INTERNATIONAL STANDARD

ISO/IEC 15026-2

First edition
2011-02-15

Systems and software engineering — Systems and software assurance —

Part 2: Assurance case

Ingénierie du logiciel et des systèmes — Assurance du logiciel et des systèmes —

Partie 2: Cas d'assurance

Reference number
ISO/IEC 15026-2:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15026-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

ISO/IEC 15026 consists of the following parts, under the general title *Systems and software engineering — Systems and software assurance*:

— *Part 1: Concepts and vocabulary* [Technical Report]

— *Part 2: Assurance case*

System integrity levels and assurance in the life cycle will form the subjects of future parts.

Introduction

The purpose of this part of ISO/IEC 15026 is to ensure the existence of types of assurance case content and restrictions on assurance case structure, thereby improving consistency and comparability among instances of assurance cases and facilitating stakeholder communications, engineering decisions, and other uses of assurance cases.

Existing standards addressing different application areas and topics related to assurance cases might use differing terminology and concepts when addressing common themes. This part of ISO/IEC 15026 is based on experience drawn from these many specialized standards and guidelines. It is applicable to any property of a system or product.

NOTE It is intended that ISO/IEC TR 15026-1 will be transformed into an International Standard.

In addition to concepts and terminology, ISO/IEC TR 15026-1 provides background and a list of related standards that could be useful in understanding and using this part of ISO/IEC 15026. Assurance cases are generally developed to support claims in areas such as safety, reliability, maintainability, human factors, operability, and security, although these assurance cases are often called by more specific names, e.g. safety case or reliability and maintainability (R&M) case.

This part of ISO/IEC 15026 uses the terminology and concepts consistent with ISO/IEC 12207:2008, ISO/IEC 15288:2008, and ISO/IEC 15289:2006. This part of ISO/IEC 15026 does not presume or require that it is applied in conjunction with ISO/IEC 12207:2008 or ISO/IEC 15288:2008.

Systems and software engineering — Systems and software assurance —

Part 2:
Assurance case

1 Scope

This part of ISO/IEC 15026 specifies minimum requirements for the structure and contents of an assurance case. 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.

This part of ISO/IEC 15026 does not place requirements on the quality of the contents of an assurance case. Rather, it places requirements on the existence of the contents and structure of an assurance case. While several notations and slightly varying terminologies are currently used in practice, this part of ISO/IEC 15026 does not require the use of a particular terminology or graphical representation. Likewise, it places no requirements on the means of physical implementation of the data, including no requirements for redundancy or co-location.

2 Conformance

An assurance case conforms to this part of ISO/IEC 15026 if it meets the requirements of Clause 6 and Clause 7.

3 Normative references

The following referenced documents are indispensable for the application of this document.

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

ISO/IEC 15289, *Systems and software engineering — Content of systems and software life cycle process information products (Documentation)*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC TR 15026-1 apply.

5 Use of this part of ISO/IEC 15026

System- or product-related needs and requirements, interactions of the system or product with its environment, and real-world events and conditions can result in an objective to obtain assurance that the system or product achieves certain claims. To meet this objective, assurance cases support these claims concerning selected

properties of the system or product. While these properties may be selected for any reason, one commonly selects them because they are risk-related and high confidence is needed in their realization in a system or product. The results of developing an assurance case are the values and their uncertainties established for each top-level claim's property. The uncertainties regarding the truth or falsehood of these claims are an essential conclusion of the assurance case.

Stakeholders can evaluate the assurance case to determine the extent of achievement of the top-level claim by the system or product and whether this achievement is shown within the allowable uncertainty or risk and any related consequences. The results regarding the top-level claim and its support along with related uncertainties and consequences constitute a basis for rationally managing risk, achieving grounds for appropriate confidence, and aiding in decision making.

Generally, stakeholders can make better decisions about a system or product when the uncertainties of conclusions regarding these properties are reduced. While an assurance case is useful for decision-making by knowledgeable stakeholders (e.g., developers and service providers), often the primary motivation for an assurance case is to support crucial decisions by stakeholders without this background, such as those involved in certification, regulation, acquisition, or audit of the system.

How the assurance case is used and the amount of effort devoted to its formulation can vary greatly due to the stringency of the properties selected, the applicable duration of the claim, the degree of uncertainty, the scope of the assumptions made, and the risk or consequences involved. Thus, the content needed in an assurance case varies depending on the stakeholder and evaluation context. For example, depending on the system requirements and the property specified by the top-level claim, an assurance case could be used for validation or verification purposes.

