The 5 C's + 1 of IoT

A COMPREHENSIVE APPROACH TO YOUR MULTIFACETED CHALLENGE IN IOT DEVICE DESIGN

KEYSIGHT TECHNOLOGIES

INTRODUCTION

Create a Bulletproof IoT Device

Ensure your IoT devices thrive in a competitive environment

Tens of billions of Internet of Things (IoT) devices surround us today. Billions more will connect to the internet in the next few years. Many individuals and organizations use IoT devices to increase productivity and profit. While IoT devices offer great convenience, having large numbers of them in a small space increases complexity in device design, test, performance, and security.

Testing these devices is one of the biggest challenges today's design engineers and device manufacturers face. IoT success demands that they address the 5 C's + 1 challenges across the entire IoT device life cycle:

- **Connectivity**
- **Continuity**
- **Compliance**
- **Coexistence**
- **Cybersecurity**

While these technical aspects are important, incorporating user's needs and behavior into product design and test early in the lifecycle is paramount to satisfy and retain customers. This brings on the additional C:

- **Customer Experience**

Addressing the multifaceted challenges of IoT device design and test requires a comprehensive approach. Design engineers and manufacturers must follow through in addressing these challenges to ensure a reliable and secure future for IoT.

Contents

CHAPTER 1

Connectivity

Discover how to ensure reliable wireless performance of your IoT device.

CHAPTER 1
Connectivity

A Strong Foundation for Your IoT

The IoT is rapidly expanding into previously unconnected industries with applications such as remote machinery, remote surgery, and energy distribution in smart grids.

Many wireless technologies support these applications. Technologies include near-field communication for mobile payments, geosynchronous satellites for unattended remote weather stations, *Bluetooth*®, wireless LAN, ZigBee, point-to-point radio, and cellular.

Connectivity presents new challenges to designers, especially for mission-critical applications, where highly complex systems and dense device deployments must work reliably and without fail. The evolving wireless standards also add complexity to device development and testing.

Five Key Challenges of Wireless Connectivity Testing

Here are five key challenges in wireless connectivity:

- **Lack of RF knowledge** – Designers need to understand which test solutions to use during the development and manufacturing phases.
- **Inability to control the device under test** – Designers must be able to simulate actual operational modes and measure radio-frequency (RF) performance over the air (OTA).
- **Insufficient RF test coverage** – Uncertainty over what RF parameters to test for in the research, design, and manufacturing phases can hamper testing.
- **High cost of test** – Companies must balance the cost of test with the need for highly scalable and reliable manufacturing test systems that easily meet increasing volumes.
- **Unreliable test results** – Finding a way to ensure the quality and reliability of mission-critical IoT devices when other test methods are insufficient.

IoT devices are under pressure to be smaller, less expensive, and longer lasting than before. Design and validation engineers need to respond to these challenges to ensure that the wireless communication to and from a mission-critical IoT operation is constant, reliable, and secure.

Managing the Challenges of Wireless Design and Test

Here are five tips to help make your design and test of IoT devices less demanding:

Tip 1:
Use lower-frequencies to extend the range if all other factors are the same. For example, a 900-MHz signal will travel farther than a 2.4-GHz signal. A 60-GHz signal has substantially less range than a 5-GHz signal.

Tip 2:
Use lower data rates, which are less susceptible to noise and interference, to extend the range and reliability for a given set of factors.

Tip 3:
Consider factors such as range of communication, number of nodes and model of interaction, data rate, power source, and regulatory issues.

Tip 4:
Look for a complete test solution that includes test hardware and software, and that can perform appropriate RF tests, without the need to write special test codes or set up a programming connection to the device.

Tip 5:
Use an OTA signaling test solution to eliminate the complexity and cost associated with parametric testers.

WANT TO LEARN MORE?

Application note:
The Menu at the IoT Café: A Guide to IoT Wireless Technologies

CHAPTER 2

Continuity

Explore the steps you can take to optimize battery life in your IoT devices.

CHAPTER 2
Continuity

A Major Hurdle for IoT Device Designers

Whether we're talking about wearable devices that send information to your computer or network-connected motion detectors in a home alarm system, extended battery life tops the requirements list for new IoT devices. Consumers often expect long battery life for their applications and devices. Smart agricultural and industrial sensors, for example, must work for long periods — often more than 10 years — between charges.

