APPLICATION NOTE

Testing the 5 C’s + 1 of IoT

Solutions for a complex challenge

The IoT is growing quickly in diverse, mission-critical applications

The internet of things (IoT) is growing very quickly, with millions or tens of millions of new devices being added daily. Most IoT devices use one or more wireless protocols, and IoT devices, especially at the edge, are usually powered by small, inexpensive batteries. Because of the rapid growth of the IoT and the many vertical markets it serves (smart cities, smart vehicles, smart factories, smart agriculture, healthcare IoT, and so on), many businesses are adapting existing products to serve IoT applications and creating new products that were previously impractical or cost-prohibitive.

The Internet of Things has many exciting and profitable opportunities. Product development teams can increase their chances for success by following a framework known as the 5 C’s + 1 of IoT.

Sample applications

Beyond the lucrative economic opportunities, many organizations are seeing the potential that IoT has for helping people by gathering ever-greater amounts of data and analyzing that data to detect and respond to problems before they spiral out of control. For example, consider smart water meters. If an underground leak occurs, the smart meter can detect the sudden increase in water going to a particular home or business and let the owner know that they have been using water at, say, 10 times the usual maximum daily rate for the past 30 minutes. This gives the customer an opportunity to shut off the water and investigate the problem quickly, before major flooding occurs.

Or consider a smart logistics application that tracks the physical location of trucks. One could easily imagine a routing application that alerts the trucking company when a truck takes an unexpected detour. It is possible that the driver had a good reason to take the detour (to avoid a traffic accident scene, for example), but it is also possible that the truck has been hijacked. An IoT application can at least give people the opportunity to investigate.

KEYSIGHT TECHNOLOGIES

Finally, consider all of the ways that IoT is helping senior citizens live more independent lives. Many senior living centers have smart security devices, motion detectors, smoke alarms, flood detectors, and carbon monoxide detectors that are monitored IoT devices that monitor various health parameters, detect falls, and allow help to be summoned quickly reduce the risk to a vulnerable population.

As with any new technology, the IoT has many technical considerations that must be properly understood and considered in order to get to market quickly and satisfy customers over a long period of time. The considerations are numerous, but they generally fall into five categories known as the

“5 C’s + 1 C of IoT.” The first five C’s are:

- Connectivity
- Continuity
- Compliance
- Coexistence
- Cybersecurity

Each of these considerations is important, and each has its own design, implementation, verification, and test challenges. Unlike a typical school test, where getting four out of five right may be good enough to pass, getting just one of the five C’s wrong may destroy a device’s chance of commercial success or derail the economic viability of an IoT project altogether.

Beyond the five C’s, there is one additional C that you must consider, and that is the customer experience. Your end user probably experiences your application through software, and that software may reside on a PC, a tablet, a smart phone, a kiosk, or other device. Furthermore, the devices probably run a variety of operating systems, none of which is under your direct control. You must therefore make sure that your software is reliable and responsive on a wide variety of platforms. Read on to learn how to minimize risk and maximize the chance that your device and application will delight users and succeed in the IoT.

Connectivity

The IoT spans a wide variety of vertical applications, including smart cities, connected vehicles, smart agriculture, smart homes, smart grid, smart environment, wearables, industrial and scientific applications, and the healthcare IoT. Despite the apparent diversity of these applications, they all rely on various forms of wireless communications, from near-field communications to personal-area networks to long-range, wide-area networks.

Challenges

There are several problems associated with ensuring robust wireless connectivity. For example, keeping up to date with evolving radio technologies is always challenging. The best solution for your application two years ago may no longer be the best solution. Even if it is, there is a good likelihood that the standard itself has evolved since you first implemented it, and you need to keep your device up to date.

Another challenge is reducing the development cycle associated with RF communications. To hit the early adopter phase of market windows and establish market share during the most profitable phase of a product life cycle, product teams must move verify quickly and qualify the performance of their devices' communications subsystems.

