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.