Are Mobile Medical Devices "Hospital Grade"?

WHITE PAPER

MEETING THE CHALLENGE OF TODAY'S HEALTHCARE WLANS

By David Hoglund, Founder and President, www.integrasystems.org

For more than a decade, the proliferation of Wi-Fi-enabled medical devices has been fast and furious. Rampant growth has been fueled by:

- The rise of "smart" infusion pumps
- Ubiquitous mobile access to electronic medical records (EMR)
- Cost-savings realized using standards-based networks (versus proprietary)

Not only are mobile devices growing in both number and complexity, use models within healthcare facilities are also rapidly evolving. Once used mainly for low-priority data, Wi-Fi now carries vital real-time voice, video, and medical applications requiring "hospital grade" connectivity, security, and mobility.

WI-FI NOW CARRIES VITAL REAL-TIME VOICE, VIDEO, AND MEDICAL APPLICATIONS REQUIRING "HOSPITAL GRADE" CONNECTIVITY, SECURITY, AND MOBILITY.

ixia
A Keysight Business

915-6112-01-7061 Rev A

For makers of medical devices and healthcare facility IT teams, the new use model places rollout schedules, profitability models, and brand reputation at unprecedented risk:

- If WLAN-enabled medical devices don't perform in a reliable and safe manner, manufacturers may need to delay the delivery of new products or even perform a total redesign;
- Going back to the drawing board can also mean re-submitting products for FDA 510K certification;
- If life-critical alarms and alerts do not occur in a timely fashion after deployment, adverse events may go unnoticed, potentially leading to serious liability or regulatory recalls;
- Last but not least, healthcare workers and facilities may lose confidence in the equipment or the manufacturer's brand.

Each of these scenarios can prove extremely costly and open the door for renewed competition. To avoid extreme consequences such as these, device manufacturers and healthcare IT teams need a means of ensuring quality and staying ahead of the technology curve in both the healthcare and wireless LAN (WLAN) industries. On their own and working together, they must minimize risk around the point of care while meeting changing regulatory mandates and dealing with different levels and stages of meaningful use.

FOR MORE THAN A DECADE, THE PROLIFERATION OF WI-FI-ENABLED MEDICAL DEVICES HAS BEEN FAST AND FURIOUS

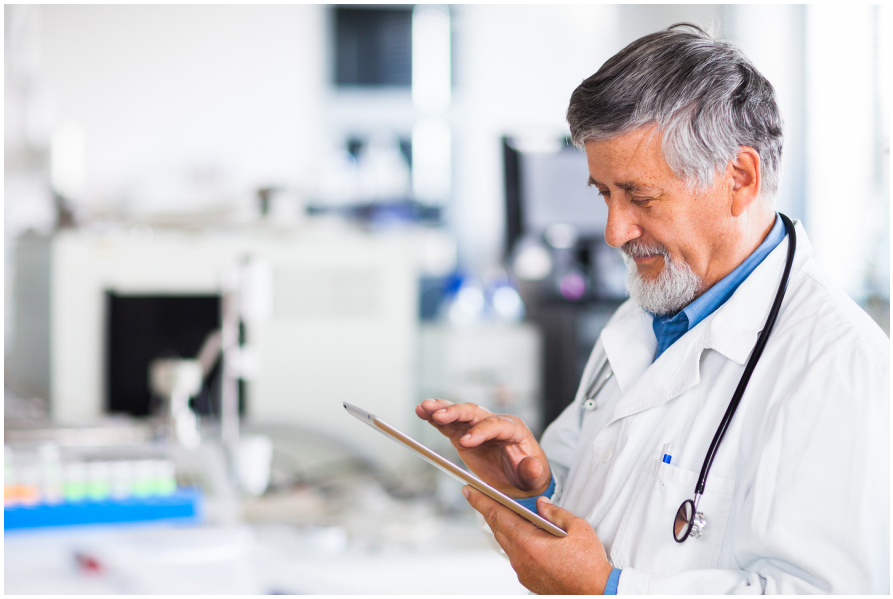
The challenge is: countless variables impact performance. Everything from inferior embedded radio strategies to lead-lined walls to not understanding requirements for consistent roaming can impact performance. To date, there's been no consistent, cost-efficient way to validate and verify quality and reliability.

