WHITE PAPER

Unleash the Power of IoT

Explore top device test challenges through 5 C's +1 of IoT

KEYSIGHT

Overview

The Internet of Things (IoT) is growing rapidly in every vertical (Figure 1). The number of connected IoT devices is forecast to reach 30.9 billion by 2025, driven by new technology standards like 5G.[1] Global spending on IoT will reach $159.8 billion by the end of 2021 and will grow at a CAGR of 26.7% between 2022 and 2025.[2] As mission-critical applications proliferate, IoT devices and systems must be able to withstand the rigors of the real world. Design engineers face tremendous technical challenges. They will need to make critical design assessments, test considerations, and trade-offs throughout the product lifecycle, from early design to manufacturing. Addressing the multifaceted challenges of designing and testing the IoT requires a comprehensive approach.

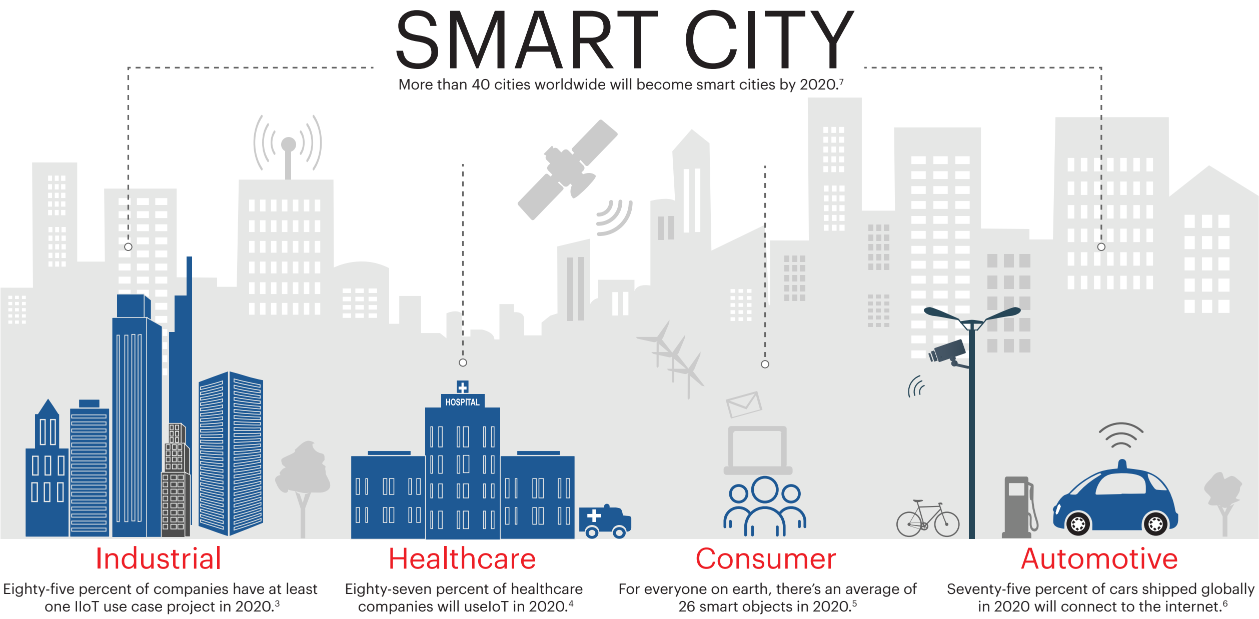

SMART CITY
More than 40 cities worldwide will become smart cities by 2020.[7]
HOSPITAL
Industrial
Eighty-five percent of companies have at least one IIoT use case project in 2020.[3]
Healthcare
Eighty-seven percent of healthcare companies will useIoT in 2020.[4]
Consumer
For everyone on earth, there's an average of 26 smart objects in 2020.[5]
Automotive
Seventy-five percent of cars shipped globally in 2020 will connect to the internet.[6]

Figure 1. IoT is rapidly growing in every vertical

IoT deployments have diversified, from consumer use to mission-critical applications for public safety, emergency response, industrial automation, and autonomous vehicles. Mission-critical applications use the convenient, low-cost, long battery life of IoT technologies and established wireless infrastructure. These technologies improve convenience, interoperability, and interconnectivity to allow real-time monitoring and control of critical devices and systems.

