LEARNING MADE EASY

Qorvo 2nd Special Edition

Internet of Things

for dummies®
A Wiley Brand

Demystify IoT communication

Learn tomorrow's smart home technology

Discover the IoT ecosystem

Brought to you by

qorvo

all around you

About Qorvo

Qorvo (Nasdaq: QRVO) makes a better world possible by providing innovative radio-frequency (RF) solutions at the center of connectivity. We combine product and technology leadership, systems-level expertise, and global manufacturing scale to quickly solve our customers' most complex technical challenges. Qorvo serves diverse high-growth segments of large global markets, including advanced wireless devices, wired and wireless networks, and defense radar and communications. We also leverage unique competitive strengths to advance 5G networks, cloud computing, the Internet of Things, and other emerging applications that expand the global framework interconnecting people, places, and things.

Visit www.qorvo.com to learn how Qorvo connects the world.

Internet of Things

Qorvo 2nd Special Edition

by Cees Links, Tony Testa, John Anderton, Wilco Van Hoogstraeten, David Schnaufer, and Cindy Warschauer

for dummies®
A Wiley Brand

Internet of Things For Dummies®, Qorvo 2nd Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-79822-4 (pbk); ISBN 978-1-119-79820-0 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: Molly Daugherty

Production Editor: Mohammed Zafar Ali

Special Help: Cees Links, Tony Testa, John Anderton, David Schnaufer, Wilco Van Hoogstraeten, Cindy Warschauer

Table of Contents

Introduction

The Internet of Things (IoT) is creating a new world — a quantifiable and measurable world — in which people can better manage their lives, cities can better manage their infrastructure, and companies can better manage their businesses. This new smart connected world will offer fundamental changes to consumers and to society, and it will profoundly transform entire industries. The rise of the IoT will create many significant improvements in our world and in our daily lives by helping us make better decisions faster with timely and higher-quality information.

About This Book

If you're interested in learning about how the IoT works, you've come to the right place. This book explains the IoT with simple language and examples that help you understand all the buzzwords and standards. You'll learn about the standards, protocols, and architectures that the IoT uses to operate, and look at the ways that the IoT powers the "smart homes" of today — and tomorrow.

Icons Used in This Book

To make it easy to navigate to the most useful information, these icons highlight key text:

TIP

The Tip icon flags information that can save you time and effort.

WARNING

Watch out for these potential pitfalls on the road ahead.

REMEMBER

Take careful note of these key takeaway points.

TECHNICAL STUFF

Read these optional passages if you crave a more technical explanation.

Beyond the Book

After reading this book, you'll probably want to find out more about the IoT. You can find out more by going to `www.qorvo.com/applications/internet-of-things`.

IN THIS CHAPTER

- Exploring the IoT market
- Understanding how the IoT will impact businesses, cities, and consumers
- Identifying the technologies behind the IoT
- Learning how the ecosystem of IoT standards align and what's changing

Chapter 1
Understanding the Internet of Things

In this chapter, I provide the basics of the Internet of Things (IoT) and its applications, key market trends, and some of the key IoT technologies. I also show you how the many standards are used and how the market is shifting toward greater interoperability.

What Is the Internet of Things?

To understand the IoT, it helps to quickly retrace how the Internet evolved as a whole.

The Internet started out as a relatively small number of military and government computers linked by wired connections. Over time, the Internet expanded and became available to millions of people across the world, and the World Wide Web made it possible for anyone to publish information for public consumption. The next leap forward came from the rapid spread of wireless connectivity. With the help of Wi-Fi and cellular communications, an enormous expansion followed. Smartphones and other Internet-connected mobile devices untethered Internet connectivity from specific locations, making it available nearly everywhere.

It wasn't just computers using the Internet, though. Many other types of devices began including simple computing and networking capabilities. The term *Internet of Things* was coined in the early 2000s to describe the ever-broadening range of Internet-connected objects and their uses. In 2005, the International Telecommunication Union (ITU) formally recognized the term. The ITU defines the IoT as "consisting of smart objects that connect to the Internet and communicate with each other with minimal or no human intervention." These objects generally connect via a gateway to an IoT platform, which consists of software tools and services that collect data from sensors, controllers, and other devices.

Today, the IoT is about connecting many different types of objects to the Internet, such as sensors, hands-free controllers, and remote monitoring devices. According to Cisco, we've already passed the point where many more "things" or objects are connected to the Internet than people — in fact, we passed that point more than ten years ago.


TECHNICAL STUFF

Figure 1-1 summarizes what's going on. At the Sense & Connect Layer, the platform connects the IoT hardware to network applications that perform data processing and storage. In the middle is the Platform Layer, where the data is stored, secured, processed, and analyzed. At the End-User Layer, it connects to end-user applications that monitor and interpret the data from IoT devices and sends instructions that tell the devices to perform actions such as locking your front door or raising the garage door.

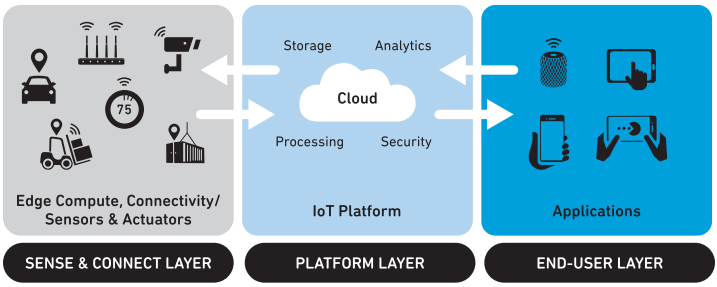


FIGURE 1-1: The layers of the IoT.

REMEMBER

IoT platforms generally provide services that are

- **Adaptable:** IoT systems can dynamically adapt to changing contexts, acting based on operating conditions, user input, or sensed information.
- **Uniquely identifiable:** Each IoT device has a unique identity, such as an Internet Protocol (IP) address. These IoT device addresses enable users to query, monitor, and control the device remotely.
- **Self-configurable:** IoT devices in the network can self-configure to enable many IoT-enabled machines to work with each other to provide full system functionality.
- **Network integrated:** IoT devices are integrated into the IoT network to enable communication between the nodes, gateways, and infrastructure.
- **Intelligent decision making:** IoT devices can make decisions that enable them to adapt to changing conditions.

Surveying IoT Markets and Trends

Consumers, businesses, and governments are all rapidly adopting the IoT. Key markets include home electronics (such as TVs and other home entertainment systems), home appliances (such as washers and dryers), automotive components and driver interfaces, and security systems. The IoT also plays heavily in wearable devices such as smart watches, fitness monitors, and health monitors. In cities, local governments are implementing the IoT to increase efficiencies and reduce expenses. Even the military is exploiting the IoT, implementing robots for surveillance and human-wearable biometrics for combat.

The future looks even brighter, according to research firms that study technology trends. Here are a few predictions that illustrate the extraordinary growth potential of the IoT:

- According to Statista, the global IoT market is projected to grow to $1.6 trillion by 2025.
- According to Frost & Sullivan, the top 600 smart cities are expected to account for 60 percent of the global gross domestic product (GDP) in 2025. Smart cities will represent a $2 trillion technology market value by 2025 with artificial intelligence (AI) and IoT being the main driving force.
- According to Strategy Analytics, the number of smart-home devices purchased is expected to exceed 1.94 billion by 2023, with device sales exceeding $78 billion by that time as well.
- According to Grand View Research, healthcare IoT is projected to be worth $534.3 billion by 2025.
- According to Grand View Research, precision agriculture, which uses IoT technology to make every agricultural process as streamlined and efficient as possible, is predicted to become a $43 billion industry by 2025.

Identifying the Wireless Standards That Enable the IoT

A wide variety of wireless technology standards are currently used to connect IoT devices. Some are familiar technologies like Bluetooth, Wi-Fi, and Zigbee, while others are less-common proprietary solutions. Figure 1-2 summarizes the present landscape. It's divided into three sections based on range. As shown in Figure 1-2, the overall IoT ecosystem has become confusing and difficult to manage from a user perspective due to the many different standards in use.

Companies that make IoT products generally select the standard(s) to use based on range and data type. For example, they may need to communicate media content or sense-and-control data. With an array of standard technologies to choose from, as well as some proprietary ones, system designers can select the best technology to optimize their end-user device performance. But this doesn't always make things easy for the end user.

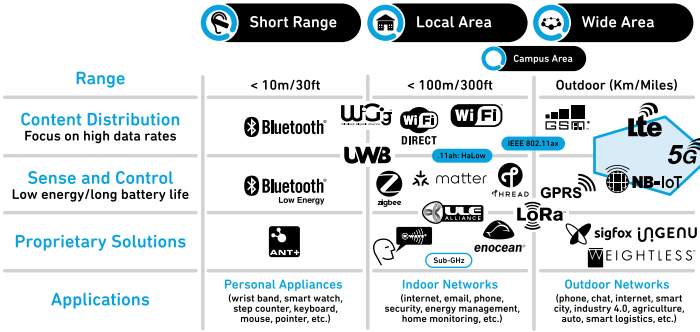


FIGURE 1-2: Early stages of the IoT, a highly fragmented standards ecosystem.

