Technical Information Report

AAMI TIR38: 2019

Medical device safety assurance case guidance

AAMI
Advancing Safety in Health Technology

Medical device safety assurance case guidance

Approved 25 January 2019 by
AAMI

Abstract: Provides guidance on how to complete an Assurance Case Report in order to comply with the new additional FDA pre-market requirements for infusion pumps. Includes a detailed but strictly hypothetical example from the medical device domain.

Keywords: safety claim, risk management, infusion pumps, quality systems

AAMI Technical Information Report

A technical information report (TIR) is a publication of the Association for the Advancement of Medical Instrumentation (AAMI) Standards Board that addresses a particular aspect of medical technology.

Although the material presented in a TIR may need further evaluation by experts, releasing the information is valuable because the industry and the professions have an immediate need for it.

A TIR differs markedly from a standard or recommended practice, and readers should understand the differences between these documents.

Standards and recommended practices are subject to a formal process of committee approval, public review, and resolution of all comments. This process of consensus is supervised by the AAMI Standards Board and, in the case of American National Standards, by the American National Standards Institute.

A TIR is not subject to the same formal approval process as a standard. However, a TIR is approved for distribution by a technical committee and the AAMI Standards Board.

Another difference is that, although both standards and TIRs are reviewed periodically, a standard must be acted on—reaffirmed, revised, or withdrawn—and the action formally approved usually every five years but at least every 10 years and a TIR must be acted on every three years.

A TIR may be developed because it is more responsive to underlying safety or performance issues than a standard or recommended practice, or because achieving consensus is extremely difficult or unlikely. Unlike a standard, a TIR permits the inclusion of differing viewpoints on technical issues.

CAUTION NOTICE: This AAMI TIR may be revised or withdrawn at any time. Because it addresses a rapidly evolving field or technology, readers are cautioned to ensure that they have also considered information that may be more recent than this document.

All standards, recommended practices, technical information reports, and other types of technical documents developed by AAMI are *voluntary*, and their application is solely within the discretion and professional judgment of the user of the document. Occasionally, voluntary technical documents are adopted by government regulatory agencies or procurement authorities, in which case the adopting agency is responsible for enforcement of its rules and regulations.

Comments on this technical information report are invited and should be sent to AAMI, Attn: Standards Department, 901 N Glebe Road, Suite 300, Arlington, VA 22203.

Published by

AAMI
901 N Glebe Road, Suite 300
Arlington, VA 22203
www.aami.org

Printed in the United States of America

ISBN 978-1-57020-712-9

Contents

Page

Figures

Committee representation

Association for the Advancement of Medical Instrumentation
Infusion Device Committee

This AAMI Technical Information Report (TIR) was developed and approved by the AAMI Infusion Device Committee.

At the time this document was published, the **AAMI Infusion Device Committee** had the following members:

Cochair: Peter Rech

Members:
Pat Baird, Philips
Michael Brady, Toxikon Corporation
Nick Chozos, Adelard LLP
Blake Collins, Christiana Care Health Srvcs
Bill Day, Near Future Corp
Sherman Eagles, SoftwareCPR
Gary Freitag, Integer
Robert Hijazi, John D Dingell VA Medical Center
Jamie Irizarry, Children's Hospital of Philadelphia
Jim Kamke, Baxter Healthcare Corporation
Lee Leichter, P/L Biomedical
Juuso Leinonen, ECRI Institute
Alan Lipschultz, HealthCare Technology Consulting LLC
Jim Milostan, Medical Specialties Distributors LLC
Marc Neubauer, FDA/CDRH
Shawn O'Connell, B Braun of America Inc
Ben Powers, Ivenix Inc
Peter Rech, Smiths Medical
Andy Rich, Children's Hospital of Philadelphia
James Shults, ICU Medical Inc
Jim Ward, Amgen Inc
Fubin Wu, GessNet

Alternates:
Steve Anthony, Ivenix Inc
Michael Brown, B Braun of America Inc
John Dumas, AbbVie
Delmont Fredricks, Smiths Medical
Christine Frysz, Integer
Thomas Johnson, AbbVie
John Learish, Christiana Care Health Srvcs
Avital Merl, Becton Dickinson & Company
Nayan Patel, Amgen Inc
Erin Sparnon, ECRI Institute
Joyce Young-Stewart, Baxter Healthcare Corporation
Kent Abrahamson, AbbVie

NOTE--Participation by federal agency representatives in the development of this document does not constitute endorsement by the federal government or any of its agencies.

