SUMMARY: AAMI PROPOSAL FOR DEVELOPMENT OF A RISK MANAGEMENT PROCESS STANDARD(S) FOR PATIENT SAFETY WITH HEALTH IT

December 2014

Introduction: AAMI is proposing the development of U.S.-centric risk management process standards for health IT, with particular emphasis and patient safety focus on clinical software systems. This summary provides context for this proposal.

Background: The use of HIT can lead to patient harm. While many aspects of HIT present a very low risk of harm, certain use scenarios in specific situations or contexts are high risk. HIT use is dependent on the quality of the underlying software as well as on its user interface (UI). ONC has promulgated "safety enhanced design" of HIT through the use of user-centered design (UCD). However, UCD is insufficient alone to assure HIT safety. Another critical component of designing for safety is the implementation of a robust auditable risk management process.

There are numerous long-standing examples of national and international standards guiding the conduct of risk management across many industries (e.g., ISO 31000, ISO 62304, IEC 27001 and NIST SP 800-30). Notably, a robust suite of international *risk management process* standards (the AAMI/ANSI/IEC 80001 series) already exists for connecting IT networks to medical devices in healthcare delivery. This work began because increasing numbers of medical devices were being designed to exchange information electronically with other technology in the heath IT ecosystem through networks that also transfer other patient data.

The international working group (administered by AAMI) that developed this suite of 80001 risk management standards recognized a number of risk management issues that needed to be addressed because of the greater complexity introduced into healthcare when connecting IT networks to medical devices, such as:

a. Inadequate consideration of the risk of use of IT networks;
b. Inadequate support from manufacturers of medical devices for the incorporation of their products into IT networks; incorrect operation or degraded performance due to combinations of medical devices and other equipment on the same IT network;
c. Incorrect operation resulting from combining medical device software and other software applications in the same IT network; and,
d. The conflict between the need for strict change control for medical devices with the need for rapid response to threats of cyber-attack.

Association for the Advancement of Medical Instrumentation
4301 N. Fairfax Drive Suite 301
Arlington, VA 22203-1633
T +1-703-525-4890 F +1-703-276-0793
www.aami.org

The first issues addressed by the 80001 suite of risk management standards were the roles, responsibilities, and activities necessary for effective risk management. Subsequent parts of the series focused on step-by-step implementation, security capabilities, and considerations for wireless networks, alarm management, responsibility agreements, and healthcare delivery organization (HDO) self-assessment.[1] Two digestible articles about the application of the 80001 suite of standards are attached to this summary as Exhibits B and C. They are included here solely to provide additional context about the value and use of the 80001 series. For those who want to review the 80001 series in details, the standards are available at: http://my.aami.org/store/SearchResults.aspx?searchterm=80001&searchoption=ALL

Risk Management Process Standard(s) for Health IT: Health IT has continued to progress rapidly since the adoption of Meaningful Use for HIT technology, and the leaders of the 80001 standards work realized that risk management process standards are greatly needed for health IT and related clinical software systems because of the even greater patient safety risks that have been introduced into healthcare with the proliferation, dispersed accountability, variety, and complexity of health IT. In September 2014, these leaders disseminated a draft roadmap, entitled "Health Software and Health IT Safety Standards, Future State Architecture, Framework and Roadmap." That framework is attached to this summary as Exhibit D. Most importantly, the figure on Page 5 that exhibit is a potential visual roadmap for the development of standards that address patient safety risk across the full life cycle of health IT use – from design and development, to implementation, use, upgrades and obsolescence.

Just as during the initial development of the 80001 series, it is clear now that the first area that must be addressed in a suite of risk management process standards for health IT is roles and responsibilities. As illustrated in the figure on Page 5 of the draft roadmap, there are many players and activities with different roles and responsibilities across the full life cycle of health IT: Standardization of the roles and responsibilities for the HIT risk management processes will serve the needs of both vendors and HDOs[2]. Again, standardization of roles and responsibilities would be only of the many aspects of a full life cycle risk management process to be addressed.

The standards work envisioned in the draft roadmap is proposed to be within ISO Technical Committee 215, Health informatics, which is managed by the American Health Information Management Association (AHIMA). Much of the standards development will be done by a joint working group under ISO/TC 215 and IEC that is administered by AAMI.

For the development of the U.S.-centric risk management process standard (or suite of standards), AAMI proposes that a new national committee be formed with membership

[1] See Exhibit A for a full list of the parts of the AAMI/ANSI/IEC 80001 series of standards

[2] A robust risk management process entails much more than roles and responsibilities, and this example is used only to illustrate that similar work has already been done in the 80001 series.

comprised of vendors, providers, and other experts in the health IT space who have a stake in standard(s) that will be established.

U.S. Centric, Consensus-Based Approach: AAMI proposes that this work start in the U.S. with North American vendors and providers, because that is where the urgent need exists and where the biggest stakeholders are located. Ultimately, work efforts should migrate to align with the international standards development work in both ISO and IEC, but not until it is clear that the U.S.-based work is far enough along to be ready for a more international approach and focus. AAMI has taken this approach successfully in the past with other standards.

AAMI strongly agrees with the federal government's support for private, consensus-based standards development as an alternative to government regulation when a private solution can achieve government aims.[3] AAMI believes that it is ideally suited to convene this new American consensus-based standards committee because AAMI:

a. Has deep expertise in developing standards related to healthcare technology, including risk management, human factors and quality systems;
b. Is a neutral organization with no "agenda" on any aspect of HIT other than supporting the entire healthcare community to advance patient safety;
c. Is an ANSI-accredited consensus-based standards development organization; and,
d. Has a long and successful track record of convening multi-disciplinary stakeholders to work together to solve complex, seemingly intractable problems that cannot be successfully solved by any single stakeholder group.

Getting Stakeholder Engagement: AAMI is a non-profit organization and our funding model for standards development requires that industry fund the development of standards through either membership in AAMI or payment of a corporate participation fee. Clinicians and other staff of HDOs are not expected to fund participation. Government entities are welcome to participate and pay a much more modest membership fee. While AAMI is proposing to shepherd the development of a risk management standard for health IT, the process will only be successful if the major HIT vendors, knowledgeable providers, and other relevant stakeholders are willing participants in the process. This means that they need to see the need for and value of participation (particularly the vendors). Because AAMI is a neutral organization and does not participate in advocacy activities, it is not positioned to "persuade" vendors, providers, or HDOs of this need. Thus, to be successful, ONC and other governmental and HIT leaders will need to articulate the importance of, and advocate for, this process.

[3] Office of Management and Budget (OMB) Circular A-119 "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities" (1998), which has been updated in 2014 and the updated final draft can be accessed here: http://www.whitehouse.gov/sites/default/files/omb/inforeg/revisions-to-a-119-for-public-comments.pdf. Note in particular on page 20 of the updated final draft: "*In accordance with section 12(d) of the NTTAA (found as a "note" to 15 U.S.C. § 272), all Federal agencies must use existing voluntary consensus standards in lieu of agencies' developing and using their own or other standards in their procurement, regulatory, or other agency activities, except when use of an existing voluntary consensus standard would be inconsistent with law or otherwise impractical.*"

Contact Information:

Mary Logan, AAMI President & CEO (mlogan@aami.org)

Carol Herman, AAMI Senior Vice-President, Standards Policies and Programs (cherman@aami.org)

Primary Contact: Joe Lewelling, AAMI Vice-President, Standards Policy and Programs (jlewelling@aami.org)

EXHIBIT A

80001 Standards (AAMI/ANSI/ISO/IEC)

- IEC 80001-1:2010
  Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities (published)

- IEC/TIR 80001-2-1:2012
  Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples (published)

- IEC/TIR 80001-2-2:2012
  Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the communication of medical device security needs, risks and controls (published)

- IEC/TIR 80001-2-3:2012
  Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks (published)

- IEC/TIR 80001-2-4:2012
  Application of risk management for IT-networks incorporating medical devices – Part 2-4: General implementation guidance for Healthcare Delivery Organizations (published)

- IEC/TIR 80001-2-5
  Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance – Guidance for distributed alarm systems (in press)

- ISO/TIR 80001-2-6,
  Application of risk management for IT-networks incorporating medical devices – Part 2-6: Application guidance – Guidance for responsibility agreements (published)

- ISO/TIR 80001-2-7
  Application of risk management for IT-networks incorporating medical devices – Part 2-7: Application guidance – Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1 (in press)

- IEC/DTIR 80001-2-8
  Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2 (in development)

- IEC/NP TIR 80001-2-9
  Application of risk management for IT-networks incorporating medical devices – Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2security capabilities (proposed)

Using 80001 to Manage Medical Devices on the IT Network

Stephen L. Grimes

Healthcare technology today is considerably different than it was 20 to 40 years ago. Yet, much of what is done by healthcare technology managers in support of medical technology has not changed. The tools and procedures still used by most clinical engineering services have evolved little to address some of the unique challenges posed by new healthcare technologies that are at once more pervasive, more complex and more susceptible to failures that may have catastrophic consequences for patients and healthcare operations.