Wi-Fi Alliance certification testing, as we'll see, is a good start, but it's far from enough. Leading manufacturers must now employ Wi-Fi-centric testing as a necessary and cost-effective strategy for ensuring performance, reputation, and profitability.

Fortunately, test procedures are evolving, enabling manufacturers to effectively "bring the hospital into the lab." By recreating and subjecting new device designs to realistic deployment conditions, manufacturers and IT professionals with varying levels of Wi-Fi expertise can uncover and address issues throughout design, development, and ultimately deployment in healthcare environments.

This paper will take a quick look at two real-world examples of product releases gone wrong and overview the risks & challenges

inherent in optimizing performance of mobile medical devices. We'll then outline best practices for cost-effectively mitigating risk and euring quality in life-critical deployment scenarios.



CHAPTER 1: GOING MOBILE: THE CHALLENGE

It was not until the extended version of 802.11, 802.11b, was approved in 1999 that medical device manufacturers began expanding into the realm of wireless networking. Until then, infusion pumps had been standalone, non-intelligent devices with no need to connect to wired or wireless networks. Similarly, mobile patient monitoring was primarily limited to proprietary WMTS (Wireless Medical Telemetry Service) transmitters, receivers, and antenna systems.

Today, the majority if not all leading infusion pump companies are deploying wireless-enabled "smart pumps," and many patient monitoring companies are equipping portable monitors and telemetry solutions worn by patients for wireless. Though some still cling to the notion of WMTS as the wireless platform of choice, visionary companies recognized that 802.11a/b/g was a viable alternative more than a decade ago.

Though rising rapidly in number, mobile healthcare applications and devices are still relatively new and rife with challenges. Medical device manufacturers are device manufacturers first and foremost; rarely is wireless a core competency. Those grappling

IT WAS NOT UNTIL THE EXTENDED VERSION OF 802.11, 802.11B, WAS APPROVED IN 1999 THAT MEDICAL DEVICE MANUFACTURERS BEGAN EXPANDING INTO THE REALM OF WIRELESS NETWORKING.

with Wi-Fi for the first time "don't know what they don't know," both from an internal design and a deployment perspective.

Nor is Wi-Fi just another network interface. Along with an overall lack of veteran expertise, a host of challenges exist in ensuring and optimizing device performance including:

The Evolution of Healthcare WLAN Deployments

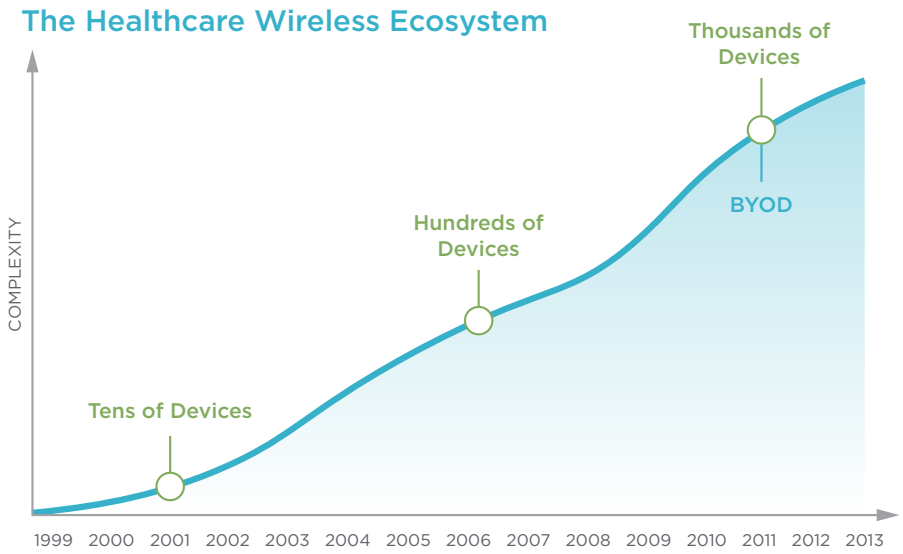
Early on, healthcare institutions tended to build out their WLANs in a limited fashion, in limited areas, with no strategic process in place. Deployments chiefly consisted of laptops on carts deployed outside patient rooms for charting or BCMA applications, and site design was less critical.

