White Paper

Emerson's Secure Bluetooth® Wireless Technology Implementation

EMERSON™

Table of Contents

Introduction

Bluetooth® technology is a standard for short-range wireless communication between devices such as mobile phones, computers, transmitters, and other electronic devices. Emerson leverages Bluetooth wireless communication as a method to easily configure, maintain, and troubleshoot field devices via the AMS Device Configurator application. The AMS Device Configurator Bluetooth app uses FDI packages to communicate with field instruments and provides an app experience similar to AMS Device Manager and AMS Trex at communication speeds up to 10x faster than traditional HART® connections. The cybersecurity of Emerson's products is of utmost importance and Emerson works hard to deliver secure solutions. Emerson's products enabled with Bluetooth wireless technology have been developed with many security features that will enable you to use them securely. These security features cannot be disabled, either inadvertently or intentionally. This white paper will address Emerson's technology implementation strategy for delivering a secure solution, information on using and hardening Bluetooth communication security features, and recommendations for defense in depth strategies.

Secure Product Development Processes

Development and Testing

Emerson has incorporated cybersecurity into each aspect of the product development process. Cybersecurity requirements are defined to ensure they are considered from the start. Periodic secure design, architecture, and code reviews are conducted throughout the development lifecycle of the product. In addition, extensive threat modeling is performed to ensure threats are considered and addressed.

Once the Bluetooth interface has reached a level of maturity that it can be tested, it undergoes penetration testing. Penetration testers use the same techniques malicious actors would employ and Emerson uses the results of this testing to further improve the security of the products. This penetration testing is not only conducted by Emerson's dedicated team of highly trained penetration testers but also sent to third party penetration testers. Penetration testing against the Bluetooth solution will be performed periodically so that, as new testing techniques are developed or new threats are discovered, the product will continue to stay in a defendable state by following Security Best Practices.

In addition to penetration testing, Emerson continuously monitors for new Bluetooth communication vulnerabilities using the latest, industry accepted security tools to proactively search for threats which may affect the products. Emerson's field devices are designed in a modular approach meaning that even if Bluetooth communication is disrupted, the primary function of the field device will continue to operate as expected. This modular approach also means that Bluetooth functionality does not impact device SIL certification.

Secure Communications

Bluetooth technology contains two communication channels:

- **Broadcast** (also known as advertising): Emerson field devices will broadcast important field device data such as tag, status, and process variables.
- **Connection**: This is a point-to-point communication between the field device and AMS Device Configurator. With Emerson's Bluetooth technology implementation, a secure connection is only made upon a user successfully entering the factory key or user-created passwords into AMS Device Configurator.

Emerson's solution was developed for industrial applications. This means that field device data is considered confidential and needs to be protected. With standard Bluetooth technology, there is optional security for broadcast data, limited authentication options for field devices without displays or buttons, and built-in developer mode that can be used to bypass some security.

To address these concerns, the Emerson solution contains extensive end-to-end application layer security to protect field device data. This application layer security is modeled after industry standard Transport Layer Security (TLS) protocol and adapted to fit low power, embedded industrial applications. All sensitive broadcast data is encrypted. Secure connection is established via a role-based password-authenticated key exchange through the AMS Device Configurator application. A description of roles, default status, password type, and permissions is shown in Table 1. After a secure connection is established, all communicated field device data between the AMS Device Configurator application and the field device is encrypted with AES-256 bit encryption.

All security keys used to protect data on both the field device and the AMS Device Configurator application are protected and cannot be extracted. If a key compromise is suspected, there is support in AMS Device Configurator to change and/or disable security keys. Neither the field devices nor AMS Device Configurator have any undocumented access which means that end users have complete control over who and how the field devices are accessed.

Table 1. Bluetooth® Connectivity Roles and Permissions

Role	Default Status from Factory	Password	Role Permissions
Factory Admin	Enabled (Can be disabled by Administrator role)	Factory key	▪ Read/write device parameters ▪ Modify Bluetooth security settings ▪ Install firmware updates
Administrator	Disabled	User-defined	▪ Read/write device parameters ▪ Modify Bluetooth security settings ▪ Install firmware updates
Maintenance	Disabled	User-defined	▪ Read/write device parameters

Provisioning

Establish Connection

Communication with Emerson field devices over Bluetooth communication requires the AMS Device Configurator application (Figure 1). For the list of currently supported operating systems, visit Emerson.com/Automation-Solutions-Bluetooth.

