WHITE PAPER

Security and Reliability of Mobile Healthcare Devices: Best Practices

The Medical Device Market — a Mobility Overview

The evolution of Wi-Fi has reduced the number of adverse events resulting from medication delivery and infusion therapy. There were several advances that converged at the same to enable the land rush of Wi-Fi. In 1999, the extended set of 802.11b functionality was approved, and a year later the Wi-Fi Alliance was born. 802.11b made wireless functionality comparable with wired Ethernet and the Wi-Fi Alliance ensured interoperability among vendors.

At approximately the same time, the Department of Veterans Affairs launched Bar Code Medication Administration (BCMA) application. This nurse-inspired application fostered the first use of wireless-enabled laptops and mobile computing in the healthcare market. The BCMA application was part of a broader push for patient safety that continues today. Five “rights” of medication administration also worked to reduce preventable medical errors by giving the right drug to the right patient, by the right delivery route, in the right dose, and at the right time.

KEYSIGHT TECHNOLOGIES

This requirement necessitated the evolution of the “smart infusion pump”. The smart infusion pump is a wireless networked device that can download drug libraries to the infusion pump and provide a continuous feedback loop to the clinician. In 2016, to reduce alarm fatigue, innovations that take advantage of mobile computing, e.g., hand-held devices to prioritize alarms became the norm. Applications such as BCMA, and the use of smart infusion pumps, are integral to reducing risk at the point of care. Ensuring that these applications work correctly is vital. This requires testing during product design. It also requires validating in complex healthcare mixed-use deployments to ensure the highest level of reliability, performance, and security.

There is a need to ensure that connected, life critical medical applications are reliable 24/7.

The Healthcare Wireless Ecosystem is Unlike any Other Vertical Market Today

Thousands of wireless clients, from real-time life critical (such as patient monitoring) to near real-time (infusion pumps) will need to meet strict security and use quality of service (QoS) standards to meet HIPAA and FDA market requirements. Add the smart phones and application-specific devices for handling alarm management that must work within the ecosystem of WLAN enabled network devices, and bullet-proof security is a must.

Understanding Technical Specifications

The wireless healthcare ecosystem is a complex market. While the Wi-Fi Alliance provides standards of interoperability, it is only the first step. Healthcare mobility requires a high degree of secure roaming, while ensuring a persistent connection to the enterprise. Published specifications of a manufacturer's WLAN adapter that indicate compliance to 802.11i and 80211e may exist. However, it may not document behind-the-curtains testing and compliance that validates the reliability of roaming algorithms to ensure a secure enterprise connection.

A convergence has happened today with multiple healthcare applications requiring the highest quality of mobile service experience.

Many healthcare institutions employ WPA 2 enterprise security, but differ in how they implement security methodologies, which can impact device and application performance.

Why Test Medical Devices During Design?

Engineering teams may choose to design a WLAN adapter by the published specifications and/or the Wi-Fi Alliance stamp of approval, or based on lowest cost. However, stress testing for performance of enterprise roaming, and the passing of required enterprise security requirements is highly recommended. This should be done prior to the design and build of the final product. The best way to accomplish this is to conduct proactive testing using an ecosystem-testing model that mirrors the healthcare enterprise.

Proactive testing makes good business sense. It is a small up-front expenditure that is a fraction of the overall product cost, based on potential non-approval by the FDA and/or non-performance of a product.

What does testing actually involve?

A comprehensive methodology for testing medical client devices includes controlled lab testing, as well as assessment of field performance that is validated and verified for a typical healthcare ecosystem. It also includes a mixed-use environment with data-, voice-, video- and WLAN-enabled medical devices.

In addition, include baseline network performance, using golden clients to obtain a best-case understanding, and assess real-world performance and security by simulating live network conditions. Generating high-traffic loads and interference allows realistic and thorough assessment of the resilience, co- existence and security capabilities of the devices. Such 360-degree testing includes medical device applications, coupled with traditional network traffic - data, voice and video. It is important to validate and verify reliability, speed and security of these devices and applications end-to-end. Testing needs to be at every level: the device's processor, its data connection, its application, and the network. End-to-end testing should span every element of the application's

delivery path – data center infrastructure to on-premises medical devices.

In Wi-Fi patient monitoring, you need to transmit vital signs and alarms with 100% reliability. It is also imperative to test the handoffs in roaming from access point to access point, while maintaining the enterprise security connection.

