discussion regarding the recommended architecture of Emerson's wireless solutions. This paper also describes the security mechanisms which restrict or prevent access to various parts of the system.
PA33: Connect wirelessly	BP.33.01: Service set identifier (SSID)	RE(1): During scheduled maintenance testing the Vendor's system shall verify that remote maintenance and remote engineering of wireless devices connected to layer 3 is only possible via a wired connection through the ASD firewall. NOTE Direct access to these devices using wireless connections is not allowed.	See Emerson Wireless Security *Wireless*HART® and Wi-Fi™ Security. This paper contains discussion regarding the recommended architecture of Emerson's wireless solutions. This paper also describes the security mechanisms which restrict or prevent access to various parts of the system.
PA33: Connect wirelessly	BP.33.02: Wireless device maintenance	BR: scheduled maintenance testing the Vendor's system shall re-verify, where applicable, that maintenance and engineering of wireless devices connected to Layer 1 or Layer 2 are routed through the control system management workstation. Note: Direct access to these devices using wireless connections which bypass the DCS is not allowed.	See Emerson Wireless Security *Wireless*HART® and Wi-Fi™ Security. This paper contains discussion regarding the recommended architecture of Emerson's wireless solutions. This paper also describes the security mechanisms which restrict or prevent access to various parts of the system.

PA33: Connect wirelessly	BP.33.02: Wireless device maintenance	RE(1): During scheduled maintenance testing the Vendor's system shall verify that remote maintenance and remote engineering of wireless devices connected to Layer 3 is only be possible via wired connections through the ASD firewall. Note: Direct access to these devices using wireless connections is not allowed.	See Emerson Wireless Security *Wireless*HART® and Wi-Fi™ Security. This paper contains discussion regarding the recommended architecture of Emerson's wireless solutions. This paper also describes the security mechanisms which restrict or prevent access to various parts of the system.

*Wireless*HART device security

Configuration of *Wireless*HART devices is exactly the same as for wired HART devices and is performed from the same user interface. For guidelines on the configuration of *Wireless*HART devices, refer to Smart Wireless Field Network: Recommendations for Planning, Installation, and Commissioning.

The response time for *Wireless*HART devices can be greater than for wired devices. For this reason, the use of *Wireless*HART devices in control loops must be approved by site personnel responsible for the control system.

Process area category	Base practice	Requirements	Compliance
PA12: Connect wirelessly	BP.12.02: Configuration methods	BR: The Vendor's system should provide the capability for the control system to configure wireless field instruments in a similar manner used to configure to wired field instruments.	Emerson's Smart Wireless devices can be configured with a field communicator or using AMS Device Manager, just as with a wired device.
PA12: Connect wirelessly	BP.12.02: Configuration methods	RE(1): The Vendor's system should provide the capability to view the latest configuration of a wireless field device used for monitoring and control from the control system.	Current device configurations for Emerson's Smart Wireless devices can be viewed with a field communicator or using AMS Device Manager, just as with a wired device.
PA23: Connect wirelessly	BP.23.03: Safeguarding functions	RE(1): During system testing and commissioning the Vendor shall verify that due to the response time of wireless devices, their use as part of a control loop is approved by the Principal.	If a wireless device is used as part of a control loop, it must be approved by the end user at the time of system commissioning.
PA33: Connect wirelessly	BP.33.03: Safeguarding functions	RE(1): During scheduled maintenance testing the Vendor's system shall re-verify that due to the response time of wireless devices, their use as part of a control loop is approved by the Principal.	If a wireless device is used as part of a control loop, it must be approved by the end user at the time of system maintenance.

Site activity

Site activity will consist of project implementation and ongoing maintenance.

Project implementation

Staff training

Emerson Process Management can provide resources to ensure that the staff is adequately trained on the use of the *Wireless*HART system. The training can be in the form of freely available documentation or in the form of on-site support.

Security contact

A trained system cyber security lead or maintenance support contact may be assigned for a customer project as required by the scope of work. If an Emerson Process Management cyber security lead is assigned, it is expected that a primary customer cyber security contact will also be identified.

The recommended architecture defined in *Emerson Wireless Security – Wireless*HART® and *Wi-Fi™ Security* is fully compliant with the WIB requirements. Emerson Process Management cyber security leads understand the recommended architecture and practices and are able to provide guidance when needed.

PA02: Designate a security contact	BP.02.01: Nominate the role	BR: The Vendor shall nominate a Control System Security Focal Point in its organization who is responsible and accountable for the following activities. a. Acting as liaison with the Principal, as appropriate, about compliance of the Vendor system with this document. b. Communicating the Vendor point of view on the control system security to the Principal staff c. Ensuring that tenders to the Principal are aligned and in compliance with both this document and the Vendor internal requirements for control system security d. Communicating deviations from, or other issues not conforming with, this document to the Principal organization requesting the tender. Note: The evidence requirement in the Vendor Submittal only requires that a control system security focal point be designated
PA02: Designate a security contact	BP.02.01: Nominate the role	RE (1): Providing the Principal with timely information about cyber security vulnerabilities in the Vendor supplied systems and services.