Unreliable and short battery life causes a disruption, rather than making lives easier, as intended. For those who implement IoT strategies at the core of their business, inefficient power consumption becomes problematic.

Key Insights IoT Device Designers Need

Ensuring long battery runtime is often a challenge requiring these tasks:

- integrating sensing, processing, control, and communication components to understand the behavior of peripherals and their respective power consumption
- understanding measurement requirements of low-power devices (Figure 1)
- achieving an optimal balance between performance and power consumption to maximize battery life
- reducing circuit design cycles to meet time-to-market goals

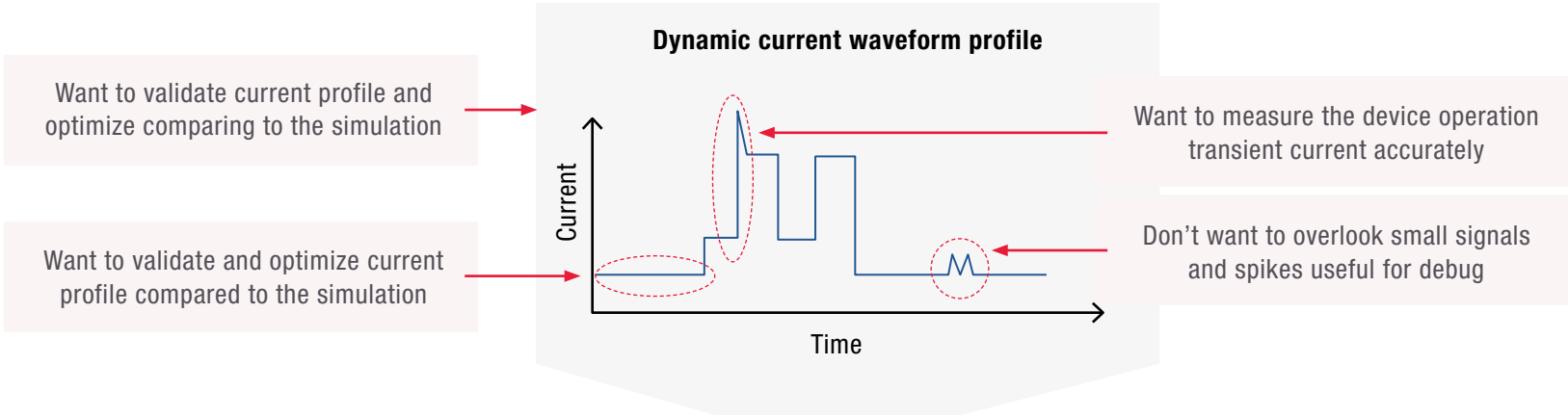


Figure 1. Example of low-power device and measurement requirements

Note: Battery-powered IoT devices sleep, wake up, and perform essential tasks (for example, sensing, measuring, and edge computing). The devices then communicate with a base station or peer node before returning to a sleep cycle. Each of these tasks draws current.

Maximizing IoT Device Battery Life

Here are four tips to maximize battery life:

Tip 1:
Visualize the current consumption from nanoampere to ampere, covering the wide current range of IoT devices from sleep to active modes.

