Evolution of The Connected Healthcare System

Technology in the healthcare industry has evolved tremendously over the last five years. Technology is now compact, faster, and more affordable. The expectation is that all new healthcare devices and tools are intelligent — with multiple sensors connected wirelessly to each other and the internet. The combination of advances in the Internet of Things (IoT), artificial intelligence (AI), machine learning (ML), and cloud services impact the changes you see in healthcare today.

In this white paper, you will learn about four critical technology changes in the healthcare industry today:

- healthcare IoT evolution
- management of connected medical devices
- speculation on the design and test process
- progression of IoT test solutions for the future

> "Everyone is trying to find a sweet spot for each of the wireless protocols and for the right use case. Healthcare devices need to be designed to be robust and operate seamlessly no matter where the patient is located."
>
> PHIL RAYMOND
> Head, Wireless Competency and Solution Architecture CoE, Philips Healthcare

Healthcare IoT Evolution

Technological advancement has dramatically changed the healthcare landscape. With the introduction of innovative solutions such as biosensors, wearables, and mobile applications, healthcare providers have access to real-time health data to access patient records and provide patient care remotely.

Many healthcare vendors are taking advantage of IoT to bring revolutionary products to the marketplace. In a recent Keysight interview, Phil Raymond, head of wireless competency and solution architecture CoE for Philips Healthcare, said healthcare IoT has initiated one of the most significant changes in the healthcare industry over the last five years. This is evident in both the connectivity of medical devices and the generated data.

With Philips Healthcare's vision to create a continuum of connected care, data is a byproduct of the process. The rate at which data is available from the IoT is increasing exponentially. IDC forecasts that the global data sphere will grow to 163 zettabytes by 2025.

The rate at which IoT devices are creating data is increasing exponentially. IDC forecasts that the global data sphere will grow to 163 zettabytes by 2025.

"The data has mostly been operating in a silo, whether at a nursing station, in the back-end server, or the device itself," Raymond said. "Interoperable data is critical to improve the future of healthcare and to reduce costs. As data becomes easily accessible, artificial intelligence and machine learning are slowly becoming mainstream at the clinical level."

AI and ML are no longer fiction. The potential for AI in healthcare is increasing as it's integrated into the healthcare ecosystem. Healthcare providers and device makers are combining AI and IoT to create advanced medical applications and devices for robot-assisted surgery, virtual nursing assistance, and administrative workflow assistance. Using these technologies, healthcare professionals provide a better quality of care tailored to each patient.

Management of Connected Medical Devices

IoT in the healthcare industry continues to thrive; however, some challenges need attention. Top challenges include interference, interoperability, communication protocols, and data security and privacy.

Interference

There has been a radical shift from wired to wireless medical devices, employing numerous protocols, including Wi-Fi and *Bluetooth*®. As many of these wireless technologies share the same radio-frequency spectrum, they are bound to interfere with the operation of other devices. Connected medical devices require testing to ensure their ability to operate correctly in the presence of other equipment.

The main focus in this form of testing is to measure and optimize performance in a fully controlled, impaired environment. When using different operating protocols, unexplained communications failures become commonplace. Failure to communicate is problematic, especially in a healthcare environment where life-critical incidents can occur.

Without testing critical medical devices to ensure their ability to operate properly in the presence of other equipment using dissimilar operating protocols, unexplained communications failures will become commonplace.

Interoperability

Medical devices such as smart infusion pumps, electrocardiograms, and wireless blood pressure monitors are critical to monitoring patient health. Impaired connectivity or interoperability issues in these devices can lead to communication errors during life-critical incidents. Caregivers rely on these devices to monitor patients remotely, so interoperability is vital. Qualifying these devices from end to end is critical in validating interoperability.

Communication protocols

The advances in wireless communication protocols have significantly boosted the potential of IoT devices. Each protocol has its barriers, and not one protocol today covers the considerable demands and scenarios of an IoT device's operation. "Because of that, IoT devices have multiple choices of connectivity," Raymond said. "Just like with cell phones where there's *Bluetooth*®, Wi-Fi, and near-field communication (NFC) connectivity, different requirements and use cases will drive the implementation of different radios in end devices."

> “Across the different industry regulatory bodies (FDA), security is a top theme. It will continue to drive challenges and drive barriers to adoption.”
>
> - PHIL RAYMOND
> Philips Healthcare

Data security and privacy

Connected medical devices have proliferated in healthcare facilities around the world. The resulting explosion of health data has created additional risks and vulnerabilities. In fact, many healthcare providers underestimate the cybersecurity and privacy risks that connected medical devices pose. Sensitive health data is a preferred target of hackers. That’s why the European Union’s General Data Protection Regulation requires medical device manufacturers to integrate new requirements to maintain compliance.