The goal: Interoperability

Interoperability is the ability of a product or system to work with other products or systems, both at present and in the future, without any restrictions.

Consumers want all their wireless home devices to communicate in a plug-and-play fashion. They don't want to go through the chore of making sure that the new IoT device they want to buy will work with their current network. They want to be able to buy any wireless product and have it work automatically. Today, however, that's just not possible. Buying a connected door lock or light bulb is complicated because you need to consider how it will communicate with your other home devices, including those that use Alexa, Google Assistant, or Siri.

WARNING

Some manufacturers are adopting wireless standards for basic connectivity but adding their own proprietary solutions for controlling and interacting with IoT devices. This practice comes at a price, however, especially for users who must navigate a complicated purchase and installation process because their new devices don't fit as easily as they expected into their existing network.

Matter to the rescue

To increase interoperability and reduce the overall complexity for consumers, industry leaders like Amazon, Apple, Google, and Samsung are getting together to support a single new standard called Matter. As shown in Figure 1-3, the ecosystem can be much less complicated if it uses fewer standards and a protocol like Matter. Matter will make IoT devices much easier to use for consumers, while also unifying the protocol landscape.

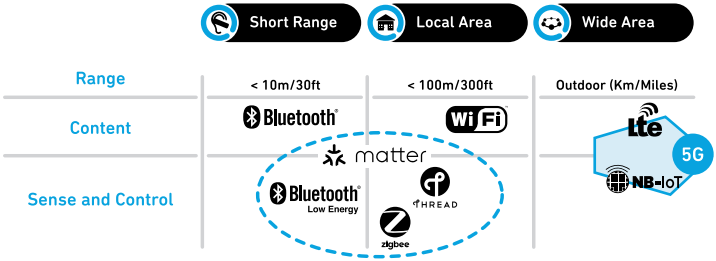


FIGURE 1-3: The open IoT standards in the marketplace.

Matter is still in its infancy, but it represents a step in the right direction. The overall goal of Matter is to provide plug-and-play consumer IoT devices for the connected home. It will deliver a layer on top of the Internet Protocol (IP) that will include a set of predefined schemes for all Matter-connected devices. This will enable devices to understand what kind of objects they're communicating with and what those objects can do.

For example, a thermostat may share data about temperature and fan operation. The new Matter standard will support both applications with a common way to communicate to the thermostat and fan.

Matter will enable end devices or nodes, which are the "things" of the IoT, and these "things" will talk with the many Wi-Fi network pods.

TECHNICAL STUFF

Pods, are strategically positioned throughout the network, such as a home, and automatically connect themselves to the main router. This main router then connects to the Internet. This eliminates wireless dead zones and the need to be close to a router or repeater, thus extending the network signal.

In summary, Matter is allowing the convergence of several elements of the IoT, such as Wi-Fi, Zigbee, Bluetooth, and Bluetooth Low Energy. Bringing these individual standards of the IoT together, will help the IoT further enable interoperability — the entire ecosystem will be more plug-and-play.

Ultimately, Matter will allow the average nontechnical consumer to choose a favorite IoT product without being locked into a proprietary non-interoperable ecosystem.

Ultra-wideband

Also shown in Figure 1-2 is another up-and-coming technology called *ultra-wideband* (UWB). UWB is rapidly being adopted for micro-location-based IoT solutions. It enables accurate and reliable device distance and location measurement, both indoors and outdoors, while consuming very little power.

UWB is a radio technology based on the IEEE 802.15.4a and 802.15.4z standards that enables a more precise measure of the Time of Flight (ToF) of a radio signal, leading to centimeter accuracy distance/location measurements. It's capable of communicating at up to 27 Mbps while using extremely little energy, so devices can operate on a coin-size battery for many years without needing to be recharged or replaced. UWB also offers a new way of securely communicating over wireless, opening the door for new forms of secure transactions.

This technology standard will create new IoT use cases in areas such as the smart home, secure automobile keyless entry, secure payment processing, and Industry 4.0. You can explore UWB further in another Qorvo book called *Ultra-Wideband For Dummies,* Qorvo Special Edition located on Qorvo's Design Hub (`www.qorvo.com/design-hub/ebooks`).

UWB fits nicely into the IoT ecosystem. It's secure, accurate, and battery operated, and it can be used in many applications in the IoT. Although it will fit in many applications, some yet to be explored, UWB will initially be targeting use cases in hands-free access control, location-based services, and peer-to-peer applications. It's already one of the radio-frequency (RF) chains inside new smartphones, enabling smart car access, secure building access, and smart home device connectivity.

People and businesses want to be able to locate and find pretty much anything in real time, whatever the size. For IoT and smart home applications, UWB asset tagging is much more accurate than previously used Bluetooth or Wi-Fi. With Bluetooth and Wi-Fi, the asset tag could allow you to get to a roundabout location, but using UWB, you receive an exact location. For example, a Bluetooth tag would show that you left your keys inside a room or area in the living room. But UWB would show you that the asset tag or your keys have fallen under the cushion on your couch.

UWB also opens a new world in using gestures, meaning voice commands can sometimes be secondary to enabling applications. For example, lights would automatically turn on when you enter a room or your computer would turn on when you sit down at the desk. UWB brings these types of applications to reality, kicking off many new and revolutionary use cases.

To make sure that interoperability is maintained with using UWB, the consortium Fine Ranging (FiRa) is already regrouping more than 50 companies from the semiconductor, mobile, infrastructure, and consumer space to actively work on the definition of protocols to guarantee interoperability. This will make it possible for developers to use UWB in many new applications, such as augmented reality, smart home applications, and mobile payments.

5G and Wi-Fi 6/6E

5G and Wi-Fi 6/6E are two pivotal technologies advancing the use of the IoT, as businesses, homes, and cities around the globe move toward digitizing their wireless and wired ecosystems. These two technologies are driving many improvements in integration, packaging, and performance.

Wi-Fi 6/6E, the latest version of the Wi-Fi standard, offers much higher data rates and coverage than previous versions. This newer edition also extends the security protocol, making it more difficult to hack device passwords.

Wi-Fi 6 provides faster speeds, more capacity (both in data rate and connected users or devices), lower power consumption, and improved security. Wi-Fi 6E will offer the features and capabilities of Wi-Fi 6 — including higher performance, lower latency, and faster data rates — while extending Wi-Fi into the 6 GHz realm. It will also more than double the capacity of Wi-Fi 6 spectrum, providing an additional seven 160 MHz channels of non-overlapping bandwidth. These additional channels will reduce congestion, boost performance, and reduce latency.

Wi-Fi 6/6E covers small-scale networks that support IoT devices such as smart thermostats and security cameras. In contrast, cellular networks like 5G provide global coverage for mobile devices. Together, 5G and Wi-Fi 6/6E help the IoT realize its full potential.

5G networks can be configured to meet the needs of many different applications, each supporting different types of user devices. The applications can be broadly divided into three categories:

- Enhanced mobile broadband (eMMB)
- Ultra-reliable low-latency (uRLLC)
- Massive machine-type communications (mMTC)

The IoT includes both mMTC and uRLLC applications.

These 5G applications will open the door to even more IoT devices and data. Moreover, 5G will increase the adoption of edge computing for faster data processing close to the point of action, which will provide a springboard to further drive the IoT within our wireless and wired ecosystems. However, unlike Wi-Fi, which is an unlicensed technology, cellular 5G is a licensed service, so deploying new device connections may involve paying additional fees.

Explore more on 5G at `www.qorvo.com/design-hub/ebooks/5g-rf-for-dummies`.

A BIT MORE ON WI-FI 6 AND 6E

Wi-Fi 6E will offer the features and capabilities of Wi-Fi 6 — including higher performance, low latency, and faster data rates. It also extends Wi-Fi 6 into the 6 GHz realm.

This additional 6 GHz spectrum availability has been referred to as a monumental addition since Wi-Fi first became offered. The 6 GHz Wi-Fi 6E spectrum provides additional non-overlapping channels, which more than doubles the capacity of current Wi-Fi 6 spectrum.

Wi-Fi 6 operates in 2.4 GHz and 5 GHz bands up to 5835 MHz. For Wi-Fi 6E, the Wi-Fi Alliance allows for fourteen 80 MHz channels and seven 160 MHz channels. Wi-Fi 6E adds seven 160 MHz channels in the frequency range from 5,925 to 7,125 MHz.

