Technical Note 172

Bluetooth control panel security

Review of security measures

Bluetooth connectivity is available on several ABB drive families, such as the 180, 380, 480, 580 and ACS880 series. Depending on the specific drive family, Bluetooth comes either as a standard or optional accessory. The addition of Bluetooth allows interface to the ABB app Drivetune. The Drivetune app provides additional flexibility and functionality for commissioning and troubleshooting the drive. Questions regarding security will naturally come up with any product that offers a wireless connection method. This technical note reviews ABB's implementation of Bluetooth to show multiple layers of security.

First, let us review how a device (phone, tablet, PC) is connected to the drive over Bluetooth. The drive's Bluetooth transceiver is in the control panel. The user physically accesses the control panel to activate Bluetooth. At that time, a pairing code is displayed on the control panel's LCD screen. That pairing code is then entered into the Drivetune app on the user's device. The device now pairs to the drive. While this process sounds simple, there are many layers of security throughout the process.

Pairing is an important aspect of Bluetooth security. The ABB Bluetooth control panel supports two pairing modes. The default, and most secure mode allows the drive to become discoverable for up to 5 minutes after the panel's "?" button is pressed for 2 seconds. The Bluetooth control panel generates a random 6-digit pairing code each time. The pairing mode will time out if that 6-digit code is not entered into the device within those first 5 minutes. Alternatively, the drive can be configured to always be discoverable and retain the same pairing code. This alternative configuration provides additional ease of use but is less secure. The 6-digit pairing code is generally accepted to provide an excellent level of security as it provides 1,000,000 different possibilities. The user determines which pairing configuration approach best fits their needs. The remainder of this document assumes the most secure pairing mode is chosen. Specifically for security reasons, the drive does not support automatic pairing. Automatic pairing is often used with consumer electronics.

There is also a physical layer of security with respect to the pairing mode. An unauthorized user with malicious intent first needs physical access to the drive's Bluetooth control panel to activate the pairing mode. Drives are typically in areas not easily accessed by the public. Facilities that have policies regarding wireless connectivity to devices like drives are also the same facilities that typically have strong physical access security practices in place.

The drive also supports multiple passcode authentication for Bluetooth connectivity. The 6-digit pairing code itself is one layer of protection. An additional layer can be added by disabling Bluetooth functionality by the drive via parameter 96.102 bit 7 "Disable panel Bluetooth." The parameter 96.102 is passcode protected by an 8-digit passcode. The user can set that passcode to a unique code and disable Bluetooth. In this situation to activate a Bluetooth connection, first the user must enter the 8-digit code to unlock 96.102, then allow Bluetooth via 96.102 bit 7, hold the "?" button for 2 seconds to enter the pairing mode, and finally take the randomly generated 6-digit code and enter it into their device. This implementation with two levels of passcodes protects against the unauthorized user who may gain physical access to the drive. Even if they gained physical access to the drive, the 8-digit passcode prevents them from enabling Bluetooth.

The fact that the Bluetooth hardware is located on the drive's control panel, and not on the drive's control board, provides flexibility for the user. For example, even if the drive comes standard with a Bluetooth panel, the drive can instead be ordered with a non-Bluetooth control panel. If a drive with a Bluetooth capable panel is ordered, but later the user determines Bluetooth is not desirable due to their in-house security policy, then the panel can be easily swapped out with the non-Bluetooth version. To balance in-house security requirements regarding wireless connectivity, yet still be able to take advantage of the ABB Drivetune app, some users will have non-Bluetooth control panels by default on the drive but keep a Bluetooth version of the panel with the facility manager. This approach allows the Bluetooth panel to

be used on an as-needed basis. As the bottom two drives in Figure 1 show, the Bluetooth control panels are easily identified by the "Bluetooth" text at the top of the control panel. The top three panels in Figure 1 do not include Bluetooth.

Figure 1 Bluetooth control panels

Bluetooth encryption is considered secure. Bluetooth is a global wireless standard managed by the Bluetooth Special Interest Group (SIG). The ABB Bluetooth control panel meets the Bluetooth SIG standards and is compliant to the Bluetooth 4.0 specification. The control panel is Bluetooth Smart Ready (dual mode), supporting both classic and low energy Bluetooth devices. The control panel has a Bluetooth Qualified Design certification. The custom encryption algorithm for Bluetooth classic (Android) is based on SAFER+ (E21, E22), message authentication (E1), and data encryption (E0). The custom encryption algorithm for Bluetooth LE (iOS) is based on AES. The key length is 128.

ABB also has its own cyber security guidelines for hardware and software. The Bluetooth control panel and Drivetune app both fulfill all those cyber security requirements. For example, the Bluetooth control panel passed the ABB security assessment along with robustness testing done by the ABB Device Security Assurance Center. ABB also provides cyber security guidance for drive installation, more information can be found here.

This technical note reviewed Bluetooth related security for the ABB Bluetooth control panel, showing a very strong security approach. The most secure pairing method requires physical access to the control panel to activate the pairing mode. A random 6-digit code is created each time the drive is paired to a device. If there is a security concern that an unauthorized person would have physical access to the drive's control panel, then an additional unique 8-digit passcode can be required to first enable Bluetooth functionality before pairing and its 6-digit passcode occurs. The Bluetooth hardware on the control panel, opposed to the drive's control board, adds security flexibility. The Bluetooth control panel can be physically removed from the drive and installed only when required by authorized facility personnel.