How to Ensure IoT Devices Work in Their Intended Environment

LOCATE AND IDENTIFY INTERFERENCE

KEYSIGHT TECHNOLOGIES

IoT Coexistence Testing

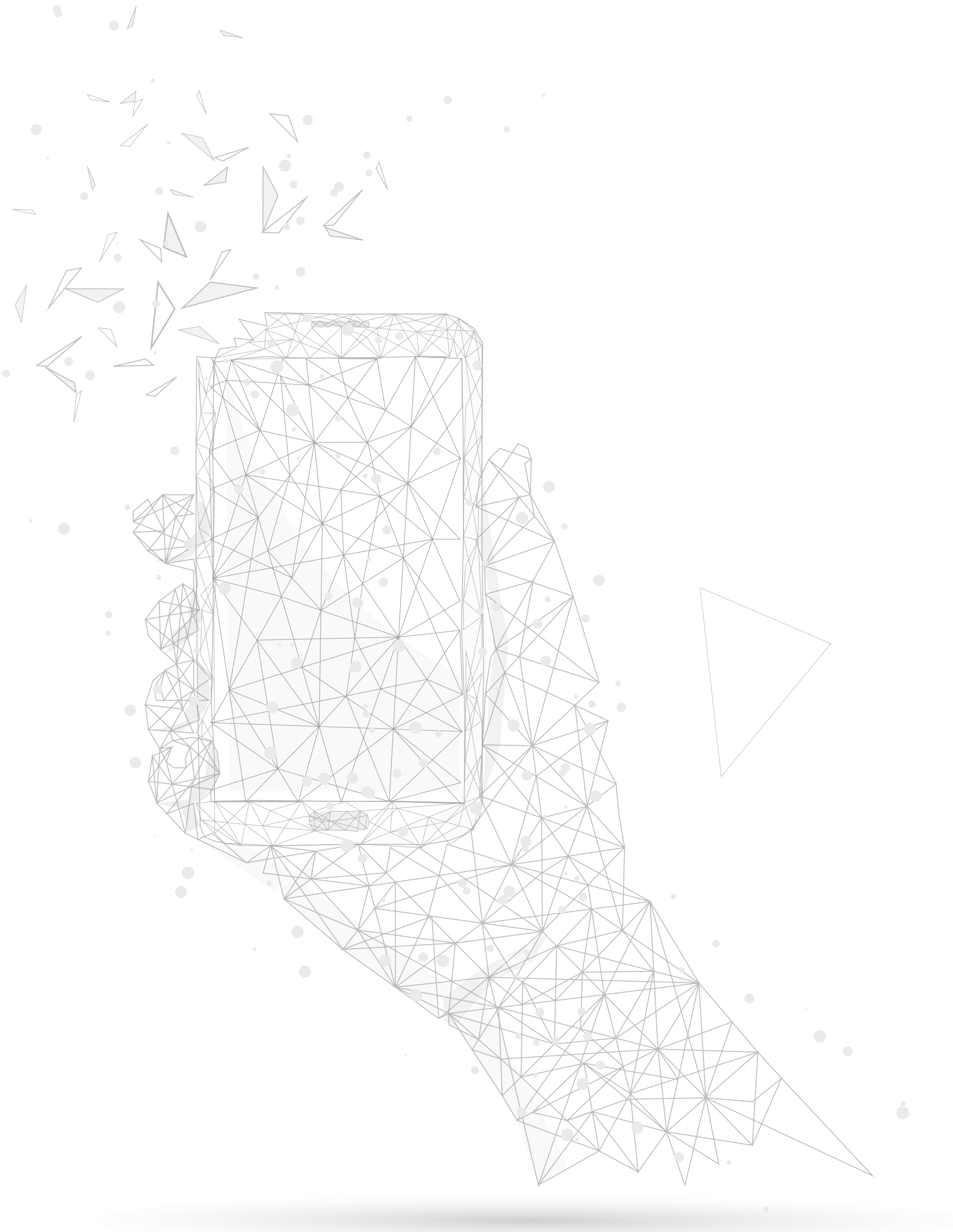
Ensuring IoT devices work all the time, every time

Coexistence is essential for stable, reliable communication in the Internet of Things (IoT). Without coexistence, IoT devices can't be counted on to operate as intended in crowded wireless environments. Your device may be unable to detect other IoT devices or cooperatively share the airwaves and may behave in unexpected or even dangerous ways.

It is challenging to ensure IoT device coexistence. You cannot have a high degree of confidence about coexistence unless you take appropriate actions during the design process.

The single most important action you can take is to perform coexistence testing. This helps you determine your device's tolerance to other radio signals and characterizes its behavior in the presence of alternate radio protocols.

Coexistence testing is the only way to accurately evaluate your device's ability to maintain its functional wireless performance (FWP) in the presence of intended and unintended (interfering) signals. It is critical to understand the details of coexistence testing, and how to perform it accurately and efficiently, to ensure the success of your IoT device.



Contents

There are **4 main steps** to ensure an IoT device works in its intended environment.

STEP ONE

Pick Your Protocol

STEP ONE

Pick Your Protocol

Customers Expect Reliable, Quality Connectivity

Coexistence issues impact the performance of your IoT device in a crowded wireless environment. Data can be lost, voice quality may degrade, and your device's operating range and battery life may decrease. Solving these problems begins the moment you select the wireless standard(s) your device will support.

The vast number of wireless standards makes it difficult, if not impossible, to allocate separate frequency spectrum to each. Different standards share the same frequency bands, and as new applications are added, interference is inevitable.

Wireless standards employ a variety of techniques to help them peacefully coexist. Which one you chose depends on your intended application and the environment in which it will be used. Before deciding, make sure you fully understand how your choice will aid or hinder coexistence.

