We get technical

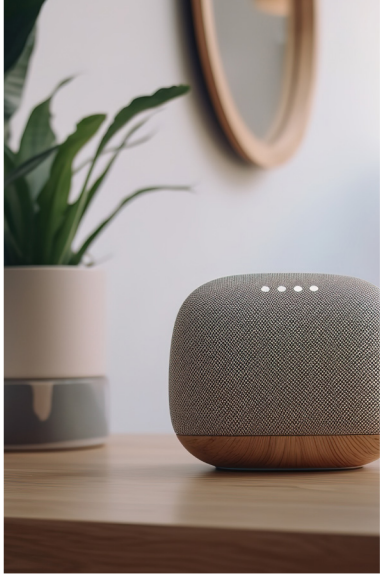
Taking Matter into your own hands

5G putting the smart in today's smart homes

Is Ultra-Wide Band the next big wireless technology

Wi-Fi 6 offering smart connections to smart homes

DigiKey



contents

Editor’s note

The Internet of Things (IoT) has emerged as a transformative and revolutionary concept, reshaping the way we interact with technology and the world around us.

At the core of IoT is the seamless communication between devices, which enables them to work in tandem, share information, and make intelligent decisions without human intervention. Through the use of sensors, IoT devices can perceive their environment, gather data, and react accordingly, leading to a level of automation and efficiency that was once only imagined in science fiction.

The applications of IoT are vast and diverse, permeating almost every aspect of our lives. In smart homes, IoT technology allows us to remotely control lighting, thermostats, and security systems, enhancing comfort and energy efficiency. In industrial automation, smart factories leverage IoT to optimise manufacturing processes, predict maintenance needs, and improve overall productivity.

Whether you’re an entrepreneur seeking innovative solutions, a developer diving into IoT projects, or an individual curious about the evolving tech-driven world, this practical guide will equip you with a comprehensive understanding of the Internet of Things and its far-reaching implications.

For more information,
please check out our website at
www.digikey.com/automation.

Taking Matter into your own hands: Increasing compatibility among smart home products

Written by:
Paige West,
Editor at Electronic Specifier

Matter (formerly Project Connected Home over IP, or Project CHIP) is a new, royalty-free connectivity standard that promises to increase the compatibility among smart home products

Matter was founded in 2019 by the Connectivity Standards Alliance (CSA) with the goal of simplifying development for manufacturers and increasing compatibility for consumers

It is built around members' shared belief that smart home devices should be secure, reliable, and seamless to use.

Matter has the potential to transform the Internet of Things (IoT) from a plethora of disconnected devices to an interoperable, 'plug-and-play' network.

How does Matter work?

To fully grasp the implications of Matter on the IoT, specifically smart home technologies and the working principle of this novel IoT standard, this section begins by exploring the several layers of the Open System Interconnection (OSI) reference model.

The OSI reference model describes the tasks and conventions that network systems require to communicate with one another[1]. The specifications of this conceptual model remain available for public consumption, hence the term 'open system'. The key objective of the model includes assisting vendors and communications software developers to produce interoperable network systems.

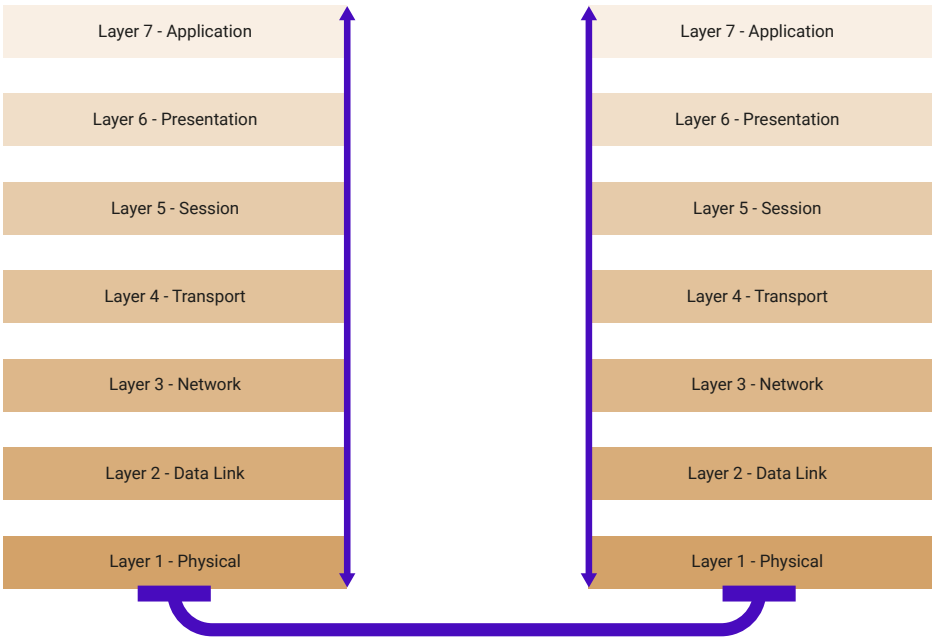


Figure 1. The seven layers of the OSI Reference Model

The structure of the OSI reference model relies on a widely accepted technique known as layering. This technique partitions communication functions into a vertical set of layers, with each performing a related set of functions while enriching and utilising the services of the next layer below. The ITU-T X.200 standards detail seven specific layers for the OSI reference model, including the physical, data link, network, transport, session, presentation, and application layers, in ascending order [2].

Figure 1 presents the seven layers of the OSI reference model.

The application layer, which doubles as the highest in the OSI model, is the closest to the end user. In other words, this layer allows users to directly interact with the software application that initiates communication between client and server. This first layer offers several communication functions, including file sharing, database access, and message handling through common protocols such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Trivial File Transfer Protocol (TFTP), Server

Message Block/Common Internet File System (SMB/CIFS), and Simple Mail Transfer Protocol (SMTP).

A key distinction of the application layer from its counterparts is its ability to differentiate between the application entity and the application [3]. This distinction is evident in an e-transport website that incorporates the ride ordering logic into the application while using HTTP to communicate with customers and a remote database protocol to store orders. Moreover, end users can improve their interaction with the website through the protocol by simply clicking on a button.

Matter utilises the OSI application layer-based working principle to enable communication between devices in smart homes due to the inability of the devices to rely on user interpretation. For instance, Matter can allow seamless communication between a smart light switch and light bulb and a thermostat and furnace. Figure 2 presents the Matter IoT standard architecture overview.

The Matter standard defines several functionalities for its application layer. However, these functionalities fit into three primary areas:

- Device installation and setup for customers
- Sending and receiving messages among smart devices and message content

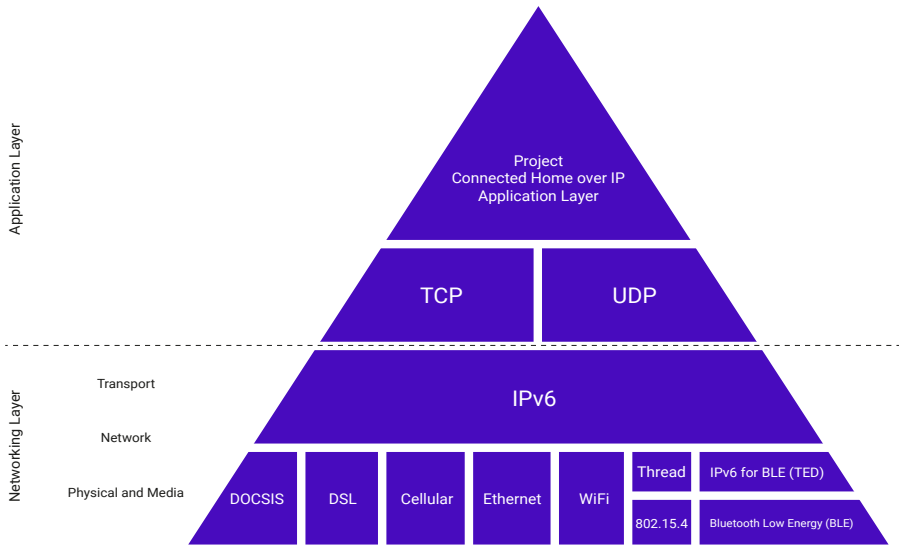


Figure 2. Matter Standard Architecture Pyramid. Credit: GitHub

Device security requirements

Matter promises device-to-device interoperability, which can significantly boost customer confidence by defining a standard for each of the above areas. In terms of device installation and setup, Matter involves a few steps: these include the secure installation of the device to the home network, naming the device, pairing the device with other smart devices within the network and setting up normal operations.

Note that the user can add the device to the smart home network via a simple pairing mechanism supported by Amazon, Apple, Google, and other manufacturers. Moreover, Matter defines application-level messaging, security, as well as data types and formats. Due to Matter-defined standards, smart device manufacturers can incorporate relevant features and user controls into user interface devices such as an Alexa voice-activated speaker, iPhone, and so on (see application section). With its advanced security capabilities, Matter ensures secure over-the-air software updates across all devices in the smart home network.

Put briefly, Matter will ensure the reliable and seamless connectivity between devices in smart home applications. When a customer receives a device designed with the Matter standard, that device will come preloaded with relevant sets of credentials and software that prove its unique certification status. The user can then add this Matter-incorporated device by scanning a QR code with their smartphone and pressing the pair button on

the device. After verifying the initial credentials of the device, the smartphone will then set up the user network. After this, the device comes online and is ready for use, enabling seamless control with a smartphone or any other smart device in the smart home network (for example, a speaker or a smartwatch, smart refrigerator, and so on).

Figure 3 outlines the steps for adding a Matter-incorporated device to a smart home network.

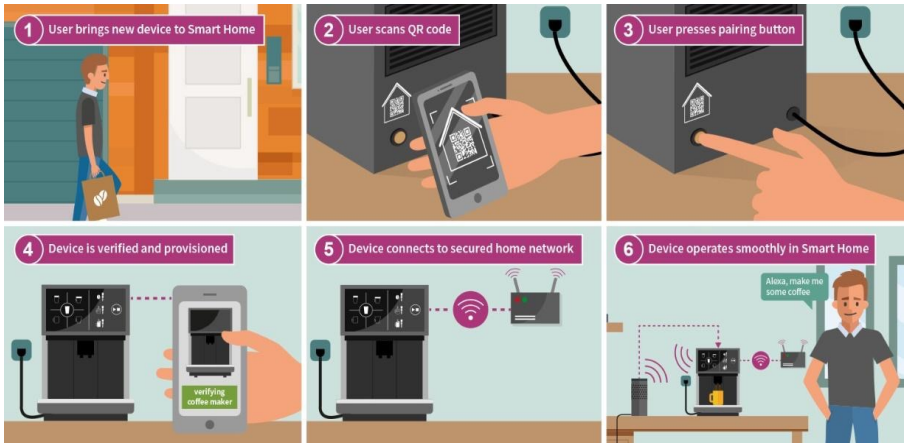


Figure 3. Adding a Matter-incorporated device to a smart home network. Credit: Infineon Technologies

Matter components

Matter deploys its application layer on devices, controllers, and IPv6 (internet protocol version 6)-based networks to enhance the interoperability architectural goal. Moreover, the standard supports Wi-Fi and Thread for core, Bluetooth Low Energy (BLE), and operational communications for device setup and commissioning simplification. The main features of the Matter application layer include the following [4]:

The application, which supports the high order business logic of a device

The data model that describes the functionalities of devices

The interaction model represents a set of actions for interaction with the devices

Action framing, which frames the action initially constructed

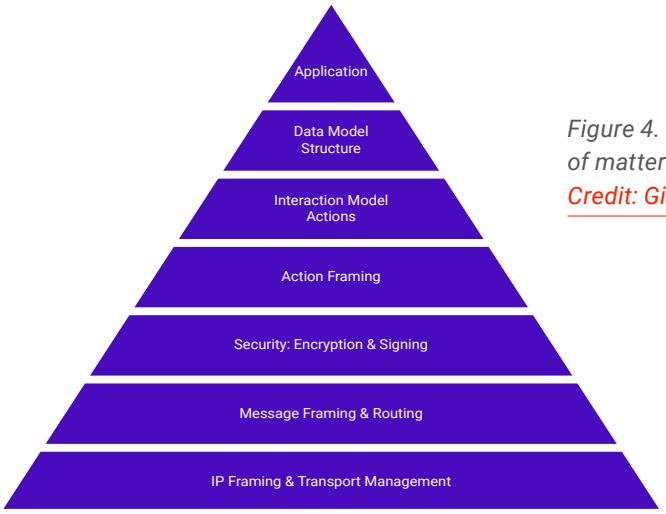


Figure 4. Main components of matter application layer. Credit: GitHub

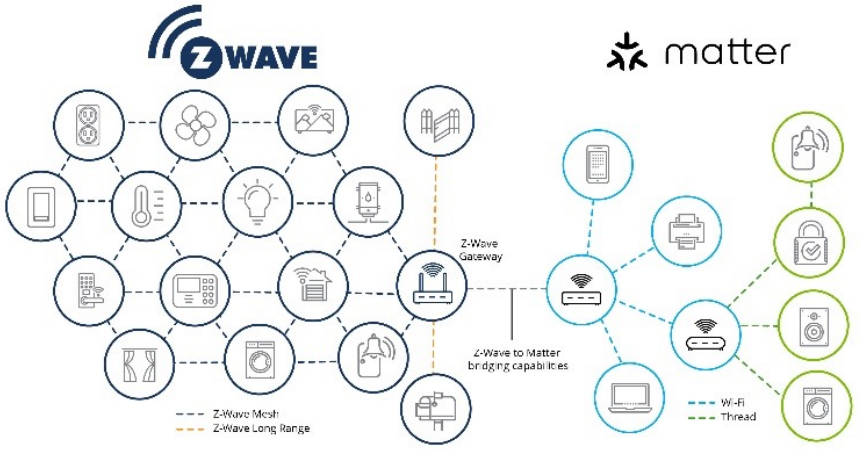


Figure 5. A map that shows how Wi-Fi and Thread devices will connect in a Matter network, as well as how Z-Wave devices could be bridged into the Matter network. Z-Wave (and Zigbee) networks have IP at the gateway level enabling cloud connectivity to Matter. Credit: Z-Wave Alliance

by the interaction model into a prescriptive packed binary format

Security layer that receives the encoded action frame for further encryption, ensuring data security and authentication

Message framing and routing layer for payload format construction and message properties and routing information specification

The IP framing and transport management layer sends the constructed payload to the underlying transport protocol for data IP management

The project has set a goal of a twice-yearly release cycle. Matter 1.1 was released in May 2023 – the updates in 1.1 make it easier for device makers and developers to get started with Matter, and to more easily certify products they've developed and get them to users faster. There is also enhanced support for battery-operated devices which is an important feature across many smart home categories.

Developers interested in learning more about these enhancements can access the software development kit (SDK) on GitHub[4] or download the specifications from the Alliance website[5].

Benefits of Matter

Key benefits that Matter bring to smart home technology include advanced security, universal interoperability, seamless user experiences, reliable connectivity, state-of-the-art control and compute, and intuitive sensing[6].

The development of the Matter standard has experienced the incorporation of a proven, robust, and pervasive security against data and privacy breaches. Moreover, Matter ensures that products from all project members will work seamlessly together, allowing easy control with a preferred system. Matter also enables the co-existence of several low-power wireless solutions to ensure reliable connectivity for the smart home network.

Additionally, this new IoT standard ensures advanced control and computation through low-power, high-performance microcontrollers (MCUs) that utilise human-machine interface (HMI), AI, display, sensing, and security, and ensure intuitive sensing through highly accurate and reliable smart device situational awareness.

Smart home applications

This section looks at some of the Matter-enabled products currently on the market and how some of the biggest brands in consumer electronics have deployed the new technology, which runs on supported IP networks like Wi-Fi and Thread (Figure 5).

Matter's 1.0 version supports a subset (albeit a significant one) of smart home product categories and the features within each. These categories include lightbulbs, light switches, lighting controllers, plugs and outlets, door locks, thermostats and HVAC controllers, blinds and shades, home security sensors, garage door controllers, wireless access points, bridges, televisions, streaming video players, and smart home control devices.

Matter 1.1 enhances support for Intermittently Connected Devices (ICDs). Sometimes called 'sleepy devices,' these are typically battery-powered devices like contact, motion, and temperature sensors as well as door locks and switches that need to conserve power for optimal operation and lifespan. The additional support reduces the likelihood that a device will be reported as offline when users or platforms interact with it.

Smart lighting

Smart lighting is arguably one of the most popular aspects of a smart home, allowing users to dim, brighten and even change the colour of their lights wirelessly.

Smart lighting company WiZ was one of the first to update all its smart bulbs, lamps, and plugs manufactured in early 2021 or later to Matter. The latest version of the company's app, WiZ v2, introduces a convenient feature that allows users to seamlessly transfer any compatible product to the new smart home standard within the app itself. Once migrated, these products can be easily integrated

into any Matter-compatible platform, such as Apple Home.

Philips Hue users will be able to benefit from greater interoperability when the Philips Hue Bridge smart lighting hub is automatically enriched with Matter. The smart lighting hub connects and controls all Philips Hue products, from indoor and outdoor lights to entertainment features, smart accessories, and more. Once Matter has been incorporated, users will benefit from a simplified connected experience when integrating with other smart home devices.

Figure 6. Amazon is bringing Matter to Alexa devices. Credit: Amazon

Smart security

Smart security systems are an integral part of the smart home.

Perhaps one of the most significant announcements in this area comes from Netatmo which announced its first Matter product in 2022: a smart security sensor. Designed to improve home security, the sensor is equipped with a contact sensor and infrared motion detector and can be placed on windows and doors to detect their opening. With Matter and Thread compatibility, the sensor can interact with other connected products around the house regardless of the given brand.

Amazon Alexa

Amazon had previously limited the activation of Matter-over-Wi-Fi to a selection of its smart speakers, and the configuration of a Matter device with Alexa was restricted to Android phones. However, Amazon has expanded its support for Matter by enabling it on all second-generation smart speakers, including the Echo Plus, Echo Dot, and Echo. This brings the total count of Amazon Alexa Matter controllers to 20, providing users with more options for controlling their smart home devices.

Amazon has said that it will extend its Frustration-Free Setup (FFS) to make Matter set up even easier with Alexa. No device side software development kit (SDK) is needed to support Frustration-Free Setup for Matter devices.

Google Nest and Android

Google has brought Matter to its Nest and Android products. Users can control Matter devices instantly via Matter-enabled Android apps, Google Assistant, the Google Home app, Android Power Controls, and compatible Google devices.

Devices with Thread built-in like Nest Wi-Fi, Nest Hub Max and the second-generation Nest Hub will become connection points for Matter devices. All Nest displays and speakers (the Nest Hub and Nest Mini) will automatically update to control Matter devices. This will create stronger and faster connectivity across the smart home and give users a more reliable experience.

Google has also partnered with Samsung to build a smoother Multi-Admin experience. When launching the Google Home app, users will now have the ability to view Matter devices that have been configured using Samsung SmartThings. Users can effortlessly incorporate these devices into the Google Home ecosystem, and vice versa, enabling seamless integration between the two platforms.

Samsung SmartThings

Samsung has unveiled a Matter-certified smart home hub that serves as a central device capable of connecting and configuring multiple smart home devices from various brands.

The Samsung SmartThings Station allows users to connect various devices such as thermostats, lighting fixtures, and power outlets, among others, all from a convenient mobile app. Moreover, the Station hub includes a dedicated button that can be programmed with different tap patterns to activate personalised and specific routines according to the user's preferences.

For Samsung Galaxy device owners, the Station offers an additional benefit of tracking registered products like their phone or a Galaxy SmartTag.