Wi-Fi 6E is a Wi-Fi 6 standard implementation. This new 6 GHz spectrum will work similarly to enhance and expand Wi-Fi 6 beyond the

(continued)

(continued)

5 GHz band, by offering additional non-overlapping channels. These additional channels will reduce congestion — especially in areas where several networks are operating simultaneously. By offering the addition of seven channels with 160 MHz each, it will boost performance and reduce latency while in range, but as with other high-frequency ranges, it will still struggle on the distance and obstacle signal attenuation it can transmit and receive, unlike the 2.4 GHz Wi-Fi channel range.

Wi-Fi 6E boosts performance and uses multiple-input multiple-output (MIMO) and open spectrum to overcome the inherent range challenges in the high-frequency channels, ensuring full home or building coverage and providing optimal throughput/capacity.

Wi-Fi 6/6E will also help provide the same experience to many more users on a single network. In addition, Wi-Fi 6 will have speeds of 1.2 Gbps per stream, where Wi-Fi 6E will meet theoretical speeds from 5.4 Gbps to 10 Gbps, which is a big improvement over both Wi-Fi 5 and Wi-Fi 6.

IN THIS CHAPTER

- Exploring the IoT ecosystem
- Finding out about the IoT architectures
- Looking at IoT networking protocols in more detail

Chapter 2
IoT Architecture and Technology Protocols

In this chapter, I introduce you to the technology architectures used to support Internet of Things (IoT) applications and examine some of the key IoT technologies and wireless protocols in more detail.

Digging into the IoT Ecosystem

From a high-level perspective, the IoT landscape is a heterogeneous network, with the cloud computing layer being responsible for retrieving and acting on information gained from other layers. Figure 2-1 provides a basic picture of that.

IoT-related data can be stored in multiple locations within an IoT network. Sensors, gateways, and local devices in the network and cloud-based systems can store differing amounts of data.

Cloud computing

The cloud computing layer at the center of Figure 2-1 plays a critical role in the ecosystem, storing a vast amount of information and making decisions based on that data. It enables effective integration of data from the solution components. Adding the cloud to the IoT can also add security, availability, scalability, and performance, because cloud storage/database providers embrace those capabilities in order to achieve industry success.

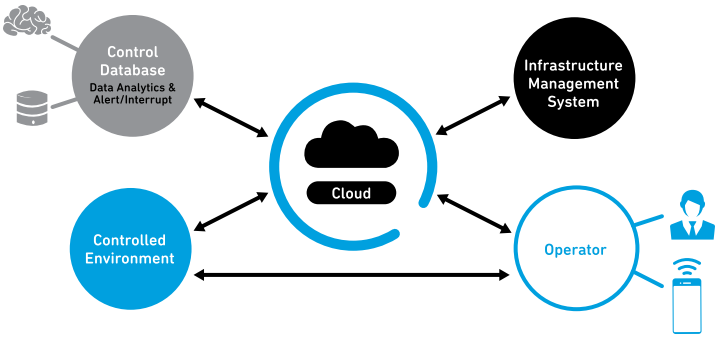


FIGURE 2-1: The IoT ecosystem model.

The IoT smart home, for example, relies heavily on the cloud for its computing capabilities. As shown in Figure 2-2, the smart home has a sensor and home connectivity layer that collects data from different nodes and then provides this information to cloud servers for decision making.

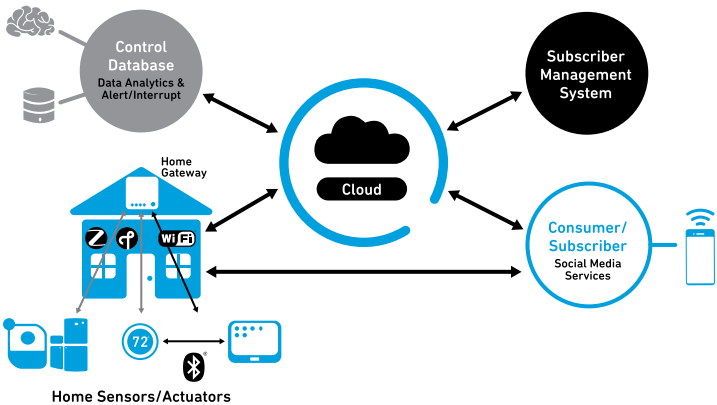


FIGURE 2-2: The IoT ecosystem supporting the smart home.

Edge computing

Sometimes sending IoT data to the cloud for processing doesn't make sense. Although the cloud can crunch large amounts of data, it has downsides, such as communication latency. Plus, sometimes the cloud isn't available, or a faster processing turnaround time is required.

This is where edge computing can help. *Edge computing* occurs when data is processed and stored at its source on the sensor or gateway, and the network only leverages the cloud if additional processing is required. Some endpoint devices don't always send data back to the cloud. Instead, they use edge computing to store and process the data at the source. This helps enable a more real-time experience for the end user. It also helps maintain the security of the network.

Edge computing can be especially useful if there are constraints on power or bandwidth. Using sensors to perform useful processing on data streams at the edge of the network reduces power consumption and uses bandwidth efficiently. Edge computing also helps protect user privacy by storing and analyzing data at the source rather than sending identifiable information to the cloud. As IoT technology advances and latency becomes a bigger issue, edge computing will become more widespread to enable real-time processing.

Examining the IoT Architecture

Some IoT applications have already come to fruition, such as the ability to wirelessly control a home thermostat or use a phone to open car doors. But the potential future applications of the IoT are much broader and larger in scale. Imagine using your phone to find a parking space or owning a refrigerator that knows when items need to be replenished and orders them automatically. Imagine sensors in bridges and other infrastructure that automatically inform engineers when repair or maintenance is required. Imagine location-based technology that informs you when you're in close proximity to someone with a highly contagious illness or to a harmful substance or environment. These future applications will require IoT architecture platforms that perform a massive amount of data transfer and processing behind the scenes.

This IoT platform/architecture consists of several internally connected layers (refer to Figure 1-1). Here's a closer look at the individual components that exist within the IoT platform layers:

- **Sensors and actuators**: IoT sensors and actuators measure things like temperature, sound, moisture, and vibration. In a typical IoT smart home, a smart device like a thermostat has

an embedded communication unit that connects to the home network. The sensors and actuators in the thermostat convert these physical measurements into electrical values that drive the system.

- **IoT gateways:** The gateway carries data between the local network and the Internet. The electronic values from sensors and actuators are received and then uploaded into the local network using network protocols such as Bluetooth, Bluetooth Low Energy (BLE), Cellular, LoRaWAN, Thread, Wi-Fi, or Zigbee. The gateway creates a meshed backbone to distribute the collected data and send responses to devices.
- **Cloud-based IoT platform:** The data transmitted through the gateway is stored and processed within a cloud-based IoT platform or in a company's data centers. This data is then used to perform intelligent actions and make decisions.
- **Applications:** Ultimately, the data from IoT devices is used in applications to help people or organizations make better decisions or take specific actions. The applications push information from the cloud into applications on smartphones, tablets, or computers. The application layer is the most important to users because it's their interface to the IoT network, allowing them to control and monitor the many elements of the IoT system, sometimes in real time.

Looking at Some IoT Protocols

Communication protocols form the backbone of IoT systems, connecting IoT devices to the network and ultimately to applications and users. These standards-based and proprietary protocols enable data to pass between the different layers of the IoT architecture by defining data exchange formats, data encoding, addressing schemes for devices, and the way that data packets are routed from node to destination.

The IoT ecosystem includes a range of different protocols supporting short-range, local, and wide area networks, all of which coexist. Each technology has specific characteristics in terms of range, sensing and control, and the ability to transmit different types of information (refer to Figures 1-2 and 1-3). Together, these technologies can provide seamless coverage at all wireless

ranges and capabilities. For example, Bluetooth works well for short-range applications, while narrowband IoT (NB-IoT) works well for long-range applications.

Here is a summary of some key network protocols:

- The **IEEE 802.15.4 standard** is a collection of Low-Rate Wireless Personal Area Network (LR-WPAN) standards. These standards provide low-cost, low-speed communications for power-constrained devices. They form the basis of specifications for high-level communication protocols such as Zigbee. Zigbee is a mesh network designed for low-power operation, used in smart homes and in smart-energy applications for utilities. Zigbee is based on the IEEE 802.15.4 Physical Layer (PHY) and Medium Access Control (MAC) standards.
- **Wi-Fi** is a collection of IEEE 802.11 Wireless Local Area Network (WLAN) communication standards. Wi-Fi provides high data rates to both indoor and outdoor locations and is very widely used.
- **Bluetooth** is an open standard maintained by the Bluetooth Special Interest Group (SIG). It is a low-cost wireless communication technology suitable for data transmission between mobile devices over short distances, such as 8 to 10 meters. It's used in applications like audio streaming, cars, speakers, and headsets.
- **Bluetooth Low Energy (BLE)** is part of the Bluetooth standard. It's designed specifically for lower-power operation. BLE devices commonly use coin cell batteries to operate. BLE is used in IoT devices such as light bulbs and light switches.
- **Thread** is a low-power, secure, and Internet-based mesh networking technology for IoT products. In 2014, the Thread Group was formed as a working group to help the adoption of Thread. Thread supports existing IPv6-based connectivity standards, on its secure, low-power, mesh network.
- **LoRa** is for long-range communications and is a low-power wide-area network (LPWAN) protocol developed by LoRa Alliance. This technology is optimal for enabling sensors for large-scale agriculture applications.

