Technical Specification

# ISO/TS 81001-2-1

First edition
2025-01

# 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*



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



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

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.

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*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 81001-1:2021 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

**3.1**
**assumption**
intentionally unsubstantiated statement

Note 1 to entry: An assumption is used in the reasoning of a goal.

Note 2 to entry: Adapted from Reference [10].

**3.2**
**assurance**
grounds for justified confidence that a goal has been or will be achieved

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.1.1, modified — "claim" was replaced by "goal".]

**3.3**
**argument**
connected series of goals intended to establish an overall goal

Note 1 to entry: Adapted from Reference [10].

**3.4**
**confidence**
proposition being asserted by the author that is a true or false statement

Note 1 to entry: Adapted from Reference [10].

**3.5**
**goal**
true-false statement about the limitations on the values of an unambiguously defined property – called the claim's property – and limitations on the uncertainty of the property's values falling within these limitations during the claim's duration of applicability under stated conditions

Note 1 to entry: Uncertainties may also be associated with the duration of applicability and the stated conditions.

Note 2 to entry: A claim potentially contains the following:

— property of the system-of-interest;

— limitations on the value of the property associated with the claim (e.g. on its range);

— limitations on the uncertainty of the property value meeting its limitations;

— limitations on duration of claim's applicability;

— duration-related uncertainty;

— limitations on conditions associated with the claim; and

— condition-related uncertainty.

Note 3 to entry: The term “limitations” is used to fit the many situations that can exist. Values can be a single value or multiple single values, a range of values or multiple ranges of values, and can be multi-dimensional. The boundaries of these limitations are sometimes not sharp, e.g. they can involve probability distributions and can be incremental.

Note 4 to entry: The term ‘claim’ is sometimes used as a synonym for ‘goal’.

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.1.4, modified — The preferred term “claim” was changed to “goal”; Note 4 to entry was added.]

**3.6**
**context**
reference to the system documentation towards an assertion regarding capabilities and properties external to the system

Note 1 to entry: A context can be justified by the intended use and notably the intended operational environment of the respective system.

Note 2 to entry: A context can be used in the reasoning of a strategy.

Note 3 to entry: Adapted from Reference [16].

**3.7**
**evidence**
directly measurable characteristics of a process and/or product that represent objective, demonstrable proof that a specific activity satisfied a specific requirement

[SOURCE: ISO/IEC 21827:2008, 3.19]



**3.8**
**justification**
type of claim which is raised as part of an assurance case and which is not further refined

**3.9**
**solution**
reference to an artefact that points to a technical implementation



Note 1 to entry: A solution can be used in the reasoning of a strategy.

**3.10**
**strategy**
argument demonstrating plausibility of one (or multiple) goal(s) based on related support in a context, based on assumptions and using evidence, justifications and solutions and other sub goals (which can then not be supported by that strategy instance to ensure cycle-free reasoning)

**3.11**
**responsibility agreement**
document(s) that together fully define the responsibilities of all stakeholders

Note 1 to entry: This agreement can be a legal document, e.g. a contract.

[SOURCE: ISO 81001-1:2021, 3.1.9]

**3.12**
**security control**
management, operational and technical controls (i.e. safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information

[SOURCE: ISO 12812-1:2017, 3.54]

**3.13**
**security pattern**
means of documenting and reusing successful argument structures

Note 1 to entry: Adapted from Reference [15].

# 4 Assurance case

## 4.1 Concepts

Assurance that a health IT system achieves certain objectives is particularly important when the system and its interaction with the environment are complex and evolving. Assurance cases establish goal(s) that relate to selected properties of the health IT system and argue for the truth of those goals(s).

Assurance cases are generally developed to support goals in areas such as safety, reliability, maintainability, human factors, operability, and security. Whilst this document focuses on safety and security, assurance case methods are applicable to any property of a system. These assurance cases are often called by more specific names, e.g. safety case or dependability case. ISO/IEC/IEEE 15026-1 provides concepts, terminology, background and a list of standards related to assurance cases.

An assurance case is a structured, solution-based argument used to demonstrate confidence that a system holds a particular critical property.

An argument is a connected, hierarchical series of goals intended to establish an overall goal. The argument in an assurance case shows how a high-level goal is supported by a number of sub goals, which, in turn are supported by detailed presentation of a solution(s). It is the combination of goals and solution that provide confidence in the overall high-level goal made for the characteristic of the system.

A solution which is defined as scientific fact, or empirical outcome, provides a basis that demonstrates that the goal has been achieved. An argument without a solution is unfounded whilst a solution presented out of the context of an argument is unexplained.



Presenting the argument and solution in a structured way reduces the likelihood of uncertainty and allows for a better analysis of the achievement of the set of objectives (the goals).

Additional assurance case concepts such as assumptions, justifications and context enable other factors and considerations to be expressed which will support the interpretation and the validity of the assurance case.

## 4.2 Healthcare delivery organizations (HDO)

An assurance case can be established for any element of a health IT system, the health IT system itself and the entire health IT infrastructure, addressing any network component, e.g. the radiology network, network communication components, medical devices, accessories and even components of devices.

HDOs can use the assurance case, as outlined in this document, to form part of a broader assurance case addressing additional critical properties such as safety, reliability, maintainability, etc.