EARLY ON, HEALTHCARE INSTITUTIONS TENDED TO BUILD OUT THEIR WLANS IN A LIMITED FASHION, IN LIMITED AREAS, WITH NO STRATEGIC PROCESS IN PLACE.

Most medical device manufacturers created design and deployment architectures based on a VLAN and 802.11q trunking with a common ESSID for the specific service model. For example, there might be a specific VLAN and ESSID for all infusion devices as well as separate VLAN and ESSID for patient monitoring.

Since the manufacturer may not have been able to truly assess actual service requirements or characterize the performance of the WLAN ecosystem as a whole, the "ad hoc" approach to deployment added a level of risk in terms of device and application performance. For example, what if a critical patient care alarm, alert, and/or recording does not get documented correctly?

The next phase of evolution was marked by the introduction of wireless voice over IP, which added complexity and required a somewhat stronger signal strength (-65 dBm vs -85 dBm). But it was not until recent years that wireless LANs in healthcare environments evolved drastically in scale and complexity, basically introducing a whole new wireless business model.



The hospital of today must deliver ubiquitous WLAN coverage in order to meet mobility requirements. Modern WLANs must in turn be designed to support the data requirements of 802.11n clients, voice, video, and hundreds if not thousands of WLAN-enabled medical devices.

What is the new use model for wireless-enabled medical devices?

WLAN-enabled medical devices now often encompass not one or ten but hundreds of "highly mobile" devices on an enterprise network. Healthcare facility WLANs still support stationary laptops outside patient rooms, but the new generation of wireless medical equipment tends to be truly mobile: devices "move with the patient" for hours or even days to the ER, radiology, the intensive care unit, etc.

Interoperability and coexistence have increased in importance as the typical WLAN ecosystem grew to include:

- Hundreds of infusion pumps trying to download drug libraries at the same time
- WLAN-based telemetry transmitters sending alarms and waveform data to a central station
- Caregivers placing wireless voice over IP calls

- Nurse call systems being alerted
- PACS images being sent to laptops
- Guest access by patients
- The emerging BYOD (bring your own device) trend

And unlike wide open warehouse environments and manufacturing facilities, hospitals rank among the most challenging RF environments. Signals from WLAN-enabled infusion pumps, telemetry, and patient monitors may need to penetrate tile-lined bathrooms as well as several RF-reflective obstacles to reach an access point fifty feet down the hall. Lead-lined walls in Radiology rooms, varying stages of construction, fluids, reflective metal surfaces and other environmental factors can also impede wireless signals.

Nor can device manufacturers trust that network design and configuration will automatically be optimal for their products' performance. Traditional wireless "site surveys" conducted by integrators typically reflect the model of laptops stationed outside patient rooms. More often than not, they fail to consider the unique design and application requirements of a particular facility.

And once again, highly sensitive real-time traffic from WLAN-enabled medical devices must now share the same enterprise network with real-time multimedia applications. To ensure the absolute fidelity of patient data, alarms, events, and recordings, providers must be able to absolutely guarantee real-time medical transactions will be passed through the network in a reliable fashion.

The upshot: The use model for mobile medical devices has changed. Manufacturers need to be able to recreate user environments in the lab to assess and optimize device performance in live networks. Those considering embedding 802.11a/b/g/n client radios into their devices need to test and validate performance in various RF environments, under varying traffic loads, and for specific application environments. Emerging Wi-Fi test solutions let manufacturers "bring the hospital to the lab" and generate realistic traffic to perform comprehensive load testing and simulate high-stress conditions. Conducting this type of assessment prior to deployment is proving to be essential in guaranteeing timely, successful product launches.

WLAN-ENABLED MEDICAL DEVICES NOW OFTEN ENCOMPASS NOT ONE OR TEN BUT HUNDREDS OF "HIGHLY MOBILE" DEVICES ON AN ENTERPRISE NETWORK.