- **Cellular standards** like 5G provide a network backbone for IoT services, supporting both high data rates and long-range communications. A commonly used cellular IoT standard is NB-IoT, used in smart parking, utility management, and manufacturing automation.

These messaging protocols are used to share data across devices and with the cloud. The IoT protocols are a critical part of the IoT technology stack and, without them, hardware simply wouldn't work. IoT protocols enable the IoT device to exchange data in a controlled and meaningful way.

For example, smart devices of the IoT are called "smart" because not only are they able to talk with each other, but if they encounter problems they can automatically mitigate the issue or call for help via the network. This interaction is only possible through protocol communications or a common language that the IoT devices are given.

IN THIS CHAPTER

- Discovering how smart-home IoT sensors, beacons, and actuators communicate
- Understanding how mesh/one pod per room communication is enabling the IoT smart home
- Identifying the importance of real-time smart-home connectivity
- Seeing what the future looks like in the IoT

Chapter 3
The Smart Home of Today and Tomorrow

In this chapter, I take a deep dive into how the Internet of Things (IoT) powers the smart home and how mesh/one pod per room networks enable IoT connectivity. I also look at some IoT challenges and how new advancements in technology are helping to address them.

Surveying Today's Smart Home

The smart-home concept has taken off over the past several years, as manufacturers have developed an ever-broadening range of devices that can connect to home networks. Smart-home networks enable homeowners to use resources efficiently, control devices and appliances using voice commands, and make decisions based on data from devices. The potential of the smart home is vast: It can be used to improve energy efficiency, comfort, security, entertainment, and convenience.

Most of today's smart homes are equipped with many IoT devices, hubs, and sensors that communicate via the home network/gateway and ultimately with the cloud. The owner can control it all from anywhere in the household or even remotely through the Internet.

Smart-home systems may include several wireless connectivity standards relevant to home applications. Table 3-1 shows the characteristics of some of these standards and the differences between them. Moreover, these home networks may consist of several interconnected networks operating under the main gateway.

TABLE 3-1 Smart-Home Open Standards and Some Key Characteristics

Wireless Protocol	Wi-Fi	Zigbee/Thread	Bluetooth
Standard	IEEE 802.11	IEEE 802.15.4	IEEE 802.15.1
Frequency band	2.4, 5, 6 GHz	2.4 GHz	2.4 GHz
Nominal range	150 meters	100 meters	10 meters
Data rate	11 Gbps	250 Kbps	1 Mbps

Many of today's smart homes are made up of an ad hoc collection of nodes. A *node* is a piece of hardware that has its own unique address on the network; a node can be either a device or a hub:

- **Devices:** A *device* (for example, a thermostat or a light bulb) generally has only one connection to the network. Devices may or may not need to keep track of real time, depending on their function.
- **Hubs:** A *hub* is a box that manages the network's traffic; it may have many connections because it connects to multiple devices. Hubs must keep track of real time to dispatch events efficiently and effectively.

A single-hub network consists of one hub node and one or more device nodes. The hub manages the exchange of events and information between the devices in the network. A multi-hub network contains more than one type of hub, as shown in Figure 3-1. The

network layout in Figure 3-1 has two hubs, each using a different network protocol (Bluetooth versus Zigbee). Individual devices connect to one of the hubs. The hubs are then connected to the gateway, which is able to communicate with both.

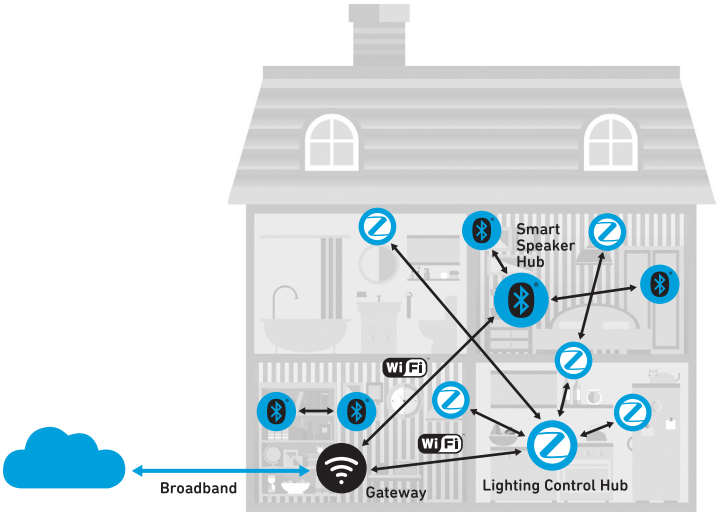


FIGURE 3-1: A smart home with Zigbee and Bluetooth hubs.

The Mesh Network/One Pod Per Room

To create a more connected smart home with more reliable communications, consumers are moving towards a newer topology known as a mesh network, which is sometimes referred to as *one pod per room.* Mesh networking easily extends wireless device ranges and provides consistent high data rates throughout offices, homes, and even outdoors. Additionally, mesh networking using one pod per room with multiprotocol capabilities can reduce the overhead of having multiple mesh systems within the home.

Mesh networks are an important development in the evolution of Wi-Fi, particularly in the smart home. Wi-Fi mesh systems include a router that connects to the main Internet connection and multiple satellite router-like devices, or nodes, placed around the home to provide full Wi-Fi home IoT coverage (see Figure 3-2). Such state-of-the-art mesh networks provide full redundancy and maximize network performance.

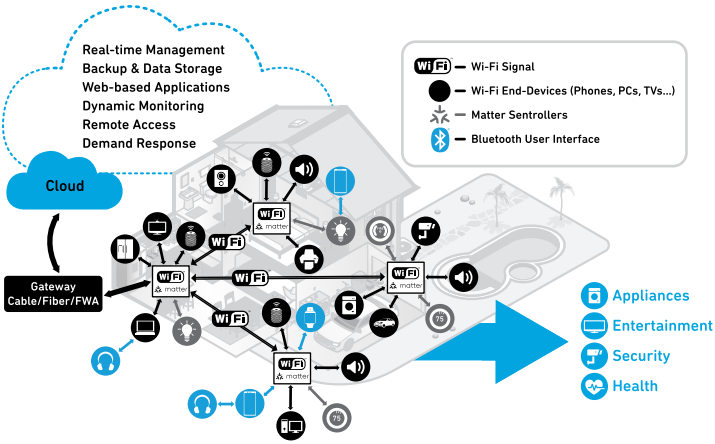


FIGURE 3-2: Smart-home devices in a mesh network infrastructure.

The more nodes, the farther the connection spreads, as shown in Figure 3-3. Mesh networks effectively extend signal range to an entire home, increasing reliability and enabling real-time communication with all devices. Advancements in Wi-Fi deployments allow for separating spectrum and ensuring dedicated backhaul data paths for information to and from the cloud. They also provide dedicated streams for devices. Moreover, some devices store data, which can save users money, further increase network reliability, and enable smarter data-driven applications.

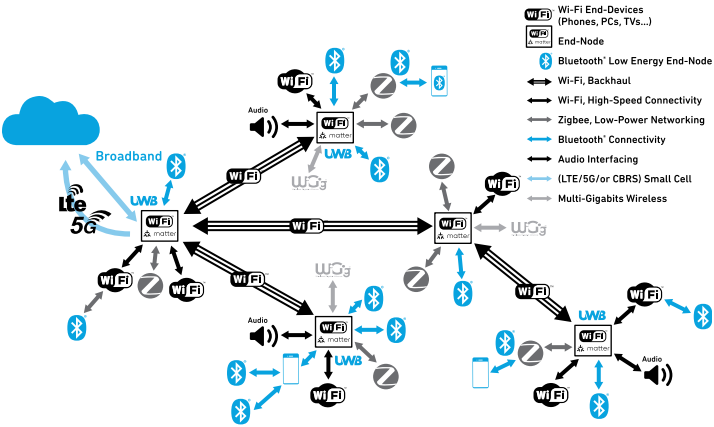


FIGURE 3-3: A distributed one pod per room IoT connectivity network.

A mesh network can also self-configure. Therefore, it can automatically incorporate a new node into the existing network without requiring adjustment by a network administrator. This makes the network even more adaptable and expandable. The mesh network can also self-heal by automatically finding the fastest and most reliable signal to transmit data, even when a node is blocked or loses signal.

