Medical Device Risk Management And Safety Cases

Paul L. Jones and Al Taylor

Safety assurance cases have been used in different industry sectors such as nuclear power, transportation, and military systems for many years. In 2010, the U.S. Food and Drug Administration (FDA) launched the Infusion Pump Improvement Initiative to address observed infusion pump safety problems. As part of this initiative, the agency began to review safety assurance cases submitted within premarket device notifications for drug infusion pumps.[1]

At this time, the FDA has not specified a format for safety assurance case submissions. Therefore, seeing a wide variation in safety case organization, content, and soundness is not surprising. Based on review of numerous safety case submissions received to date, a common approach followed by many manufacturers has been to convert existing risk/hazard analysis work (typically presented in tabular format) to a graphical representation. The result, in general, was numerous diagrams that were difficult to review, comprehend, and develop confidence in.

This report discusses how artifacts from a risk management process based on ANSI/AAMI/ISO 14971:2007[2] might be organized into a safety assurance case and how the safety case development process can contribute to the risk analysis process. Notions of argument and evidence sufficiency and their relationship to confidence are introduced. A sample risk analysis and safety case pattern using ANSI/AAMI/ISO 14971:2007 artifacts are presented. Also, a sample design safety case template is presented that demonstrates how the safety case approach is broader than ANSI/AAMI/ISO 14971:2007.

The terminology used in this article is based on ANSI/AAMI/ISO 14971:2007[2] and ISO/IEC TR15026-1:2010,[3] though certain terms are not explicitly defined in these standards.

Scope

Of note, the safety case discussion in this report is limited to design risk space, in the context of ANSI/AAMI/ISO 14971:2007, shown in Figure 1. A comprehensive and complete safety assurance case ultimately would need to address all aspects of a device's life cycle. However, FDA currently is focused on reviewing design-centric safety assurance cases as part of Class II 510(k) reviews.

Basic Concepts of Risk Management And Safety Cases

Risk as a Measure of Safety

Broadly speaking, ANSI/AAMI/ISO 14971:2007 establishes a process for managing risk that includes identifying hazards[2] and hazardous situations, estimating risk arising from each hazardous situation, evaluating the acceptability of risk arising from each hazardous situation, implementing risk control measures for unacceptable risks, verifying and validating the effectiveness of risk control measures, and evaluating the acceptability of residual risks, both individually and collectively.

About the Authors

Paul L. Jones is a senior systems/software engineer at the Center for Devices and Radiological Health of the U.S. Food and Drug Administration in Silver Spring, MD. E-mail: paul.jones@fda.hhs.gov

Al Taylor is a laboratory-based electrical engineer at the Center for Devices and Radiological Health of the U.S. Food and Drug Administration in Rockville, MD. E-mail: alford.taylor@fda.hhs.gov

In the context of ANSI/AAMI/ISO 14971:2007, judgments concerning the acceptability of risk are based on documented acceptability criteria. In the event that the residual risk is judged to be unacceptable after all practicable risk control measures have been implemented, a risk-benefit evaluation can be undertaken to justify the acceptability of the residual risk. A device is said to be safe if it is free from unacceptable risk (i.e., all foreseeable risks have been mitigated to the extent practicable and the overall residual risk is deemed acceptable). Of note, this is the top-level claim of Figure 1.

Safety Assurance Case Composition

ISO/IEC TR15026-1[3] is one of a suite of assurance case standards and technical reports that cover assurance case development (also see references 4 and 5). TR15026-1 defines an assurance case as follows: "Representation of a claim or claims, and the support for these claims. NOTE: An assurance case is [a] reasoned, auditable artefact created to support the contention its claim or claims are satisfied. It contains the following and their relationships: one or more claims about properties; arguments that logically link the evidence and any assumptions to the claim(s); a body of evidence and possibly assumptions supporting these arguments for the claim(s)."

A safety assurance case, or safety case, is an assurance case that addresses safety. In its "atomic" form; therefore, a safety case consists of a safety-related claim, argument, and evidence tuple (plus supporting elements; e.g., assumption, justification, context). A safety assurance case includes from one to many safety-related claim tuples.

Figure 1 presents a safety assurance case claim structure that is completely arbitrary but logical from a product development perspective. It provides a framework for arguing that risks for various aspects of device product realization are acceptable. The current work focuses on the "design risks are acceptable" claim, where the context of the claim is "foreseeable use or misuse."