Radio Strategy Misconceptions

One popular misconception that frequently compromises performance is that "all 802.11a/b/g radios are created equal." Selecting a sub-par, low-cost radio can undermine the performance of a life-critical medical device that costs thousands of dollars, thus exposing the manufacturer to catastrophic consequences.

Another costly misconception is that a radio obtaining a stamp of approval from the Wi-Fi Alliance means everything will work fine. Nothing could be further from the truth.

The Wi-Fi Alliance was founded in 1999, the same year that the IEEE approved the extended version of 802.11, 802.11b, for the specific purpose of ensuring interoperability between client radios and wireless access points. The interoperability testing conducted does not include modeling the specific characteristics of a data, voice, video, or medical device client or the simulation of different mixed client traffic load environments. Nor does it measure application performance.

Obtaining the Wi-Fi Alliance's stamp of approval is a great start, but it's far from the end. The fact that a radio is Wi-Fi approved, or subscribes to 802.11i and 802.11e, does not demonstrate how well the roaming algorithms will work, or assess the passing of security supplicants. Many healthcare institutions employ WPA2 enterprise but differ in how they implement security methodologies, which in turn impacts device and application performance.

The upshot: In selecting the optimal WLAN-embedded radio, device manufacturers must assess components' ultimate ability to meet intended use for quality of service, roaming, and varying security implementations. As the mobile healthcare ecosystem grows ever more complex, embedded radio strategies must be able to accommodate all enterprise-grade security strategies and effectively roam amidst a myriad of traffic types throughout highly mobile environment.

ONE POPULAR MISCONCEPTION THAT FREQUENTLY COMPROMISES PERFORMANCE IS THAT "ALL 802.11A/B/G RADIOS ARE CREATED EQUAL."

The FDA 510k Regulatory Approval Process

The FDA has promulgated draft standards for the wireless-enabled medical device. Manufacturers need a reliable means of validating and verifying the critical functionality of an application

outside of the traditional closed loop patient data, physiological waveforms, and alarms/alerts.

In the past, “closed loop” defined the traditional patient monitoring network in which the bedside monitor was connected to the central station via a proprietary network, and not part of the wired or wireless enterprise network. Infusion pumps and other medical equipment often operated as standalone devices.

In today’s highly networked environments, manufacturers must be able to demonstrate, validate, and verify that WLAN-enabled medical device applications work as intended with demonstrated risk avoidance. To meet and maintain regulatory approval, networked applications and devices—whether one or several hundred—must be shown to work as intended in the wireless RF environment in the presence of other application traffic.

Nor is that enough. Medical equipment manufacturers must also keep up with change as WLAN infrastructures evolve. Access point and controller manufacturers generally roll out new firmware and software much more often than medical devices are updated. These upgrades and modifications can alter the way applications work compared with how they performed when originally tested and validated for FDA 510k submittal.

The WLAN medical device manufacturer is obligated to continue to validate and verify that the application works “as intended” as the enterprise network infrastructure evolves. If they choose to partner with a new player that has not yet been tested, the are further obligated to validate and verify that the application works as intended per the original FDA 510k submittal.

The upshot: Manufacturers must validate and verify intended use, conducting a thorough hazards analysis before releasing new products and maintaining ongoing test processes and environments after a launch. Testing should include network “load testing” and security testing to demonstrate that devices will work in a reliable and secure fashion in a shared 802.11 network architecture or environment. Ideally, the test environment for medical client devices should include WLAN APs and controllers from multiple manufacturers and successive iterations of software and firmware.

Meeting the ANSI/AAMI/IEC 80001-1:2010 Standard

As medical devices and information management systems converge, the IEC 80001 standard prescribes risk management in IT networks incorporating medical devices, addressing diverse risks related to patients, operators, and third parties. Part 1 overviews roles, responsibilities, and activities, aiming to ensure the delivery of safe, high-quality healthcare, as well as the security and privacy of patient data.