The changing technology requirements driven by IEEE, ongoing advancements in Wi-Fi technology, and updates to device software and applications, requires continuous testing. The continuous testing lifecycle commences during device or application development, and then continues through live deployment. A WLAN-enabled medical device has to initially obtain a FDA 510(k) approval. Changing firmware and software should not affect the performance, reliability or security of such devices. Continuous testing ensures that the WLAN medical device application will still meet approved intended use requirements. Manufacturers must validate and verify intended use, conducting a thorough hazards analysis before releasing new products, and maintain ongoing test processes and environments after a product launch.

Details of this testing should include network loading to ensure the WLAN- enabled medical device solution works reliably and securely in a shared 802.11 network architecture or environment. Conducting this type of testing in the presence of other devices that are typically found in hospitals (e.g., VoIP phones, wireless infusion pumps, wireless laptops and video) is essential to recreating realistic conditions to fully understand the impact on a given device or application behavior. The testing also ensures that multiple WLAN- enabled medical devices added to a shared 802.11 network environment do not degrade network performance.

Mixed-use traffic is typical of network traffic in hospitals today. It can include but is not limited to, wireless data (laptops on carts), voice over IP traffic, and other wireless-enabled medical devices that can be demonstrated at any level of bandwidth saturation. Testing demonstrates that the WLAN-enabled medical device solution will withstand increasing traffic load conditions to the point of network failure, which is difficult to do

Being proactive with device and enterprise testing can save a lot of headaches. This includes a reduction of risk for regulatory approval, faster time to market, and lower costs for deployment.

and rarely ever done in traditional on-site testing.

In summary, this gold standard testing includes:

- Medical device connectivity testing to evaluate the "networked medical device" performance at normal operational ranges from the nearest AP and in the presence of other network traffic such as Wi-Fi laptops, VoIP phones, scanners and other various interferences
- Medical device roaming testing to verify the roaming behavior of the device between two APs in the presence of other mobile devices
- Medical device hospital deployment testing to quantify the performance of the medical device application in a hospital environment and verify that the medical device application does not degrade the network's performance

Validation and verification testing is not static… But constant throughout the enterprise product lifecycle.

What are the potential consequences for "non-testing"?

A medical device manufacturer decided not to test…so what?

Many assume that having the Wi-Fi Alliance stamp of approval on the WLAN embedded adaptor is the "gold standard". Some vendors may have simply skipped the testing process, resulting in continually dropped network connections in the field. **If testing were done at the beginning of the design build, it would become apparent that the roaming algorithms inherent in the WLAN adapter simply were not enterprise grade. The company could have saved millions of dollars, a costly FDA recall, a total product re- design, and damaged market reputation.**

Security Validation and Testing — Why?

Breaches occur to networks and devices due to technology "gotchas", as well as human factor security practices. There is a definitive need to lock down any edge device that can serve as a portal to the network if it is breached by an outside-in cyber-attack. Mitigating this risk requires implementing protection as a "system of systems" through multiple layers of security.

Another key challenge to healthcare systems is the assurance of an end-to- end security strategy with enforced policies on a consistent basis. Security is a moving target that always needs to be updated. It is highly recommended that a healthcare enterprise test and validate those networked (wired and wireless) medical and non-medical devices before they access the network.

Guidance from the FDA on cybersecurity

Healthcare information security breaches cost the industry up to $6 billion annually. Average cost of a data breach for healthcare organizations is estimated to be more than $2.1 Million.

“Manufacturers should develop a set of cybersecurity controls to assure medical device cybersecurity and maintain medical device functionality and safety.

The FDA recognizes that medical device security is a shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices. Failure to maintain cybersecurity can result in compromised device functionality, loss of data (medical or personal) availability or integrity, or exposure of other connected devices or networks to security threats. This in turn may have the potential to result in patient illness, injury, or death.”

Cybersecurity design principles related to medical devices include:

- Medical devices typically have a long product design lifecycle of seven to ten years. They all use proprietary embedded operating systems. The system as a whole with firmware and software must meet FDA 510(k) regulatory approval before these devices can be sold in the commercial market.
- Product designs that do not utilize any SNMP agents that are typically found in enterprise network management.

Meeting WLAN-enabled medical device application latency requirements starts with the right device design. All current enterprise security schemas need to be tested - from the lowest level to the highest. This testing is important to any type of regulatory submittal. It demonstrates that the manufacturer has validated and verified that the application meets the intended use.

The intended use in this case is the healthcare enterprise and ecosystem of application-generated traffic. The following are the advised security schemas to test while traffic generation occurs.