Within the "design risks are acceptable" claim, an argument is constructed justifying that the device is free from unacceptable risks arising from the design of the product.

Within the "manufacturing risks are acceptable" claim, an argument is constructed justifying that the device is free from unacceptable risks arising from the design of the systems used to manufacture the product (where we holistically mean the manufacturing systems used to produce, distribute, install, service, maintain, and retire the product from cradle to grave).

Within the "risk management (RM)/quality management (QM) systems are adequate" claim, an argument is constructed justifying that the quality and risk management systems that underlie the design and manufacturing of the product are adequate, given the technologies used and the composition of the manufacturer's organization.

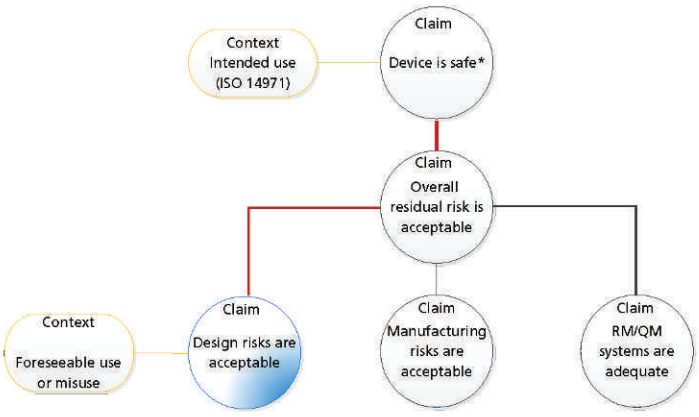


Figure 1. Design risk claim contribution to the "device is safe" (root) claim. Abbreviations used: QM, quality management. RM, risk management. In the context of ANSI/AAMI/ISO 14971:2007, a device is said to be safe if it is free from unacceptable risk (i.e., if all foreseeable risks have been mitigated to the extent practicable and the overall residual risk is acceptable).

Safety Case Presentation Considerations

A safety case report can be presented in many different configurations and formats. The best of these is constructed in a manner that enables a reviewer to comprehend the information quickly and ultimately develop confidence in the top-level claim (e.g., "the device is safe").

Narrative language can readily do the job but can rapidly become overwhelming when trying to establish relationships among different elements of the narrative. Tabular format has been used for decades. However, tables can also hide interrelationships among table elements. Graphical formats offer another alternative. Although they can serve to elucidate infor-

mation relationships, they also can become rapidly incomprehensible when in very large graphs/diagrams.

A general consensus exists among the assurance case community that it will require use of all three presentation formats to make the best (safety) assurance case(s). The ability to transition seamlessly among narrative, tabular, and graphical presentation formats provides the best of these possibilities. Further, safety case presentations are necessarily abstract. Beneath this abstraction lie design life cycle details, rationale, and evidence artifacts that serve to justify claims. To facilitate the development and review of safety cases, links between safety case elements and corresponding concrete design artifacts must be established. This suggests the need for tools to support requirements of this type; such tools include TurboAC (GessNet, El Dorado Hills, CA), ASCE (Adelard, London), and NOR-STA (NOR-STA, Gdańsk, Poland).

Risk Management

ANSI/AAMI/ISO 14971:2007 provides a risk management process for the medical device industry that serves to broadly establish a basis for claiming that a device is safe. Each step of the process calls for a degree of analysis that yields artifacts ranging from identified hazardous situations to verification of risk control measures. Each of these steps is discussed below in terms of how its artifact(s) contribute to establishing the acceptability of risk and the safety case.

Identification of Hazards and Hazardous Situations

Section 4.3 of ANSI/AAMI/ISO 14971:2007 requires the manufacturer to "compile documentation on known and foreseeable hazards" under both normal and fault conditions. Section 4.4 of ANSI/AAMI/ISO 14971:2007 further requires the recording of reasonably foreseeable sequences or combinations of events and circumstances (causes) that can result in a hazardous situation. This arguably is the most important design activity in establishing device safety, as the hazardous situations identified in this step are the basis for subsequent risk analysis steps.

ANSI/AAMI/ISO 14971:2007 carefully distinguishes between hazards, which are "potential sources of harm," and hazardous situations, which are "circumstances in which people, property, or the environment are exposed to a hazard." The point of the hazard analysis effort is to identify not only hazards but also the circumstances that might reasonably lead to harm. There is a purely pragmatic reason for this: By addressing the circumstances—or in other words, by limiting the exposure to potential sources of harm—risk can be mitigated.

