Journal of Diabetes Science and Technology
Volume 2, Issue 5, September 2008

EDITORIAL

Designing an Artificial Pancreas System to Be Compatible with Other Medical Devices

David C. Klonoff, M.D., FACP

Introduction

Any artificial pancreas system must demonstrate acceptable levels of safety and effectiveness in order to be approved for use. Many such systems will be used in hospital settings in close proximity to other medical devices. In such settings, a third feature of an artificial pancreas will need to be demonstrated. This feature is compatibility. The most important features of compatibility in hospital-based medical devices are (1) interoperability; (2) resistance to electromagnetic interference (EMI) from other electronic equipment, including emitters such as radio frequency identification (RFID) systems; and (3) integration with bar code identification systems. Compatibility is becoming an increasingly important feature of medical devices such as closed-loop systems for control of glucose.

Interoperability

Interoperability refers to the capability of two systems of different types, models, or manufacturers to cooperate using exchanged information whether connected to each other directly or through a communication system. When medical systems are used simultaneously by the same operators and they are not compatible, then problems can arise from the lack of communication between systems. The Plug-and-Play program of the Center for Integration of Medicine and Innovative Technology is committed to promoting three types of interoperability in an operating room environment. These include (1) Plug-and-Play system architecture, (2) open standards for data communication, and (3) interoperability standards for device integration. These important features of future medical devices should be applied to future artificial pancreas systems as well, because such systems will be utilized adjacent to, and in some cases connected to, other medical monitors and drug delivery systems.

Electromagnetic Interference

Electromagnetic compatibility (EMC), which is a state of no EMI, is a necessary feature of an artificial system. On December 26, 2006, the Food and Drug Administration (FDA) posted a notice on their website regarding this topic.[1] This notice stated that EMC means that a device is compatible with (i.e., no interference is caused by) its electromagnetic (EM) environment and it does not emit levels of EM energy that cause EMI in other devices in the vicinity. A medical device can be vulnerable to EMI if the levels of EM energy in the environment exceed the EM immunity (resistance) to which the device was designed and tested. The different forms of EM energy that can cause EMI are conducted, radiated, and electrostatic discharge.

Author Affiliation: Mills-Peninsula Health Services, San Mateo, California

Abbreviations: (CT) computed tomography, (EM) electromagnetic, (EMC) electromagnetic compatibility, (EMI) electromagnetic interference, (FDA) Food and Drug Administration, (JAMA) Journal of the American Medical Association, (RF) radiofrequency, (RFID) radio frequency identification, (WSAN) wireless sensor and actuator network

Keywords: artificial, device, electromagnetic, interface, pancreas, radiation

Corresponding Author: David C. Klonoff, M.D., FACP, Mills-Peninsula Health Services, 100 South San Mateo Drive, Room 3124, San Mateo, CA 94401; email address *dklonoff@yahoo.com*

J Diabetes Sci Technol 2008;2(5):741-745

Food and Drug Administration Interest in Electromagnetic Interference

More recently, on July 14, 2008, the FDA posted a report of a specific type of EMI that can cause the malfunction of nearby medical devices.[2] The report stated that the x rays used during computed tomography (CT) examinations may cause some implanted and external electronic medical devices to malfunction. The report acknowledged that most patients with electronic medical devices undergo CT scans without any adverse consequences. However, the FDA has received a small number of reports of adverse events in which CT scans may have interfered with electronic medical devices, including pacemakers, defibrillators, neurostimulators, and implanted or externally worn drug infusion pumps. A basic component of an artificial pancreas is an insulin pump, which means that both of these FDA reports, issued within the past 21 months, announce the possibility of malfunction of an artificial pancreas system because of EMI. The FDA is currently developing new methods for testing the immunity of implantable medical devices to magnetic fields.[3,4]

Wireless Sensor and Actuator Networks

The components of a wireless sensor and actuator network (WSAN) include a sensor that wirelessly transmits a signal to an actuator that stores the data and takes an action.[5] An artificial pancreas is an example of a WSAN. Other such networks include cardiac pacemakers, cardiac defibrillators, cochlear implants, and neurostimulators. EMI can degrade a WSAN if there is enough power to impact electronic signal transmission, and EMI can result in the loss of data or taking an inappropriate action. If, in an artificial pancreas system, the sensor is a continuous glucose monitor and the actuator is an insulin pump, then continuous glucose data might be lost or an inappropriate dose of insulin might be delivered.

Radiofrequency Identification Systems

An RFID system contains two components: a reader and a tag. A reader sends out a radiofrequency (RF) pulse that triggers a response from a tag in the vicinity that is part of its network. The reader then reads the response to determine which unique tag is in the vicinity. An RFID tag is a small device that can be attached to a piece of equipment, a worker's identification badge, or a patient's identification bracelet (**Figure 1**). RFID tags contain antennas that allow them to receive and respond to RF queries from an RFID reader. They transmit data back to the reader using RF. There are two types of

Figure 1. Use of an RFID reader to identify a patient. The RFID tag is on the wristband of the patient. This figure is courtesy of HealthTech Wire/Grundig Business Systems.

