The effects of an increasingly interconnected world are being felt in healthcare facilities everywhere. Vendor products—from the simplest medical devices to hospital-wide patient monitoring systems to complex electronic health record (EHR) systems—interconnect into systems of systems. More and more, vendors are installing systems in hospitals without a complete view of how they will be associated with other systems and how the infrastructure will evolve. As a result, the mission-critical burden of technology risk assessment and attending to unintended consequence avoidance falls increasingly on hospital staff.

To manage this evolving situation, hospitals need to adopt the tools that medical device vendors have learned to use over the past few decades, especially the concept of risk assessment. As designers quickly discovered, medical device design is all about risk management.

There is no such thing as a perfect medical device. Even the simplest medical device, such as a tongue depressor, can present risks—for example, slivers—to the patient. Aspirin has been hailed as a wonder drug, but when you read the label, there are numerous contraindications and risks associated with taking it. Similarly, the use of a blood pressure cuff has risks and benefits. The key point is that in all cases, the benefits associated with using the devices outweigh the foreseen risks to the patient or caregiver.

In order to assess the risk, you also have to understand the use context. Let’s consider some scenarios concerning a patient being monitored on a wireless monitor. The risk to the patient varies depending on whether he or she is on a transport accompanied by a nurse, accompanied by an orderly, or is left unattended in a hallway, as can be the case in an emergency room (ER) overflow situation.

When a manufacturer submits a product to the U.S. Food and Drug Administration (FDA), one of the key statements is the “intended use,” which guides the regulatory review. Manufacturers can limit the intended use based on their risk analysis, which may signal that some scenarios present undue risk to the patient. They may decide, for example, that one of the above scenarios is too risky and may provide a warning. The hospital should pay attention to the manufacturer’s statement of intended use, as well as all “instructions for use” (IFU) warnings to assure the medical device or system is not being used in a way the manufacturer did not intend or consider.

When a hospital integrates a medical device or system within its infrastructure, even if the hospital is adhering to the intended use, there is an additional burden on the hospital to assure that controls are in place to maintain an acceptable level of risk to the patient. We have arrived at this point as a result of technology changes occurring gradually over the past four decades.
40 Years of Networking
In the 1970s, patient monitors were “networked” together using analog signals. Cable harnesses were run from patient monitors to central stations with each signal requiring its own wire. In the 1980s, we started to see the adoption of serial communication, such as variations of synchronous data link control/high-level datal link control (SDLC/HDLC) or proprietary protocols. In the 1990s, we saw the start of the transition to Ethernet, though at the time other competing technologies such as Token Ring needed to be considered. At the time, the bandwidth (10 mbit/second) which was shared among all devices and the nondeterministic nature of Ethernet kept many medical device engineers up at night. The installation of the first digital picture archiving and communication systems (PACS) required considerable bandwidth modeling and prestaging of images to get appropriate performance. This evolution mirrored changes in the general world of information technology (IT) as small stand-alone departmental systems were connected in unified enterprise infrastructures as the technology matured.

As we moved into the 21st century, wired infrastructure matured to the extent that hospitals started to think about merging patient monitoring and other medical device networks with their wired infrastructure. Networking technology had reached the point that each device could get a dedicated 10/100 Mbit/second connection, which was more than enough to meet the bandwidth requirements.

Wireless also brings with it other issues, such as interference, security, and an inherent lower level of reliability than wired networks.

What Does Wireless Have to Do with It?
Just when we thought we were safe, wireless technology such as Wi-Fi was introduced and has become wildly popular. Unfortunately, wireless brings back some of the technical challenges of the past with devices needing to share limited available bandwidth (typically ~20 mbit/sec). This may be fine for a stand-alone single use, such as a patient monitoring network, but since the radio frequency (RF) spectrum must be shared, there are many other uses and users clamoring for the same limited resource. Wireless also brings with it other issues, such as interference, security, and an inherent lower level of reliability than wired networks.

This situation has, at times, impacted the performance of wireless medical devices. In addition, the performance and capabilities of a wireless infrastructure differs considerably from one infrastructure vendor to the next. As a result, something that may work with Vendor A may not work with Vendor B or may not work as well, potentially negatively affecting the performance and resulting in unintended consequences.