Distinguishing between events and circumstances also is important. A discrete event often is the trigger or proximal cause of an adverse event, but only if circumstances have created the conditions necessary for its occurrence. For example, three ingredients are needed to start a fire: fuel, an oxidizer, and an ignition source (heat). Any time circumstances create the potential for these ingredients to combine, a hazardous situation exists. The ignition source often is an event, such as a lightning strike on a mountain top, but other circumstances dictate whether that lightning strike will result in a fire and how much damage the fire will cause. In another common scenario, the ignition source such as a hot surface is continuously present in the environment, and the triggering event might be a leak that causes fuel to be spilled on the hot surface. The resulting fire is not caused by the triggering event but rather by the circumstances that permit the ingredients (heat, oxygen, and fuel) to combine in proportions that support combustion.

Neither FDA guidance[6] nor ANSI/AAMI/ISO 14971:2007 requires the use of a specific technique for identification of hazards and hazardous situations. Annexes in the standard provide examples of hazards and summarize several common techniques such as fault tree analysis, failure mode and effects analysis, and hazard and operability study (also see references 7–9). Other techniques, such as event tree analysis[10] and systems-theoretic process analysis,[11] used in safety-critical industry sectors also should be considered and used as appropriate. Each technique has strengths and weaknesses that depend on intent, resources, and the level of completeness of the device design. Several techniques should be used in a complementary iterative manner to help ensure a comprehensive hazard analysis as a design evolves. (This applies to postmarket corrective,

The point of the hazard analysis effort is to identify not only hazards but also the circumstances that might reasonably lead to harm. There is a purely pragmatic reason for this: By addressing the circumstances—or in other words, by limiting the exposure to potential sources of harm—risk can be mitigated.

perfective, and adaptive type activities as well.)

Results of the hazard identification process (i.e., hazardous situations) and their associated causes (i.e., events, circumstances) are communicated in the corresponding fields of Figure 2.

Estimation and Evaluation of Risk(s) for Each Hazardous Situation

Section 4.4 of ANSI/AAMI/ISO 14971:2007 states, "For each identified hazardous situation, the associated risk(s) shall be estimated using available information or data. ... The results of these activities shall be recorded in the risk management file." Section 5 of the standard further requires that an evaluation of each risk be performed using criteria defined in the risk management plan.

As explained in the standard, the risk estimation step documents the nature of the risks arising from each hazardous situation, the probability of occurrence of the hazardous event, and the severity of the resulting harm—to the extent that these can be determined a priori. When a range of outcomes is possible, the risk associated with each outcome should be estimated, particularly if different circumstances influence which outcome is likely to be realized.

Manufacturers sometimes assert that they have employed "the best practices of the medical device industry." However, where software is concerned, the manufacturer should be embracing the best practices of the software engineering profession.

The evaluation step follows the estimation step; at this stage of the process, a judgment is made concerning the acceptability of the risk, based on defined criteria. Annex D.3 of ANSI/AAMI/ISO 14971:2007 provides notions of risk estimation and risk matrices. Unfortunately, many of those who use the standard take the risk matrix examples literally and purport to apply (qualitative or quantitative) probabilities/likelihoods associated with risk across all hazardous situations, their causal factors, and risk control measures. Doing so 1) obfuscates the rationale behind the use of a particular risk control measure and 2) fails to account for the variation in risk for each component and combination of device components, thereby affecting the credibility of the risk analysis. For example, it is not unusual for a manufacturer to submit a hazardous situation potentially caused by a software component and claim that an initial risk level of 10^{-4} is reduced to a risk level of 10^{-6} after testing. Clearly, this is an unjustifiable risk (reduction) argument for software, if for no other reason than software faults are systematic, not random.

Annex D.4 enumerates methods of determining acceptable risk, which include, but are not limited to[2]:

- "using applicable standards that specify requirements, which, if implemented, will indicate achievement of acceptability concerning particular kinds of medical devices or particular risks;
- comparing levels of risk evident from medical devices already in use;
- evaluating clinical study data, especially for new technology or new intended uses;
- taking into account the state of the art and available information such as technology and practice existing at the time of design.

'State of the art' is used here to mean what is currently and generally accepted as good practice. Various methods can be used to determine "state of the art" for a particular medical device, such as:

- standards used for the same or similar devices;
- best practices as used in other devices of the same or similar type;
- results of accepted scientific research"

Risk estimation often is subjective. Its contribution to a risk acceptability argument is consequently weak and therefore provides little confidence to reviewers. When credible risk estimation can be made, it should be presented. However, in many cases, a more justifiable argument relies on what the current work refers to as *safety decision rationale*, which is based on sources identified above (Annex D.4) and the use of best safety-critical industry development practices (e.g., model-based design, formal methods) and the corresponding results (artifacts).

