White Paper

Emerson's Secure Bluetooth® Wireless Technology Implementation

EMERSON™

Introduction

Bluetooth® technology is a standard for short-range wireless communication between devices such as mobile phones, computers, transmitters, and other electronic devices. Emerson has added Bluetooth wireless communication to some field devices as a method for easy configuration and viewing of information via the AMS Device Configurator application. 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 which will help ensure that your facility stays secure. Emerson's Bluetooth solution is secure out of the box. These security features are enabled by default and cannot be disabled, either inadvertently or intentionally.

Product Development and Testing

To start with, Emerson has incorporated cybersecurity into each aspect of the product development process. At early stages of the 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 to these security reviews, extensive threat modeling is performed to ensure threats are considered and mitigated. Once the product has reached a level of maturity that it can be tested, the product undergoes penetration testing. Penetration testers use the same techniques hackers 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 even after the product is in service so that as new testing techniques are developed, or new threats are discovered the product will continue to stay secure.

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 device will continue to operate as expected.

Encryption and Authentication

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 no built-in security for broadcast data, limited authentication options for field devices without displays, and built-in developer mode on Android™ devices 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. After a secure connection is established, all Bluetooth communication between the AMS Device Configurator application and the field device is encrypted with strong 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 security keys. It is also worth mentioning that neither the field devices nor AMS Device Configurator have any undocumented backdoors which means that end users have complete control over who and how the devices are accessed.

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

On all shipped devices, the factory key can be found on disposable wire-on tag (Figure 1) intended for ease of commissioning, and also on the device electronics. See product documentation for exact location. 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.

Figure 1. Transmitter with disposable wire-on tag.

If a user-defined password is lost, it's possible to reset it when logged in as Factory Admin. It's also possible to reset Bluetooth technology security to its initial state when it left the factory. In this case only the Factory Admin role will be enabled, and the factory key will be needed to securely connect to the field device.

Provisioning

When received from the factory, the only security role that will be enabled will be the Factory Admin role. In order to make a secure connection with the field device, the user will need to enter the factory key into the AMS Device Configurator application. Once a secure connection is made, the Administrator and Maintenance roles can be enabled with user-defined passwords (Figure 2). Once an Administrator role is enabled, the Factory Admin role can optionally be disabled.

When connecting with the factory key or user-defined passwords, AMS Device Configurator can optionally save those credentials in the application.

After making a secure connection, AMS Device Configurator will be able to decrypt broadcast data in the Device List. 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.

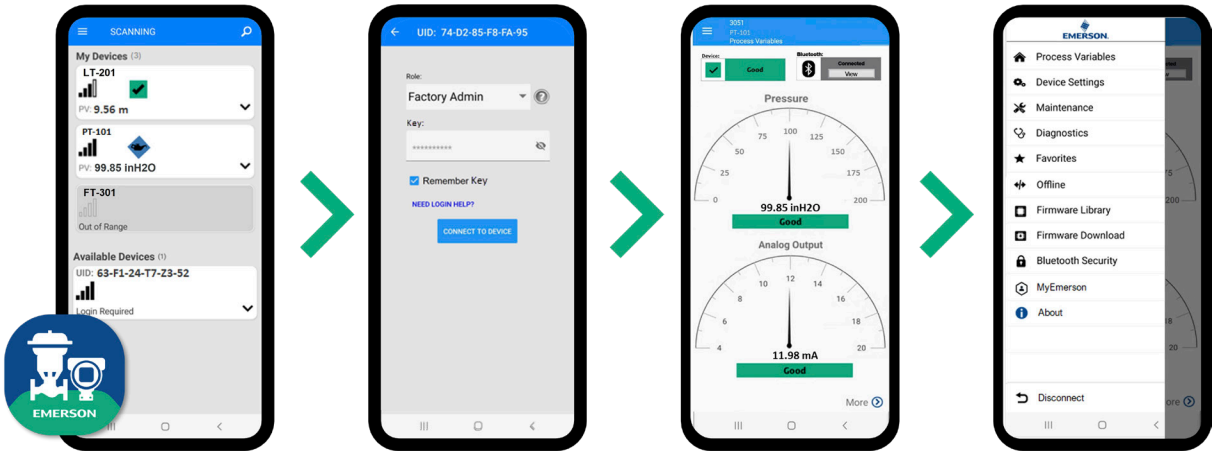

Figure 2. Device list, secure connection, and device descriptor via the AMS Device Configurator application.

Threat Monitoring

As mentioned above, 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.

Firmware updates can be applied to the field device with AMS Device Configurator using the firmware update process. The firmware updates themselves are 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.

Deprovisioning

When a device has reached the end of its useful life, users should deprovision the device as defined in the manual. There are two options for deprovisioning. The first is a two-step process that can be used without authentication. When using the unauthenticated, two-step process, a special message must be sent via the wired HART®, Modbus® or IO-Link interfaces. After the wired message is received from the device, users must enter the factory key into the AMS Device Configurator application.

The second method for deprovisioning can be used if the user is authenticated and has administrative level permissions. Using AMS Device Configurator, the authenticated, admin level user can navigate to the Bluetooth Security section of the AMS Device Configurator application and perform reset 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 device may not be reprovisioned in the future.

Security Best Practices

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 Bluetooth enabled products, but all systems used within the facility. Unauthorized personnel can potentially cause significant damage (either intentionally or unintentionally) to end users' equipment.

Emerson recommends enabling write protects on devices and end users are also encouraged to follow additional security best practices as well. Defense in Depth (DiD) 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 protecting passwords and other important data and changing default passwords. It is also important to remember that end users always have the option to disable Bluetooth communication via the Device Dashboard (DD), when necessary, 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.

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

Linkedin.com/company/Emerson-Automation-Solutions

Twitter.com/EMR_Automation

Facebook.com/EmersonAutomationSolutions

YouTube.com/EmersonAutomationSolutions

00870-1100-6129 Rev AA, January 2023

EMERSON™