Bluetooth® low energy and the automotive transformation

Texas Instruments

Khanh Tuan Le
Systems Engineer
Texas Instruments

Introduction

The automotive industry has been experiencing a tremendous transformation. For many consumers, cars are evolving from being just a transport medium to becoming an integral part of their digital lives. The modern automobile is a technology hub hosting wireless technologies like GPS, *Bluetooth*®, Wi-Fi®, near field communication (NFC) and cellular (4G/5G), all serving as complementary connectivity options to help enhance functionality, user safety and comfort.

One of the latest developments in the midst of this transformation is automotive original equipment manufacturers' (OEMs) embrace of Bluetooth low energy technology (**Figure 1**) because of its technical merits and embedded presence in smartphones. The intent is to enable consumers to use their Bluetooth low energy-equipped smartphones and portable devices to manage applications revolving around in-vehicle control, personalized infotainment, vehicle diagnostics, car access, vehicle sharing and piloted parking. As the industry also evolves to be greener, replacing cables using low-power wireless technology is another major potential for Bluetooth low energy.

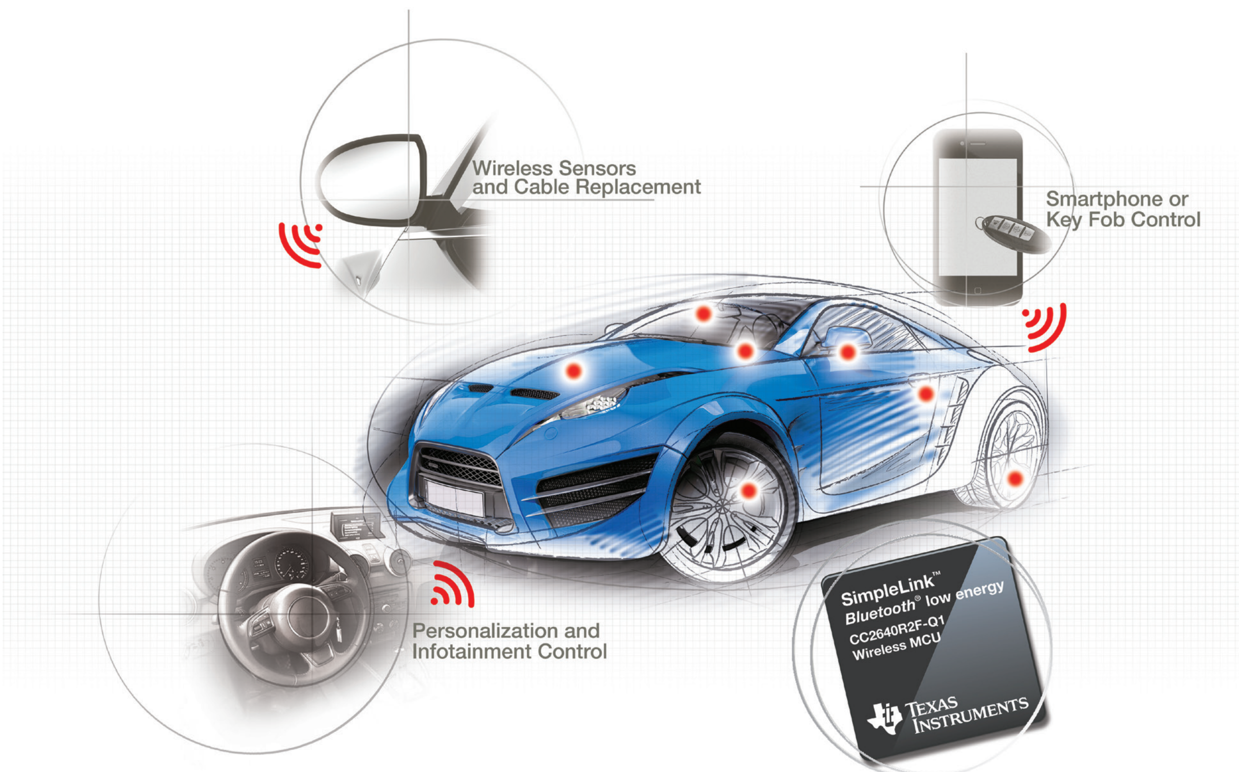

Figure 1*. Bluetooth low energy-enabled applications as part of the automotive transformation.*

Bluetooth low energy in automotive applications

Embedded into modern smartphones, wearables and tablets, Bluetooth low energy technology enables consumers to use their own mobile devices to interact with any Bluetooth low energy-enabled device.