The concept of "best practices" requires elaboration. Manufacturers sometimes assert that they have employed "the best practices of the medical device industry." However, where software is concerned, the manufacturer should be embracing the best practices of the software engineering profession. More generally, manu-

facturers should employ practices appropriate for the technologies used in their devices.

Distinguishing between *process* and *product* standards and practices also is important. Robust quality and risk management systems have been documented as being key to managing the complexity inherent in modern medical devices; however, having a robust process is not sufficient. For any given technology, the relevant body of knowledge has identified specific design features and implementation practices that should be observed, as documented in textbooks, consensus standards, and the professional literature.

For example, a safety decision rationale for software might make note of the fact that a rigorous software development process adhering to IEC 62304 was used in its development but would also make reference to safety-related architectural features of the software, quantitative code quality metrics,[12] the results of static analysis,[13] and the incorporation of defensive measures such as watchdog timers.

When constructing a safety case, especially if the degree of risk is, in practical terms, unknowable, an argument based on a safety decision rationale generally provides a more convincing basis for justifying the sufficiency of an acceptable risk claim than an argument based solely on risk estimation. In a broader sense, aggregated safety decision rationale (arguments), appropriate evidence, and associated claims serve to establish confidence in the top-level claim (from Figure 1) that the device is safe. This safety decision rationale is communicated in the corresponding field of Figure 2.

Implementation of Risk Control Measures And Evaluation of Residual Risk

As stated in Section 6 of ANSI/AAMI/ISO 14971:2007, when a given risk is judged to be unacceptable, the manufacturer must implement risk control measures "that are appropriate to reduce the risk to an acceptable level." The effectiveness of each risk control measure is required to be verified and the results recorded in the risk management file. As such, conformance to the standard requires establishing evidence that a risk control measure has been verified as effective (in the context of design specifications and expected results/behavior) and validated as fit for purpose (in the context of device intended use).

Risk control measures, verification of effectiveness, and verification of implementation (validation) are communicated in the corresponding fields of Figure 2.

Ultimately, after all practicable mitigations have been implemented and a "final" risk evaluation has been performed (overall residual risk), considering whether the benefits of using the device outweigh the risks may be necessary. The rationale for such a decision should be included in the safety case as well.

Summarizing Risk Analysis Results

FDA guidance[4] recommends submitting the following software risk/hazard analysis artifacts in tabular format: identification of the hazardous event, cause(s) of the hazard, severity of the hazard, method of control, corrective measures taken, and verification [of] the method of control.

The current work offers a refinement to the recommended tabular format that is more consistent with ANSI/AAMI/ISO 14971:2007