A relatively new challenge is that wireless IoT devices are increasingly moving into mission-critical applications. The reliability of quickly establishing and maintaining robust connections, even during roaming, is therefore becoming more important than ever. Finally, there is the ever-present desire to improve and ensure product manufacturing quality while reducing manufacturing test costs.

Solutions

There are many approaches to manufacturing test of wireless devices, and they range from simple golden radio tests to comprehensive, one-box testers. The golden radio testers verify basic functionality, but they do not always detect manufacturing defects that might cause a device to fail in the real world. Comprehensive parametric test, on the other hand, is very thorough, but it can be slow and expensive.

The Keysight IOT8720A IoT wireless test solution (Figure 1) provides more functionality than a golden radio test, but at a much lower cost than a full parametric test. In addition to verifying basic functional performance by communicating with the device, it measures transmit power, advertising interval, and packet error rate. By reporting these key parameters, it can identify manufacturing defects that a golden radio approach might miss.

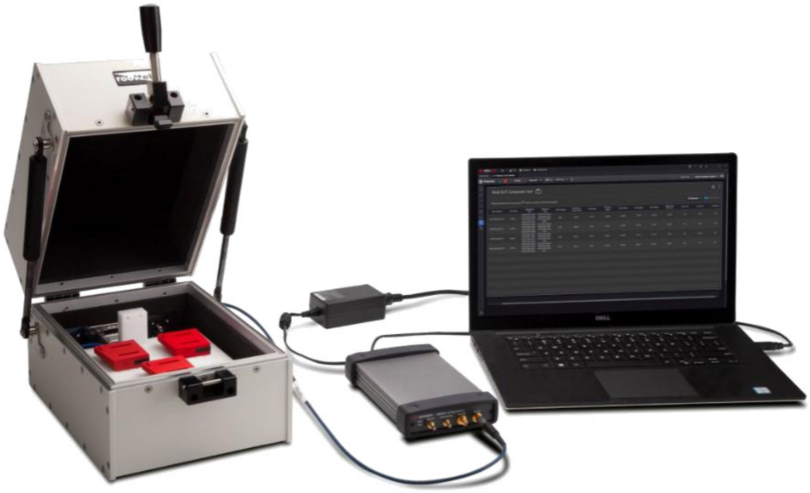
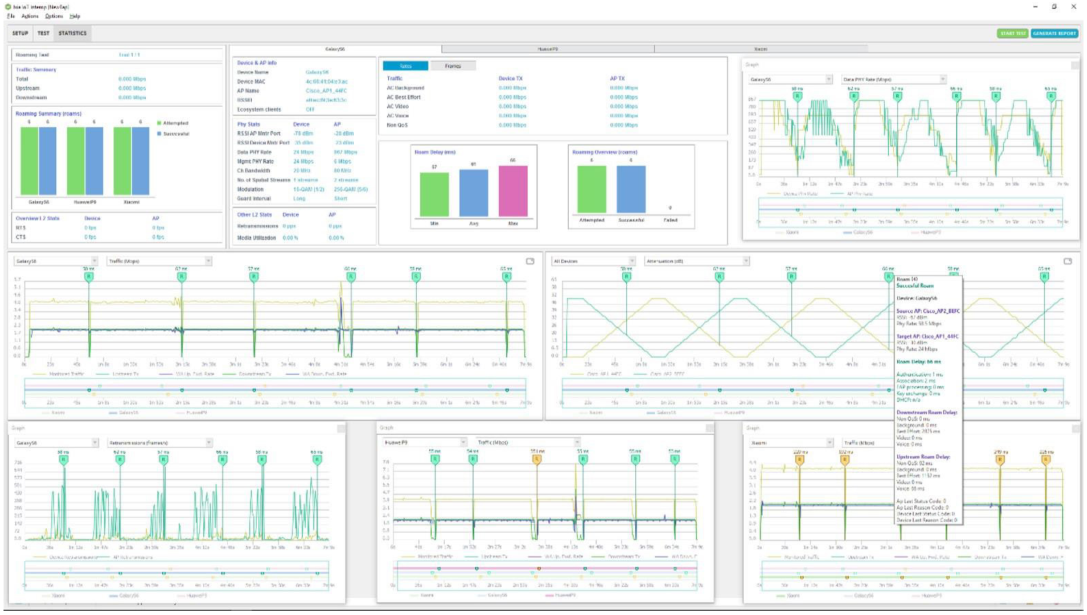