This part of ISO/IEC 15026 is intended to be utilized while developing and maintaining assurance cases. When developing a new system or product or making a major change, the development of the assurance case should be integral within processes, plans, engineering, activities, and decisions related to the development of the system or product of interest.

In order to provide the needed flexibility and cover the many areas where assurance cases are utilized, this part of this International Standard uses a general approach and calls for a mapping between it and the contents of any conforming assurance case. The requirements for this mapping are in 7.2.

NOTE 1 The term “uncertainty” is used as a general term to mean "lack of certainty." Different communities restrict the application of this term to limited usage, e.g., to predictions of future events, to physical measurements already made, or to unknowns, but in this International Standard the term applies to any uncertainty.

NOTE 2 Selecting the top-level claim and the properties it involves is not restricted by this part of ISO/IEC 15026 but may be specified in stakeholder requirements or established by an approval authority for the system or product. Top-level claims might be a portion of the total requirements and specification but might be something internal to the system, related to something the system depends upon, or only indirectly related to the primary system of interest.

NOTE 3 Limitations of a system’s or product’s assurance case should be reflected in the guidance; transition, operations, and maintenance documentation; training; operator and user aids; data collection capabilities; and services included in or accompanying the system or product. Knowledge of these limitations allows avoidance and recognition of violations of relevant assumptions or the conditions related to the top-level claims.

NOTE 4 The text often refers to a single assurance case or to a single top-level claim; however, a system or product may have multiple assurance cases, and an assurance case may have multiple top-level claims.

6 Structure and contents of an assurance case

6.1 General

This part of ISO/IEC 15026’s description of assurance case structure and contents uses the term “components” for the main parts of an assurance case and describes the relationships among these components. The following general requirements apply:

a) The components of an assurance case shall be unambiguous, identifiable, and accessible.

NOTE Ambiguity may be avoided by associating a component with information on its context, such as: definitions of the terms used, the environment of the system or product, and the identities of entities responsible for a component's development or maintenance.

b) Each component shall be uniquely identified and shall be able to have its origin identified, its history ascertained, and its integrity assured.

c) For each component, the component's contents, the information related to it, and the other components with which it has relationships shall be identifiable and accessible."

NOTE For each component, its description and needed other components, e.g., evidence for claims and related information such as test case results, are identifiable and accessible.

d) An assurance case shall contain the auxiliary contents required by ISO/IEC 15289 for this type of documentation.

NOTE This part of ISO/IEC 15026 places no restrictions on how these auxiliary contents are included and no requirement that the assurance case be a separate document.

6.2 Overall structure

The five principal components of an assurance case are claims, arguments, evidence, justifications, and assumptions.

Figure 1 describes the structure of assurance cases. It is not normative.

Claims

A claim is a proposition to be assured about the system of concern. It may be accompanied with auxiliary information such as the range of some date mentioned in the proposition or the uncertainty of the proposition.

Justifications, Arguments, Evidence and Assurance Cases

Justifications, arguments, evidence and assurance cases are defined mutually recursively in this figure.

Given a claim c, a justification j of c is a reason why c has been chosen.

Comment: Therefore, a justification is defined relative to a claim c. An argument (defined below) is also defined relative to a claim, but it is different from justification because a justification is a reason for the choice of a claim, while an argument is a reason why a claim is true.

Given a claim c and a set es of evidence, an argument that assures c using es is defined to be a reason why the truth of c is deduced from the main part of evidence in the set es.

Evidence is either a fact, a datum, an object, a claim or an assurance case. A claim is called an assumption if it appears in an assurance case as evidence. The main part of the evidence is defined according to the form of the evidence; if the evidence is either a fact, datum, object or a claim, its main part is itself; but if the evidence is an assurance case a_0, its main part is the claim of a_0.

Comment: It will be clarified below in this figure that the evidence of an assurance case is used by an argument of that assurance case to assure that its claim holds.

Comment: A claim appearing as evidence is called an assumption because such evidence is a proposition without any reason why it is true. When a reason for its truth is provided, it is expected that an assurance case, whose argument is that reason, is constructed and provided as the evidence instead of providing only the claim as evidence.

An assurance case is defined to be a quadruple of a claim c, a justification j of c, a set es of evidence and an argument g which assures c using es. Let $a = (c, j, es, g)$ be an assurance case; c is defined to be the claim of a; similarly, j is defined to be the justification of a, es to be the set of evidence of a, and g to be the argument of a.