SmartThings is an open platform that brings together devices, developers, and services into a large integrated ecosystem. Matter-enabled devices will join other products and brands already available within the SmartThings' ecosystem, including devices from Google, eve Systems, Honeywell Home by Resideo, Linksys, Nanoleaf, Philips Hue, Schlage, Wemo, and Yale.

Can Matter deliver on its promise?

As this discussion has illustrated, Matter is well on its way to becoming the common language for all smart devices. Despite being delayed three times, the promise of a more safe, reliable, and seamless network for smart devices can now be visualised.

Tobin Richardson, CEO of the Connectivity Standards Alliance (CSA), believes that Matter will signify "the end of walled gardens in the smart home" and "open the field for better experiences by any manufacturer" supported by a global, secure, and open standard for interoperability.

Since the release of Matter 1.0 in October 2022, there have been 17,991 downloads of the specification with 1,135 new products certified by the Alliance. Matter's momentum has resulted in more than 60 members joining the Alliance since the specification's release.

Members are now focused on making Matter easier to use and getting products to market. An Interoperability Testing Facility (ITF) has opened in Portland, Oregon providing interoperability testing services to members of the Alliance. It includes a range of Matter controllers, hubs, and end devices configured to check the most typical sets of devices and installation configurations found in residential settings.

The next version of Matter, with new features and device type support, is expected late 2023.

References:

1. Jasud, Ms. Priti V. The OSI Model: Overview on the Seven Layers of Computer Networks International Journal for Innovative Research in Science & Technology
2. ITU-T X.200 standard International Telecommunications Union
3. Tomsho, Greg. Guide to Networking Essentials, 7th Edition 2016 Cengage Learning
4. Project CHIP, Connected Home IP Github
5. Matter 1.1 Specifications Connectivity Standards Alliance
6. The new revolutionary standard for smart home: Matter Infineon Technologies

5G putting the ‘smart’ in today’s smart homes

Written by:
Sam Holland,
Editor at IoT Insider

5G is a crucial and ever-more prevalent communications technology throughout urban areas, particularly smart cities. Far from simply a boost in smartphone Internet speeds, 5G is purpose-built for on-the-go activities such as location services, augmented reality, and even mission-critical applications like driver assistance systems

What is less well known, however, is that 5G is also suited to smart homes and their applications. As the following sections will discuss, 5G can offer functionality that is similar to that of Wi-Fi, along with even higher reliability and security. This is particularly when compared to the iterations that precede Wi-Fi 6 (namely the most recent version of Wi-Fi that is discussed elsewhere in this ebook).

Defining smart homes in the context of 5G

To detail the benefits of 5G in a smart home, it is important to consider the particular way in which the word 'smart' will be used to consider the value of 5G and its applications. The word 'smart' will be used in this discussion to qualify a level of Internet connectivity that facilitates the reliable interoperation of connected consumer devices. This is to the point that such smart devices can collectively achieve a degree of automation that cannot be supported by traditional Internet-connected homes.

This is vital as it is a flawed notion that a home becomes a smart home as soon as its Internet capabilities have successfully facilitated the use of one or more smart devices, such as voice-activated systems like smart speakers (discussed later). Again, while smart speakers are an increasingly common feature of traditional modern homes, they are not a prerequisite for, or even necessarily a defining characteristic of, a smart home.

With the importance of connectivity, reliability, and automation in mind, this discussion will consider the value of 5G in wearable technologies and other smart devices in smart homes. The next pages will cover 5G's technical specifications before going on to discuss the technology's chief features that facilitate smart device performance, miniaturisation, automation, and more.

5G technical specifications

5G technology offers improved capabilities compared to preceding communications technologies in terms of speed, latency, error rate, and range. With an estimated speed ranging from 50Mbit/s (megabits per second) to over 1,000Mbit/s – in other words 1 gigabits per second – 5G technology has the capacity to be 10 times faster than 4G.

On top of this, 5G offers a theoretical air latency that ranges

from 8 to 10 milliseconds. However, industry leaders such as Verizon have reported a 5G latency of 30 milliseconds during its early deployment. Various observations have identified a reduced 5G latency of 10 to 20 milliseconds close to 5G towers and an increased 5G latency of 50 to 500 milliseconds during handovers.

5G also leverages an adaptive modulation and coding scheme to maintain an ultra-low bit error rate. For low-band, mid-band, and high-band 5G, the estimated ranges are respectively:

- 600 to 900 megahertz
- 1.7 to 4.7 gigahertz
- 24 to 47 gigahertz

The high speeds of 5G do still require a consideration of users' network infrastructure to be best utilised, however. Reflective of this, the next section discusses the concept of 5G network slicing[1].

Network slicing

5G technology has the capability of supporting several smart home

applications, many of which will be covered throughout this discussion. Correspondingly, users are increasingly incorporating a network slicing concept into their smart home systems to achieve the high efficiency and reliability that is required of their interconnected smart devices. 5G network slicing is the process by which a network architecture allows virtual and independent network multiplexing, all within the same physical network infrastructure.

In the context of smart homes, such a use of 5G network slicing ensures that the network slices meet various requirements for specific smart home applications by establishing an isolated end-to-end network. The following paragraphs explore the following:

A generic 5G network slicing framework

A typical 5G network slicing case for a smart home network

To address the former, Figure 1[2] presents an architecture that maps out common elements of different solutions into a unified, generic framework.

The framework comprises two blocks:

A three-tier architecture block, which includes the service layer, network function layer, and infrastructure layer

The network slice controller block, which manages all of the three above-mentioned layers to ensure the efficient coordinated coexistence of multiple slices

The service layer interfaces with 5G network business entities that share the underlying physical network (such entities may be mobile virtual network operators and third-party service providers, for instance), and it also provides appropriate service requirements. The network function layer ensures the development of each network slice in line with the service instance requests from the upper layer. The infrastructure layer, on the other hand, provides the physical network topology required for 5G network multiplexing and the physical network resources needed to host several network functions in each slice.

The following subsection presents a 5G network slicing use case that reflects the capability of 5G to boost the efficiency of smart home systems.

Figure 2[3] illustrates a typical 5G network slicing framework for smart homes.

To meet the security requirements of smart home security systems, engineers specialised in 5G will usually isolate the system into a dedicated end-to-end network slice. Such engineers assign an AUSF (Authentication Server Function) for the system to carry out the device authentication before granting access to a network slice. The network slice for eMBB (enhanced Mobile Broadband) network slice, moreover, ensures the connectivity of high data rate-intensive devices,

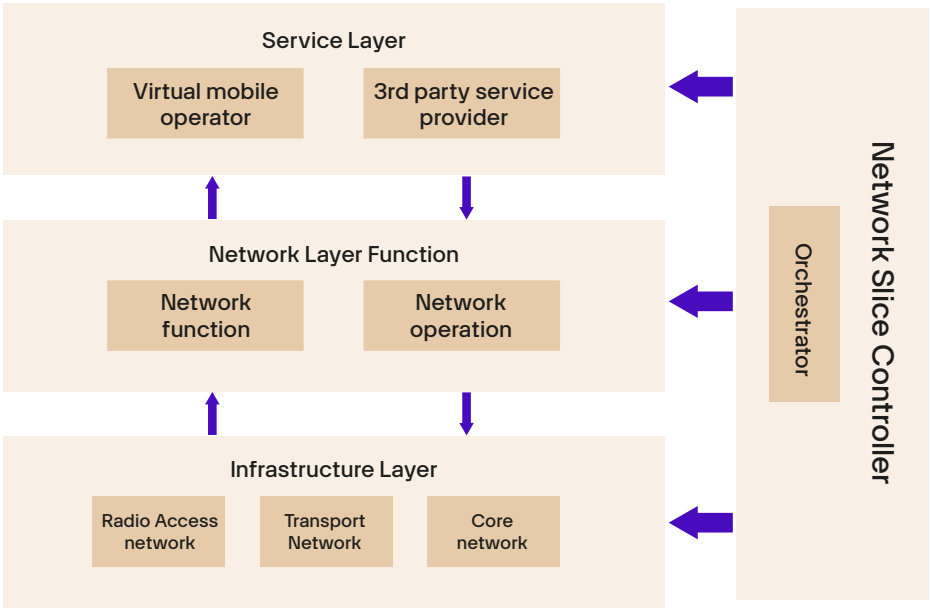


Figure 1. A diagram that covers the generic framework for 5G network slicing. Credit: Foukas et al. (2017)

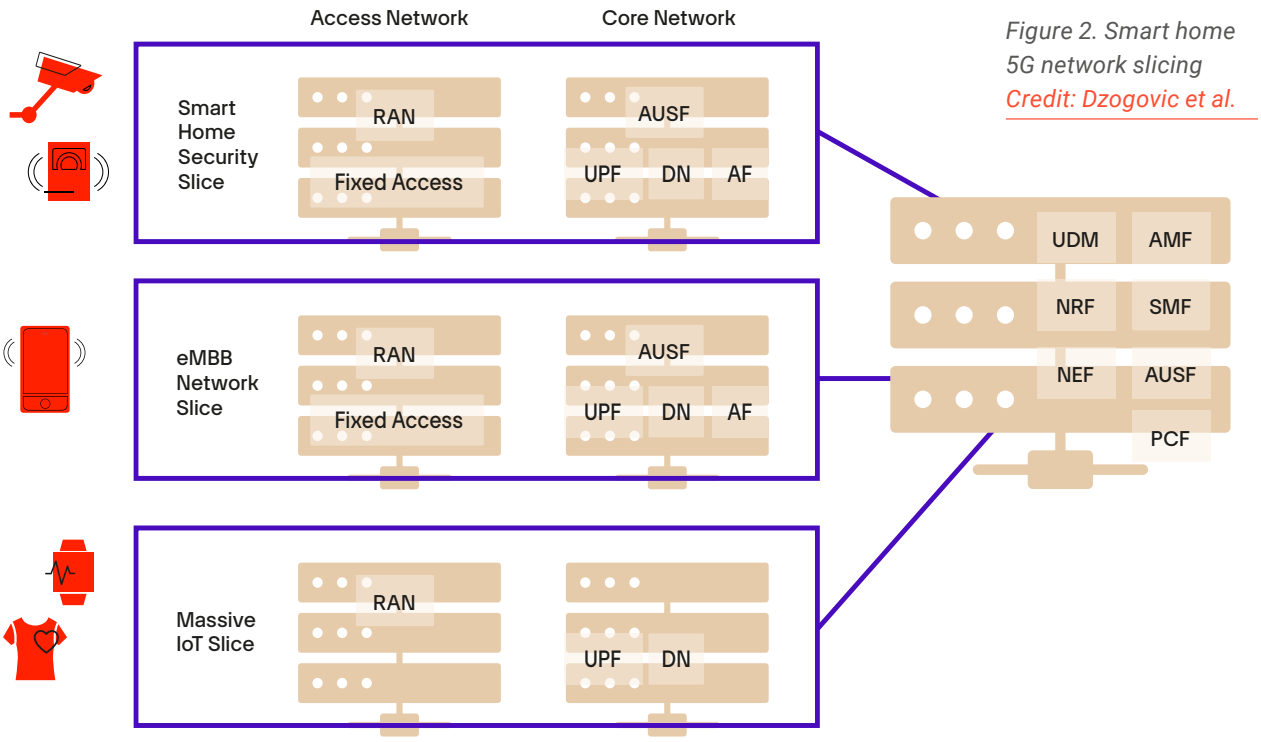


Figure 2. Smart home 5G network slicing
Credit: Dzogovic et al.

including tablets, smartphones, cameras, and laptops.

Users can gain access to this network slice through a single, comprehensive subscription for home and mobile devices for individuals or an entire household. In contrast to eMBB, the Massive IoT network slice ensures lower data rate connectivity for low-power devices, such as sensors (smoke/gas detectors, motion sensors, proximity sensors, and so on), and other home appliances, including coffee machines, washing machines, air conditioners, electric cookers, and refrigerators.

The next section discusses the benefits of 5G's capacity to accommodate both high data rate-intensive and low-power devices.

Benefits of 5G for smart home applications

5G exhibits faster broadband speeds than Wi-Fi 5 and its preceding iterations. It offers a LPWAN (low-power wide-area network), making it suitable for smart home products that rely on reliable and constant connectivity. With its high capacity and wireless infrastructure, the technology respectively allows the connection of more devices than a local network-enabled smart home system and limited reliance on existing wired infrastructure.

5G technology also offers other benefits in a wide range of smart home applications, including improved interoperability, low latency, enhanced encryption, advanced connectivity, increased wearable sensor adoption, and the potential for device miniaturisation (discussed later).

Existing smart home devices face significant challenges[4] in terms of their ability to communicate and interact with each other. Providing a solution to these limitations, 5G offers a unified wireless standard[5], which offers users' smart home ecosystems a significant boost in interoperability. Moreover, the low latency of the technology allows users and stakeholders to see rapid improvements in smart home functions, some of which are covered in the following subsections.

Speed and security in voice-activated smart home systems

In a smart home, 5G-enabled voice-activated systems (such as smart speakers) can receive voice commands from its user and achieve a near-instantaneous response, translating to higher user safety and security. Consider that hackers can exploit the vulnerability of existing smart home systems, particularly when their devices are both connected by and reliant on the 128-bit encryption of 4G.

By offering a security standard with twice as many bits as its predecessor, 5G's 256-bit encryption means that it is far better designed than its latest predecessor for protecting smart home devices from cyber attacks. (Malicious agents will require 2,256 different combinations to break a 256-bit encryption system, which renders the hacking process virtually impossible.)

5G also offers smart speakers, such as Amazon Echos and Google Homes, the ability to expedite the rate at which intelligent virtual assistant (IVA) software, such as Alexa, can respond to a user's spoken commands. Smart speakers, which are connected to traditional Wi-Fi routers, are in increasing use throughout modern (not even necessarily smart) homes. However, they are restricted in terms of their response times. This is owing to how compute-intensive it is for the IVAs' software to digitally process their users' voice data, largely due to the complexity of both human speech patterns and natural language itself.

Currently, smart speaker manufacturers attempt to counteract this challenge by focusing on moving their products' voice processing capabilities from the Cloud to the Edge, but the speed of such a system is still flawed owing to most users' Wi-Fi limitations. When compared to both 4G and Wi-Fi 5, the low latency of 5G has the potential to bring a marked increase in the speed of all manner of voice-controlled systems – not just those in stationary smart speakers, but those in on-the-go interfaces such as the iPhone-based version of Siri.

Healthcare Wearables and Hardware Miniaturisation

5G offers wide-scale connectivity improvements compared to previous networks. Such enhancements from 4G mean that the technology can significantly boost the adoption of smart home systems across several areas. For instance, industry predictions[6] refer to a notable boost in 5G-enabled wearable sensors adoption, which is beneficial for monitoring the wellbeing of users both in and out of the smart home.

5G allows medical personnel to offer effective communication and remote medical assistance to patients in the comfort of their homes. The collective term for devices that enable users to experience a remote or virtual location as if they are physically present in that location is 'telepresence', which will be vital to the accuracy and safety of remote healthcare diagnoses and treatments. Aided by a rise in wearable sensors, 5G may offer the precision needed for telepresence which preceding technologies will not be able to achieve.

5G-enabled Cloud computing is also facilitating the migration of processing power to conventional hardware systems, which is bringing a significant level of miniaturisation to existing devices. This is leading to greater viability for lightweight and compact devices that may ensure a better experience for smart home users. This is particularly important for at-home patients whose wearable sensors would otherwise be uncomfortable and unwieldy.

Considering the future of smart homes

As this discussion has covered, the connectivity, reliability, and accuracy of 5G offer technological benefits that range from network slicing to advancements in medical technology.

These advantages, among many others, mean that there are innumerable smart home capabilities offered by the

fifth generation of cellular communications. The question does arise, however: how will 5G support what are (at the time of writing) only prospective commercial smart devices? To revisit the earlier discussion of defining a smart home, consider once more that the term 'smart' hinges on how much automation is offered by the user's domestic devices.

In view of this, perhaps the future of the 5G-connected smart home will involve commercial home robots that offer users a level of home automation[6] that cannot be realised by even the most efficient smart devices on the market today.

References:

1. Shunliang Zhang. An Overview of Network Slicing for 5G 2019 Institute of Electrical and Electronics Engineers (IEEE)
2. Xenofon Foukas, Georgios Patounas, Ahmed Elmokashfi, Mahesh K. Marina. Network Slicing in 5G: Survey and Challenges 2017 Institute of Electrical and Electronics Engineers (IEEE)
3. Linh-An Phan and Taehong Kim. Breaking Down the Compatibility Problem in Smart Homes: A Dynamically Updatable Gateway Platform 2020 National Library of Medicine
4. Everything you need to know about 5G. Qualcomm
5. 5G, the Internet of Things (IoT) and Wearable Devices GSMA 2019
6. Revolutionizing Wearables for 5G: 5G Technologies: Recent Developments and Future Perspectives for Wearable Devices and Antennas 2017 Institute of Electrical and Electronics Engineers (IEEE)

Is Ultra-Wideband (UWB) the next big wireless technology for smart homes?

Written by:
Paige West,
Editor at Electronic Specifier

The absence of highly accurate indoor location technologies is currently hindering the smart home from becoming truly interconnected and fully automated [1]. Ultra-wideband (or UWB) has the potential to solve this problem – it is a fast, secure, and low power radio technology used to determine location with precise accuracy.

UWB is not a new technology (Figure 1): it was originally used for military radar applications but for various reasons, such as power restrictions, it was unable to succeed.

However, it has recently re-emerged and since 2019, UWB has evolved and expanded into mainstream consumer technology. With the help of organisations like the UWB Alliance and the FiRa Consortium, who are dedicated to the promotion and growth of the technology, it has been predicted that by 2025 there will be over one billion annual device shipments of UWB technology [1].

Due to its high-accuracy, reliability, and robustness, UWB can offer a much more seamless, automated and personalised experience within the smart home which will be the focus for the remainder of this article.

How UWB works

One key difference between conventional radio transmissions and UWB is the nature of information transmission. Conventional systems transmit information by varying several elements, including the phase of a sinusoidal wave, power levels, and frequency. UWB-based transmissions, on the other hand, generate radio energy at specific time intervals, occupy large bandwidths, and enable time modulation or pulse position. UWB can also encode pulse polarity and amplitude or use orthogonal pulses to transmit information. Industry leaders are increasingly incorporating this technology into several devices for a wide range of applications, including security, patient monitoring, entertainment, and general smart

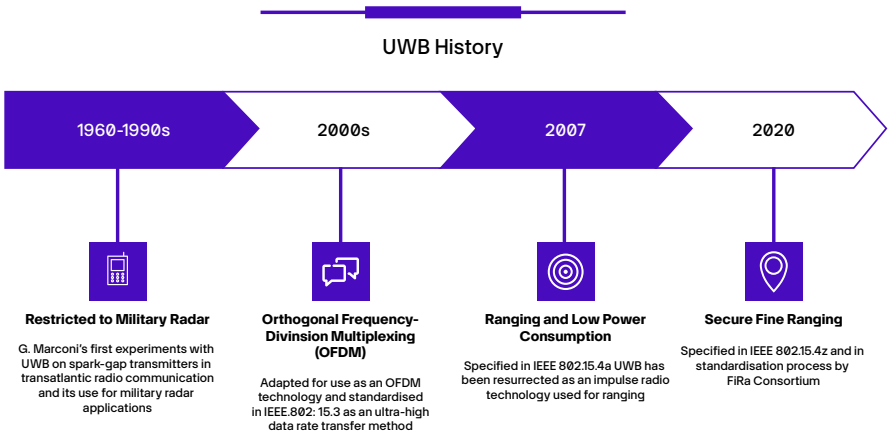


Figure 1: The history of UWB. Credit: ABI Research

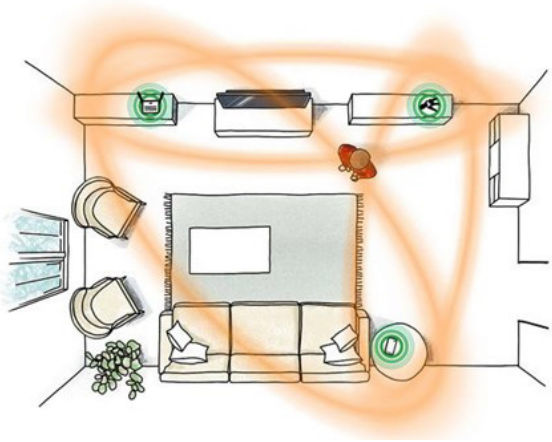


Figure 2: Schematic for UWB Radio-Equipped Devices for Smart Home Applications.
Credit: Ledergerber & D'Andrea (2020)

home applications [2], e.g., light and temperature monitoring and control (see applications section).