80001-1 specifies general requirements for achieving essential properties such as safety, effectiveness, data & system security, and interoperability. The section also defines responsibilities for parties such as medical device manufacturers, non-medical device manufacturers, the responsible organization, network integrators, and others engaged in installing, reconfiguring, maintaining, decommissioning IT networks that incorporate medical devices.

Implementing IEC 80001-1 aids in the successful deployment and management of networked medical technology to truly realize the anticipated clinical and organizational benefits. It also helps in understanding and addressing the requirements of the FDA's MDDS regulation, and is integral to successfully deploying technology in support of the Office of the National Coordinator for Health Information Technology's meaningful use requirements.

AS MEDICAL DEVICES AND INFORMATION MANAGEMENT SYSTEMS CONVERGE, THE IEC 80001 STANDARD PRESCRIBES RISK MANAGEMENT IN IT NETWORKS INCORPORATING MEDICAL DEVICES, ADDRESSING DIVERSE RISKS RELATED TO PATIENTS, OPERATORS, AND THIRD PARTIES.

"BYOD"

The "bring your own device" or BYOD trend continues to escalate with medical staff, patients, and visitors bringing more and more personal smartphones, tablets, and laptops with them everywhere they go. Flooded with additional devices, Wi-Fi bandwidth usage in corporate and healthcare environments becomes much harder to control and predict.

Modern mixes of devices may entail various forms of hardware and software that may be beyond the original design of the system; for example, legacy 802.11b-compliant devices may not operate optimally due to complicated OS and application requirements. Such devices may malfunction, bring excessive load to the network, or even increase vulnerability to attack, and need to be isolated out for not performing correctly.

The majority of BYOD consumer devices now incorporate embedded 802.11a/g/n radios and are designed with a focus on

the user interface and experience. It is important to understand how these devices will impact the functionality of the network as a whole.

The author remembers as an example in which the introduction of an iPhone and unique software code requiring the DHCP request brought an entire university healthcare system's wireless LAN network to its knees. This would hardly be acceptable today! Before delivering new devices for use in healthcare environments, manufacturers must proactively anticipate ever-more-complex mixes of clients and time-sensitive applications that will coexist and contend for available network resources.

Going Forward: "Lifecycle Testing" Essential

Wi-Fi deployments are not going to get easier anytime soon. The author considers the current environment the "wild, wild west of wireless": a combination of wireless-enabled data devices, laptops, the BYOD era, voice over IP, WLAN-enabled RTLS, wireless infusion devices, WLAN-enabled patient monitoring, pulse oximetry, etc.

Already, hospital WLANs are far from static yet there are no published standards for deployment or what the multi-faceted application healthcare environment should look like. A definitive need exists for strategic validation and verification strategies and "Best Practices" that begin early on in designing new devices and continue beyond product launch and deployment.

As we have just seen, these strategies should deliver:

- Proof that WLAN-enabled medical devices will operate safely, effectively, and as intended, with the ability to adapt to changes in infrastructure and technology;
- Assurance throughout the FDA 510k process that applications will operate as intended to the right design models;
- A means of demonstrating devices' ability to meet network load and environmental requirements;
- Confirmation that adding a new medical device to the shared wired or wireless 802.11 environment will not degrade the network performance of other life-critical applications on the shared enterprise network;

WI-FI DEPLOYMENTS ARE NOT GOING TO GET EASIER ANYTIME SOON.

- Ongoing verification of real-world performance as network infrastructures and environments change.

So let's see what this testing looks like . . .

CHAPTER 2: PRODUCT RELEASES GONE WRONG

Case Study 1: The High Cost of Inexpensive Radios

Upon deployment in hospitals, wireless connections dropped and the clinical application failed to perform correctly as devices became highly mobile. The failure of the solution to perform as expected ultimately resulted in the FDA requiring a recall of the deployed units from the field which was followed by a more thorough evaluation of the hardware platform.

During follow-up testing after the recall it was discovered that the roaming algorithms were not robust enough to withstand the rigors of a hospital environment. While in initial design, the hardware platform may have connected to the network in an "isolated" laboratory environment, but it may not may have been tested in a highly mobile enterprise environment where roaming occurs and continued authentication is required.

