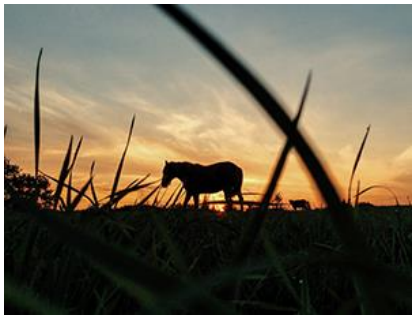
www.pipelinepub.com
Volume 17, Issue 9

Taming the IoT Wild West

By: Brian Davis



The Internet of Things (IoT) can be described as the Wild West of the RF world. It's a relatively new frontier with an immensely diverse array of technologies, multiple standards from different global organizations, and little compatibility. All are competing for marketshare and not everyone will be left standing. Test and measurement can be considered the sheriff, providing a means to develop, produce, and verify designs and well-performing IoT devices and networks.

Naturally, IoT brings a new set of challenges, particularly in mission-critical applications such as healthcare, factory automation, transportation, and utilities. The stakes are highest in these mission-critical IoT operations, so it's crucial that UE and networks operate at optimal efficiency. This is especially true in the RF domain, where environments significantly change once they reach the end users.

Although cost is a major factor in many IoT designs, given what's at stake in mission-critical applications, factors such as data reliability, security, and ease of use are much more essential. Rigorous testing of IoT products is a necessity for these reasons. A failure to meet RF standards can lead to regulatory scrutiny, or a downtime in manufacturing operations that can cost millions of dollars.

Maintaining connectivity

RF connectivity is the common bond in the numerous IoT use cases. It is employed in environments from factories and hospitals to automobiles and electrical grids. It can be short-range wireless links utilizing cellular, Wi-Fi, and Bluetooth®, or long-range low-power wide-area network (LPWAN) technologies such as LoRa, Sigfox, and NB-IoT.

Mission-critical applications, including industrial IoT and medical body area networks, are exploring the power of added connectivity given their gravity. Connectivity services such as these enhance human decision-making in highly dynamic environments that call for another level of data reliability to prevent the high cost of failure.

Enduring connectivity is a collaboration between network and UE. For example, it won't be uncommon for there to be interference between two different UE using various technologies and within proximity to each other. For this reason, corralling all these technologies into UE that operate according to specification and with high reliability across IoT networks is critical at every level of the ecosystem, from chipsets and UE manufacturers to service providers and private network operators.

Standards impact

The emerging IoT standards are meant to address the critical needs of their respective application. While this often leads to confusion—particularly in the realm of test—this proliferation is necessary to effectively optimize hardware and firmware criteria.

Standards guide testing processes. Cellular technology is predominantly led by 3GPP. The global organization establishes specifications every four years, though incremental steps are taken between major releases. 3GPP does not cover conformance and compliance testing, however. 3GPP Release 13 (R13) included narrowband IoT and focused on more nimble communications methods, more efficient battery consumption, low power, and low data rates.

Other short-range technologies utilized in IoT environments, such as Bluetooth and Wi-Fi, have their own standards, as well. The Bluetooth Special Interest Group (SIG) passed version 5.2 in early 2021. It continues a focus on Bluetooth Low Energy (BLE), as well as high-speed, both of which are critical for IoT. The latest Wi-Fi technology—Wi-Fi 6e—is based upon the IEEE 802.11ax standard and outlines performance specifications for the 6 GHz spectrum. It will bring faster speeds to IoT environments.

A recent poll conducted by Anritsu found that these are the three predominant technologies for IoT UE designs. Cellular and Wi-Fi are used in 51 percent of designs, followed closely by Bluetooth (48 percent), according to poll respondents. Zigbee (25 percent) was a distant fourth.

Comprehensive testing

Ensuring UE operation and security within an IoT network requires comprehensive testing. As clearly evident, test solutions must support multiple wireless standards. Fortunately, the critical tests that need to be made are the same across these technologies. They must also be conducted quickly, reliably, and consistently in every case.

Transmit power, bandwidth, spectrum emissions, adjacent channel power (ACP), EVM, frequency error, phase noise, and sensitivity measurements all must be performed. Figure 1 is a display from a test instrument that includes key measurements. Below is a bit more detail on some of these tests.

Figure 1: Sample display from test instrument
click to enlarge

Adjacent Channel Power (ACP) – This measurement determines the power in a specified frequency channel bandwidth relative to the total carrier power. It is an important test in that it assures transmission quality and determines if power is leaking from the transmitter.

Error Vector Magnitude (EVM) – EVM measures how accurately a wireless system transmits symbols within its constellation.

Transmit power – The average power for an RF signal burst is measured to determine the power delivered to the antenna system.

