A look at Bluetooth technologies and why they matter for your medical device – Part 1: Overview

In the race to create more connected medical devices, many medical manufacturers are opting to leverage Bluetooth technology to connect to devices with WiFi and cellular capabilities and transfer their data to the cloud where it's most beneficial.

The most significant consideration that device developers who intend to use Bluetooth have to deal with is which protocol is right for their system. To choose wisely, they must clearly define the connectivity needs of their system right from the start.

Despite the similarities in their names, each Bluetooth protocol utilizes different methods to connect and transmit data. As a result, it's a choice that can impact a device's operation greatly.

What is Bluetooth?
Bluetooth is wireless communication standard that facilitates electronic device connectivity and is managed by the Bluetooth Special Interest Group (SIG). At the time of the writing, there are several versions, with Bluetooth 5 being the newest addition. For the sake of brevity, we'll focus on the most currently prevalent versions in the medical device space: Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) and Bluetooth Low Energy (LE). Each implementation has different use cases and uses different chipsets to meet essential hardware requirements.

Differences

Despite the shared name, BLE is actually a different animal. Launched in 2010, it was a clean-sheet design technology meant to achieve goals of low power consumption and latency while accommodating the widest possible interoperable range of devices. As a result, BLE data throughput rates can fluctuate depending on which smartphone platform you're utilizing.

Bluetooth Classic facilitates relatively short-range, continuous wireless connection, which makes it ideal for use cases such as streaming audio and data. Conversely, BLE allows for short bursts of long-range radio connection, making it ideal for uses requiring dependable, periodic device-to-handset data transactions, while also extending battery life (small devices are said to run as much as 5-10 years on a single coin battery).

Pairing, Bonding and Encryption

To determine which protocol is a fit, it is important to understand fundamentally how Bluetooth works.

Pairing, Bonding and Encryption are terms common to the use of Bluetooth Classic and BLE. Pairing is the process by which involved devices exchange their identity information to establish trust and ready encryption keys for future data exchanges. Depending upon the user requirements and capabilities of the device, both protocols include several options for pairing.

Pairing establishes *keys* which can then be used to encrypt a link. A specific *key distribution* is then performed to share the keys. The keys can be used to encrypt a link in future reconnections, verify signed data, or perform random address resolution.

With the connective methodology known as Burst-based, the device advertises on a schedule for smartphone response. When the smartphone responds, a *handshake* (bonding) is made, facilitating a confirmed transfer of the data packet to the smartphone before closing the connection. Data is then transferred from the smartphone to the cloud.

Encryption is the process of converting information or data into a code in order to protect sensitive information transmitted online.

BLE supports the ability to send authenticated data over an unencrypted transport between two devices with a trusted relationship. This means that in some circumstances where the communication channel is not encrypted, the device could still utilize a method to maintain and ensure the data authentication.

In certain instances, bonding and encryption can be done in one operation. It depends upon what the specific requirements are in relation to that device's operation.

There are different pairing considerations for device operations using Bluetooth Classic or BLE. With Bluetooth Classic, pairing is required. With BLE there are two options: One is that pairing is not required and data is advertised publicly. Secondly, secured pairing can be enabled on a BLE device to ensure that only authorized devices are connected. Connection without pairing can place the system at greater risk of cyber threats such as Man-In-The-Middle attacks (MITM)—an important risk consideration, especially for medical devices.

To ensure that communication is always secure and protected, the Bluetooth Core Specification provides several features to cover the encryption, trust, data integrity and privacy of user data. In addition, BLE supports a feature that reduces the ability to track the device over a given period of time by changing the Bluetooth device address on a frequent basis. The address changes are resolved by trusted devices and in order to use it, all devices involved need to have been paired in advance.

Bluetooth and BLE: The Differences in Connectivity and Transfer

As stated above, with BLE's burst-based methodology, the device advertises on a schedule for smartphone response. When the smartphone responds, a bonding is accomplished, which facilitates a confirmed transfer of the data packet to the smartphone before closing the connection.

This means that that energy-intensive act of establishing and maintaining a connection for data transfer is limited to scheduled requests, thus conserving valuable battery power on the device. This efficiency is also, in part, where it gets its name.

For Bluetooth Classic, continuous connectivity is just what the term implies. This method requires that the device be "on" all the time to facilitate a continuous stream of data between the device and the smartphone.

With Continuous connectivity you can have a near-real-time, "live" feed. For instance, if you are doing continuous, remote monitoring of ECG and other vital signs and sending out alerts based on differentials to baseline patterns, you will need to employ this method in your system. For further information, see our case study on remote ECG monitoring.

There's more to consider. In Part 2, we'll explore security considerations, restrictions and a few example use applications.