To further consider monitoring applications, UWB radio-equipped devices can track movements within their surroundings by detecting channel impulse response changes of each communication channel and intersecting their corresponding multi-static radar network.

Figure 2 presents a conceptualised UWB-based monitoring application.

Designers of this simplified UWB-based system achieved adequate motion tracking by ensuring the UWB radio-equipped devices could carry out the following:

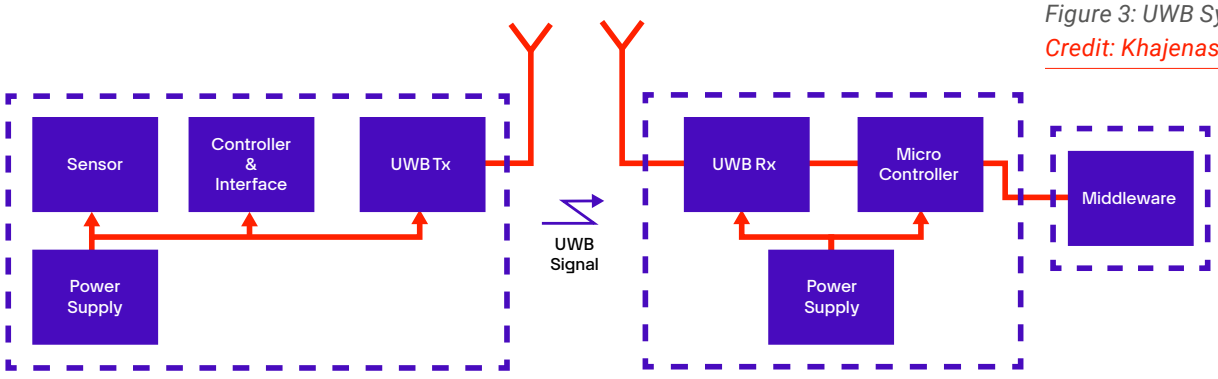
- localise themselves to each other
- track the changes in the channel impulse response of each communication channel
- fuse each observed change into a position estimate of a nearby person

To further explore the working principles of a UWB-equipped smart home system, the remainder of this section explores a use case: one that incorporates a low-energy UWB sensor node software and hardware design into room temperature monitoring. Figure 3 presents a typical UWB system architecture and refers (left to right) to the UWB signal transmitter and receiver within the sensor node and the control system, respectively.

To summarise the working principle of the UWB system architecture, the sensor node converts the physical information, e.g., room temperature, to digital bits, modulates it in the UWB pulse generator, and transmits it through the UWB antenna. The energy detection receiver then demodulates the received data and uploads it to the middleware at the receiver side, ensuring adequate temperature monitoring in smart homes. Since users prefer to access environmental parameters measured by the sensor nodes through a hardware-independent interface in smart home applications, this use case incorporates a software infrastructure. Figure 4 presents the software framework.

The image to the left shows the software infrastructure layout, while the right represents the measured temperature layout. A dedicated interface of the software framework receives all the information coming from the wireless sensor nodes (WSNs). Relevant information (i.e., temperature measurement) remains available for the end-user to view and manage in the application-client layer of the framework. This UWB-enabled software-hardware integration aids the deployment

Figure 3: UWB System Architecture.
Credit: Khajenasiri et al. (2014)



of adequate solutions for overall energy management in smart homes, depending on customer requirements.

Other smart home applications will be explored later in this article.

Table 1 compares some existing wireless connection standards, alongside UWB. The table shows that UWB offers the lowest energy per bit and the highest maximum bit rate. Moreover, UWB is widely associated with high data rates, low power consumption, and wide bandwidth. Other key characteristics of the ultra-wideband technology include large channel capacity, carrier-free signalling, innovative modulation techniques, and resistance to multipath fading and jamming [3].

Technical specifications of UWB

Standard	Energy per bit (nJ/bit)	Maximum bit rate (Mb/s)	Maximum range (m)
ZigBee	296	0.25	75
Bluetooth	34	1	15
Wi-Fi	130	54	100
UWB	5	100	10

Table 1: Comparison of Various Wireless Standards. Credit: Khajenasiri et al. (2015)

Large channel capacity

The US Federal Communications Commission (FCC) describes any signal with a bandwidth of over 500MHz as an ultra-wideband signal. The independence of the large channel capacity of UBW signals on the signal-to-noise ratio (SNR) allows them to thrive in noisy environments.

Carrier-free signal

The capability of UWB technology to directly modulate data in the form of pulses during transmission significantly minimises hardware requirements for incorporating this technology into smart home systems. Moreover, this capability results in lower implementation costs given that UWB does not require advanced equipment such as equalisers, frequency mixers, shaping filters, and digital to analogue converters.

Modulation techniques

UWB uses Pulse Position Modulation (PPM), Code-Division Multiple Access (CDMA), and Orthogonal Frequency Division Multiplexing (OFDM) techniques to create pulses and minimise interference in UWB signals. While PPM shifts the pulses in the time domain to result in small time duration pulses (approximately 1ns), CDMA and OFDMA prevent the possible interception of signals by nearby users and eliminate signal interference, respectively.

Resistance to multipath fading and jamming

The wide bandwidth of a UWB signal makes it resistant to multipath fading, which is a common occurrence in narrowband signals. Moreover, unlike narrowband signals that jamming devices can easily block, these devices cannot completely block UWB signals.

Benefits of UWB

UWB is beneficial in smart home applications for access control, real-time location systems (RTLS), device tracking, indoor navigation, point-and-trigger control, etc [4].

UWB can track the exact locations of smart home users when they enter or exit their homes, allowing them instant and hands-free access after verifying their security credentials. This wireless tracking capability of the technology makes it ideal for access control in smart home systems.

Incorporating UWB technology into smart home systems allows

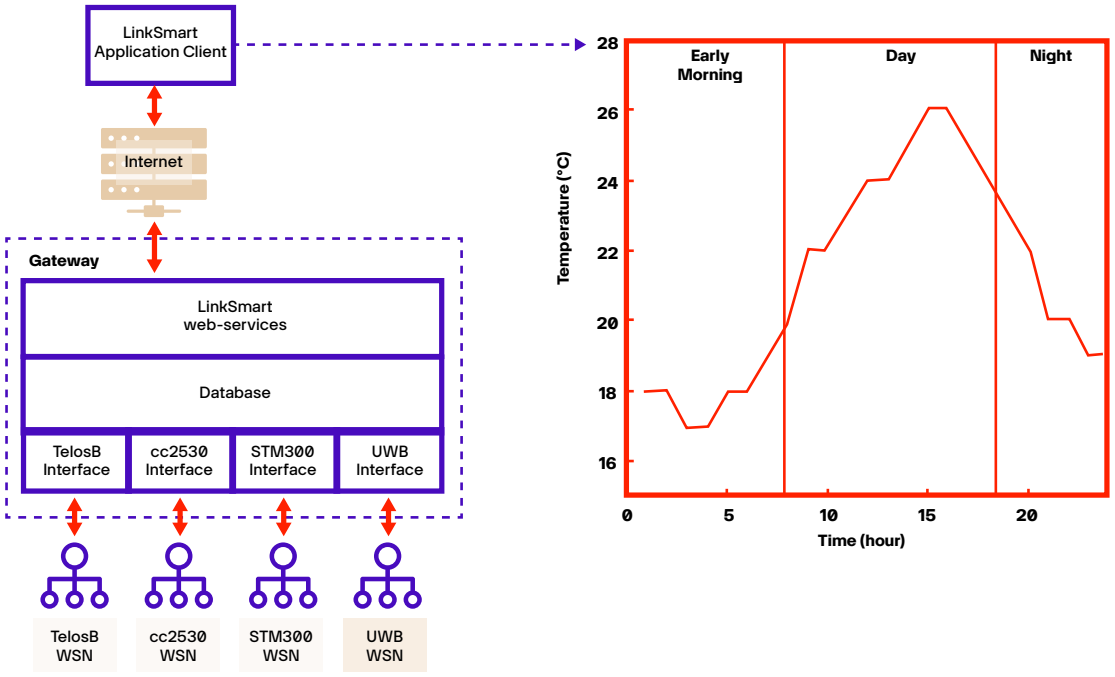


Figure 4: Software Framework for the UWB Temperature Monitoring Application. Credit: Khajenasiri et al. (2014)

caregivers to track patient movements within their homes through a Real-Time Locating System (RTLS). This application is possible due to the capability of UWB to deliver centimetre-level location accuracy, ultra-low latency, and robustness in harsh environments.

Users can also track personal items by incorporating a UWB tag into them (see application section). This technology offers higher accuracy, directional, and lower latency positioning than other alternatives, such as the Bluetooth Low Energy (BLE) solution, which has a significant dominance in this space. Moreover, designers can integrate UWB and BLE solutions into a single personal tracking device for initial pairing and handover.

The capability of UWB to provide accurate positioning within buildings and exceptional performance in non-line-of-sight scenarios makes it ideal for indoor smart home navigation. Although voice-activated commands are the de-facto standard for simple tasks, several home automation and control tasks are hard to describe. However, with the high accuracy and direction capabilities of UWB signals, users can use smartphones to detect the specific smart home device or appliance and perform specific operations using the relevant control panel in the smartphone display. This 'point-and-trigger' functionality is ideal for turning off and on a TV, changing radio stations, turning up the thermostat, casting audio or video from a smartphone to the TV or speaker, selecting the colour or brightness of a smart light bulb, etc.

Figure 5: UWB for Point-and-Trigger Control. Credit: NXP

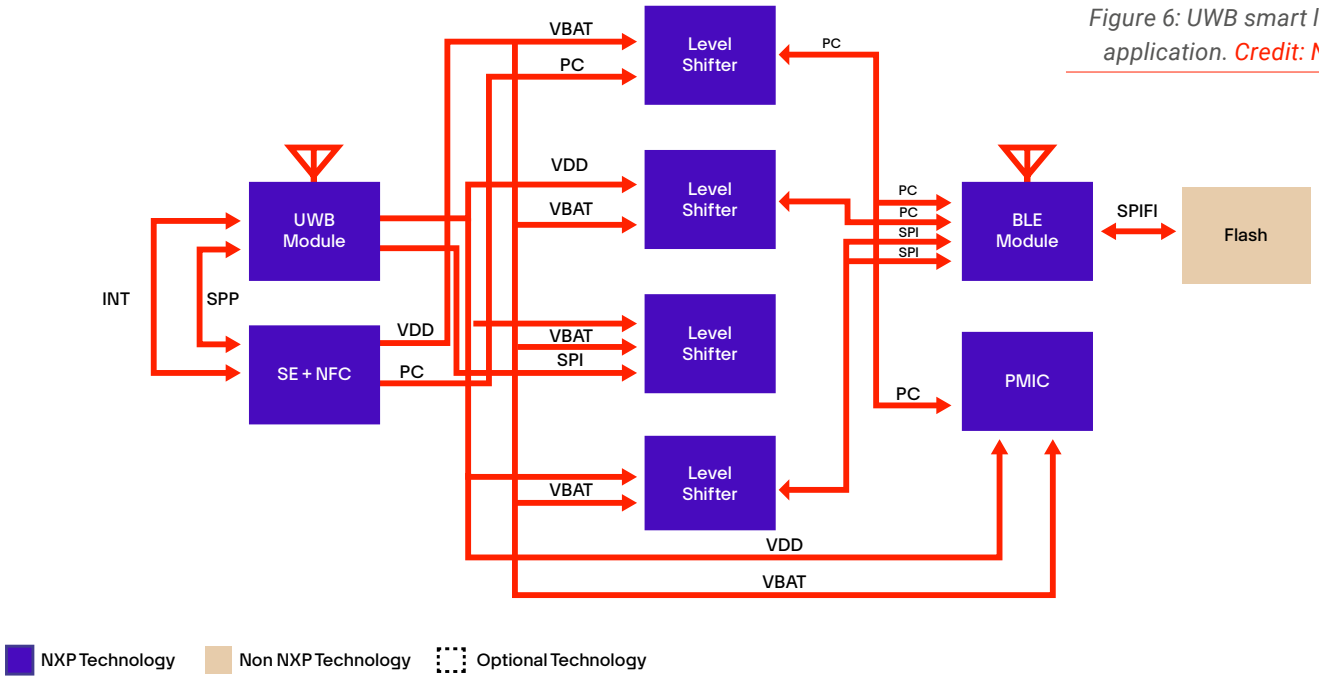


Figure 6: UWB smart lock application. Credit: NXP

Smart home applications

Charlie Zhang, Board Chair of the FiRa Consortium and Senior Vice President, Engineering, Samsung Research America, sees many exciting new applications that can benefit from UWB technology, and this section explores some of the most promising in more detail – namely, residential access control and the tracking of personal devices, as mentioned in the previous segment.

Smart lock

Physical and information security is a growing concern in the connected world. Smart locks are one piece of the puzzle in controlling access to both information and physical spaces.

A smart lock can use UWB to communicate with a user's smartphone, adding an additional layer of security, and interactions can range from something as simple as status LEDs to LCD panels with touchscreen control.

NXP provide a variety of connectivity options like UWB and supply analogue components to complete the design of the smart lock (Figure 6).

Smart keys

Digital car keys allow users to unlock/lock their car door or start the engine using a smartphone.

LG Innotek has developed a digital car key module that utilises UWB technology. The digital key can detect the location of a smartphone five times more precisely than existing key modules. The module's error range between the actual smartphone's location and the recognition location has been reduced from 50cm to under 10cm.

The more precisely a digital car key module detects the location of a smartphone, the more diverse and more convenient functions can be implemented.

A similar application has been developed by Bosch: its perfectly keyless system, based on UWB technology, has a 20cm localisation accuracy and, similarly to the

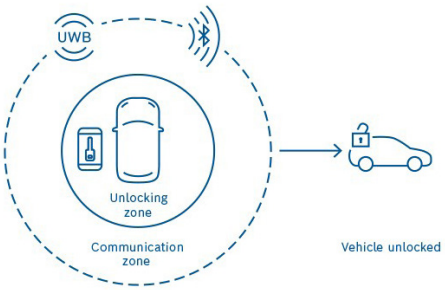


Figure 7: Perfectly keyless system uses UWB technology to automatically unlock a car. Credit: Bosch

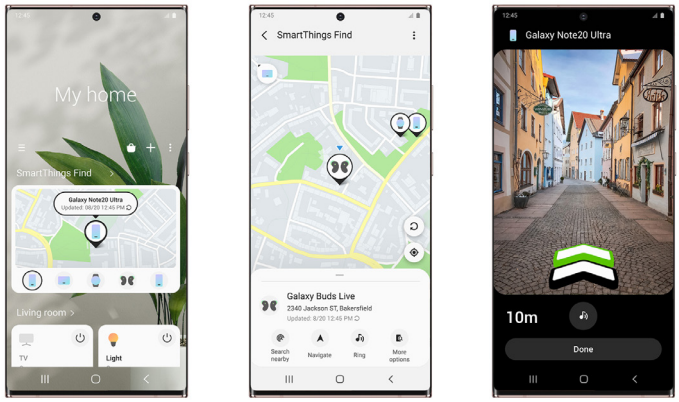


Figure 8: SmartThings Find uses Bluetooth Low Energy (BLE) and ultra-wideband (UWB) technologies to help people find select Galaxy smartphones, tablets, smartwatches and earbuds. Credit: Samsung

above, can unlock the user's car automatically as they approach, start the engine, and even guide users to their car in large parking areas. The smartphone only connects with the digital system when it is within the communication range of the vehicle (Figure 7).

Smartphone

Smartphones are set to lead the UWB market [1]. The first company to apply the technology was Apple, which integrated UWB into its U1 chip for the iPhone 11 in September 2019.

The technology can also be found in Apple's AirDrop. With AirDrop, UWB provides spatial awareness capabilities, enabling two UWB-enabled iPhones (or other devices in the future) to register that they are pointed at each other, allowing for wireless data transfer. Apple is also expected to release UWB-enabled personal trackers, AirTags, which will allow users to locate lost items with an UWB-enabled iPhone.

Now switching to Android applications, Samsung's Galaxy Note20 Ultra features UWB technology. The smartphone contains NXP's Secure UWB fine-ranging solution, bringing users powerful tools to help maximise their time and simplify their daily routines.

UWB is also enhancing Samsung's Nearby Share app for device-to-device file transfers. Users simply need to point their phone at another UWB-equipped device and Nearby Share automatically lists that device at the top of their sharing panel.

Samsung has also integrated UWB into its SmartThings Find application (Figure 8) which uses augmented reality (AR) to show users the exact direction, distance, and location of other UWB-equipped devices. For example, the Galaxy SmartTag+ is currently being equipped with UWB technology so it can pinpoint the location of items such as bags, keys, and purses with greater accuracy.

Smart sensing

One of UWB's unique aspects is that is can be used in radar type functions. NOVELDA, developer of the world's most accurate and reliable human presence sensor, released a UWB sensor for the smart home that uses impulse radar to give any device the ability to accurately sense human presence.

By detecting the tiny movements humans make when we breathe, the sensor can detect human presence even if subjects are lying under a duvet or wearing layers of clothing.

This level of presence detection will provide more accurate touch-free interaction with smart home devices such as touchless-screen displays, lighting, HVAC control and wireless health monitors.

The future of UWB

As this discussion has highlighted, UWB is ideally suited for the high-precision ranging, low power consumption, high data rates and wide bandwidth requirements for next generation consumer electronic devices and smart home appliances.

However, whilst the technology is

not new, consumer awareness is still lacking. This need for greater awareness is just one of many hurdles the technology still needs to overcome – others include standardisation, interoperability and widespread chipset and device availability.

Having said that, UWB is on its way to becoming the next big wireless technology for smart homes.

A major milestone was reached in August 2020 with the publication of the next-gen IEEE 802.15.4z UWB standard. The standard saw improvements in ranging integrity and multiple other technical advances with updates to the High Rate PRF (HRP), and Low Rate PRF (LRP) UWB PHY Physical layers, as well as the MAC layer clauses in the IEEE 802.15.4 standard.

2021 saw the FiRa Consortium launch the initial phase of its certification programme. The programme is the first to provide baseline testing and certification focused on UWB's pinpoint location and spacing capabilities, one of the key steps needed to facilitate interoperability of devices. The first products were certified at the end of 2021 and many more are expected to be certified over the coming years.