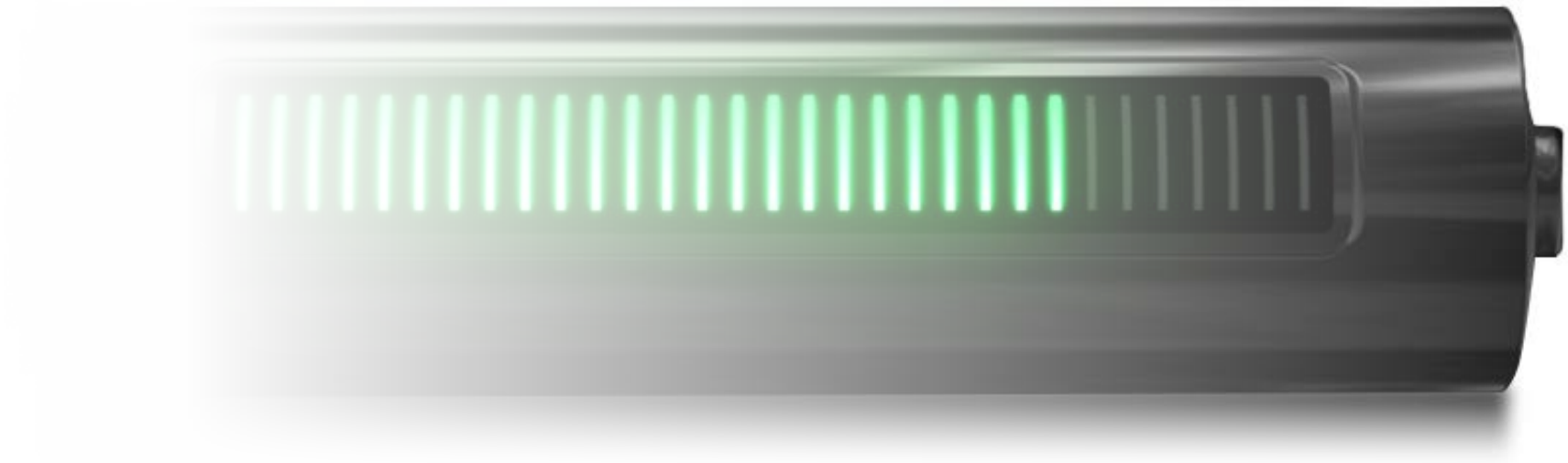
Tip 2:
Correlate the current consumption waveform with subsystem events (such as RF radio on, pump on, and display on) to gain better insight into current consumption of the subsystem.

Tip 3:
Perform OTA signaling control of the device to simulate real-world operations and measure current consumption during those operations.

Tip 4:
Calculate the total time spent, measure current drawn by each event or subsystem, and estimate the device battery life while simulating real-world operations.

WANT TO LEARN MORE?

eBook:
Four Tips to Optimize IoT Device Battery Life



CHAPTER 3

Compliance

Find out more about regulatory standards and their test requirements.

CHAPTER 3
Compliance

Keep Up with Evolving Regulations

Wireless devices bring convenience to users. However, as the use of the common wireless standards grows, congestion causes wireless communication failure, a problem that is intermittent and hard to trace. To address the congestion, standards bodies and regulatory agencies have issued recommendations and regulations to ensure effective and efficient use of the radio spectrum. Regulatory bodies include the US Federal Communications Commission and the European Commission, which governs the regulatory in European Union. Other regulatory bodies include the Korea Communications Commission and Innovation, Science, and Economic Development Canada.

For IoT device makers, it is essential to accomplish pre-compliance and compliance testing throughout the product life cycle — from design to test validation, manufacturing, and deployment. This helps manufacturers achieve first-to-market breakthroughs and stay competitive in the market.

Roadblocks to Global Market Access

IoT device manufacturers must certify their products for compliance with regulatory frameworks in markets worldwide.

They often face challenges complying with different regulations around the world while trying to stay ahead in the competitive market. Challenges include these:

- Time-to-market pressure – Design engineers often scramble to meet tight product introduction schedules and ensure smooth global market penetration while complying with the latest regulations.
- Complexity in regulatory test – Regulations change from time to time, which makes regulatory testing complex. Slow upgrades from test equipment suppliers add stress to the timeline.
- High capital investment – Large regulatory test systems often require large financial commitments.