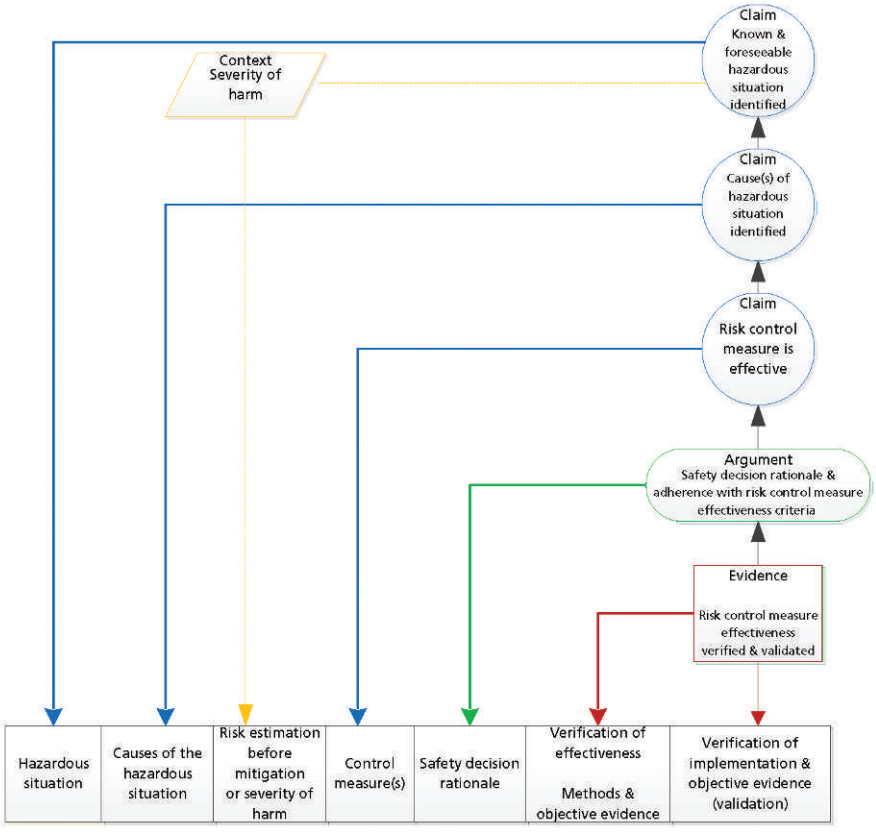


Figure 2. Risk analysis table and safety case pattern using ANSI/AAMI/ISO 14971:2007 risk management process artifacts

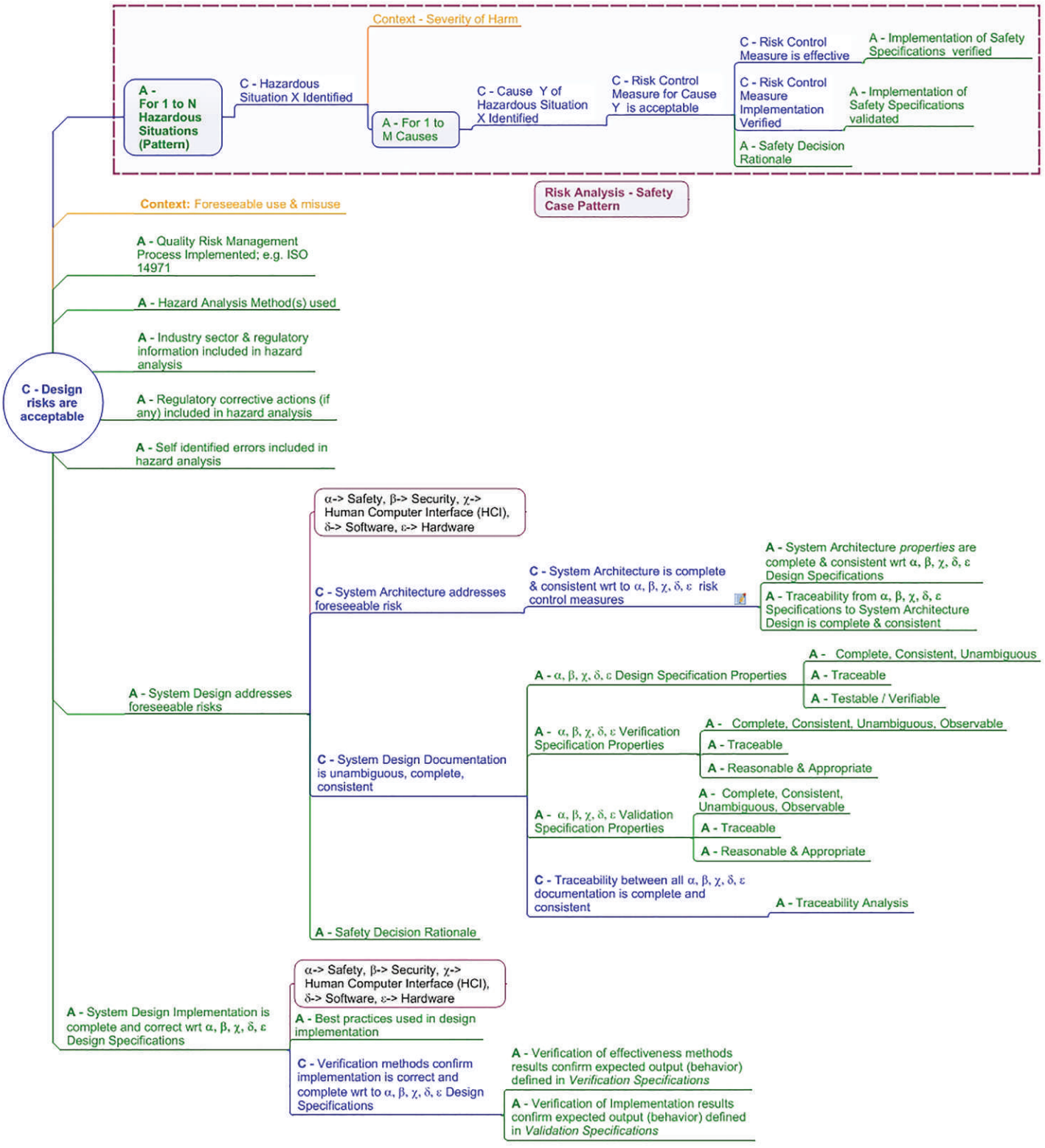


Figure 3. Example device design safety case template. Abbreviations used: A, argument; C, claim.