Just how has the healthcare technology landscape changed?

Exponential Growth

There is ample evidence of the exponential growth in healthcare technologies in recent years. One of the largest healthcare providers in the United States, Kaiser Permanente, claims that between 1997 and 2007, their spending on health technologies and related procedures increased 9.3 fold![1] There is also evidence that this growth trend will only continue rapidly upward in spite of today's tough economic climate. In a recent survey conducted by Boston-based L.E.K. Consulting of 200 hospital executives, 60% of those surveyed told researchers that they expect to spend more on medical devices in 2011, up from only 38% who saw spending increases a year ago.[2] These increases are driven by the industry's recognition that healthcare technology plays a critical role in enabling the delivery of quality, safe and effective care. It was the Institute of Medicine's seminal report of 2000, "To Err is Human," that claimed what most of us have come to accept today, that "technology ... has to be recognized as a 'member' of the work team." We have come to heavily depend on this "member" of the team and our ability to deliver care can be severely compromised when that team member is not ready and available.

Increased Diversity, Complexity, and Connectivity

From advances in computerization, networking (wired & wireless), imaging, robotics, micro/nano technologies, genomics and telemedicine, healthcare technologies have significantly evolved in complexity and diversity and will only continue to do so at ever increasing rates. A 2009 Networking and Information Technology Research and Development (NITRD) Program report describes how "older generations of mechanical, analog and electromechanical devices ...

The tools and procedures still used by most clinical engineering services have evolved little to address some of the unique challenges posed by new healthcare technologies that are at once more pervasive, more complex and more susceptible to failures that may have catastrophic consequences for patients and healthcare operations.

About the Author

Stephen L. Grimes is chief technology officer of Linc Health and a member of the IEC joint working group that developed IEC 80001. E-mail: Stephen.Grimes@LincHealth.com.

About the 80001 Standard

ANSI/AAMI/IEC 80001, *Application of risk management for IT networks incorporating medical devices—Part 1: Roles, responsibilities and activities* was adopted as an American National Standard in October 2010. It offers a process for how healthcare organizations can manage risk and consider potential impacts on patient safety in an environment where more medical devices are being attached to IT networks.

To order IEC 80001-1, call (877) 249-8226 or visit the AAMI Marketplace at http://marketplace.aami.org. List price $100, AAMI member price $50. Order code 8000101 or 8000101-PDF, source code PB.

have been largely replaced by devices and systems based on information technologies" and how these devices/systems are "often connected to other devices in increasingly complex configurations, potentially creating systems of systems that span scales from tiny ... to ultralarge."[3] Formerly passive technologies have largely been replaced by new systems of systems (SoS) that actively control critical physiological processes and functions. A 2010 survey conducted by the College of Healthcare Information Management Executives (CHIME) concluded that 23% of medical devices in their inventory were networked; an additional 8% were network-capable but not yet connected.[4]

Risk Management And the 80001 Standards

Changes associated with major increases in technology proliferation, diversity, complexity, and connectivity represent a major challenge and require a new mindset by those who are responsible for supporting these technologies. Perhaps foremost among the requisite mindset and skills necessary to address these new challenges is our adoption of and our approach to risk management. There is little evidence to indicate risk management is currently applied in little more than a narrow or superficial manner. Effective risk management is key to identifying substantive risks and applying available resources in a manner that most effectively addresses those risks. Absent effective risk management, resources are not applied where they are most needed and new vulnerabilities introduced by new technologies go unaddressed, often with dire consequences.

Our limitations in successfully managing the support of these new technologies is evidenced by that fact that, since the year 2000, there have been a growing number of reports by individuals and organizations of major medical system failures. Around 2004, Brian Fitzgerald of the U.S. Food and Drug Administration (FDA) had begun taking note of these reports. In December of 2005, he convened a meeting at FDA headquarters with experts from medical device manufacturers, healthcare providers (clinical engineering), and other relevant parties to discuss how to deal with the increasing number of complex systems and the new vulnerabilities they introduced.

That meeting concluded that while manufacturers had guidelines for effectively addressing risks associated with the development and manufacture of medical devices/systems (e.g., ISO/IEC 14971[5]), there were no comparable, adequate guidelines that healthcare providers could employ to ensure the medical devices/systems they deployed were being appropriately

Update on 80001 Technical Reports

Four technical reports (TRs) have been completed to date and are currently going through the review and approval process:

- IEC TR 80001-2-1 Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step by step risk management of medical IT-networks; Practical applications and examples
- IEC TR 80001-2-2 Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the communication of medical device security needs, risks and controls
- IEC TR 80001-2-3 Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks
- IEC TR 80001-2-4 Application of risk management for IT-networks incorporating medical devices – Part 2-4: General implementation guidance for healthcare delivery organizations

In addition, there are several TRs in preliminary stages of work. Titles are not firm yet, but the topics are:

- Guidance for responsibility agreements
- Guidance on how IEC 80001-1 and ISO/IEC 20000-2:2005, Information technology – Service management – Part 2: Code of practice, could be used together
- Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1
- Technical report on integration of alarm systems in the healthcare environment

supported. The outcome of the meeting was the establishment of a new workgroup under the auspices of the ISO/IEC. This workgroup was to include representatives from the world community of medical device manufacturers, healthcare providers, and standards development organizations who would develop guidelines for healthcare providers on how to best manage risks associated with the rapidly growing number of critical systems they were deploying.

U.S. and international experts (including medical device manufacturers, government and regulatory authorities, and clinical and information technology specialists from the healthcare provider community) met regularly over the next four years to develop a practical, high-level guideline that could be adopted by healthcare delivery organizations (HDOs) and that would be scalable to any size organization. In the summer of 2010, the final draft of ANSI/AAMI/IEC 80001-1:2010 *Application of risk management to information technology (IT) networks incorporating medical devices*[6] was formally approved and the final document was released in October 2010 as an international standard.

The lack of updated tools and procedures—and an appropriate organizational framework in which to apply them—has been a major limiting factor in healthcare technology managers' ability to effectively address the reality of today's healthcare technology. With the adoption of 80001, these managers now have an important guideline from which to begin building those tools and procedures. These managers will also find that 80001 integrates well with one of the few other tools developed in recent years to address medical device security issues—namely, the Manufacturer's Disclosure Statement for Medical Device Security[7] (generally referred to as the MDS2). The MDS2 (which is currently being updated to more closely link to 80001) is a NEMA standard intended to provide medical device manufacturers with a standard means and format for communicating information about a medical device's security features with healthcare providers in order for those providers to effectively manage security related risks associated with that device. The original MDS[2] gained broad acceptance from both manufacturers and providers and it is likely the new version tailored to address 80001's security elements will also.

With the adoption of 80001, these managers now have an important guideline from which to begin building those tools and procedures.

Practical Advice on Implementing 80001

The three articles that follow describe the work of several technical committees that were involved in the development of 80001 under IEC Subcommittee 62A Joint Working Group 7. These articles describe the first set of guidance documents or technical reports (TR) under development and soon to be released. These documents are intended to provide additional assistance to organizations attempting to do an effective implementation of 80001:

- Nick Mankovich and Brian Fitzgerald's article "Managing Security Risks with 80001" addresses issues associated with data security in networked medical devices and the kinds of processes appropriate for ensuring the integrity, availability and confidentiality of that device data. Ensuring data security will be critical and a substantial element in the future of all effective healthcare technology management services.
- Mike Papa's article "Responsibility Agreements Ensure Accountability Under 80001" explains the rationale and key steps in implementing responsibility agreements. Responsibility agreements ensure the systematic identification of all stakeholders and the clear delineation of all responsibilities—a key aspect of any successful risk mitigation.
- Karen Delvecchio's article "Step-by-Step Risk Management for Medical IT Networks" details how one technical report will provide HDOs with fundamentals of the risk management process and an overview of how these fundamentals should be applied. This article, and the technical report of which it is the subject, are particularly important because they describe processes which are critical to managing new complex technologies but with which most HDOs previously have had little exposure.

Note that these articles are written by members of the core team involved in developing 80001 and represent their views on how

To Get Involved

To get involved in the work of the committee developing the 80001 documents, contact Sherman Eagles at Sherman@80001Experts.com or Todd Cooper at Todd@80001Experts.com.

best to implement various aspects of the standard. There are likely to be some changes prior to final release of the Technical Reports and additional interpretations.

