White Paper

5 Key Test Considerations for Cellular IoT Devices

A Guide for Designers and Developers Creating Cellular IoT Devices

Cellular IoT: A Huge Market Opportunity

The internet of things has powerful applications and implications for almost every industry and individual. In critical services like healthcare, transportation and logistics, for example, it can help improve service quality and reliability, by giving everyone access to the information and insight they need to deliver the very best service at critical moments.

Cellular modules have made it easy to build robust IoT devices, but cellular has some unique pitfalls that developers and designers that are new to the technology may not know how to avoid.

For consumers, it's connecting every aspect of our digital lives, to create something far greater than the sum of its parts. When devices and components can talk to each other, services can be enhanced in new and exciting ways, enabling developers to imagine entirely new products, and improve the functionality of existing ones.

Cellular connectivity takes IoT to the next level. With cellular-enabled IoT devices, you can deploy connected devices anywhere they can connect to a 3G, 4G or other cellular network. That can take just about any form, from a smart energy meter that automatically reports its readings to the supplier, to a new generation of standalone personal fitness trackers.

For designers and developers seeking to bring new devices to market, the ability to connect smart devices to a central control system via a cellular network represents a huge opportunity.

27 BILLION CONNECTED DEVICES IN USE GLOBALLY BY 2025—MACHINA RESEARCH

Modules Make it Easy to Design New Cellular-Connected IoT Devices

The barriers to entry into this exciting market are falling, thanks to the widespread availability of modules: pre-tested, pre-built, pre-packed cellular modems that can be quickly and easily integrated into a device design. Modules have made it extremely simple and cost-effective to add cellular connectivity to devices, even for developers with limited knowledge of cellular.

Modules don't just make building a device simpler; they also greatly simplify testing. With the average cost of testing a smartphone reaching between $1.5 and $2 million, pre-tested modules can save designers and developers millions of dollars—and bring IoT innovation within easy reach for developers without that kind of test budget. But cellular IoT testing doesn't begin and end in the module itself.

For those who are new to the world of cellular IoT, there are a number of testing challenges of which to be aware. If they aren't properly addressed, devices can end up delivering inferior experiences, failing in the field, or never making it to market at all.

This paper sets out the five key test considerations when designing and developing new cellular IoT devices, analyzes the risks of not addressing them adequately, and presents practical advice on how best to tackle them and make the most of the new cellular IoT opportunity.

Five Key Test Considerations when Designing and Developing Cellular IoT Devices

While modules may have vastly opened up the field for cellular IoT device development, there is still a lot to think about before bringing a new device design to market. Here are five key considerations that every cellular IoT designer or developer should incorporate into the R&D process.

#1) What are the Cellular Use Cases for the Device?

For your device to perform properly, you need to identify and analyze every aspect of your unique use case for cellular and design around them.

Up front, it's worth asking yourself these types of questions:

- Will the device be mobile or static?
- Will it have high or low data demands?
- Can it carry voice as well as data, and if so, what are the regulatory implications?
- Will it be used in critical infrastructure or safety-of-life scenarios? If so, can it make priority bandwidth requests to the networks it will be deployed on?
- Is location awareness important to its proper functioning?
- Which generation of cellular will it use?

By fully scoping out your own use case for cellular, you can build up a full picture of the parameters that your device will need to be tested within to gain a clear idea of its real-world performance and ensure that it's fit for purpose.

#2) Will it Pass the Relevant Carrier Acceptance Tests?

Every network operator has acceptance tests to ensure that no malicious or vulnerable devices can connect to the network and introduce threats.

Products that fail the acceptance test will not be allowed to connect to the carrier's network, so passing the test is critical. Tests have been simplified in recent years, but they must still remain a key consideration throughout the design and development process.

#3) Is the Device Resistant to Cyber-Attack?

With greater connectivity comes greater vulnerability to malicious cyber-attacks. While cellular networks, especially 4G LTE, are relatively secure, they are just one link in an otherwise weak chain. Attacks can leverage a compromised enterprise network, weak device-to-server encryption, insufficient password and policy enforcement, and physical access in the field.

#4) Can the Device Maintain Consistent and Reliable Network Connectivity Throughout its Lifetime?

Consistent and reliable connectivity is the key to ensuring that your new devices will perform to specification across all locations and scenarios in which they are used. In test terms, that means making sure they will:

- Work with all of the primary and roaming networks they will need to connect to throughout their lifetime
- Connect to local and regional networks in all geographies where they are likely to be used
- Be resistant to any kind of disruption that could affect connectivity

#5) Will a Battery-Powered Device Perform to Specification for its Full Projected Lifespan?

If your device relies on a battery, you need to anticipate conditions that could impact its battery life and thus reduce its useful lifespan. In the cellular world, a device's power consumption is affected by network conditions.