Many of today's mesh networks use what's called tri-band Wi-Fi gateways and end-nodes. Tri-band Wi-Fi improves data capacity and coverage using 2.4 GHz, 5.2 GHz, and 5.6 GHz bands inside the gateways and end-nodes. In the tri-band system the second 5.6 GHz band acts as a dedicated communication line between two routers on the network to speed up the entire system by as much as 180 percent over older dual-band configured systems.

So, the advantages of Wi-Fi tri-band are clear. To begin, it helps to connect more wireless devices to the Internet using the faster 5 GHz band, and with Wi-Fi 6E, the 5 and 6 GHz band. And if your network is a mesh system with multiple routers scattered throughout the space, this higher band acts as a dedicated communication line between the two routers to speed up the entire system.

A tri-band system's third radio is also used for backhauling communications between mesh routers. So, it creates a dedicated wire solely for the purpose of data flow between routers. Although dual-band systems use the same Wi-Fi bandwidth to connect to other routers and access points, while in tri-band the end devices are immediately available for devices to connect. This improves efficiency by 50 percent especially as more network devices are added.

Plus, because this radio speed is faster, the fast connection speeds found at the DSL/cable modem don't stop there. Instead, they're carried through to the entire network. This is very beneficial for Wi-Fi video streaming to your smart TVs and cameras scattered throughout the smart homes of today and tomorrow.

To future-proof your existing home network system, you'll want to use a tri-band system. Gigabit services will soon be a reality for everyone, and implementing a tri-band system is the best way ensure capacity and speed in the future.

Another key development in mesh network systems is the introduction of filter technology to further increase capacity and range of the one pod per room topology. Using bandBoost filters help maximize capacity and range by boosting band isolation in tri-band mesh systems. Using edgeBoost filters boosts capacity and range by maximizing output power at the Wi-Fi channels close to the band edge. We further elaborate on these topics as well as how they address coexistence challenges in a mesh network in the following section.

As discussed in Chapter 1, leading manufacturers are developing a new standard called Matter to increase device interoperability and reduce complexity in mesh networks. During the transition toward Matter, multi-standard radios will be needed. These radios will future-proof the network to support migration to Matter and provide backward compatibility to connect nodes that use legacy standards. Though Matter is still being finalized, with rollout projected sometime in 2021, the collaboration among standards bodies and leading manufacturers is driving increased industry adoption.

Overcoming the Challenges

Let's next explore some of the challenges facing IoT smart-home network and device manufacturers.

Interoperability

Interoperability is the ability of systems, applications, and services to work together reliably in a predictable fashion. This helps to ensure that technology is easy to use and leads to speedy adoption. Every user expects their electronic wireless and wired devices to easily connect and work together with minimal effort, otherwise known as plug-and-play. It's no different in a smart-home network, which will be made up of numerous devices developed by many different manufacturers.

Interoperability and certification programs help to ensure interoperability between devices using several of the key IoT standards. The reason Wi-Fi has been so successful is because of its interoperability program run by the Wi-Fi Alliance, which has one of the world's most trusted certification regimes. There are tens of thousands of certified Wi-Fi devices with proven seamless connectivity.

Today, Zigbee 3.0 also provides the same level of interoperability, again due to partnerships and certifications. Communication between products using Zigbee and Thread is also certified because of partnerships between the two groups. Bluetooth also has certification programs that cover the entire protocol stack, as well as the application profile, helping Bluetooth and Bluetooth Low Energy (BLE) achieve an optimal communication experience.

These alliances and certifications have been critical in providing consolidation in a fragmented smart-home IoT device environment with a myriad of standards. Manufacturers of devices using these many protocols must adhere to these certification and alliance criteria to get their products approved prior to selling into the market. This ensures that users experience the plug-and-play interoperability they expect.

RF interference

Radio-frequency (RF) complexity in smart-home networks has increased with each generation of wireless technology. Many home RF communication devices use standards with overlapping or closely aligned frequency bands. Sometimes the bands are so close to each other they cause one communication band to interfere with the transmitting and receiving signals from the other.

IoT and 5G add yet another level of complexity, intensifying the challenges for smart-home device design engineers. Today's smart-home IoT devices must support many RF paths, with sometimes larger bandwidths, and maintain low power consumption — all without interference between standards and the data they're transmitting or receiving. With so many standards operating on one network, mitigating interference is imperative.

RF filters to mitigate interference

Luckily, advancements in RF filter technology have greatly decreased the potential for different protocol standards to interfere with each other. RF filters are evolving to support the expanded requirements of IoT, 5G, and Industry 4.0. Complex multi-filter modules such as bulk acoustic wave (BAW) are increasingly being used to address coexistence, capacity, and range in RF systems.

Additionally, smaller filter form factors are helping IoT product manufacturers squeeze increasingly complex RF front end (RFFE) architectures into tiny devices, by facilitating the development of integrated modules. At the same time, today's filter technology is

helping mitigate the problem of heat dissipation associated with higher frequencies and smaller form factors.

Different filters for different needs

Depending on the filtering need, different filters are used. Some filters optimize coexistence with other devices; others help improve system, capacity, range, and performance.

For example, coexistence filters (such as Qorvo coexBoost filters) are used in the RF path, targeting applications where signals need to operate simultaneously. These coexistence filters have steep bandedge skirts. They're crucial for maintaining signal quality and making sure that signals can coexist with other signals that use adjacent frequencies. This coexistence must be maintained on both the RF transmitter and receiver paths. An example of this is the need for coexistence between the band 40 cellular signal and the 2.4 GHz Wi-Fi band. Band 40 operates from 2,300 to 2,400 MHz, while the 2.4 GHz Wi-Fi band operates from 2,412 to 2,484 MHz. This means that the high end of the band 40 channel is only 12 MHz from the 2.4 GHz Wi-Fi band. So, steep filter skirts are required on both band 40 and the Wi-Fi band. These coexistence filters protect each band from interference by rejecting signals in the adjacent band.

Other filters are designed to help achieve maximum capacity and range performance. Examples are filters (such as Qorvo edgeBoost and bandBoost filters). These filters allow designers to push the limit on RFFE output power at the edge of each channel band while meeting the Federal Communications Commissions (FCC) requirement for power spectral density. They also help lower the spectral density to help increase output power performance, as shown in Figure 3-4. These filters enable operators and manufacturers to deliver high-speed data and greater bandwidth by using spectrum that may otherwise be unusable. As shown in Figure 3-4, using the bandedge filter improves power density by several decibels.

As a real-life example, let's assume you're in a house with several individuals using Wi-Fi and mobile phones, as shown in Figure 3-5. The 2.4 GHz Wi-Fi spectrum is divided into 11 channels, from channel 1 at the low end of the band to channel 11 at the high end. As an example, let's assume you're on Wi-Fi using channel 5, streaming a football game and experiencing no buffering or interruption. But then new mobile users arrive and begin to take over your channel 5 Wi-Fi capacity. The gateway unit adjusts and bounces you to channel 1 to free more capacity on channel 5.

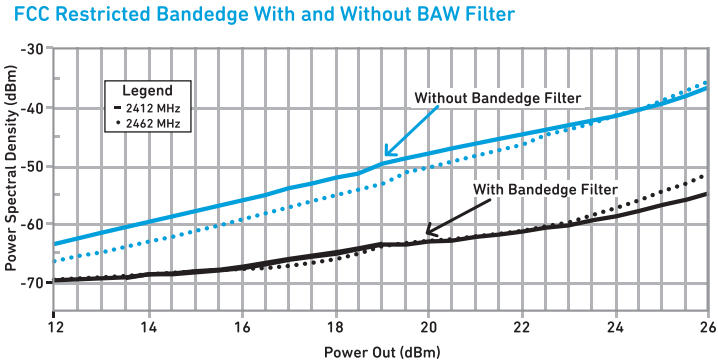


FIGURE 3-4: FCC restricted bandedge with and without bandedge filter (Qorvo edgeBoost filter).

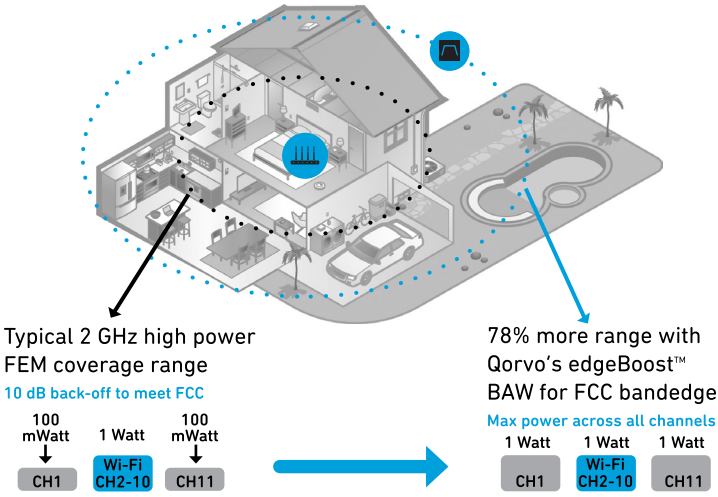


FIGURE 3-5: Filters that enable maximum coverage and throughput (Qorvo edgeBoost filters).