Foreword

A challenge with ANSI/AAMI/ISO 14971 is that it does not require a formal, organized summary of why the device is safe for its intended use. While ANSI/AAMI/ISO 14971 requires a series of discrete analyses and reports, there is no overview document that provides a roadmap to product risk. Although ANSI/AAMI/ISO 14971 requires a risk management report, this report is at a very high level. The requirements of ANSI/AAMI/ISO 14971 ensure that an overall residual risk evaluation has taken place, and that a risk management report ensures that:

a) the risk management plan has been appropriately implemented;

b) appropriate methods are in place to obtain relevant production and post-production information.

Thus, a risk management file created according to these tenets would not actually summarize the findings and actions from risk management activities, only state that they exist; it would not *tell the story of safety*.

A reviewer is often faced with thousands of pages of design documentation, with no overall summary as to why the designers believe the product is safe. Additionally, if the reviewer is interested in a particular issue, there is no roadmap to finding that issue within the design documentation. The set of risk management documents may contain discrete elements with no traceability as to how they fit together.

ISO/IEC 15026-2:2011 defines it as:

> An assurance case includes a top-level claim for a property of a system or product (or set of claims), systematic argumentation regarding this claim, and the evidence and explicit assumptions that underlie this argumentation. Arguing through multiple levels of subordinate claims, this structured argumentation connects the top-level claim to the evidence and assumptions.

An assurance case is a systematic, structured methodology for supporting a stated claim. The claim may be related to safety, reliability, maintainability, security, etc. A safety assurance case is an assurance case with a top-level claim of safety.

The medical device safety assurance case outlined in this technical information report (TIR) provides a comprehensive and organized summary of product risk and the mitigations therein.

The medical device safety assurance case functions to mitigate the following three arguments wherein risk may be produced within the context of the device's intended use:

1. Design requirements and specifications are adequate for the device's intended use and have been adequately verified and validated.

2. All reasonably foreseeable, worst-case hazards are identified and the associated risk is mitigated and/or controlled, with supporting evidence, such that the device is safe for its intended use.

3. The device's reliability is established, with supporting evidence, at a system and/or component level commensurate with the level of risk associated with the device's intended use.

This TIR provides information useful to creating and maintaining safety assurance cases for medical devices, including drug delivery combination products. It does this in the context of ANSI/AAMI/ISO 14971 and ISO/IEC 15026-2. A safety assurance case serves as a detailed risk management report that, as part of the risk management file, should be maintained according to the requirements of ANSI/AAMI/ISO 14971. There is additional discussion about the relationship between risk management and safety assurance cases in clause 7.

While the examples used in this TIR are based on infusion pumps, the same principles apply to developing safety assurance cases for any medical device, including drug delivery combination products.

Suggestions for improving this recommended practice are invited. Comments and suggested revisions should be sent to Technical Programs, AAMI, 901 N Glebe Road, Suite 300, Arlington, VA 22203.

NOTE—This foreword does not contain provisions of the AAMI TIR38, *Medical device safety assurance case guidance* (AAMI TIR38:2019), but it does provide important information about the development and intended use of the document.

Introduction

Risk management for medical devices begins at product conception and continues as an active process throughout product realization, maintenance, and retirement. The importance of clear and thorough documentation that is maintained throughout the lifecycle cannot be overemphasized.

Traditional risk analysis tools such as hazards analysis, fault tree analysis, failure modes and effect analysis, each provide useful insights into the risk profile of a particular system / product / process. However, none of these tools tells the complete, integrated safety story. These traditional tools are each a chapter in the overall story, each speaking to a certain aspect of *risk*, but few techniques are specifically tasked to structure the summary of a risk management file demonstrating *safety*. Without this story, it is difficult to know if risk management is complete.