A Comprehensive Approach to Your Multifaceted Challenge in IoT Device Design

While IoT devices offer great convenience, having large numbers in a small space increases complexity in device design, test, performance, and security. Testing these devices is one of the biggest challenges for design engineers and device manufacturers. They need to address the 5 C's + 1 challenges across the IoT device lifecycle:

Connectivity ensures that your IoT devices connect to other IoT devices, the cloud, and the world around them.

Continuity requires that your IoT devices have extended battery life to do their jobs.

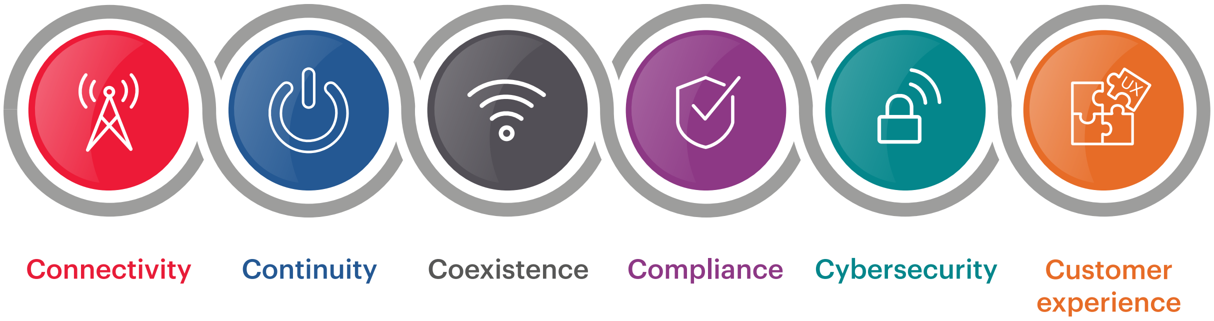
Compliance requires that your IoT devices adhere to global regulations.

Coexistence ensures that your IoT devices work harmoniously in crowded IoT environments.

Cybersecurity safeguards your data from cyberthreats.

While these technical aspects are important, incorporating users' needs and behavior into product design and test early in the lifecycle is paramount to satisfy and retain customers. Beyond the 5 C's of IoT, customer experience testing is essential.

Customer experience ensures your IoT devices deliver the highest quality customer experience.



The First C: Connectivity

In IoT, wireless connectivity is the key to enabling a seamless flow of information to and from the device, infrastructure, cloud, and applications. With complex systems and dense device deployments, connectivity is a top challenge device designers face. Devices need to work reliably, without failure, even in the toughest environments. Fast-evolving wireless standards add complexity to device development and testing. IoT device designers and engineers face common challenges in these areas:

- **Lack of RF knowledge**
  Many companies are designing their first wireless products. Often times, they have insufficient in-house expertise to select the appropriate test solutions for use in the development and manufacturing phases. Traditional RF test gear is too expensive and complex to operate. Establishing test methodologies to obtain accurate and reliable measurement results requires substantial RF and programming knowledge.

- **Inability to control the device under test (DUT)**
  The miniaturization of electronics means circuit board designs are shrinking, with antennas built into circuit boards and input / output ports eliminated. Designers face challenges around how to control the DUT without having a physical connection to simulate actual operation modes. How do they measure radio-frequency (RF) performance over-the-air (OTA)?

- **Insufficient RF test coverage**
  What are the RF parameters to cover in the R&D and manufacturing phases? During product development, the device will probably need to run through a full lineup of tests in accordance with the relevant wireless standard to ensure compliance. For manufacturing, there should be no further need for precision RF tests. But what RF tests help filter manufacturing defects?