RFID tags: active and passive. Active RFID tags contain a built-in battery power supply. These tags are activated by a signal from the reader (although active tags can also be manufactured to transmit continuously or in response to environmental triggers). Passive RFID tags do not contain a power supply and must be awakened by a reader that may be up to 30 ft away. They rely on the power emitted by an RFID reader to transmit data. The signal from passive tags is usually weaker than the signal from active tags.

A patient wearing an artificial pancreas system must be on alert when in the vicinity of a CT scanner or magnetic resonance imaging system to monitor the performance of the system or even disconnect the pump and dose manually with insulin. A patient would not know whether they are in the presence of a handheld RFID or bar code reader that can be carried throughout a hospital to locate or confirm the identity of pieces of equipment, patients, or even employees of the hospital, although handheld RFID readers would not likely cause interference unless they were in very close proximity to the patient. Such handheld RFID readers can be used to check whether tagged sponges were left behind after surgery.[6]

Until recently, there was little concern in the medical community that EMI was degrading the performance

of approved hospital equipment. When modern cellular telephones are used in a normal way, no noticeable interference or interaction occurs with medical devices.[7] In response to a report this year that iPods can cause interference with pacemakers,[8] a follow-up study by the FDA reported no interference effects in pacemakers exposed to iPods.[9] Thus there was a general belief that medical devices are currently constructed with safeguards for protection from stray RF energy affecting their performance and that only specific frequencies that are designated through communication protocols can penetrate these devices.

Controversy

A controversial recent report has prompted medical engineers to reevaluate the effects of EMI on medical equipment. On June 25, 2008, the Journal of the American Medical Association (JAMA) published an original article from Europe that, for the first time in the medical literature, investigated whether EMI from RFID systems can induce potentially hazardous incidents in critical care medical equipment.[10] Without a patient being connected, EMI from both active and passive RFID systems was assessed in the proximity of 41 medical devices, 3 times per device, for a total of 123 EMI tests. The devices tested included nine infusion/syringe pumps, four mechanical ventilators, four anesthesia devices, three external pacemakers, three intra-aortic balloon pumps, three defibrillators, three monitors, two hemofiltration/dialysis devices, two pacemaker programmers, two intensive care unit beds, a fluid warmer, a cardiopulmonary bypass device, an autologous blood recovery device, a 12-lead EKG, an operating table, and a hypo/hyperthermia vacuum pump. In the 123 tests, RFID induced 34 EMI incidents. These occurred in 26 tests with passive tags and 8 tests with active tags. These incidents were classified as hazardous in 22 tests, significant in 2 tests, and light in 10 tests. The median distance between the RFID reader and the medical device in the EMI incidents was 30 cm. The authors concluded that RFID induces potentially hazardous incidents in medical devices. They recommended greater on-site EMI testing in critical care settings and updates of international standards.

The article has prompted a vigorous debate within the medical instrumentation community. The problem with the article was that they used RFID readers with 2–4 W of power, but most RFID readers in hospitals use no more than 1 W. The high-powered readers used in the study were therefore more likely to cause EMI than would the ones that are most typically used in practice. Most (26 of 34) of the tests that showed EMI were from passive tags. These tags usually transmit less powerful signals than active tags. This unexpected preponderance of EMI incidents with passive tags suggests that in the study, the RFID reader used with the passive tags contained an unusually high power source.

A second study of the potential for EMI due to RFID usage in a patient care environment was recently conducted in Indiana and is currently in press.[11] The study tested five devices from each of five classes of medical devices: noninvasive blood pressure monitors, pulse oximeter monitors, pumps, electrocardiogram monitors, and sequential compression devices. The study was conducted following a procedure that was unlike the JAMA study. The devices performed properly in 100% of the 1600 tests conducted.

Based on my reading of the medical literature on EMI and my own experience working in hospitals, my assessment of the current risk of EMI from RFID affecting hospital equipment, such as an artificial pancreas, is contained in the following four principles: (1) In a worst case scenario, any medical device can be degraded by EMI. (2) In a best case scenario, current medical devices are safe from EMI. (3) If something can go wrong, then it usually will go wrong eventually. (4) Constant vigilance is needed to assess new sources of EMI and new equipment whose performance might be degraded by EMI.