terminology (and a safety assurance case). This refinement will be called a *risk analysis report* and includes:

- Hazardous situation
- Cause of the hazardous situation
- Severity of harm
- (Risk) control measure(s)
- Safety decision rationale
- Verification of effectiveness method(s) and objective evidence (verification)
- Verification of implementation and objective evidence (validation)

The information listed above should be available in the ANSI/AAMI/ISO 14971:2007 risk management file, in conformance to the standard. Figure 2 demonstrates how this information might be presented in tabular format.

Safety Case

Figure 2 shows how the safety case tuples (claims, arguments, evidence) correspond to the risk analysis report artifacts listed above. Severity of harm is included to provide context for the identified hazardous situations prior to mitigation. Figure 2 also presents a safety case pattern implicit in the risk analysis table. This pattern is duplicated in each row of the risk analysis table (Figure 3).

The safety case presented in Figure 2 is compelling, but insufficient, because it represents only a portion of a necessarily broader device (system) safety argument. Figure 3 provides an example of what this additional argumentation might include. Of note, the risk analysis safety case pattern in Figure 3 represents a generalization of the safety case pattern in Figure 2 (for all "N" hazardous situations).

In the device design safety case template shown in Figure 3, a claim that "design risks are acceptable" is made, supported by a generalized extension of the safety case (argument) pattern in Figure 2, various hazard-related arguments, and system design and implementation arguments. System design and implementation arguments address safety, security, human-computer interfaces, software, and hardware.

Hazard Causal Chain (Hazard, Failure Mode, Cause, Control)	Severity (Harm)	Safety Decision Rationale	Verification	Validation
Air in line	Major (Embolism)	The OUS field performance review has confirmed devices with same/similar design and risk controls haven't had air in line hazardous situation occurred over last 3 year period		Field performance review report #124
I-System alarms and stops infusion when harmful air bubbles or accumulated amount of air detected		Safety testing confirms pump's conformance to IEC60601-24 on bubble size and accumulated amount of air and IEC60601-1-8 on alarm systems. Failure modes are analyzed and mitigated.	Verification Test Case# 563	[IEC60601-24 Testing #112 , IEC60601-1-8 Testing# 321]
Air in line sensor fails		Simulated validation testing confirms faulty sensor alarm generated and infusion stopped before the air gets into the patient when there is air passing the sensor and the sensor has a malfunction		Simulation Test Report
A-Software checks the detector signals every second and alarms when abnormal sensor values detected		Software verification confirms software checks detector's signal every second, detects the malfunction when there is an abnormal value, and generates alarm when there is a sensor malfunction	Verification Test Case# 864	
Pump fails to stop the infusion when air in line alarm condition detected				
*Loose IV connectors		Standard testing confirms connector's conformance with ISO 594		Conformance Report# 423
A-Require ISO 594 compliant connector		Connector component selection criteria is defined in the Billing of Materials Specification	BOM Spec# 365	

Figure 4. Table from Figure 2 using GessNet TurboAC tool. Abbreviations used: A, additional risk control; I, initial risk control. Blue text in the first column—indicates "risk control measure." The blue dots in the fourth and fifth columns are indicators for evidence link. GessNet TurboAC, ASCE, and NOR-STA tools are used in the FDA Office of Science and Engineering Laboratories. The mention of commercial products, their sources, or their use in connection with material reported herein is not to be construed as either an actual or implied endorsement of such products by the Department of Health & Human Services.

Using state-of-the-art system and software engineering technology (e.g., model-based design/engineering, formal methods, static analysis), completeness and consistency properties can be mechanically demonstrated and documented. Further, the properties can be (independently) verified, serving as a "measure" of design quality. Acknowledging weaknesses associated with the use of models, these methods have proven themselves extremely effective in many safety-critical industry sectors. To the extent that one can "trust" device design and implementation artifacts, one can have confidence in the likelihood that the device will perform as intended.