Bluetooth low energy is attractive for automotive applications because of its ability to work with applications on now-ubiquitous smartphones.

The idea behind virtually connecting smartphones with automobiles is to increase driver and passenger convenience and to bring a consumer's personalized entertainment and connected experience into the car environment safely and easily.

Examples of Bluetooth low energy-enabled automotive applications revolving around smartphones include:

- **Smart vehicle access.** The driver's smartphone functions as a virtual key, with secured information recognized by the vehicle that allows specific functions (lock/unlock/engine start) to occur. Bidirectional communications between the phone and the car take place via Bluetooth low energy.
- **Car sharing.** Smart vehicle access using a dynamic virtual key facilitates a secure and convenient way to lend and rent cars. A smartphone app receives the necessary codes to access the assigned vehicle. When the driver approaches the vehicle, Bluetooth low energy communications authenticate the codes on the smartphone, enabling drivers to access certain functions. In addition to function access, the time and duration of access are also pre-configurable.
- **Vehicle diagnostics information.** Vehicle diagnostics information such as tire pressure, fuel level, battery status and temperature can be sent from the vehicle directly—or in some cases through a standard key fob (for security or longer range) to a smartphone using Bluetooth low energy. Smartphones can also display diagnostic information to help drivers understand cryptic warning lights.
- **Driver assistance and personalization.** The vehicle can automatically recognize the smartphone as the driver approaches and activate interior and/or exterior lighting, personalize seat positions, and adjust seating, ventilation and air conditioning (HVAC) settings and infotainment preferences.
- **Piloted/assisted/remote parking.** The idea behind it is simple: the user exits the vehicle, pulls out the smartphone and activates an app and the car drives itself off to a parking spot nearby. Piloted parking is a very efficient and convenient way to park a car in tight parking spaces where manual parking is difficult and getting in and out of the car is practically impossible due to space limitations. The sensing and maneuvering operations required to self-park involve many sensors located around the vehicle, as well as embedded intelligence inside the vehicle. Communication between the car and a smartphone app via Bluetooth low energy can activate and monitor the parking process. (Typically, a certain "drive" motion on a smartphone touchscreen is required to maintain the process; if the driver lifts their finger from the screen or the drive motion ceases, the vehicle will immediately stop.)

Determining position or location finding with use-case-dependent requirements for resolution and accuracy will be tremendously important for smartphone-assisted and other automotive applications in and around connected cars. The most well-known techniques for location finding include estimating the received signal strength (RSSI) or time of flight (TOF) in order to determine the distance between the transmitter and the receiver, and estimation of the angle of arrival (AOA) or angle of departure (AOD), which can further extend to triangulation. Location finding with high accuracy and resolution in real wireless environments is highly challenging, and satisfactory solutions will need to combine several or all of these techniques.

Determination of position can be used in a wide range of applications, including relay attack prevention and customization of certain functions based on the driver's position. Although Bluetooth low energy doesn't inherently include location features today, both the Bluetooth low energy specification and innovative Bluetooth low energy-based automotive systems will likely evolve to address location challenges in the near future.

Bluetooth low energy functionality of the smart vehicle access including Passive Entry Passive Start (PEPS) and other smartphone-related applications (piloted parking, car sharing, etc.) can typically be implemented in the vehicle as part of the Body Control Module (BCM), Electronic Control Unit (ECU), telematics module or similar. These designs can use a dual-mode Bluetooth or single-mode Bluetooth low energy integrated circuit (IC).

Figure 2 shows an example of Bluetooth low energy-enabled car access use case, where the Bluetooth functionality on the car side is implemented in the BCM and the Bluetooth-equipped key can be either a traditional key fob, a wearable or a smartphone.

Replacing cables is another potential application of Bluetooth low energy. Currently, most vehicle sensors connect to ECUs with physical wires. As the complexity of vehicles increases, the number of wires needed to connect sensors leads to increased weight and cost. Furthermore, wired connections can limit sensor locations and hence the range of applications.

