Wireless Medical Systems  
Risks, Challenges, And Opportunities

Donald Witters

Envision a wireless patient monitoring system at a large busy hospital suddenly loses connection with several patients. The staff scrambles to reconnect the patients to wired monitors while the clinical engineering department tries to figure out the problem. The cause is traced to the new digital television broadcast which has completely overwhelmed the medical system. Consider drug infusion pumps, active implantable medical devices, wireless nurse call units, or blood collection systems where the wireless link is slowed, intermittent, disrupted, or cannot be reliably established. Visualize a patient just home from a procedure where a new pacemaker generator was implanted because the old device battery was at the end of its life. He is awakened by an alarm that indicates battery end of life only to find that the alarm was from the old pacemaker that the patient had placed near his bed. These are real events.

The benefits and opportunities for innovation via wireless technology are numerous and can outweigh the risks. This article focuses on key technical aspects that, if managed well, can help make the path to market and market adoption much more likely.

Risk Recognition and Vigilance
The problems described above occurred because the risks associated with wireless technology were inadequately recognized and attended to. However, even if the medical device manufacturer takes care through design and implementation, and the user maintains good oversight, the world of wireless technology changes so rapidly that these preplanned risk mitigations, by themselves, become insufficient. Premarket recognition of the risks combined with postmarket vigilance in keeping up with wireless technology changes are hallmarks for safe and effective medical systems.

The risks can be minimized by addressing key technical areas that include quality of service (QoS), data integrity (e.g., data throughput, latency, and data corruption), coexistence with other wireless equipment, wireless security, and electromagnetic compatibility (EMC). This brief overview is drawn from

About the Author
Donald Witters is a biomedical engineer with the Office of Science and Engineering Laboratories, CDRH at the U.S. Food and Drug Administration. E-mail: donald.witters@fda.hhs.gov.

Case Study
Managing Conflicting Requirements

Project: A hospital chooses to deploy 802.11-based active RF-ID tags to support equipment location and tracking

Problem: The clinical staff begins to complain about loss of data on 802.11-based patient monitoring systems.

Cause: The biomedical department contacts the manufacturer whose engineers prove that the APs are not acknowledging data even when a sniffer successfully receives the data. When asset tracking is disabled, the problem goes away. The AP vendor changes a configuration to “fix” the issue, but asset tracking doesn’t update regularly. The solution was to install separate APs for the sole function of asset tracking.

Recommended Practice: With 80001, the risk manager would have queried the AP manufacturer about side effects of asset tracking, learned it requires the APs to implement off-channel scanning, and determined this was unacceptable. Hospital would learn the true cost of the installation up front.

—Steven Baker and Ken Fuchs

Horizons Fall 2011 49

136-002 Horizons Revisions: 4 04-28-11
Information in the FDA draft guidance Radio-Frequency Wireless Technology in Medical Devices and other resources.

While this article deals with the uses of wireless technology for communications and control of data and information, the reader should not lose sight of other types of wireless electromagnetic energy and technology used in medical applications. Such applications include diathermy, ablation and magnetic resonance imaging (MRI) technologies that are complex with unique risks.

The rapid pace of wireless technology deployment and acceptance outside medical systems can compound misconceptions about complexities and risks. Some believe that the information technology (IT) community and radio engineers have all things well under control and there are few if any risks in using wireless technology. The reality is not so simple. In a world hungry for the mobility that wireless technology offers, the convergence of IT with medical systems poses challenges and introduces the need for risk management where it may not have been addressed previously. The key point is that risk management is a fundamental part of healthcare and extends to wireless medical devices and systems. The IEC 80001-1:2010 standard for networked medical devices offers a pathway for dealing with these risks.

The risks associated with medical devices and systems that incorporate wireless technology are complex and multifaceted. To help take advantage of wireless technology in medical devices it can be useful to partition risks into high- and low-priority categories. Examples of low-priority risks include wireless transmission of noncritical patient history or billing that contains few, if any, immediate time needs. Examples of high-priority risks include wireless transmission of information for drug delivery or therapies, remote control, critical patient monitoring, and high-priority alarms. These present immediate needs for the information carried wirelessly and even momentary lapse of the wireless technology for high priority signals can have very serious consequences.

At its foundation, wireless technology is based on the broadcast of electromagnetic energy with unique characteristics that simultaneously makes it a source and a victim of electromagnetic interference (EMI). In general, electrically powered medical devices should be designed and tested for electromagnetic compatibility (EMC) which strives to eliminate disruption of the medical device function by electromagnetic disturbances. However, dealing with EMC does not encompass all risks stemming from the incorporation of wireless functions and links. EMC safety issues have long been recognized and are commonly dealt with through national and international consensus standards. However, there are limitations to these standards. For example, the widely referenced IEC 60601-1-2 for medical electrical equipment EMC exempts immunity testing in the frequency range of the wireless receiver of the medical equipment.

Unfortunately, at present there is a dearth of standards specifically dealing with the risks presented by wireless technology incorporated into medical devices. The wireless technology standards such as the Institute of Electrical and Electronics Engineers (IEEE) 802.11 wireless standards, International Organization for Standards (ISO) standards for radio frequency identification (RFID), and others, speak primarily to technology and characteristics to reproduce the standard’s implementation and verify operation. Even with these standards the products produced can vary in performance that might make them unsuitable for certain medical applications such as higher priority risk uses.

The lack of standards specific to medical wireless uses presents opportunities to create novel and innovative approaches focused on the unique needs of medical systems. For example, there is need of standards for testing wireless systems in the dynamic environments where medical devices are used. Consensus information and guidelines with step-by-step instructions for designing, testing, and maintaining wireless systems and networks in healthcare are sorely needed.