In 2022, SPARK Microsystems, a Canadian fabless semiconductor company specialising in next-generation UWB, and the UWB Alliance, an international non-profit organisation dedicated to the promotion and growth of the UWB industry, initiated a joint effort to test the coexistence and aggregation capabilities of UWB technology in environments where other UWB or other wireless protocols and radio devices are in use. Preliminary results of phase one with multiple UWB devices indicate generally good coexistence performance, with the tested devices showing no measurable performance impact from other interfering UWB devices.

In summary, it has been noted by Zhang that "UWB is fast becoming a pillar of wireless local connectivity technology alongside Wi-Fi and Bluetooth" and it has been predicted that UWB's adoption within smartphones and vehicles will be a catalyst for large scale adoption across a range of IoT applications [1].

References:

1. Zignani, Andrew; Tomsett, Stephanie. Ultra-Wideband (UWB) For The IoT - A Fine Ranging Revolution ABI Research
2. Iman Khajenasiri; Peng Zhu; Marian Verhelst; Georges Gielen Low-energy UWB transceiver implementation for smart home energy management Institute of Electrical and Electronics Engineers (IEEE)
3. P.S, Sharma; Vijay Sandeep; Shukla, Manoj. Ultra-Wideband Technology: Standards, Characteristics, Applications Research Gate August 2020
4. Zignani, Andrew How UWB Expands Into the IoT - Where We Stand Today NXP Semiconductors

Wi-Fi 6: Offering smart connections to smart homes

Written by:
Sam Holland,
Editor at IoT Insider

Wi-Fi 6 is the name given to the IEEE (Institute of Electrical and Electronics Engineers) standard known as 802.11ax, and it follows Wi-Fi 5 (IEEE 802.11ac). Due largely to its hardware offering much higher efficiency than its preceding iterations, Wi-Fi 6 is equipped to benefit and optimise smart homes in ways that can only be achieved with the 802.11ax standard.

This discussion considers both the technical specifications and benefits of Wi-Fi 6 in the context of smart homes.

Wi-Fi 6 hardware

To consider the principles of Wi-Fi 6 in smart homes, it is necessary to explore the overall design of a Wi-Fi-connected smart home system. The Institute of Physics-published journal 'The Application of Wifi Technology in Smart Home'[1] identifies the key elements of a Wi-Fi connected smart home system:

- A central processing unit (CPU)
- A smartphone that serves as a carrier control terminal
- An intelligent control system
- The Wi-Fi module

The intelligent control system comprises an audio-visual equipment control system, home lighting intelligent control system, home appliances intelligent control system, and an Android smartphone system, which work together to ensure the proper functioning of the smart home. The intelligent control system sends control commands to the CPU using a Wi-Fi 6 network. After receiving the command, the CPU parses it to perform several functions in the smart home, including setting the air conditioner, switching on and off lights, controlling doors and windows, and so on.

In addition, users can utilise the Wi-Fi-connected smartphone to gain access to the real-time data provided by the CPU about the smart home system. Designers incorporate a CPU, Wi-Fi 6 module, and a control terminal into the smart home design.

The control terminal, which includes the smartphone, transmits information to the Wi-Fi 6 module connected to a similar network through Wi-Fi 6. The module then

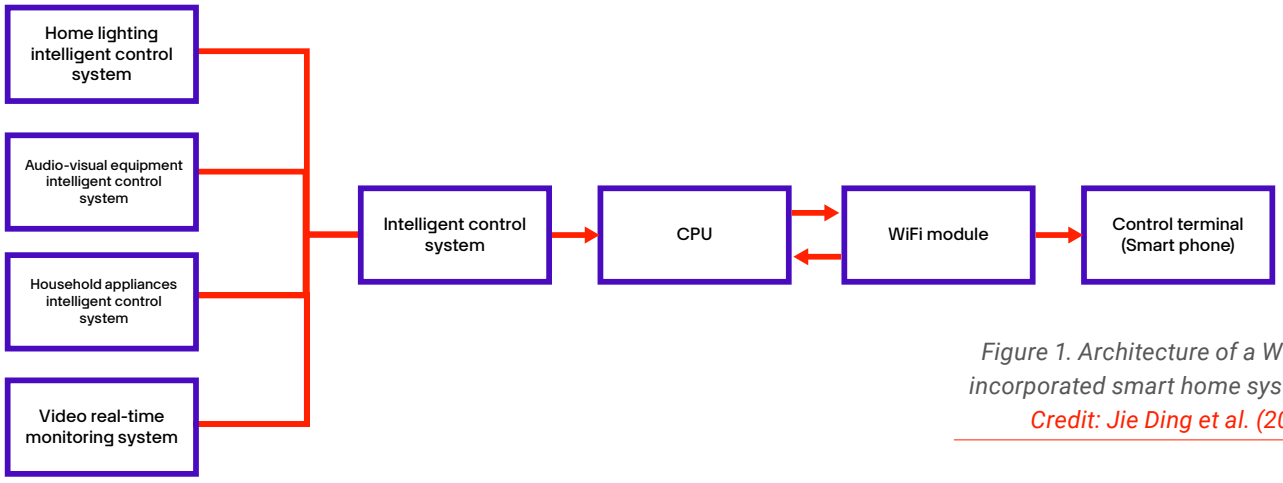


Figure 1. Architecture of a Wi-Fi-incorporated smart home system
Credit: Jie Ding et al. (2018)

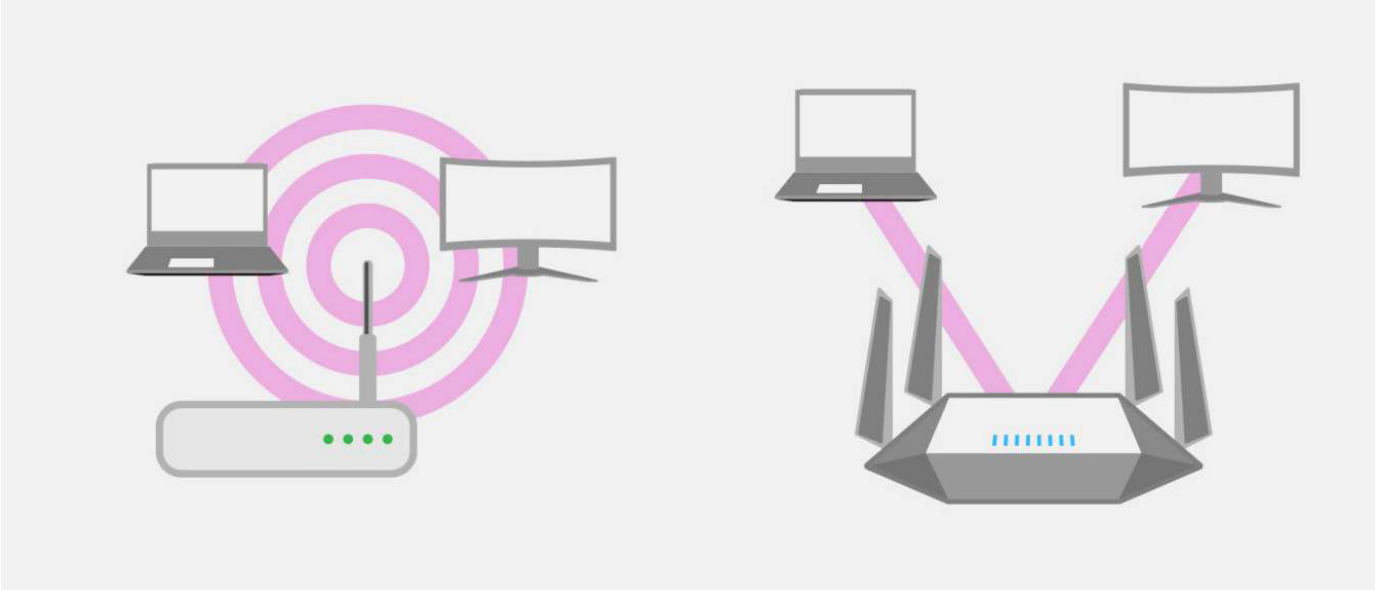


Figure 2. A diagram of the beamforming process achieved by Wi-Fi 6 (right) in comparison to a standard Wi-Fi connection that does not use beamforming (left) Credit: Intel

transmits this incoming signal to the CPU through a serial port. The CPU assumes control over the smart home appliances in line with the smartphone-initiated incoming instructions. From all indications, Wi-Fi remains an essential element of the overall process of the smart home system. Figure 1 presents the structure of an example of a Wi-Fi-connected smart home system.

The primary role of the CPU includes communicating with the host computer to collect and analyse real-time instructions from the smartphone and use such instructions to carry out relevant operations.

In addition to providing power for the Wi-Fi 6 wireless module, the CPU also ensures effective communication with the module through the serial port. Depending on the designer's chosen Wi-Fi module within the smart home system, users may enjoy high-frequency applications with a high likelihood of extending to 5G dual-band and LTE (Long Term Evolution) data module applications, which can dramatically improve the performance and memory, as well as radiofrequency optimisations.

Technical details of Wi-Fi 6

Unlike Wi-Fi 5 and older versions of the technology, Wi-Fi 6 exhibits several improvements to wireless connectivity, making it ideal for the increasingly demanding requirements of smart home applications. This section explores several technical specifications of the Wi-Fi 6 technology.

QAM, OBSS management, and beamforming for improved quality of service

Wi-Fi 6 offers a dense QAM (quadrature amplitude modulation) of up to 1,024, which translates to improved throughput and enhanced capacity for various applications in both smart homes and smart buildings. This capability allows the encoding of more data bits and offers the Wi-Fi 6 wireless access point a 25% increase in data when compared to Wi-Fi 5. The 1,024 QAM specification of Wi-Fi 6 enables the technology to offer improved quality of service (or QoS) in densely populated locations, such as stadiums, convention centres, transportation hubs, and auditoriums.

Other technical specifications of

the Wi-Fi 6 technology include high speeds of up to 9.6 gigabytes per second, 75% less latency than Wi-Fi 5, and a high integration of wired and wireless signals. Similarly, the OBSS management feature of Wi-Fi 6 is able to minimise network congestion (OBSS stands for overlapping basic service sets, which is when neighbouring access points interfere with each other and affect the performance of the given wireless local area network, or WLAN).

Unlike older versions of Wi-Fi technology that wait for a clear channel before transmitting, the Wi-Fi 6 technology can identify and ignore noise within the local network and enable continued signal transmission. The combination of OBSS and OFDMA (discussed in the next section) features in Wi-Fi 6 offers the technology high efficiency for effective communication in crowded networks.

Additionally, conventional Wi-Fi routers send wireless signals in all directions. However, Wi-Fi 6 offers a beamforming feature, which allows its router to efficiently detect the location of a device requesting data and transmits a more localised data stream in the direction of the device. With an improved Wi-Fi Protected Access 3 (WPA3) security protocol and an added Dragonfly Key Exchange system (or SAE – Simultaneous Authentication of Equals), Wi-Fi 6 offers the highest and most robust security option ever.

On top of this, Wi-Fi 6's target wake time (TWT) feature allows Wi-Fi 6 technology to increase the device's battery life. Devices can spend less time and energy searching for a wireless signal through the TWT feature that allows Wi-Fi 6 routers to effectively communicate with the Wi-Fi radio of the devices and only activate it when it needs to be awake.

OFDMA and MU-MIMO for multiplexing and bi-directional connections

Wi-Fi 6 has the ability to connect to devices with better efficiency than its predecessors. This is chiefly due to Wi-Fi 6's ability to carry 12 spatial streams (also known as data streams), on the two frequency bands: 2.4GHz and 5GHz (this is known as a dual-band configuration).

In contrast, Wi-Fi 6's closest counterpart, Wi-Fi 5, has a limit of eight spatial streams. Such streams are independent streams of data that travel between a transmitter and a receiver. 802.11ax's capacity to carry multiple spatial streams is a product of its two core features: OFDMA (orthogonal frequency-division multiple access) and MU-MIMO (multi-user, multiple-input, multiple-output).

The IEEE defines OFDMA and MU-MIMO as respectively "a modulation scheme that converts a high-rate data stream into a number of low-rate streams that are transmitted on parallel subcarriers [secondary modulated signal frequencies within the primary frequency, i.e. carrier]"[2]; and the system by which "a set of … wireless stations [access points] forms a user group and uses different spatial streams for simultaneous transmission and reception"[3].

OFDMA grants Wi-Fi 6 unprecedented throughput for multi-device, bi-directional connections across the given smart home network; moreover, MU-MIMO allows the optimal use of both Wi-Fi 6 routers as well as Wi-Fi 6-enabled smart devices. Both MU-MIMO and OFDMA therefore facilitate Wi-Fi 6's capacity for multiplexing (discussed below), which is the networking technique that allows multiple analogue and digital signals to be transmitted over a shared connection.

Multiplexing and its benefits to smart homes

Naturally, if too many connected devices are introduced to any Wi-Fi network, the data speed of each product slows as a result. Wi-Fi 6 is designed to combat this problem by offering, not only four more spatial streams than Wi-Fi 5, but both downlink (router to device) and uplink (device to router) multiplexing.

This is in contrast to Wi-Fi 5, which despite being the first Wi-Fi iteration to offer MU-MIMO, offers a downlink connection only. This means that Wi-Fi 5 routers can only send more than one stream simultaneously to multiple users' devices (e.g. laptops) – but such devices cannot transmit multiple streams to routers.

In other words, Wi-Fi 6, by being the first Wi-Fi standard[2] to offer an uplink connection, offers bi-directional connectivity between routers and devices, therefore allowing more reliable multiplexing than that of previous iterations. Such an advancement in communications efficiency opens the door to advancements in smart home safety and security applications.

This is especially in terms of connected sensors, which are integral to the data collection capabilities offered by smart homes. For instance, in the 2021 paper 'Design and Implementation of Low-Cost Smart Home System with Sensor Multiplexing'[4], the researchers explain how the detection of hazards (such as dangerous gases and intruders) in the smart home can be carried out using their "extendable, cheap, and multi-faceted" sensor multiplexing system. The researchers explain that the sensors' data can be efficiently uploaded to an IoT cloud platform and go on to consider Wi-Fi for remote observance a "major development" in home automation systems.

By offering the benefits of both OFDMA and MU-MIMO, Wi-Fi 6 has the potential to prove integral to further research and development into the use of multiplexing within smart home automation and security systems.

The next section explores further efficiency and security benefits of Wi-Fi 6.

Further efficiency and security benefits of Wi-Fi 6

The technical specifications of the Wi-Fi 6 technology make it beneficial to a plethora of smart home applications. For instance, Wi-Fi 6's said OBSS feature (namely BSS [basic service sets] colouring) minimises interference within the wireless network from a neighbour's router by ignoring unwanted signals, allowing for a more efficient smart home system.

Another key benefit of Wi-Fi 6-connected smart home systems is its improved WPA3 256-bit encryption security technology that gives users a higher feeling of security. The WPA3 (Wi-Fi Protected Access 3) security protocol enhances Wi-Fi security for home users, therefore providing them with a similar connection

Figure 3. A diagram that shows a reduction in overlapping basic service set interference with Wi-Fi 6's BSS colouring feature. Credit: tp-link

experience to that of previous technologies but with the SAE (Simultaneous Authentication of Equals) protocol exchange, which protects user passphrases from brute-force 'dictionary attacks'.

Taking stock of the smart home benefits and applications of Wi-Fi 6

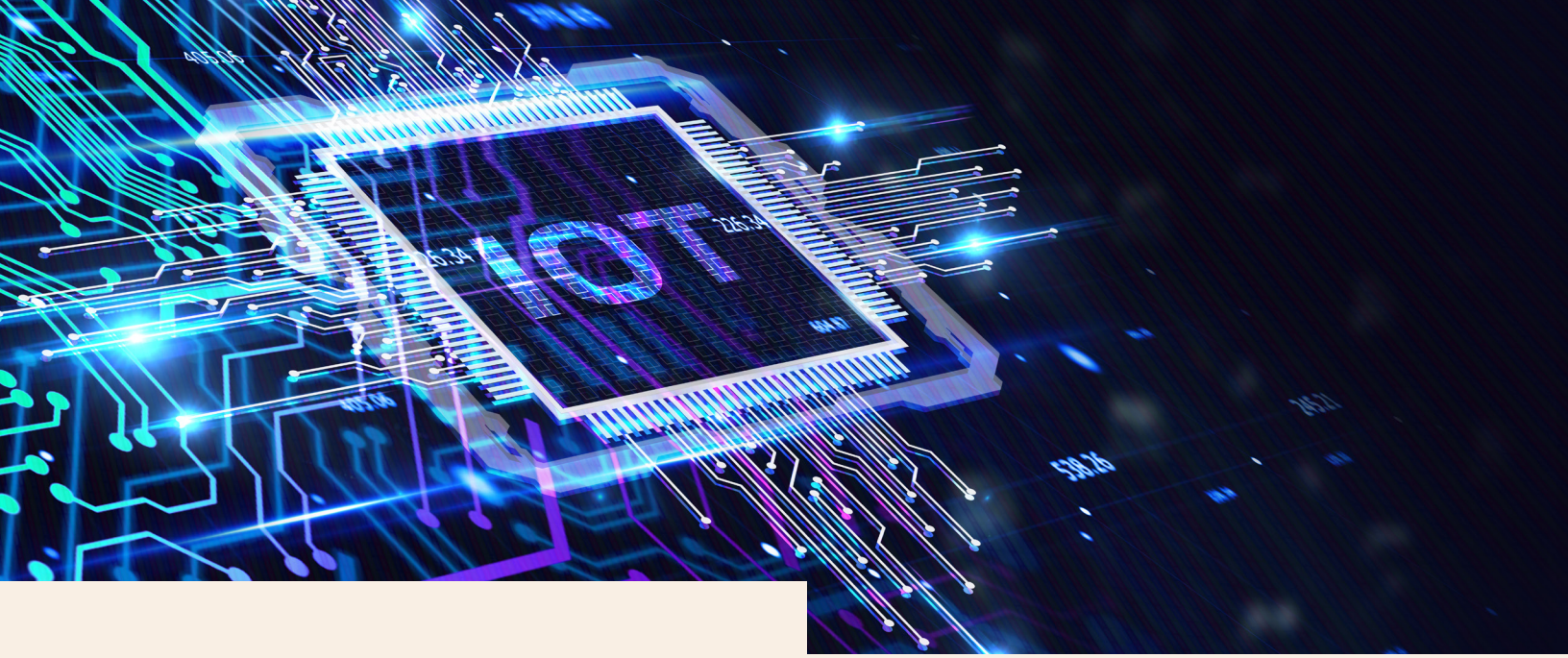
Ultimately, Wi-Fi 6 offers the following benefits and more:

- Faster Wi-Fi speeds
- The higher capacity needed to handle more smart devices, higher data rates, and increased stability and efficiency
- Higher bandwidth of up to 160MHz
- Minimised latency and reduced power consumption (particularly owing to Wi-Fi 6's target wake time capability)

These improvements from its predecessor make Wi-Fi 6's capabilities ideal for demanding smart home systems and even offer a platform for further research and development into revolutionary domestic safety technologies, such as connected home security sensors, data encryption, and much more.

References:

1. Jie Ding et al. The Application of Wifi Technology in Smart Home IOP Science 2018
2. Orthogonal Frequency Division Multiplexing (OFDM) Institute of Electrical and Electronics Engineers (IEEE)
3. Raja Karmakar; Samiran Chattopadhyay; Sandip Chakraborty. Intelligent MU-MIMO User Selection With Dynamic Link Adaptation in IEEE 802.11ax Institute of Electrical and Electronics Engineers (IEEE)
4. Wi-Fi CERTIFIED 6™ Release 2 adds new features for advanced Wi-Fi® applications Wi-Fi Alliance January 2022
5. S. Nagendram, P. Kanakaraja, M. S. R. KiranNag & K. Akhil. Design and Implementation of Low-Cost Smart Home System with Sensor Multiplexing Springer Link 2021



How to use multiband embedded antennas in IoT designs

Contributed By:
Steven Keeping,
Contributing Author, Digikey

Antenna design can make or break a wireless product. The challenge is even greater for an increasingly diverse array of wireless Internet of Things (IoT) designs where regulations limit the transmit power in the allocated frequency bands, even as the engineer strives to maximise throughput and range.