For example, a device may have an expected lifespan of three years under normal conditions. But when devices live on the cell edge they may occasionally lose connectivity, and if the device software's retry strategy for communication errors is too aggressive, that may drain its battery much faster. Scenarios that could affect battery life should be built into any test regime—especially for devices that will be deployed in locations that make onsite maintenance or replacement difficult.

The 3 Big Reasons IoT Testing Matters

Proper, thorough testing is the key to effectively overcoming each of these challenges—but they're not the only reasons why testing cellular IoT devices is so important.

Here are three big reasons why you need to make cellular testing a top priority:

Getting it Wrong Delays Time-to-Market

Debugging cellular devices can take longer than wireless technologies such as Wi-Fi. Testing on a live 3G or LTE network only exposes the device to the local conditions at the time, and is likely to miss important corner cases that will happen in the real world. In a highly competitive market, no device developer can afford the kind of slowdowns that field failures can cause. It's essential that in your mission to get to market quickly, you don't sacrifice the quality or rigour of your device connectivity testing.

A Poorly Performing Device May Impact Critical Services

If your device has a role to play in critical infrastructure, is used to safeguard life or property, or serves an essential operational purpose, the impacts of inadequate testing can be huge. For example, if a smart traffic light loses network connectivity, traffic management systems may fail, causing widespread disruption.

An Insecure Device Can Cause Widespread Damage

If your device is vulnerable to cyberattack, user data can end up becoming compromised, which can have a detrimental impact on your reputation and lead to costly product recalls. In 2016, for example, one model of webcam had to be recalled as a vulnerability allowed hackers to use it to orchestrate a **DDoS attack** that affected much of the internet on the U.S. east coast.

70% of the Most Common IoT Devices are Vulnerable to Attack–HP

Five Best Practices for Critical IoT Device Testing

So, what must you to do ensure your testing is adequate to overcome those challenges? Here are five best practices to help you get started.

#1) Test with a Repeatable Cellular Network

Testing cellular devices on the local live network is a trouble-prone exercise.

- The live network doesn't provide a mechanism to probe or capture packets
- Security testing across the cellular link will provide results that are inconsistent with what the device may see in the field, as each carrier has their own network security
- Accurate battery testing requires exercising the device across a set of cellular network conditions, such as strong vs. weak signal, sporadic interference, and congested conditions

Rather than using the local live network to test, look to the emerging generation of network emulators that make it straightforward to bring a repeatable cellular test bed into any hardware or software lab.

#2) Understand the Different Scenarios in Which Your Device May be Used

Listing out all the individual scenarios and use cases that you need to test your device in is critical to ensuring truly robust testing. That list is going to include:

- Moving the device between different networks and network types
- Ensuring that the device will be able to function as the network environment changes
- Testing over-the-air device updates in case any will need to be rolled out in the future
- Determining how the device will hold up against potential malicious attack attempts

Emulating as many conditions as possible will help you understand exactly how your devices may be impacted in the real world.

To do that, you'll first need to build a comprehensive list of test cases, then ensure that you have access to the appropriate test equipment.

#3) Test Based on Real-World Scenarios

Tests should reproduce real-world scenarios as faithfully as possible, to allow you to build up a reliable picture of real cellular connectivity performance.

When selecting your testing equipment, seek out tools that can help you accurately emulate those kinds of scenarios. That may sound expensive, but the new generation of testing tools has dramatically reduced the cost of conducting these kinds of tests.

#4) Look at your Devices Through a Hacker's Eyes

Smart devices are an attractive attack surface, so an important part of your testing is going to be identifying exactly where your devices are vulnerable.

Cyberattacks on cellular IoT devices are increasing in number and sophistication, so it pays to use tools that can emulate as many kinds of malicious attacks as possible.

With test equipment and software that can simulate multiple different types of attacks, you can accurately understand how your device will hold up against each one—not just in terms of whether it was compromised, but also what impact the attack had on factors like battery life.

#5) Approach Testing as an Ongoing Process, Not a One-Off Event

Testing shouldn't be something that ends once your device is in the hands of a user or deployed in the field. With a continuous approach to testing, you can work to deliver stronger, more robust devices in the future, as well as keep your existing device portfolio as strong as possible with the help of frequent updates.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

How Spirent Can Help

For many developers, testing and assuring cellular IoT device performance brings a number of new challenges. To get the most from your testing, it helps to have an expert partner. Spirent has drawn on decades of network and device testing experience to create a cost-effective lab solution for IoT developers. Our integrated suite of tools covers the four major aspects of IoT testing and assurance:

- Connectivity testing
- Security testing
- Battery life testing
- Carrier acceptance testing

See Spirent IoT Testing in Action

Explore case studies and more today, and see how our testing and assurance solutions have helped IoT developers to bring innovative products to market, fast.

View Now

Talk to us today about how we can help you test and assure your cellular IoT devices.

spirent™
Promise. Assured.

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defense
info@spirentfederal.com | spirentfederal.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev B | 08/18