RESEARCH

Management and Risk Assessment of Wireless Medical Devices in the Hospital

Allie Paquette, Frank Painter, Jennifer Leigh Jackson

In today’s healthcare environment, wireless coexistence of medical devices is becoming more and more prevalent. Healthcare is among the most mobile work environments where clinicians need timely access to data in order to deliver efficient and effective care. Optimizing patient flow requires just-in-time delivery of medical devices at the point of care with seamless connectivity to both electronic medical records (EMR) and data connectivity to clinical decision makers. These factors are driving an increasing demand for mobile, wireless medical device technology. Reliable and always available wireless communication is the key component to allow medical devices to be able to move with the patient, while continuing to record and communicate patient data.

Mobile wireless connectivity requirements differ depending on the intended use. Each application has demands on the connectivity infrastructure such as availability, reliability, and data payload capability. For example, an electrocardiogram (ECG) telemetry system requires real time streaming of data and alarms from the patient to remote viewing stations. While the streaming component of the ECG waveform has a relative tolerance for lost data packets, the alarms associated with ECG monitoring are of a much more critical nature; the loss of a patient alarm could result in patient injury.

Alternatively, smart infusion pumps that use the wireless network only to update drug libraries are occasional and opportunistic connectors. Therefore continuous streaming data, highly reliable network availability, and low latency are requirements for life critical applications like alarms, yet not as critical for applications such as infusion pumps not sending alarms. Furthermore, these wireless medical device applications may share radio frequency (RF) spectrum resources with a host of other nonmedical device applications, such as wireless phones, barcode scanners, Bluetooth headsets, laptop computers, and remote control units. Additional traffic in the RF spectrum can affect reliable data transfer if these demands are not recognized and managed appropriately.

In the face of high investment of network infrastructure and related security and performance management, it is imperative that healthcare administrators understand the costs, benefits, and risks of incorporating medical devices on the hospital’s wireless enterprise network.¹

In order to assess the risks of incorporating wireless medical devices onto a hospital’s wireless network, thorough evaluation and testing of these devices is an essential component of the implementation process for which clinical engineers are uniquely qualified. The

About the Authors

Allie Paquette is an MS candidate at the University of Connecticut and an ACCE Scholar. E-mail: alliepaq@gmail.com

Jennifer Jackson, MBA, CCE, is a project clinical engineer at the Biomedical Engineering Department with Brigham & Women’s Hospital in Boston. E-mail: jenniferleighjackson@gmail.com

Frank Painter is the clinical engineering internship program director and adjunct professor at the University of Connecticut. E-mail: frpainter@earthlink.net
process should include four major steps:
1. Characterization of RF spectrum usage in the hospital environment
2. Identification, classification and mitigation of risks using a tool based on the recently ratified ANSI/AAMI/IEC 80001-1 standard
3. Development of a test environment within the hospital
4. Validation of the device performance in the test environment

Wireless Technology

Radio Frequency Basics
The radio frequency spectrum spans a wide range of frequencies, the use of which is allocated by international and federal governments (i.e., International Telecommunication Union) for different uses. Of interest to wireless medical device connectivity are the wireless medical telemetry system (WMTS) band and the industrial, scientific, and medical (ISM) band. WMTS covers frequency bands 608–614MHz, 1395–1400MHz, and 1429–1432MHz; the majority of new telemetry installations will fall within these frequencies. The total available spectrum for WMTS is therefore 14MHz, a limiting factor governing the number of supportable devices unless frequency reuse is considered. The two most commonly used ISM bands are the unlicensed 2.4GHz spectrum under which fall the majority of 802.11b/g/n wireless radio cards, and the 5.15GHz–5.825GHz spectrum which supports the more recent 802.11 a/n wireless radio cards. The 2.4 spectrum is populated by many device types other than wireless medical devices including cordless phones, Bluetooth, wireless video cameras, barcode scanners, and baby monitors, and hence is very crowded. This spectrum is also limited by the availability of only three nonoverlapping channels (1, 6, and 11) within the 802.11 b/g/n communications. These limitations are driving newer designs for both commercial and medical devices to be implemented in the 5GHz spectrum where the 802.11 a/n standards provide much greater spectrum availability and 23 non-overlapping channels.

Wireless Standards
Currently, the most pervasive wireless technology is 802.11. However, it is important to note that other technologies do exist such as Bluetooth (802.15.1), Zigbee (802.15.4), and others which are short-range wireless communications standards ideally suited for body area networks (BANs) or personal area networks (PANs). Emerging technologies such as body worn smart sensors will use these standards to communicate with each other and a “personal server” wirelessly.