Another important factor for reviewer confidence is traceability among design and implementation artifacts. A lack of traceability results in design inconsistencies and (safety) implementation errors.[14] A trace analysis report that addresses the completeness and consistency properties of design and implementation documentation serves to justify quality properties of these artifacts. Using computer-based tools, traceability (links) can be easily managed and make it easy for both a developer and reviewer to quickly refer to the linked information/artifacts (Figure 4).

The whole point of constructing a safety case is to provide a reviewer with sufficient confidence that a device is reasonably safe for its intended use. To the extent that the reviewer of the safety case can identify reasons to doubt the claims, arguments, or evidence presented, confidence in device safety is correspondingly eroded. For example, if a claim that "risk control measures for known and foreseeable hazards are acceptable" is based on an argument (and/or evidence) that only one hazard analysis method was used, then a reviewer likely will have doubts regarding the comprehensiveness of the hazard analysis. If the hazard analysis method used presents as inconsistent with best practices, another level of doubt is raised. Similarly, if no safety decision rationale for a risk control measure exists, it will be difficult to establish confidence that the risk control measure is reducing risk to an acceptable level or that a basis exists for an overall residual risk claim. Ultimately, if the safety case raises too many reasons for doubt, the reviewer won't have sufficient confidence in the safety of the device.[15] This in turn, for example, could result in "additional information" requests and delays in regulatory decisions.

Discussion

The importance of establishing risk acceptability criteria and, in particular, safety decision rationales for risk analysis activities and the safety case cannot be overstated. When including a risk/hazard analysis table, which is common in submissions, the presence of a safety decision rationale strengthens the presentation and helps establish a convincing safety case (Figure 2). Most importantly, a safety decision rationale establishes a basis upon which risk control measures can be assessed and claims of (device) safety can be made.

The definition of safety in Federal regulation 21 CFR 860.7(d)(1) is different from the definition in ANSI/AAMI/ISO 14971:2007. This might pose a dilemma for manufacturers and regulators. However, upon closer examination, the semantic and conceptual framework of ANSI/AAMI/ISO 14971:2007 is fully consistent with the meaning and intent of the regulation. Thus, using the definition presented in the standard should not pose a regulatory problem as long as it is used within the context of a risk management system that fully conforms to the standard. The following facts support this contention:

- ANSI/AAMI/ISO 14971:2007 establishes a comprehensive risk management process covering all stages of the product life cycle.
- The standard is used internationally and widely accepted as definitive.
- The standard has been cited as a normative reference in many other international medical device standards.
- FDA has formally "recognized" the standard as providing an acceptable methodology for managing risk associated with the use of a medical device.

Conclusion

The current report demonstrates how one can leverage work done in conformance to ANSI/AAMI/ISO 14971:2007 to create a risk analysis report suitable for internal and external (regulatory) review. The report also can serve as part of a safety case, as illustrated in Figure 2 and more broadly in Figure 3. Further, organization of this information is consistent with existing FDA guidance.[6] In fact, the table shown

Additional Resources

- **Jones, PL, Jorgens J 3rd, Taylor AR Jr, Webber M.** Risk Management in the Design of Medical Device Software Systems. *Biomed Instrum Technol.* 2002;36(4):237–66.
- **Kelly TP.** Arguing Safety: A Systematic Approach to Safety Case Management. DPhil Thesis YCST99-05, Department of Computer Science, University of York, UK; 1998.
- **Eagles S, Wu F.** Reducing Risks and Recalls: Safety Assurance Cases for Medical Devices. *Biomed Instrum Technol.* 2014;48(1):24–32.
- **Government Printing Office.** 21 CFR 860.7(d)(1). Available at: www.gpo.gov/fdsys/pkg/CFR-2012-title21-vol8/pdf/CFR-2012-title21-vol8-sec860-7.pdf. Accessed April 24, 2014.

in Figure 2 is consistent with risk/hazard analysis tables manufacturers have been submitting for many years. The only difference is that the safety decision rationale is copied from the risk management file into the risk analysis report presentation, whereas risk reduction/estimation information is not.

The best safety case eliminates doubts in its claims, arguments, and evidence. A safety case is broader than the risk analysis work encapsulated in ANSI/AAMI/ISO 14971:2007, in that it organizes all of the safety-related work into a comprehensive argument justifying a claim that the device is safe. ■

The best safety case eliminates doubts in its claims, arguments, and evidence.