Security

Any system with wireless communication is subject to interception of data and compromised privacy. Design features intended to promote compatibility of an artificial pancreas with other medical devices may reduce its security capabilities. An artificial pancreas system must contain safety features to prevent unauthorized interrogation of glucose data or reprogramming of the insulin delivery rate. Even when secure communication technology and restricted access to glucose and insulin data are programmed into an artificial pancreas system, at times, these safeguards might be burdensome. Security and data privacy in medical devices, while desirable, will inevitably conflict with other desirable qualities of such devices, such as accessibility, utility, and longevity.[12] Regarding accessibility in an emergency situation such as severe hypoglycemia, it is important for emergency personnel to be able to access the recent glucose levels and insulin delivery rates as well as be able to reset the insulin delivery algorithm. If the patient is alone, it might be useful to access the patient's name and some medical history from the artificial pancreas system. Regarding

usability, any long-distance communication between medical devices, such as between a continuous glucose monitor and either an insulin pump or a base station for relaying data to an artificial pancreas telemedicine support system, is subject to exposure to interception, interference, or even reprogramming. The advantage of flexibility of use becomes offset by potentially decreased usability of the device. Regarding device longevity, robust security mechanisms are energy intensive and can necessitate more frequent replacement of costly disposable parts of an artificial pancreas, such as the continuous glucose sensor or the motor of an insulin pump. Protection from breaches of privacy or unauthorized reprogramming attacks on artificial pancreas systems will require novel cryptographic security technology or wearable cloaking devices.

Bar Code Identification

A bar code reader is an electronic device for identifying unique bar codes printed on various surfaces, such as product labels or patient information bracelets. A bar code reader consists of a light source in the visible or infrared range, a photodiode for detecting reflected light, a decoder for translating the light data into digital data, and a computer (connected to the reader by a cable) for converting the light data into useful information.

Bar code identification is often used in hospitals for keeping track of inventory and confirming the identity of patients so that correct medications can be administered (**Figure 2**). This technology is intended to confirm five rights of medication administration: right patient, right drug, right dose, right route, and right time. Compared with RFID, this technology is less costly and avoids the use of RF EM energy. Unlike RFID, bar code reading requires the reader to be in close proximity to the object being inventoried, and the method is subject to errors from smudging or damage to the bar code label.

Bar code identification will be increasingly utilized in hospitals for tasks that could be involved in maintaining an artificial pancreas, such as confirming a patient's identity, identifying a component of an artificial pancreas, or refilling insulin into an insulin infusion pump. The theoretical perfect accuracy of this technology in confirming patient, device, or drug identity was recently challenged in a report on the occurrences, causes, and threats to patient safety due to workarounds of bar code medication administration.[13] Koppel *et al*. identified 15 types of workarounds, including affixing patient identification bar codes to computer carts, scanners, doorjambs, or nurses' belt rings and carrying several patients' prescanned medications on carts. They also identified 31 types of causes of workarounds, such as unreadable medication bar codes (crinkled, smudged, torn, missing, covered by another label), malfunctioning scanners, unreadable or missing patient identification wristbands (chewed, soaked, missing), non-bar coded medications, failing batteries, uncertain wireless connectivity, and emergencies. They found that nurses overrode bar code medication administration alerts for 4.2% of patients charted and for 10.3% of medications charted. Possible consequences of such workarounds could include wrong administration of insulin or misidentification of components of an artificial pancreas in the hospital environment.

Solutions

Both RFID and bar code reading in a hospital could lead to problems of incompatibility between an artificial pancreas and other medical devices. The RFID incompatibility problem will require electrical engineering solutions to eliminate the EMI problem. The bar code misuse problem will require human factors and engineering solutions to eliminate workarounds.

EMI caused by RFID systems can be identified and prevented. Every potentially affected device in a setting where RFID will be used should be tested using the communication protocol of the RFID system.[14] The

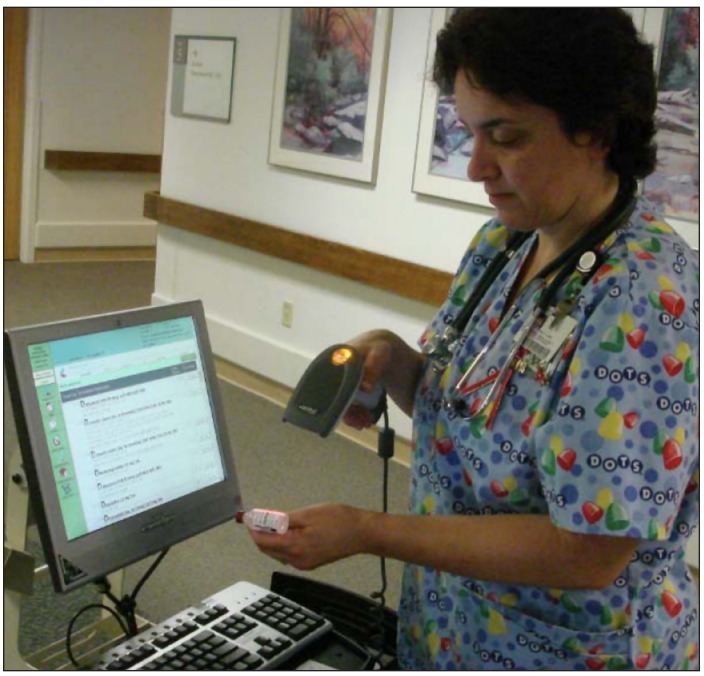

Figure 2. Use of barcode identification to confirm which patient is to receive a dose of insulin. The barcode is on the bottle of insulin. The barcode reader is connected to a computer. This figure is courtesy of Judy Gray, R.N,