Figure 1. Keysight IOT8720A wireless test solution

While proper manufacturing test is important, one should not rely on manufacturing test alone to ensure robust communications. For example, a Wi-Fi test development process should simulate deployment and optimize device performance throughout the project. This includes the following:

- Range testing to simulate various distances between the DUT and the access point (AP)
- RF level analysis of the DUT's receiver and transmitter
- Simulation of roaming and handoffs between access points
- Ecosystem test to simulate busy environments
- Advanced analysis to verify interoperability
- Throughput testing to characterize device performance over different types of traffic

Keysight's Ixia IoT solution (Figure 2) provides all of these features and more. It also includes automation features to accelerate testing, which is critical for the product development process. It allows the user to replicate "real-world" deployments in lab environments and to use advanced analytics to quickly find root causes of problems.



Roaming Test	Trial 1.1.1
Traffic Summary	
Total	0.000 Mbps
Upstream	0.000 Mbps
Downstream	0.000 Mbps

Overview L2 Stats	Device	AP
RTS	0 fps	0 fps
CTS	0 fps	0 fps

Device & AP Info	
Device Name	GalaxyS6
Device MAC	4c:66:41:04:e3:ac
AP Name	Cisco_AP1_44FC
BSSID	[illegible]
Ecosystem clients	Off

Phy Stats	Device	AP
RSSI AP Mntr Port	-78 dBm	-28 dBm
RSSI Device Mntr Port	-35 dBm	-23 dBm
Data PHY Rate	24 Mbps	867 Mbps
Mgmt PHY Rate	24 Mbps	6 Mbps
Ch Bandwidth	20 MHz	80 MHz
No. of Spatial Streams	1 streams	2 streams
Modulation	16-QAM (1/2)	256-QAM (5/6)
Guard Interval	Long	Short

Other L2 Stats	Device	AP
Retransmissions	0 pps	0 pps
Media Utilization	0.00 %	0.00 %

Traffic	Device TX	AP TX
AC Background	0.000 Mbps	0.000 Mbps
AC Best Effort	0.000 Mbps	0.000 Mbps
AC Video	0.000 Mbps	0.000 Mbps
AC Voice	0.000 Mbps	0.000 Mbps
Non QoS	0.000 Mbps	0.000 Mbps

Roam [4]
Successful Roam

Device: GalaxyS6

Source AP: Cisco_AP2_BEFC
RSSI: -67 dBm
Phy Rate: 58.5 Mbps

Target AP: Cisco_AP1_44FC
RSSI: -30 dBm
Phy Rate: 24 Mbps

Roam Delay: 66 ms

Authentication: 1 ms
Association: 2 ms
EAP processing: 0 ms
Key exchange: 0 ms
DHCP: n/a

Downstream Roam Delay:
Non QoS: 0 ms
Background: 0 ms
Best Effort: 2825 ms
Video: 0 ms
Voice: 0 ms

Upstream Roam Delay:
Non QoS: 92 ms
Background: 0 ms
Best Effort: 1152 ms
Video: 0 ms
Voice: 98 ms

Ap Last Status Code: 0
Ap Last Reason Code: 0
Device Last Status Code: 0
Device Last Reason Code: 0

Figure 2. Ixia IoT dashboard view with real-time statistics

Challenges

Battery-powered devices have been around for more than a century, but the tools used to measure the charge consumption of, say, a flashlight or a transistor radio are insufficient for IoT devices. A typical IoT device spends most of its time in states of very low activity, such as hibernate or sleep modes. The device consumes just enough power to stay “on” for several minutes or hours, at which point it wakes up, performs its functions, and then returns to sleep. Depending on the application, the device may also transmit data to a gateway, router, or base station, or it may wait and transmit a large block of data at once, thus saving the battery power associated with hand-shaking and data transmission overhead.

