WHITE PAPER

Meeting New Challenges in Connected Medical Devices

Reduce risk, ensure efficacy, and accelerate time to patient help

KEYSIGHT

New Opportunities and New Challenges

As the need for less expensive and more accessible health care continues to increase, many practitioners and medical are relying on connected medical devices to monitor vital signs, perform electrical or chemical analyses, diagnose medical conditions, and even treat patients by administering things treatments such as electrical pulses or insulin. These technologies are improving the length and quality of countless lives, and they bring healthcare to patients outside of medical facilities. This extends the benefits of sophisticated technologies to persons who could otherwise not obtain or afford these treatments in a hospital setting.

This increased reach and growth, however, also means that the expectations, requirements, and challenges associated with these devices are increasing. Here are a few of the more significant issues that connected medical device designers and manufacturers face:

- The increasing number of wireless devices makes wireless coexistence both more important and more difficult.
- The cybersecurity threat landscape becomes greater.
- The demand by consumers, insurance companies, and governments for reduced healthcare costs puts additional pressure on device vendors, which makes hitting the highly profitable early adopter phase more critical than ever.
- The increasing use of devices by non-specialists on a variety of hardware and software platforms drives greater testing challenges for device firmware and associated apps.

Solving these problems drives a virtuous cycle, in which successful devices drive high adoption, which provides additional revenue for device vendors who can then produce additional devices. When connected medical devices work properly, everybody benefits: patients receive safe, low-risk and efficacious care, practitioners are able to help more patients, costs decrease, and the device manufacturers are rewarded with profit and growth.

Wireless Coexistence

The increasing use of connected medical devices alone is enough to make the problem of wireless coexistence more challenging than ever. However, the problem is further exacerbated by the growth in wireless consumer devices, such as cell phone, tablets, laptops, smart watches, wireless audio devices, and so on. In addition, the growth of the internet of things (IoT) into more demanding applications (smart cities, industrial IoT, smart buildings, smart grid, and smart agriculture) is consuming bandwidth and making collisions even more likely.

In addition, customers using these devices have increasing expectations for quality of service, even during while roaming and in demanding applications. Furthermore, standards from governmental and non-governmental regulatory and standards bodies, such as IEC 60601-2-27, continue to become more challenging to protect patients and practitioners from compromised essential performance. For example, the U.S. Food and Drug Administration (FDA) provides links to descriptions of several technologies that can help medical device designers and manufacturers improve the coexistence of their devices:

- Monitoring Radiated Coexistence Testing Using GMM-Based Classifier describes an approach using a classifier based on Gaussian mixture model (GMM) to categorize over-the-air (OTA) power measurements during radiated open environment coexistence testing (ROECT).
- Estimating the Likelihood of Wireless Coexistence Using Logistic Regression: Emphasis on Medical Devices proposes a framework that uses logistic regression to integrate the results of coexistence testing to estimate the likelihood of coexistence for a system under test.
- An experimental method for evaluating wireless coexistence of a Bluetooth medical device describes a method to evaluate reasonable worst-case interactions between wireless networks. This allows the engineer to determine three key metrics:
    - the maximum operational distance between wireless medical device nodes in a noise-free space
    - the minimum separation between IEEE 802.11n interfering nodes and the *Bluetooth*® device under test
    - the maximum channel occupancy of an interfering IEEE 802.11 network. When a list consists only of single words or sentence fragments, do not use periods or other terminating punctuation.

A similar article, Experimental Method for Evaluating Wireless Coexistence of Wi-Fi Medical Devices, address a similar methodology that evaluates the wireless coexistence of Wi-Fi connected medical devices.

Regardless of what coexistence testing method you use, you can reduce risk by using high-quality signal generators and signal analyzers. It is also often a good practice to use a hand-held signal analyzer with real-time signal analysis (RTSA) capabilities to monitor and document the electromagnetic environment during the test.