There is a subtle difference between a risk-based focus and a safety-based focus. Risk management is required to support claims of safety, but it is not clear that they alone are always sufficient to demonstrate safety. Much like the relationship between verification and validation, the goals of risk management and safety assurance cases are related but distinctly different.

The purpose of a medical device safety assurance case ("safety case" in this document) is to tell this story of safety to the original designers, regulators, maintainers, integrators, and potentially even customers. The safety case accomplishes this storytelling by taking the information developed under risk management processes and explaining what decisions were made, why the decisions are reasonable in the context of the intended use of the device, and where the reviewer can look for additional information.

A safety case explains how:

1) all reasonably foreseeable hazards have been identified for the device;

2) hazards / hazardous situations have been effectively mitigated;

3) evidence supporting effective mitigations is adequate;

4) evidence demonstrates that mitigations will remain effective over the product's lifetime;

5) a robust process has been followed throughout steps 1 through 4 and the risk is outweighed by the benefit of the product.

Items 1 through 3 are described in detail in ANSI/AAMI/ISO 14971 and item 5, robustness of the process applied, is related to the quality system in general (i.e. linking elements of design control to support the safety case claims).

A safety case meets these goals by explaining the elements and documents of the applied risk management process and why the process has been robust (i.e. in control and with a high level of assurance) by making implicit design decisions explicit and by acting as a structured index in the design files.

To realize the full benefit, the Safety Case development process must be ongoing during product design. In this way, the designers can appropriately address new hazards and faults as they arise and better inform and document the design tradeoffs and choices they make.

Medical device safety assurance case guidance

1 Purpose

The purpose of this TIR is to provide guidance on the development of safety cases for the design of a medical device. It is intended primarily for product developers, quality assurance, regulatory reviewers and auditors – anyone who requires a clear and complete story regarding the safety of a medical device's design.

Even though drug delivery devices have been primarily used within examples shown, the same definitions and approach can be used for any medical device.

2 Scope

This TIR is a safety case development reference for medical device design. The TIR is intended to provide a framework within which experience, insight, and judgment are applied systematically to assure and document the safety of a medical device's design.

This TIR is not intended to be a prescriptive guidance for the development and documentation of safety cases. This TIR also does not address all necessary activities required to assure that the device, as presented to the user / patient, is fit for use.

In order to simplify this TIR, this guidance has an assumption that the reader is familiar with the hazards for a particular type of product and is not designing a new-to-world product. While the techniques in this guidance can be used for innovative products, this TIR is targeted at existing, well understood products.

Finally, this guidance is written with a focus on "design safety assurance", emphasizing design inputs, design outputs, verification, and validation. The same techniques can be used for developing a "good manufacturing practice (GMP) safety assurance", which accounts for verification and validation of the manufacturing and quality process controls. It is suggested, though not required, that a safety case include both aspects of the design and GMP elements of the medical device in order to effectively argue that the device as a system is safe and effective.

3 Relationship to other standards and FDA guidance

The ISO/IEC 15026 series of standards defines terms, establishes concepts and their relationships, and specifies minimum requirements for the structure and content of an assurance case. It is recommended that the standard be followed throughout the development of a safety case.

— ISO/IEC 15026-1:2013, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

— ISO/IEC 15026-2:2011, *Systems and software engineering — Systems and software assurance — Part 2: Assurance case*

The ISO/IEC 15026 series does not currently include information that is specific to medical devices; for example, a common question on how to integrate existing medical device risk management processes with safety cases is not addressed by ISO/IEC 15026. This TIR attempts to bridge that gap.

— ANSI/AAMI/ISO 14971:2007/(R)2016, *Medical devices – Application of risk management to medical devices*

Risk management is the foundation for safety case development. The ANSI/AAMI/ISO 14971 standard provides guidance on the processes that can be used to obtain the necessary information to complete a safety case. However, it should be noted that there is additional work beyond ANSI/AAMI/ISO 14971 that is needed to complete a safety case. This TIR attempts to correlate traditional elements of risk management outlined in ANSI/AAMI/ISO 14971 with the process of developing and maintaining a successful safety assurance case.

— IEC TR 80001-2-9:2017, *Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities*