- **The high cost of test**
  The proliferation of IoT devices means the demand for them will increase exponentially. Manufacturers need a highly scalable and reliable manufacturing test system that easily meets this increasing volume.

- **Unreliable test results**
  With IoT devices deployed in mission-critical applications such as smart grid, connected car, and mission-critical medical devices, traditional low-cost manufacturing test methods using companion devices, such as the golden radio method, are insufficient to ensure device quality. Such methods offer limited test coverage that can result in catastrophic operational failure and even costly product recalls.

Responding to these challenges requires careful selection of a design and test solution that is highly flexible, configurable, and scalable.

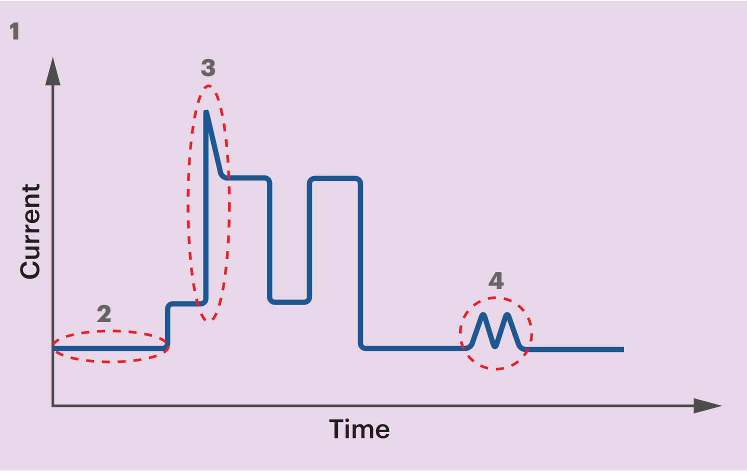
- The test solution should be flexible to test many devices with various radio formats and upgradable to support revisions or new radio formats.
- The software must be able to control both the DUT and tester to put the device in various operational modes to assess real RF performance.
- The hardware must enable OTA RF measurements without needing a physical connection to the device or chipset-specific control software.
- The test system must be simple, inexpensive, and applicable to both design validation and manufacturing to minimize measurement correlation issues across these different phases.
- The solution should be highly scalable and reconfigurable to enable multi-DUT testing for potential production expansion.

The Second C: Continuity

Battery life is an essential parameter for IoT devices. It provides a huge competitive edge and factors into consumers' buying decisions. Smart meter or industrial wireless sensors must work for long periods between charges — often 10 years or more. For medical devices such as pacemakers, battery life can mean the difference between life and death. Wireless communication standards groups are also defining new low-power-consumption operating modes, such as NB-IoT, LTE-M, LoRa, and Sigfox, that offer limited active operation time.

Integrated circuit (IC) designers, device designers, and test engineers face challenges when it comes to the battery life of IoT devices:

- To meet long battery life requirements, designers need to build ICs with deep sleep modes that consume minimal current, reduce the clock speed and instruction sets, and implement low battery voltages.
- Device designers who integrate sensing, processing, control, and communication components into the final product need to understand how the peripherals behave and consume power. Eventually, they will need to optimize the firmware and software of the device to simplify operation and reduce power consumption.
- Device designers and test engineers need to measure with widely varying current levels at every step of the device lifecycle. Low-power IoT devices spend most of their time in sleep or idle mode and only occasionally wake up to transmit and receive data.
- Power consumption of IoT devices varies significantly — from microseconds to seconds, and from picoamperes to amperes. Measuring this fast-changing and wide current range is a challenge for device designers and test engineers. Figure 2 shows an example of low-power device and measurement requirements.