If the Wi-Fi unit doesn't have bandedge filters, your Wi-Fi strength and streaming degrade to the point where buffering occurs, interrupting your viewing and causing you to miss vital moments in the game. That's because in order to meet the FCC requirement, the gateway must back off its power in channel 1 so it doesn't interfere with adjacent cellular bands. However, if the gateway unit has bandedge filters, it doesn't need to back off power in channels 1 and 11, so you can continue streaming your game on channel 1 without buffering and the associated interruptions.

Maintaining a seamless, energy-efficient, and reliable connection

Some manufacturers create products that use several standards. This further enhances interoperability in IoT networks because it enables their product to communicate with a broader range of other devices. With dynamic multi-protocol support, a node can communicate with multiple devices using different standards.

For example, a smart-home network may include both Zigbee devices and BLE devices. In a mesh node with dynamic multi-protocol support for both Zigbee/Matter and BLE devices, the communication portion of the device automatically switches back and forth between these standards, communicating on one standard at a time.

Qorvo IoT communication products used in smart-home devices add yet another capability by supporting ConcurrentConnect technology, which continuously receives and translates communications, as shown in Figure 3-6. This additional innovation implements protocol switching in a faster, more reliable way to reduce data packet losses, while still maintaining dynamic multi-protocol support.

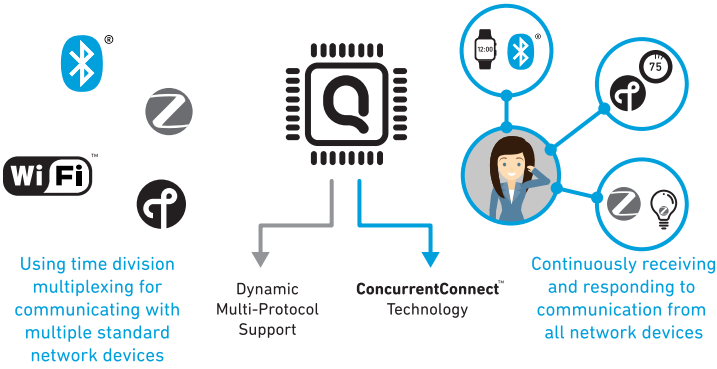


FIGURE 3-6: Dynamic multi-protocol support and a ConcurrentConnect integrated circuit.

For example, referring to Figure 3-6; on the left it shows that IoT communication products incorporate dynamic multiprotocol support. This multiprotocol support allows communication between several IoT devices that use different standards. Thus, allowing it to switch from one protocol to another when required. But

Qorvo adds another level of complexity called ConcurrentConnect technology in its IoT RF devices. The addition of ConcurrentConnect technology makes IoT device communication more reliable and seamless by incorporating the ability to continuously receive and transmit device communications from all network devices simultaneously. Therefore, the communication switch from each protocol is seamless, mitigating the need for repeat pinging and possible dropped communication.

Consider an actual network situation. Without ConcurrentConnect technology Zigbee/Matter and Bluetooth Low Energy (BLE) devices will switch back and forth between standards — communicating with one standard at a time. But the switching between protocols causes a lag, triggering dropped communications. While devices with ConcurrentConnect technology allows instantaneous switching from BLE to Zigbee/Matter with little or no dropped communications. This is because ConcurrentConnect technology eliminates the lag in protocol switching. Thus, communications will be faster, more efficient, more scalable, and able to receive more data packets in a shorter amount of time.

Creating an ease-of-use self-management IoT network

Most users of IoT networks want a plug-and-play scenario with little or minimal setup or interaction. We all just want it to work after powering up. This puts the ownership of ease-of-use on the product manufacturer. This challenge is not always an easy one to tackle, because each user's network is different. To help attain this goal, a mesh IoT network in the home should be self-managing and self-healing so that consumers can be assured of continuous operation without the need to get involved in the technical details of managing networks. The IoT network should be able to operate, monitor, and notify users of potential issues that occur prior to a full shutdown of the network. Individual nodes and gateways must operate and collaborate with each other while adapting to network failures and environmental changes. The subsystems in the smart-home network monitor signal strengths, battery life, and more — always adapting and notifying the user so that performance is optimized.

Mesh networking offers real-world advantages for IoT applications, because it's always available and accessible. A mesh network uses a self-healing algorithm that automatically chooses

the best route to send data even if some nodes have inadvertently lost their connection. The algorithm ensures that traffic is routed only through available and functioning connections. Thus, the mesh network continues operating even when some nodes are not working. Mesh networking also enables devices to communicate directly with each other without having to route all communications via the gateway.

Network security and privacy

Implementing adequate security and privacy measures can be a significant challenge in IoT deployment. Today's IoT networks are generally fragmented, using a variety of protocols and technologies, which makes security and privacy difficult to control.

This reality is a strong argument for standardization, which will help improve security and privacy. It will also provide greater ease of use and scalability, enabling users to easily add devices to the network. Standardization helps users create their own optimal IoT network design in a secure way.

Using a mesh network, as described earlier, puts control and security power in the palm of the owner's hands. Typically, these mesh systems are set up, controlled, and monitored using an app. The app helps with network setup and ensures that a secure password is set. The app also helps to manage network issues, check data speeds, setting of parental controls, and more. Some of the systems help the owner see who is connected to the system network at any time.

Updates on your computer and smartphone are necessary to keep those devices secure. The same goes for the mesh network. However, the mesh network, typically updates itself, leaving the owner without the worry of performing annoying actionable updates.

Some mesh networks also have pay subscription fees for enhanced security features, like protection from hackers, website threats, and security scans. Included in these subscriptions could also be security from threats against malware, viruses, hackers, and even cybercriminals.

If you have a smart home with network-connected security cameras, thermostats, and other IoT smart devices, a mesh system is a very helpful addition. The mesh system features can help protect the entire network, including these devices, from cyberattacks.

Power consumption

Fossil fuel levels across the globe are depleting at accelerated speeds. The pressure to reduce power consumption and provide a greener product is intensifying. This same pressure is being felt by manufacturers and suppliers producing today's IoT devices. This trend will only intensify as world leaders push for more green initiatives. Some of the IoT products use only coin-size batteries (some lasting up to ten years), but producing these batteries consumes fossil fuels. Plus, many IoT devices don't use coin-size batteries; instead, they use power from the grid. So, to keep power consumption requirements in check, software and hardware are sometimes being added to some of these IoT devices to ensure they're in sleep mode when not communicating.

In manufacturing environments, not only are IoT technology devices driving efficiency and automation like never before, but these devices must also still be designed to use less energy when operating. IoT device manufacturers have already set their eyes on producing lower-power-consuming products. By doing so, their products are more efficient, smaller, and sleeker. Everyone wins by trying to produce gadgets that use less energy when operating, the consumer, business, and manufacturer. Many companies can gain from keeping the IoT at the forefront of renewable energy. Implementing IoT sensors on generation, transmission, and distribution equipment can enable remote asset monitoring and management. Plus, installing IoT throughout the manufacturing environment can aid in reducing costs associated with lighting, heating, cooling, and safety.

A smart-home network can include many communication devices operating 24/7. Because these devices consume energy even when they aren't actively communicating, efficiency and power consumption will always be a design concern. IoT devices must be optimized for power-efficient operation regardless of the protocol they use.

Here's a high-level summary of the power consumption of different standards:

- Wi-Fi and Matter (Zigbee, Thread) have similar signal range, but Wi-Fi consumes way more power because of supporting the high data range.

- Matter (Zigbee, Thread) and BLE have a comparable power consumption and are both developed to conserve battery power.
- Matter (Zigbee, Thread) consumes about 1 percent to 3 percent of the power that Wi-Fi consumes, depending on the application.

With green initiatives being implemented globally, driving lower power consumption across the IoT network is a must. Both users and manufacturers are aiming for lower power consumption without reducing performance and overall IoT connectivity goals. Devices can ensure continuous operation by automatically notifying users when batteries need replacement.

The Importance of Always-on Connectivity

IoT networks in the home and workplace have expanded dramatically over the last few years. At the same time, our reliance on these networks has also increased. More people are working from home offices. Families are using their home networks for video chatting, gaming, watching TV, monitoring their health, and securing their homes. There is a real need for low-latency always-on reliable connections to ensure 24/7 support for these use cases.

Luckily, the wireless providers in all areas are responding with rollouts, including the transition to 5G networks. No longer will we have to worry about whether we'll have connectivity or a fast data connection. Instead, our concerns will focus on higher-level network attributes such as privacy and security as we increasingly rely on IoT networks for the smart home, smart city, Industry 4.0, V2X, and other aspects of our lives. These new concerns are driving all manufacturers and wireless service providers to respond by placing security at the forefront of their network and device designs.