system's maximum amount of power and the minimum distance from the reader to the device will be specified by the protocol. There is no good reason to test RFID systems with higher power sources or shorter distances than those that are supposed to be used. If EMI is discovered, then it will be necessary to modify the RFID system or to work with the device manufacturer to increase the shielding on the device from RF or to increase the amount filtering from EM energy in the RF range.

Any medical device that contains a motor or generates an electrical signal can cause EMI. For example, electrosurgical units can generate significant interference. Any type of electronic device can be adversely affected if placed near a powerful source of EMI, which means that an artificial pancreas system or its components could be impacted during surgery if an electrosurgical unit was used. Power from any source of EMI dissipates exponentially with distance. Therefore, in many instances, the best approach to overcoming EMI is to separate the patient and the source of the interference.

The complexity of hospital device technology and RFID systems precludes development of a single perfect solution, especially in a hospital setting that is dynamic in terms of equipment, staffing, and sometimes, device placement. Misuse of bar code reading can be prevented through a combination of thoughtful equipment design, adequate hospital staff training, and ongoing assessment of whether the technology is meeting the needs of the users.

An artificial pancreas system is being developed in a world of increasing use of electronic identification technologies that will be applied to this system when it is developed. Incompatibility of technologies is a potential problem when new technologies must be combined with older technologies or with each other. The best solution to eliminating incompatibility of an artificial pancreas with other medical devices is to always expect the unexpected.

References:

1. http://www.fda.gov/cdrh/emc/. Accessed August 14, 2008.
2. FDA preliminary public health notification: possible malfunction of electronic medical devices caused by computed tomography (CT) scanning. http://www.fda.gov/cdrh/safety/071408-ctscanning.html. Accessed August 14, 2008.
3. Buzduga V, Witters DM, Casamento JP, Kainz W. Testing the immunity of active implantable medical devices to CW magnetic fields up to 1 MHz by an immersion method. IEEE Trans Biomed Eng. 2007;54(9):1679–86.
4. Kainz W, Casamento JP, Ruggera PS, Chan DD, Witters DM. Implantable cardiac pacemaker electromagnetic compatibility testing in a novel security system simulator. IEEE Trans Biomed Eng. 2005;52(3):520–30.
5. Frampton KD. Vibro-acoustic control with a distributed sensor network. J Acoust Soc Am. 2006 Apr; 119(4):2170–7.
6. Rogers A, Jones E, Oleynikov D. Radio frequency identification (RFID) applied to surgical sponges. Surg Endosc. 2007; 21(7):1235–7.
7. Tri JL, Severson RP, Hyberger LK, Hayes DL. Use of cellular telephones in the hospital environment. Mayo Clin Proc. 2007; 82(3):282–5.
8. Thaker JP, Patel MB, Jongnarangsin K, Liepa VV, Thakur RK. Electromagnetic interference with pacemakers caused by portable media players. Heart Rhythm. 2008;5(4):538–44.
9. Bassen H. Low frequency magnetic emissions and resulting induced voltages in a pacemaker by iPod portable music players. Biomed Eng Online. 2008;7:7.
10. van der Togt R, van Lieshout EJ, Hensbroek R, Beinat E, Binnekade JM, Bakker PJ. Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment. JAMA. 2008;299(24):2884–90.
11. Christe B, Cooney E, Maggioli G, Doty DR, Frye RD, Short J. Testing potential interference with RFID usage in the patient care environment. Biomed Instrumentation Technol. In press.
12. Halperin D, Heydt-Benjamin TS, Fu K, Kohno T, Maisel WH. Security and privacy for implantable medical devices. Pervasive Computing. 2008: 7(1):30–9
13. Koppel R, Leonard CE, Localio AR, Cohen A, Auten R, Strom BL. Identifying and quantifying medication errors: evaluation of rapidly discontinued medication orders submitted to a computerized physician order entry system. J Am Med Inform Assoc. 2008;15:461–5.
14. Herkert R. Electromagnetic environmental effects testing of medical devices including those used for the treatment of diabetes. J Diab Sci Technol. 2008;2(5):809-13.