Conclusion

80001 and the technical reports described in the articles in this section represent a new approach specifically designed to prepare healthcare technology managers, clinical systems engineers and other stakeholders to effectively support today's increasingly critical and complex technologies. Their help comes none too soon and will be instrumental in preparing us for the challenge. ■

References

1. **Halvorson G.** Health Care Will Not Reform Itself. CRC Press, 2009.
2. **L.E.K. Consulting.** Healthcare Reform Shifts Hospital Priorities, Creates New Opportunities for Medtech Companies. *Executive Insights* 8(4), 2011.
3. **NITRD.** High-Confidence Medical Devices: Cyber-Physical Systems for 21st Century Care. Report by the Networking and Information Technology Research and Development (NITRD), High Confidence Software and Systems Coordinating Group, February 2009.
4. **Symantec.** Networked Medical Devices: Security and Privacy Threats. Symantec White Paper, 2011.
5. **ISO 14971:2007.** *Medical devices—Application of risk management to medical devices.*
6. **IEC 80001-1:2010.** *Application of risk management for IT-networks incorporating medical devices—Part 1: Roles, responsibilities and activities.*
7. **MDS2.** Manufacturer's Disclosure Statement for Medical Device Security. Developed by Medical Device Security Workgroup of the Healthcare Information and Management Systems Society (HIMSS), subsequently adopted by the National Electrical Manufacturers Association (NEMA). Available at www.himss.org/ASP/topics_FocusDynamic.asp?faid=99 (accessed July 26, 2010).

Step-by-Step Risk Management for Medical IT Networks

Karen Delvecchio

Hospital network infrastructures can carry critical and sensitive data and therefore become a significant subsystem in a complex interaction of sophisticated systems. In the last decade, healthcare technologies have become increasingly interconnected and codependent. IT networks supporting medical devices that have historically been segregated are now more likely to be combined into one enterprise IT network. This convergence facilitates more capable and connected systems that can drive better care by enabling efficient clinical decision making throughout the hospital, while allowing healthcare delivery organizations (HDOs, such as hospitals) to optimize and leverage a common IT infrastructure. But with all these benefits come new risks that need to be managed. A network's role in the delivery of care warrants deliberate and purposeful risk management.

In October 2010, the IEC released a new standard titled IEC 80001-1: *Application of risk management for IT-networks incorporating medical devices* (hereafter called 80001). The goal of 80001 is to manage the risk that comes along with using technology for the benefit of the patient, allowing us to realize the upside of medical IT networks (IT networks in healthcare facilities that incorporate medical devices) while ensuring that any potential risks are controlled and minimized. The standard defines a framework for applying a risk management process to the incorporation of medical devices into shared enterprise IT networks.

80001 Overview

80001 defines a medical IT network as any IT network in which at least one of the nodes is a medical device as classified by regulation. It clearly defines positions, functions, activities, policies, procedures, and documentation needed to manage risk during incorporation of medical devices into IT networks. It also requires a comprehensive risk management policy to be put in place to protect three key properties: safety, effectiveness, and data and system security. The standard is addressed to three audiences:

1. The hospital, or HDO, is responsible for owning and managing the overall risk management of its medical IT networks. This entity is referred to as the Responsible Organization (RO) in the standard
2. The medical device manufacturer (MDM) supports the process by providing information about the medical devices that will allow them to be successfully connected to the network, and also information that will support the hospital's system-wide risk management of the network
3. Other providers of IT equipment or services that may not be a medical device also provide technical information to support medical device incorporation and risk management

Figure 1 shows how these audiences are all involved in risk management of medical IT networks. The standard does not address segregated networks dedicated to one single MDM, either built by or as specified by the

About the Author

Karen Delvecchio is a lead systems engineer for patient monitoring networks for GE Healthcare developing network infrastructure and networked-client capabilities with emphasis on risk management. E-mail: Karen.Delvecchio@med.ge.com.

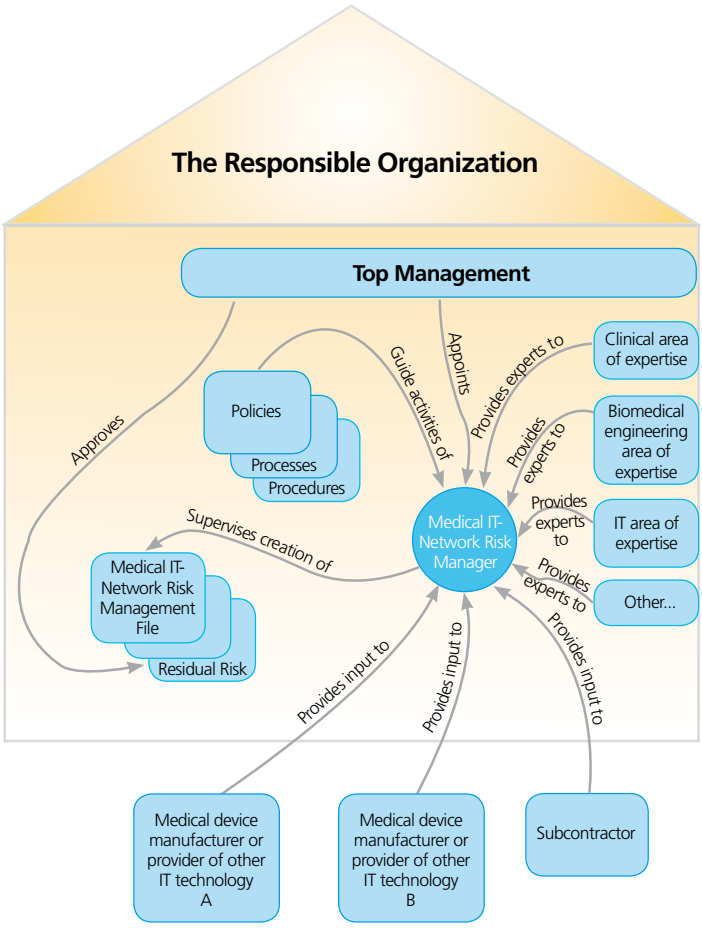


Figure 1. The "house of 80001" as depicted in the standard. Many sources of information and many interested parties, both internal and external to the Responsible Organization, are necessary to execute meaningful risk management for medical IT networks.

manufacturer. These are considered part of the medical device delivered by the manufacturer. Also out of scope is any premarket risk management of medical devices.

Because there are many different organizations and departments—both within and outside the hospital—that are required to engage to support successful risk management, an international standard is considered the best way to organize and maintain this effort.

The requirements set forth in 80001 generally fall into one of these four topics:

1. Roles and responsibilities – who are the different players and what do they do?
2. The risk assessment process itself – an organized way to analyze and evaluate risk
3. How the risk management process fits into the lifecycle of the medical IT network
4. Documentation of all of the above

The risk assessment process itself (Figure 2) is the subject of an IEC technical report scheduled for publication in late 2011 titled 80001-2-1 *Application of risk management for IT-networks incorporating medical devices: Step-by-step risk management of medical-IT networks; Practical applications and examples* (hereafter called Technical Report 2-1).

Step-by-Step Risk Management

Risk management is a topic rich in theory and has been a source of many intellectual and philosophical debates and discussions. But eventually the time comes to put the right players in a room, put the fingers to the keyboard, apply the procedures, and decide as an organization whether you believe your system is safe enough to be applied to patients. Risk is another language and must be adopted consistently by every member of the risk management team. This language is used to bridge the gap between the native languages spoken by these team members, be it clinical, technological, business, or security. Once the players are assembled and the language is understood, the group must proceed through logical steps to facilitate what is ultimately a hypothetical exercise.

Technical Report 2-1 will provide further explanation of the actual performance of the risk assessment, which is only one section of the 80001 standard. Note that many other requirements specified in 80001 must be met before proceeding with the risk assessment: allocating resources, establishing risk management policies and procedures, defining probability, severity, and acceptability scales (HDO); supplying required network characteristics and relevant hazardous situations (MDM); and supplying network design information, etc, of the network infrastructure components (other providers of IT). Beyond the requirements specified in the standard, the parties may choose to develop responsibility agreements to specify further detail. (For more on responsibility agreements, see the article on page 33).

Fundamental Risk Analysis

The risk management process called out in 80001 is based on a well-established method for risk assessment. Assessment involves three main activities:

- Analyze – identify hazards and estimate risk
- Evaluate – determine acceptability
- Control – implementing designs or procedures that lower risk

As shown in Figure 2, these activities are executed in an iterative fashion until the evaluation determines that the risk level is acceptable.

Risk is another language and must be adopted consistently by every member of the risk management team. This language is used to bridge the gap between the native languages spoken by these team members, be it clinical, technological, business, or security.