Spectrum emissions – This measurement determines the out-of-channel emissions compared to the in-channel power. It is used to calculate if the excess emissions will cause interference.

Frequency error – This measurement ensures that the frequency hasn't leaked into another adjacent frequency.

Influence of 5G

With its high speed, large bandwidths, and low latency, 5G is a panacea for IoT, particularly mission-critical use cases. It does create new testing challenges, however, especially at Frequency

Range 2 (FR2), where millimeter (mmWave) bands are used. Unlike sub-6 GHz environments—used in 4G and 5G Frequency Range 1 (FR1)—antennas can't be bypassed, so coupled testing is not possible. With mmWave UE, antennas are integrated with the base stand and the RF front end. As a result, antenna-oriented measurements, such as total radiated power and peak beam surge, must be added to the list of necessary tests.

Ensuring compatibility

Given the use of multiple technologies within an IoT network, measurements must be made on the UE to ensure these technologies do not interfere with each other. Cellular and Wi-Fi desense and co-existence measurements verify that UE implementing both technologies is compliant. It is a particularly important test because cellular and Wi-Fi signals can easily overlap.

An OTA configuration with dedicated test systems and software allows the necessary tests to be made in the same environment. This is necessary to simulate a real-world scenario, so accurate and repeatable measurements can be made. Figure 2 is a display of an OTA evaluation. Since the antenna characteristics are displayed in a 2D/3D graph, it's possible to intuitively grasp the measurement results.

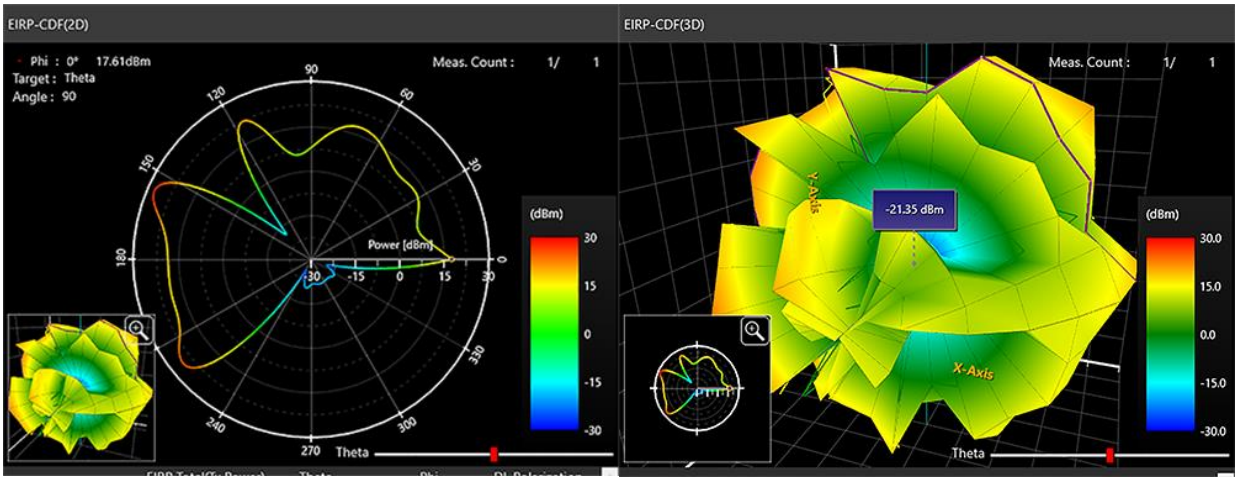


Figure 2: 2D (left) and 3D (right) graphs make it possible to intuitively grasp OTA measurement results.

Another common co-existence scenario is Bluetooth and Wi-Fi, because both share the same band in the 2.4 GHz range. A test solution must support both technologies. For Bluetooth verification, functionality such as adaptive frequency hopping (AFH) is beneficial. It facilitates analysis of interference from, and co-existence with, interfering signals, and provides graphical displays of frame error rate (FER) and masked channels when interfering signals are introduced.

Transmit power mode measurements are also key UE verification tools. Output power is troublesome for WLAN. When a UE connects to an access point or another device, a power surge occurs. Often, the power spike is not measured because it is "bursty." A transmit power mode measurement allows verification that the power levels are within specification and will not

interfere with the network or other device. Figure 3 is an instrument display showing an IQ constellation, power profile, and spectrum mask of a WLAN signal.

Figure 3: Instrument display showing IQ constellation, power profile, and spectrum mask of a WLAN signal
click to enlarge

Taming the IoT Wild West

Taming the Wild West known as IoT requires a comprehensive testing strategy for UE and networks. Testing characteristics, capabilities, and considerations can all be done with modern equipment that can simulate and measure test specifications and real-world scenarios. By doing so, all IoT use cases, including mission-critical networks, will meet key performance indicators (KPIs).