HDO's can use this document for one or more of the following:

a) support the understanding and communication of safety and security risks associated with components of the health IT system that are provided by third party organizations;

b) assess and manage safety and security risks associated with the deployment and use of health IT systems and health IT infrastructures in their own organizations;

c) demonstrate their own conformity with IEC 80001-1 and ISO 81001-1.

## 4.3 Manufacturers

An assurance case is an important tool for providing HDOs with the appropriate level of information about the safety and security characteristics of a manufacturer's product(s) to support the HDOs' risk management of their health IT systems (that can incorporate health software products including medical devices), which are being implemented in the HDOs' health IT infrastructure.

This document also provides guidance to manufacturers in developing a security case to demonstrate confidence in the achievement of IEC/TS 81001-2-2[1)].

An assurance case can be treated as a 'living artefact' which begins at the outset of the system/software development lifecycle (SDLC) and is continuously developed and updated during design, production and operation of the manufacturer's product(s).

The assurance case may act as a supporting document to the manufacturer disclosure statement for medical device security (MDS2).

## 4.4 Other stakeholders

Stakeholders (involved in conformity assessment, certification, regulation, acquisition or audit) can evaluate the assurance case to determine the extent of achievement of the top-level goal (e.g. that the health IT product is safe or secure) and whether this achievement is demonstrated within the allowable uncertainty or risk and any related consequences. The results regarding the top-level goal and its support along with related uncertainties and consequences constitute a basis for rationally managing risk and aiding in decision making.

This document is also for use by organizations who build, acquire, operate, maintain, use or decommission health software and health IT systems (including medical devices), as well as by those creating standards addressing safety, effectiveness and security of health IT systems. It is applicable to all organizations involved, regardless of their size, complexity, or business model.

The quality of artefacts gathered and documented during the development of the assurance case should be agreed to and documented as part of a responsibility agreement between the relevant stakeholders (as currently practised by security assurance cases). This document will provide guidance and methodology, using specific notations, to support, develop and interpret assurance cases in a systematic manner.



## 4.5 Benefits

The assurance case has been commonly applied to the safety domain, specifically addressing safety concerns for systems, however the use of an assurance case has expanded and nowadays addresses other critical properties such as dependability, reliability, and security across a range of safety critical domains such as automotive, railway, defence and aviation. An assurance case is called a safety case when used to argue the safety of a system. Similarly, they are referred to as assurance cases and dependability cases when arguing respectively.

A significant benefit of an assurance case is that it provides a mechanism to facilitate effective communication of the particular characteristics of a product between stakeholders. The rationale, the justification for the relevance of the rationale and its supporting confirmatory evidence can be presented and appraised in a systematic way.

As a manufacturer, an assurance case can be used to establish confidence that the requirements of a standard have been satisfied. An argument reflecting the architecture of a standard can guide a manufacturer in generating and collating supporting evidence; gaps or weaknesses in the evidence will become apparent.

If a manufacturer incorporates a third-party product in their own product, an assurance case can be used to communicate third party assurance requirements and also to collate and integrate assurance evidence associated with the third party product into the manufacturer's product assurance case.

1) Under preparation. Stage at the time of publication: IEC/CD TS 81001-2-2.

The concept of an assurance case model or pattern encourages soundness and completeness as it can introduce efficiency and improve the assurance culture within an organization by providing a framework that supports consistency in the assurance process.

The impact of changes or modifications to a product can be more readily assessed if there is an assurance case established for the product. For example, if software changes are proposed to a functional module, the need for and significance of supporting test evidence required to maintain the integrity of that function will be apparent. This contributes to pro-active risk management.

The philosophy of an assurance case provides flexibility to enable the rigour of the assurance case and its supporting evidence base to be proportionate to the risk profile of the product. Justifications or assumptions can be presented to explain why an element of an assurance argument or evidence is not required given the assessed risk profile.

Managing the assurance case as a living artefact provides on-going visibility of assurance maturity and an opportunity to influence its development and final sufficiency. Contradictions in the argument or gaps in the evidence will be revealed sooner in the lifecycle with greater opportunity for correction. The cost of corrective change to a product is proportionate to the phase at which the correction is made, i.e. it is cheaper to correct requirement deficiencies before product design then it is correct them post product implementation.

### 4.6 Requirements

The following requirements apply when an organization develops an assurance case:

— Goals: The organization shall define one or more goal(s) to express the assurance claim that is being made as part of a new assurance case.

— Justification: The organization shall justify the rationale for the definition of the top-level goal.

— Argument: The organization shall express arguments that logically link the defined goal(s) to the solutions.

— Solutions: The organization shall provide a body of evidence that demonstrates that the goal(s) has been satisfied.



## 5 General requirements and recommendations

### 5.1 Principles

The principal objective of an assurance case is to present a well-organised and reasoned proposition, based on objective evidence, that a system is acceptably safe and secure in a given context.

The development of an assurance case is an iterative process and is aligned and integrated within the system development and deployment lifecycle. Formalisation of an assurance case occurs at key lifecycle milestones and supports stakeholder decision making, for example at the point of clinical deployment or system modification.

### 5.2 Assurance case development process

#### 5.2.1 General

An assurance case can be developed following many different approaches; it is not the purpose of this document to prescribe a specific approach. However, the process for developing safety cases as published in Reference [9] and as incorporated into the [SCSC-141C] Goal Structuring Notation Community Standard[10] has been adopted. This approach, referred to as the “6-step method” is presented in Figure 1 and described in 5.2.2 to 5.2.7.