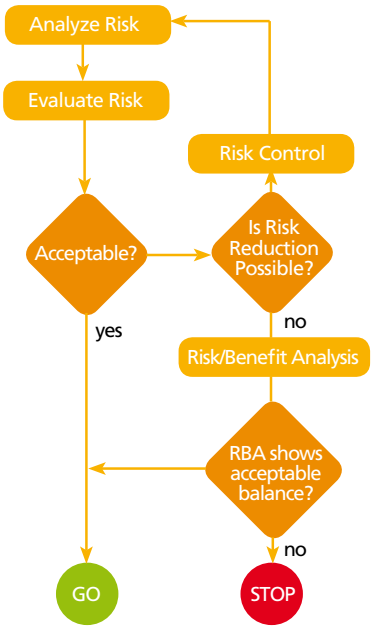


Figure 2. During risk assessment, the steps of analyze, evaluate, and control are executed iteratively until the risk level is determined to be acceptable.

To fully analyze risk of a system, one needs to clearly define the system under analysis. This involves two aspects:

1. The technical design, details, and scope of the network under analysis
2. The context in which the system is used. Context includes information such as patient acuity, clinical workflows, existing IT or biomedical procedures, and anything that would aid in the estimation of risk.

Risk is a combination of probability and severity. In other words, something that is likely to happen frequently with minor consequences can be just as undesirable as something that is very unlikely to happen, but has very severe consequences. For purposes of risk assessment, we consider risk somewhat quantifiable, at least in terms of a level of risk. This level is weighed against the benefit of placing the system in to use, and a determination is made as to whether the benefits outweigh the risk. This determination happens in the evaluation step. Typically, risk levels below a certain level are considered acceptable and risk levels above a certain level are considered unacceptable, regardless of the benefit. For the grey area in between, it is more important to weigh the benefits against the risk in order to complete evaluation.

Terminology

During the risk assessment meetings and discussions, several people representing different skill sets and interests will speculate on what could go wrong, who or what might be negatively affected if it did, how likely this is to happen, and how severe the consequences could be. These are certainly difficult discussions, but they are nearly impossible if the group does not first have a common language to use. Note that one chain of events in a medical IT network can start with something very technical deep inside the network, and end in something clinical at the bedside or point of care.

The critical terms used in Technical Report 2-1 are hazard, hazardous situation, sequence of events (or cause), and unintended consequence (UC). Figure 3 shows these terms and how they are related to each other. Hazards are categories of things that could be detrimental to one or more of the key properties. Examples are electrical energy, equipment suspended from the ceiling or wall, and, in the case of medical IT networks, loss or degradation of function. A hazardous situation is a circumstance in which a person or the organization is exposed to the hazard. A disconnected Ethernet cable (loss of function) is benign until the time when critical traffic needed to make a time-sensitive care decision is lost due to that failure. A cause, also called a foreseeable sequence of events, creates the hazard if it was not already inherent to the system (the disconnection of the Ethernet cable leads to loss of function) or creates the hazardous situation (a broken fixture results in a falling suspended mass). Given the occurrence of a hazardous situation, one can predict possible unintended consequences that may result. Unintended consequence is a more

During the risk assessment meetings and discussions, several people representing different skill sets and interests will speculate on what could go wrong, who or what might be negatively affected if it did, how likely this is to happen, and how severe the consequences could be.

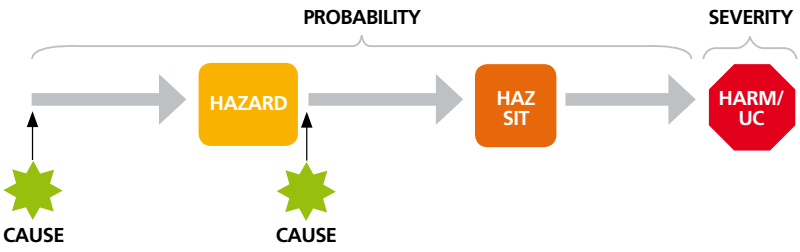


Figure 3. It is very important for a risk assessment team to understand and consistently use risk terminology.

general term for 'Harm' which is used in 80001. In the case of safety, this could be physical injury of varying degrees of severity. Note that even when a hazardous situation occurs, it's not guaranteed that an unintended consequence occurs. For example, an alarm is missed, yet no one is hurt.

The Steps

With the fundamentals of risk assessment established and the terminology agreed upon, we can examine the detailed steps involved in completing the risk assessment of a system, in this case the medical IT network.

Steps 1 and 2 are to identify hazards and causes. Assessing risk involves thinking about all the ways the system under analysis, in this case the medical IT network, can impact the key properties. This thought process can go top-down, in other words, what are the ways this system can be dangerous (hazards), and how could this happen (causes)? Or it can go bottom-up, in other words, what are the things that can break or fail in this system (causes), and how might that expose us to a hazard and become a hazardous situation? There may be multiple causes per hazardous situation and multiple hazardous situations per cause.

While risk must be shared and ultimately controlled by those who own and maintain the network, it is important to ensure that there is appropriate information flow between the hospital, medical device manufacturer, and other IT providers such that a thorough risk analysis can be completed.

Step 3 is to determine possible unintended consequences that may result from each hazardous situation, based on everything the team knows about the system under analysis and the context in which it is used. The team must also assign a severity level to the unintended consequence.

Step 4 is a particularly difficult one. Here the team must estimate the probability of occurrence of the entire chain (error/fault through to unintended consequence).

The estimations in steps 3 and 4 for severity and probability are made using scales that the organization established ahead of time. At this point, the analysis is complete, and risk can be calculated using the values determined in these steps. This calculation follows the organization's pre-established formula showing risk level as a function of severity and probability (typically a matrix).

In **Step 5,** the risk level of these hazardous situations is evaluated for risk acceptability, based on the HDO's pre-defined criteria for acceptability. If it is not acceptable, the HDO can choose to forgo the system or activity that would give rise to this hazardous situation, or the organization can put measures in place to control or lower the risk.

In **Step 6,** risk control measures are identified. Control measures can be network design decisions, other technical methods, or they can be procedural, warnings, etc. They may lower risk in one of several ways: by lowering the probability that the event happens, by lowering the probability that an unintended consequence occurs given the occurrence of the hazardous situation, or by lowering the severity of the unintended consequence.

Steps 7 and 8 are to implement and verify the risk control measures. Implementation involves building the network infrastructure to include the design mitigations identified, label it accordingly, and instantiate procedural mitigations, etc. Then it must be verified (checked) that the mitigations are in fact included in the final system. Verification also includes checking the effectiveness of the mitigation. Execution of this step will vary depending on the type of mitigation. Design mitigations can likely be verified to be effective in a test lab. Procedural or workflow mitigations can be evaluated theoretically, and then monitored in the live phase of the network.

Step 9 is to determine if any new risks arose during the process of mitigating the original list of risks. For example, very strict security measures may have been proposed, but these may lead to a situation in which a clinician cannot access data or functionality from a critical system in an emergency.

And finally, in **Step 10** the overall residual risk is evaluated. Once everything is complete, each hazardous situation identified may have a residual risk associated with it. These should be evaluated in aggregate for overall acceptability.

Relationship of Multiple Risk Analyses

Medical IT networks are complex, highly dynamic super systems of medical devices and IT equipment. While risk must be shared and ultimately controlled by those who own and maintain the network, it is important to ensure that there is appropriate information flow between the hospital, medical device manufacturer, and other IT providers such that a thorough risk analysis can be completed.

Applying risk management at a subsystem level is no small task. Converging multiple subsystem risk analyses is difficult, and the complexity increases significantly at a super-system level, particularly when the systems are delivered by multiple companies and organizations, as is the case with medical IT networks.

Timing of Risk Analyses

While it may be understood that each of the three target audiences for the standard have a part to play in the overall risk management of the final system of systems, it is important to understand how these risk analyses relate to each other, particularly for the MDM and HDO who both execute independent risk analyses. The notion that HDO risk analysis in relation to MDM risk analysis "picks up where the other left off" is a bit of a misnomer. Rather, they are analyzing the same hazards with respect to the medical IT network.

Both the MDM and the RO perform risk analyses, as shown in Figure 4. Each are analyzing the risks associated with incorporating the medical device into an IT network, or the "IN USE" portion of the timeline shown here. MDM activities are shown above the timeline, HDO activities are shown below. The actual topic of both of these risk analyses is the "IN USE" portion.