Comment: The definition of assurance cases depends on that of arguments, the definition of arguments depends on that of evidence, and the definition of evidence depends on that of assurance cases. These definitions, however, are not circular, but mutually recursive with each other.

Comment: For mathematically oriented readers, the following recursive definition of the set of assurance cases might help. The set A of assurance cases and the set E of evidence are defined by the following recursive equations.

$$A_0 = C \times \{ j_0 \in J(c_0) \mid c_0 \in C \} \times \wp_f(E) \times \{ g_0 \in G(c_0, es_0) \mid c_0 \in C, es_0 \in \wp_f(E) \}$$

$$A = \{ (c, j, es, g) \in A_0 \mid j \in J(c), g \in G(c, es) \}$$

$$E = F + D + O + C + A$$

where

$J(c)$	is the set of all justifications for a claim c;
C	is the set of claims;
$\wp_f(E)$	is the set of all finite subsets of E (finite powerset of E);
$G(c_0, es_0)$	is the set of arguments which assures a claim c_0 using a set es_0 of evidence;
F	is the set of facts, D is the set of data;
O	is the set of objects;
$M \times N$	is the direct product of M and N, for any sets M and N; and
$M + N$	is the discriminated union (direct sum) of M and N for any sets M and N.

Figure 1 — Structure of assurance cases (informative)

The following requirements apply to the structure of an assurance case:

a) An assurance case shall have one or more top-level claims that are the ultimate goals of its argumentation.

NOTE Multiple top-level claims are equivalent to their conjunction.

b) An argument shall be supported by one or more claims, evidence, or assumptions.

NOTE 1 An argument is used to show how the components directly underlying it relate to a claim or set of claims. The set of underlying components for an argument comprises a collection of evidence, assumptions, or lower-level claims.

NOTE 2 Since one argument cannot directly support another argument; a lower-level argument should attach to a lower-level claim that in turn attaches to the higher-level argument.

c) A claim shall be supported either by just one argument, or by one or more claims, evidence, or assumptions.

NOTE Every claim in an assurance case requires support, which can take different forms. Therefore, a claim is never a bottom component of an assurance case. One (and only one) argument can be used to support a claim. Alternatively, a claim can be supported (directly, and not via an argument) by some collection of evidence, assumptions, or lower-level claims.

d) A claim, argument, evidence, or assumption shall not support itself either directly or indirectly.

NOTE A single claim, argument, evidence, or assumption may be used to support multiple components.

6.3 Claims

6.3.1 Form of claim

A claim shall be a true-false statement that states the limitations on the values of an unambiguously defined property—called the claim's property, limitations on the uncertainty of the property's value meeting the limitations on it, and limitations on conditions under which the claim is applicable.

6.3.2 Claim contents

As indicated in the following list, a claim shall have the required contents and may have the optional contents:

a) Claim's property (required).

b) Limitations on the value of the property associated with the claim (e.g., on its range) (required).

c) Limitations on the uncertainty of the property value meeting its limitations (required).

d) Limitations on duration of claim's applicability (optional).

e) Duration-related uncertainty (optional).

f) Limitations on conditions under which the claim is applicable (required).

g) Condition-related uncertainty (optional).

h) If a property in a claim applies to some subset of systems, products, or their elements, their identification including relevant versions or instances (conditionally required).

i) Consequences or risks if they are relevant to claim (conditionally required).

NOTE 1 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, or multi-dimensional. The boundaries of these limitations sometimes involve probability distributions, are incremental, or have other fuzzy aspects.

NOTE 2 Uncertainties also may be associated with the duration of applicability and the stated conditions. Particular claims need not include all possible uncertainties and commonly include only one. Where accurate, uncertainties may be zero.

6.3.3 Coverage of conditions

The conditions, including any specified durations, covered by the combination of assurance case components supporting a claim shall together cover the conditions, including any specified duration, for which the claim is applicable.

6.3.4 Justification of the choice of top-level claims

Because the choice of a top-level claim and its property is critical in order to meet the objective of an assurance case and drives the assurance case's formulation, a top-level claim shall have a justification for its choice.

NOTE Justification for the top-level claim serves as a means for communicating risk among stakeholders of the system and for recording agreement.

6.4 Arguments

6.4.1 Argument characteristics

An argument is used to show how the components directly underlying it relate to a claim or set of claims. An argument can be particularly useful if it is in the form of an engineering calculation or logic proof and not in the form of an assurance case.