Figure 1. AMS Device Configurator application

From the factory, each field device is assigned a UID (unique identifier) and factory key that are used to establish a secure connection through AMS Device Configurator. This factory key is randomly generated and unique to the field device. The factory key can be found on disposable wire-on tag (Figure 2) intended for ease of commissioning, and typically also on the field device electronics. See product documentation for exact location of UID and key information. It is important to understand that Emerson does not retain a copy of these factory keys and cannot provide this information in the event it is lost.

When a field device is received from the factory, the only role enabled is the Factory Admin and only the factory key can be used to connect to the field device. Role statuses can be modified after provisioning.

To establish first-time connection with a field device:

1. Launch AMS Device Configurator
2. Select the UID of the field device you want to connect with
3. Enter the factory key for this field device under the Factory Admin role

When connecting under any security role, AMS Device Configurator can optionally save the associated credentials in the application.

Figure 2. Transmitter with disposable wire-on tag

After making a secure connection, AMS Device Configurator will be able to decrypt broadcast data in the Device List (Figure 3). When making critical process decisions, Emerson recommends users securely connect to the field device(s) to ensure the most accurate, up-to-date process data is being used.

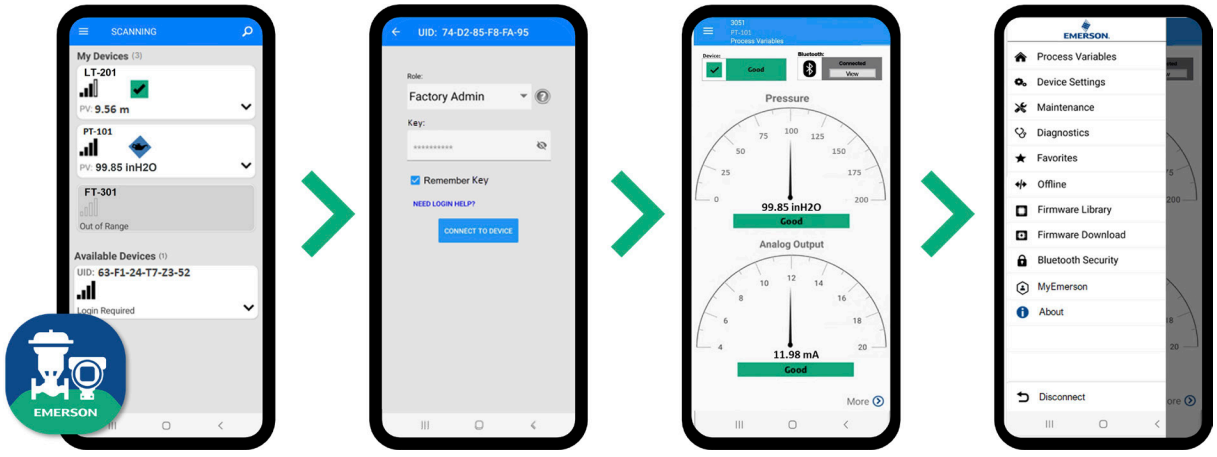

Figure 3. Device list, secure connection, and device descriptor via the AMS Device Configurator application

Set Up User-Defined Passwords

Once a secure connection is made using the Factory Admin Role, the Administrator and Maintenance roles can be enabled with user-defined passwords.