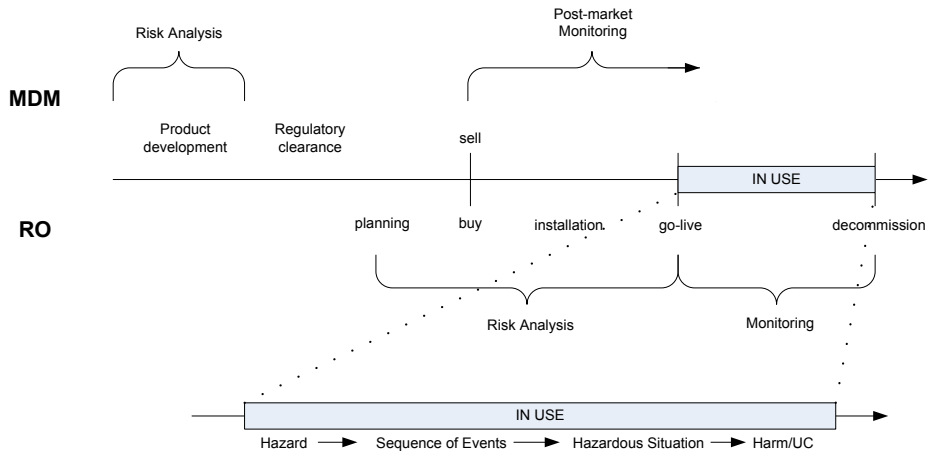


Figure 4. Timeline for Risk Analyses

Medical device manufacturers recursively perform risk analysis during product development, from conception through design and testing. Typically, this is per ISO 14971.[1] This risk analysis encompasses everything that could be hazardous about the device in its intended use or foreseeable misuse. One portion of this includes risks associated with operation of the device on a network.

At the point where the risk analysis shows the overall risk to be at an acceptable level per the MDM's risk policies, the design may proceed to market (after any required regulatory clearance).

Responsible organizations recursively perform their risk analysis during the project intended to incorporate the device into the enterprise network. During this process, information from the MDM is used. First, a list of required characteristics of the network (i.e., what does it need to be/do to support the device connection) is used to ensure that the network can support the device. Secondly, a list of MDM-identified potentially hazardous situations specifically related to incorporation of this device into the network can be used as one source of input during **Steps 1 and 2** (Identification of Hazards and Causes). All of this information is provided so that the HDO can properly estimate and manage risk. For example, the MDM explains how the device will react in the case of a lost connection. It might alarm or somehow notify the user of this condition. The HDO may determine that this situation is detectable and no further risk control is required, or they may choose to add further risk control measures to the network to reduce the possibility of a lost connection. The HDO will also use information from the network equipment or service providers to support the risk assessment, such as mean time between failures data, test strategies, failure modes, best practices, etc.

At the point where the risk analysis shows the overall risk to be at an acceptable level per the HDO's risk policies, the medical IT network may go live.

Content of Risk Analyses

Now consider the actual content and topic of both risk analyses. Both the MDM and the HDO are analyzing the risk of hazardous situations related to the fact that the medical device is functioning on a network once it is live and in use, presumably using the network connectivity for some functionality. Both the MDM and the HDO are identifying hazards and hazardous situations, speculating on possible causes and potential resultant harms or unintended consequences that exist once the medical IT network is in operation. There are three main differences between these two assessment activities:

1. The policies and procedures governing the risk analyses. As there is no single universally accepted way to specify probability, severity, or risk acceptability, these are specific to the organization.
2. What is known about the context of the medical IT network. An MDM may provide a device in many different markets or segments with varying use cases, workflows, and network designs, whereas the HDO can more clearly specify the context of the use of the medical IT network, including specific workflows, procedures, typical user and patient profile, and network availability.

Question	Medical Device Manufacturer	Responsible Organization
When is risk assessment performed?	During product development (pre-market)	During medical IT network project execution (pre-go-live)
What is the subject of risk assessment (relevant to 80001)?	Networked operation of the medical device ('In Use' portion of Figure 4)	
Where can potential mitigations be applied (design, protective measures, labeling)?	Medical device	Network infrastructure
What is treated as a black box during risk assessment with general failure modes?	Network infrastructure	Medical device

Table 1. Simplified summary explanation of timing and content of medical IT network Risk Analyses

Common system-level failure modes that should be considered by the MDM. Causes of these failure modes are considered and mitigated by the HDO.

- **Intermittent connectivity:** intermittent dropped packets without complete connection loss
- **Lost connectivity:** connection completely lost for a sustained period
- **Loss of control:** attacker utilizing network security vulnerability to take control of the system or render the system unusable
- **Corrupted data:** bits flipped or dropped during transport
- **Incorrect or inappropriate timing of data:** The network delay or jitter (i.e., variation of delay) exceeds expected or allowable limits
- **Foreign packets:** unrecognized packet type or failure parsing
- **Excessive packets received:** from broadcast or multicast storm, UDP flooding, denial of service, or any other reason
- **Exposure of Private Data:** how might private data be compromised?

3. Where in the overall system each organization has the power to apply risk control measures, as discussed below. The MDM may apply design and labeling mitigations to the medical device. The HDO may apply design and labeling mitigations to the network itself, or to the procedures and workflows associated with it.

Scope of Risk and Control

As mentioned above, one of the main differences between these two risk assessments is the degree of control over each of the subsystems that make up the entire system under analysis.

As an MDM develops products intended to operate on shared, general-purpose networks such as hospital enterprise IT infrastructures, cellular networks, Internet, etc., the network will have to be treated as a black box having certain system-level failure modes (see sidebar). These should be considered as causes or foreseeable sequences of events. Typically they will lead to hazardous situations within the category of lost or degraded function.

As an HDO develops an enterprise network, the devices to be incorporated will have to be treated as black boxes with certain network requirements and behaviors, including behavior in the presence of a network failure. The HDO will consider the same system-level failure modes (see sidebar). However, with ownership of and insight into the network infrastructure design and operation, these failure modes must be further broken down into more specific causes. For example, lost connectivity may result from an overloaded link, network hardware failure, network software (OS) failure, improper QoS configurations, overly aggressive security, faulty cabling, accidental disconnection of cabling, power loss, EMI, etc. Each of these more specific causes can be evaluated for probability of occurrence, and each may have specific risk control measures applied. This is an important step in the risk management process because reducing the probability of the failure is a very effective way to reduce risk.

In terms of risk control measures, the HDO is not in a position to apply mitigations to the networked device other than by controlling configurations and workflows. Rather, the HDO can implement mitigations in the design or labeling of the network infrastructure.

Conversely, the MDM is not in a position to apply mitigations within the network to reduce the probability of these failure modes. Rather, the MDM can implement mitigations in the design or labeling of the device.

Layers Within a System of Systems—Locations of Errors and Faults

Part of risk analysis involves considering all the ways the system (in this case the medical IT network) can fail. To do so, an understanding of the layers that make up the entire system is important, as well as what types of errors and faults could exist at each layer. The medical IT network can be considered in two general layers, the network infrastructure (switches, routers, APs, cables, etc.), and the devices connected to it (servers, hosts, medical devices, etc.). In each layer there are subsystems (individual components) and systems (subsystems working together). The network infrastructure system would be all of the network components (switches, routers, APs, etc.) working together to transport data between the connected devices.

Each layer can then be taken independently and examined for errors and faults. Errors in either layer may be functional (the system does not do what it is expected to do) or performance related (it fails under loaded or edge conditions). Additionally, the overall system and the interactions between the layers (interoperability) must be considered.

As the HDO is assessing risk in the network infrastructure layer, there are two categories of faults to examine.

1. Faults that are outside of HDO control. These are either errors that existed in the devices upon delivery to the HDO (e.g.,

software error in the operating system of a network component) or failures that occur during usage (port hardware failure or power supply failure). Information from the IT device manufacturer as well as pre-go-live testing can expose these possible faults and help identify workarounds.

2. Faults that are within control of the HDO or network designer/owner/maintainer. These include network design, topology, and configuration. An overloaded uplink or improper AP spacing are examples. It is the responsibility of the HDO to verify that the network design is correct and appropriate given the information from the network infrastructure component supplier and the MDM.

80001: Supporting Convergence of Devices and IT Networks

Converged healthcare networks enable efficient patient data flow between medical devices and IT systems, so clinicians can access meaningful clinical information throughout the enterprise, supporting quick and effective clinical decision-making. Additionally, consolidating technology onto a common IT infrastructure can help some organizations realize cost efficiencies. Enabling these complex interactions between networked hospital systems requires sophisticated risk management. All parties involved must understand the interactions between the systems, how the risk management efforts relate to each other, and how to collaboratively design the system and manage the system risk. ■

Enabling these complex interactions between networked hospital systems requires sophisticated risk management. All parties involved must understand the interactions between the systems, how the risk management efforts relate to each other, and how to collaboratively design the system and manage the system risk.

Reference

1. **ISO 14971:2007.** *Medical devices—Application of risk management to medical devices.* International Organization for Standardization. Geneva, Switzerland.

EXHIBIT D

For more information, contact Joe Lewelling, AAMI's VP of Standards Development & Emerging Technologies, at jlewelling@aami.org.