1. Want to validate current profile and optimize comparing to the simulation
2. Need to evaluate and reduce sleep current consumption
3. Want to measure the device operation transient current accurately
4. Don't want to overlook small signals and spikes useful for debug

Figure 2. Example of low-power device and measurement requirements

To address these challenges, IC designers, device designers, and test engineers must:

- Visualize the current consumption from nano-ampere to ampere (nA to A), meeting the wide current range of IoT devices from sleep to active modes.
- Automatically correlate their current consumption waveforms with subsystem events (e.g., RF radio on, pump on, and display on) to identify design weaknesses. Doing so gives the designer better insight into the current consumption contribution of the device's subsystems.
- Perform OTA signaling control of the device to simulate real-world operations and measure current consumption during these operations.
- Automatically calculate the total time spent, determine current drawn by each event or subsystem, and estimate the device battery life simulating real-world operations.

With these capabilities, designers and test engineers can detect design weaknesses early, speed up the product development cycle, and maximize battery life performance.

The Third C: Compliance

Compliance is about making sure your IoT devices adhere to radio standards and global regulatory requirements before getting market access.

There are two main categories of certification tests, as shown in Figure 3.

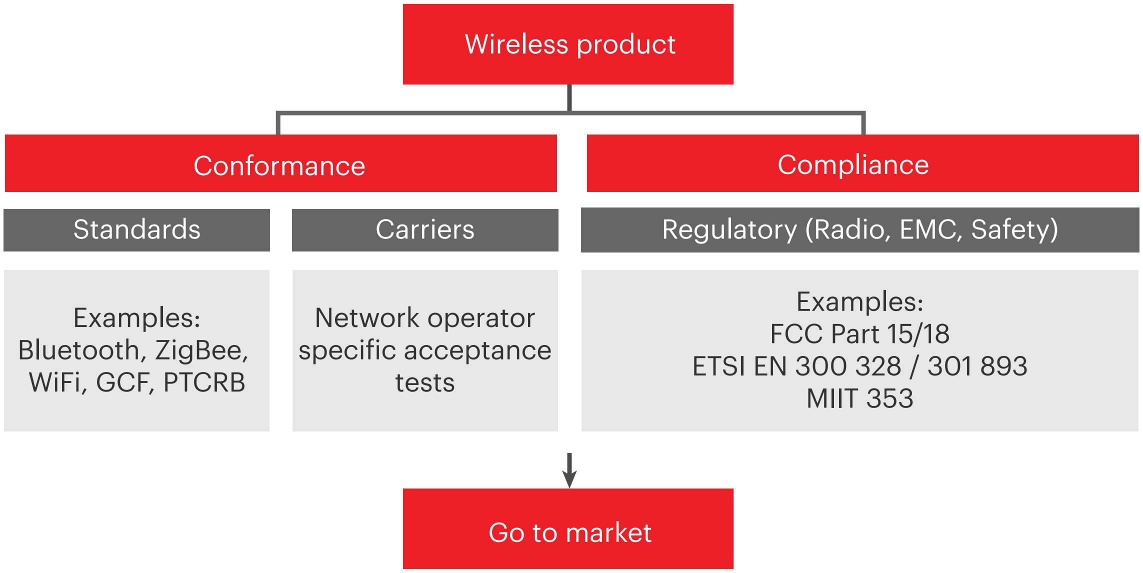

Wireless product
Conformance
Compliance
Standards
Carriers
Regulatory (Radio, EMC, Safety)
Examples: Bluetooth, ZigBee, WiFi, GCF, PTCRB
Network operator specific acceptance tests
Examples: FCC Part 15/18 ETSI EN 300 328 / 301 893 MIIT 353
Go to market

Figure 3. Two main categories of certification tests

IoT device manufacturers often face challenges complying with different requirements around the world.

- Time-to-market pressure: Device designers 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. A slow upgrade from the test equipment supplier adds stress to the timeline.
- High capital investment: An extensive regulatory test system often requires high capital investment.

The following tips can help manufacturers reduce the risk of failure and keep the product release schedule in place and within budget.