To enable the Administrator and/or Maintenance Roles:

1. Open the Bluetooth Security menu

   On an Android system:

   a. Connect to the field device under the Factory Admin role
   b. Select the menu icon in the top left corner to expose the Bluetooth Security Menu option (Figure 4)

   On a Windows system:

   a. From the main AMS Device Configurator screen, select the lock icon on the desired field device tile (Figure 5)
   b. Connect to the field device under the Factory Admin role

2. Select Modify Role to enable the Administrator and/or Maintenance roles and configure a user-defined password

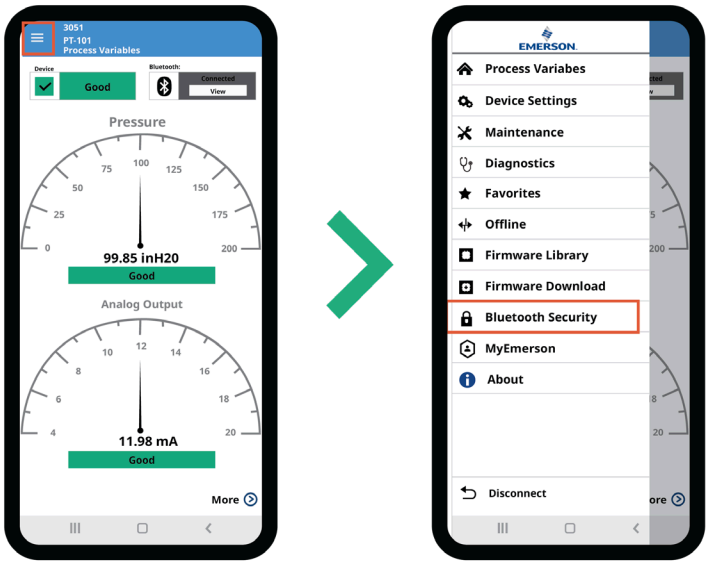

Figure 4. Bluetooth Security menu location on AMS Device Configurator for Android

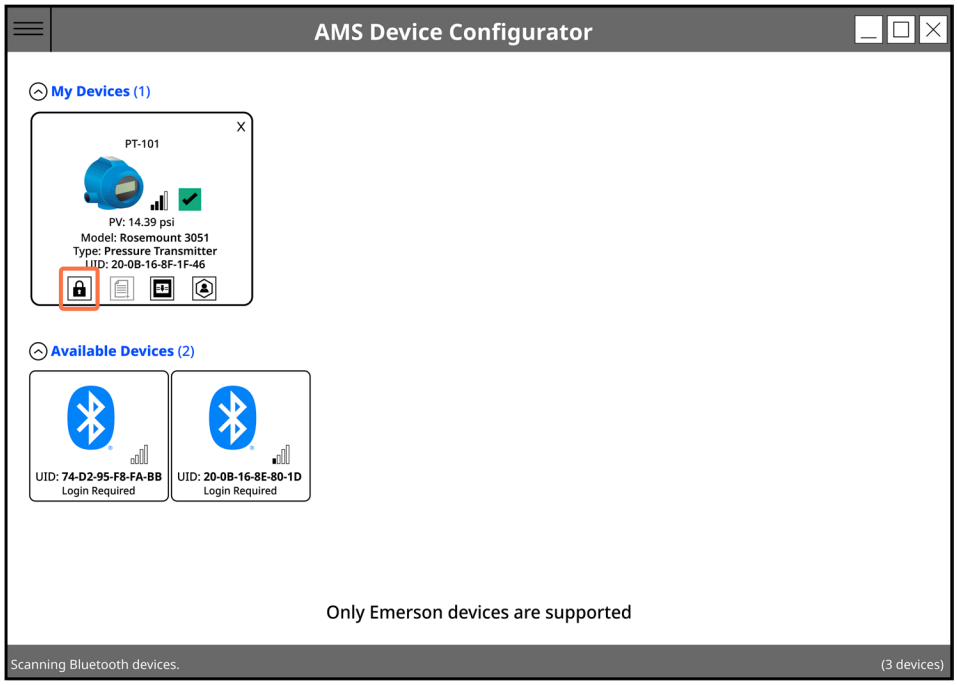

Figure 5. Bluetooth Security menu location on AMS Device Configurator for Windows

Disable the Factory Admin Role

Once the Administrator role is enabled, the Factory Admin role can optionally be disabled. This makes it so that the only way to connect with the field device is with a user-defined password under the Administrator or Maintenance roles, until the Factory Admin role is re-enabled or a Bluetooth Security reset is performed.

