Best Practices in Applying Medical Device Risk Management Terminology

Fubin Wu and Alan Kusinitz

ANSI/AAMI/ISO 14971:2007 defines harm as "physical injury or damage to the health of people, or damage to property or the environment," hazard as "potential source of harm," and hazardous situation as a "circumstance in which people, property, or the environment are exposed to one or more hazard(s)."[1] These definitions are distinct in wording. However, when used in real-world situations, confusion frequently occurs in the application of these terms. For example, one organization's use of hazard might be interpreted as a harm, hazardous situation, failure mode, or cause by another organization. Even within the same organization, these terms sometimes are used interchangeably without distinction.

Inconsistent use of these terms might not be considered a critical issue, as long as their use results in identification of all elements of risk and adequate risk control measures. However, this issue becomes critical in today's international regulatory environment and complex healthcare system, in which more stakeholders are involved in risk management, more devices are interconnected, and the results of one risk analysis may become input to another risk analysis. This article illustrates best practices in the use of these terms and associated benefits to stakeholders, such as risk management engineers, independent reviewers (e.g., the U.S. Food and Drug Administration [FDA]), healthcare institutions (and their information technology and biomedical staff), and ultimately patients.

Understanding Risk Management Terminology

Although the terms in ANSI/AAMI/ISO 14971:2007 may seem simple in concept, applying them effectively in practice can be difficult. To address this issue, these terms have been mapped into a framework of risk analysis taxonomy (Figure 1). The goal is to illustrate these terms and interrelations in a logical fashion so that risk management engineers, independent reviewers, and device system integrators (e.g., hospitals) can comprehend and apply them effectively. As a result, our explanations can be summarized as follows.

Hazards

A hazard is a *potential* source of harm. It is a potential source because harm can occur only when people (property or environment) are exposed to one or multiple hazards. Hazards exist with or without medical devices and do not have the property of probability. They are just *things* (i.e., nouns without modifiers). ANSI/AAMI/ISO 14971:2007 lists a number of hazard categories and specific hazards in Annex E.1. Good examples include electromagnetic energy, gravity, radiation, heat/cold (i.e., temperature), loss of (therapeutic) function, and incorrect (therapeutic) function or output.

Hazardous Situations

A hazardous situation is the circumstance in which people (property or environment) are

About the Authors

Fubin Wu is cofounder of GessNet risk management software in Sacramento, CA. E-mail: fubin.wu@gessnet.com

Alan Kusinitz is managing partner at Crisis Prevention and Recovery LLC, Full RegulatoryCPR, and SoftwareCPR Services in Boston, MA. E-mail: alan@softwarecpr.com

exposed to one or more hazards. Hazardous situations have the property of probability—a key component of the probability of harm. For example, releasing radiation into an imaging room creates a hazardous situation by exposing a patient or caregiver to the hazard of radiation. As a less obvious but equally important example, providing incorrect dosage information to a clinician creates a hazardous situation because the clinician may take an action that exposes the patient to unnecessary or incorrect radiation. The potential to contribute to a hazardous situation is what brings a specific device or functionality into the realm of risk analysis.

Harm and Risk

Risk is a "combination of the probability of occurrence of harm and the severity of that harm."[1] Harm is only possible when a hazardous situation occurs. Thus, we always estimate the risk of harm arising from a hazardous situation. In Annex E of ANSI/AAMI/ISO 14971:2007, a simplified diagram describes the cascade of events leading from a hazard to a hazardous situation to harm.

Causes

Causes are faults, defects, failure modes, conditions, and events that can contribute to the occurrence of hazardous situations. Causes are specific to a device and have the property of probability. A cause probability affects the probability of hazardous situations and harms to which the cause can lead. Causes can be categorized in various ways. For example, causes can be categorized based on their level of effect on a device, such as system (e.g., system failure modes), subsystem (e.g., software failure modes), and basic (i.e., the initiating events in a causal chain leading to a hazardous situation) causes. They also can be categorized based on their sources (i.e., basic causes), such as software, hardware, environmental, and use error. These categorizations help to proactively and completely identify all causes of hazardous situations.