- Incorporate precompliance testing in the early stages of product development. Consider investing in in-house precompliance test solutions to carry out tests at every stage of the design cycle. Fixing an issue early in the design phase rather than later saves time and money.
- Choose a scalable, reconfigurable precompliance test system. Some test equipment providers offer scalable compliance test systems so you can start with a basic lower-cost test system and scale it up when needed.
- Reduce test time through an automated test. Regulatory testing is complex and time-consuming. Some of the tests take days to complete if performed manually. Capitalize on an automated test system available in the market to help save time in compliance and precompliance testing.

The Fourth C: Coexistence

The rapid increase of connected devices has made the wireless environment dense and congested. Standards bodies have developed methodologies and collision-avoidance techniques to improve the performance of device operation in the presence of other signals — adaptive frequency hopping, listen before talk, and cooperative collision avoidance. How good are they in a mixed-signal environment? When radio formats do not detect other signals, collision and data loss will happen. Consumer devices such as wireless headsets and wearables may face annoying delays or pauses. However, a medical device such as an infusion pump that stops working because of cell-phone interference is life-threatening.

Although coexistence testing is important, there is a lack of compliance or certification regime. In the U.S., the Federal Communications Commission (FCC) regulates emissions for wireless devices, and the Food and Drug Administration (FDA) regulates medical device safety. It is up to manufacturers, however, to take responsibility and conduct the appropriate testing. The Institute of Electrical and Electronics Engineers (IEEE) established some guidance in ANSI (American National Standard for Evaluation of Wireless Coexistence) C63.27 to provide key considerations for coexistence testing, such as evaluation process, test setup, and risk-based testing tiers.

1. Characterize the target environment
   - What interferers are present? What are the frequencies, protocols, and signal strengths?
2. Define the device functional wireless performance (FWP)
   - What must it communicate? How often should the communications take place? What is the maximum delay allowed? What is the required sustained data rate?
3. Develop a test plan
   - Choose the test setup — coaxial test setup, using chambers, or open-air setup?
   - Define the risk tiers. Tier 1 failures pose a significant risk, such as death orserious injury, while Tier 4 failures have negligible risk mainly resulting in inconveniences or discomfort.
   - Define the pass/fail criteria. It could be the data rate, latency, or error rate.
4. Execute the test
   - Monitor the RF environment and signal to and from the DUT.
   - Test without interferers to establish reference performance.
   - Test with interferers until failure occurs.
5. Create a report

Figure 4. Key steps to performing proper coexistence testing, leveraging the guidance provided in ANSI C63.27

With this guidance, manufacturers can assess the potential risk and the ability of their device to successfully maintain its FWP in the presence of unintended signals in the operating environment.

The Fifth C: Cybersecurity

Cyberattacks can happen in many layers — from devices and communication networks to the cloud and applications. Any connected device has the potential to act as a gateway to systems that offer more value. For example, a hacker might use an IoT device to gain access to a national power distribution center or defense system and bring it down.

To minimize the risk of cyberattack, enterprises now realize they need to take extreme measures to build a robust IoT infrastructure. Here is a recommended layered approach:

Security at the device level

Closing security gaps starts at the device level. Most security breaches originate from endpoints. Device designers need to consider security at the earliest stage of device development and perform continuous validation throughout the product lifecycle to ensure security and quality-of-service.

Security at the network level

Adopt an information security framework — a series of policies and procedures that guide businesses on ways to lower their risk and vulnerabilities. As an example, the National Institute of Standards and Technology (NIST) outlines five key activities in its framework for a good security program:

- **Identify** the data and processes you need to protect and conduct a proper risk assessment.
- **Protect** those assets through physical and administrative controls.
- **Detect** threats within the network at all times.
- **Respond** to threats with a documented and tested incident response plan.
- **Recover** any lost assets, if applicable.

Security at the enterprise level

Educating everyone on the importance of data security — arguably the lowest-cost security measure — provides the highest return on investment. C-level executives and boards, not just the IT department, need to be aware of the risk to the organization of a cyberattack.

Even after you have incorporated all the recommended steps, the network may still be compromised. The true test is how long it takes to recover. A resilient network will defend itself against threats and minimize financial loss to the organization.