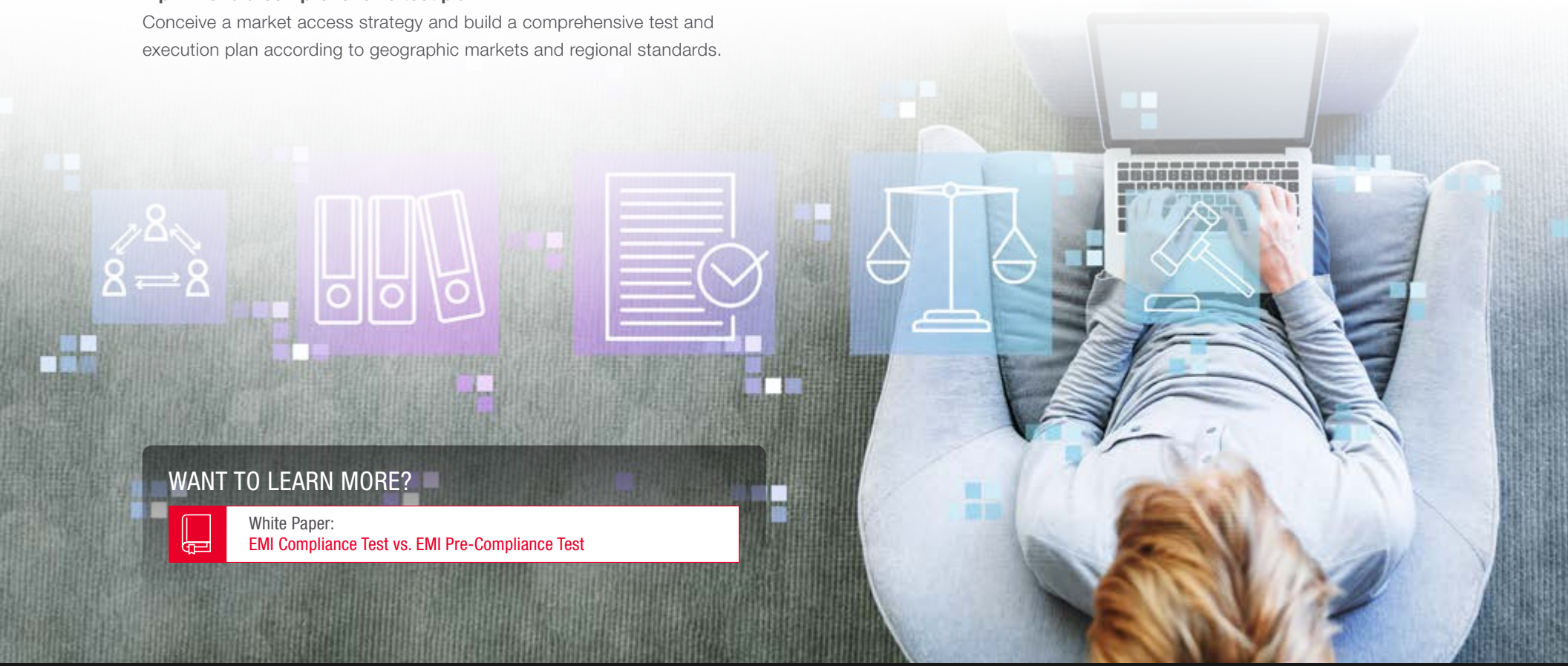
Breaking the Barrier to Success in the Real World

Despite the challenges, IoT device manufacturers can keep to a product release schedule by following these tips:

Tip 1: Incorporate a pre-compliance test plan into your device design schedule.
Device designers must include pre-compliance testing at every stage of their design cycle and execute it according to plan. Fixing an issue early in the design stage, rather than later, saves both time and money.

Tip 2: Build a comprehensive test plan.
Conceive a market access strategy and build a comprehensive test and execution plan according to geographic markets and regional standards.

Tip 3: Capitalize on automated testing to reduce pre-compliance test time
Executing a comprehensive test plan consumes a lot of time. IoT device manufacturers should use an automated test system to speed testing and provide measurement insights into failures.



WANT TO LEARN MORE?

White Paper:
EMI Compliance Test vs. EMI Pre-Compliance Test

CHAPTER 4

Coexistence

Understand the interference challenges your device faces and how to design around them.

CHAPTER 4
Coexistence

Ensure Reliable Performance Alongside Other Smart Devices

Wireless devices and networks are susceptible to disruption, especially in the shared license-free industrial, scientific, and medical bands at 2.4 and 5 GHz. Since most IoT devices and sensors rely on an active wireless connection to transmit data, interference can be detrimental to the resulting information. Wireless connections might drop intermittently. Data may become corrupted and unreadable.

Coexistence is the ability of a wireless device to operate in the presence of other devices using dissimilar operating protocols. It is essential for stable, reliable communication in the IoT world. The only way to ensure reliable wireless network performance and succeed in the wireless IoT world — especially in healthcare environments — is to properly test for radio coexistence.