Wireless chipset manufacturers like Redpine Signals understand the importance of securing sensitive data in connected medical devices. The company produces a Federal Information Processing Standard 140-2-certified Wi-Fi module. The module enables system designers and device makers to ensure that their connected healthcare products handle sensitive data easily. The company is working to build more robust wireless chipsets that operate in complex healthcare scenarios, engineering manager Govardhan Mattela said in an interview.

According to Raymond, robustness and security are two critical considerations. “Across the industry regulatory bodies (FDA), security has been one of the top themes that will continue to drive challenges and create barriers to adoption.”

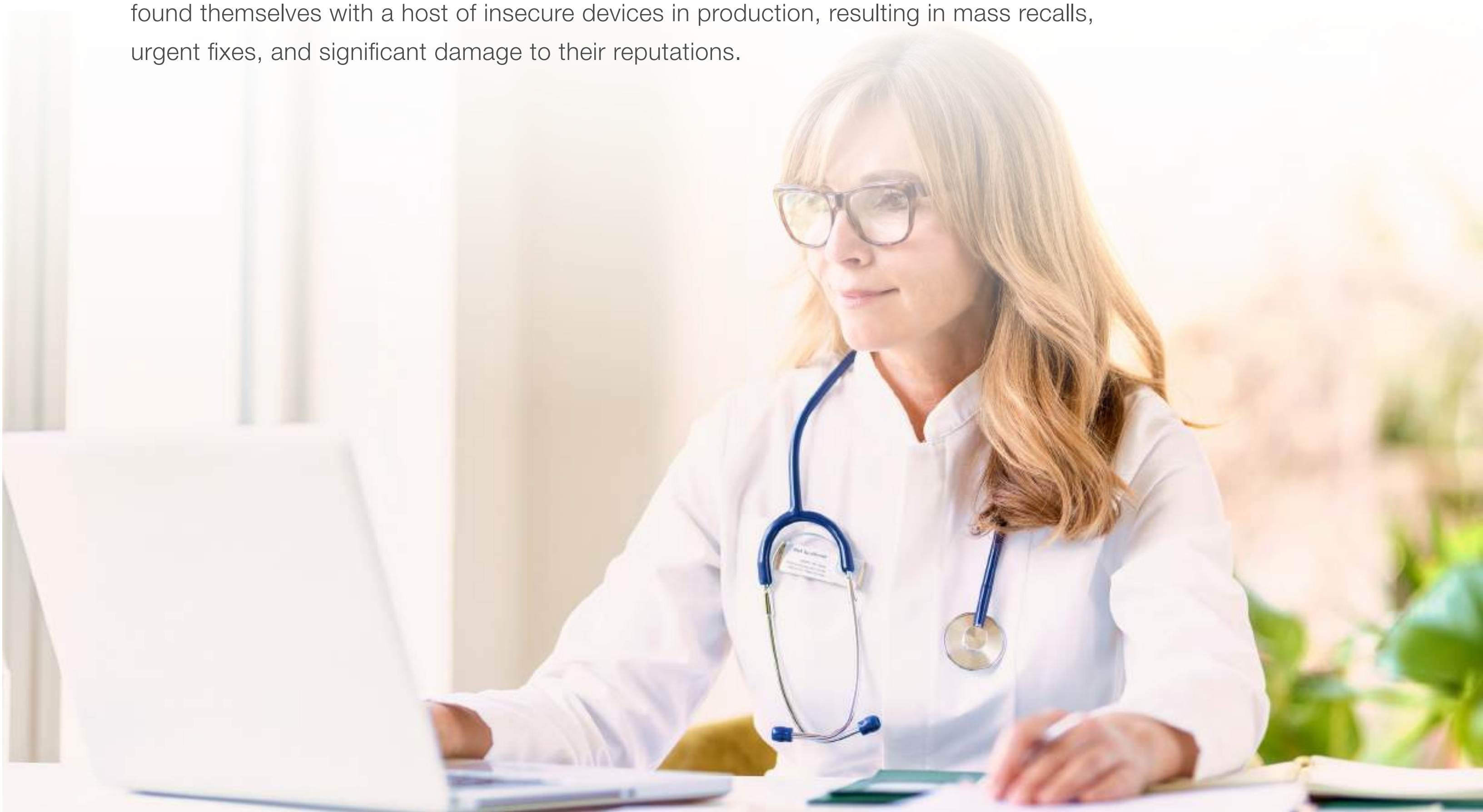
Cybersecurity device validation

Patient privacy and data protection in connected medical devices are enormous challenges for manufacturers and healthcare providers. But there's an even greater concern: patient safety. With the critical applications of connected medical devices, there's zero room for error. If a device ships with an insecure or non-resilient network interface, there is a substantial risk that an attacker can disable or hijack it. In a worst-case scenario, a cybercriminal could use the device to jeopardize a patient's health. For example, an attacker could force a provider to pay a ransom by threatening to put a device into high-power-draw state, make it stop receiving instructions, or even send incorrect telemetry data.