References

1. **McGowan R, Stevens A, Chapman R.** Food and Drug Administration Review of Safety Assurance Cases for Medical Devices. *J Clin Eng*. 2014;39(2):96–8.
2. **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.
3. **International Standards Organization.** ISO/IEC TR15026-1:2010, *Systems and software engineering—Systems and software assurance—Part 1: Concepts and vocabulary*. Geneva: International Standards Organization; 2014.
4. **International Electrotechnical Commission.** ISO 15026-2:2012, *Systems and software engineering—Systems and software assurance—Part 2: Assurance case*. Geneva: International Electrotechnical Commission; 2012.
5. **International Electrotechnical Commission.** ISO 15026-4:2012, *Systems and software engineering—Systems and software assurance—Part 4: Assurance in the life cycle*. Geneva: International Electrotechnical Commission; 2012.
6. **U.S. Food and Drug Administration.** Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices. Available at www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm089543.htm. Accessed February 10, 2015.
7. **International Electrotechnical Commission.** IEC 61025:2006, *Fault tree analysis (FTA)*. 2nd ed. Geneva: International Electrotechnical Commission; 2006.
8. **International Electrotechnical Commission.** IEC 60812:2006, *Analysis techniques for system reliability—Procedure for failure mode and effects analysis (FMEA)*. 2nd ed. Geneva: International Electrotechnical Commission; 2006.
9. **International Electrotechnical Commission.** IEC 61882:2001, *Hazard and operability studies (HAZOP studies)—Application guide*. 1st ed. Geneva: International Electrotechnical Commission; 2001.
10. **International Electrotechnical Commission.** IEC 62502:2010, *Analysis techniques for dependability—event tree analysis (ETA)*. 1st ed. Geneva: International Electrotechnical Commission; 2010.
11. **Leveson NG.** *Engineering a Safer World: Systems Thinking Applied to Safety (Engineering Systems)*. Cambridge, MA: MIT Press, 2012.
12. **Software Engineering Institute.** Overview of Team Software Process (TSP). Available at www.sei.cmu.edu/tsp. Accessed February 10, 2015.
13. **Jetley R, Jones P, Anderson P.** *Static Analysis of Medical Device Software Using CodeSonar*. Proceedings of the 2008 ACM SIGPLAN Workshop on Static Analysis, June 7–13, 2008, Tucson, AZ. New York: Association for Computing Machinery; 2008:22–9.
14. **Mäder P, Jones P, Zhang Y, Cleland-Huang J.** Strategic Traceability for Safety-Critical Projects. *IEEE Software*. 2013;30(3):58–66.
15. **Goodenough JB, Weinstock CB, Klein AZ.** Toward a Theory of Assurance Case Confidence. Available at: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=28067. Accessed February 10, 2015.

ANSI/AAMI ES60601-1:2005

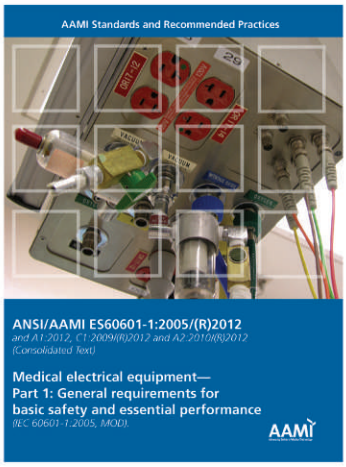
Medical electrical equipment—Part 1: General requirements for basic safety and essential performance (includes Amendment 1:2012)

This is the consolidated text of 60601-1 and the 2012 Amendment. Done in track changes so you can easily see the nearly 500 changes made by the Amendment.

Available in multiple formats, including the popular travel-size.

Order Code: 606011, 606011-PDF, 606011-CD, or 606011-PE
List $660 / AAMI member $396

Only need the Amendment?
Order Code: 606011-A or 606011-A-PDF
List $170 / AAMI member $102



Measuring Only 5.5" x 7" Don't Miss the Travel-size format!

ANSI/AAMI/IEC 60601-1-8:2006 & A1:2012

Medical Electrical Equipment—Part 1-8: General requirements for basic safety and essential performance — Collateral Standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems

This defines the roles, responsibilities and activities that are necessary for risk management of IT-networks incorporating medical devices to address safety, effectiveness, and data and system security.

Order code: 6010108 or 6010108-PDF
List $560 / AAMI member $336

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

SOURCE CODE: PB

AAMI
Advancing Safety in Healthcare Technology