This chapter examines some of the common IoT standard options available:

- ZigBee
- NFC
- Thread
- NB-IoT
- Bluetooth Low Energy (BLE)
- Cat-M1
- Z-Wave
- LoRa
- Wi-Sun
- SigFox
- WiFi

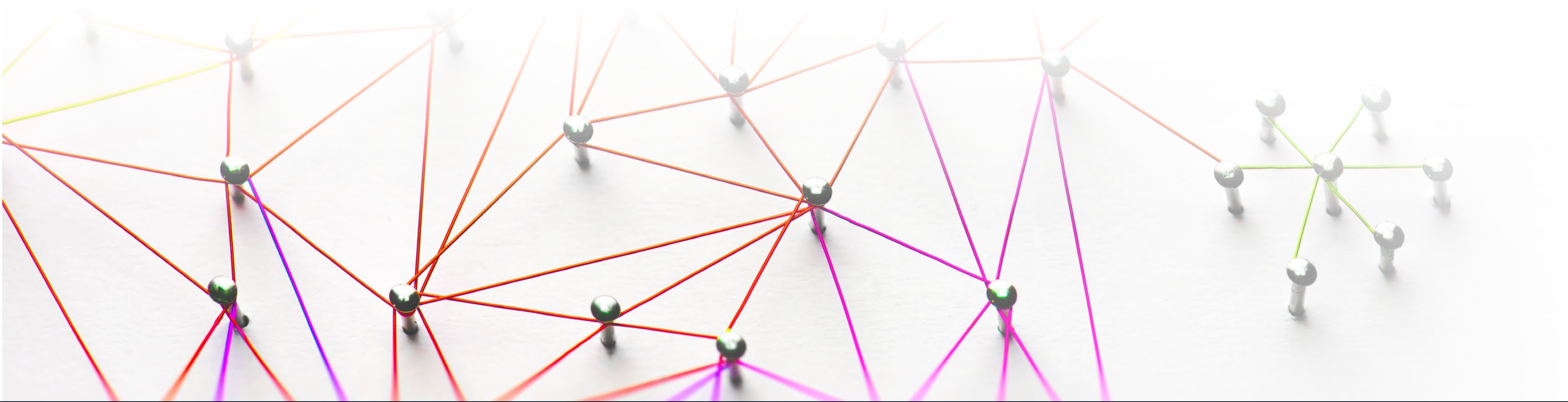
Wireless standards for the IoT fall into two categories: short and long range.

Short-range standards

include Bluetooth® Low Energy (BLE), WiFi, Near Field Communication (NFC), ZigBee, and Wi-Sun. They typically have a range of 10 to 30 meters, although under good conditions, all are capable of providing greater range. Short-range standards are used for wearables, smart home applications, payment systems, and building automation applications.

Long-range standards,

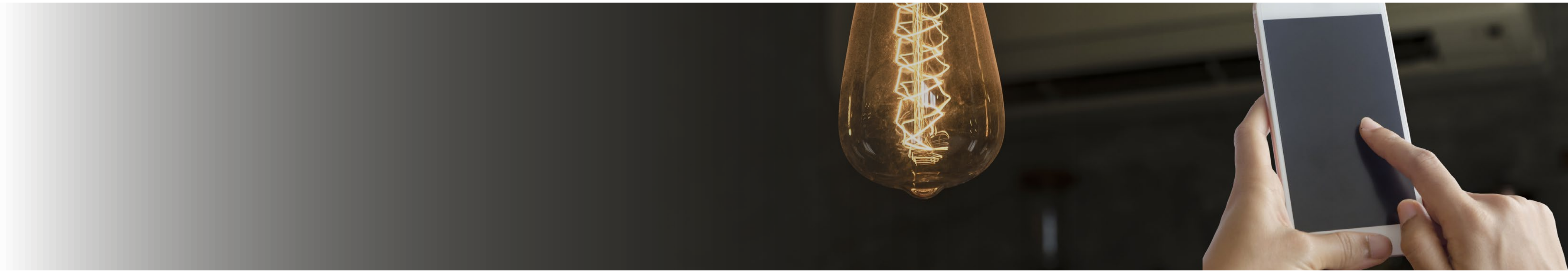
such as Narrowband (NB)-IoT, Cat-M1, LoRa, and SigFox, are used in applications where the coverage area is expected to be much larger. Examples include smart city, smart energy, and industrial IoT (IIoT) applications.



ZigBee

ZigBee is based on the IEEE 802.15.4 physical (PHY) and media access control (MAC) layers. Both specifications contain a great deal of functionality specifically designed to promote coexistence and mitigation of interference. ZigBee inherently supports tree, star, and mesh networking so groups of devices can cooperatively pass data in short hops to thousands of controlling nodes. To learn more, visit www.zigbee.org.

ZigBee	
Frequency	800, 900, 2400 MHz
Bandwidth	2 MHz
Data Rate	40 kbps to 250 kbps
Modulation	BPSK OQPSK
Range	10 m
Network	WPAN
Applications	Home automation, smart grid. and remote control



Thread (802.15.4)

Thread is also based on the IEEE 802.15.4 PHY and MAC; however, it uses the IPv6 over low-power Wireless Personal Area Network (6LoWPAN) protocol. It's a robust, encrypted mesh network designed to securely and reliably connect hundreds of home-automation products and devices. To help prevent interference, it uses a listen-before-send technique prior to every data transmission. To learn more, visit www.threadgroup.com.

Thread (802.15.4)	
Frequency	800, 900, 2400 MHz
Bandwidth	2 MHz
Data Rate	40 kbps to 250 kbps
Modulation	BFSK, FSK, OQPSK
Range	10 m
Network	WPAN
Applications	Mesh network for home and support 6LoWPAN

Bluetooth Low Energy (BLE)

BLE is the evolution of *Bluetooth* intended for low-battery-drain operations. Designed with lower data throughput in mind, BLE significantly reduces power consumption in *Bluetooth* devices, enabling 10 years of operation using coin-cell batteries. To ensure peaceful coexistence with *Bluetooth* on the same device, BLE and *Bluetooth* use a common MAC layer. To learn more, visit www.bluetooth.org.