In addition, there was probably no way to demonstrate that 1-x1,000s of these devices could pass data in a converged (data, voice, video) real-life healthcare environment. Since the embedded radio was part of the integrated hardware platform, the product needed to be completely redesigned. Had the manufacturer tested the embedded WLAN radio before making its selection, they would likely have specified a different component and avoided the costly remediation effort that followed.

Case Study 2: Proactive Testing Prevents Poor Performance

In a similar instance, another device manufacturer selected a WLAN module and also planned to go into production without testing of the module. This time the company was advised to at least test roaming performance as well as the module's ability to meet the security requirements of modern day enterprise WLANs.

Testing revealed that the WLAN module had difficulty passing the correct security supplicants. While it was demonstrated by the manufacturer that a secure connection could be established, the issue showed up when the network was stressed by adding load and capacity and introducing significant roaming scenarios. During testing that included replicating a real-world situation, the supplicant could not be passed and the network connection dropped. Here, the manufacturer decided not to move forward with the selection of the original WLAN module and avoided the lost time, embarrassing field issues, and steep costs associated with remediating issues upon deployment.

CHAPTER 3: MITIGATING RISK: BRINGING THE HOSPITAL TO THE LAB

A higher caliber of testing is needed to assure the reliable performance and scalability of modern mobile healthcare applications. A proven methodology and several core capabilities can be deemed essential.

Proven Methodology

A comprehensive methodology for testing medical client devices proceeds from highly controlled lab testing to assessing performance in the field via open air. Testing should include validating components such as radios, chipsets, and driver firmware and, once that's done, progress to assessing the real-world performance of the medical device itself.

The proven methodologies developed by Wi-Fi test experts at Ixia include:

1. Baselining network performance using "golden" clients to obtain a "best-case" picture;
2. Baselining device performance under ideal network conditions where it's the only client communicating with APs under optimal conditions;
3. Assessing range and roaming capabilities by varying RF signal attenuation to prompt devices under test (DUTs) to move away from and between specific APs. This includes:
   - Determining device association to the WLAN at various ranges

A HIGHER CALIBER OF TESTING IS NEEDED TO ASSURE THE RELIABLE PERFORMANCE AND SCALABILITY OF MODERN MOBILE HEALTHCARE APPLICATIONS.

- Measuring the accuracy of device throughput, latency, and packet loss characteristics
- Assessing performance as devices travel across multiple APs to emulate patient mobility

Testing should progress from simple setups using only two APs at a time to complex scenarios where the device sees multiple available access points broadcasting at different signal strengths.

4. Assessing real-world performance and security by simulating live network conditions. Generating high traffic loads and interference allows the resilience, coexistence, and security capabilities of devices to be realistically and thoroughly assessed. User-configured clients should be generated to populate a realistic network ecosystem containing device traffic typically found in healthcare environments—voice over IP, data from wireless infusion pumps, wireless laptop transactions, video, etc.—all generating simultaneous network traffic;
5. Measuring interoperability with multiple APs and mobile clients and major customers' preferred WLAN equipment vendors;
6. Quantifying application performance and quality of experience (QoE) from the user perspective;
7. Reproducing field conditions and modeling "what if" scenarios in the lab to simulate individual customer environments
8. Onsite assessment to ensure successful customer deployments out of the gate
9. Ongoing lab and site testing of network firmware changes & devices software upgrades

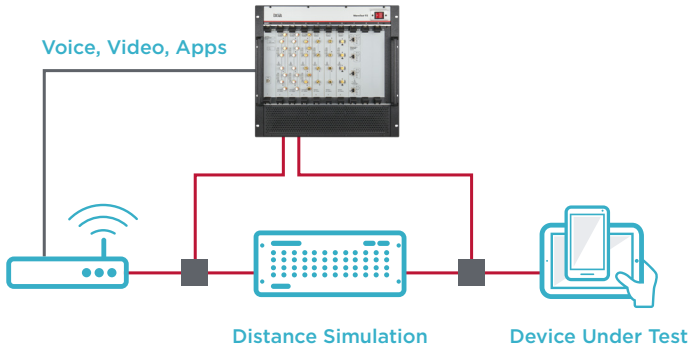
Essential Test Capabilities

Several critical capabilities are required to conduct basic performance testing of networks, devices, and applications, as well as specialized testing of roaming, interoperability, and other key aspects of performance.