Beyond the 5 C’s of IoT: Customer Experience

The first five C’s — connectivity, continuity, compliance, coexistence, and cybersecurity — are all important. However, the additional C, customer experience, will set your device ahead of the competition. Complex products that include end-to-end customer experience testing is essential to ensure it reaches the pinnacle of its performance limit, satisfies customer needs, and withstand real-world use cases.

Fortunately, there are integrated solutions that can tackle design and validation challenges that engineers face today. The best approach to test end-to-end customer experience is an intelligent model-based test solution that can help optimize the product. The solution that includes these four components provides a comprehensive test coverage of the entire range of potential user journeys.

- Device physical modeling that has an instrument measurement control interface to create a digital twin of the test instrument.
- Equipment with advanced automation that replaces manual human interactions, enabling quicker and more precise development.
- Software or application modeling that simulates real user scenarios to test the complete customer journey to provide quick and effective design validation of the entire system.
- Cloud-based software modeling with machine-learning data analysis algorithms to profile user behavior to improve the end-user experience.

Putting the 5 C’s + 1 into Perspective

IoT is opening doors to exciting new applications and opportunities for many industries. But it also brings unprecedented challenges that require thinking in new ways to meet mission-critical requirements. Take pacemakers, for example. Suppose a surgeon implants a pacemaker under the skin of a patient to monitor and control his / her heartbeat. Through wireless connectivity, the doctor can monitor the patient’s heart activities and plan future treatment.

Despite its potential, the success of the pacemaker and other mission-critical IoT devices is closely related to the 5 C’s + 1:

- the energy efficiency of the pacemaker, because replacing the built-in battery means opening up the chest
- the amount of current leakage that can cause muscle overstimulation
- the robustness of the connectivity to ensure uninterrupted data transmission in any environment
- the protection of transmitted information
- the ability to speed through the lengthy FCC and FDA regulatory and clinical processes
- the comprehensive test coverage of the entire usage journey of a pacemaker patient

Researchers are still working on all these areas. With a careful assessment of the 5 C’s + 1 challenges, remote monitoring of patients using implanted wireless pacemakers will help improve their quality of life. With this, the uptake rate of wireless pacemakers is likely to grow rapidly.

Successful IoT implementation requires designers and engineers to overcome technical challenges. A deep understanding of the technical challenges and the key design and test considerations will build a strong foundation to derisk IoT development and deployment across the ecosystem. Use of the right design, validation, compliance testing, and manufacturing tools throughout the product lifecycle will also help ensure IoT delivers on its promises.

1. Lueth, Knud L. "State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time. Last modified November 19, 2020. https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/.

2. Wegner, Philipp. "Global IoT spending to grow 24% in 2021, led by investment in IoT software and IoT security. Last modified June 16, 2021. https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/.

3. Berry, Jen. "Industrial Internet of Things (IoT) Trends to Dominate in 2020." MobiDev. Last modified November 5, 2019. https://mobidev.biz/blog/industrial-iot-internet-of-things-trends.

4. "State of IoT Healthcare." Aruba. n.d. https://www.arubanetworks.com/assets/infographic/Aruba_IoT_Healthcare_Infographic.pdf.

5. "A Guide to the Internet of Things: How billions of Online Objects Are Making the Web Wiser." Intel. n.d. https://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png.

6. Greenough, John. "The 'Connected Car' Is Creating a Massive New Business Opportunity for Auto, Tech, and Telecom Companies." Business Insider. Last modified March 11, 2015. https://www.businessinsider.com/connected-car-forecasts-top-manufacturers-2015-2.

7. "Smart Cities: A Futuristic Vision." SC Actual Smart City. Accessed March 31, 2020. https://www.thesmartcityjournal.com/en/articles/1333-smart-cities-futuristic-vision.

This information is subject to change without notice. © Keysight Technologies, 2020 - 2023, Published in USA, February 14, 2023, 7120-1139.EN