BLE	
Frequency	2.4 Ghz
Bandwidth	1 MHz
Data Rate	1 Mbps
Modulation	GFSK
Range	50 m
Network	WPAN
Applications	Automotive, healthcare, security, and home entertainment

Z-Wave

The Z-Wave protocol is an interoperable, wireless, RF-based communications technology for home automation. It is designed specifically for control, monitoring, and status reading applications in residential and light commercial environments. Z-Wave mitigates interference issues and increases range by using the less crowded sub-GHz frequency bands (915 MHz in the U.S. and 868 MHz band in Europe). To learn more, visit www.z-wavealliance.org

Z-Wave	
Frequency	868.42 MHz 908.42 MHz
Bandwidth	200 kHz
Data Rate	9.6 kbps -100 kbps
Modulation	BFSK GFSK
Range	100 m
Network	WPAN
Applications	Remote controls, smoke alarms, and security sensors. Owned by Denmark Zensys

Wi-Sun (802.15.4g)

Wi-Sun (Wireless Smart Ubiquitous Network) is a physical layer amendment to the IEEE 802.15.4g standard for local and metropolitan area networks. It provides a low data rate wireless network supporting large-scale IoT in large, geographically dispersed smart utility and smart city networks. It has minimal network infrastructure requirements and can potentially support millions of fixed endpoints. Wi-Sun's resilience to interference comes from its highly resilient protocol and use of frequency hopping. To learn more, visit www.wi-sun.org.

Wi-Sun	
Frequency	800, 900, 2400 MHz
Bandwidth	200 kHz to 1.2 MHz
Data Rate	50 kbps to 1 Mbps
Modulation	FSK, OFDM, OQPSK
Range	1000 m
Network	WNAN
Applications	FAN and HAN Smart Utility Networks, Smart Grid, and Smart Metering

Wi-Fi

The IEEE 802.11 Wi-Fi protocol is the most widely used wireless internet connectivity technology today and has many variations. 802.11ah (HaLow) was created for low data rate, long range sensors, and controllers. HaLow uses time slot assignments to avoid collisions and ensure performance in crowded wireless environments. To learn more, visit www.wi-fi.org.

802.11ah	
Frequency	Sub GHz
Bandwidth	1 to 16 MHz
Data Rate	150 kbps to 78 Mbps
Modulation	OFDM
Range	1000 m
Network	WLAN
Applications	Target for IoT, wearable devices or extended range

NFC (ISO/IEC18092)

Near-field communication (NFC) is based on ISO 14443. It operates at 13.56 MHz and is used for access control, mobile payment systems, passports, and ticketing. NFC devices can behave as terminals (proximity-coupling devices) or readers and are very short-range devices. To avoid interference from RFID devices, NFC employs an anti-collision protocol. To learn more, visit www.emvco.org and www.nfcforum.org.

NFC	
Frequency	13.56 MHz
Bandwidth	1 MHz
Data Rate	848 kbps
Modulation	FSK, ASK
Range	20 cm
Network	P2P
Applications	Contactless payment, easy other connection (Wi-Fi, BT) identity and access

LTE-M (Cat-M1)

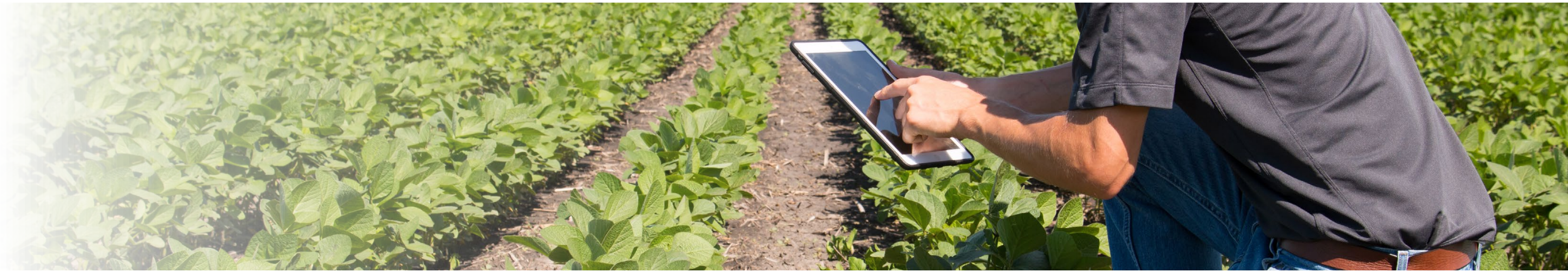
Cat-M1 uses cellular LTE licensed spectrum. It is well-suited for applications that require deep coverage where latency, mobility, and data speed requirements are less stringent. By making LTE-M compatible with LTE, it is possible to re-use the same hardware and share spectrum without coexistence issues, but it requires a contract with a cellular service provider. To learn more, visit www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/.

LTE-M Catagory 0/1 (LTE Rel. 12/13)	
Frequency	LTE bands
Bandwidth	1.4 MHz
Data Rate	200 kbps ~ 1Mbps
Modulation	OFDM
Range	1000 m
Network	WAN
Applications	Lower speed and power versions of LTE in 3GPP Release 12/13. Cat-M1 is expected to be used on machine-to-machine (M2M) applications for industrial IoT.

NB-IoT

NB-IoT is a low data rate, long-range addition to the LTE cellular network. Like LTE-M, it uses licensed spectrum. NB-IoT offers from 20 to 250 Kbits/second data rates, depending on what parts of the LTE resource blocks are being used. The standard's air interface is optimized to ensure harmonious coexistence with LTE, but it requires a contract with a cellular service provider. To learn more, visit: www.gsma.com/iot/narrow-band-internet-of-things-nb-iot.

