Medical Device Safety: Addressing the Issues

Written by Mary Mosley

Potential safety issues for active implantable medical devices (AIMDs; eg, pacemakers), include cybersecurity, electromagnetic interference, abandoned pacemaker leads, and magnetic resonance imaging (MRI).

Any device, including an AIMD, on a wireless network is potentially susceptible to emerging threats, stated Ken Hoyme, MSEE, Adventium Labs, Minneapolis, Minnesota, USA. However, the known benefits of these devices continue to outweigh the possible risks, he said. Device security is a journey that requires ongoing assessment, mitigation, and monitoring. He noted that the right of patients to have secure devices should be driven by manufacturers, not by regulatory requirements.

The multidisciplinary issue of cybersecurity will require such a solution, stated Mitchell J. Shein, MS, United States Food and Drug Administration (FDA), Silver Spring, Maryland, USA. The Association for the Advancement of Medical Instrumentation (AAMI) is actively collaborating with the clinical community, medical device industry, and FDA to address this issue, as well as others.

Far-field telemetry poses risks because of its medium level of power, electromagnetic coupling, frequency (400–900 MHz), proprietary protocols, and design to work within a range of <100 ft. Medical devices use commercial and medical device standards (wireless medical telemetry systems, medical body area networks). The use of commercial device standards may be more vulnerable depending on how they are secured and internetworked, stated Hoyme.

The FDA issued draft guidance for device risk management in 2013 that called for harm and likelihood assessments by industry, and a guidance document is now being developed by the AAMI's Device Security Working Group. The FDA has called for manufacturers to include cybersecurity elements in device design and develop methods to protect and assess AIMD safety (Table 1). Standard system device design should include algorithms to detect intrusion, logs for device access, and basic safety practices. Documentation and labeling should include evidence that current protections are implemented and information regarding safeguarding of devices, stated Shein. Actions for health care providers to ensure device safety are listed in Table 2.

Official Peer-Reviewed Highlights From

Heart Rhythm 2014
35th Annual Scientific Sessions
May 7–10, 2014 San Francisco, CA

Heart Rhythm Society

CARDIAC DEVICES AND SAFETY

AIMDs are designed and manufactured to meet or exceed government regulations and industry electromagnetic compatibility standards and to include immunity to emissions that can cause electromagnetic interference, according to Ronald Reitan, MSEE, Boston Scientific, Natick, Massachusetts, USA. However, electromagnetic interference threats remain, including electromagnetic field sources with emissions that exceed current AIMD immunity, reasonably foreseeable exposure durations, and separation distances that are known to cause clinically significant reactions. Immunity standards are 14 years behind current technology and are being updated by the AAMI.

New emitters of electromagnetic interference that are within the current maximum permissible exposure (MPE) regulations and do not consider the presence of a cardiovascular implantable electronic device (CIED) are potential threats to current devices. Current regulations consider biological safety but do not account for device safety. Patients with AIMDs are not a protected class and are at risk, noted Dr. Reitan. The International Commission on Non-Ionizing Radiation Protection issued revised MPE guidelines in 2010 with higher levels of allowable exposure [International Commission on Non-Ionizing Radiation Protection. *Health Phys* 2010], and the Federal Communications Commission is determining standards for adopting new MPE guidelines for exposure below 100 kHz. These higher MPE levels are a concern in relation to AIMDs, and the AAMI working group has commented on and is monitoring the Federal Communications Commission's rule making.

Unknown threats to AIMDs being examined by the AAMI working group for setting standards are electromagnetic pulse cannons used by law enforcement agencies, hybrid electric vehicle

Table 1. Device Design Elements for Cybersecurity

Confidentiality
Document methods for maintaining the confidentiality of the information, data, and the identity of the device.
Integrity
Define and implement methods to maintain the integrity of the data.
Availability
Ensure that the device design includes the ability to meet the data availability requirement for the device.
Risk assessment
Include cybersecurity risks and mitigations in the risk management process.

Table 2. Actions for Health Care Workers to Ensure the Cybersecurity of Devices

Help minimize system access.
Do not share passwords or post login information next to device.
Work with IT/BME to ensure that login features are activated.
Understand how you are accessing the device.
Check device settings to ensure that they have not been tampered with.
Remember that anything that allows access to a network can be used to access private information.

BME=biomedical engineering; IT=information technology.

chargers, and Trans-European Trunked Radio (TETRA), a relatively new technology primarily used by law enforcement and emergency responders in mobile and handheld radios, human body communication (smart watches), smart meters, wireless power transfer, and other electronic devices.

The modulation (17 Hz) and frequency (150 and 380 MHz) combinations of TETRA have not been tested by the International Organization for Standardization. Despite this, TETRA is currently being used around the world. Although guidelines in Austria recommended 30 cm as a safe distance between TETRA transmitters and implants, on the basis of a 2010 study conducted in Austria with 21 pacemakers and 6 implantable defibrillators [Cecil S et al. URSI 2011], the true safety is unclear because of study limitations, including interference not being classified as clinically significant observations, unrealistic setting of devices to maximum sensitivity, and the device mix not being representative of current models.

The AAMI working group, with the FDA, is currently conducting a study of TETRA safety. It is also conducting a study on the effects of high-voltage distribution, developing standardized tests for electronic article surveillance and radiofrequency identification emitters, and revising International Organization for Standardization 14117 standards to close gaps related to scope (broader range of CIEDs), usability (industry and regulators), and efficacy (maximizing CIED immunity).

MRI SAFETY AND IDENTIFYING AIMDS

MRI poses potential harm in patients with AIMDs, whose function may be affected by the electromagnetic frequency. MRI is contraindicated in patients with abandoned pacemaker leads. Abandoned leads can severely overheat during scans (1.5 T, 4 W/kg), as shown by experiments conducted by Robert A. Stevenson, PhD, Greatbatch Medical, Santa Clarita, California, USA. Work is under way to develop special energy-dissipating lead caps to mitigate unsafe heating, which may provide a safe solution to allow MRI in these patients.

The second edition of the International Organization for Standardization 10974 technical specifications for the assessment of the safety of MRI for patients with AIMDs is expected in early 2016. It will provide guidance only for "nonsensing" AIMDs for various types of threats, including device heating, force and torque, combined field exposure, and gradient-induced unintended stimulation. This horizontal standard is intended to serve as a foundation for the development of vertical standards for specific devices or settings. The CIED vertical standard is the first being developed by AAMI and will set requirements and test protocols for the safety of patients with pacemakers and implantable cardioverter defibrillators.

An urgent public health issue is the need for a uniform approach to identify all powered AIMDs, including cardiac rhythm management devices, in patients presenting to emergency or operating rooms and other health care settings to ensure their safety and reduce associated risks, stated G. Frank O. Tyers, MD, Vancouver Coastal Health Hospitals, Vancouver, British Columbia, Canada.

Prof. Tyers called for a generic system capable of immediate, accurate, and detailed identification of all AIMDs to address the current lack of uniformity by manufacturers, including the magnet response rate. A current approach of placing a magnet over an AIMD does not accurately identify and could actually damage the device. Until solutions are developed, such as a universal interrogator or the placement of radiofrequency identification chips within devices, he stated that all AIMDs should have alarm warnings that magnet placement may be hazardous for patients or implanted devices. The AAMI's Cardiac Rhythm Device Committee is developing standards, including the Unified Recommended Replacement Time Magnet Response Requirements.