Conventional design guidelines advise strip antennas with a length of half the wavelength of the signal it is intended to receive. For a dipole antenna, this translates to 6.25cm for the 2.4GHz frequency band. But for wireless IoT products, this design advice presents two major challenges. First, space is typically at a premium, so accommodating a relatively lengthy antenna is difficult. Second, IoT products typically access multiple radio frequencies to connect to Bluetooth low energy (Bluetooth LE), Wi-Fi, GPS, and/or cellular. This means having to accommodate multiple antennas, each requiring their own impedance matching circuit, which adds to the cost, complexity, and bulk of the design.

Embedded antennas offer a solution to the space and cost constraints of multiband IoT product design. These monolithic

antennas feature compact dimensions and can cope with several different frequencies while offering good performance. However, there is a trade-off: in a like-for-like application, the performance of a multiband embedded antenna will fall short of a single-band strip antenna. This makes it even more important that the designer closely adheres to key design guidelines to maximise the embedded antenna's efficiency across all operational frequencies.

These guidelines extend beyond just antenna selection and positioning; the embedded component forms just one part of the 'antenna system.' To construct an efficient system, the antenna must be carefully paired with a suitable printed circuit board (PC board) ground plane and impedance matching circuit to optimise performance. The design of each part of the system significantly affects the overall antenna system efficiency, and the design of the impedance matching circuit can be particularly challenging for multiband embedded antennas.

This article provides a brief introduction to antennas and the challenges facing designers of wireless IoT devices. It then introduces multiband embedded antennas and explains how to design them in and ensure they are matched with the ground plane and impedance matching circuit to optimise performance.

Antenna basics

An antenna converts voltage and current to produce the transmitted RF signal, and in turn, it converts an incoming RF signal to voltage and current at the receiver. Optimising the antenna's efficiency ensures it converts as much of the transmitter power into radiated radio energy and harvests as much energy as possible from the incoming signal to feed the receiver. The efficacy with which it performs these roles largely determines the range and throughput of an IoT device.

Antenna efficiency (typically measured in decibels (dB)) is determined by several factors, but a key factor is impedance. Significant mismatch between the antenna's impedance (which is related to the voltage and current at its input) and the impedance of the voltage source driving the antenna, results in poor antenna efficacy. The key to boosting efficacy is to equalise the two impedances.

Any power reflected by an antenna on a transmission line due to impedance mismatch interferes with the forward traveling power and creates a standing voltage wave. A common measure of how well the impedance is equalised is the voltage standing wave ratio (VSWR). A VSWR of 1 indicates no impedance mismatch loss, while higher numbers indicate increasing losses. For example, a VSWR of 3.0 indicates about 75% of the power is delivered to the antenna. A VSWR of six or more indicates poor efficiency and the design should be revised (Table 1).

A further complication is that antenna impedance changes with frequency. This is not a problem when the system is tuned to a single frequency, but IoT products often use radios operating at multiple frequencies. This is necessary to accommodate a mix of multiple interfaces, such as Bluetooth LE (2.4 GHz), Wi-Fi (2.4, 5, and increasingly 6 GHz), LTE-M/NB-IoT cellular (operating on several bands in the 700 to 2,200 MHz allocation), and GPS (1,227 and 1,575MHz).

VSWR	Loss (dB)
1:1	0
2:1	0.51
3:1	1.25
6:1	3.1
10:1	4.81
20:1	7.41

Table 1: High VSWR causes greater losses. The designer should consider revising the design if VSWR exceeds 6:1. Image source: Steven Keeping

One option for multiband

products is to use a separate impedance-matched antenna for each frequency, but that adds considerable complexity, size, and expense. An alternative is to use a single embedded antenna and design circuitry to ensure good impedance matching to cover a range of operational frequencies.

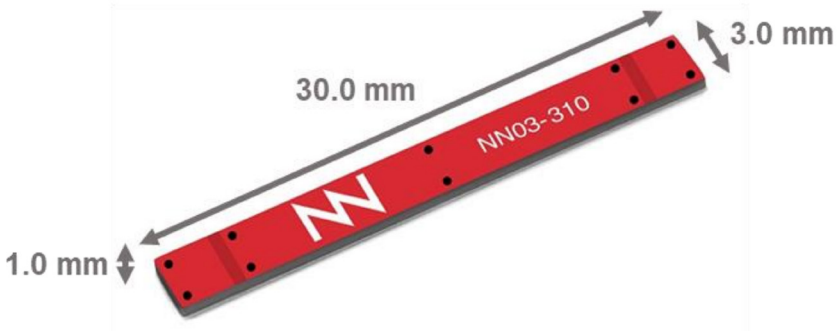
Antenna selection and placement

There are several vendors offering mature embedded antenna designs. With knowledge of the end product's intended operational frequency band(s), it is relatively simple to narrow down the shortlist of suitable antennas from a supplier catalogue. For example, Ignion (formerly Fractus Antennas) offers a range of components suitable for IoT products, including the ALL MXTEND NN02-220 antenna and the TRIO MXTEND NN03-310 antenna.

The NN02-220 is a multiband antenna suitable for cellular 2G, 3G, 4G, and 5G, plus NB-IoT/LTE-M cellular applications and is supplied in a 24 x 12 x 2mm package. With appropriate system design, the antenna can reach an efficiency approaching 70% and a VSWR of less than 3:1. It features an omnidirectional radiation pattern, providing approximately equal transmission and reception in all directions.

The NN03-310 covers the same frequency bands as the NN02-220 but adds GNSS, Bluetooth LE, Wi-Fi 6E, and ultrawideband (UWB). It measures 30 x 3 x 1mm and has performance figures similar to its sister product with efficiency approaching 65%, a VSWR of less than 3:1, and an omnidirectional radiation pattern (Figure 1).

Figure 1: The Ignion NN03-310 is an embedded antenna for cellular, GNSS, short-range RF, Wi-Fi, and UWB. Image source: Ignion



Once the embedded antenna has been selected, the next step is to consider the ground plane. The size of the ground plane has a large impact on antenna efficiency. For example, at an operational frequency of 900MHz, in a like-for-like comparison, a 10cm2 ground plane might exhibit 30% efficiency, whereas a 40cm2 ground plane would boost the efficiency to 60%. Therefore, within the constraints of the end-product form factor, it is good design practice to use as large a PC board as possible and then dedicate one complete layer of the pc board to the ground plane. Note that as the frequency increases, the ground plane size has less impact on antenna efficiency. Above a few GHz, the impact is negligible.

The position of the antenna on the pc board also has a large influence on the design's transmit power and receive sensitivity. Manufacturer guidelines recommend placement at the corner of the IoT device. It is also important to place the chip antenna as far as possible from other active components that could generate electromagnetic interference (EMI) during operation. For the transmission power levels typical of cellular IoT devices, a minimum clearance area of 20mm from other components is satisfactory. The ground plane should also be kept clear of this area.

The PC board pads and traces connecting the chip antenna to the rest of the circuitry should be the only copper conductors in the clearance area. It's also good practice to keep the antenna away from housing screws, brackets, and other metallic parts. For example, on the Nordic Semiconductor nRF6943 cellular IoT development board, the antenna is placed at one side of the board with a

The nRF6943 is designed to assist engineers in the development of IoT devices using short-range wireless (Bluetooth LE), LTE-M/NB-IoT, and GPS.

gap between it and the other components, and at a distance from the mounting screw (Figure 2).

The nRF6943 is designed to assist engineers in the development of IoT devices using short-range wireless (Bluetooth LE), LTE-M/NB-IoT, and GPS.

Matching circuit design

The most important part of the antenna system design is the impedance matching circuit, which sits between the chip antenna and the IoT device's transceiver. The purpose of the matching circuit is to limit transmit/receive losses by matching the impedance of the transmitter power sources with that of the antenna (typically 50 Ω for a low-power IoT product).

The engineering task is to not only design the appropriate circuit topology, but also to select the appropriate inductor and capacitor values to 'transform' the voltage source impedance such that it matches the antenna impedance. The use of high-quality factor (Q) and tight tolerance components enhances performance. For a single operating frequency band, for example 2.4GHz, the design is relatively straightforward, but for an IoT product operating in multiple frequency bands, the matching circuit becomes much more complex.

To assist designers, antenna suppliers such as Ignion offer software that makes the job much easier. Armed with knowledge of the pc board size, choice of chip antenna, frequency band requirements, and S11 parameters (the reflection coefficient for the system which is a proxy for the target efficiency), designers can use Ignion's software package to not only design the matching circuits, but also determine the exact component values needed to approach the S11 parameter target. With the assistance of the software, provided the PC board is large enough, it's possible to design an antenna system with just one embedded antenna and matching circuit that meets the needs of a full multiband system.

However, if the PC board (and hence the ground plane) is small,

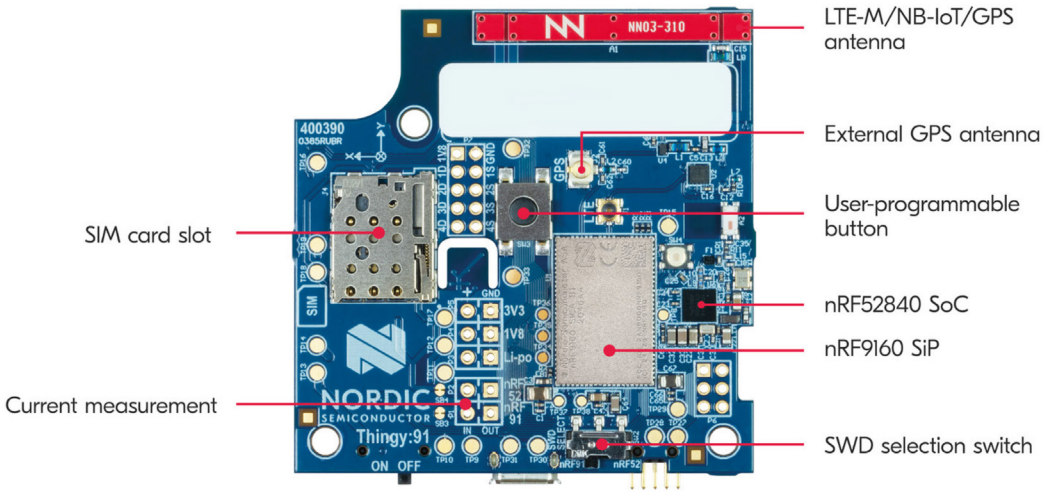


Figure 2: The nRF6943 cellular IoT development board showing the position of the multiband antenna at the top, with wide clearance area (partially covered by white label) between the antenna and other components. Image source: Nordic Semiconductor

a multiband antenna system with a single matching circuit can fail to perform well. One solution – employed on Nordic's nRF6943 – is to incorporate more than one matching network, with each accessed as needed through an MCU-controlled switch. The benefit of doing this is improved performance across all frequency ranges, with the downside that cost, and complexity increase when compared to a single matching circuit. These downsides are mitigated to an extent because each matching circuit only needs to transform the impedance for a single frequency band and will consist of just a few components.

Figure 3 shows an example of the NN03-310 used in a reference design on a small PC board using three matching circuits (or matching networks (MN) as Ignion calls them). MN sections a, b, and c form the matching circuit for operation in the 824 – 960MHz and 1,710 – 1,990MHz cellular bands;

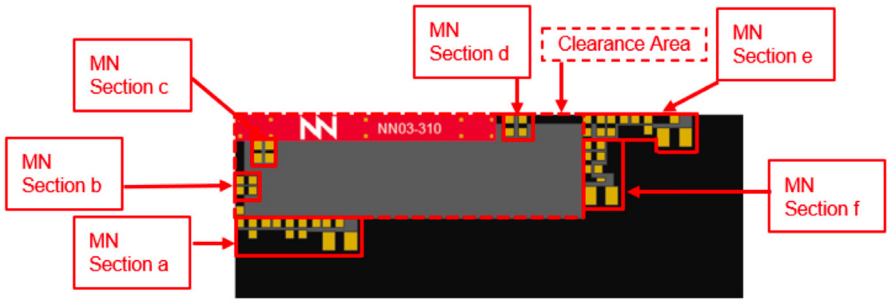


Figure 3: Reference design using the NN03-310 antenna in a multiband design showing the matching circuit positions. Image source: Ignion

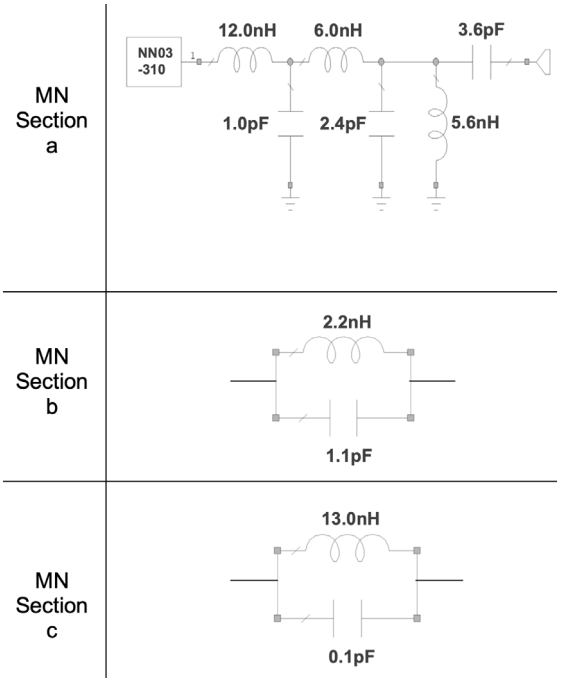


Figure 4: Matching circuit for sections a, b, and c (cellular operation) shown in Figure 3 with component values calculated using the Ignion design software. Image source: Ignion

MN sections d and e suit the 1,561 – 1,606MHz GNSS frequencies; and MN section f is the matching network for 2.4GHz (Bluetooth LE or Wi-Fi) operation. Figure 4 shows the design and component values for the cellular matching circuit (section a, b, and c), and Figure 5 shows the simulated performance of the complete design.

Testing the antenna system

Even though the matching circuit software will provide a good estimate of antenna system frequency response and efficacy, an actual prototype must be tested to ensure it demonstrates not only the predicted radiative efficiency, but that it is also approximately omnidirectional.

The first test can be done by connecting a 50 Ω micro-coaxial cable to the antenna, grounded at three or four points on the pc board, and then connecting that cable to a network analyser. The results will not only indicate efficiency but also frequency response and bandwidth. The test typically reveals if some adjustment to the matching circuit components is needed.

Ignion has made initial testing easier by supplying evaluation

boards for both the NN02-220 and NN03-310 antennas, the EB_NN02-220-1B-2R-1P and EB_NN03-310-M+5G, respectively. In each case, the evaluation boards include the antenna, impedance matching circuits, and the grounded 50 Ω micro-coaxial cable (Figure 6).

A designer can plug the evaluation boards into a network analyser to familiarise themselves with the frequency response they might expect from a similar prototype design, before moving on to product testing.

The final examination of the cellular IoT device's performance should be made in an anechoic chamber. This is the ultimate test of a design which often reveals weaknesses in efficiency and omnidirectional performance that don't show up during network analyser testing. Deficiencies might require a revised embedded antenna selection, ground plane and clearance area redesign, and/or matching circuit tuning.

Conclusion

The small size and multi-frequency operation of many IoT products makes antenna implementation a challenge. Separate antennas and matching circuits for each frequency can be tough to accommodate, and they add complexity and cost.

Embedded antennas offer an option to save space by using a single device to serve multiple frequencies. The trade-off is that ground plane, clearance, and matching circuit design becomes even more difficult. However, embedded antenna suppliers offer proven design advice and software modelling tools that can ease the design cycle. Even with this assistance, the task is not trivial, and antenna system design often comes down to repeatedly testing a design's performance and then refining the layout.

Figure 6: The Ignion antenna evaluation boards include a grounded 50 Ω micro-coaxial cable which can be connected to a network analyser. Image source: Ignion

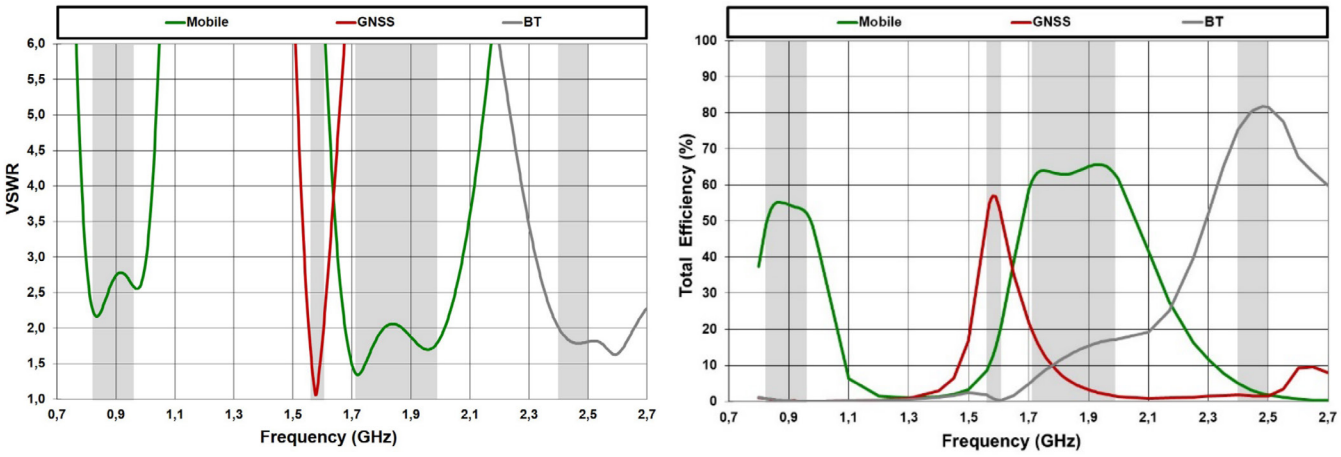


Figure 5: Simulated VSWR and efficiency results for the reference design shown in Figure 3, using the NN03-310 and matching circuit's component values calculated by the Ignion design software. Image source: Ignion

How to use GNSS modules to create location aware smart city solutions

Written by:
Jeff Shepard,
Contributing Author, DigiKey

Location-aware services (LAS) in smart cities are being deployed across various areas, including government services, transport, traffic management, energy, healthcare, and water and waste, and creating safer, more sustainable, and better-connected cities. There is often a need to understand the distances between nearby devices in these applications. The demand for position-based capability using multi-constellation global navigation satellite system (GNSS) receivers for Europe's Galileo, the USA's GPS, Russia's GLONASS, and China's BeiDou navigation satellite systems is growing in LAS applications. The benefits of using multi-constellation GNSS receivers include better availability of the position, navigation, and timing (PNT) signals, increased accuracy and integrity, and improved robustness. But developing multi-constellation receivers is a complex and time-consuming activity.

This article reviews important system design considerations when using multi-constellation GNSS receivers before presenting GNSS platforms and development environments from u-blox, Microchip Technology, MikroElektronika, Thales, and Arduino for the efficient and cost-effective development of location-aware smart city applications.