As a result, the current waveform for an IoT device is highly dynamic, moving very quickly from sleeping at microamps to operating at perhaps hundreds of milliamps and then returning just as quickly back to the sleep mode. There are several key challenges associated with this scenario.

The engineer must be able to:

- Measure very low currents with precision.
- Measure the full dynamic range of the current waveform without glitching during range changes.
- See the waveform in order to identify both typical and anomalous charge consumption behavior.
- Identify how much charge is consumed by various events in order to understand the implications of various hardware, device configuration, and firmware programming decisions.

Solutions

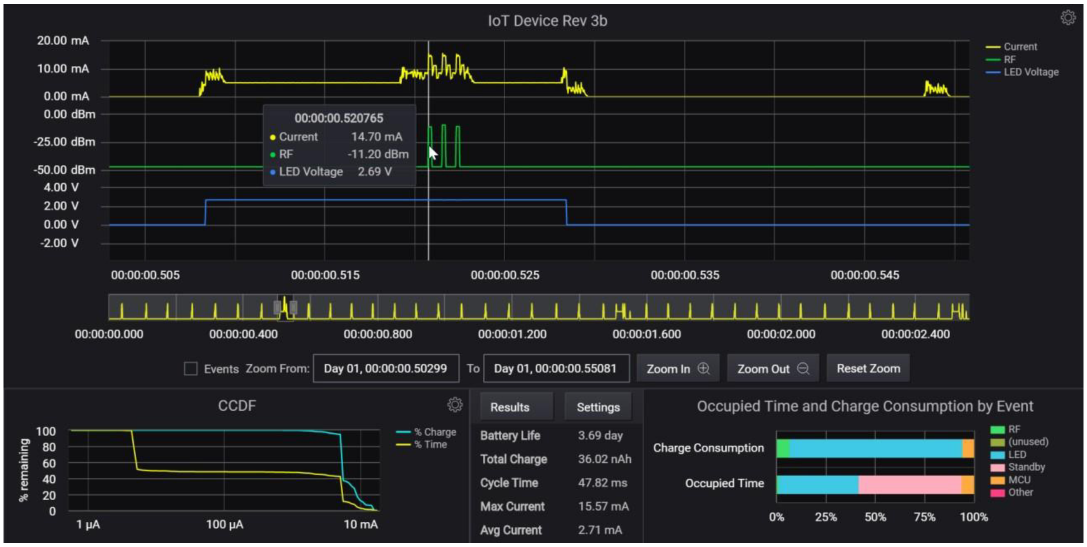
A digital multimeter (DMM) is a relatively common and inexpensive tool that is appropriate for measuring low currents with precision (Figure 3). Some DMMs also have good visualization capabilities. A DMM will typically not have the dynamic range or measurement bandwidth necessary to properly measure fast transients in IoT device current waveforms.

Figure 3. Keysight 34465A 6½ Digit Multimeter

A DC power analyzer with source-measure units (SMUs) has much better bandwidth than a DMM, and it also has better visualization tools. An SMU, such as the N6781A, also has seamless ranging, which means it can measure at both the low and high ends of a current waveform without the glitching commonly associated with range changes.

An event-based power analysis solution, which is based on a DC power analyzer, can provide engineers with the necessary numeric and visual insights to properly make product development decisions. By combining a DC power analyzer with an RF event detector and analysis software, engineers can quickly see what various operational events cost in terms of charge consumption.

For example, the Keysight X8712A battery life optimization solution can correlate battery charge consumption with RF and DC subcircuit events to optimize battery life (Figure 4).