Using wireless sensors can help reduce vehicle weight and save fuel consumption. Replacing cables between mirrors, windows and the vehicle trunk with Bluetooth low energy technology can also improve connection reliability and offer manufacturing flexibility by eliminating physical connections. **Figure 3** on the following page illustrates how the Bluetooth low energy wireless link can replace the wires between the window, or mirrors and the BCM.

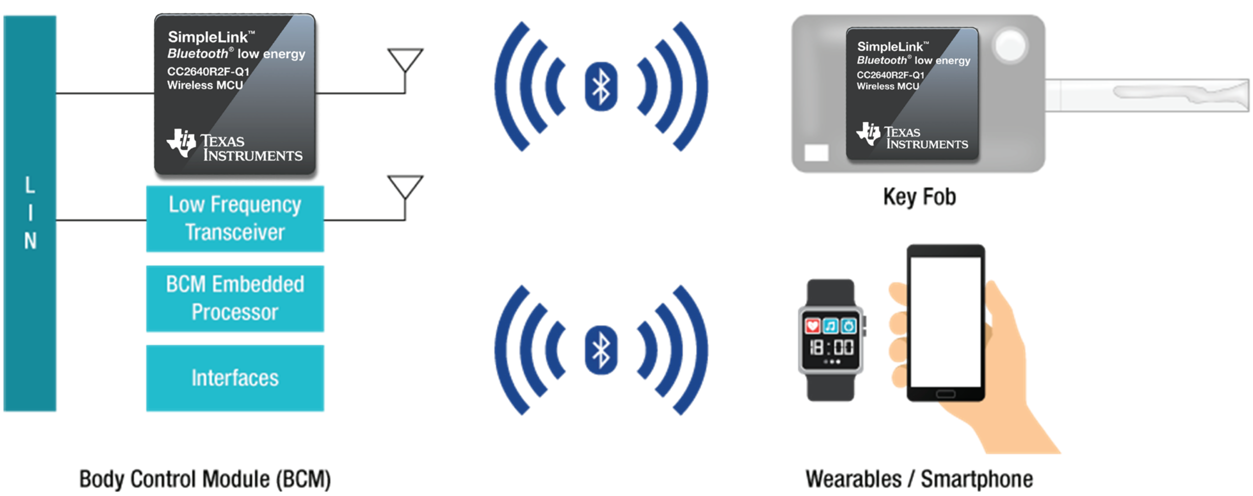

Figure 2. *Bluetooth low energy-enabled car access block diagram.*

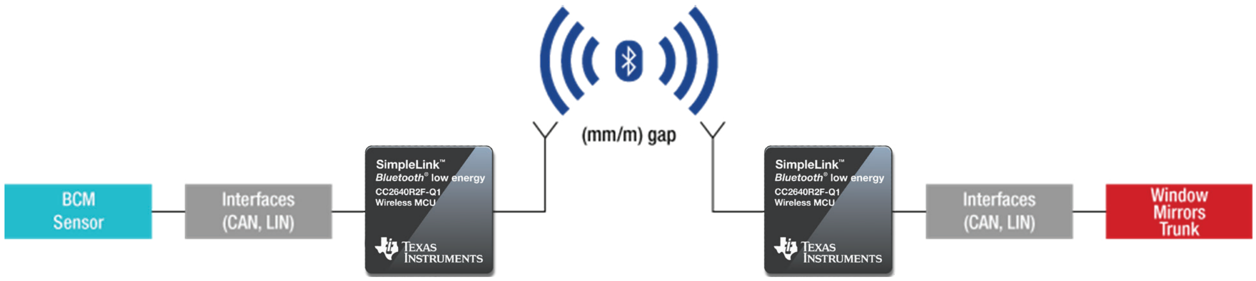

***Figure 3**. Bluetooth low energy-enabled cable replacement concept.*

Cable replacement is typically best served by single-mode Bluetooth low energy ICs given the low-power and low-cost requirements.

There are likely other potential in-car features and functions that could become a reality once the need to run wires isn't an issue. For example, many car dashboards have a limited amount of space for buttons. Combining wireless sensors and a large in-car display or a smartphone would be a good solution to address such challenges.