Note that you may not modify the role that you are actively connected through. The Administrator role must be used to disable the Factory Admin role.

To disable the Factory Admin role:

1. Open the Bluetooth Security menu

   On an Android system:

   a. Connect to the field device under the Administrator role
   b. Select the menu icon in the top left corner to expose the Bluetooth Security Menu option (Figure 4)

   On a Windows system:

   a. From the main AMS Device Configurator screen, select the lock icon on the desired field device tile (Figure 5)
   b. Connect to the field device under the Administrator role

2. Select Modify Role to disable the Factory Admin role

Operation and Maintenance

Maintain devices on which Bluetooth technology is enabled according to your company's security policy. Multiple features exist within the Bluetooth technology implementation to aid in security maintenance.

Change Password

Only the Administrator and Maintenance roles allow for user-defined passwords. Administrative rights to modify Bluetooth security settings, including role passwords, are granted under the Factory Admin and Administrator roles. If all user-defined passwords are lost or unknown and the Factory Admin role has been disabled, see Reset Bluetooth Security.

To change a user-defined password for the Administrator or Maintenance roles:

1. Open the Bluetooth Security menu

   On an Android system:

   a. Connect to the field device under the Factory Admin or Administrator role
   b. Select the menu icon in the top left corner to expose the Bluetooth Security Menu option (Figure 4)

   On a Windows system:

   a. From the main AMS Device Configurator screen, select the lock icon on the desired field device tile (Figure 5)
   b. Connect to the field device under the Factory Admin or Administrator role

2. Select Modify Role.
3. Select the role for which you would like to modify the password, and follow the prompts. Select Update Password / Enable Role when finished.

Updating Bluetooth Firmware

Bluetooth firmware updates can be applied to the field device with AMS Device Configurator using the firmware update process. The firmware updates themselves are encrypted and digitally signed to ensure they are authentic, and no tampering has taken place. If either the field device or the AMS Device Configurator application identifies the firmware update as invalid, it will not be applied. Devices may only be updated with a newer version of the Bluetooth firmware to ensure that older firmware updates with known vulnerabilities cannot be applied. Note that administrative rights to modify Bluetooth security settings, including updating Bluetooth firmware, may only be performed when connected via the Factory Admin or Administrator roles.

Secure Device List Broadcast Data

Emerson field devices broadcast encrypted field device data such as tag, status, and process variables. Only after making a secure connection, AMS Device Configurator can decrypt broadcast

data in the Device List. AMS Device Configurator allows a new encryption key to be generated to secure broadcasted field device data displayed on the Device List. If rotated, all instances of AMS Device Configurator will need to reestablish secure Bluetooth communication to this device to view Device List information for this tag. Note that administrative rights to modify Bluetooth security settings, including rotating the broadcasting key, may only be performed when connected via the Factory Admin or Administrator roles.

To rotate the broadcasting key for a device:

1. Open the Bluetooth Security menu

   On an Android system:

   a. Connect to the field device under the Factory Admin or Administrator role
   b. Select the menu icon in the top left corner to expose the Bluetooth Security Menu option (Figure 4)

   On a Windows system:

   a. From the main AMS Device Configurator screen, select the lock icon on the device tile (Figure 5)
   b. Connect to the field device under the Factory Admin or Administrator role

2. Select Rotate Broadcasting Key
3. Select Confirm Security Rotation

Reset Bluetooth Security

This process resets Bluetooth security settings to factory conditions. In this state, only the Factory Admin role is enabled, and the UID and factory key are needed to connect with the field device. This can be performed over the Bluetooth connection or through local access to the device.