00:00:00.520765

Current	14.70 mA
RF	-11.20 dBm
LED Voltage	2.69 V

□ Events Zoom From: Day 01, 00:00:00.50299 To Day 01, 00:00:00.55081

Battery Life	3.69 day
Total Charge	36.02 nAh
Cycle Time	47.82 ms
Max Current	15.57 mA
Avg Current	2.71 mA

Figure 4. Event-based power analysis performed on Keysight X8712A battery life optimization solution

Compliance

Compliance differs from cybersecurity, continuity, and connectivity because compliance has legal implications and can be enforced by government agencies with professional law enforcement. In the U.S., devices with radio transmitters must comply with standards from with the Federal Communications Commission (FCC), and FCC compliance is accepted by some other countries. The European Union uses a regulatory scheme called RED/CE, and this is also accepted in various countries. Virtually every country in the world has some sort of regulatory body that regulates RF transmitters.

Challenges

In addition to knowing what standards apply to a given IoT device in various countries, device developers face several additional challenges. The standards are being incrementally updated, which means that developers must keep up to date. Manual testing is possible, but it requires a highly skilled compliance test engineer. In addition, the evolving standards mandate effective and efficient use of radio spectrum, and this results in very complex test items that make manual testing almost impossible.

Furthermore, the increasing RF congestion in the unlicensed industrial, scientific, and medical (ISM) bands has led to interference that makes compliance more important and challenging than ever. This is complicated, however, by time-consuming data acquisition, complex new tests that require automation, and the large volume of data that must be processed into results.

Solutions

The Keysight IOT0047A wireless device regulatory test solution (Figure 5) provides dedicated software that allows the user to cover the latest test cases for ETSI EN300-328/301-893, FCC Part 15.247/407, and DFS. It supports many different technologies associated with IoT devices, including frequency hopping, adaptivity, MIMO up to 8 channels, and common radio formats such as WLAN, *Bluetooth*® and Zigbee®. It simplifies test automation and improves speed using the signaling test method (with IOT8720A wireless test solution or companion device), it reduces test complexity with readily available software, and its report generation function proves adherence to regulatory standards.

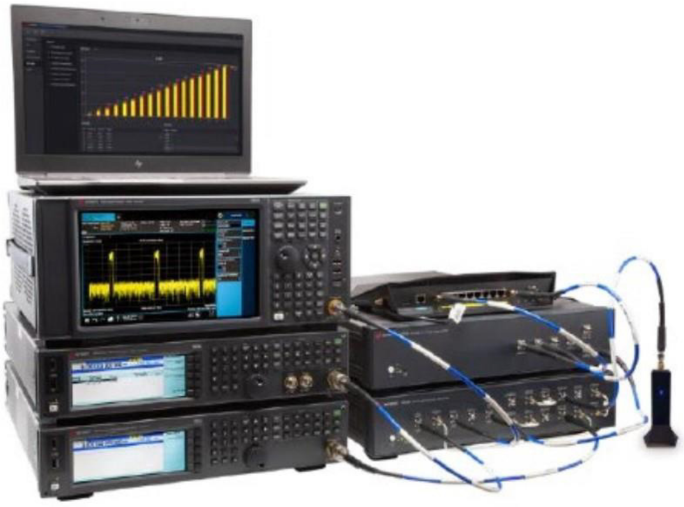


Figure 5. Keysight IOT0047A wireless device regulatory test solution

Coexistence

Because of the increasing use of unlicensed spectrum, especially around 2.4 GHz, the ability for devices to continue operation without interfering with each other is becoming more challenging. Testing for proper coexistence is therefore also becoming both more challenging and more important.

Challenges

If all of the devices in the 2.4-GHz band used the same wireless formats, coexistence could be largely mitigated on the protocol level. Unfortunately, there are many different wireless formats in the 2.4-GHz band, and some transmitters around 2.4-GHz follow no wireless format at all: microwave ovens.

When these incompatible radio formats collide, they slow throughput, cause increased retries, and result in a general failure of devices to achieve their wireless performance goals. One side effect of this is that extra battery charge is consumed, which shortens battery runtime.