Effective wireless client testing consists of four critical components:

- **Traffic generation** enabling realistic network and environmental conditions to be simulated and variables such as increasing distance, roaming, and interference to be systematically introduced;
- **Test automation** allowing hundreds of tests to be run and repeated quickly, unattended. Data plane (throughput/file transfer times), control plane (roaming/range), and pass/fail "user experience" tests should all be automated. Lab automation also promotes fast testing of new OS, driver & code revisions;
- **Performance analysis** that rapidly pinpoints potential problem areas. Users should be able to measure the performance of the DUT using all industry-standard authentication/encryption mechanisms including WEP, WPA-PSK, WPA2-PSK, WPA-EAP-TLS etc.;
- **Wi-Fi expertise:** Wi-Fi isn't just another network interface, and knowing what to look for, and what do to about it produces dramatic cost- and time-savings.

[See Appendix for guidelines and procedures for testing specific capabilities.]



Typical Client Test Setup

Taken in total, validation and verification should address two critical, complementary aspects of performance:

- **Impact of device on the network:** Demonstrate that the intended wireless-enabled medical device will not cause the degradation of application performance, waveform display, alarms, or the recording capabilities of other wireless medical devices within multiple proximity ranges

SEVERAL CRITICAL CAPABILITIES ARE REQUIRED TO CONDUCT BASIC PERFORMANCE TESTING OF NETWORKS, DEVICES, AND APPLICATIONS, AS WELL AS SPECIALIZED TESTING OF ROAMING, INTEROPERABILITY, AND OTHER KEY ASPECTS OF PERFORMANCE

- **Impact of the network environment on devices:** Validate that the Wi-Fi-enabled device or application itself will not be compromised in terms of performance, waveform display, application operation, alarm annunciation, and/or recording capabilities

Once the device manufacturer feels confident on both counts, system integrators, service providers, and healthcare facility IT departments must do their part in ensuring the overall network environment functions optimally. The ideal way to achieve this is by extending the same test systems and best practices to the field and working together to identify and remedy unexpected surprises.

The test solution already mentioned, IxVeriWave from Ixia, delivers a "lab to field" solution with test systems, suites, and methodologies optimized for the challenges of today's high-pressure healthcare environments. The next chapter contains a brief introduction.

CHAPTER 4: IXIA WI-FI CLIENT AND SITE ASSESSMENTS: TESTING FOR THE MEDICAL DEVICE LIFECYCLE

Ixia equips the world's leading manufacturers, service providers, system integrators, and enterprises to test, assess, and optimize the design and deployment of new technology. The industry's premier lab-to-field solution for Wi-Fi network and device testing, Ixia's IxVeriWave is preferred by prominent manufacturers of WLAN infrastructure equipment and mobile devices, as well as service providers and end-users worldwide.

IxVeriWave represents the industry gold standard in testing WLAN performance and site readiness throughout design, development, and deployment. Employing a client-centric or user-focused model, Ixia's mobile client testing addresses the entire product lifecycle delivering:

- Traffic generation
- Signal attenuation
- Performance measurement
- Automation
- Site assessment
- Industry-specific test suites

TAKEN IN TOTAL, VALIDATION AND VERIFICATION SHOULD ADDRESS TWO CRITICAL, COMPLEMENTARY ASPECTS OF PERFORMANCE

IxVeriWave delivers the powerful analytics needed to harden and optimize new product designs, reduce cost, and speed identification of potential problems early on in the development and QA cycles. The actionable insight delivered by Ixia systems and "Testing as a Service" (TaaS) solutions helps speed time-to-market and mitigate risk while securing the delivery of high-performing devices, applications, networks, and services.

Going forward, Ixia leads the industry in innovating 802.11n and 802.11ac test solutions helping to bring next-generation Wi-Fi network capacities to fruition. Ixia's client test methodology represents a compelling industry "standard" medical device manufacturers and the healthcare industry can use to fully leverage Wi-Fi's increasing capacity and performance capabilities, now and into the future.