**Addressing Wireless Risks**

A reasonable way to begin addressing risks related to wirelessly enabled medical device systems is with a detailed description of the medical device and the wireless technology it incorporates. The information should include the wireless characteristics and capabilities (e.g.,
Wireless networking includes wireless frequencies, output power, and effective range, the wireless functions related to the medical device use, and expected performance. A summary of this information should also be located in the instruction manuals for wireless medical systems, which can provide valuable information for use and maintenance.

Additionally, the following key points should be addressed in the design, testing, and maintenance of the medical device system:

**Quality of Service (QoS):** This includes specific information about the wireless technology needed for safe and effective device performance and use. The information should include a brief description of the wireless technology, programming, configuration settings, and metrics and tolerances for parameters such as dropped data packets or errors.

**Data Integrity:** This deals with the ability of the wireless system to successfully transmit and receive digital data packets within the tolerances needed by the medical device’s intended use. Nearly all digital wireless communications systems lose data or have errors during typical operation. The key for medical systems is to recognize and appropriately deal with these so as to maintain device operation within prescribed tolerances.

**Coexistence:** In our world of ever-increasing and changing wireless technology, and with significant numbers of medical systems utilizing the same small frequency ranges, the risks related to the ability of the wireless signals to coexist in a shared environment looms large. For example, how well will the device perform its functions in the presence of other like devices as may be the case in a physician’s waiting room with two or more devices in or on patients sitting side by side? Testing should be performed to verify that the medical device and its functions will perform safely and effectively in the presence of an array of other wireless technologies. This should include broadband emitters such as a leaking microwave oven that is well known to disrupt the operation of Bluetooth technology and IEEE 802.11 wireless products operating in the same frequency band.

Unfortunately, there is an absence of standards focused on medical device coexistence that encompass realistic simulation of wireless traffic. In the absence of consensus testing methods, an approach loosely based upon ad-hoc testing from the C63.18 document has been used. Figure 1 illustrates the general method to observe effects on performance of the medical device wireless link (red arrow) while being exposed to a number of wirelessly enabled equipment that can be expected in the vicinity. Key factors include orientation and separation distance of the sample wireless interferers.

**Security:** Design, implementation, and verification of security measures appropriate for the medical device risks should be a building block for the wireless medical systems. Given the risks involved and consequences for medical systems use of the highest level wireless security available is a wise way to minimize risks. This includes enabling the

---

**Case Study**

**Managing Replacement of Potentially Interfering Equipment**

**Project:** A hospital replaces one of two industrial microwave ovens

**Problem:** Several months later, the clinicians report issues with 802.11-based patient monitoring running in the 2.4 GHz band.

**Cause:** Investigation discovers the patient-monitoring issues began months before they were reported and traced to the time of the replacement of the microwave ovens. Before replacement, the ovens operated in phase. After the replacement, they did not run in phase. Solution was to add additional APs at larger distance from the interfering microwave ovens.

**Recommended Practice:** IEC 80001-1 wireless TR recommends cataloging all RF sources and periodic reviews. This database and timely reviews could be used to determine that the duty cycle of RFI increased and help determine root cause faster.

—Steven Baker and Ken Fuchs

---

© Copyright AAMI 2011. Single user license only. Copying, networking, and distribution prohibited.
security features that are available, which may take user activation to operate.

- EMC: The requirements of EMC specifically challenges the wireless equipment and signals. Many new wireless technologies have capabilities that allow them to dynamically adjust to minimize EMI effects. Nonetheless, it is important to test wireless medical devices for wireless EMC because of the limitations inherent in the consensus standards and the risks involved.

Opportunities and Challenges

The world of wireless technology offers much for healthcare and is rapidly changing yet confined to limited resources—the radio spectrum is wide but finite. Simultaneously, there is wider integration and use of wireless technology in healthcare that present nearly boundless opportunities. Large expansion of wireless technology is expected in the home-use arena where there are opportunities for greater function, but this also poses greater challenges because of less knowledgeable user oversight.

This use expansion allows many opportunities to create products and services such as wirelessly enabled patient-monitoring systems, plug-and-play protocols, and much needed design and testing services specific to the unique needs of healthcare and medical delivery. The moment is also ripe to develop consensus information and standards aimed toward efficient, safe, effective, and secure use of wireless technology in healthcare. Opportunities abound to create innovative approaches and pathways to market, including regulatory authorities who are reaching out to engage stakeholders.

The challenges of making the wireless devices and systems truly interoperable requires research, risk awareness and management, stakeholder engagement, consensus standards and information, and a proactive approach to safe, secure, reliable deployment.

References


Case Study

Security Hole

Project: Hospital installs some new wireless medical devices on its 802.11b/g network

Problem: War driver hacks into the wireless network and has access to the entire hospital network and has access to the entire hospital network and compromises the security of servers which contain sensitive medical data.

Cause: After investigating the issue, IT realizes that the new devices only support WEP encryption which allowed the hacker to use a widely available tool that deciphered the WEP key after only a few minutes. Solution was to keep Wi-Fi devices with weak encryption on a separate ESSID/VLAN while using a firewall to quarantine this traffic.

Recommended Practice: An 80001 risk management analysis would have uncovered this risk to the network and the hospital would have considered different ways of managing this risk such as installing a firewall or installing a separate wireless network dedicated to the medical device (not always possible). Sometimes the best answer is to remain wired until security issues are resolved.

—Steven Baker and Ken Fuchs