For wireless applications, the usable frequency spectrum must follow regional and global regulations. Bluetooth low energy wireless technology operates in the 2.4-GHz industrial-scientific-medical (ISM) band, which is available worldwide. This is particularly important when using Bluetooth low energy for in-vehicle networks to replace cables. If carmakers used the sub-1GHz (ultra-high frequency [UHF]) bands, they would need to customize the network frequency based on the target market region.

Bluetooth low energy technology background

With its ubiquitous and simple characteristics, Bluetooth technology has played a pivotal role in revolutionizing wireless communication for a vast number of applications, ranging from personal training gadgets to advanced medical and automotive systems.

As I mentioned, Bluetooth operates in the 2.4-GHz ISM frequency band, which is allocated for unlicensed operations worldwide. There are two flavors in the Bluetooth standard: basic rate/enhanced data rate (BR/EDR), commonly referred to as "classic" Bluetooth, and Bluetooth low energy. Both flavors are complementary and optimized for different applications. While classic Bluetooth is intended for high-throughput, high-duty-cycle applications such as wireless headsets or speakers, Bluetooth low energy is optimal for low-duty-cycle applications with modest data-throughput requirements, such as a heart-rate belts or car key fobs.

From a technical perspective, there are essentially three different types of devices: single-mode classic Bluetooth, single-mode Bluetooth low energy and dual-mode Bluetooth. Dual-mode devices can communicate with both classic Bluetooth and Bluetooth low energy devices. Bluetooth low energy devices by definition cannot communicate with classic Bluetooth devices; they can only communicate with other Bluetooth low energy devices (either single or dual mode). Bluetooth low energy was introduced as part of the Bluetooth 4.0 Core Specification in 2010. It is a radio standard designed for the lowest possible power consumption and specifically optimized for low-complexity, low-cost and low-bandwidth wireless applications.

Since its introduction, Bluetooth low energy has evolved through the ratification of revisions Bluetooth 4.1 (December 2013), 4.2 (December 2014) and 5.0 (December 2016). Major updates include security enhancements in 4.2 and additional data rates in 5.0.

In addition to the instrumental prerequisite of being one of the supported wireless technologies on smartphones, Bluetooth low energy has the technical and commercial merits for automotive applications: low power, high security, a robust wireless link and a strong industry ecosystem.

Low power

The most common use cases for Bluetooth low energy, including those in the automotive space, share small amounts of data and can operate for years on a single coin-cell battery. The number of ECUs in cars is constantly growing to enhance users' safety, functionality and comfort. Adding more electronics entails more stringent power consumption requirements. High electrical power consumption means reduced fuel economy, and excessive power consumption in the ignition off mode can deplete the car battery and prevent the vehicle from starting after prolonged parking. As a result, every system's power consumption during any and all operating conditions needs to be minimized. Low-power merit of the Bluetooth low energy technology is therefore essential to wireless automotive applications.

Bluetooth low energy is tailored from the physical layer (PHY) to higher operational layers to keep power consumption to a minimum. At the PHY, Bluetooth low energy specifies relatively relaxed channel spacing (2 MHz) and selectivity requirements, and uses the constant-envelope Gaussian frequency shift keying (GFSK) modulation scheme, which allows the use of power-efficient nonlinear power amplifier designs. Bluetooth low energy specifies only 37 channels and performs discovery on three channels. Discovery and connection times can be kept as low as a few milliseconds given this simple channelization scheme. Low power consumption at the network protocol layer is achieved by efficient duty cycled operation (allowing the device to stay connected in sleep mode and briefly waking up to transmit a small amount of data), together with strict power management and low transmission overhead. These relaxed requirements allow semiconductor vendors to optimize sleep and active currents and shorten switching times. These optimizations enable (single-mode) BLE devices to be simple, low power and low cost.

Current single-mode Bluetooth low energy ICs typically integrate all functionality in a sensor-type device except the sensing element itself. The Texas Instruments (TI) SimpleLink™ Bluetooth low energy CC2640 family, including an automotive-grade Automotive Electronics Council (AEC)-Q100 qualified device (the CC2640R2F-Q1), is an example of a single-mode Bluetooth low energy wireless microcontroller (MCU) solution containing a radio-frequency (RF) transceiver, an MCU and peripherals, as well as embedded nonvolatile memory (Flash). The CC2640 device draws only around 6 mA (peak) in radio transmit (TX) or receive (RX) modes and consumes ~1 µA of standby power with a low-power clock running. The on-chip reprogrammable Flash memory enables easy and quick firmware upgrades, including over-the-air (OTA) upgradability devices in the field.