Best Practices

Best Practice 1

Best practice 1 is to distinguish hazards and causes. This is done by defining hazards at the top level in direct relation to people, property, or environment (e.g., clinical level for people) so that risk analysis can be performed with a focus on potential impact to people (property and environment) and risk analysis results can be structured systematically.

There are practices where certain causes (e.g., system failure modes, subsystem failure modes, basic causes) are referred to as hazards. This use of the term hazard isn't technically wrong per the definition of hazard in ANSI/AAMI/ISO 14971:2007. However, lacking further distinction from hazards that are at top level in

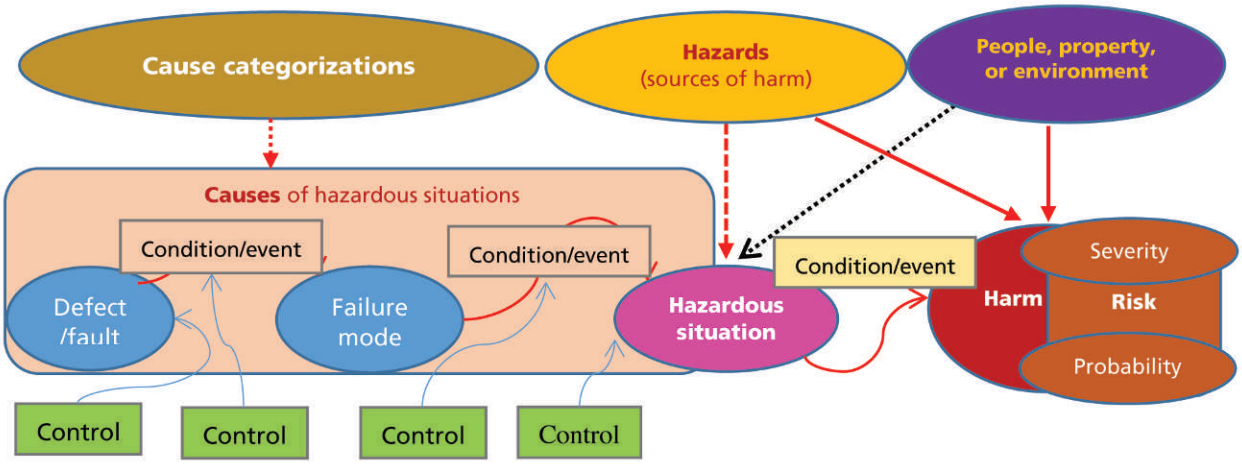


Figure 1. Risk analysis taxonomy and causal chains

relation to people (property or environment), confusion can result. Risk is a combination of severity and probability of harm. Harm is physical injury or damage to people (property, or environment).

For harm to occur, something must be capable of producing harm. The things that can produce harm alone when exposed to people (property or environment) are conceptually different from those that cannot produce harm themselves but can contribute to the occurrence of hazardous situations. For example, "divide by zero" is one of the common causes for a software failure, which can contribute to a hazardous situation that can lead to harm. But for the harm to occur, a specific clinical impact (e.g., incorrect dosage therapy) that can actually harm people (property or environment) must be present.

A "divide by zero" software bug and "incorrect dosage therapy" both can be regarded as potential sources of harm within the ANSI/AAMI/ISO 14971:2007 definition, but "incorrect dosage therapy" can result in harm to patients. The software bug can cause or contribute to various situations that may expose patients to incorrect therapy, but many other software bugs, hardware failures, and use errors also could result in the potential exposure to incorrect therapy.

If we treat every potential cause for the exposure of "incorrect dosage therapy" as a hazard itself, confusion with the top-level hazard "incorrect dosage therapy" can result, thereby complicating the risk analysis by introducing a large number of "hazards" and "hazardous situations." At the same time, it deemphasizes early focus on clinical impact and subsequent focus on chains of events (rather than individual causes) during product development. From an independent review perspective, a flat, unstructured, lengthy list of hazards would be difficult for reviewers to navigate in order to gain understanding of how a device can potentially harm people (property or environment) and what systematic risk controls are in place to ensure safety.