NFC	
Frequency	GSM/LTE band
Bandwidth	180 kHz
Data Rate	Up to 250 kbps
Modulation	BPSK, QPSK, opt 16QAM
Range	10's of km
Network	WAN
Applications	Critical infrastructure and agriculture



LoRa

LoRa technology uses sub-1-Gigahertz radio frequencies in unlicensed spectrum at VHF, UHF, and 800-930 MHz frequencies. LoRa signals can penetrate deep into buildings and reach locations that aren't accessible to higher frequency equipment. However, LoRa networks deployed near one another can create interference. The use of directional antennae and multiple base stations can be used to enable coexistence. To learn more, visit www.lora-aliance.org.

LoRa	
Frequency	Sub GHz
Bandwidth	125 kHz
Data Rate	0.3 to 50 kbps
Modulation	GFSK, CSS
Range	32 Km
Network	WAN
Applications	Critical infrastructure and agriculture

SigFox

SigFox is a low power, wide area network technology, operating in the sub-1 GHz bands. It provides a network of cellular-like gateways that connect to the Internet and the cloud. Unlike LoRa, which targets both commercial and private networks, SigFox only targets commercial networks. To mitigate interference, SigFox uses Differential Phase Shift Keying (DPSK) at very low bandwidth for device-to-cloud communication, and to achieve long range with low power. To learn more, visit www.sigfox.com/en/sigfox-iot-radio-technology.

SigFox	
Frequency	Sub GHz
Bandwidth	600 Hz
Data Rate	Up to 500 kbps
Modulation	BPSK, GFSK
Range	10's of km
Network	WAN
Applications	Critical infrastructure and agriculture

STEP TWO

Understand Coexistence

STEP TWO

Understand Coexistence

Interference of Things

Customers expect IoT devices to operate seamlessly, regardless of which standard they are built on, and no matter how dense the wireless environment. How exactly do you achieve that?

First, you need to understand the term coexistence.

This chapter covers the basics on coexistence, including:

- Defining Coexistence
- Factors Creating Coexistence Concerns
- Introduction to Coexistence Testing

Defining Coexistence

Coexistence is the ability of wireless equipment to operate in the presence of other equipment using dissimilar operating protocols or standards. When two pieces of wireless equipment are near one another, and operating on the same or a close frequency, they will both be affected. The densest spectrum utilization is in the license-free “ISM” bands at 2.4 and 5 GHz. *Bluetooth* devices, microwave ovens, cordless phones, and wireless surveillance cameras are all examples of wireless equipment that can cause interference. Licensed spectrum such as cellular phone bands are more tightly controlled, but their transmissions can affect users of nearby frequency bands.