High security

Protecting a consumers' private information is important for every wireless system; for automotive applications, security is of paramount importance. Secure communications keep exchanged data safe and at the same time prevent unauthorized devices from injecting data to trigger unintended operation of an automotive system.

The Bluetooth low energy security toolbox includes:

- **Pairing and key generation/exchange.** The pairing mechanism is the process where the devices involved in a communication exchange their identity information to establish trust and get the encryption keys ready for future data exchange. The four options for pairing, included in Bluetooth 4.2 and later revisions, are just works, passkey entry, out of band (OOB) and numeric comparison. Bluetooth core specification version 4.2 introduced the Federal Information Processing Standard (FIPS)-compliant elliptical curve Hellman-Diffie (ECDH) algorithm for key exchange. This was a great security enhancement to the pairing process.
- **Encryption.** Encryption in Bluetooth low energy uses the Advanced Encryption Standard (AES) in the Counter Mode with Cipher Block Chaining Message Authentication Code protocol. This function generates 128-bit encrypted data from 128-bit key and 128-bit plain-text data using the AES 128-bit block cypher as defined in FIPS 197.
- **Signed data.** Bluetooth low energy supports the ability to send authenticated data over an unencrypted channel between two devices with a trusted relationship. The transmitter first signs the data packets with a secure signature comprising a message authentication code generated by the signing algorithm and a counter (to protect against a replay attack). Upon reception, if the receiver verifies the signature, the data is presumably from a trusted source.
- **Privacy.** Bluetooth low energy supports a feature that reduces the ability to track a Bluetooth low energy device over a period of time by changing the device address frequently. Only trusted devices can resolve this private address.

The Bluetooth low energy toolbox supports five basic security services:

- **Pairing and bonding** to create one or more shared secret keys and store those keys for use in subsequent secure connections.
- **Authentication** to verify the identity of communicating Bluetooth low energy-enabled devices based on their address.
- **Confidentiality** to prevent information compromise caused by eavesdropping, and ensure that only authorized devices can access and understand exchanged data.
- **Authorization** to allow the control of resources and ensure that a device is authorized to use a service before permitting it to do so.
- **Message integrity** to verify that data exchanged between two Bluetooth low energy devices has not been altered or compromised in transit.

To protect communications from unauthorized access, wireless automotive systems must prevent passive eavesdropping and man-in-the-middle (MITM) attacks. Passive eavesdropping is secretly listening to (or “sniffing”) the private communication of others without their consent. Bluetooth low energy-based automotive systems can protect against passive eavesdropping by using a key to encrypt data. Bluetooth low energy Secure Connections uses the ECDH public key cryptography to combat passive eavesdropping attacks. The ECDH algorithm provides a very strong mechanism when exchanging keys over an unsecured channel and makes it extremely difficult for a malicious device to guess the encryption key.

In an MITM attack, as two Bluetooth low energy devices (such as a car and a smartphone virtual key) try to communicate with each other, a third device inserts itself between them and emulates each device to the other. Authentication through secure pairing or signed data can protect against MITM attacks and ensure that a vehicle is communicating with the intended virtual key and not an unauthorized attacker.

It is possible to efficiently integrate Bluetooth low energy security features on single-mode Bluetooth low energy ICs. For example, TI's SimpleLink CC2640R2F-Q1 wireless MCU is an AEC-Q100-qualified temperature grade 2 (–40°C to +105°C) Bluetooth low energy wireless MCU that supports all Bluetooth 4.2 and 5.0 security features. The CC2640R2F-Q1 device includes a highly efficient AES encryption hardware module, a cryptography library in read-only memory (ROM) (elliptic curve), a true random number generator (TRNG) and related security signal processing. These features are effective tools that can enable automotive designers to implement Bluetooth low energy security and other customized security solutions for their applications.