An argument has the following characteristics:

a) The argument shall be stated in a manner that uses the components directly below it.

b) The argument shall reach a conclusion or conclusions that relate to each claim it supports.

c) The argument shall establish the uncertainties of each conclusion it reaches.

d) The argument shall contain the information needed to establish its effect on uncertainty.

6.4.2 Justification of argument's method of reasoning

An argument shall have an associated justification for the validity or merit of its method of reasoning (e.g., calculating or arguing).

NOTE A variety of methods of reasoning can be used within arguments. These methods, including the tools they use, vary in their applicability, power, resulting accuracy and uncertainty, and ease of use. Arguments are used to support or detract from claims. The claims, evidence, and assumptions underlying an argument have uncertainties associated with them, and the argument might affect the uncertainty of the claim using it.

6.5 Evidence

6.5.1 Evidence contents

Evidence shall contain tangible data or information.

NOTE Many kinds of evidence exist. Among these are human experience reports, history, observations, measurements, tests, evaluative and compliance results, correctness of design rationale, analyses, comparison of artefacts, reviews, and defects and other quality assurance and field data. Evidence can already exist, be newly created or collected, or be planned for the future. The evidence should support or detract from the claims in the assurance case. The body of evidence can become quite large and should be organized, located, and presented to be understandable to those who review, approve, or directly use it.

6.5.2 Associated information

Evidence shall contain or have associated with it information regarding its:

a) Definition.

b) Scope of applicability.

c) Uncertainty, including the reliability of its source (e.g., authenticity, trustworthiness, and competence) and the measurement accuracy.

NOTE This information may take any form including one or more assurance cases or portions thereof.

6.5.3 Associated assumptions

Any assumptions related to evidence shall be included in the assurance case.

6.6 Assumptions

6.6.1 Form of Assumption

An assumption shall take the form of a claim and a reason for it.

6.6.2 Assumption contents

An assumption can have one of three kinds of origins. Two kinds are inherently true given their context and role within the assurance case. These are (1) an assumption implied by the specified conditions restricting the applicability of the claim(s) it supports and (2) an assumption inherent in a method of argumentation, e.g., as a statement of an alternative that is one of a set of alternative assumptions that together cover all the relevant possibilities, such as stating each case in a proof by cases. These two kinds of assumptions have zero uncertainty.

The third kind of an assumption is not inherently true; rather it is a claim not fully warranted by evidence. This third kind of assumption shall:

a) Contain a claim and a reason for it.

b) Contain an indication, identification, or description of the basis of the estimate of the uncertainty regarding the truth of the assumption.

NOTE For best results, such assumptions should have one or more of the following characteristics: have low uncertainty or low risk because they are of low criticality in argumentation, have a weak impact on the argumentation, have a weak effect on critical values or consequences, or are few in number.

6.6.3 Associated evidence

If an assumption is partially warranted or contradicted by evidence, this evidence shall be associated with it.

6.7 Justifications

A top-level claim has a justification for its choice (6.3.4) and an argument has a justification for its method of argumentation (6.4.2).

6.8 Combining assurance cases

If an assurance case incorporates another assurance case, the incorporated assurance case's top-level claim or claims shall each be placed within the original assurance case's structure at points where claims are allowed.

NOTE A portion of an assurance case may also be a part of other assurance cases.

7 Required outcomes of using Part 2 assurance case

7.1 Outcomes

Application of this part of ISO/IEC 15026 has the following outcomes:

a) An assurance case meeting the requirements of Clause 6 shall be provided as an element of the system.

NOTE As an element of the system, the assurance case is generally expected to be delivered with the system and maintained as the system is maintained.

b) A logical mapping meeting the requirements of 7.2 shall be provided as a part of the assurance case.

c) Records documenting the fulfilment of the requirements of this part of ISO/IEC 15026 shall be identified and referenced by the assurance case.

d) Identification of the entity or entities asserting conformance shall be provided in the assurance case.

7.2 Mapping to this part of ISO/IEC 15026

An assurance case shall:

a) Include an unambiguous mapping to the components and relationships in Clause 6.

b) Cover all the contents specified in Clause 6 unless documented justification is provided for doing otherwise.

NOTE 1 Because this mapping has to map from assurance cases that are developed within several specialities and utilize many notations, the mapping may take any unambiguous form.

NOTE 2 The mapping may assign a meaning and mapping to a component that is missing if that mapping is unambiguous. For example, if a particular kind of uncertainty is not explicitly specified, then the mapping might state that this is equivalent to it being specified and equalling zero.