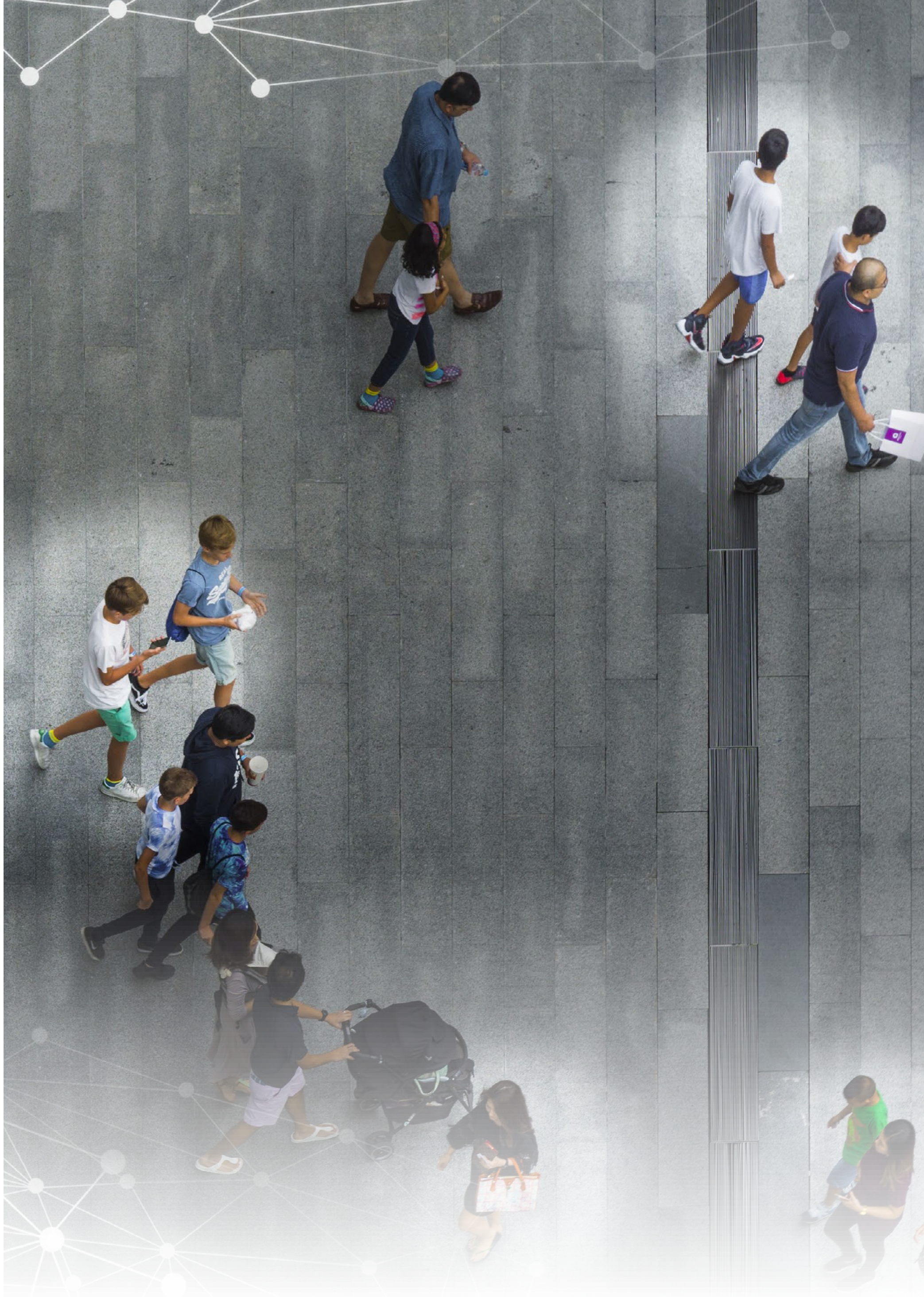
Factors Creating Coexistence Concerns

In general, four key factors drive coexistence concerns.

They are:

- Increased use of wireless technology for critical equipment connectivity
- Intensive use of unlicensed or shared spectrum
- Higher deployment rates of sensitive equipment, including medical devices (intravenous infusion pumps, pacemakers), and emergency detection devices (such as those found in a connected vehicle)
- Massive deployments of sensors for smart cities, industrial applications and beyond

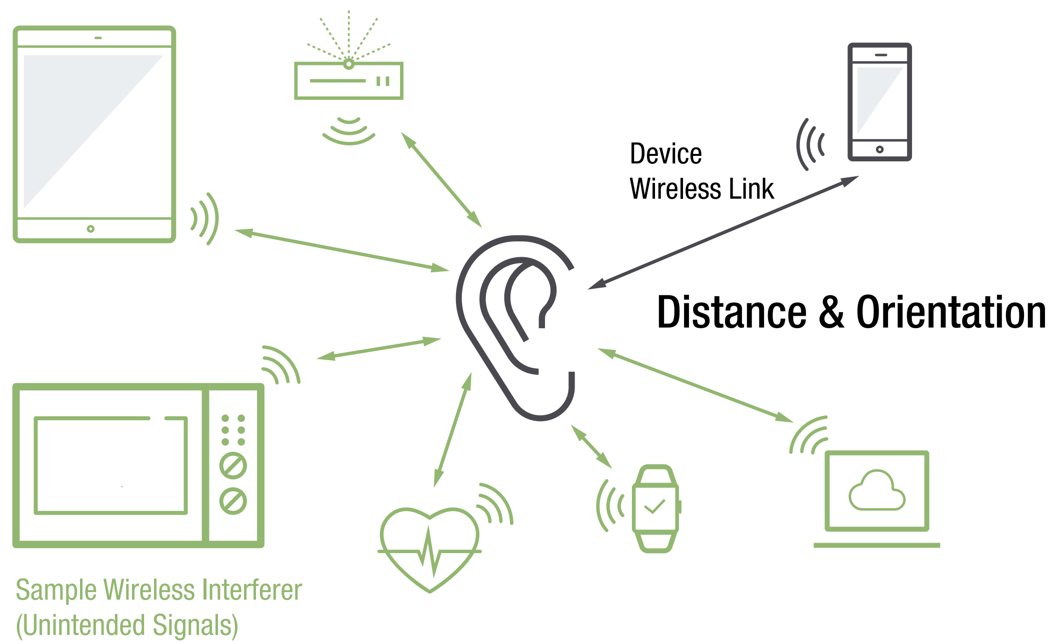
These factors directly impact the communications reliability of your IoT device.



To better understand coexistence, consider the example of a smart hearing aid that is communicating with a mobile phone in a hospital.

Along the corridor to a patient's room, there are wireless LAN access points set up, nurse call stations, *Bluetooth* devices at the nursing station, microwave ovens in the pantry, and medical devices (e.g., IV infusion pumps and cardiac monitors reporting on patient status) that sound alarms. There are also smartphones and/or tablets that visitors may bring with them, all using cellular, LTE, *Bluetooth*, and Wi-Fi at the same time.

In this scenario, these different devices and standards are all sources of interference, potentially disrupting the optimal operation of the different wireless devices around them. With sensors everywhere today, the interference problem will only get worse.



Introduction to Coexistence Testing

Coexistence testing evaluates the ability of a device to maintain its functional wireless performance (FWP) in different RF environments, whether in a crowded wireless environment like a hospital, or a mixed environment such as a train or subway station.

Coexistence testing is not the same thing as Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) testing, nor is it the same as protocol compliance testing. It does not have fixed pass/fail limits. Coexistence testing evaluates both the intended and unintended/interference signal impact on your device.

The basic concept of coexistence testing requires the equipment under test (EUT) to initiate communications with its companion device. In parallel, a signal generator is set up to generate an unintended interference signal, intended to disturb the communication. A signal analyzer monitors both the intended signal between the EUT and its companion device, and the unintended signal. The EUT's operation is also monitored for degraded performance using the Key Performance Indicator (KPI) metric.

EMI/EMC Tests

Measure the proper operation of circuits against fixed standards of emissions across intended and unintended frequencies

≠

Coexistence Test

Measures FWP in the presence of interference

≠

Protocol Compliance Tests

Ensure that networks of similar devices using the same standard can communicate and share the channel, following the rules of that standard

STEP THREE

Pick Your Technique

STEP THREE

Pick Your Technique

Coexistence Factors at the Physical Layer

You've picked your protocol and now you have a better understanding of coexistence and how it can negatively impact your device's FWP. What's next?

Different standards are unable to cooperatively share channels. A Bluetooth device, for example, using frequency-hopping spread spectrum (FHSS), cannot detect and understand an 802.11 transmission using orthogonal frequency-division multiplexing (OFDM) or direct sequence spread spectrum (DSSS) modulation on the same radio frequencies.