The IEEE 802.11 standard on wireless local area networks (WLANs) is a living document defining the evolving standards of wireless communication. 802.11b defines operation in the 2.4GHz ISM band using high rate direct sequence spread spectrum (HR-DSSS) communication technology. 802.11a uses the 5GHz band with orthogonal frequency division multiplexing (OFDM) communication; this spectrum allows for higher data rates, has greater bandwidth, and substantially more nonoverlapping channels. 802.11g uses the 2.4GHz ISM band with extended rate physical (ERP) OFDM for high data rates and ERP-DSSS to maintain backwards compatibility with 802.11b devices. In 2009, 802.11n was added to the standard. The primary goal of 802.11n was to increase the throughput in both the 2.4GHz and 5GHz frequency bands; however the greatest advantage is in the 5GHz band due to the much greater number of nonoverlapping channels than that which is possible in the 2.4GHz spectrum (23 channels vs. 3 channels). High throughput is achieved through a technique called multiple-input, multiple-output (MIMO), along with OFDM. MIMO uses multiple receiving and transmitting antennas and can receive multiple signals that would have previously been considered interference from multipath. The net result of MIMO is a more robust wireless infrastructure for sustained connectivity under ever changing environmental conditions (e.g., a metal cart moving down a hallway can substantially alter RF reflections and thus change multipath patterns). An 802.11n infrastructure improves

The 2.4 spectrum is populated by many device types other than wireless medical devices including cordless phones, Bluetooth, wireless video cameras, barcode scanners, and baby monitors.
the communications link to any 802.11a client by taking advantage of the improved infrastructure capabilities inherent in 802.11n. 802.11n also enables high throughput by “channel bonding,” i.e., creating 40 MHz-wide channels from two adjacent 20 MHz channels, and sending data via each of the bonded channels. In this case, 802.11n allows for only 1 orthogonal channel in the 2.4 GHz band and 11 in the 5 GHz band.2

Security
The security of any network is important, especially a hospital’s wireless network containing mission critical patient data and potentially life-critical patient monitoring information. The Health Insurance Portability and Accountability Act (HIPAA) requires the protection of identifiable patient information. There are security measures inherent within the 802.11 suite of standards, as well as additional security precautions that can be implemented on a network to ensure the protection of patient data.

In terms of inherent network security mechanisms, earlier versions were insufficient, but significant improvement came when the 802.11i amendment became part of the 2007 standard. 802.11i defined a robust security network (RSN) that incorporated authentication and authorization using an extensible authentication protocol (EAP), yielding a second generation of Wi-Fi protected access (WPA2) enterprise security. WPA2 uses counter mode with cipher block chaining message authentication code protocol (CCMP) encryption, an advanced encryption standard (AES) cipher, and dynamic key generation.2

In addition to the encryption and authentication protocols, wireless networks can be protected by intrusion detection systems (IDS), which monitor wireless network activity and/or intrusion prevention systems (IPS) that mitigate the risks by isolating the intruder. A wireless intrusion detection system (WIDS) usually consists of a server, management consoles, and sensors.2 However, the configuration settings of these network appliances can have a dramatic effect on the reliability of the network that supports medical devices. For example, some IDS will flood an intruder with broadcast traffic during which connectivity to all other client devices, including life critical medical devices, is interrupted. This behavior is a major risk under 80001-1 requiring a mitigation strategy if life-critical alarms are supported by the network.

Wireless Medical Devices
In the Hospital
There are many medical device types and other related hospital systems that are currently using wireless communication. Whether these devices/systems are deployed on hospital’s enterprise wireless network or on a separate network exclusively for medical devices varies across different hospitals. Regardless, more and more devices are including the capability to function wirelessly whether it is to transmit critical alarms, transmit physiological waveform data, or provide real-time control.4

One of the first wireless medical device applications in the hospital was ECG telemetry. These devices emerged from the NASA program in the late 1960s and shared the locally unused sections of the very high frequency (VHF) and ultra high frequency (UHF) bands. The telemetry system wirelessly transmits the patient data to a central station for real-time monitoring.

