Technical Article

How to Create a Robust Building Security System with TI’s SimpleLink MCU Platform

Casey O'Grady

It’s hard to imagine a world before smartphones. What used to be a futuristic plot on the Jetson’s is now the reality we live in. As we strive to connect more of our lives, homes and buildings, the design complexities can rapidly escalate. Learning wireless protocols and acquiring radio-frequency (RF) design experience can be an overwhelming venture. Add network security and power budgets into the mix, and you’ll quickly feel like a freshman walking into their first college lecture.

Take a home or building security system as an example. There are door and window sensors, motion detectors, smoke detectors, smart locks, and a security panel that need to connect wirelessly, comply with local regulatory requirements and perform with high accuracy at the lowest power consumption. That’s a big task to execute. But I have a few simple pointers that can help you avoid the headache and design with ease.

1. Select a Platform That Supports Multiple Wireless Protocols.

A building security system may have multiple RF technologies and will often leverage multiple protocols. These are the leading players for building security applications:

- **Sub 1-GHz** is a dominant technology for any security sensor because of its extremely long range capabilities and great wall penetration for indoor applications. You can use this protocol to create a low-power star network of sensors that report data to a gateway or collector.
- **Zigbee®** is a great technology for device-to-device communication, as it is a proven solution for a mesh network. It’s popular in electronic smart locks, door and window sensors, and smoke detectors, with well-defined security procedures to protect data.
- ***Bluetooth*® Low Energy** is an emerging technology that’s often used in conjunction with Sub 1-GHz or Zigbee. Bluetooth Low Energy’s inherent smartphone connectivity makes it a great choice for configuring a network and diagnostic alerts. With the range enhancements of Bluetooth 5, this low-power protocol is also a good fit for battery-operated sensors within a home or for appliances such as electronic smart locks.
- **Thread** is also an emergent technology designed to control and connect products such as motion sensors, gas detectors or gateways. Thread uses the 2.4GHz industrial, scientific and medical (ISM) band to create a secure mesh network and is based on Internet Protocol version 6 (IPv6), giving it a natural connection to existing networks. Thread supports device-to-device, device-to-smartphone, and device-to-cloud communication, which makes it easy to use and extremely scalable.
- Dynamic Multi-protocol **Manager (DMM)** is a great technology to implement multiple protocols in a single chip solution such as smart meters, locks & thermostats. DMM is a software module that enables a single radio to operate multiple wireless protocols concurrently by switching between them in real time. This is also known as “Time Multiplexing”, in which the radio switches between the two protocol stacks by changing the settings, channels, and other parameters.

You can implement building security systems using any one of these technologies or a combination of several of them. Thus, it’s a good idea to choose a hardware platform that can address multiple protocols and give you software flexibility depending on your application.

2. Address Network Security.

Security is a key concern, especially in building security systems. Consumers want to know that their personal information will remain protected. When choosing a wireless platform, security must be at the forefront of your decision. Let’s take a look at the security measures of the wireless protocols I just reviewed:

- In **Sub 1-GHz**, designers can implement the Advanced Encryption Standard (AES) algorithm and authentication, as well as message integrity to ensure network security.
- ***Bluetooth* Low Energy** also leverages AES hardware encryption. The Bluetooth low energy 4.2 specification implemented increased security to prevent man-in-the-middle attacks and correct pairing vulnerabilities.
- **Zigbee** has defined procedures to ensure the secure request and exchange of keys, and uses install codes to eliminate the use of well-known keys as well as AES encryption.
- **Thread** implements IP-based security with Datagram Transport Layer Security (DTLS), password-based authentication and AES encryption.

With each of these protocols, it's important to assess the threats in your system and use security enablers to address these concerns.

3. Seek High Performance and Low Power.

When designing a building security system, you have to take range and power seriously. Extending the battery life of door and window sensors, electronic smart locks, and smoke detectors helps create a positive experience with the end product. Not only do you have to evaluate a device's receiver and transmitter current; you must also evaluate the sleep current to ensure maximum battery life.

Likewise, ensuring maximum coverage within a home is paramount. Whether it's controlling a large number of devices within a mesh network or simply using a smartphone to control one device, it's imperative that users can maintain a reliable connection. Output power and sensitivity are the critical parameters you need to determine the achievable range. By leveraging a large link budget, a security system will be able to cover a greater distance within a home or building.

Conclusion

Designing a security system can be challenging, especially when it comes to the many connectivity options, network security and performance. With the flexibility to support Sub 1-GHz, Bluetooth Low Energy, Zigbee, Thread and dual-band protocols, TI's wireless microcontrollers (MCUs) are geared to provide robust and secure solutions for building security systems.

These powerful devices feature more memory, peripherals, flexibility and processing power, as well as excellent RF performance at extremely low power consumption. As you design a building security system, keep the suggestions above in mind to unlock the most innovative designs yet.

Additional Resources:

The SimpleLink multi-standard CC2652P wireless MCU (Thread, Zigbee, Bluetooth 5 with integrated Power Amplifier)

- Get started with the LAUNCXL-CC2652P LaunchPad development kit and the CC26X2 SDK.

The SimpleLink Bluetooth 5 CC2642R wireless MCU

- Get started with the LAUNCXL-CC26X2R1 LaunchPad development kit and the CC26X2 SDK.

The SimpleLink Sub-1 GHZ CC1312R wireless MCU

- Get started with the LAUNCHXL-CC1312R1 LaunchPad development kit and the CC13x2 SDK

The SimpleLink multiband CC1352R wireless MCU (Sub-1 GHz + *Bluetooth* Low Energy, Thread, Zigbee).

- Get started with the LAUNCHXL-CC1352R1 LaunchPad development kit and the CC13x2 SDK.

Read this blog on all the SimpleLink MCU platform devices

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

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