While there are efforts to improve coexistence in standards underway, no active cooperation has been defined to date.

This chapter covers three techniques you can use to improve the coexistence of your device and networks:

- Physical Separation
- Frequency Separation
- Time Separation

Each technique faces its own unique challenges when used in difficult RF environments.

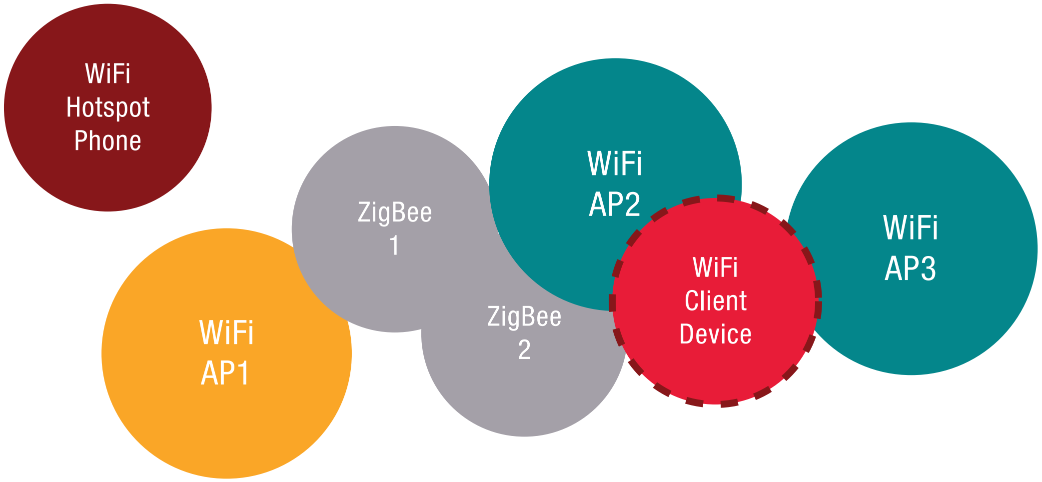
Technique 1: Physical Separation

Physical separation reduces interference by reducing competition for shared spectrum and reducing the signal strength so that the signals are more localized.

By physically separating different networks, interference is reduced, and interfering signals from another network are weaker. Physical separation increases the probability that each network, and the devices it supports, can operate simultaneously without errors.

Challenge

The technique doesn't work well in dense wireless locations. A prime example is the healthcare environment, where hundreds or thousands of wireless IoT devices may operate on the same 2.4-GHz ISM band using incompatible protocols. Here, it's impractical to use physical separation as a means of reducing interference.



Technique 2: Frequency Separation

Frequency separation is a technique used to improve the performance of mixed wireless networks.

When one network operates on a different frequency from another network, interference between the two, and between the devices operating in those networks, is reduced. This occurs whether the two networks are close to one another or not.

Challenge

While frequency separation is a valid technique, it's not always effective for the 2.4-GHz ISM band, which is occupied by overlapping *Bluetooth*, ZigBee, and 802.11 channels. You can't dictate which channels your neighbors use in shared spectrum.

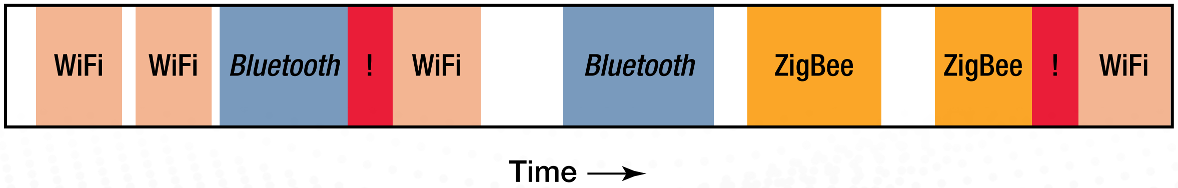
	802.11a/g/n...	802.15.4 (ZigBee)	802.15.2 (Bluetooth)
Non-overlapping Channels (2.4 GHz)	3	16	79
Bandwidth	22 MHz	5 MHz	1 MHz

Technique 3: Time Separation

Time separation is a technique whereby transmissions are sent and received at different times to avoid collisions and interference. This technique is possible because most radio networks and protocols are explicitly designed not to transmit 100% of the time. Rather, they use only small chunks of time to transmit.

Challenge

Most radio standards aren't designed to detect other network transmissions and cooperatively share channels. As the volume of data being transferred increases, more time is spent sending data and the corresponding acknowledgments. This increases the chance of a device being "deaf" to other protocols transmitting during a critical data transfer. Transmissions may collide, potentially causing errors and requiring data to be retransmitted, which means even more congestion when data is transmitted two or more times until properly received.



STEP FOUR

Create Your Test Plan

STEP FOUR

Create Your Test Plan

Delivering Reliable Device and Network Performance

Implementing one or more of the coexistence techniques previously described is essential to delivering reliable device and network performance.

Testing these implementations is critical to producing the highest quality device and gaining the utmost confidence that it will work as intended in any RF environment.

There are five steps you need to take to create an optimal coexistence test plan:

- Characterize the Expected RF Environment
- Choose Your Test Signals
- Define Functional Wireless Performance
- Choose a Physical Format
- Perform the Coexistence Test

Step 1: Characterize the Expected RF Environment

To characterize the RF environment where your device is expected to operate, you must perform field measurements in the frequency band of interest. You need to develop a model of signals present in the target environment, the strength of those signals, and the spectrum they use.

A traditional swept spectrum analyzer is often ineffective for this task. Device digital transmissions are very short and can come and go before the sweep reaches the frequency in use, leaving them undetected.

For accurate field measurements, a Real-Time Spectrum Analyzer (RTSA) is recommended. The RTSA enables you to continually sample spectrum with a high-speed analog-to-digital converter (ADC).