Best Practice 2

Best practice 2 is including the concept of risk causal chains and defining and identifying harms, hazardous situations, and causes within the context of the causal chains.

Kusinitz[2] states, "In general, it is better to spend less time on refining probabilities and risk estimates and more time identifying hazardous situations, their potential causes and effective risk control measures." The concept of risk causal chains provides an effective way to execute this thinking. An end-to-end risk causal chain contains harms, hazardous situations, failure modes, and causes, including conditions and events (Figure 1).

In the context of a specific device or healthcare system, these factors affect each other in a cause-and-effect manner, and they all affect the probability of harms. A harm, as one end of a causal chain, should be specified at a level to which a severity rating can be explicitly assigned. Hazardous situations should be best identified at the boundaries between a device and patients, users, or interfaced outside systems, in order to ensure that causes and risk controls are focused within the scope of a device's capabilities.

Cause should be detailed at the level at which one can ensure adequate risk control. Causes can be individually sufficient to create a hazardous situation, or they may be potential contributing factors that are part of the causal chains that can lead to hazardous situations and harms within the context of a specific device or healthcare system. Due to the complexity of most medical devices, focusing on causal chains (i.e., sequences of events), rather than each cause individually, is recommended. Controlling for each cause individually, without also addressing causal chains and interactions, lacks system-level consideration of all risks and interactions and therefore may not be sufficient or systematically optimized to mitigate all applicable risks. This can lead to unnecessary complexity in the design, which can reduce safety.

Best Practice 3

Best practice 3 is to distinguish among different types of causes. That is, causes of hazardous situations should be properly categorized to ensure adequate coverage of applicable causes.

Depending on the intended use of a medical device and associated design solutions, different types of causes (e.g., environmental, software, electrical, mechanical) can contribute

Controlling for each cause individually, without also addressing causal chains and interactions, lacks system-level consideration of all risks and interactions and therefore may not be sufficient or systematically optimized to mitigate all applicable risks.

to the occurrence of hazardous situations associated with a device. The completeness of cause identification is key to the effectiveness of the risk management process because it directly affects whether all risks are properly identified and mitigated. Causes traditionally are identified through various risk analysis techniques, including failure mode and effects analysis, fault tree analysis, and hazard and operability analysis. These analysis techniques provide categorizations (e.g., design, function, use error, process) to brainstorm and identify more detailed causes. However, they may not necessarily provide adequate categorizations for all basic causes. In addition, for independent reviewers to assess the completeness of the cause identification, it would be more effective to also categorize the causes from a common sources perspective.

In the case of a medical device with embedded software, common causes of software failures are potential sources of hazardous situations. An independent reviewer may want to know whether these common causes are adequately addressed. For example, the FDA infusion pump guidance[3] provides a list of common cause categories of device failures that may contribute to hazardous situations, and it recommends that infusion pump manufacturers provide an analysis and demonstrate how these types of causes have been adequately addressed.

The completeness of cause identification is key to the effectiveness of the risk management process because it directly affects whether all risks are properly identified and mitigated.

IEC 80002-1 divides causes into two types—specific causes directly related to the functionality of the device (e.g., erroneous calculation of radiation dosage) and common causes with indirect and difficult-to-predict impact (e.g., memory corruption)—and it suggests that risk analysis should address both. Depending on the characteristics of a particular device, causes should be categorized in multiple ways to ensure identification of all relevant causes and to allow independent reviewers to effectively assess whether causes that are known per common knowledge (e.g., standards, guidance) are adequately covered. For risk management engineers, proper categorization of those causes provides an effective tool for proactively identifying risk control measures for applicable categories of common causes without relying on the availability of detailed design information.

Best Practice 4

Best practice 4 is including terms of context, assumptions, and rationale as part of risk analysis and requiring their inclusion in risk management reports.

Safety is relative and subjective. Eliminating all risks for a medical device is not possible. As such, risk management involves a comprehensive thought process (e.g., analyses, judgments, determinations). Documenting the information used in this thought process, in order to assess the adequacy of the risk analysis results and conclusions, is critical. According to Eagles and Wu,[4] the assurance case method introduces the terms of context, assumption, and argument (i.e., rationale)—terms that can be adopted during the risk management process to close the information gap.