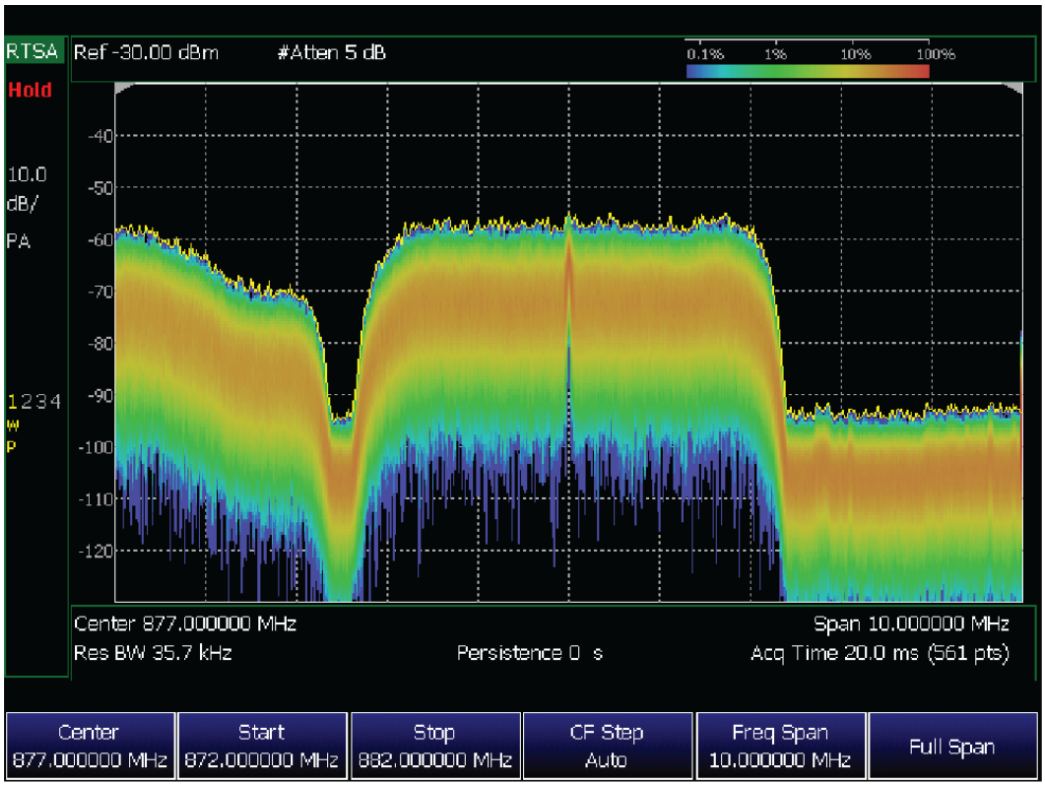

Figure 1. A signal captured using FieldFox's RTSA density display where the interfering signal appears in the middle of the screen

Cybersecurity

The rapid growth in connected medical devices has made increased the temptation and the opportunity for malicious actors to engage in cybercrime for three reasons. First, the sheer size of the attack surface is increasingly large and growing by the minute. Second, the move of connected medical devices into increasingly mission-critical and life-sustaining applications makes the monetary value of a successful breach in a ransomware scenario more lucrative. Third, the increasing use of inexpensive devices by patients outside of medical facilities means that the responsibility for specifying, provisioning, and maintaining appropriate cybersecurity defenses has moved out of the hands of hospital information technology professionals and into the hands of individual users, many of whom lack the mindset or the education to perform these tasks appropriately.

Furthermore, some medical device manufacturers have incorporated wireless chipsets and modules into their devices with little cybersecurity testing, incorrectly assuming that the chipset manufacturers had adequately ensured that their components were secure against cyberattacks.

Researchers at the Singapore University of Technology and Design (SUTD) have identified two families of cybersecurity exposures and vulnerabilities, which they dubbed SweynTooth and BrakTooth. In their article, Unleashing Mayhem over Bluetooth Low Energy, the SUTD team exposes "flaws in specific BLE SoC implementations that allow an attacker in radio range to trigger deadlocks, crashes and buffer

overflows or completely bypass security." The SUTD team has documented these flaws in mainstream products from well-known vendors, most of whom have released patches to fix the flaws.

Another set of defects identified by SUTD researchers is called BrakTooth. A white paper from the SUTD team, BRAKTOOTH: Causing Havoc on Bluetooth Link Manager, describes a set of cybersecurity exposures and vulnerabilities that affects more than 1,400 products. The paper describes BrakTooth as, a "family of new security vulnerabilities in commercial BT stacks that range from denial of service (DoS) via firmware crashes and deadlocks in commodity hardware to arbitrary code execution (ACE) in certain IoTs." Again, these flaws were demonstrated to occur in devices from many well-known manufacturers.