Improvements in GNSS technology, especially reduced power requirements, have been instrumental in the increased use of the GNSS and the proliferation of LAS in smart city applications. The GNSS receiver power consumption reduction has been from 120mW in 2010 to 25mW in 2020 (Figure 1). In fact, GNSS receiver power demand has declined faster than the power needs of most other LAS system components. Older GNSS technologies were power-hungry compared with the other system elements. Today, GNSS power needs are often only a single-digit

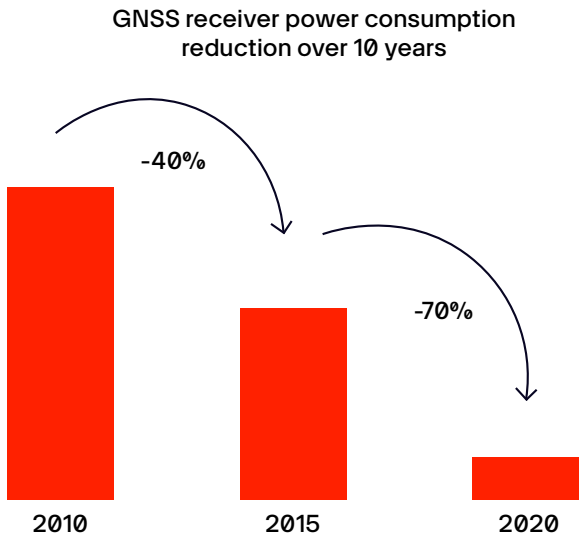


Figure 1: GNSS receiver power consumption has declined from 120mW in 2010 to 25mW in 2020. Image source: u-blox

percentage of the overall power budget.

Power consumption challenges

While GNSS receiver power consumption has declined dramatically, the complexities of getting the optimal power/performance solution have multiplied. Not every LAS design needs continuous GNSS position estimations or high levels of position accuracy. Designers have various tools to optimise GNSS performance and power consumption, including hardware optimisation and firmware-based approaches.

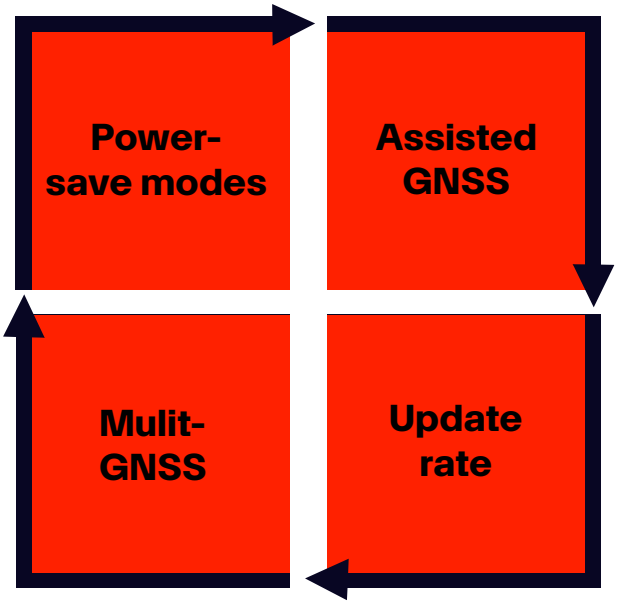


Figure 2: In addition to using the most efficient hardware solution, designers have several firmware tools to optimise GNSS performance and energy consumption. Image source: u-blox

The use of low-power components, especially low-noise RF amplifiers (LNAs), oscillators, and real-time clocks (RTCs), is the first step in developing energy-efficient GNSS solutions. The choice between active and passive antennas is a good example. Passive antennas are lower in cost and more efficient but don't meet the needs of every application. An active antenna may be a good choice in urban canyons, inside buildings, or other locations with poor signal strength. The LNA in the active antenna significantly increases the ability to receive weak signals but also consumes significant amounts of power. When power consumption is critical, and antenna size is not as important, a larger passive antenna can often provide the same performance as a smaller active antenna while still providing high position availability and accuracy levels.

Most GNSS receivers can provide update rates of 10Hz or higher, but most LAS applications work well with much slower and less power-consuming update rates. Selecting the optimal update rate can have the largest impact on power consumption. In addition to the hardware-based considerations, designers have a range of firmware tools available when optimising power consumption, including update rates, the number of concurrently tracked GNSS constellations, assisted GNSS, and a variety of power-saving modes (Figure 2).

It may be necessary to track multiple GNSS constellations concurrently in challenging environments. While receiving signals using various bands can ensure a robust position determination, it also increases power consumption. It's important to understand the specific operating environment, especially how open the sky view is, and use the minimum number of GNSS signals required to support the needs of the particular LAS application.

Turning the GNSS function off saves the most energy but results in a cold start every time it's turned on. The time to first fix (TTFF) for a cold start can be 30 seconds, or longer, depending on the availability and strength

of the GNSS signals and the size and placement of the antenna. Assisted GNSS can reduce the TTFF while still providing accurate information. Assisted GNSS can be implemented in several ways, including the current and predicted satellite location and timing parameters (called 'ephemeris data'), almanac, and accurate time and satellite status correction data for the satellite systems downloaded over the Internet in real-time or at intervals of up to several days. Some GNSS receivers have an autonomous mode that internally calculates GNSS orbit predictions, eliminating the need for external data and connectivity. However, using autonomous mode can require that the receiver be turned on periodically to download current ephemeris data.

Power save modes

In addition to connectivity options such as assisted GNSS, many GNSS receivers enable designers to select from a range of tradeoffs between update rates and power consumption, including continuous tracking, cyclic tracking, on/off operation, and snapshot positioning (Figure 3). Selecting the optimal tracking mode is another important consideration when defining the performance of a specific application. If operating conditions change, making the optimal power-saving mode unavailable, the system should automatically switch to the next most energy-saving mode to ensure continuous functionality.

Continuous tracking is suited for applications that require a few updates per second. The GNSS receiver acquires its position in this mode, establishes a position fix, downloads almanac, and ephemeris data, and then switches to tracking mode to reduce power consumption.

Cyclic tracking involves several seconds in between position updates and is useful when the signals and/or the antennas are sufficiently large to ensure position signals are accessible as needed. Additional power savings can be achieved if the tracking does not require the acquisition of new satellites.

On/Off operation involves switching between acquisition/tracing activities and sleep mode. The time in sleep is typically several minutes and on/off operation requires strong GNSS signals to minimise the TTFF and, therefore, the power consumption following each sleep period.

Snapshot positioning saves power by using the GNSS receiver for local signal processing combined with cloud computing resources for the more compute-intensive position estimation processing. When an internet connection is available, snapshot positioning can reduce GNSS receiver power consumption by a factor of ten. This solution can be an effective power-saving strategy when only a few position updates per day are needed.

Embedded antenna supports GNSS augmentation

Designers can turn to the SAM-M8Q patch antenna module from u-blox for systems that benefit from the concurrent reception

Update rate	Sub-second	Seconds	Minutes	Hours
Power-save mode	Continuous tracking	Cyclic tracking	On/Off operation	Snapshot positioning

Figure 3: Energy-saving operating modes need to be matched with required update rates to optimise GNSS system performance.
Image source: u-blox

of GPS, Galileo, and GLONASS GNSS signals (Figure 4). Using three constellations at once results in high position accuracy in challenging environments such as urban canyons or when receiving weak signals. To speed positioning and improve accuracy, the SAM-M8Q supports augmentation functions, including a quasi-zenith satellite system (QZSS), GPS aided GEO augmented navigation (GAGAN), and indoor messaging system (IMES), together with wide area augmentation system (WAAS), European geostationary navigation overlay service (EGNOS), and the MTSAT satellite augmentation system (MSAS).

The SAM-M8Q module can also use the u-blox AssistNow assistance service that provides GNSS broadcast parameters, including ephemeris data, almanac, plus time or rough position, to reduce the TTFF significantly. The extended validity of AssistNow Offline data (up to 35 days) and AssistNow Autonomous data (up to 3 days) supports faster TTFF even after an extended time.

This Internet of Things (IoT) Google Cloud development platform provides a simple way to connect and secure PIC MCU-based applications. GNSS 4 click from MikroElektronika contains a SAM-M8Q module and is designed with the PIC-IoT WG Development Board from Microchip Technology to speed the development of LAS smart city applications (Figure 5).

Figure 4: The SAM-M8Q module supports concurrent reception of up to three GNSS sources (GPS, Galileo, GLONASS). Image source: u-blox

The PIC-IoT WG development board provides Google Cloud IoT users a way to accelerate the development of secure Cloud-connected applications. In addition, the PIC-IoT WG board provides designers with analytics and machine learning tools.

Multi-constellation GNSS plus wireless connectivity

For small LAS devices such as trackers that can benefit from multi-constellation GNSS support (GPS/Galileo/ GLONASS) and global LPWAN LTE connectivity from a single module leveraging Rel. 14-second generation Cat. M1/ NB1/NB2, designers can turn to the Cinterion TX62 module from Thales (Figure 6). Solution size can be further optimised using the module's flexible architecture that supports running applications using a host processor or inside the module using the integrated processor. The TX62 supports

3GPP power saving mode (PSM) and extended discontinuous reception (eDRx) for power-sensitive applications. PSM sleep times tend to be much longer than eDRX. These longer sleep times allow the device to enter into a deeper, lower power sleep mode than eDRX. PSM sleep power is under ten microamps, while eDRX sleep power is up to 30 microamps.

TX62 security features include secure key storage and certificate handling to support trustful enrolment in Cloud platforms while

Figure 5: The GNSS 4 click board carries the SAM-M8Q patch antenna module from u-blox. Image source: DigiKey

protecting the device and data, plus trusted identities pre-integrated into the root of the TX62 during manufacturing. When needed, designers can specify an optional integrated eSIM that can simplify logistics and manufacturing processes and improve flexibility in the field through dynamic subscription updates and remote provisioning.

LAS development in Arduino Portenta H7 applications is simplified using the Portenta Cat. M1/NB IoT GNSS Shield (Figure 7). The shield combines the Edge computing power of the Portenta H7 with the connectivity of the TX62 to enable the development of LAS asset tracking and remote monitoring in smart city applications as well as industrial, agriculture, utility, and other areas. The basic Portenta Cat. M1/NB IoT GNSS Shield does not include a GSM/UMTS antenna. Instead of searching for a compatible antenna, designers can use the Arduino dipole pentaband waterproof antenna.

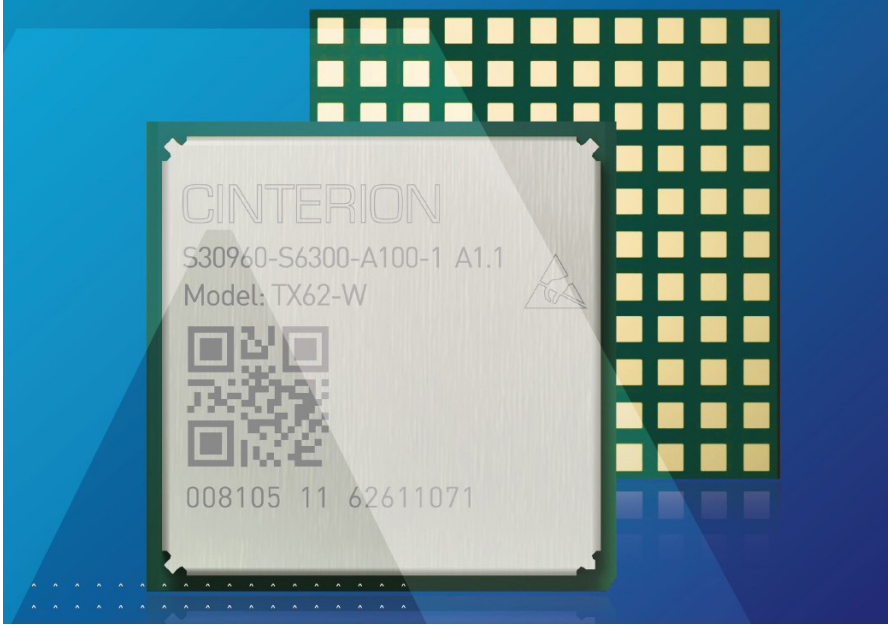


Figure 6: The TX62 IoT module supports LTE-M, NB1, and NB2 communications and multi-constellation GNSS.
Image source: Thales

Additional benefits of the Portenta CAT.M1/NB IoT GNSS shield include:

- Ability to change connectivity without changing the board
- Add positioning plus NB-IoT, CAT.M1 any Portenta-based design
- Significantly lowered communication bandwidth requirements in IoT devices
- Compact 66 x 25.4mm format
- -40 to +85°C operation (-104°F to 185°F)

Summary

Advances in low-power and high-performance GNSS technology are factors driving the growth of LAS smart city applications. However, simply using the most energy-efficient hardware is only the starting point; it's equally important to optimise the firmware to arrive at an optimal and energy-efficient solution. There are numerous combinations of hardware and firmware available to choose from when developing GNSS-based LAS applications and designers can turn to a variety of eval tools to speed the development process.

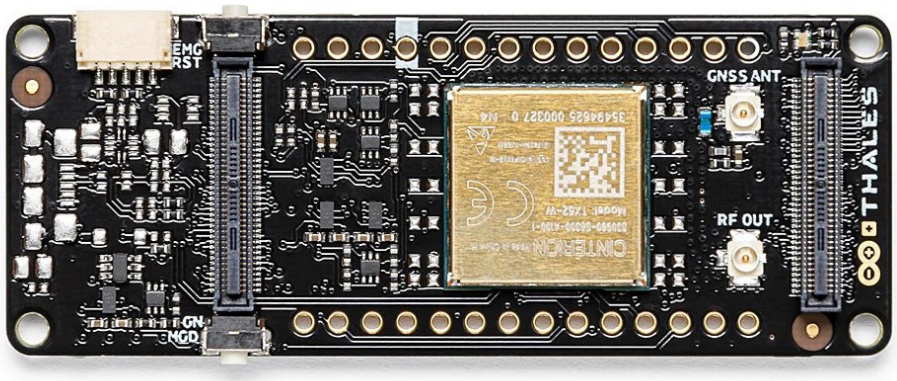
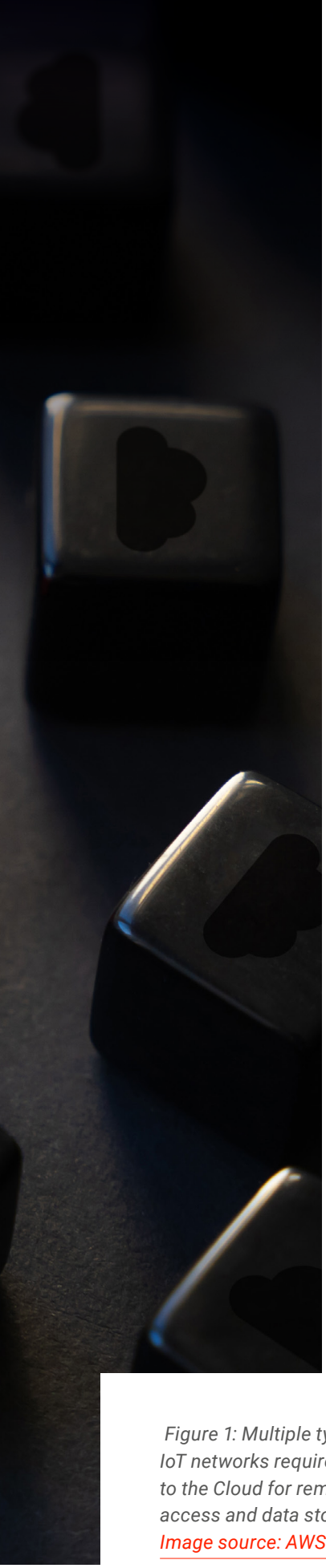


Figure 7: The Portenta CAT.M1/NB IoT GNSS Shield includes the TX62-W IoT module (large yellow square).
Image source: Arduino

How to quickly connect IoT nodes to Amazon AWS and Microsoft Azure Clouds

Written by:
Jeff Shepard
Contributing Author, DigiKey



Cloud connectivity using services like the Amazon AWS and Microsoft Azure Clouds is highly valued in a range of Internet of things (IoT) applications, including industrial and building automation, smart medicine and transportation, consumer appliances, and smart cities. In these applications, Cloud connectivity is an indispensable support feature but not the device's primary function. Cloud storage of the zettabytes of data produced by many IoT networks and Cloud-enabled remote access to IoT devices are increasingly important (Figure 1).

Maintaining privacy, obtaining the needed security certifications, ensuring interoperability, and managing communication latencies are important aspects of developing effective Cloud connectivity solutions. Each of these challenges can be dealt with, but they can also divert time and resources away from development of the primary device functionality.

Instead of developing Cloud connectivity from the ground up, designers can turn to Cloud connectivity development kits to speed up the process. These kits are available for microcontroller unit (MCU)-based designs and field programmable gate array (FPGA)-based designs and support all the elements needed for quickly connecting IoT devices to the Amazon AWS and Microsoft Azure Clouds.

This article reviews the building blocks and architectures for Cloud connectivity, looks at event-driven Cloud architectures for gathering and managing data from large-scale sensor networks, and reviews the International Standards Organisation/International Electrotechnical Commission (ISO/IEC) 27017 and 27018 guidelines for Cloud security. It then presents Cloud connectivity development

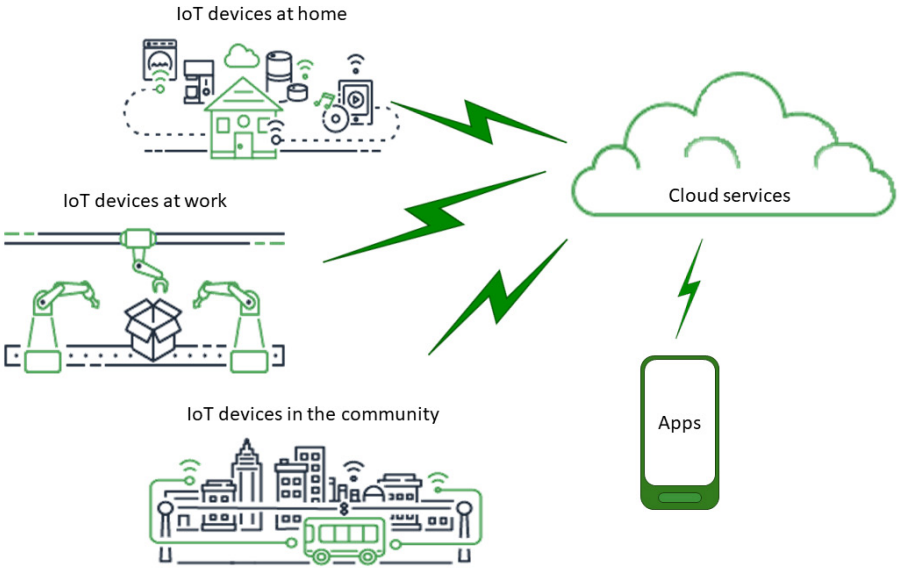


Figure 1: Multiple types of IoT networks require access to the Cloud for remote access and data storage. Image source: AWS

kits from Renesas and Terasic for MCU and FPGA-based IoT devices, along with an MCU from Renesas and an FPGA from Intel.

Cloud services are distributed large-scale data processing and storage resources connected to the Internet. Elements in a typical Cloud environment include (Figure 2):

Devices and sensors – Devices can include hardware or software that interacts with the immediate environment or responds to communications from the Cloud. Devices can range from actuators and motors to Human Machine Interfaces (HMIs) like touch screens and apps on mobile handsets. Sensors measure specific environmental parameters and send the data to the Cloud for analysis, storage, and/or decision making. Devices and sensors can be directly connected to the Cloud using the Internet, or they can connect indirectly using a gateway.