Benefits of Applying Best Practices

By defining risk management terms using the taxonomy shown in Figure 1, we can use the terms more consistently. In doing so, proactive risk management activities become more intuitive, the risk analysis process becomes more comprehensive, and risk analysis results can be communicated and reviewed more effectively.

Benefits to Risk Management Engineers

As illustrated in Figure 1, a desirable risk analysis should develop a comprehensive understanding of hazards, harms, hazardous situations, failure modes, and causes, including events and conditions that trigger the propagation of cause-and-effect relationships. Adopting a comprehensive understanding early in the process of risk analysis leads to simpler and more effective risk control measures.

If the approach described above is used, then the list of top hazards for a given device should be very short. The hazard categories described in Annex E of ANSI/AAMI/ISO 14971:2007, including therapeutic hazards, energy hazards, and biological and chemical hazards, can help ensure comprehensive identification. Then, particular hazards within each category can be applied for a given device. From there, one can enumerate scenarios in which people, property, or environment can be exposed to applicable hazards (i.e., hazardous situations). Given known potential hazardous situations, the need for proper safety features (as risk control

measures) can be identified prior to the design phase. Because all of these activities can start as early as the product concept phase, safety requirements can be defined proactively. As use conditions, product definition, and design continue to be detailed, lower-level causal chains and common causes of failures can be proactively analyzed for applicability, specificity, and corresponding risk control measures.

Benefits to Independent Reviewers

Lack of consistency in risk management terminology can be particularly challenging for reviewers (e.g., regulators, senior management, risk reviewers) who are not directly involved in design of the medical device. Determining whether the device is acceptably safe for market distribution becomes an important issue for those with critical stakes in device safety. The inconsistency issue with existing risk management terminology makes it difficult for a reviewer to use risk analysis results effectively in making informed determinations and contributes to confusion, which can lead to differences of opinion on acceptability of residual risk.

As described above, both top hazards and common cause categorizations are relatively well known across similar devices; reviewers can use these as entry points for their review process. With these entry points, reviewers can navigate to further details that are device specific. Reviewers also can use other common knowledge such as standards and guidance (e.g., FDA infusion pump guidance, IEC 80002-1), recalls, and adverse events to challenge whether the risk analysis is complete and adequate. In addition, the inclusion of context, assumption, and rationale reduces reliance on often arbitrary severity and probability numerical ratings and makes it possible for independent reviewers (e.g., FDA) to access the information that is critical to understanding the safety conclusions made by risk management engineers and manufacturers.

Benefits to Patient Safety

By applying the best practices described above, hazards and harms can be used more consistently, which can enable multiple medical

Adopting a comprehensive understanding early in the process of risk analysis leads to simpler and more effective risk control measures.

devices to be connected with a risk causal chain analysis across the entire patient care system.

For example, consider a system to provide blood transfusions to patients. This system could involve several devices: blood establishment software for facilitating the blood collection/storage and tracking of individual blood units, a blood unit dispenser in a hospital for automatically identifying and releasing a blood unit, other devices that may be involved with the actual blood testing or transfusion, and perhaps wireless-enabled information systems providing connectivity among the devices.

Overall, one common hazard for all of these devices is unsuitable blood (e.g., ABO-incompatible blood, blood containing infectious diseases, blood processed without following safety standards). Avoiding of the hazardous situation of transfusing unsuitable blood, which could cause various harms (e.g., transfusion reaction, infectious disease), is essential. The system hazard of unsuitable blood and associated harms can be consistently used in the risk analysis for each of the devices and system involved in the blood transfusion. The difference in risk analysis among these devices and systems may only be the identification of an intermediate hazardous situation, its associated causes, and any other hazards unique to their role in the process (such as harm to the donor).

For example, for the blood establishment software, a typical hazardous situation leading to a transfusion with incompatible blood would be that the blood type is mislabeled or otherwise misidentified in the system. For the blood unit dispenser machine, it could be that the wrong type blood unit is dispensed. For the blood transfusion devices, it would be that a mismatched blood unit is transfused. The total risk that an end patient is facing with this system would have contributing factors from each of the devices in the system.