Coexistence Challenges

Key factors that drive coexistence concerns include

- 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 (for example, intravenous infusion pumps and pacemakers) and emergency detection devices such as those found in connected vehicles
- massive deployments of sensors for smart cities, industrial applications, and beyond

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

Five Key Steps to Improve Coexistence

Here are the necessary steps to perform proper coexistence testing, leveraging the key considerations in ANSI C63.27 (American National Standard for Evaluation of Wireless Coexistence):

1. **Characterize the target environment.**
    - What interferers are present? What are the frequencies, protocols, and signal strengths?
2. **Define the device functional wireless performance.**
    - What must it communicate? How often does the communication take place? What is the maximum delay allowed? What is the required sustained data rate?
3. **Develop the test plan.**
    - Choose the test setup.
    - Define the risk tiers.
    - Define the pass / fail criteria.
4. **Execute the test.**
    - Monitor the RF environment and signal to and from the device under test.
    - Test without interferers to establish reference performance.
    - Test with interferers until failure occurs.
5. **Create a report.**

WANT TO LEARN MORE?

eBook:
How to Ensure IoT Devices Work in Their Intended Environment

CHAPTER 5

Cybersecurity

Learn how to strengthen the security of your IoT network.

CHAPTER 5
Cybersecurity

Internet of Things, or Internet of Threats?

For IoT devices, cyberattacks are a massive threat to users, manufacturers, and operators. For example, an attack against a connected medical device's radio interface can impede its essential performance — potentially injuring or even killing a patient.

The Threat of Upstream Vulnerabilities in the Supply Chain

One of the most overlooked threats to connected devices is upstream supply chain vulnerabilities. These kinds of vulnerabilities hide deep inside the protocol stacks on embedded system on chip (SoC) sets, which come from third-party manufacturers. Notoriously hard to find, these vulnerabilities often go undetected in security scans and frequently make their way onto devices in production. Left unchecked, they enable attackers to bypass onboard security controls — making it easy to crash, deadlock, or freeze a device.

Take Control of Device Security with Protocol Fuzzing

Device manufacturers are the last line of defense for their products. Since they bear ultimate responsibility for the products they ship, it is important they rigorously validate the security of all onboard components. Identifying protocol-level vulnerabilities demands a comprehensive testing mechanism known as protocol fuzzing. This process injects various errors into a communication exchange to confuse the entity at the other end of a connection. This type of testing is intricate, detailed, and systematic, so automation is a must. Where a simple chipset takes a matter of minutes to test, a more complex system could take days of continuous testing.

As IoT devices become more complex, protocol fuzzing will become even more critical in maintaining both device security and trust in advancing technologies. Fortunately, toolkits are becoming more widely available and easier to use — even for quality control teams who have little to no experience in cybersecurity.

WANT TO LEARN MORE?

White paper:
Security Resilience — The Paradigm Shift Is Here

CHAPTER 6

Customer Experience

Build Customer Experience-Centered IoT Devices.

CHAPTER 6
Customer Experience

Build Customer Experience-Centered IoT Devices

Today, IoT device manufacturers test wireless devices at the component, device, and software application levels, assuming that the integration is perfect and without errors. This approach may put lives and reputations at risk as a device can fail in a real-world environment. The failure of medical devices such as pacemakers and infusion pumps can be life-threatening. As IoT systems become more complex and mission critical, end-to-end customer experience testing is essential to deliver the highest-quality device and best possible customer experience across the entire journey.

Testing Beyond the 5 C's of IoT

The first five C's — connectivity, continuity, compliance, coexistence, and cybersecurity — are all important. However, the sixth C, customer experience, will set your device apart from the competition.

Users generally experience IoT devices through software and firmware applications. Testing these applications can be very difficult for a number of reasons:

- Software often includes features that users can customize. The number of possible paths and permutations of various settings can be too extensive to test manually.
- IoT applications often run on different hardware platforms — PCs, tablets, kiosks, smartphones, smartwatches, and other common consumer devices. To complicate matters, an IoT application may involve several different platforms. End-to-end customer experience testing must incorporate all platforms, including the various hardware revisions and operating systems that need support.
- Market pressure to quickly release each IoT device and software updates means you must test using an automated approach.