FOR DISCUSSION ONLY
September 19, 2014

Health Software Ad hoc group Draft Report – September 2014
Health Software and Health IT Safety Standards
FUTURE STATE Architecture/Framework and Roadmap – DRAFT Report

BACKGROUND

Following informal discussions between JWG7 members from IEC TC 62 / SC 62A and ISO TC 215 in May and October of 2012, ISO TC 215 adopted a resolution at its meeting in Vienna in October, 2012, setting up an ad hoc group to consider how future health software safety standards could address the needs of both communities in a consistent and comprehensive manner.

Resolved that TC 215:
Approves the creation of a Health Software Ad hoc group to create a report that provides guidance on the future development of health software work items that establishes:

1. Guiding principles
2. Common terms and definitions
3. Development roadmap

The group shall be convened for a period of two years from date of formation and have the following co-leaders:
Sherman Eagles (US)
Neil Gardner (CA)
The Group shall be coordinated with JWG7 and include members from ISO TC 215 and IEC SC62A.
The Group shall adopt an approach consistent with the ISO TC 215 Common Terminology Initiative.

The other members of the health software ad hoc group are:
Oliver Christ (DE)
Todd Cooper (US)
Kathy Dallest (AU)
Björn-Eric Erlandsson (SE)
John Fox (UK)
Ross Fraser (CA)
Akihide Hashizume (JP)
Masaaki Hirai (JP)
Patty Krantz (US)
Peter Linders (NL)
Vince McCauley (AU)
Erich Murrell (US)
Toshiaki Nakazato (JP)
Gerd Neumann (DE)
James Savage (UK)
Trish Williams (AU)

This document is our draft report representing the work done by the ad hoc group, regarding a framework for health software and health IT safety standards, and the roadmap for the future development of standards. We welcome feedback on this document and will consider all feedback as we prepare our final report following the October (ISO TC215) and November (IEC SC62A) meetings.

1 INTRODUCTION

In the first year of our Ad Hoc group's mandate we focused on common concepts and definitions for health software safety, and worked with in-flight standards development such as *IEC 82304-1 Health Software – Part 1: General requirements for product safety* in this regard. This was also a year when significant new focus was being placed by national governments in several other forums on the important policy issues - such as the need to address health software which is increasingly configurable, runs on a variety of platforms including mobile devices, and is often developed by non-traditional suppliers in much shorter cycles using components. In particular, both the International Medical Device Regulators Forum (IMDRF) and the U.S. federally mandated FDA Safety and Innovation Act (FDASIA) review recognized the complexity of this space and the need to adopt new approaches to protecting the safety of the public, while not stifling badly needed innovation in health care delivery enabled by electronic health software systems.

Our discussions led to an increased awareness that health includes physical, mental and social well-being and not merely the absence of disease or infirmity (per WHO's definition). Our review of recent reports such as the 2012 Institute of Medicine report on Health IT and Patient Safety resulted in an understanding that health software will be used in a complex sociotechnical environment (see section 1.1 below for a definition of the sociotechnical environment) and cannot be considered safe if the risk management is constrained to the health software itself. In addition to the software itself, safety of health software must also consider the people using the health software, the other system components necessary for the software to run and the broader technical and information infrastructure that the health software operates within (including networks, security, servers, databases, integration with other systems, etc.). **While our initial focus was on health software, we have recognized that the architecture of health software safety standards must also address the safety of the broader Health IT system, and the socio-technical environment of which health software is a component**.

As we complete the second and final year of our group's mandate, these policy directions are important in establishing the need for standards development in the emerging field of Health Software and Health IT safety. In many ways, these emerging policy directions are consistent with our preceding analysis in *ISO TR17791 Health informatics — Guidance on standards for enabling safety in health software*, which concluded that while existing medical device standards provide an excellent starting point, the existing ISO and IEC health software standards are insufficient.

Our group's objectives for 2014 were to:

- Propose an overarching architecture/framework that describes the desired future state for health software safety standards.
- Map the content of existing standards and any other emerging new sources of health software standards and best practices that major countries have adopted, against the proposed framework, and,
- Finally develop a 'roadmap' for health software standards development which builds on our existing standards assets and fills the highest priority gaps – i.e. by proposing new standards, extending the scope of existing standards to address the priority gaps and aligning definitions and concepts across each of the standards in this space as they come up for revision.

We know (from the earlier work on TR17791) that the current landscape is cluttered and has a number of overlaps and gaps. This is natural, as we were at an earlier state of maturity in our awareness and understanding of the issues, and because health software technologies have evolved significantly since the original standards work was done in the medical device context of the time.

1.1 Health IT socio-technical environment

Health software now takes many forms, is typically implemented with other components as a Health IT system**,** and is also interconnected as part of a larger socio-technical environment (or the 'ecosystem' in ISO TR17791). This environment includes:

- **Information and technology** (e.g. hardware, software, networks, interfaces to other systems and data),
- **people** (e.g. clinicians, patients, consumers, caregivers, administrators),
- **care processes** (e.g. clinical workflow, decision algorithms and care protocols),
- **organization** (e.g. capacity, governance, configuration decisions about how health IT is applied), and
- **external environment** (e.g. regulations, public opinion, ambient conditions).

Until now there has been no overarching framework and plan to guide standards development, so health software safety has been addressed in a rather ad hoc way by adding appendages to various existing standards structures, and developing a series of technical reports providing guidance on evolving best practices for specific issues.

The analysis in ISO TR17791 was an important driver for establishing our Ad Hoc group and provides an important foundation by inspiring the following guiding principles that we established.

Our **guiding principles** are that the architecture framework guiding further development of standards for health software and health IT systems should:

- Address the full software product lifecycle and ensure any added burden is commensurate with risk;
- Recognize the broader socio-technical environment that health software systems are implemented in;
- Target the consumers of the standards – fostering their engagement, adoption, use and application;
- Leverage source standards by adding additional guidance and specificity;
- Be forward-looking and adaptable to changes in technology and how software is used; and
- Be agnostic as to whether software is regulated (but supportive of regulatory needs).

2 HIGH LEVEL FRAMEWORK/ARCHITECTURE

Conceptually the framework at its highest level includes four major components:

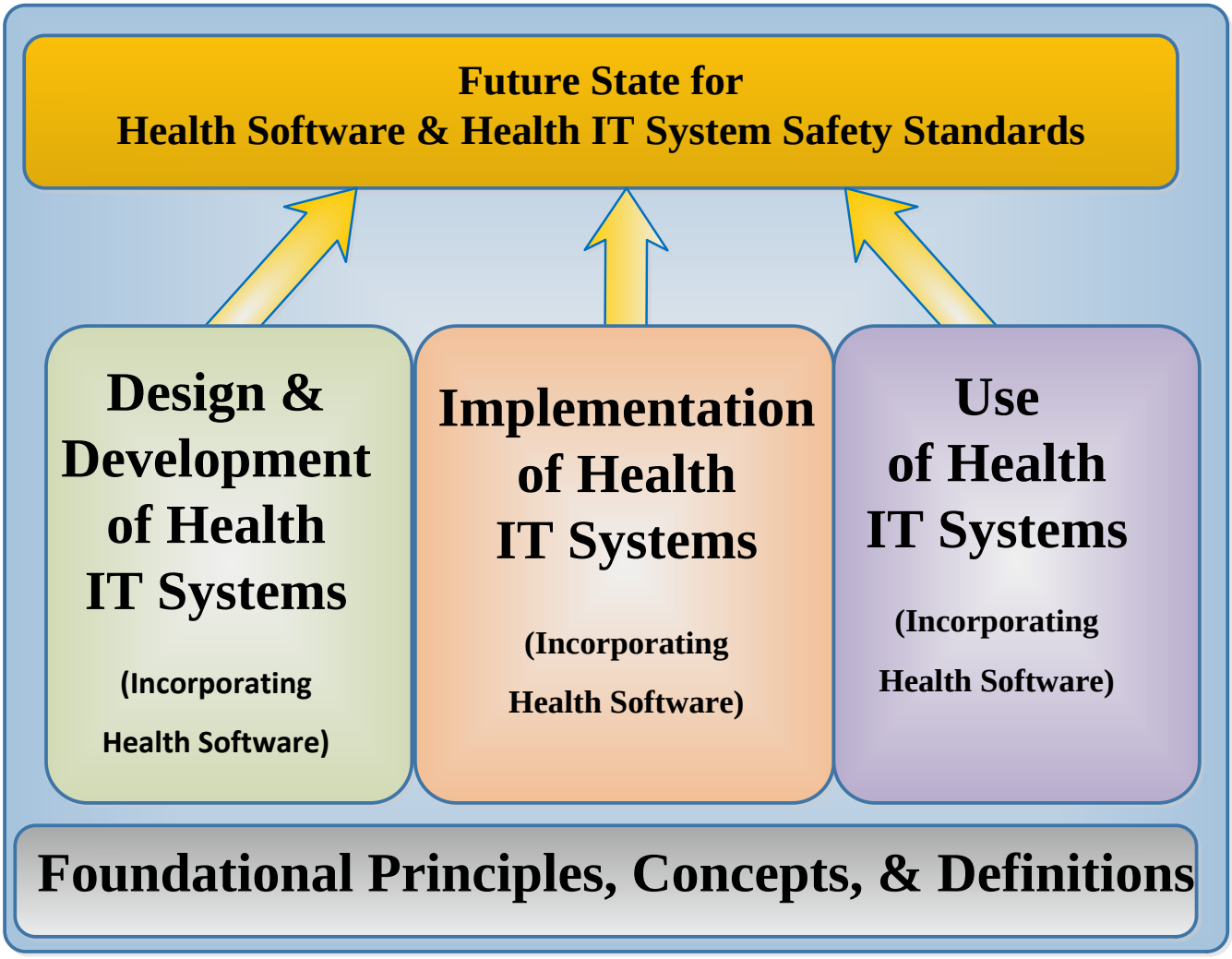
1. A foundational set of standards covering the key health software safety principles, concepts, definitions and common contexts for the use of health software in a health IT system, since many of the same foundational concepts apply across the two key dimensions that we are most concerned with:
    - The target groups of customers (developers, implementers and system operators) who are expected to use the standards
    - The stages of the software lifecycle recognizing their dependencies and hand-offs