Genesis of ANSI/AAMI/IEC 80001
In 2008, The Joint Commission issued a Sentinel Event Alert, which stated, “As health information technology (HIT) and ‘converging technologies’—interrelationships between medical devices and HIT—are increasingly adopted by healthcare organizations, users must be mindful of the safety risks and preventable adverse events that these implementations can create or perpetuate.”

In response, the FDA, manufacturers, and healthcare delivery organizations (HDOs) convened to work on this issue through a joint effort of ISO TC215 and IEC 62A, which created Joint Working Group 7 (JWG7). Over the course of five years, the group created the initial ANSI/AAMI/IEC 80001-1 standard as well as a number of technical reports that provide additional guidance on special topics, including wireless networking and security.

The primary goal of the ISO/IEC 80001 series of standards is to assure that the safety, effectiveness, and data and system security of networked medical devices is not degraded in the context of the intended use of the device as determined by the “responsible organization” that is deploying the medical devices (e.g., hospital).

Basics of Risk Assessment
Built on the same risk-management model that medical device manufacturers use during
What can go wrong? What are the possible unintended consequences that could result? And are they significant enough that risk controls need to be designed and implemented to ensure an acceptable level of safety?

<table>
<thead>
<tr>
<th>Improbable</th>
<th>Very unlikely that use will result in any Unintended Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote</td>
<td>Not likely to result in any Unintended Consequence</td>
</tr>
<tr>
<td>Occasional</td>
<td>Somewhat likely to result in any Unintended Consequence</td>
</tr>
<tr>
<td>Probable</td>
<td>Very likely to result in any Unintended Consequence</td>
</tr>
<tr>
<td>Frequent</td>
<td>Unintended Consequences occur frequently or occur every time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scale</th>
<th>Safety</th>
<th>Effectiveness</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Severe injury, death</td>
<td>Planned operation is no longer possible</td>
<td>May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of information or services.</td>
</tr>
<tr>
<td>High</td>
<td>permanent impairment of body function or permanent damage of a body structure</td>
<td>Planned operation is disrupted or delayed</td>
<td>May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of information or services.</td>
</tr>
<tr>
<td>Medium</td>
<td>Temporary and minor injury, medical intervention required</td>
<td>Inconveniencing to disrupted effect on operation</td>
<td>Will result in some tangible consequence, albeit negligible and perhaps only noted by a few individuals or agencies. May cause embarrassment. Will require some expenditure of resources to repair.</td>
</tr>
<tr>
<td>Low</td>
<td>Temporary discomfort, reversible without medical intervention</td>
<td>Very limited or inconveniencing effect on operation</td>
<td>Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.</td>
</tr>
<tr>
<td>Negligible</td>
<td>Minor and short term discomfort</td>
<td>No or very limited impact on operation</td>
<td>Will have no impact if threat is realized and exploits vulnerability.</td>
</tr>
</tbody>
</table>

Table 1. Risk Probability and Severity Assessment Scales

*In the case of medical device manufacturers, the focus is on performing risk management during the development of a product in pursuit of regulatory approval to place it on the market; whereas, the risk management performed by hospitals is focused on what happens after the “sale” when networked technologies must operate safety, effectively, and securely as a convergent multi-vendor system-of-systems.

†For example, a patient monitoring network the entire network is considered a regulated medical device in and of its own right and is developed and managed by the manufacturer. See 80001-1:2010, Table C.1 - IT-NETWORK scenarios that can be encountered in a clinical environment.
hazard, during which a cable may be unintentionally disconnected in a patch panel that may result in a delay or non-provision of care. Depending on the specific patient condition, the therapy being provided along with related monitoring, the resulting harm could range from negligible to catastrophic. Depending on the processes and policies enacted around work involving patch panels, the probability may range from improbable to frequent.

Two tables provide examples of tools that are often used to guide the risk analysis process (steps 1 – 4 above). In Table 1, two scales are provided to help determine the probability and severity of a given harm resulting from a hazardous situation. These are used in steps 3 and 4, respectively.

Once the severity and probability have been estimated, a table similar to Table 2 could help determine whether the identified harm is severe enough to warrant the design and deployment of risk-control measures, whether additional analysis needs to be performed to determine more precisely the nature of the risk, or whether the hazardous situation represents a significant threat to patient safety, system effectiveness, or data and system security.