Testing Your IoT Device to Maximize Its Performance

Testing the device's end-to-end customer experience ensures that your complex IoT solution reaches the pinnacle of its performance limit, satisfies customer needs, and withstands real-world use cases.

A modern artificial intelligence-assisted approach to model-based testing emulates user behavior to test any technology at every layer. A customer experience testing solution needs to incorporate these components:

- Device modeling with a measurement control interface that creates a digital twin of the test instrument to measure performance.
- Equipment that uses advanced automation to replace manual human interactions to enable quick and more precise development.
- Software or application modeling to simulate real user scenarios to test the complete customer journey for quick and effective end-to-end design validation.
- Cloud-based software modeling with machine-learning data analysis algorithms to profile user behavior to improve the end-user experience.

End-to-end customer experience testing provides two major benefits:

- Seamless user experience ensures that the digital ecosystem works as intended — timely and error-free — from the user's perspective.
- Deep insights into the complete user journey enable IoT device manufacturers to continuously optimize and enhance their products to provide better user experiences.

WANT TO LEARN MORE?

Application note:
Testing the 5 C's + 1 of IoT

SUMMARY

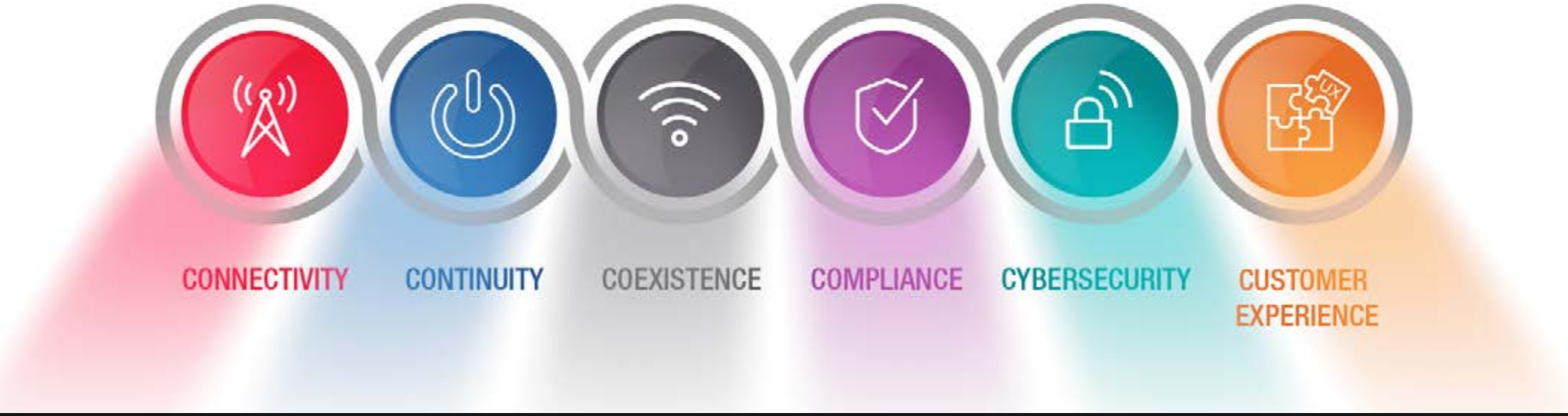
Rigorous design and test are paramount to building robust and resilient IoT devices.

A robust and resilient IoT device gives you an advantage in the ever-competitive marketplace. Building a device based on the 5 C's + 1 of IoT ensures that your complex IoT device reaches the pinnacle of its performance limit.

No doubt it will be a challenging process to deploy at every stage of the device life cycle — from simulation to research and development, conformance, manufacturing, and field deployment. Following the comprehensive 5 C's approach can ensure that your device is reliable and secure.

For information on how Keysight's solutions can help you address the 5 C's challenge, check out this link:

Get SMARTer with Keysight



Information is subject to change without notice. | 7120-1182.EN © Keysight Technologies, 2020 - 2022 | Published in USA, March 22, 2022 | keysight.com