Solutions

There are basically four ways to test for coexistence, and each has advantages and drawbacks. In all four approaches, you should monitor the electromagnetic environment with a portable instrument with real-time spectrum analysis (RTSA) capabilities, such as a FieldFox handheld RF and microwave analyzer (Figure 6).

Figure 6. Keysight FieldFox Handheld Microwave Analyzer

Open air test method

In the open air test method, you simply expose the equipment under test (EUT) to a companion device and whatever transmitters and receivers happen to be in the environment. This is very simple and inexpensive, but it is the least controlled and least repeatable of the four methods. It also requires the most time of the four methods. Ambient signals may interfere in unreproducible ways, and this approach may not be accepted by regulatory agencies, such as the U.S. Food and Drug Administration (FDA).

Single-chamber test method

A second method is to put the EUT and its companion device into a relatively large anechoic chamber along with a vector signal generator (Figure 7) to generate unintended signals and a signal analyzer (Figure 8) to measure the combined signals. The advantages of this approach are that a large chamber has room for realistic physical separation. This allows for multiple EUT orientations, and paired interfering devices are possible.

Figure 7. Keysight N5182B MXG vector signal generator

Dual-chamber test method

In the dual-chamber approach, one chamber contains the EUT, and the other contains the paired device and a signal analyzer. An interference source outside the chambers goes through a power divider/combiner into an antenna that transmits to the EUT. An attenuated transmission path connects the two chambers.

Figure 8. Keysight N9020B MXA signal analyzer

Coaxial test method

In the coaxial test method, all of the equipment is connected via coaxial cables. This approach produces the most reproducible results, and if your vector signal generator has high bandwidth, you can simulate multiple interfering signals at once. The vector signal generator can present worst case interference and controlled conditions because it does not back off, unlike adaptive devices.

Cybersecurity

Cybersecurity is perhaps the most important consideration for IoT applications. Creating an unsecure application or device may lead to consequences that are worse than not having an application in the first place. Cybersecurity is not something that can be added as an afterthought; it must be considered, designed for, implemented, and tested throughout the process.

Challenges

The vulnerability of the IoT is well-known, and a survey by the Poneman Institute and shared assessments concluded that 76% of risk professionals believe that cyberattacks on their organization are likely to be executed through the IoT. This perception is well-grounded, as 98% of all IoT device traffic is unencrypted. Both personal and confidential business data are exposed on the network, and this provides cybercriminals with the ability to monitor unencrypted network traffic, collect personal or confidential information, and exploit that data for profit on the dark web.

Cybersecurity for IoT devices presents new challenges. Traditional IT devices, such as laptops, tablets, and phones, can apply security updates quickly. On the other hand, many IoT devices have firmware that is difficult or impossible to update. Furthermore, vulnerabilities in IoT devices can be expensive, damaging, and outright dangerous once exploited. A hostile actor could bring traffic to a standstill in a major city, including first responders. Cybersecurity events launched by a nation-state could be extraordinarily dangerous, especially if combined with a physical attack.

The healthcare IoT is particularly important, and it is also vulnerable. Most healthcare virtual local-area networks (VLANs) mix IoT and IT assets, and this can lead to the rapid propagation from users’ computers to vulnerable healthcare IoT devices on the same network. In addition, many threats to healthcare organizations involve imaging devices, and these threats disrupt the quality of care and allow attackers to obtain patient data. In addition to generating customer complaints, exfiltrated data may lead to HIPAA enforcement or FDA monitoring or both. For these reasons, healthcare IoT cybersecurity represents a significant concern.

Solutions

Ensuring resiliency and security in deployed IOT devices requires comprehensive, automated IOT security testing throughout the product development process. Development organizations must embrace continuous security validation in their continuous integration / continuous delivery (CI/CD) pipelines. Product development teams must conduct exhaustive device testing using the most relevant, up-to-date attacks available, from low-level protocol fuzzing to upper layer attacks. Protocol fuzzing finds the unknown vulnerabilities, and application-layer attacks, such as password brute-forcing and encryption strength validation, discover vulnerabilities against known attack types.