The scope of responsibilities of cyber security contacts shall be established between Emerson Process Management and the customer organization. Recommended areas of coordination include:

- Liaisons between the two organizations, as appropriate, with respect to issues related to the customer's system compliance with relevant security standards and Emerson Process Management's recommended practices and architecture
- Ensure tenders are aligned and in compliance with cyber security policies and procedures per scope of product and services being offered. Any deviations from cyber security policies and procedures are communicated.
- Ensure that the customer has access to timely information about cyber-security vulnerabilities in the supplied systems and services.

Segmented design

Emerson's *Wireless*HART system is designed to be implemented as a part of a segmented network. The Emerson *Wireless*HART Gateway supports an internal firewall which will help enforce separation between the wireless field devices and the rest of the system. The Gateway firewall inspects both incoming and outgoing data packets and if desired, an additional, external firewall can be used with the *Wireless*HART system. *Emerson Wireless Security – WirelessHART®* and *Wi-Fi™ Security* contains additional architecture information.

Risk assessment and identification of sensitive data

Security risk assessments are conducted to ensure that proper safeguards are present in the system. Risk assessments are often performed prior to installation to provide guidance for hardening the system and after installation to respond to changes in the system, changes in threat profiles, and changes in the environment where the system is installed.

In general, risk assessments identify resources of the system/process that need to be protected and the external and internal access paths that can be used to access them. These access paths are further examined to identify potential points where unauthorized access can occur and the safeguards needed to harden these points.

More specifically, risk assessments generally consist of determining what needs to be protected, what types of losses (compromises) are of importance, what types of attacks are possible and probable, where the system is vulnerable to attack, and what safeguards (countermeasures) are appropriate. Since WirelessHART is very secure and data is always encrypted, this will simplify the risk assessment.

Access restrictions on external interfaces

During initial design, interfaces between external applications and the *Wireless*HART Gateway should be designated as trusted or untrusted based on the customer security policies. The Gateway firewall should be configured and unused ports disabled. User accounts should be setup to control access to the Gateway.

Looking at the *Wireless*HART network, only devices which are configured with the correct Join Key and Network ID will be able to join the network. The Join Key and Network ID are configured on the field devices using a wired HART port. Once the field device has joined a network, the Join Key and Network ID are not able to be changed without removing the field device from the *Wireless*HART network. As mentioned, the same Join Key can be used for each device or a whitelist/ACL can be created where each field device has its own Join Key. All communication between the Gateway and the *Wireless*HART field devices is encrypted.

Installation of anti-virus software and security patches

Anti-virus is not applicable to the wireless field devices or to the Gateway. The Gateway does support secure firmware upgrades in the field.

Setup of accounts and passwords

The Gateway allows for multiple password-protected, role-based accounts with different permissions. These accounts restrict who can access the system and what they can do. Passwords are encrypted when stored and used.

Solution maintenance

Maintenance is performed periodically to ensure that the requirements of the system are still being met. The sections below discuss various aspects of the maintenance.

Security updates and anti-virus updates

Anti-virus is not applicable to the wireless field devices or to the Gateway. The Gateway does support secure firmware upgrades in the field.

Backups and restore

The *Wireless*HART Gateway supports backup and restore functionality as documented in the Gateway user's manual. This allows the Emerson's *Wireless*HART system flexibility to fit into an end users overall system and procedures.

Routine maintenance

As a part of the end users routine maintenance, an effort should be made to ensure that the security of the system has not degraded. Verification should be performed to confirm that the *Wireless*HART system is still physically separated from the rest of the system in a secure fashion as designed. The end user should verify that the correct privileges exist for the users on the Gateway and that passwords are encrypted. For example, if an end user has left the company or changed jobs, their account should be deleted, and shared accounts should have their passwords changed. The end user should ensure that all unused ports on the Gateway continue to be disabled. Periodically, a verification activity should be performed to ensure that no unauthorized devices have joined or attempted to join the network. Any and all incidents should be managed per the customer's internal processes and procedures.

1.6 Conclusion

Emerson's self-organizing wireless mesh networks were designed with security in mind, not as an afterthought. Emerson's Smart Wireless technology has proven reliability which can meet the requirements defined by the WIB. Emerson's wireless field network provides a secure, flexible solution which has become a reliable part of a wide variety of industries and applications.

Technical Note
00840-0300-4420, Rev AA
August 2013

Emerson Process Management
Rosemount Division
8200 Market Boulevard
Chanhassen, MN 55317 USA
T (U.S.) 1 800 999 9307
T (International) 952 906 8888
F 952 906 8889
www.rosemount.com

Rosemount Temperature GmbH
Frankenstrasse 21
63791 Karlstein
Germany
T 49 6188 992 0
F 49 6188 992 112

Emerson Process Management Asia Pacific
Private Limited
1 Pandan Crescent
Singapore 128461
T 65 6777 8211
F 65 6777 0947
Enquiries@AP.EmersonProcess.com

Emerson Process Managment
No. 6 North Street
Hepingli, Dong Cheng District
Beijing 110013, China
T 86 10 6428 2233
F 86 10 6422 8586

Emerson Process Management
Latin America
1300 Concord Terrace, Suite 400
Sunrise Florida 33323 USA
Tel + 1 954 846 5030

EMERSON
Process Management