Applying consistent best practices in risk management terminology is essential to analysis of a system of interconnected devices.

Conclusion

With medical technology continuously evolving, more advanced and complex medical devices may be developed in the near future. For example, a closed-loop infusion system (e.g., artificial pancreas device) could automatically administer insulin infusion therapies based on real-time blood glucose monitoring. The total risks to patients associated with these types of systems can only be assessed fully by leveraging individual device- or system-based risk analysis. Applying consistent best practices in risk management terminology is essential to analysis of a system of interconnected devices.

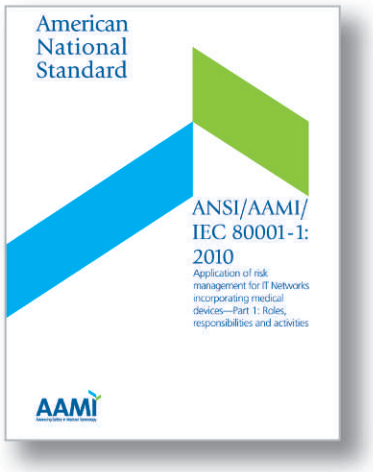
The risk management terms identified in ANSI/AAMI/ISO 14971:2007 have distinct meanings that should be used properly. The term hazard should be defined to distinguish clinical hazards from causes and failure modes. Causes of hazardous situations should be properly categorized. In addition, causal chains, context, and assumptions should be defined and included in risk analysis. This will help ensure a common unders tanding, comprehensiveness, simplicity, and consistency in risk management and review. The consistent and meaningful use of risk management terms can benefit risk management engineers, risk management reviewers, users, and ultimately patients. ■

Acknowledgments: To Harvey Rudolph, independent consultant and former FDA deputy director of the medical devices laboratory, and Sherman Eagles, partner at SoftwareCPR and lead instructor for the AAMI *Safety Assurance Case for Medical Devices* course, for valuable assistance in reviewing and commenting on the article.

References

1. **Association for the Advancement of Medical Instrumentation.** ANSI/AAMI/ISO 14971:2007, *Medical devices—Application of risk management to medical devices*. Arlington, VA: Association for the Advancement of Medical Instrumentation; 2007.
2. **Kusinitz A.** Use and Misuses of Probability in Medical Device Risk Management. *Biomed Instrum Technol*. 2005;39(5):381–5.
3. **U.S. Food and Drug Administration.** Infusion Pumps Total Product Life Cycle: Guidance for Industry and FDA Staff . Available at: www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM209337.pdf. Accessed January 23, 2015.
4. **Eagles S, Wu F.** Reducing Risks and Recalls: Safety Assurance Cases for Medical Devices. *Biomed Instrum Technol*. 2014;48(1):24–32.

AAMI Guidance For Healthcare Providers Managing Medical IT-Networks



ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT Networks incorporating medical devices— Part 1: Roles, responsibilities and activities*

Order Code: 8000101 or 8000101-PDF
List $130 / AAMI member $78

TIR80001-2-1:2012, *Part 2-1: Step by step risk management of medical IT-networks; Practical applications and examples*

Order Code: 800010201 or 800010201-PDF
List $150 / AAMI member $90

TIR80001-2-2:2012, *Part 2-2: Guidance for the communication of medical device security needs, risks and controls*

Order Code: 800010202 or 800010202-PDF
List $150 / AAMI member $90

TIR80001-2-3:2012, *Part 2-3: Guidance for wireless networks*

Order Code: 800010203 or 800010203-PDF
List $140 / AAMI member $84

TIR80001-2-4:2012, *Part 2-4: General implementation guidance for healthcare delivery organizations*

Order Code: 800010204 or 800010204-PDF
List $110 / AAMI member $66

Order your Copy Today!
Call +1-877-249-8226
Visit http://my.aami.org/store

SOURCE CODE: PB

AAMI
Advancing Safety in Medical Technology