With Keysight's IOT Security Assessment, comprehensive IOT security validation is just a few clicks away. Development organizations can easily integrate Keysight's API-driven solution into their development pipelines with a single API for control and reporting. Its modular and extensible framework makes it is easy to plug in additional existing or third-party attack modules and control them all from that single API. Keysight IOT Security Assessment can validate virtually any connected device against a broad range of attacks, known and unknown, so that critical devices can be secured before leaving the development environment.

Keysight IOT Security Assessment builds on 20+ years of leadership in network security testing to reveal security exposures across any network technology. The ongoing research from Keysight's Application and Threat Intelligence team ensures regular updates, so subscribers have access to the latest protocol fuzzing and attack techniques. It is a proven technology that has already been used to find dozens of common vulnerabilities and exposures (CVEs), all of which have been responsibly disclosed and published. It is obviously much less expensive to find and fix vulnerabilities before you send IoT devices out in the wild where they are much more expensive, or impossible, to fix.

Beyond the 5 C's: Customer Experience

The first five C's—connectivity, continuity, compliance, coexistence, and cybersecurity—are all important, but a sixth C, customer experience, can set a device apart from its competition or cause an application to fail altogether. Users generally experience IoT devices through software and firmware applications, and testing these applications can be very difficult.

The first reason that software testing is difficult is that the software often contains many features, and these features are highly customizable by the user. The number of possible paths through the software is extremely large, and the number of permutations of the various setting can easily run into the millions or billions. There are simply far too many variations to test, although automated software testing tools that use artificial intelligence can test many more possibilities than even a team of human testers can.

A second major hurdle is that many IoT applications run on many different hardware platforms. It is relatively simple to test an application on a PC. It is much more challenging to make sure that a given application works on PCs, tablets, kiosks, smart phones, smart watches, and other common hardware.

An additional complication for software testing is the fact that each hardware has revisions and operating systems that must be supported. For example, a recent evaluation of smart phones and operating systems considered nearly 30 cell phone variations from just three hardware vendors. Furthermore, testing an IoT application end-to-end may involve several different platforms (Figure 9). For example, consider a typical healthcare application. One system may monitor patient data in real time. A second system at a nurses' station might display data and provide alerts and alarms. The nurse might want to send a screen capture or data file to an on-call physician, who sees the information on a third device. Finally, some of this data may need to be store into an electronic medical records (EMR) system, which involves a fourth level of complexity. In addition, the patient or patient's representative may need to access this information on a PC or tablet via a patient portal running on a browser.

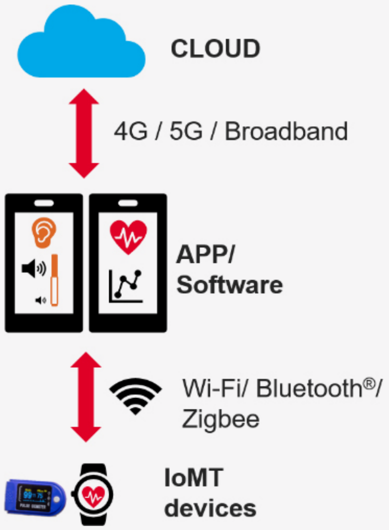


Figure 9. A simple Internet of Medical Things (IoMT) application

Finally, the speed expectations of the modern era introduces two additional challenges. The software tester must measure and evaluate the responsiveness of the applications, and the time to market pressures mean that the software testing itself must be completed quickly, which means that it must run in an automated fashion, without pause.

Conclusion

The IoT presents many exciting and transformational opportunities in dozens of vertical markets, but the design and test challenges are formidable. By using the framework of the 5 C's + 1 of IoT— connectivity, continuity, compliance, coexistence, cybersecurity, and customer experience—product development teams can quickly bring products to market that will satisfy customer needs and withstand the rigors of the real world.

Bluetooth® and the *Bluetooth*® logos are registered trademarks owned by Bluetooth SIG, Inc., and any use of such marks by Keysight Technologies is under license.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus