

An Introduction to IEC 80001: Aiming for Patient Safety in the Networked Healthcare Environment

Sherman Eagles

Editor's note: At press time, the second draft of IEC/CD2 80001, Application of risk management for IT-networks incorporating medical devices was scheduled to be issued for comment in late November 2008, at which time it will be placed on AAMI Public Review. To order a copy of the draft when it is made available, visit the AAMI marketplace at <http://marketplace.aami.org>.

For some years, the automation of hospital administrative work flow has been seen as a means to reduce costs associated with delivering healthcare. The publication of the Institute of Medicine report, *To Err is Human: Building a Safer Health System*,¹ which documented a high level of mistakes in patient clinical care, and the subsequent report, *Crossing the Health Care Chasm: A New Health System for the 21st Century*,² added patient safety to the benefits to be gained with automation. Healthcare institutions and the industry that provides them with information technology (IT) products endorsed both reports and sought to rapidly implement solutions that would improve both the cost and the safety of healthcare.

From the beginning, these solutions acknowledged that privacy of medical data was a concern, and the need to address it when automating was clear. But there was little discussion of the potential for new safety risks being created with additional automation. Research and development work targeted how to connect clinical information to networks, with data security being seen only as a possible privacy concern. As often happens when one problem is solved, new problems that had not been considered began to make an appearance.

Risks in the Networked Environment

Complex networked systems, including medical devices, have now become common, and with this added sophistication, new behaviors and unexpected consequences have begun to appear that are outside the control of the medical device manufacturer. We are all aware of intentional security attacks on networks, and these viruses and



“ The goal of IEC 80001 is to apply appropriate risk management consistent with ISO 14971 to address the key properties of safety, effectiveness, data and system security, and interoperability.
—Sherman Eagles

worms have affected hospitals with consequent impact on patient care. An example occurred when Microsoft identified a security vulnerability in the Windows operating system and informed its users. A hospital IT department began updating their systems, but found that they could not upgrade medical devices because the device manufacturer needed to ensure the device would continue to be validated for safe use after the change. While waiting for the medical device maker to implement and test the changes—six months after the vulnerability was identified and a patch was available—the vulnerability was exploited, resulting in the entire hospital network being shut down.

An example of a different unexpected behavior occurred in Europe. After a hospital introduced a new application on its network, intermittent problems began to occur with other networked medical equipment that had previously been working fine. The maintenance engineers sent by the manufacturer of the failing equipment could find nothing wrong with it, but intermittent failures kept occurring. At last, it was discovered that the new application was sending large amounts of data over the network identified as voice data. These data got a high priority on the network, allowing fast data transmission times and quick response by the application, but completely utilizing the capacity of the network, causing the other networked medical equipment to intermittently be unable to communicate. The occasional loss of network services was causing the existing equipment to fail. When confronted with this situation, the provider of the new

application pointed out that the hospital had not specified how data were to be transmitted and that the application met all conditions of their contract with the hospital. Had the consequences of the behavior of the new application been foreseen, the hospital could have taken steps to prevent it from causing problems, but when it occurred unexpectedly, new problems arose.

The adoption of new technology—such as wireless communication networks—greatly increases the likelihood of new problems. Problems can now be the result not just of interactions between devices connected to the network, but also because of interaction with other wireless transmitters that are not part of the network. It is difficult, perhaps impossible, for medical device manufacturers to mitigate all these risks when devices are incorporated into wireless networks, and hospitals can no longer isolate different classes of medical devices on separate network cables.

Launch of the IEC 80001 Effort

The response to these emerging problems has been an industry effort to document good practices that could help prevent them. FDA published a cybersecurity guidance³ to clarify its view of medical device manufacturers' and hospitals' responsibilities. A joint industry security and privacy committee produced a white paper on security risk management for manufacturers.⁴ The Healthcare Information and Management Systems Society (HIMSS) developed a manufacturer disclosure statement for medical device security.⁵ AdvaMed held a workshop on cybersecurity; presentations at conferences and meetings have discussed the problems and efforts to resolve them. In 2006, the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) determined there was a need for a standard to define the requirements of a process for addressing the new problems that might emerge when medical devices are connected to a network. This proposed standard is IEC 80001, *Application of risk management for IT-networks incorporating medical devices*.

IEC 80001 is being developed by a joint working group of IEC 62A, the committee on common aspects of electrical equipment used in medical practice, and ISO 215, the committee on health informatics, with strong liaison to ISO 210, the committee on quality management and corresponding general aspects for medical devices. ISO 210 is the technical committee responsible for developing the international standard for risk management for

medical devices, ANSI/AAMI/ISO 14971:2007, *Medical devices—Application of risk management to medical devices, 3ed*. The joint working group has also invited participation by additional experts with expertise in the area, especially those working in hospital or clinical environments.

The joint working group, which started meeting in January 2007, has circulated a committee draft for comments and is currently resolving the comments that were received. A second committee draft will be circulated before the end of 2008, with a scheduled approval of the standard coming in late 2010.

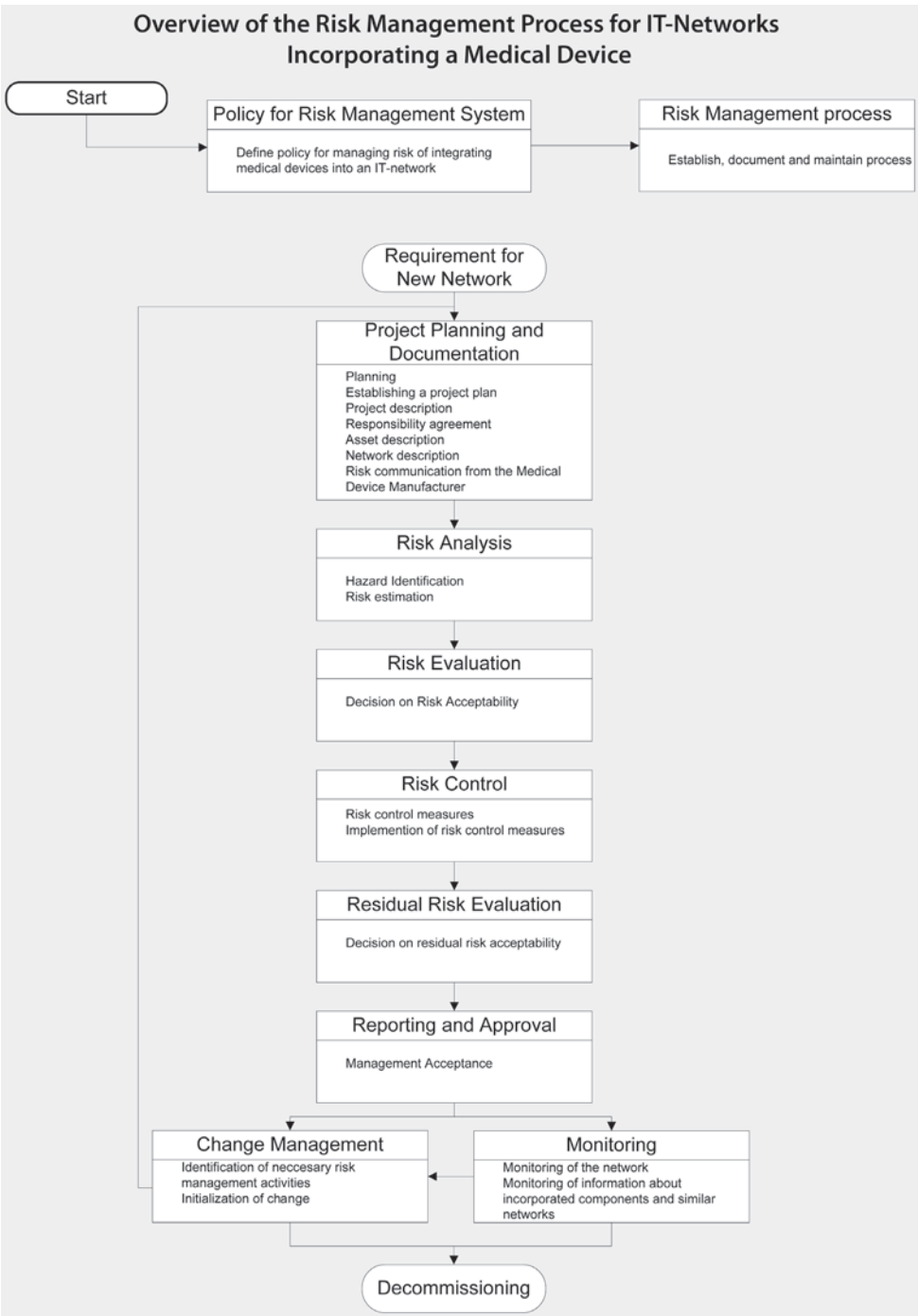
The goal of IEC 80001 is to apply appropriate risk management consistent with ISO 14971 to address the key properties of safety, effectiveness, data and system security, and interoperability. These properties are considered necessary to maintain patient well-being. The standard recognizes that risk management must be applied throughout the entire life cycle of the network—that is, through all the changes that occur during the life of the network. The first draft of IEC 80001 included requirements for the roles, responsibilities, and life cycle risk management process needed to address the key properties for networks with medical devices.

Roles and Responsibilities for Risk Management

In IEC 80001, roles and responsibilities for risk management start with the responsible organization—the institution that owns and has overall responsibility for the network. Within the responsible organization the role of top management is defined. Top management is the executive function that directs and controls the responsible organization and has the ultimate accountability for the network. Top management has responsibility for:

- establishing a policy for how the institution will manage risk for the network so that the key properties are maintained
- establishing the process for applying risk management throughout the life cycle of the network
- assigning people to execute the risk management process
- providing the necessary resources
- specifying the criteria by which risk is determined to be acceptable
- approving the results of the risk management process.

One of the key roles that top management must assign is that of medical IT integration risk manager. This role,



Source: IEC/CD2 80001, Application of risk management for IT-networks incorporating medical devices

which may be filled by a single expert or an expert group, is responsible for the execution of the risk management process to ensure the key properties. The medical IT integration risk manager needs skills in network technology, clinical use of medical devices, and risk management.

In addition to these roles, two others of importance are the manufacturers of the medical devices that are connected to the network, and the suppliers of the net-

work technology.

The medical device manufacturers are responsible for providing all the information about their device that is necessary for the responsible organization to execute its risk management process for the network. This would include relevant technical documentation, and might include specifications of the medical device and information from the manufacturers' risk management activities.

The specific information provided by the medical device manufacturer will vary depending on the intended use of the medical device and the network to which it is connected. The responsible organization also may require information that is proprietary or not generally made publicly available by the medical device manufacturer.

These situations are addressed by the provision in the standard for a responsibility agreement between the responsible organization and each stakeholder that specifies the responsibilities of each party. While the exact format of the responsibility agreement is not explicit in the standard, it is expected that these agreements will ensure that the information and assistance necessary to successfully execute the responsible organization's risk management process will be provided by medical device manufacturers, while protecting the intellectual property of the organization supplying the information.

Organizations providing non-medical equipment and software for the network also have the responsibility to provide all relevant information necessary for the responsible organization to successfully execute its risk management process. In this case, such information might include product technical manuals, recommended product configurations, known problems with the product, and how the product was tested and verified. As with medical device manufacturers, this information will vary depending on the use of the products and the intended use of the network. There will also need to be responsibility agreements between the responsible organization and these technology suppliers that document the specific responsibilities of each party.

The Risk Management Process

Once responsibilities have been assigned and agreements are in place, the medical IT integration risk manager can assemble a network risk management team with the necessary skills to perform the responsible organization's risk management process.

The risk management process described in IEC 80001 has the same activities as the risk management process in ISO 14971 which is used by medical device manufacturers to demonstrate safety of their products. This process in IEC 80001 includes planning the risk management activities, documenting the network assets and architecture, identifying hazards and hazardous situations that could arise from the network, and identifying the events that might cause them to occur. After each hazardous situation has been identified, it is evaluated to determine

A Call for Help

IEC 80001 is still under development. If it is to meet the needs of people managing networks in hospitals, they need to be involved. Their input and review is essential so that all necessary requirements will be included without forcing unneeded activity and effort. The second committee draft of IEC 80001 will be available by the end of 2008. Interested parties should get involved, review it, and make comments. For more information, contact one of the co-conveners of the joint working group, Sherman Eagles at seagles@softwarecpr.com or Todd Cooper at t.cooper@ieee.org.

the impact on the key properties if it should occur, and the likelihood of occurrence. This evaluation provides an estimated risk, which can be used to prioritize the complete set of hazards and hazardous situations, and can be compared to the risk acceptability criteria specified by top management.

“ IEC 80001 provides a framework for a rigorous risk management process throughout the entire life cycle of a network incorporating medical devices.

For each of the hazardous situations that have an unacceptable level of risk, risk control measures should be identified and implemented. When considering options for risk control measures, priority should be given to those that control the risk by design so that it is not possible for the risk to occur. If this cannot be achieved, protective measures such as alarms should be used. If neither of these methods are possible, information such as warnings or training should be considered. In any case, the effectiveness of the risk control measure should be considered and the risk of the hazardous situation occurring after implementation of the risk control measure should be estimated to determine if the risk has been reduced to an acceptable level or if additional risk control measures may be necessary. The risk remaining after control measures have been implemented is called the residual risk, and the goal of the process is to reduce the overall residual risk from all hazards and hazardous situations to an acceptable level. Top management acceptance of this overall residual risk provides the authority to proceed with operation of the network incorporating the medical devices.

Once the control measures are in place and the network

is in operation, it should be monitored to ensure that the key properties are maintained, and any changes made to it should be evaluated for their impact on the overall risk. The risk management process must be applied to changes—whether to the network configuration or to a specific medical device connected to the network—to determine if they introduce new hazardous situations or if they reduce the effectiveness of existing risk control measures. This level of control requires comprehensive management of the network configuration so that no changes can be made without considering their impact on the risk.

IEC 80001 provides a framework for a rigorous risk management process throughout the entire life cycle of a network incorporating medical devices. But only skillful application of this process by knowledgeable people representing all the roles identified in the standard will result in a network that can be relied upon to provide a safe environment for patient care. ■

References

1. **Institute of Medicine.** *To Err is Human: Building a Safer Health System.* Washington, D.C.: National Academy Press, 1999.

2. —. *Crossing the Quality Chasm: A New Health System for the 21st Century.* Washington, D.C.: National Academy Press, 2001.

3. **U.S. Food and Drug Administration Center for Devices and Radiological Health.** *Guidance for Industry—Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software.* Washington, D.C.: U.S. Department of Health and Human Services, 2005.

4. **Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC).** *Information Security Risk Management for Healthcare Systems.* Washington, D.C.: MITA (Medical Imaging & Technology Alliance), 2007.

5. **The Healthcare Information and Management Systems Society.** *Manufacturer Disclosure Statement for Medical Device Security—MDS2.* Chicago, IL: The Healthcare Information and Management Systems Society, 2004.

Sherman Eagles is co-convenor of the joint ISO and IEC working group that is developing IEC 80001. He retired from Medtronic in June 2008 and joined SoftwareCPR, a consulting group specializing in regulated medical software. Eagles is chair of the medical device software working group of AdvaMed and represents AdvaMed on the Global Harmonization Task Force (GHTF) software committee. He is co-chair of AAMI's Medical Device Software Committee, and convenor of three international standards working groups responsible for safety requirements for programmable electrical medical systems, medical device software life cycle processes, and risk management for IT networks that include medical devices.



Innovative
Biomedical Test Instruments
ISO9001-2000 Registered

More of Everything: New Products - Performance - Quality - Reliability - Value

Pressure Meters



Patient Simulators



Electrical Safety Analyzers



Pacemaker Analyzers



Ventilator Analyzer



Mini NIBP Simulator



Defibrillator Testers



Netech Corporation • 60 Bethpage Drive, Hicksville, NY 11801 • USA
800-547-6557 • Ph: 516-433-7400 • Fax: 516-433-7458 • www.GoNetech.com