



Technical Specification

ISO/TS 81001-2-1

Health software and health IT systems safety, effectiveness and security —

Part 2-1: Coordination — Guidance and requirements for the use of assurance cases for safety and security

*Sécurité, efficacité et sûreté des logiciels de santé et des systèmes
TI de santé —*

*Partie 2-1: Coordination — Orientations et exigences relatives à
l'utilisation des dossiers d'assurance en matière de sûreté et de
sécurité*

**First edition
2025-01**



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	2
3 Terms and definitions	2
4 Assurance case	4
4.1 Concepts.....	4
4.2 Healthcare delivery organizations (HDO).....	4
4.3 Manufacturers.....	5
4.4 Other stakeholders.....	5
4.5 Benefits.....	5
4.6 Requirements.....	6
5 General requirements and recommendations	6
5.1 Principles.....	6
5.2 Assurance case development process.....	6
5.2.1 General.....	6
5.2.2 Step 1: identify the goal.....	7
5.2.3 Step 2: define the basis of the goal.....	7
5.2.4 Step 3: identify the strategy.....	8
5.2.5 Step 4: define the basis on which the strategy is stated.....	8
5.2.6 Step 5: elaborate the strategy.....	8
5.2.7 Step 6: identify the solution.....	8
5.3 General considerations.....	8
5.4 Argument considerations.....	9
5.5 Evidence considerations.....	9
5.6 Notation.....	10
5.6.1 General.....	10
5.6.2 Goal.....	10
5.6.3 Strategy.....	10
5.6.4 Solution.....	10
5.6.5 Context.....	11
5.6.6 Assumption.....	11
5.6.7 Justification.....	11
5.6.8 SupportedBy relationship.....	12
5.6.9 InContextOf relationship.....	12
6 Developing an assurance case using GSN	12
6.1 General.....	12
6.2 Step 1: identify the goal.....	13
6.3 Step 2: define the basis on which the goal is stated.....	13
6.4 Step 3: identify the strategy used to support the goal.....	13
6.5 Step 4: define the basis on which the strategy is stated.....	14
6.6 Step 5: elaborate the strategy.....	14
6.7 Repeat Step 2: define the basis on which the goal is stated.....	15
6.8 Repeat Step 4: define the basis on which the strategy is stated.....	16
6.9 Step 6: identify the basic solution.....	17
7 Assurance case change management	18
8 Security assurance case	18
Annex A (informative) Generic risk-based HIT assurance case pattern	20
Annex B (informative) IEC 80001-1 Compliance assurance case pattern	23
Annex C (informative) AI assurance case pattern	31

ISO/TS 81001-2-1:2025(en)

Annex D (informative) **Security assurance case pattern**..... 43
Annex E (informative) **Assurance notation cross reference** 44
Annex F (informative) **Summary of assurance case requirements relative to organizations**..... 45
Bibliography..... 46

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared jointly by Technical Committee ISO/TC 215, *Health informatics*, and Technical Committee IEC/TC 62, *Medical equipment, software, and systems*, Subcommittee SC A, *Common aspects of medical equipment, software, and systems*.

A list of all parts in the ISO/IEC 81001 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

ISO 81001-1 provides the principles, concepts, terms and definitions for health software and health IT systems, and the key properties of safety, effectiveness and security, across the full life cycle. ISO 81001-1 and all parts of the ISO/IEC 81001 series documents are applicable to stakeholders such as health software manufacturers (including medical device manufacturers) and healthcare delivery organizations (HDOs). This document provides guidance in developing comprehensible and compelling assurance cases in support of safe, secure and effective deployment of health software and health IT systems.

While the benefits of digital health support are widely accepted, the potential for inadvertent and adverse impacts on safety, effectiveness and security caused by health software and health IT systems is also becoming more apparent. Today's sophisticated health software and health IT systems provide advanced levels of decision support and integrate patient data from multiple sources across organizational lines, and across the continuum of care. This creates benefits to the patient and healthcare system, but it also increases the likelihood of software-induced adverse events causing harm to both patients and healthcare organizations. Design flaws, coding errors, security vulnerabilities, incorrect implementation or configuration, data integrity issues, faults in decision support tools, poor alignment with clinical workflows and improper maintenance and use of health software and health IT systems are examples of events with the potential to cause harm. Managing safety, effectiveness and security for health software and health IT systems (including medical devices), requires a comprehensive and coordinated approach to optimizing these three properties.

