INTERNATIONAL STANDARD

ISO/IEC 15026-4

First edition
2012-10-01

Systems and software engineering — Systems and software assurance —

Part 4: Assurance in the life cycle

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

Partie 4: Assurance du cycle de vie

Reference number
ISO/IEC 15026-4:2012(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 shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15026-4 was prepared by Joint Technical Committee ISO/TC 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*

— *Part 3: System integrity levels*

— *Part 4: Assurance in the life cycle*

Introduction

In its entirety, ISO/IEC 15026 consists of multiple parts:

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

NOTE ISO/IEC TR 15026-1 is intended to be replaced by an International Standard.

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

c) ISO/IEC 15026-3, *System and software engineering — Systems and software assurance — Part 3: System integrity levels*

d) ISO/IEC 15026-4, *System and software engineering — Systems and software assurance — Part 4: Assurance in the life cycle*

Many specialized standards and guidelines address specific application areas and topics related to assurance and use different concepts and terminology when addressing common themes. ISO/IEC TR 15026-1 provides terminology and concepts used in all parts of ISO/IEC 15026.

ISO/IEC 15026-2 provides minimum requirements for the structure and contents of assurance cases that treat claims regarding properties of a system or software product selected for special treatment. The results of performing the life cycle activities and tasks referenced in this part of ISO/IEC 15026 can be recorded in the form of the assurance case described in ISO/IEC 15026-2.

ISO/IEC 15026-3 addresses the assignment of integrity levels for selected elements of a system. Where ISO/IEC 15026-2 is applicable, it can bring useful structure, aid, and direction to defining claims and showing their achievement through the use of integrity levels and accompanying integrity level requirements.

ISO/IEC 15026-2, ISO/IEC 15026-3 and ISO/IEC 15026-4 all use the concepts and vocabulary defined in ISO/IEC TR 15026-1; however, any part can be applied independently of the others and the use of one does not require the use of any others.

Systems and software engineering — Systems and software assurance —

Part 4:
Assurance in the life cycle

1 Scope

This part of ISO/IEC 15026 gives guidance and recommendations for conducting selected processes, activities and tasks for systems and software products requiring assurance claims for properties selected for special attention, called critical properties. This part of ISO/IEC 15026 specifies a property-independent list of processes, activities and tasks to achieve the claim and show the achievement of the claim. This part of ISO/IEC 15026 establishes the processes, activities, tasks, guidance and recommendations in the context of a defined life cycle model and set of life cycle processes for system and/or software life cycle management.

NOTE The stakeholders determine which of the system or software properties are selected for special attention and require assurance claims. This part of ISO/IEC 15026 uses the term “critical” to distinguish those properties from other requirements.

2 Conformance

Conformance may be claimed to this part of ISO/IEC 15026 with respect to the systems assurance process view and/or the software assurance process view. Thus, conformance to this part of ISO/IEC 15026 can be achieved in either or both of the following ways:

a) Demonstrating that the required outcomes of the systems assurance process view (6.1.2) have been achieved, in addition to conforming to the Agreement, Project, and Technical processes of ISO/IEC 15288.

b) Demonstrating that the required outcomes of the software assurance process view (6.2.2) have been achieved, in addition to conforming to the Agreement, Project, Technical, and Software Specific processes of ISO/IEC 12207:2008.

A claim of conformance is relevant only to specific claims regarding designated systems or software.

Conformance to ISO/IEC 15026 Part 2 can assist in achieving the outcomes required by the two process views in this part of ISO/IEC 15026.

NOTE Parties to an agreement may choose to incorporate selected portions of this part of the International Standard into the terms of the agreement. However, compliance with the agreement does not justify a claim of conformance to this part of the International Standard. A claim of conformance can only be justified as explained above.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced documents (including any amendments) applies.

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

This part requires activities and tasks in the context of complete sets of life cycle processes that comprise life cycle models for projects. The two sets of life cycle processes are provided in:

ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*

ISO/IEC 12207:2008, *Systems and software engineering — Software life cycle processes*

The assurance guidance and recommendations referenced in this part of ISO/IEC 15026 are to be understood in terms of their being in the context of the processes, activities and tasks of ISO/IEC 15288 and ISO/IEC 12207.

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC TR 15026-1, ISO/IEC 15288:2008, and ISO/IEC 12207:2008 apply.

5 Key concepts for and use of this part of ISO/IEC 15026

5.1 Life cycle approach

It is presumed that the user of this International Standard is using a defined life cycle model and set of life cycle processes for system and/or software life cycle management. Across the life cycle, the systems and software process views in Clause 6 use the guidance and recommendations in Clause 7 for the performance of specific processes, activities, and tasks in order to achieve and show the achievement of assurance claims. Since all processes of ISO/IEC 15288 and ISO/IEC 12207 are applied iteratively and recursively in the life cycle, the guidance and recommendations for assurance are also applied iteratively and recursively. In that way, the achievement of assurance can be checked during each iteration or recursion.

NOTE See ISO/IEC TR 24748-1 for more information about life cycle models and the iteration and recursion of processes.

5.2 Assurance claims

When system or software product requirements call for assurance of one or more critical properties of the system or software product, the overall claims for assurance regarding these properties' values are referred to in ISO/IEC 15026 as assurance claims. Commonly, such critical properties are in areas where substantial risk or consequences are involved such as reliability and maintainability, safety, security, or human factors.

NOTE The material in this clause is adopted from ISO/IEC 15026-2.

Achieving assurance claims normally includes all the considerations involved in achieving stringent requirements. A requirement is defined in ISO/IEC 29148 as “statement which translates or expresses a need and its associated constraints and conditions” and a claim is defined in ISO/IEC TR 15026-1 as “statement of something to be true including associated conditions and limitations.” This part of ISO/IEC 15026 considers requirements to be statements of values for variables and claims to be statements of requirements to be true.

While assurance claims can be derived from a number of sources, they are normally motivated by potential real-world adverse consequences related to the intended uses of the system and justified as deriving from system or software requirements. Each assurance claim is fully and unambiguously specified including:

a) “Assurance claims” — that is, the top-level claims, including

   1) Values for the variables of the critical property required for its achievement.

   2) Limitations on allowable uncertainties regarding this achievement.

   3) Conditions and/or durations of applicability under which it applies.