Gateways – Provide communications platforms like Wi-Fi, Ethernet, cellular, or other wireless protocols that support access to and from the Cloud for devices and sensors that are not directly connected to the Internet. Gateways can also provide initial filtering, aggregation, and data processing before being sent to the Cloud.

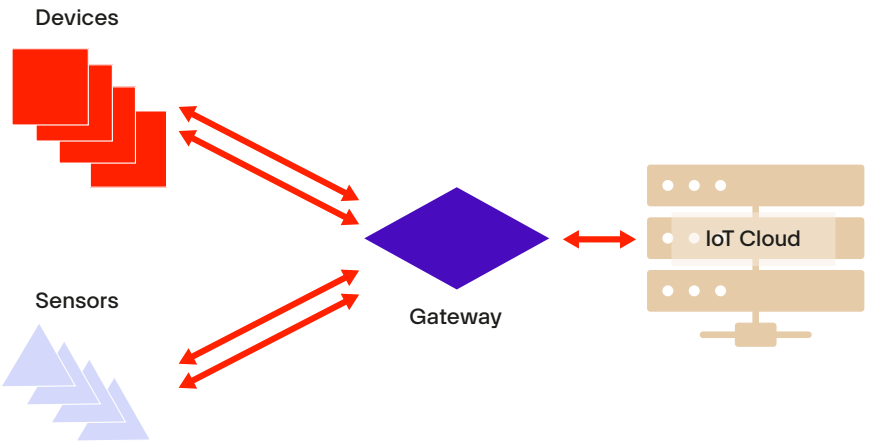


Figure 2: IoT Cloud services can be connected to networks of sensors and devices through a dedicated gateway. Image source: Renesas

IoT Cloud – Is a scalable, cost-effective way to support widely dispersed devices and sensors, and provide large-scale storage, processing, and analysis for big data. IoT Cloud services are third-party hosted infrastructures and platforms like Amazon AWS and Microsoft Azure. They can include only hardware but often also provide a wide range of software packages to support data analytics, reporting, and decision making.

Event-driven Cloud architecture for IoT sensor data

IoT sensor information derived from medical devices, automotive systems, building automation controls, and Industry 4.0 systems can be automatically sent to the Cloud for collection, analysis, and decision making using an event-driven Cloud architecture. The basic architecture includes several elements (Figure 3).

The IoT sensor data is collected using an IoT Edge runtime and Cloud service that aggregates data and performs initial analysis close to the source. This Edge service reacts autonomously when new data arrives, filters it, aggregates it into the proper format, and securely sends it to the Cloud and local network devices as appropriate.

An Edge-to-Cloud interface service ingests the data into the Cloud. In addition to providing an Edge connection service, the interface should be secure and scalable and connect with Cloud applications and other devices as appropriate.

The ingested data is then transformed as needed for further processing and can be stored for future reference. Data transformation can include enrichment and simple formatting to support downstream analysis and business intelligence reporting. Initial analytics can also be used to prepare the data for the machine

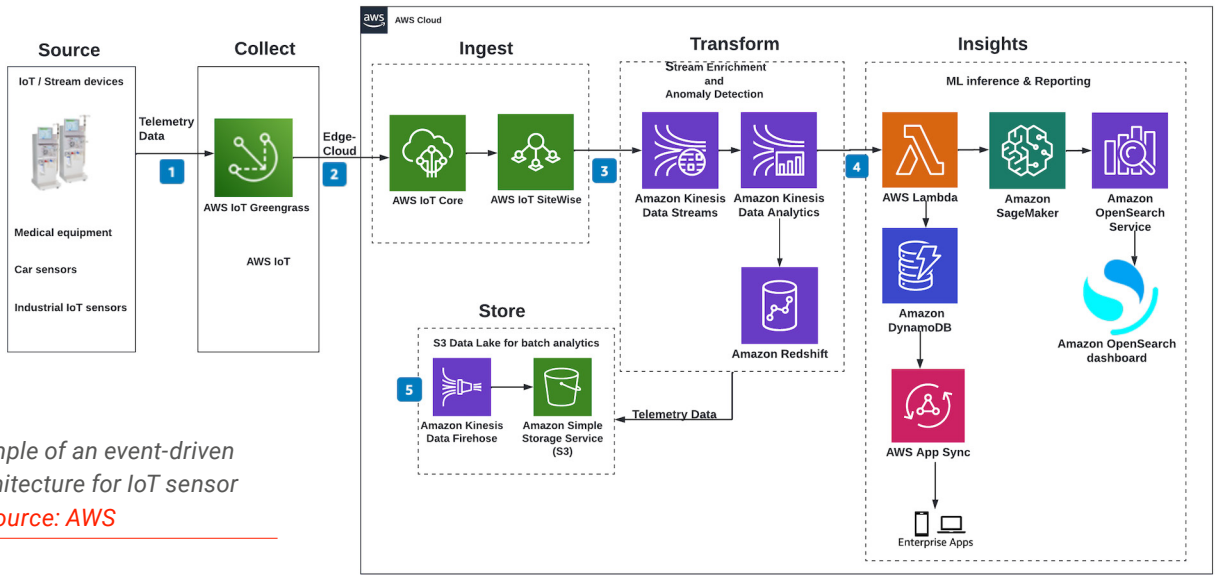


Figure 3: Example of an event-driven reference architecture for IoT sensor data. Image source: AWS

learning (ML) processing in the next step. In addition, anomalous data can be identified that may require accelerated analysis and decision making.

ML training and analysis are ongoing processes as more and more data becomes available. In this final block of the architecture, mobile apps or business applications can be used to access the raw data in near real-time or look at the results of the ML processing. Automatic reporting and alerts can provide the insights needed to support manual or automatic management of the devices that were the sources of the original sensor data.

IEC 27017 and IEC 27018 – why you need both

Developers of Cloud solutions need IEC 27017 and IEC 27018. 27017 defines information security controls for Cloud services, while 27018 defines how to protect user privacy in the Cloud. They were developed under the ISO/IEC JTC 1/SC 27 joint subcommittee and are part of the IEC 27002 family of security standards.

IEC 27017 provides recommended practices for both Cloud service providers and Cloud service customers. It is designed to help customers understand the shared responsibilities in the Cloud and provides customers with insights on what they should expect from Cloud service suppliers. For example, it adds seven additional controls for Cloud services to the 37 controls specified in the base IEC 27002 standard. The additional controls relate to the following:

- Division of responsibilities between service providers and Cloud users
- Return of assets at the end of a Cloud contract
- Separation and protection of the user's virtual environment
- Virtual machine configuration responsibilities
- Administrative procedures and operations to support the Cloud environment
- Monitoring and reporting Cloud activity
- Alignment and coordination of the Cloud and virtual network environments

IEC 27018 was developed to help Cloud service providers assess risk and implement controls for protecting users' personally identifiable information (PII). When combined with IEC 27002, IEC 27018 creates a standard set of security controls and categories and controls for public Cloud computing service providers that process PII. Among its several objectives, IEC 27018 outlines how to provide a mechanism for Cloud service customers to exercise audit and compliance rights. This mechanism is especially important where individual Cloud service

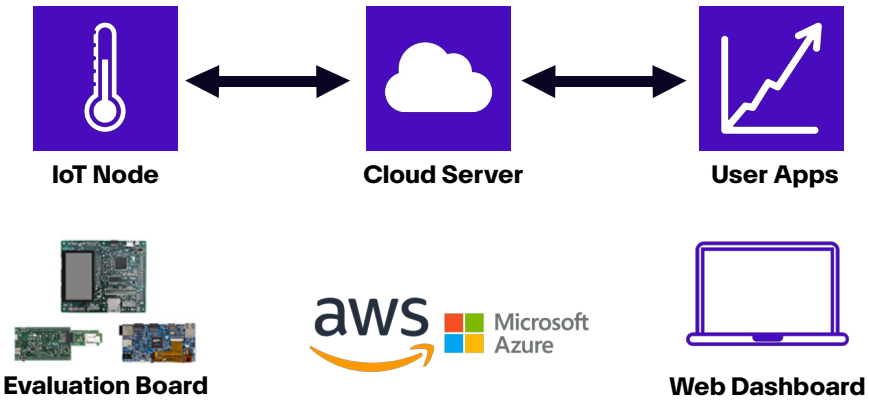


Figure 4: Developers can use the eval boards in the RX65N Cloud kit to quickly implement IoT devices with connectivity to the Amazon AWS and Microsoft Azure Clouds. Image source: Renesas

customer audits of data hosted in a multiparty, Cloud environment using virtualised servers can be technically challenging and increase risks to existing physical and logical network security controls. The standard has several advantages, including:

- Increased security for customer PPI data and information
- Increased platform reliability for Cloud users and customers
- Helps speed deployment of global operations
- It defines legal obligations and protections for Cloud providers and users
- MCU-based Cloud connection dev platform

The RX65N Cloud kit from Renesas provides a platform for designers of industrial and building automation, smart home, smart meters, office automation, and general IoT applications to prototype and evaluate IoT equipment. Two variations are available: the RTK5RX65N0S01000BE, which supports development of systems for use in the US, and the RTK5RX65N0S00000BE for the rest of the world. Both provide quick connectivity to the Amazon AWS and Microsoft Azure Clouds (Figure 4). Using these kits, designers who do not have previous experience with developing IoT devices can quickly start using a solution in a Cloud connection environment.

The RX65N Cloud kit supports flexible development with several sensors, user interfaces, and communication functions. It also provides sample programs to speed application development. The sample programs can be edited and debugged. The included application notes provide details of the operation of the applications. The sample programs are ported based on Amazon FreeRTOS and can be freely expanded, changed, and deleted using available source code libraries. The kit has AWS qualification, so it can communicate with AWS safely and securely and includes (Figure 5):

- Cloud option board with temperature/humidity sensor, light sensor, and 3-axis accelerometer, plus a USB port for serial communication and a second USB port for debugging
- Wi-Fi communication module based on the Silex SX-ULPGN Pmod module
- All necessary power management
- RX65N target board that

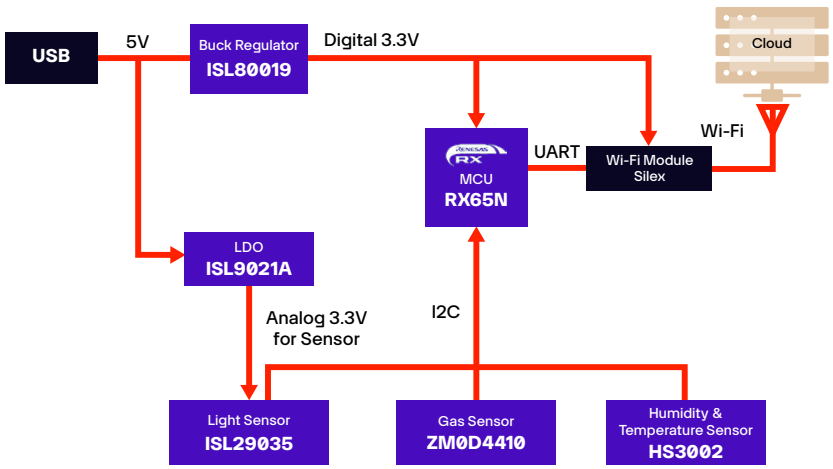


Figure 5: The RX65N Cloud kit is AWS-qualified and includes everything needed to connect IoT devices securely. Image source: Renesas

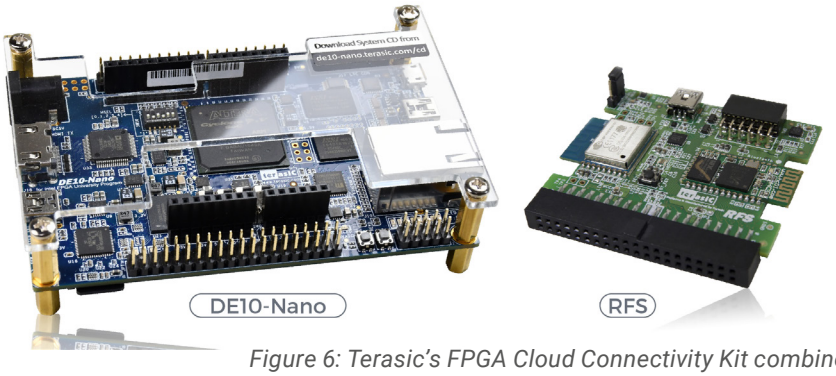


Figure 6: Terasic's FPGA Cloud Connectivity Kit combines the DE10-Nano Cyclone V SoC FPGA board and the RFS daughter card. Image source: Terasic

includes the R5F565NEDDFP MCU rated for operation from -40 to +85°C

Renesas' RX65N MCUs are well suited for Cloud and sensor solution endpoint devices. Features include:

- 120MHz operation with single-precision FPU
- 2.7 to 3.6 V operation
- Only 0.19 mA/MHz is needed to support all peripheral functions
- Four low-power modes for power/performance optimization
- Communication interfaces include Ethernet, USB, CAN, SD host/slave interface, and quad SPI
- Program Flash up to 2 MB, SRAM up to 640 KB
- DualBank function simplified firmware updates

Security:

- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 Level 3 Cryptographic Module Validation Program (CMVP) certification
- Renesas' proprietary hardware secure IP (Trusted Secure IP) is integrated and realises a high level of root-of-trust
- Available encryption engines include AES, TRNG, TDES, RSA, ECC, SHA
- Equipped with functions that protect Flash memory from unintended access
- Cloud connectivity with an FPGA

Designers that need FPGA performance and Cloud connectivity can turn to Terasic's FPGA Cloud Connectivity Kit, which combines an Intel Cyclone V system on chip (SoC) FPGA, like the 5CSEBA5U23C8N, with Cloud connectivity. This dev kit is certified with Cloud service providers, including Microsoft Azure, and includes open source design examples that walk designers through the process of connecting an Edge device to the Cloud. The FPGA Cloud Connectivity Kit includes (Figure 6):

- DE10-Nano Cyclone V SoC FPGA Board
- RFS daughter card with:
- Wi-Fi, using ESP-WROOM-02 module with up to 100-meter range
- 9-axis sensor with accelerometer, gyroscope, and magnetometer
- Ambient light sensor
- Humidity and temperature sensor
- UART to USB
- 2x6 TMD GPIO Header
- Bluetooth SPP, using HC-05 module with up to 10-metre range

The Intel Cyclone SoC FPGA is a customisable ARM processor-based SoC that supports lower system power, lower cost, and less board space by integrating a hard processor system (HPS) that includes processors, peripherals, and a memory controller, with a low-power FPGA fabric using a high-bandwidth interconnect. These SoCs are especially suited for high-performance IoT Edge applications.

Summary

Adding Cloud connectivity to IoT devices and sensors need not be a difficult task that diverts resources from the design of the primary device functionality. Designers can turn to MCU and FPGA-based environments that support quick and efficient connectivity to the Amazon AWS and Microsoft Azure Clouds. These development kits include comprehensive suites of sensors, wired and wireless communications options, and sample application programs that provide safe and secure Cloud connectivity.

Use multiprotocol wireless modules to simplify IoT product design and certification

Written by:
Steven Keeping,
Contributing Author, DigiKey

Figure 1: Bluetooth LE is well suited to smart home sensors such as cameras and thermostats. Its interoperability with smartphones simplifies the configuration of compatible products. Image source: Nordic Semiconductor

Wireless connectivity allows designers to turn dumb products into smart, integrated elements of the Internet of Things (IoT) that can send data to the Cloud for artificial intelligence (AI)-based analysis while allowing devices to receive over-the-air (OTA) instructions, firmware updates, and security enhancements.

But adding a wireless link to a product is not trivial. Before the design phase can even start, designers need to choose a wireless protocol, which can be daunting. For example, several wireless standards operate in the popular, license-free 2.4GHz spectrum. Each one of these standards represents a trade-off in terms of range, throughput, and power consumption. Selecting the best one for a given application requires careful evaluation of its requirements against a protocol's characteristics.

Then, even with highly integrated modern transceivers, designing the radio frequency (RF) circuit is a challenge for many design teams, leading to cost and schedule overruns. Moreover, an RF product will need to be certified for operation, which in itself can be an involved, complex, and time-consuming process.

One solution is to base the design on a certified module that uses a multiprotocol system-on-chip (SoC). This eliminates the complexity of RF design with discrete components and allows for flexibility in the choice of wireless protocol. This module approach presents designers with a drop-in wireless solution, making it much easier to integrate wireless connectivity into products and pass certification.

This article considers the benefits of wireless connectivity, looks at the strengths of some key 2.4GHz wireless protocols, briefly analyses hardware design issues, and introduces a suitable RF module from Würth Elektronik. The article also discusses the certification process required to satisfy global regulations, considers application software development, and introduces a software development kit (SDK) to help designers get started with the module.

The advantages of multiprotocol transceivers

No single short-range wireless sector dominates because each makes trade-offs to satisfy their target applications. For example, greater range and/or throughput comes at the cost of increased power consumption. Other important factors to consider are interference immunity, mesh networking capability, and Internet protocol (IP) interoperability.

Of the various established short-range wireless technologies, there are three clear leaders: Bluetooth Low Energy (Bluetooth LE), Zigbee, and Thread. They

share some similarities due to a shared DNA from the IEEE 802.15.4 specification. That specification describes physical (PHY) and media access control (MAC) layers for low data rate wireless personal area networks (WPANs). The technologies generally operate at 2.4GHz, although there are some sub-GHz variants of Zigbee.

Bluetooth LE is suited to IoT applications such as smart home sensors where data transmission rates are modest and occur infrequently (Figure 1). Bluetooth LE's interoperability with the Bluetooth chips hosted by most smartphones is also a big advantage for consumer-oriented applications such as wearables. Key downsides to the technology are the requirement for an expensive and power-hungry gateway to connect to the Cloud and clunky mesh networking capabilities.

Zigbee is also a good choice for low power and low throughput applications in industrial automation, commercial, and the home. Its throughput is lower than Bluetooth LE, while its range and

Previously, a designer had to choose one wireless technology and then redesign the product if there was a demand for a variant using a different protocol. But because the protocols use PHYs based on a similar architecture and operate in the 2.4GHz spectrum, many silicon vendors offer multiprotocol transceivers.

power consumption is similar. Zigbee is not interoperable with smartphones, nor does it offer native IP capability. A key advantage of Zigbee comes from it being designed from the ground up for mesh networking.

Thread, like Zigbee, operates using the IEEE 802.15.4 PHY and MAC and has been designed to support large mesh networks of up to 250 devices. Where Thread differs from Zigbee is through its use of 6LoWPAN (a combination of IPv6 and low-power WPANs), making connectivity with other devices and the cloud straightforward, albeit via a network edge device called a border router. (See, *A Brief Guide to What Matters in Short-Range Wireless Technologies*.)

While standards-based protocols dominate, there is still a niche for 2.4GHz proprietary protocols. Though they limit connectivity to other devices equipped with the same manufacturer's chip, such protocols can be finely tuned to optimize power consumption, range, interference immunity, or other important operational parameters. An IEEE 802.15.4 PHY and MAC is perfectly capable of supporting 2.4GHz proprietary wireless technology.

The popularity of these three short-range protocols and the flexibility offered by 2.4GHz proprietary technology makes it difficult to choose the right one to suit the widest set of applications. Previously, a designer had to choose one wireless technology and then redesign the product if there was a demand for a variant using a different protocol. But because the protocols use PHYs based on a similar architecture and operate in the 2.4GHz spectrum, many silicon vendors offer multiprotocol transceivers.