When characterizing your expected RF environment, the RTSA first performs a real-time fast Fourier transform to identify the types of signals present. Other spectrum analysis software may be required to precisely identify what protocols are in use. Then, the strength of the signals present and their rates of transmission are identified.

Step 2: Choose Your Test Signals

Once you've identified the signals present in the target environment, you need to select the type and number of signals needed to generate or model the coexistence test.

This may require you to select three different tiers of test signals.

For example, you may need to choose a single Wi-Fi network passing data at the lowest tier, and two Wi-Fi signals and one Bluetooth signal passing data at higher data rates. At the highest tier, three Wi-Fi signals and five Bluetooth signals may be needed. These interference tiers correspond to increasing levels of risk; a concept quite familiar to device designers.

Step 3: Define Functional Wireless Performance

FWP is a metric used to determine the success or failure of your device under test (DUT) in a certain environment. The metric defines the important behavior required of the DUT in its radio channel.

For this step, you need to compile a list of the required functions your device must perform to be considered as operating properly, and to coexist with other devices.

These functions may include:

- Startup and connection to the wireless network in a facility
- Successful and prompt sending of status reports
- Up to five data exchanges per minute while roaming between access points (APs)

The FWP requirements you compile will depend on the type and application of your device and its defined “normal” operating behavior.

Step 4: Choose A Physical Format

The final step in creating your coexistence test plan is to choose the physical format of your test.

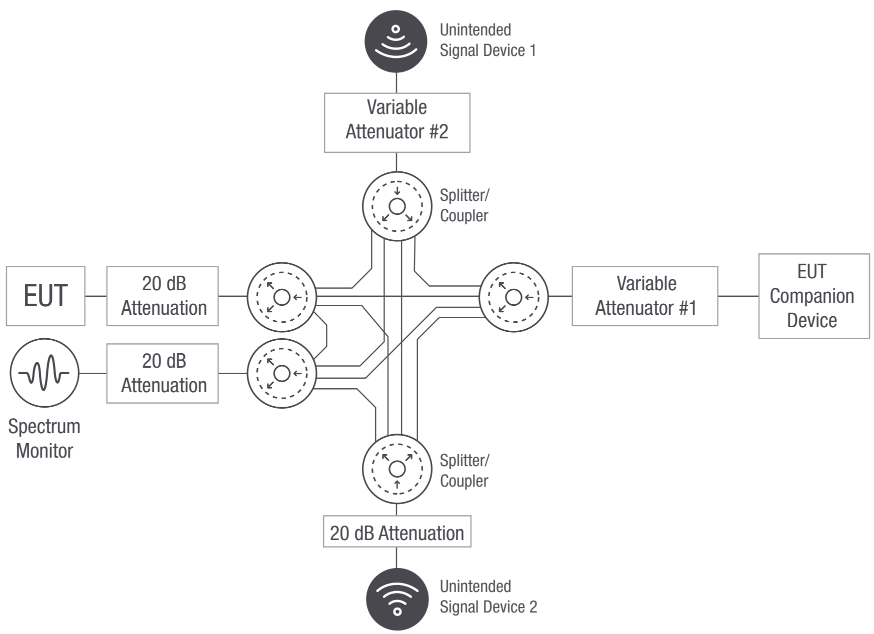
There are **four ways** to configure test equipment for coexistence testing. Each configuration is made up of similar components:

- Your DUT
- The device that connects or pairs with the DUT
- The competing network devices
- A spectrum analyzer

The configuration you choose will depend on practical considerations. Do you have access to an external antenna connection on the DUT? Will your device operate in a multiple-input multiple-output (MIMO) network? Does your device have directional antennas?

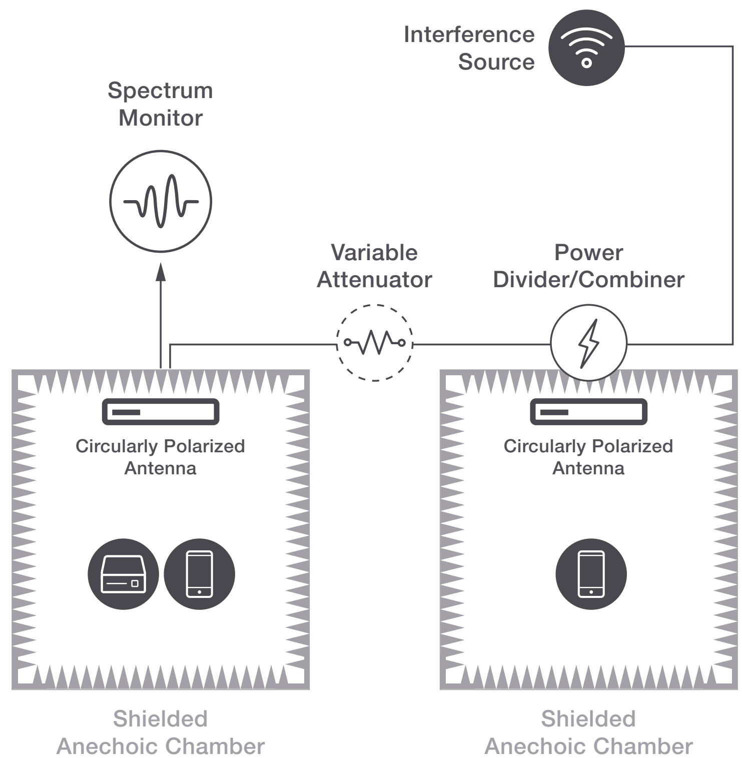
Method 1: Conducted/Wired Test

- This test is performed by combining the intended and unintended signals and connecting them to an access port next to, or in place of, the antenna
- Effects of the antenna are excluded from testing
- It is possible to account for MIMO and beamforming, but potentially challenging
- Most repeatable, but least realistic test method