WEP with 64 bit and 128 bit keys

IEEE802.1x with EAP-TLS and WEP encryption

IEEE802.1x with EAP-TTLS and WEP encryption

IEEE802.1x with EAP-PEAPv0/MSCHAPv2 and WEP Encryption

IEEE802.1x with EAP-PEAPv1/EAP-GTC and WEP Encryption

IEEE802.1x with EAP-LEAP and WEP Encryption

WPA-Personal with TKIP Encryption

WPA-Enterprise with EAP-TLS and TKIP Encryption

WPA-Enterprise with EAP-TTLS and TKIP Encryption

WPA-Enterprise with EAP-PEAPv0/MSCHAPv2 and TKIP

WPA-Enterprise with EAP-PEAPv1/EAP-GTC and TKIP Encryption

WPA-Enterprise with EAP-LEAP and TKIP Encryption

WPA2-Enterprise with EAP-TLS and CCMP Encryption

WPA2-Enterprise with EAP-TTLS and CCMP Encryption

WPA2-Enterprise with EAP-PEAPv0/MSCHAPv2 and CCMP Encryption

WPA2-Enterprise with EAP-PEAPv1/EAP-GTC and CCMP Encryption

WPA2-Enterprise with EAP-LEAP and CCMP Encryption

Some of the Requirements for Regulatory Approval

The following document citation issued by U.S. FDA is provided for reference purposes, and the recommendations are considered non-binding. The documents address best practices associated with QoS of medical devices for device manufacturers and healthcare administrators.

U.S. Department of Health and Human Services Food and Drug Administration

Center for Devices and Radiological Health Office of Science and Engineering Laboratories Center for Biologics Evaluation and Research.

Radio Frequency Wireless Technology in Medical Devices - Guidance for Industry and Food and Drug Administration Staff

The above-referenced document was issues on August 13, 2013.

Reduction of Risk and Cost – Impacting the Total Cost of Ownership

- Recent research from The Ponemon Institute shows that early discovery of issues provides massive savings. They found that bugs found in development are over 90 times cheaper to fix than when found in production. Creating updates for live services without affecting customer experience is far costlier than making changes prior to release. The ROI of this testing is significant. Cost avoidance includes finding a bug at development is $80, at build $240, at QA/Test, $960 but escalates at production to $7,600
- Reducing the risk to manufacturing, regulatory approval, and enterprise deployments impacts design-build budgets, as well as marketing product launch costs
- Not validating the appropriate WLAN-embedded adapter early in the design cycle potentially costs millions of dollars in re-design and/or a regulatory recall
- Ensuring the highest degree of security protects the device and network from any potential issues from cybersecurity threats. Using consistent methodologies for testing for a FDA 510(k) approval will ensure a quick and reliable approval process
- Creating an ecosystem-testing environment validates and verifies the correct enterprise WLAN and network design, while creating the best deployment plan. From the start of the selection of the WLAN adapter, through regulatory testing, and then to final development, WLAN ecosystem testing is not a “nice to have” but a “must have”

What are Testing Best Practices?

- Testing should occur at the earliest decision point of design to validate and verify that the WLAN or network technology chosen works as advertised
- Up-front testing will serve as the foundation for any regulatory submittal required. All medical device companies going forward will need to submit detailed testing for secure networked medical device connectivity, as well as wireless co-existence testing
- Up-front testing will also develop the correct deployment guidelines and need requirement support in the field
- Continuous testing must be part of the internal regulatory process

The enterprise WLAN marketplace is not static. As changes in software and firmware occur in the WLAN, manufactures must validate and verity that the application still performs according to the intended use. This is not only needed to ensure continued regulatory compliance, but best ISO standards.

Conclusion

For the Medical Device Manufacturer:

The requirement for a 360-degree test is needed for today's WLAN-enabled medical device space, and should include:

- End-to-end testing for each element to quickly find issues before they impact the bottom line.
- Validation and verification of design elements to avoid an entire product re-design.
- Applications, networks and devices to prove performance, security, and reliability.
- Continuous, multi-stage testing for updates before they affect your reputation.
- Continuous validation throughout the product lifecycle to meet security and quality of service requirements.

For the Enterprise:

WLAN deployment for healthcare should include a site assessment to measure the performance of multiple client devices and quantify the end-user experience in real-world network environments, including:

- measuring the wireless experience from the user or client perspective
- creating a live network ecosystem to assess how devices and applications perform and co-exist in real world environments
- modeling “what if” scenarios as new users, devices, applications, and technologies are added to the network over time

References

“Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices” (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm) and “Guidance to Industry: Cybersecurity for Networked Medical Devices

Containing Off-the-Shelf (OTS) Software” (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm).

http://www.ixiacom.com/wi-fi-test

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

KEYSIGHT TECHNOLOGIES

This information is subject to change without notice. © Keysight Technologies, 2016 - 2020, Published in USA, May 27, 2020, 3120-1080.EN