The relationship between the risk assessment concepts is summarized in Figure 1, along with the standardized definitions of each key term. Note that it all begins with a complete understanding of the potential hazards and hazardous situations that may occur. A “starter set” of these hazards is included in the 8001 guidance documents included in the reference list; however, as required in the IEC 80001-1:2010 standard, technology providers—both medical device manufacturers and information technology suppliers—are required to identify those

---

**Table 2.** Risk Acceptability Matrix

<table>
<thead>
<tr>
<th>Unintended Consequence for Security: Effectiveness and Data and System Security</th>
<th>Increasing Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Improbable</td>
</tr>
<tr>
<td>Increasing Severity</td>
<td></td>
</tr>
<tr>
<td>Catastrophic</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Negligible</td>
<td></td>
</tr>
</tbody>
</table>

Low Risk is acceptable. Risk has little effect on goals, no additional control measures required.

Moderate Risk acceptability needs further consideration. Risk has some effect on goals but can be accepted when balanced with benefit. RO must pre-define policies in Risk Management Plan for risks in this level. Policies can include special team reviews (IT, clinical) or review boards, rationales, top management signoff, showing risk has been reduced as low as practicable, etc.

High Risk to goals is unacceptable, risk must be reduced before Medical IT network can be used, either by reducing likelihood or by reducing severity.

§Note these are only examples; different variations of these may be created to address changes in care contexts, technologies being managed, etc., and may be updated as experience is gained performing risk assessment activities.

¶IEC 80001-2-1:2012, Section 2.1 provides a discussion of the differences between hazards and hazardous situations.
hazards that must be considered when performing these risk assessment activities.

Risk assessment is just the start. Once it is completed and there is a determination that use of a technology poses significant risks, the focus switches to risk control or mitigation and a final determination as to whether the technology is safe and clinically effective enough to outweigh the risks associated with its use. Details about risk-management activities subsequent to risk assessment are provided in the standards and articles identified in the reference list.

Starting an 80001-based risk-management program—even the initial risk-assessment activities—has posed a significant challenge to healthcare providers.

Starting a Risk-Assessment Program
Starting an 8001-based risk-management program—even the initial risk-assessment activities—has posed a significant challenge to healthcare providers. Some have characterized it as an “unfunded mandate” and even suggested that until the FDA or accreditation organizations require it—or worse, until there is a high-profile catastrophe that could have been averted by risk management—there will be little interest in investing in such a program.

In the meantime, networked technology becomes increasingly interwoven with care delivery on a daily basis, and as a result, the potential for disastrous unintended consequences grows. Short of enacting a comprehensive enterprise-wide program, smaller more manageable projects should be selected to which risk management may be applied. Once these projects are completed, the results may be evaluated, improved, and applied to successive projects, incrementally building a core competency in risk management.

One approach for such a project is illustrated in Figure 2. Data is collected on present capabilities and technology needs of the organization, followed by a determination of readiness to begin the risk management process, both in terms of the needed information to drive the activities as well as competencies and capabilities (e.g., trained personnel, assessment models, and policies).

When the needed information is in place, a risk assessment may be performed to determine the organization’s technology vulnerability. This will result in an action plan to both control the identified risks and determine how best to improve the organization’s overall maturity in managing its networked technology—establishing benchmarks early on that may be used later to determine progress.

The important point is to get started and not wait until all the conditions are perfect.

In the meantime, the ISO/IEC JWG7 is not resting on its laurels, but is pushing ahead developing guidance on “responsibility agreements” (between technology suppliers and users to lay the foundation for multi-stakeholder collaboration for medical network risk management), risk management of distributed alarm systems, and an 8001 self-assessment model, providing detailed guidance on how to perform readiness assessments, with more in the pipeline.

In an increasingly connected healthcare environment, risk assessment as part of an overall technology management program is emerging as a mission-critical component for all hospitals. The resources and tools are in place today to get started in this important area. Do not let your patients and your ability to provide quality care fall victim to conse-
quences that could have been avoided if someone had made the effort to perform the analysis and take appropriate action.

References