There was an incident at Baylor University Hospital in Texas in which a new local high powered digital TV broadcaster came online and significantly interfered with the hospital’s telemetry system.5 The same problem occurred at Methodist Dallas Medical Center, and these two incidents became the catalyst for the FCC to create WMTS. Since the FCC ruling, the majority of medical telemetry vendors have migrated from a one-way communications link to a two-way link to improve connectivity reliability and offer more features.

However, the FCC ruling did not define how the spectrum would allow coexistence of two medical telemetry systems in a single facility, nor did it protect medical telemetry systems for adjacent channel interference.4 The use of the licensed WMTS band for telemetry did not eliminate the interference problem as anticipated. For example, in 2002 a Kansas hospital experienced intermittent severe dropouts which were determined to be caused by TV channel 38’s new digital TV36 transmitter. The fix resulted in limiting their use of the spectrum from 608–614MHz to 610–612MHz. Similar problems affected a New Jersey hospital in 2003.
In addition to interference from television channels, problems still arise from electromagnetic interference (EMI) from medical devices and other equipment within the hospital environment. In 2004, an endoscopic positioning system moved unexpectedly during a procedure. This occurrence was later attributed to a coexistence incompatibility with a wireless microphone in use at the time. In 2010, a physiological monitor intermittently displayed a “flat” ECG waveforms and presented asystole alarms. These events could be reproduced when a wireless radio-enabled laptop or a smart phone were restarted in proximity with the device.

An alternative example of a wireless medical device that uses the ISM bands on a shared-spectrum basis is pulse oximetry monitors that continuously monitor the patient and send the data wirelessly to a centralized monitoring station. Infusion pumps also have wireless capabilities that use the ISM band, but the application is different; currently it is not for continuous monitoring of the infusion information (although some vendors may be moving in this direction), but rather for updating the drug library on smart pumps, interfacing the physicians’ orders with the pump, and recording the pump infusion information to the EMR. ECG carts, ultrasound machines, and ventilators also use ISM-based wireless communications, each with its own unique network connectivity requirements.

The number of device types and the degree of wireless capabilities in medical devices is expected to continue to grow rapidly. A report conducted by ABI Research in 2009 estimates there will be 5.7 million patients monitored with wireless medical devices in 2014 as compared to 320,000 in 2009. Greystone Research Associates reports in-house wireless monitors will grow 13% per year between now in 2014.

In addition to medical devices, other systems related to the delivery of healthcare use wireless technology, such as voice over Wi-Fi (VoWiFi) that can be used for communication between clinicians on patient floors. Another is real time location systems (RTLS) that can be used to track assets. This has benefits for clinicians in need of high-volume equipment such as infusion pumps, as well as for the clinical engineering department that needs to locate equipment for routine maintenance. These are in addition to the proliferation of mobile computers, commonly known as “workstation on wheels” or WOWS, that run applications such as medication administration or vital signs charting. The constant challenges of interference affecting wireless communication are strong motivation for proper risk assessment, testing, and validation of performance.

**Risk Assessment and ANSI/AAMI/IEC 80001-1**

It is in every clinical engineering department’s best interest to provide effective and efficient management of networked medical device systems. In December 2008, The Joint Commission issued Sentinel Event Alert # 42 that called out the need to shift some focus to these converging technologies. There currently exist several standards that touch upon the safety requirements of medical devices. The IEC 60601 family, for example, includes guidance on the electromagnetic compatibility for medical electrical equipment (ANSI/AAMI/IEC 60601-1-2:2001). With these, there are several reference standards for wireless medical devices, including the Federal Communications Commission’s guidance on personal radio services, such as WMTS (47 CFR Part 95). Yet, it is a daunting task to first read all of the available documentation and then identify and implement the relevant points as part of the management plan. If hospitals are to be more involved with onsite testing and management of such networked systems, more dedicated resources are needed.

In response to the accelerating adoption of medical devices to IT networks, the International Electrotechnical Commission (IEC) recently ratified the 80001-1, *Application of risk Management for IT networks incorporating medical devices*. The goal of this standard is to improve patient safety in the IT-integrated health care environment. In the 2010 edition of *IT Horizons*, Todd Cooper and Sherman Eagles say the goal of the standard is to address “the need to consider the potential safety impacts in
the design and implementation of IT-networks incorporating a medical device prior to putting them into service.\textsuperscript{11}

Several technical reports associated with IEC 80001-1 are under development, one of which will focus specifically on wireless medical devices.\textsuperscript{12} Recommendations are given in the technical report regarding what to consider when adding wireless medical devices onto IT networks. One recommendation is segregating life-critical network traffic from general purpose IT traffic. The wireless technical report recommends categorizing medical devices by their device performance characteristics, and designing the network to meet the most stringent needs. The document also describes the important performance characteristics that should be verified as a part of the testing and mitigation process.