As health software and health IT systems move through their life cycle stages, multiple organizations are involved. As described in ISO 81001-1, these organizations need to communicate and share information to properly assess and manage the safety, effectiveness, and security in carrying out their respective roles. It is important that this transfer of knowledge and information is sufficiently formalized and predictable so that different stakeholders can communicate and manage these risks in a timely and effective way across life cycle stages and between roles.

Assurance cases are therefore useful tools for communicating risk across the life cycle of health IT systems, given the rigour that is required within, and the inter-dependence of, the different organizations involved at the various life cycle steps. Manufacturers can utilize an assurance case to communicate the risks associated with their products to an HDO. HDOs can build upon the information the manufacturer has provided and develop their assurance case as the product is integrated, configured, and implemented for use within their particular sociotechnical ecosystem context. In this way, assurance cases provide a continuous thread for all roles involved during the life cycle in managing the collective risks of all the components across the health IT infrastructure, including the health software, medical devices and other health IT systems that make up these complex sociotechnical ecosystems. Additionally, assurance case reports can be generated for the purpose of communicating risks from one stakeholder to another as ownership of a health IT systems changes.

IEC 80001-1 provides the roles, responsibilities, and activities necessary for effective risk management to minimize the impact or likelihood of such events and establishes the concept of an assurance case as the principal artefact to demonstrate that the application of risk management has been effective before, during and after the implementation of a health IT system within a health IT infrastructure. The assurance case is the principal mechanism for demonstrating compliance with IEC 80001-1.

Additionally, an assurance case can demonstrate confidence in the safety and security properties of a system throughout its lifecycle and a means for demonstrating the relationship, correlation and improved analysis of safety, security, and effectiveness.

The purpose of this document is to:

- provide guidance to those organisations that are responsible for addressing the requirements of IEC 80001-1 and illustrate how those requirements can be demonstrated through the use of an assurance case;
- provide guidance to illustrate to organisations how the concept of an assurance case can be used to facilitate effective dialogue and management of health software (including medical devices) and health IT system safety and security risks across organisational boundaries and between all stakeholders.

ISO/TS 81001-2-1:2025(en)

NOTE The 6-step method that is presented in [5.2](#) is reproduced from original work published in 'The Six-Step Method for Developing Goal Structures' in Reference [\[9\]](#). The material is reproduced here with the permission of the original author, who retains rights to the material.

Health software and health IT systems safety, effectiveness and security —

Part 2-1:

Coordination — Guidance and requirements for the use of assurance cases for safety and security

1 Scope

This document establishes requirements and gives guidance on assurance case framework for healthcare delivery organizations (HDOs) and for health software and medical device manufacturers (MDMs) and can be used to support the communication and information transfer between all parties. An assurance case can be used to communicate information and knowledge about different risks to other roles.

This document establishes:

- an assurance case framework for HDOs and health software and MDMs for identifying, developing, interpreting, updating and maintaining assurance cases.
- one of the possible means to bridge the gap between manufacturers and HDOs in providing adequate information to support the HDOs risk management of IT-networks;
- best practice by leveraging ISO/IEC/IEEE 15026-2 and other standards to identify key considerations and for the structure and contents of an assurance case, e.g. iterative and continuous approaches;
- example structure, method and format to improve the consistency and comparability of assurance cases.

This document is applicable to all parties involved in the health software and health IT systems life cycle, including:

- a) organizations, health informatics professionals and clinical leaders specifying, acquiring, designing, developing, integrating, implementing and operating health software and health IT systems, for example health software developers and MDMs, system integrators, system administrators (including cloud and other IT service providers);
- b) healthcare service delivery organizations, healthcare providers and others who use health software and health IT systems in providing health services;
- c) governments, health system funders, monitoring agencies, professional organizations and customers seeking confidence in an organization's ability to consistently provide safe, effective and secure health software, health IT systems and services;
- d) organizations and interested parties seeking to improve communication in managing safety, effectiveness and security risks through a common understanding of the concepts and terminology used in safety, effectiveness and security management;
- e) providers of training, assessment or advice in safety, effectiveness and security risk management for health software and health IT systems;
- f) developers of related safety, effectiveness and security standards.

This document is for use by organizations and people who build, acquire, operate, maintain, use or decommission health software and health IT systems (including medical devices). It is applicable to all organizations involved, regardless of size, complexity or business model.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security — Part 1: Principles and concepts*