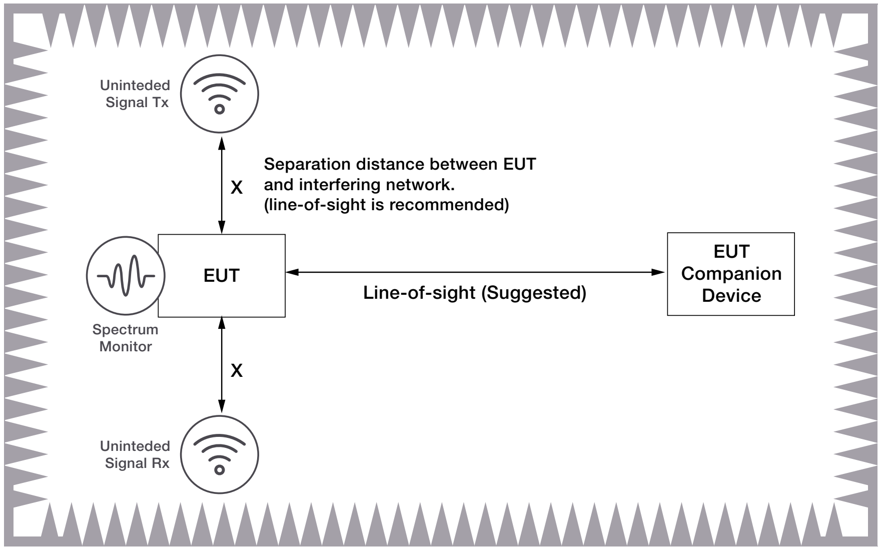
Method 2: Multiple Chamber/Hybrid Test

- Signals are generated by actual equipment and antennae. The EUT and companion device are placed in separate chambers to allow control over which signals the EUT is exposed to
- Channel effects can be accounted for
- Effects of the antennas are included in the testing



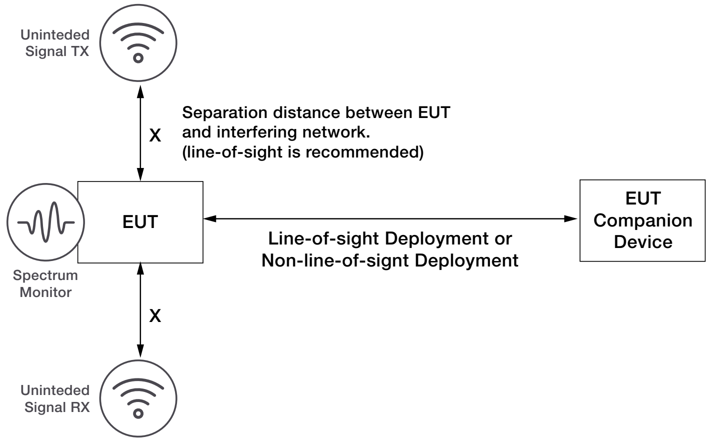
Method 3: Radiated-Anechoic Chamber (RAC) Test

- Test is conducted in a semi- or fully anechoic chamber
- Ensures that the environment does not decrease the repeatability of the test results
- Antenna effects are accounted for
- Environment may not resemble the deployment environment



Method 4: Radiated Open Environment (ROE) Test

- There is no shielded room
- Designed to be able to test any wireless device(s)
- Devices can be in a line-of-sight or non-line-of-sight configuration
- Least repeatable due to ambient signals
- Testing can be susceptible to ambient signals



Step 5: Perform the Coexistence Test

The final step is to perform coexistence testing using the test method you select.

The most efficient and cost-effective approach to coexistence testing involves complete stress testing of your device's integrated wireless module. Best practices for end-to-end testing include:

- Early testing on your device according to the wireless coexistence and interference tests specified by the appropriate standard
- Testing of device, APs, and infrastructure
- Wireless range, coexistence, and roaming testing to characterize the RF environment where your device is intended to work

After you analyze the test results and identify potential coexistence problems (e.g., radio chip and module RF performance, module firmware, CPU performance and defects, and module driver firmware defects), fix them in the lab. This approach minimizes risk to your budget and schedule, while helping to protect your reputation. The final result is a Probability (or Likelihood) of Coexistence (POC/LOC) metric, indicating the likelihood of your device's successful operation in the test environment.

Develop
Verify device features at the start of the development cycle to eliminate risks

Execute
Make use of reference tests to accelerate test programs involving leading features

Analyze
Discover and resolve defects early to ensure a faster, more cost-effective development

CONCLUSION

Achieve Coexistence

CONCLUSION

Achieve Coexistence

WHAT YOU NEED TO PERFORM IN THE REAL-WORLD

Coexistence is key to ensuring stable and reliable functional performance of your IoT device in its intended RF environment. To locate and identify interference that may adversely impact your device, we've identified 4 steps outlined in this guide.

Determine which wireless protocol to use in your IoT device by evaluating your options and the different measures available to avoid interference in Chapter 1.

Refer to Chapter 2 to gain a clear understanding as to how interference can impact your device and why coexistence is critical. Learn how coexistence testing can be used to root out undesirable behavior in the presence of interfering signals.

Explore three commonly used techniques to improve device and network coexistence and the challenges associated with each in Chapter 3.

Design your coexistence test plan with the steps found in Chapter 4. Perform the necessary testing and if interference sources cause your device to miss functional wireless parameters, identify the source and fix problems early in the lab.

Remember, it's much easier to locate and identify problems related to interference, and mitigate those problems, before your device is deployed in commercial operation. Once in a consumer's hands, any unexpected behavior from your device can erode user confidence, degrade your brand, and even result in a potentially costly recall. It is ALWAYS less costly and easier to solve coexistence issues in the lab BEFORE they become problems in the field.

To learn more about Keysight's solutions for coexistence test, go to Design and Test Solutions for the Internet of Things.