Of course, cybersecurity issues are nothing new. What makes this set of issues extraordinary in the context of connected medical devices is that the flaws have attracted the attention of the FDA. The FDA Safety Communication, SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices, provides recommendations for connected medical device manufacturers and puts the manufacturers on notice that the regulators are paying careful attention to this issue. Manufacturers are advised to, "Conduct a risk assessment, as described in FDA's cybersecurity postmarket guidance, to evaluate the impact of these vulnerabilities to affected devices and develop risk mitigation plans," and a device manufacturer who fails to properly mitigate these known cybersecurity issues could be in jeopardy if a cybercriminal exploited SweynTooth vulnerabilities in their devices.

It is imperative the connected medical device vendors demonstrate that their devices are immune to cybersecurity attacks through SweynTooth and BrakTooth flaws, and that they stay vigilant against new types of cybersecurity threats.

Need to Get to Market Quickly

A third trend that increasingly challenges to connected medical device engineers is the need to get to market quickly. Of course, time to market has always been a consideration for any medical device development team, but the pressure becomes increasingly intense as consumer expectations for new devices increase. As the world population ages and new diseases proliferate, the need for new devices becomes greater, and time to market quickly turns into time-to-patient-help. Also, much health care spending power is concentrated in the hands of insurance companies and governments. These large customers have the power to influence payment amounts, so hitting the highly profitable early adopter phase of a product adoption cycle becomes increasingly critical.

These shifts mean that regulatory compliance testing is no longer just a “check-the-box” item on a project team’s list. To reduce time-to-patient-help, regulatory compliance must become a competitive advantage that accelerates a product’s time to market ahead of competition and in time to help patients and practitioners who need the device.

The key metrics and insights to consider with respect to regulatory compliance include:

- Time to get through compliance test
- Cost to get through compliance test
- Test margins for the individual tests
- Best practices for product design
- Best practices for working with the regulatory compliance vendor
- Optional tests to consider in future projects

By changing one’s perspective on regulatory testing from an obstacle that must be passed to an opportunity to improve a product, engineers can serve both the best interests of their companies, patients, and medical practitioners with safe and efficacious devices. Furthermore, as medical devices increasingly include one or more radios (BLE, Wi-Fi, cellular), regulatory testing must go beyond EMI/EMC and include transmitter, receiver, radio behavior, and specific absorption rate (SAR) testing.

Greater Software Testing Challenges

The movement of connected medical devices from the hospital or medical center into the hands of patients is driving another major trend: the need for greater software testing. There are several reasons for this.

First, medical device engineers can no longer assume that the users of their software will be willing or able to invest time in training or to read an instruction manual.

Second, even if users read the manual, they likely do not have the medical background to understand procedures or how to interpret results. The usability therefore becomes critical to ensure that the results are accurate and that the user understands what the results imply and how to proceed.

Third, the medical device engineer cannot assume that the software runs on a personal computer or other device with a large display. Users expect to be able to run apps on cell phones, tablets, laptop computers, and other devices. In addition, they expect that the apps will run on a variety of software platforms.

Finally, users of certain types of connected medical devices may struggle with impaired vision, inexperience using modern technology, shaky hands, or hearing impairments that prevent the user from responding to audio cues or unnecessarily complex interfaces.

These shifts in the users of connected medical devices mean that the challenge of testing both the apps embedded in medical systems and offline versions of the apps face unique testing challenges that require automated test solutions to obtain the necessary test coverage.

Key metrics that connected medical device software test engineers must consider include test coverage, time to complete a test, time to modify a test to reflect design changes, and the number of hardware and software platforms covered. Engineers should also consider testing the performance of cloud applications, including initial access time, latency, and data rates provided when a medical professional needs to review or monitor a patient's condition.

Medical device engineers should refer to International Electrotechnical Commission (IEC) standard 60601-1-6, which relates to the usability of medical devices.

Conclusion

Engineers who design and test connected medical devices are providing innovative solutions that improve both the duration and the quality of patient lives. As these devices proliferate away from hospitals and medical facilities, several types of challenges become greater. The challenge of wireless coexistence becomes greater as devices experience more prevalent overlaps in space, time, and frequency. The challenge of cybersecurity becomes greater as the attack surface increases and the move into more mission-critical applications make ransomware more potentially lucrative.

The need to get to market quickly makes it more important than ever to turn regulatory compliance testing from a check-the-box item into a competitive advantage. Finally, as the number of users, hardware platforms, and software platforms increase, the software testing challenge becomes exponentially greater.

By using high-quality test solutions and guidance from organizations such as the IEC and the FDA, test engineers can overcome these challenges and provide users with safe and efficacious devices.

For more information on Keysight Technologies' products, applications, or services, please visit: www.keysight.com