Due to the extensive recommendations for the risk assessment process, there is concern about the necessary work required to implement the standard. However, work is underway to provide guidance and learning tools for healthcare delivery organizations (HDOs) on how to perform risk assessment and validate device performance based on ANSI/AAMI/IEC 80001-1.

### The State of Networked Medical Device Support

Based on the results of a small survey (47 respondents from 28 different hospital systems) distributed to ACCE membership in July of 2010, many clinical engineering professionals are gaining experience with the planning and support of network technologies such as wireless network design and supporting the medical devices on that network (Table 1). As reported, many are incorporating network and information system technologies as part of medical device lifecycle, yet few reported having the responsibility to design or troubleshoot the wireless network that hosts medical devices. While several have IT counterparts that bear the major responsibility for network management, neither group is formally trained to how to approach such a complex and hybrid system of technologies and management theories. One approach to consider is the development of a test lab to provide training, technical system analysis, and connectivity verification to clinical staff.

<table>
<thead>
<tr>
<th>Answer Choices</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical technology management</td>
<td>82.60%</td>
</tr>
<tr>
<td>Repairing and maintaining medical devices</td>
<td>67.40%</td>
</tr>
<tr>
<td>Supporting medical devices on proprietary “patient care” wired network</td>
<td>54.30%</td>
</tr>
<tr>
<td>Supporting medical devices on enterprise wired network</td>
<td>47.80%</td>
</tr>
<tr>
<td>Clinical Systems/Applications management</td>
<td>43.50%</td>
</tr>
<tr>
<td>Supporting wireless medical devices on “patient care” wireless network</td>
<td>41.30%</td>
</tr>
<tr>
<td>Supporting wireless medical devices on enterprise wireless network</td>
<td>37.00%</td>
</tr>
<tr>
<td>Use of spectrum analyzer</td>
<td>32.60%</td>
</tr>
<tr>
<td>Wired network troubleshooting</td>
<td>23.90%</td>
</tr>
<tr>
<td>Wireless network troubleshooting</td>
<td>19.60%</td>
</tr>
<tr>
<td>Repairing and maintaining IS equipment (PCs, laptops, printers)</td>
<td>17.40%</td>
</tr>
<tr>
<td>Site surveying for new wireless projects</td>
<td>17.40%</td>
</tr>
<tr>
<td>Wired network design/architecture</td>
<td>17.40%</td>
</tr>
<tr>
<td>Management of network security</td>
<td>13.00%</td>
</tr>
<tr>
<td>Wireless network design/architecture</td>
<td>13.00%</td>
</tr>
<tr>
<td>Supporting non-medical wireless devices</td>
<td>8.70%</td>
</tr>
<tr>
<td>AP management</td>
<td>4.30%</td>
</tr>
</tbody>
</table>

*Table 1.* Results from Question 4 of the CE IT Staffing Survey conducted by ACCE in July 2010: “Which of the following functions are you responsible for in your current role?” This question was answered by 46 out of 47 participants.
engineers and IT staff alike. Such a lab would establish an environment to catalyze the advancement of sustainable policies and procedures that can be used as part of the hospital’s management plan in compliance with ANSI/AAMI/IEC 80001-1.

Conclusion
It will be as important as ever to utilize currently existing assessment tools such as failure mode and effects analysis (FMEA) to identify the gaps and threats in medical device systems that utilize the wireless architecture at some level. In a sense, performing risk assessment via ANSI/AAMI/IEC 80001-1 is a technically specific FMEA for medical devices that will be deployed on the IT network. Current risk assessment tools need to be harmonized with standards such as ISO 14971 (which is a foundation for ANSI/AAMI/IEC 80001-1) and the regulatory expectations from organizations such as The Joint Commission/Joint Commission International, so that overall risk management can administrated over the lifecycle of the system. Many of the potential failures identified can be mitigated through technology, but those solutions will need to be studied and tested.

Developing assessment and management tools for the integration of medical devices onto hospital IT networks presents a leadership opportunity to clinical engineers and biomedical technicians. As patient data transmission migrates to telehealth, home health, and body area network paradigms, the need for comprehensive risk management analytics will continue to rest at the core of this new opportunity.

References