The new digital world is allowing businesses and consumers to constantly be connected. Highly connected IoT users spend most of their days online — working, going to school, gaming, doing social media, and more. Not only are we online on average 8 or more hours each day, but our IoT devices are as well. These IoT

interactions with our sensors and cameras are 24/7 online, and these sensors, cameras, and monitors are pulling us more into an always-active online scenario — especially in the IoT world.

This digital world is dynamic and allows us many different channels of communication. One of the most important channels is the Internet and IoT. Today's online communication is fast, simple, and in real time. It ensures access to information and data being always at our disposal.

In the business world, 24/7 online connectivity allows managers, staff, stakeholders, and supply chains to always have and view real-time updated information. When you're out of the office, you don't need to be out of touch with what's going on. Industry-specific products will make the early running for IoT, but with the help of Industry 4.0, driven by the push for manufacturing efficiencies and cost management, consumers are also very much part of the IoT landscape.

Consumers purchase billions of units to install inside their homes to constantly monitor, automatically update, and manually update all in the hopes of convenience, security, health, and cost reduction. The consumer IoT promises to make our environment, our homes, and our vehicles smarter, more measurable, and more communicative. It's always on and waiting for us to communicate, like Amazon's Alexa or Echo, or it's always monitoring what's going on to help us make better decisions about our home environments and associated activities.

The IoT generates vast amounts of data from being on 24/7, using sensors attached to machine parts or environmental sensors or the smart speaker inside our living rooms. This means the IoT is a big driver for creating a vast amount of data analytics to allow companies to analyze and for our smart things to get smarter.

This data comes in many different forms, from voice requests, sensor readings, video, and more. The IoT data is growing and this metadata is fed into databases to bring structure to unstructured content or fed into cognitive systems to bring new levels of decision making, understanding, and intelligence to our environment.

How much of this IoT decision-making, understanding, and intelligence is going on around us can be eye-opening. For example, many people are amazed at how many IoT devices they have

on their home networks. If you have a new home with new appliances and an Amazon Alexa or two, soon you could have up to 15 or 20 connected devices on your network. A simple survey of the apps on your phone could show you what level of IoT is in your home: a camera at your front door, inside your living room, and on your back patio; another app for your new washer and dryer, and quite possibly a refrigerator, oven, and microwave; an Amazon Alexa or two around the home. Plus, you probably have an app for some lighting around the home, which is another three or ten bulbs. . . . You get the picture. Add them all up, and you could have 10 to 20 IoT devices floating around and most likely two or three smart watches or Fitbits connected to a few phones and tablets. These are always on and communicating with your network and with each other. IoT devices are always on and sensing, monitoring, and making decisions for us and with us. A simple survey like this can be mind-boggling and fascinating at the same time — showing you that the IoT is all around you.

IN THIS CHAPTER

- Discovering how IoT sensors, beacons, and actuators are changing the world around us
- Understanding how IoT is opening new opportunities and markets
- Seeing what the future looks like in the Internet of Things

Chapter 4
Next-Generation IoT Opportunities and Use Cases

In this chapter, we look at how the Internet of Things (IoT) is creating new business cases and applications. We also look at how the IoT is reimagining and changing existing markets, making them more efficient, easier to manage, energy efficient, and overall more helpful to everyday human activities.

IoT is no longer just a buzzword — it's embedded into sensors, home communications, factories, automobiles, and local farms. Many markets are seeing the benefits received by using IoT devices, so adoption continues to grow.

So, where do market analysts say the IoT is heading? In this chapter, we explore some of the markets being influenced today and in the future by the IoT.

The Next-Generation Smart Home

The key to the smart home is connectivity. The one-pod-per-room network ensures reliable connections so that individual devices work 24/7. These *mesh networks* use algorithms to continuously repair themselves and optimize performance, ultimately making the networks almost invisible to the consumer. Plus, new communication standards and technologies like 5G are filling in the communication gaps and helping to ensure that, for consumers, everything just works.

Artificial intelligence (AI) is helping drive this "plug-and-play" transition to the invisible network.

AI is intelligence demonstrated by machines, unlike the natural intelligence displayed by humans and animals, that involves consciousness and emotionality. AI uses computer systems to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision making, and translation of language.

With advances in AI hardware and software, our voices and everyday activities will trigger IoT devices to perform actions on our behalf. We'll simply ask for something, and it will be ordered and delivered. When you remove a milk carton from your refrigerator, milk will be automatically placed on your grocery list and delivered to your smart home. As AI becomes smarter, your home networks will disappear into the background. We're already seeing our devices become smaller, sleeker, and more cosmetically appealing. With new technology advancements like AI, these devices will blend even more into our home furnishings and appliances, and we won't even notice that they exist.

In the next-generation smart home, more processing will be conducted within devices at the network edge, instead of in the cloud or the network gateway. Edge computing will become the norm, helping to ensure higher performance, reliability, and security.

Manufacturing/Industry 4.0

A slew of companies, including Cisco, Ford, General Electric, Harley-Davidson, Microsoft, and Toyota, have implemented IoT in their manufacturing processes. With the increased demand for

efficiency, traceability, and transparency, companies have been making strides to introduce ways to collect data and analyze their supply chain and manufacturing. They've done so using IoT devices, which not only makes the entire process transparent and measurable, but also allows for better decision making and process improvements.

By implementing mobile devices and sensors, which include radio-frequency identification (RFID) and location-based technology like ultra-wideband, asset tracking, inventory management, warehouse safety, and real-time visibility are all realized. With the collection of this information, both improvements in efficiency and supply chain monitoring are achievable.

With all this visibility and instantaneous data from sensors to smartphones or tablets, factories are seeing less downtime for machines and fewer bottlenecks in supply lines.

The transition to IoT Industry 4.0 will depend on a successful adoption of many new technologies such as ultra-wideband, the latest versions of Wi-Fi, 5G, private 5G, cloud computing, AI, and so on. Additionally, to accelerate smart manufacturing, it will be necessary to employ digital twins of machines and operations, as well as production automation and real-time control of equipment and tasks.

A digital twin is a virtual representation of real-world products or assets. They're used to manage the performance, effectiveness, and quality of a manufacturer's fixed assets.

Ultimately, IoT Industry 4.0 will boost productivity and help make smart machines smarter. It will provide billions of bits of data for companies, managers, and employees to make better real-time decisions. It will help them realize the goal of becoming factories operating with and without the intervention of humans inside the building.

Transportation

The connected car and *vehicle-to-everything*, or V2X (communication between a vehicle and other parts of the traffic system surrounding it), are putting us on the road toward safer and more convenient rides. Yes, the automotive technology and connected

cars are still evolving, but when they eventually turn the corner and become fully deployed, it will simplify life for both drivers and manufacturers.

Over the last several years, vehicles have become incredibly complex. They're embedded with computers and costly technology, which assists not only in driving but in maintenance as well. Now cars transfer vital data over the air back to the dealership, letting them know when things need repair or updating. Today, some cars get over-the-air computer updates wirelessly, so the owner no longer needs to schedule an appointment with the dealer for maintenance.

IoT sensors are also becoming a vital part of the transportation trucking industry. Allowing for the ability of *platooning,* where trucks drive in a group together. It's meant to increase the capacity of roads via an automated highway system. It decreases the distance between cars or trucks using electronics.

IoT networks and devices are also assisting with monitoring cargo temperatures, guidance, and speed to optimize fuel efficiency. This not only helps the trucking industry but also assists consumer and retail businesses, where packages are delivered in a timelier manner and with reduced cost.

With a vehicle-to-network capability, traffic flow will not only become safer, but also become more efficient. As the number of IoT sensors and cameras increase along our highways and roads to collect traffic information, this data will assist in alleviating traffic burdens and predict congestion points before they materialize. Some automobile manufacturers are already teaming with partners to create IoT platforms to the cloud to assist in connecting their cars to the IoT network.

Retail

Another industry adopting asset tracking is retail. The retail industry uses asset tracking to ensure food safety and to locate items in the store or in their supply chains. They also can use this technology to identify when shelf items are running low.

The IoT is also being adopted to understand consumer behaviors — for example, which items in the store are purchased faster during major weather events.

Retail has also adopted electronic shelf labels. The labels are battery-powered devices placed on the retail shelves that include a display (that is, e-paper) that graphically shows product information such as price and sales promotions. These labels can also be updated via computer, making it easy to change product descriptions and pricing.

Smart lighting is also catching on in many retail stores to save energy. Instead of having lights on all the time, some lights will go on only when motion is detected. These motion sensors can also monitor floor traffic and trends, offering retailers a range of feedback to better understand their customers.

With the adoption of retail apps in our phones and wireless technologies like Bluetooth, Wi-Fi, Zigbee, ultra-wideband, and more, the IoT has helped both small and large stores create a ubiquitous wireless retail playground. Retail can now be everywhere we are, and at any time from our homes, offices, malls, or city streets we can be engaging in buying activities, providing people with convenience and accessibility into a more efficient and effective retail experience.