Downstream vulnerabilities in the supply chain further complicate this issue. Once medical devices are deployed, it's notoriously difficult to update their firmware to patch security vulnerabilities — especially on embedded communication chipsets. It's more cost-effective to validate medical devices across the entire attack surface and address any vulnerabilities before release.

Some of the most devastating device attacks (which can cause device failure) exploit downstream vulnerabilities like these. Such bugs are often well-hidden and easily missed without extensive protocol fuzzing.

The FDA's Safety Communication on the Sweyntooth cybersecurity vulnerabilities, which affected multiple medical device manufacturers, documents a good example. In the case of Sweyntooth, critical flaws in *Bluetooth*® chipsets from numerous well-known suppliers exposed medical devices to potential crashes, deadlocks, or security bypasses. Unfortunately, medical device manufacturers didn't catch it in advance. They found themselves with a host of insecure devices in production, resulting in mass recalls, urgent fixes, and significant damage to their reputations.



Speculation On The Design And Test Process

How is the healthcare industry managing these concerns — which could potentially slow the IoT adoption? What is it doing to combat the situation? Both Redpine Signals and Philips Healthcare are committed to staying ahead of the curve by integrating resources to ensure that their products work robustly and securely in different scenarios.

With a diverse set of products entering the IoT market, Redpine Signals is automating and optimizing its product quality assurance cycle to ensure that it effectively meets the quality standards of the products, Mattela said.

Raymond, who invests his time in the Wi-Fi Alliance, revealed that the industries, government bodies, alliances, and consortiums are working independently and together to create secure and robust solutions. “Everyone is trying to find a sweet spot for each of the wireless protocols and the right use case. Healthcare devices require a robust design to operate seamlessly no matter where the patient’s location.”

With today’s challenges, the architecture of an IoT device is even more complex. For example, a smart medical device may need to interface with Wi-Fi, *Bluetooth*®, ZigBee®, and Long-Term Evolution (LTE) before it can perform. Device hardware will have to deal with the added electromagnetic interference complexity while complying with strict medical regulations.

Ultimately, design and test engineers need to stretch their design skills to understand the device architecture and the applications it supports. Device hardware, wireless communication solutions, battery life, and security all require testing, separately and together, to ensure that they can withstand the rigors of the real world.

Progression Of IoT Test Solutions For The Future

IoT device manufacturers must ensure that their products operate per the required design and test parameters, especially in life-critical applications. They need to address the challenges of testing IoT devices and applications to deliver the best experience to their customers. In many cases, this experience needs to extend throughout the length of service of the specified IoT device. With the increasing complexity of IoT devices, device manufacturers and healthcare application designers are integrating maintenance and operational capability to enable monitoring and supportability. The monitoring occurs with the deployment of software-as-a-service applications.

As Raymond points out, “Security and product supportability is a driving factor pushing device manufacturers to implement the maintenance and operational capabilities into the device and applications. Support personnel must be able to monitor the device, receive important operational measurements, and discover a failure before it happens

Consequently, the IoT device manufacturer will generate additional revenue from selling the after-sales service to support and maintain the operation of the healthcare IoT devices and systems."

Will conventional test solutions be able to handle the test requirements of future healthcare solutions? According to Raymond, test equipment and software have to evolve with the industries. "The healthcare industry needs a collaborative partnership with test and measurement companies to build specific test systems within a given period — like a test solution-as-a-service."

This strategy could benefit the healthcare and test and measurement industries significantly. IoT device manufacturers would gain assurance that their test requirements are met, while the test and measurement industry would garner greater insight into market demands to enhance their offerings.

Conclusion

The future of connected healthcare depends on how the industry handles the complex build of today's health system. With more emphasis on delivering a high-quality customer care experience, organizations must integrate devices to create effective patient care and improve the overall quality of life for millions of patients. Device makers are under pressure to ensure that healthcare products are reliable and safe. Though there are still challenges to resolve, Keysight Technologies is ready to assist with a broad range of design, test and monitoring solutions for healthcare IoT.

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