   In covering these dimensions, a foundation standard may provide information specific to health software or may reference a suitable international standard that has relevance to this model.
2. A set of standards addressing the design and development of health software (major portions of which could continue to apply to all medical devices) – e.g. updated version of *IEC 62304 Medical device software – Software life cycle processes* with expanded scope.
3. A set of standards covering the configuration, integration and other implementation steps in the lifecycle. These standards need to address the increasing degree to which health software must operate within a complex health IT socio-technical environment involving significant integration with other systems and configuration to meet local business and workflow requirements.
4. A set of standards covering the remaining steps in the lifecycle including both the technical requirements for health software, and how the software will be used to support the clinical facets of the ongoing operation and ultimately the disposal aspects of health software.

Note: In the Roadmap recommendations described in section 4, it is recommended that we leverage, align, extend and expand the scope of existing standards wherever possible, rather than creating new series of

standards. In doing so, we are recommending that the set of standards for both components 3 and 4 above (i.e. for the lifecycle stages beyond design and development) be developed as a single series by expanding the scope of the 80001 series of standards, which is beginning its review cycle.

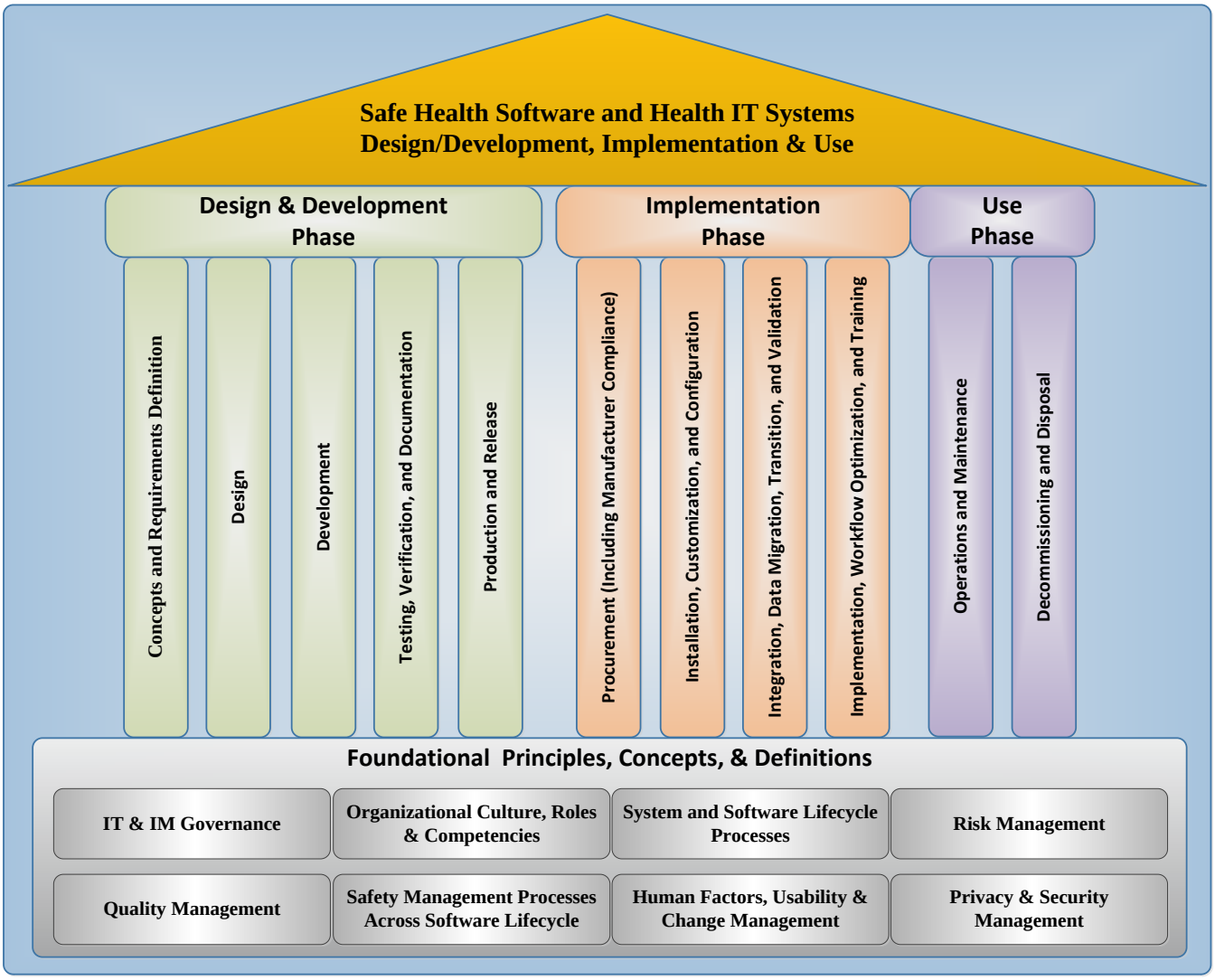
Figure 1. Conceptual model for health software and health IT system safety standards



The main rationale for this approach is that it addresses the five guiding principles outlined above. A balance needed to be achieved - no single framework and roadmap can optimize each of the individual principles. As is the case with any architecture framework, we needed to further de-compose the blocks and develop a migration path (Roadmap) from the current to future state. Since discussions are beginning on the review of *IEC 80001-1 Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsibilities and activities, IEC 62304 Medical device software – Software life cycle processes* and *ISO 27799 Health informatics -- Information security management in health using ISO/IEC 27002* agreement on a definitive standards architecture and roadmap is vital in shaping those major activities going forward, so our work should have some very immediate outcomes.

The following diagram represents our next level of decomposition of the model to a component level and allowed us to map existing and emerging standards and practices against it, in arriving at our recommended Roadmap. In this diagram the box "Foundation Principles, Concepts and Definitions" has been expanded into 8 components.

Figure 2. Component model for health software and health IT systems safety standards



3 CONTENT OUTLINE FOR THE CONCEPTUAL COMPONENTS:

From this high level framework, we have developed a content outline for the components and mapped the known contents from existing standards and best practices against that content outline, iteratively making any necessary revisions to ensure that all facets are covered and the content of the components is complementary (and not unnecessarily duplicative).

In arriving at the suggested outline and approach for the content the four conceptual blocks in the health software safety architecture framework, the following source documents were reviewed:

ISO and IEC Standards and TR's

- ISO/TR 17791 and its associated analysis of existing ISO and IEC standards as summarized in its recommendations on the gaps and overlaps

National Standards and best practices

- England's ***National Health System (***NHS) Standards covering health IT system risk management for manufacturers and implementers/users. These two standards are supported by guidance documents covering emerging themes such as middleware, tele-health and agile development.
- ONC's SAFER guidelines providing checklists for health organizations implementing health software systems covering the full range of socio-technical components
- Canada's COACH eSafety Guidelines that include both best practices and checklists
- The recent FDASIA report and the IMDRF 'Software as a Medical Device' Possible Framework for Risk Categorization and Corresponding controls

3.1 Foundational Principles, Concepts and Definitions

The purpose of these standards would be to provide all parties (from software companies through to end-user health care organizations), with a solid understanding of the principles, concepts, and terms for optimizing the safety of health software and health IT systems - so that they recognize why this area is important; understand the underpinning terminology, concepts and sources from which they are derived; and know which health software standards they should be using depending on their role in the health software and health IT systems lifecycle. These standards would cover the 8 foundational components depicted in Figure 2 above. Depending on the maturity of the initial content, they could start as a TS and then evolve to an IS. In the longer term, these standards could also eventually provide more detailed guidance on how to apply one or more of the foundational areas, across all lifecycle stages, through a series of subsequent TR's or TS's.