GOING FORWARD, IXIA LEADS THE INDUSTRY IN INNOVATING 802.11N AND 802.11AC TEST SOLUTIONS HELPING TO BRING NEXT-GENERATION WI-FI NETWORK CAPACITIES TO FRUITION

CONCLUSION

Innovations in mobility will continue to revolutionize healthcare—if the risks associated with poor performance can effectively be mitigated. With the challenge growing harder, and users more demanding, medical device manufacturers and healthcare facilities can no longer afford to leave anything to chance.

Fortunately, test infrastructures and best practices are keeping pace, helping to ensure performance and mitigate risk from the lab to the field. Testing not only plays a critical role in optimizing design and configuration, it helps in demonstrating compelling competitive advantages during product launches and in sales and marketing campaigns. Perhaps most important, repeat testing helps instill confidence in healthcare workers who are too pressed for time to bother with mobile devices that don't perform as promised out of the box.

INNOVATIONS IN MOBILITY WILL CONTINUE TO REVOLUTIONIZE HEALTHCARE—IF THE RISKS ASSOCIATED WITH POOR PERFORMANCE CAN EFFECTIVELY BE MITIGATED.

The costs of assessing new products prior to deployment pales in comparison to that of not testing. No longer optional, or even "precautionary," benchmarking new wireless designs is essential to safeguarding the wellbeing of patients, healthcare workers and facilities, and manufacturers themselves, today and into the future.

Conducting the testing now warranted by mobile medical devices is everyone's job, and to everyone's benefit. But it must begin with those creating the devices upon which success—and ultimately lives—will rely.

APPENDIX

Association Testing

Test association of WLAN-enabled medical device clients against specific access point types controlled by the various controllers. B-only mode, B/G mode, A-only mode, A/B/G-hybrid mode. Define matrix of pass, fail, or pass with limitations.

Association Load Testing

Determine the approximate limits of the number of WLAN-enabled medical device clients that can be associated to a single access point. Define matrix of pass, fail, or pass with limitations.

Authentication Testing

Test various authentication methods of WLAN-enabled medical device client through different manufacturers of enterprise wireless LAN controllers. Define matrix of pass, fail, or not supported.

Roam Testing

Verify and validate how the WLAN-enabled medical device client will roam from AP to AP.

Determine approximate signal strength at which WLAN-enabled medical device client attempts to roam.

Determine if roam time is within acceptable limits.

Traffic Load Testing

Determine the approximate limits of the capabilities of the WLAN-enabled medical device client when placed into a scenario of high AP traffic load in b/g, a, and n modes. Traffic scenario options include: high pps with low bandwidth utilization, low pps with high bandwidth utilization, high pps with high bandwidth utilization. Define the matrix of pass, fail, or pass with limitations.

Stability Testing

Operate the WLAN-enabled medical device clients for periods of not less than 3 days/72 hours in a high-load scenario on each AP/controller type and verify/confirm normal and expected operation. Define matrix of pass, fail, or pass with limitations. *

WLAN-enabled Network Behavior

Determine the threshold that will crash the WLAN-enabled medical device client when flooding it with traffic (UniCast, MultiCast, etc.)

Test with 802.1x configured on a switch while using a wired connection with the WLAN-enabled medical device client

About the Author

An internationally recognized consultant, writer, speaker, and professional blogger, David Hoglund is the Founder and Principal of Integra Systems, a provider of strategic assessments and planning services for major wireless and mobility initiatives. A renowned Subject Matter Expert (SME) in wireless and medical connectivity, David is a veteran advisor to medical device manufacturers, venture funded companies, integrators, architectural firms, and Fortune 50 companies on a global basis. Well known in the healthcare industry for his extensive knowledge of wireless technology and ecosystems, he has created test plans, implemented product testing, led FDA 510K process approval projects, and designed new product solutions.

IXIA WORLDWIDE

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(Fax) 1.818.871.1805

www.ixiacom.com

IXIA EUROPE

Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

IXIA ASIA PACIFIC

101 Thomson Road,
#29-04/05 United Square
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127