Smart Energy

The power grid was designed to deliver power on an as-needed basis, to balance supply versus demand. On a typical day, demand and supply often vary depending on time of day, weather, and season.

Basically, power to homes and offices is priced according to demand. When demand is high, the cost of power is higher than it is when demand is lower. With the IoT, this information is transmitted immediately to smart meters, thermostats, and appliances so they can draw the power they need at off-peak times, when it's the cheapest. That means consuming energy when power is less expensive for consumers and businesses. Plus, it reduces the number of consumption peaks.

Not only are energy grids getting IoT smart sensors, but now water, gas, and other utilities are adopting the technology to improve efficiency and lower overall costs.

IoT sensors can help provide better load management. These sensors, located on energy equipment can constantly monitor, analyze load, and serve to help better manage energy. They can also help manage congestion along the transmission and distribution lines and ensure efficiency across energy plants. Sensors can also detect outages and allow operators to prevent electrocution, fire, and other hazards in real time. IoT smart switches distributed along the energy grid can help isolate affected areas automatically by rerouting power as soon as a problem has been resolved.

Another benefit of using IoT in managing energy generation is cost efficiency. Sensors can enable precise generation of energy to optimize production and control. By using IoT sensors, power companies will only produce a required amount of power, which will save the company money.

Healthcare

Technology advances will also focus on our emerging needs in areas such as health care. For example, with the COVID-19 pandemic, real-time highly accurate IoT location-positioning technology can support social distancing and contact tracing.

Manufacturers are quickly responding by creating devices that meet the needs of many healthcare opportunities. More broadly, healthcare and fitness are becoming key consumer trends, driving the development of wearable fitness devices that monitor and help improve our health.

The IoT has already made its way into many of our lives when it comes to health. The Fitbit and Apple Watch, as well as our mobile phones, all have sensors to detect our steps and heart rate. This trend is only going to increase as we see the benefits of monitoring this data to better improve our health.

IoT healthcare technology is also offering piece of mind to families, especially for those taking care of elderly parents or family members. Using senior lifestyle systems helps the elderly

and their children privately share lifestyle information, enabling seniors to feel safe and live longer independently at home. These IoT devices are noninvasive and provide senior behavior pattern recognition, long-term trends, alerts, and more to help enable a better lifestyle.

Hospitals are also adopting the IoT, using sensors for neonatal units to monitor premature babies. Because these sensors can't be placed directly on the skin, they use high-definition cameras to monitor skin color, breathing, and temperature, in order to alert nurses of any changes.

Smart Cities

With the smart city, say goodbye to the difficulty in locating a parking space. With IoT devices, you'll know all the open locations of parking spaces throughout the city. You'll no longer need to drive around city blocks waiting for a parking space to open.

Stoplights with embedded video sensors can adjust their green and red lights according to where the cars are and the time of day. This will reduce congestion and smog from cars idling at red lights burning fuel. These same lights will turn on only when a pedestrian or vehicle approaches, saving even more energy.

Some smart cities have also adopted smart garbage cans that crush waste and send a message to a dispatcher requesting pickup when full. This reduces garbage collection costs, as well as fuel emissions and labor costs.

Another key attribute coming to smart cities is always on connectivity — everywhere and instantaneous. Cities are finding that enabling a fully connected experience helps both businesses and consumers. Walking through the new IoT-connected city helps consumers know where bargains are as they pass retail stores, optimizes navigation, and provides always-on connectivity to many city services.

Sensors embedded in roads will gather data such as traffic performance and flow. These IoT sensors will also provide warnings such as informing drivers of icy conditions or accidents.

Agriculture

Although we typically think of the farming industry as being behind on technology, this isn't the case. Farmers are very much early adopters of new technology. They're always looking for opportunities to reduce costs, improve efficiency, and enhance the land they live on. Today's farmers walk their farms with GPS-enabled smartphones, loaded with agriculture-related apps. Farmers use these apps, sensors, and devices to help keep track of their animals, the soil their plants grow in, the water level in the soils, and the health of their livestock.

One company has even developed a sensor that detects high counts of a particular pest and then releases the pheromones that disrupt their mating rituals, which can in turn, reduce the need for pesticides.

Greenhouses are now being automated using IoT applications and sensors. Computers are controlling temperature, watering, and other factors to help farmers optimize the plant growing process. These sensors optimize watering, helping conserve water supply and reduce expenses.

Drones are also finding their way into the IoT farming space. They're being implemented in applications on the ground, in the ground, and above the ground. No longer does the farmer need to walk many acres of land to monitor water, soil, fertilizing, and areas requiring more attention. Instead, IoT drones can do this 24 hours a day, seven days a week, without tiring, while the farmer just needs to monitor the results on a phone, laptop, or tablet. This helps farmers make better, more informed decisions when planting, replanting, thinning crops, or watering. Overall, IoT is improving plant growth and increasing crop production, which ultimately benefits the farmer and consumer.

IN THIS CHAPTER

- Realizing the benefits of the IoT
- Improving IoT performance through standardization
- Taking the IoT to the next level with new technologies on the horizon

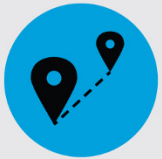
Chapter 5
Ten Key Takeaways

In a hurry? Start here! This quick list summarizes the key points from this book. Read these, and then if something catches your attention, check out the more complete explanation in earlier chapters.

- **Internet of Things (IoT) platforms rock.** IoT platforms provide services that are adaptable, self-configuring, support multiple protocols and many types of devices. Qorvo adds yet another level of multiprotocol support by introducing ConcurrentConnect technology, which provides faster, more efficient, more scalable IoT communications, and the ability to receive more data packets in a shorter amount of time.
- **Interoperability is important.** Interoperability is critical in IoT networks, which typically include multiple communications standards and devices from different manufacturers.
- **Manufacturers are standardizing their stuff.** To increase interoperability of smart-home devices and reduce complexity for consumers, industry leaders like Amazon, Apple, Google, Samsung, and many other top manufacturers are getting together to support a single new smart-home networking standard called Matter. The goal of Matter is to provide a plug-and-play solution for IoT devices.

- **Mesh networking is up and coming.** Mesh network topology, also known as *one pod per room,* is transforming smart-home networks. Mesh networking increases network reliability and performance and extends wireless device range throughout the entire smart home.
- **Mesh networks have advantages.** Mesh networks are self-healing and automatically find the best path for routing communications within the home, so the network continues operating even if some nodes stop working or lose their connection.
- **Edge computing is happening.** Edge computing will become the norm in smart-home networks. With edge computing, data is processed and stored at the source on the IoT sensor or gateway, only leveraging the cloud if additional processing is required.
- **BAW filter technology improves Wi-Fi system performance.** Using bandedge or Qorvo's Edgeboost bulk acoustic wave (BAW) filters can improve Wi-Fi signal range up to 78 percent.
- **New wireless networking technologies are helping the IoT.** Wi-Fi 6/6E and 5G are helping the IoT realize its full potential, providing reliable, fast, always-available services in any indoor or outdoor location.
- **Expect to see more artificial intelligence (AI) in the IoT in the future.** AI is helping to make networks invisible by allowing devices to act on their own instead of waiting for commands.
- **The future looks bright.** Globally, users are demanding technologies that are always available and easy to use. With the introduction of advanced RF technologies like 5G and enhancements like AI, this desire is achievable.

Superior Range - Reliability - Capacity



- Ultra-linear wide bandwidth Wi-Fi FEMs
- edgeBoost™ filtering extending range
- Antenna diversity for IoT doubling reliable range
- ConcurrentConnect™ technology maximizing capacity

Coexistence

- coexBoost™ & bandBoost™ filtering
- Integrated IoT and Wi-Fi coexistence technology

IoT Wireless Technology

- High efficiency Wi-Fi FEM technology
- Superior battery life for low power IoT
- ConcurrentConnect™ technology reduces data packet drops and retries

Energy Efficient

- Highly integrated small form-factor solutions
  - Wi-Fi iFEMs & BAWplexers
  - Multi-protocol IoT, SoC/ transceiver
  - Audio and sensing integration
- Reducing design complexity and size

Smallest Form-Factor

Learn how IoT is changing everything

The Internet of Things (IoT) is here today and here to stay! IoT technology is helping to create the smart home, smart city, smart building, and more. It helps us be more informed, better decision makers, and always connected to each other and the world around us. With the creation of new products and use cases, the IoT is entering many areas of our daily lives, helping to make many improvements in our world. Qorvo is dedicated to simplifying the complexity and fragmentation, enabling plug-and-play smart-home deployment.

Inside...

- See what the IoT can enable
- Understand IoT architecture
- Examine IoT network protocols
- Review key IoT market drivers
- See how innovation will bridge multiple standards
- Discover IoT use cases

qorvo
all around you

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-79822-4
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.