These chips allow a single hardware design to be reconfigured for several protocols simply by uploading new software. Better yet, the product could be shipped with multiple software stacks, with switching between each supervised by a microcontroller unit (MCU). This could allow, for example, Bluetooth LE to be used to configure a smart home thermostat from a smartphone before the device switches protocols to join a Thread network.

Nordic Semiconductor's nRF52840 SoC supports Bluetooth LE, Bluetooth mesh, Thread, Zigbee, IEEE 802.15.4, ANT+, and 2.4GHz proprietary stacks. The Nordic SoC also integrates an Arm Cortex-M4 MCU – which looks after the RF protocol and application software – as well as 1 megabyte (Mbyte) of flash memory and 256 kilobytes (Kbytes) of RAM. When running in Bluetooth LE mode, the SoC offers a maximum raw data throughput of 2 megabits per second (Mbits/s). The transmit current draw off its 3-volt DC input supply is 5.3 milliamps (mA) at 0 decibels referenced to 1 milliwatt (dBm) of output power, and the receive (RX) current draw is 6.4 mA at a raw data rate of 1 Mbit/s. The nRF52840's maximum transmit power is +8 dBm and its sensitivity is -96 dBm (Bluetooth LE at 1 Mbit/s).

The importance of good RF design

While wireless SoCs such as Nordic's nRF52840 are very

capable devices, it still requires considerable design skill to maximise its RF performance. In particular, the engineer needs to consider factors such as power supply filtering, external crystal timing circuits, antenna design and placement, and crucially, impedance matching.

The key parameter that differentiates a good RF circuit from a poor one is its impedance (Z). At high frequencies, such as the 2.4GHz used by a short-range radio, the impedance at a given point on an RF trace is related to the characteristic impedance of that trace, which in turn depends on the printed circuit (pc) board substrate, dimensions of the trace, its distance from the load, and the load's impedance.

It turns out that when the load impedance – which for a transmitting system will be the antenna and for a receiving system is the transceiver SoC – is equal to the characteristic impedance, the measured impedance remains the same at any distance along the trace from the load. As a result, line losses are minimised, and maximum power is transferred from the transmitter to the antenna, thereby boosting robustness and range. That makes it good design practice to build a matching network that ensures an RF device's impedance is equal to the pc board trace's characteristic impedance. (See, *Bluetooth 4.1, 4.2 and 5 Compatible Bluetooth Low Energy SoCs and Tools Meet IoT Challenges (Part 2)*.)

The matching network comprises

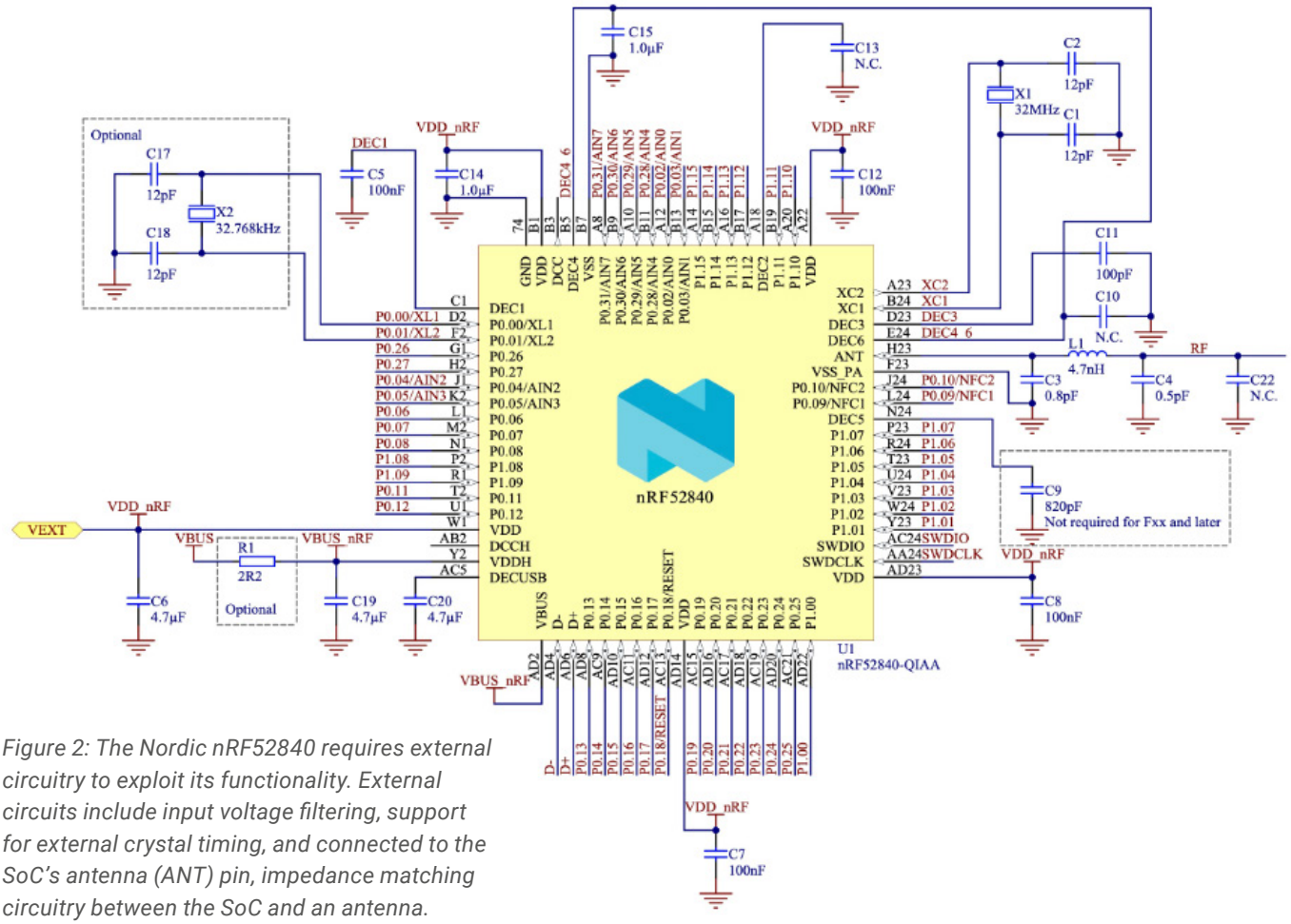


Figure 2: The Nordic nRF52840 requires external circuitry to exploit its functionality. External circuits include input voltage filtering, support for external crystal timing, and connected to the SoC's antenna (ANT) pin, impedance matching circuitry between the SoC and an antenna. Image source: Nordic Semiconductor

one or more shunt inductors and series capacitors. The designer's challenge is to choose the best network topology and component values. Manufacturers often offer simulation software to help with matching circuit design, but even after following good design rules, the resulting circuit can often exhibit disappointing RF performance, lacking range and reliability. This leads to more design iterations to revise the matching network (Figure 2).

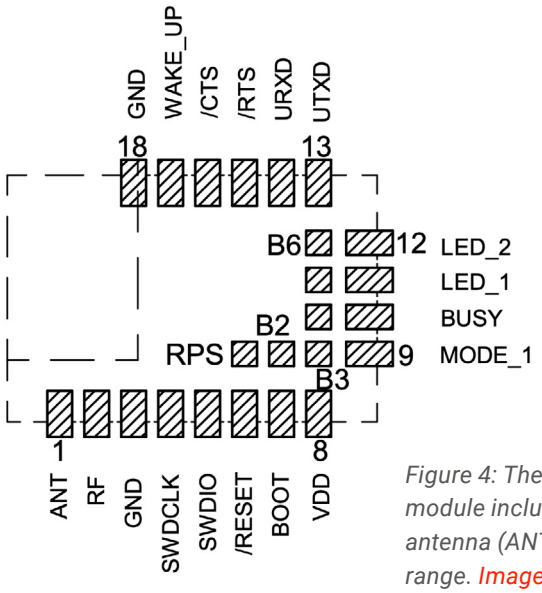


Figure 4: The Setebos-I 2.4 GHz radio module includes a pin for an external antenna (ANT) to extend the radio's range. Image source: Würth Elektronik

The advantages of a module

There are some advantages to designing a short-range wireless circuit using discrete components, notably lower bill-of-material (BoM) costs and space savings. However, even if the designer follows one of the many excellent reference designs from SoC suppliers, other factors – such as component quality and tolerances, board layout and substrate characteristics, and end-device packaging – can dramatically affect RF performance.

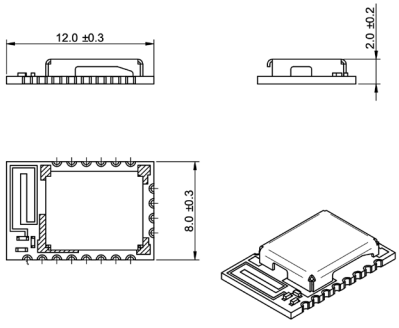


Figure 3: The Setebos-I 2.4 GHz radio module comes in a compact form factor, has a built-in antenna, and comes with a cover to limit EMI. Image source: Würth Elektronik

An alternative approach is to base the wireless connectivity around a third-party module. The modules are fully assembled, optimised, and tested solutions that enable 'drop-in' wireless connectivity. In most cases, the module will already be certified for use in global markets, saving the designer the time and money needed to pass RF regulation certification.

There are some downsides to module use. These include increased expense (depending on volume), larger end-product size, reliance on a single vendor and its ability to ship in volume, and (sometimes) a reduced number of accessible pins relative to the SoC upon which the module is based. But if design simplicity and faster-time-to-market outweigh these downsides, then a module is the answer.

One example that uses the Nordic nRF52840 at its heart is Würth Elektronik's Setebos-I 2.4GHz radio module 2611011024020. The compact module measures 12 × 8 × 2mm, has a built-in antenna, a cover to minimise electromagnetic interference (EMI), and comes with firmware to support Bluetooth 5.1 as well as proprietary 2.4GHz protocols (Figure 3). As described above, the SoC at the heart of the module is also capable of supporting Thread and Zigbee – with the addition of appropriate firmware.

The module accepts a 1.8-to-3.6-volt input, and when in sleep mode, draws just 0.4 microamperes (µA). Its operating frequency covers the Industrial, Scientific, and Medical (ISM) band, which is centred on 2.44GHz (2.402 to 2.480GHz).

Pin	Pad	Description	I/O
MODE_1	9	Operation mode pin	Input
BUSY	10	Busy pin	Output
LED_1	11	RF transmit indication	Output
LED_2	12	RF receive indication	Output
UTXD	13	UART transmit	Output
URXD	14	UART receive	Input
/RTS	15	Request to send	Output
/CTS	16	Clear to send	Input
WAKE_UP	17	Wake-up from sleep	Input
GND	18	Negative supply voltage	Supply
RPS	B1	Radio protocol selection (Proprietary or Bluetooth Low Energy 5.1)	Input
B2	B2	Programmable GPIO	I/O
B3	B3	Programmable GPIO	I/O
B4	B4	Programmable GPIO	I/O
B5	B5	Programmable GPIO	I/O
B6	B6	Programmable GPIO	I/O

Table 1: Shown are the Setebos-I 2.4GHz radio module's pin designations. LED outputs can be used to indicate radio transmission and reception. Image source: Würth Elektronik

In ideal conditions, with 0 dBm output power, the line-of-site range between the transmitter and the receiver is up to 600m, and the maximum Bluetooth LE throughput is 2Mbits/s. The module features a built-in quarter wavelength (3.13cm) antenna, but it is also possible to boost the range by connecting an external antenna to the aforementioned ANT terminal on the module (Figure 4).

The Setebos-I radio module provides access to the nRF52840 SoC's pins via solder pads. Table 1 lists the function of each module pin. Pins 'B2' to 'B6' are programmable GPIOs that are useful for connecting sensors such as temperature, humidity, and air quality devices.

Short-range wireless product certification

While the 2.4GHz band is a license-free spectrum allocation, radio devices operating in the band are still required to meet local regulations such as those dictated by the US Federal Communications Commission (FCC), European Declaration of Conformity (CE), or Telecom Engineering Centre (TELEC) in Japan. Passing the regulations requires submitting a product for testing and certification, which can be time-consuming and expensive. If the RF product fails any part of the test, a completely new submission must be made. If the module is going to be used in Bluetooth mode, it will also need a Bluetooth listing from the Bluetooth Special Interest Group (SIG).

Certification for the module doesn't automatically confer certification onto the end product using the module. But it does typically turn the certification for end products

Figure 5: Example of an ID label appended to the Setebos-I module to show that it has passed CE and FCC RF certification. Certification can generally be inherited by the end product without retesting through some simple paperwork. Image source: Würth Elektronik

into a paperwork exercise rather than an extensive retesting task – providing they don't use additional wireless devices such as Wi-Fi. The same is generally true when obtaining the Bluetooth listing. Once certified, products using the module carry a label indicating FCC, CE, and other relevant ID numbers (Figure 5).

Module makers typically go to the extent of obtaining RF certification (and Bluetooth listing if appropriate) for their modules for the regions in which they intend to sell the products. Würth Elektronik has done this for the Setebos-I radio module, though it must be used with the factory firmware. In the case of Bluetooth operation, the module is pre-certified, provided it is used with Nordic's S140 Bluetooth LE factory stack or a stack supplied via the company's nRF Connect SDK software development kit.

The Würth and Nordic firmware is robust and proven for any application. But if the designer decides to reprogram the module with either an open-standard Bluetooth LE or 2.4GHz proprietary stack, or one from an alternative commercial supplier, they will need to start the certification programs from scratch for the regions of intended operation.

Development tools for the Setebos-I radio module

For advanced developers, Nordic's nRF Connect SDK offers a comprehensive design tool for building application software for the nRF52840 SoC. The nRF Connect for VS Code extension is the recommended integrated development environment (IDE) in which to run the nRF Connect SDK. It is also possible to use the nRF Connect SDK to upload an alternative Bluetooth LE or 2.4GHz proprietary protocol to the nRF52840. (Refer to comments above about the impact this has on module certification.)

The nRF Connect SDK works with the nRF52840 DK development kit (Figure 6). The hardware features the nRF52840 SoC and supports prototype code development and testing. Once the application software is ready, the nRF52840 DK can act as a J-LINK programmer to port the code to the Setebos-I radio module's nRF52840's flash memory via the module's 'SWDCLK' and 'SWDIO' pins.

Application software built using Nordic's development tools is designed to run on the nRF52840's embedded Arm Cortex-M4 MCU.

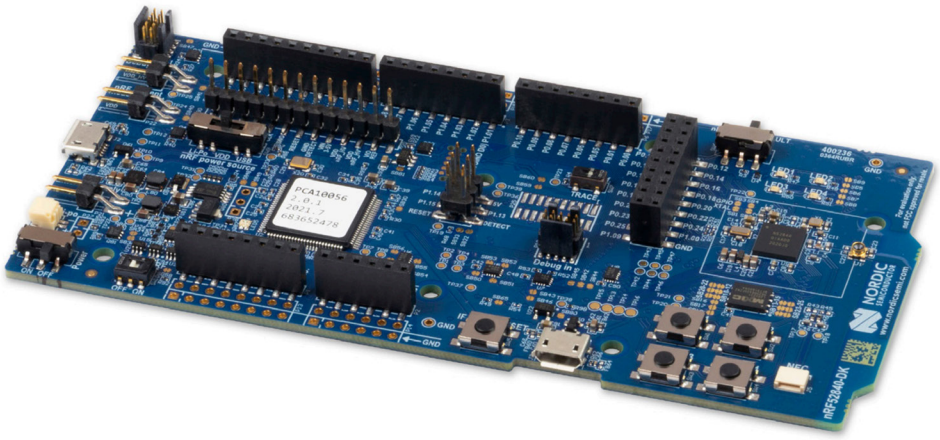


Figure 6: Nordic's nRF52840 DK can be used to develop and test application software. The development kit can then be used to program other nRF52840 SoCs, such as the one used on the Setebos-I module. Image source: Nordic Semiconductor

But it might be the case that the end product is already equipped with another MCU, and the developer wants to use that to run application code and supervise wireless connectivity. Or, the developer might be more familiar with development tools for other popular host microprocessors, such as STMicroelectronics' STM32F429ZIY6TR. This processor is also based on an Arm Cortex-M4 core.

To enable an external host microprocessor to run application software and supervise the nRF52840 SoC, Würth Elektronik offers its Wireless Connectivity SDK. The SDK is a set of software tools that enable quick software integration of the company's wireless modules with many popular processors, including the STM32F429ZIY6TR chip. The SDK consists of drivers and examples in C that use the UART, SPI, or USB peripherals of the underlying platform to communicate with the attached radio device (Figure 7). The developer simply ports the SDK C code to the host processor. This significantly reduces the time needed to design a software interface for the radio module.

The Setebos-I radio module uses a 'command interface' for configuration and operation tasks. This interface provides up to 30 commands that accomplish tasks like updating various device settings, transmitting, and receiving data, and putting the module into one of a variety of low-power modes. The connected radio device must run in command mode to use the Wireless Connectivity SDK.

Conclusion

It can be tricky to decide on a single wireless protocol for a connected product, and even more challenging to design the radio circuit from scratch. A radio module such as Würth Elektronik's Setebos-I not only offers flexibility in the choice of protocol, but it also offers a drop-in connectivity solution that meets the regulatory requirements of various operating regions. The Sebetos-1 module comes with Würth's Wireless Connectivity SDK, which makes it simple and quick for developers to control the module using their own choice of host MCU.

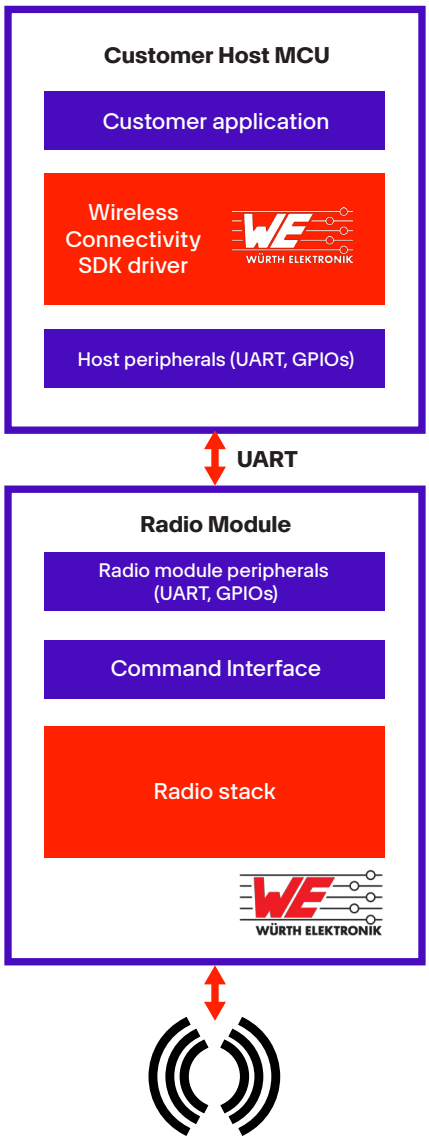


Figure 7: The Wireless Connectivity SDK Driver makes it easy for developers to drive the Setebos-I radio module via a UART port using an external host microprocessor.
Image source: Würth Elektronik


New look
Same focus
We've refreshed our brand, but our commitment to customer-centric experiences remains constant.
And as always, our goal is to accelerate progress for every designer, buyer, and builder.
Learn more at digikey.com
DigiKey
we get technical
DigiKey is an authorized distributor for all supplier partners. New products added daily. DigiKey and DigiKey Electronics are registered trademarks of DigiKey Electronics in the U.S. and other countries. © 2023 DigiKey Electronics, 701 Brooks Ave. South, Thief River Falls, MN 56701, USA
ECIA MEMBER
Supporting The Authorized Channel