To reset Bluetooth security settings through the Bluetooth connection:

1. Open the Bluetooth Security menu

   On an Android system:

   a. Connect to the field device under the Factory Admin or Administrator role
   b. Select the menu icon in the top left corner to expose the Bluetooth Security Menu option (Figure 4)

   On a Windows system:

   a. From the main AMS Device Configurator screen, select the lock icon on the desired field device tile (Figure 5)
   b. Connect to the field device under the Factory Admin or Administrator role

2. Select Reset Bluetooth Interface Security and follow the prompts to confirm.

When confirmed:

- The existing connection terminates.
- Both the Administrator and Maintenance roles are disabled. Only the Factory Admin role is enabled.
- Associated Administrator and Maintenance passwords are erased.
- The number of security resets increment. This is a parameter that can be read from the field device.
- Until the Administrator or Maintenance roles are re-enabled, subsequent connection with the field device requires connection through the Factory Admin role.

Bluetooth security settings can also be reset through a wired connection on all field devices and additionally through the local display on some field devices. To reset Bluetooth security settings through a wired or local connection:

1. Refer to the product manual for specific information on what reset paths are allowed and where to find the Reset Bluetooth Security setting for that field device.
2. Navigate to and select Reset Bluetooth Security via wired connection or local display.
3. Once Reset Bluetooth Security has been selected, the user will have 15 minutes to establish Bluetooth communication with the field device using the Factory Admin role and factory key.

   When successful Bluetooth communication is established:

   - Both the Administrator and Maintenance roles are disabled. Only the Factory Admin role is enabled.
   - Associated Administrator and Maintenance passwords are erased.
   - The number of security resets increment. This is a parameter than can be read from the field device.
   - Until the Administrator or Maintenance roles are re-configured, subsequent connection with the field device requires connection through the Factory Admin role.

Disable Bluetooth Communication

Bluetooth communication can be optionally disabled by disabling the Bluetooth radio via wired or Bluetooth connection. Refer to the product manual for specific steps for each field device.

Disposal

When a field device has reached the end of its useful life, users should deprovision the field device as defined in the product manual. To deprovision Bluetooth communication for field device disposal, Emerson recommends resetting Bluetooth security to factory conditions. For more information on this procedure, refer to Reset Bluetooth Security.

It is important to remember that when deprovisioning, it is best practice to remove and discard any labels containing the factory key. This will ensure that a field device may not be reprovisioned in the future.

Defense in Depth

Integrated Security Measures

When Bluetooth communication is specified on a field device, the system includes:

- Field device allowing only one Bluetooth connection at a time
- Factory Admin, Administrator, and Maintenance role-based permissions for the Bluetooth connection
- Password requirements for controlling access to the AMS Device Configurator application used to connect to Bluetooth devices
- Encrypted communications
- Encrypted and signed firmware updates
- Unique session keys

Security Best Practices

Beyond integrated security measures, users are encouraged to follow additional security best practices as well. Defense in Depth strategies are important because they can provide protection when other defense mechanisms are bypassed. A layered defense approach provides a higher level of defense. Other good security hygiene to follow includes:

- Enable write protect on field devices
- Protect passwords and other sensitive data
- Enable the Administrator role and configure a user-defined password, then disable the Factory Admin role
- Enable the Maintenance role for use in the majority of connections
- Follow company policy when creating and managing user-defined passwords
- Manage all roles and passwords according to company policy
- Apply security updates as released

It is also important to remember that end users always have the option to disable Bluetooth communication should that become a requirement.

To protect the mobile device running the AMS Device Configurator application, Emerson recommends managing the mobile device with a Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) system.

Physical security is an important part of any security program and fundamental to protecting your system. Emerson recommends restricting physical access of unauthorized personnel to protect assets. This is true not only for Emerson's products with Bluetooth technology, but all systems used within the facility. Unauthorized personnel can potentially cause significant damage (either intentionally or unintentionally) to end users' equipment.

Emerson Product Security

Threat Monitoring

Emerson continues to monitor for threats through the use of automated scans, periodic threat modeling, and periodic penetration testing. If a threat is identified, Emerson has a dedicated team and formalized processes to handle them. Depending on the severity of the issue, a formal security notification along with a firmware update may be issued.

Report a Vulnerability

Use Report a Vulnerability for reporting vulnerabilities back to Emerson. This will generate a response by Emerson's Product Security Incident Response Team.

For additional information, visit:
Emerson.com/Automation-Solutions-Bluetooth

00870-1100-6129 Rev BA, June 2024

EMERSON™