Bluetooth low energy technology provides several features to cover the encryption, trust, data integrity and privacy of user data in and around a connected car. Automotive OEMs, Tier 1s and third-party developers can achieve secure and reliable wireless communication through the use of these security features and other innovative techniques.

A robust wireless link

The achievable RF link budget and co-existence with other wireless systems are the main determining factors governing the robustness and reliability of a wireless connection.

The achievable Bluetooth low energy range is inherently set by a device's maximum transmit output power and best receiver sensitivity. In addition, the performance of the antenna and physical obstacles in the transmission path are major factors affecting the communication range.

Bluetooth is commonly known for short range (~10–30 m) personal area networks, and this is often what users experience with Bluetooth headsets and wireless speakers. However, both Bluetooth and Bluetooth low energy technology have much longer range potential than typically believed. Bluetooth low energy informal tests with smartphones have shown ranges of 350–500 m.

Today's Bluetooth low energy radios significantly surpass the minimum RF requirements in the core specification and therefore are capable of extending communication far beyond the initially envisioned tens-of-meters range. For example, TI's SimpleLink CC2640 devices support a receive sensitivity of –97 dBm and +5 dBm output power, or equivalently, an RF link budget of 102 dB using the standard 1-Mbps data rate.

Bluetooth 5.0 adds three new data rates to the Bluetooth low energy PHY, one of which is a new capability to increase the bandwidth to 2 Mbps. This data rate facilitates rapid and reliable OTA firmware updates or fast uploads of collected data. The other two data rates (125 kbps and 500 kbps) are specifically tailored to increase range. The 125-kbps Bluetooth low energy coded PHY option targets an approximate quadrupled range compared to the Bluetooth low energy 4.x 1-Mbps PHY through the implementation of clever signal processing that doesn't increase the overall transmission power consumption. Using the same device reference, TI CC2640 devices support a receive sensitivity of –103-dBm and +5-dBm output power, or equivalently an RF link budget of 108 dB using the 125-kbps Bluetooth low energy coded PHY option (with a 1.6 km range demonstrated outdoors). This high RF link budget can maximize range, ensure communication margins or both.

Supporting multiple data rates, Bluetooth 5.0 provides the flexibility for automotive application developers to dynamically make the best choices for their implementation, since they can tune the range and bandwidth for a variety of environments.

To improve transmission robustness, Bluetooth low energy employs the adaptive frequency hopping (AFH) scheme common to all flavors of Bluetooth to minimize interference from other wireless technologies in the 2.4-GHz ISM band. Bluetooth low energy can for instance dynamically update the frequency-hopping sequence to avoid channels where interference occurs during active communications. Frequency hopping is also a power-efficient way to mitigate multipath fading issues.

From an RF perspective, Bluetooth low energy technology is capable of satisfying the required performance for automotive applications.

A strong ecosystem

Bluetooth low energy has seen a phenomenal adaption rate and is widely supported by a large number of semiconductor vendors.

Integrated devices in vehicles must operate reliably over time under harsh voltage, current, temperature and vibration conditions. Automotive-grade semiconductor devices are therefore designed, packaged, characterized and stress-tested significantly more thoroughly than devices intended for standard commercial gadgets.

Automotive manufacturers commonly require AEC-Q100-qualified devices for their designs. The AEC-Q100 industry standard is a failure-mechanism-based stress-test qualification for packaged ICs developed by major automotive manufacturers and suppliers. It details a set of stress tests, defines the minimum stress-test-driven qualification requirements and references test conditions for the qualification of ICs.

Making AEC-Q100-qualified (automotive-grade) Bluetooth low energy ICs poses stringent requirements on the overall quality system and demands a lot of resources from semiconductor manufacturers, but the automotive market also represents a significant business opportunity. The potential of Bluetooth low energy within the automotive market drives the availability of innovative automotive-grade Bluetooth low energy integrated solutions, including TI portfolio solutions comprising low-power wireless MCUs and software stacks.

Summary

The automotive industry is undergoing one of its greatest transformations since the invention of the car more than 120 years ago. Wireless technologies play a pivotal role in this transformation. Bluetooth low energy technology has the technical merits and industry foundation to enable innovative, low-power wireless automotive solutions in modern connected cars.

IMPORTANT NOTICE FOR TI DESIGN INFORMATION AND RESOURCES

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265