The intent would also be to utilize these standards for content that applies across all lifecycle phases. As the first standards developments within the framework occur (e.g. IEC 82304-1, IEC 62304 second edition, IEC 80001-1 second edition and ISO 27799 second edition), it is important that a foundation standard develop in parallel, so that it serves as a tool within ISO TC215 and IEC TC62 to harmonize our terminology and concepts and avoid the need to otherwise unnecessarily duplicate foundational content across other standards targeted to specific lifecycles stages.

Key content includes:

- Introductory section with examples to reinforce the importance of having standards for health software and health IT systems safety. This section would describe the most common types of problems (and patient safety consequences) that can occur and the various factors that need to be addressed by through complementary vigilance and actions by the responsible parties across the software lifecycle. (sources: incident reports and research, the November 2012 IOM report and examples provided by various countries)
- Definitions and key concepts that are important here across the lifecycle – e.g. health, harm, risk management, health software, lifecycle terms, etc. (source: existing source standards from the eight areas), as well as new concepts and terms that apply across the various lifecycle stages as we harmonize the existing standards that are in review/re-development). *Note: The content of TS 25238 Classification of Safety Risks from Health Software (which has been an outstanding concern) would also be addressed here.*
- Key elements and references (drawn from the eight foundational components) that are needed for safety management strategies to reduce the risk of harm (with appropriate references to their source standards and the key controls that can be used), along with cross-cutting safety management processes.
- We anticipate foundational standards with sufficient compliance statements to support regulatory or certification needs. However, given the fact that not all health software will be regulated, and health care organizations may themselves develop and implement software for their own internal purposes, it will be important the foundation provide an end-to-end view of the principles and standards that are necessary across the software lifecycle.
- Our overarching focus in these standards is on **patient safety.** While we recognize that an understanding of good risk, quality, security, IT lifecycle, governance, information management and other source standards and

practices are essential in enabling patient safety, our intent is to describe how these standards should be utilized in a safety management strategy by drawing upon source standards in the foundational areas.

3.2 Safety Standards for Health Software Design and Development

In order to minimize the impact on existing standards and not compromise the requirements needed for medical device regulatory purposes, it is suggested that we focus on aligning the existing set of standards targeted to the development of health software and focus on any gaps or overlaps that could be addressed by:

- Improving the alignment of current standards by reducing overlaps
- Referring to the content of the foundational standard(s) as they are developed and adding appropriate content to the existing standards when necessary to fill gaps
- Adopting common definitions and concepts which can then be instantiated in the foundational standard to guide downstream health software safety standards developments and revisions, and including cross references to other standards in the 'health software safety' family

It is recommended that we first fill identified gaps by adding content to the existing standards (e.g. IEC 62304) during their review/re-development cycles and provide health-specific guidance through the foundational standards. Additional standards that are identified as needed for the design and development phase should follow the modifications to the existing standards.

Potential content includes:

- Expansion of the scope of IEC 62304 to include health software that is not regulated as a medical device
- Inclusion of requirements for creating component/unit software that is incorporated into the health IT socio-technical environment
- Additional content for developing health software that reduces the risk of cybersecurity vulnerabilities
- Possibly moving general requirements (including software safety classification requirements) to a foundation standard that can be referenced by multiple standards
- Creating, or adopting an existing, system engineering life cycle standard for health software

3.3 Safety Standards for Health IT System Implementation and Support for Clinical Use

The purpose of these standards would be to provide a comprehensive view of the key elements that organizations, which are implementing health IT systems and operating them to support clinical uses, need to have in place. These standards need to support all stages of health IT socio-technical environment implementation planning and execution - from requirements definition through acquisition, configuration, integration, data migration, training, deployment, support for clinical use and de-commissioning. There is now a much better understanding about the degree to which safety risks can be introduced at these lifecycle stages through reported incidents, research and publications (such as the November 2012 IOM Health IT and Patient Safety report), as well as experience with implementing comprehensive safety management programs based on best practices in other critical industries as developed by the National Health System (NHS) in England. We also now have some national standards and guidelines in some countries that we can draw upon as noted above.

This scope would focus on health software being implemented into a health IT system in various ways (including cloud, mobile, wired and wireless networks) and in a highly integrated socio-technical environment. Regardless of whether the software itself is regulated, the focus of these standards would be squarely on the full range of risks and contributing factors to safety in its implementation, and the requirements for a comprehensive safety management approach which takes into account the full socio-technical environment within which health care organizations would implement it.

It is recommended that the 80001 series of standards (for which the review cycle is about to begin) be leveraged and expanded in both scope and content to meet these needs to address content areas as described below. This will result in a significant expansion of 80001's risk analysis and risk control considerations.

Potential content includes:

- Articulation of the lifecycle stages that are involved, and the types of risks that are most commonly introduced as health software products are acquired, configured, implemented and used by health care delivery organizations in increasingly complex and critical socio technological environments. These include patient safety risks such as those due to:
    - Data quality, mis-identification and integration of patient data from multiple sources
    - Data accuracy, availability and integrity issues due to configuration, security or IT operations failures
    - Decision support failures due to incorrect or outdated medical logic, reference data, algorithms or alert triggers
    - Failures and inconsistencies in delivery, integration or presentation of diagnostic information or results
    - Insufficient attention to workflow, human factors, change management or training of clinicians
    - Privacy breaches, data governance issues or other causes that erode provider and consumer confidence
- Description of the need for an end-to-end safety management system and a systems engineering approach, including the main components and characteristics that are required to address the full range of risks involved, using models developed in other industries that are widely respected for their comprehensive approach and strong safety records. (This can then be subsequently expressed as an accompanying part of the standards in the form of a maturity model to assist HDOs in self-assessment and continuous quality improvement in their safety practices and embedding a culture of safety).
- Standards and best practices that HDOs should employ in assessing and mitigating these and other common risks through the requisite controls at the appropriate stages of the lifecycle – from systems selection through to de-commissioning. This would address all eight foundational components identified in the safety framework, beginning with the importance of having a risk-based approach (as described in IEC 80001-1), in order to fully address the patient safety risk of implementing systems in HDO socio-technical environments as noted above. Appropriate reference would be made to other standards that are similarly focused on HDOs (such as ISO 27799 on security) to avoid unnecessarily duplication but yet provide useful context regarding the application of established standards in the eight foundational areas to the health software systems implementation and clinical use context. Future parts of the standard can then be developed to provide more detailed requirements in the various foundational areas and address emerging technologies (as the 80001 series has done in the past) or emerging new application areas (such as personalized medicine, genomics and predictive analytics)
- Transition issues which occur at the various post-sales lifecycle stages, whether between the various units of the HDO (technical, information governance and clinical) and with their vendor partners, and articulation of the shared responsibilities, processes and agreements that need to be in place to mitigate the safety risks
- A model for the surveillance and reporting, of safety events as will be proposed at the Berlin meeting for improving the surveillance and reporting of events with respect to the safety of health software.

4 RECOMMENDED ROADMAP

As indicated in section 1 INTRODUCTION, our group's third and final task was to develop a recommended roadmap for future standards development, addressing the gap between our current set of standards for patient safety and the 'future state' framework through a sequence of manageable steps.

Flowing from the discussion of the architecture and the conceptual components in section 3 CONTENT OUTLINE, our roadmap for the transition from our current standards to the 'future state', involves the following recommendations:

4.1 Recommendations for Foundational Principles, Concepts and Definitions

Recommendation 1 – Initiate a new standard or technical specification covering the common principles, concepts, and terms necessary for standards for optimizing the safety of health IT systems across their lifecycle in today's complex socio-technical environment.

4.2 Recommendations for Safety Standards for Health Software Design and Development

Recommendation 2 - Develop the revision of IEC 62304 to cover the scope required for health software.

Recommendation 3 – Initiate a new standard or technical specification or adopt an existing standard covering the system engineering life cycle for health software and health IT systems.

4.3 Recommendations for Safety Standards for Health IT System Implementation and Support for Clinical Use

Recommendation 4 – Develop the revision of IEC 80001-1 (and its parts) to cover the content required for the Implementation and Use phases (see section 3.3).

Recommendation 5 – In the revision of ISO 27799, review the appropriate alignment with security components that are presently incorporated in several parts of IEC 80001-2.

4.4 Recommendations for Applying the Framework

Recommendation 6 – Request that all new projects that impact the patient safety of health software or health IT systems provide an explanation on their NP form of how they fit in the framework.