INTERNATIONAL STANDARD

ISO/IEC 15026-1

First edition
2013-11-01

Systems and software engineering — Systems and software assurance —

Part 1: Concepts and vocabulary

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

Partie 1: Concepts et vocabulaire

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/sist/e34e78c2-15ab-4d6a-9199-49e39d4eca8d/iso-iec-15026-1-2013

Reference number
ISO/IEC 15026-1:2013(E)

© ISO/IEC 2013

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/sist/e34e78c2-15ab-4d6a-9199-49e39d4eca8d/iso-iec-15026-1-2013

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2013

All rights reserved. Unless otherwise specified, 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
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

 © ISO/IEC 2013 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/sist/e34e78c2-15ab-4d6a-9199-49e39d4eca8d/iso-iec-15026-1-2013

© ISO/IEC 2013 – All rights reserved

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

This first edition of ISO/IEC 15026-1 cancels and replaces ISO/IEC TR 15026-1:2010, which has been technically revised.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/sist/e34e78c2-15ab-4d6a-9199-49e39d4eca8d/iso-iec-15026-1-2013

— *Part 1: Concepts and vocabulary*

— *Part 2: Assurance case*

— *Part 3: System integrity levels*

— *Part 4: Assurance in the life cycle*

The IEEE Computer Society collaborated with ISO/IEC JTC 1 in the development of the international standards of ISO/IEC 15026. *IEEE Std 1228-1994 and IEEE Standard for Safety Plan* were used as base documents in the development of this standard.

 © ISO/IEC 2013 – All rights reserved

Introduction

Software and systems assurance and closely related fields share concepts but have differing vocabularies and perspectives. This part of ISO/IEC 15026 provides a unifying set of underlying concepts and an unambiguous use of terminology across these various fields. It provides a basis for elaboration, discussion, and recording agreement and rationale regarding concepts and the vocabulary used uniformly across all parts of ISO/IEC 15026.

This part of ISO/IEC 15026 clarifies concepts needed for understanding software and systems assurance and, in particular, those central to the use of ISO/IEC 15026-2 to ISO/IEC 15026-4. It supports shared concepts, issues and terminology applicable across a range of properties, application domains, and technologies.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/sist/e34e78c2-15ab-4d6a-9199-49e39d4eca8d/iso-iec-15026-1-2013

© ISO/IEC 2013 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/sist/e34e78c2-15ab-4d6a-9199-49e39d4eca8d/iso-iec-15026-1-2013

Systems and software engineering — Systems and software assurance —

Part 1: Concepts and vocabulary

1 Scope

This part of ISO/IEC 15026 defines assurance-related terms and establishes an organized set of concepts and relationships to establish a basis for shared understanding across user communities for assurance. It provides information to users of the other parts of ISO/IEC 15026 including the combined use of multiple parts. The essential concept introduced by ISO/IEC 15026 is the statement of *claims* in an *assurance case* and the support of those claims through *argumentation* and *evidence*. These claims are in the context of assurance for properties of systems and software within life cycle processes for the system or software product.

Assurance for a service being operated and managed on an ongoing basis is not covered in ISO/IEC 15026.

2 Applicability

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2.1 Audience

ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/sist/e34e78c2-15ab-4d6a-9199-49e39d4eca8d/iso-iec-15026-1-2013

A variety of potential users of ISO/IEC 15026 exists including developers and maintainers of assurance cases and those who wish to develop, sustain, evaluate, or acquire a system that possesses requirements for specific properties in such a way as to be more certain of those properties and their requirements. ISO/IEC 15026 uses concepts and terms consistent with ISO/IEC 12207 and ISO/IEC 15288 and generally consistent with the ISO/IEC 25000 series, but the potential users of ISO/IEC 15026 need to understand differences from concepts and terms to which they may be accustomed. This part of ISO/IEC 15026 attempts to clarify these differences.

2.2 Field of applicability

The primary purpose of this part of ISO/IEC 15026 is to aid users of the other parts of ISO/IEC 15026 by providing context, concepts, and explanations for assurance, assurance cases, and integrity levels. While essential to assurance practice, details regarding exactly how to measure, demonstrate, or analyse particular properties are not covered. These are the subjects of more specialized standards of which a number are referenced and included in the Bibliography.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE These are intended to be uniform through all parts of ISO/IEC 15026.

3.1 Terms related to assurance and properties

3.1.1
assurance
grounds for justified confidence that a claim has been or will be achieved

© ISO/IEC 2013 – All rights reserved

3.1.2
claim
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 also may be associated with the duration of applicability and the stated conditions.

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

— claim's property;

— 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;

— 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 may involve probability distributions and may be incremental.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.3
assurance case
reasoned, auditable artefact created that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s)

ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/sist/e34e78c2-15ab-4d6a-9199-49e39d4eca8d/iso-iec-15026-1-2013

Note 1 to entry: An assurance case contains the following and their relationships:

— one or more claims about properties;

— arguments that logically link the evidence and any assumptions to the claim(s);

— a body of evidence and possibly assumptions supporting these arguments for the claim(s);

— justification of the choice of top-level claim and the method of reasoning.

3.1.4
dependability
collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance

Note 1 to entry: Dependability is used only for general descriptions in non-quantitative terms.

Note 2 to entry: ISO/IEC 25010[99] notes that "dependability characteristics include availability and its inherent or external influencing factors, such as: reliability, fault tolerance, recoverability, integrity, security, maintainability, durability, and maintenance support." Several standards address dependability (e.g.[64] and[69]), and many more address the qualities within it. IEC 60050-191 offers related definitions.[63]

[SOURCE: IEC 60300-1:2003]

© ISO/IEC 2013 – All rights reserved

3.2 Terms related to product and process

3.2.1
process
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: ISO/IEC 15288:2008 and ISO/IEC 12207:2008]

3.2.2
process view
description of how a specified purpose and set of outcomes may be achieved by employing the activities and tasks of existing processes

[SOURCE: ISO/IEC 15288:2008, D.3]

3.2.3
product
result of a process

Note 1 to entry: Results could be components, systems, software, services, rules, documents, or many other items.

Note 2 to entry: The "result" could in some cases be many related individual results. However, claims usually relate to specified versions of a product.

[SOURCE: ISO/IEC 15288:2008 and ISO 9000:2005]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.2.4
system
combination of interacting elements organized to achieve one or more stated purposes

Note 1 to entry: A system may be considered as a product or as the services it provides.

ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/sist/a34e78c2-15eb-4d6a-9199-49e39d4ec8d/iso-iec-15026-1-2013

Note 2 to entry: In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g. aircraft system. Alternatively, the word "system" may be substituted simply by a context-dependent synonym, e.g. aircraft, though this may then obscure a system principles perspective.

[SOURCE: ISO/IEC 15288:2008]

3.2.5
requirement
statement that translates or expresses a need and its associated constraints and conditions

Note 1 to entry: Requirements exist at different tiers and express the need in high-level form (e.g. software component requirement).

[SOURCE: ISO/IEC/IEEE 29148:2011]

3.2.6
system element
member of a set of elements that constitutes a system

Note 1 to entry: A system element is a discrete part of a system that can be implemented to fulfil specified requirements. A system element can be hardware, software, data, humans, processes (e.g. processes for providing service to users), procedures (e.g. operator instructions), facilities, materials, and naturally occurring entities (e.g. water, organisms, minerals), or any combination.

[SOURCE: ISO/IEC 15288:2008]

© ISO/IEC 2013 – All rights reserved

3.3 Terms related to integrity level

3.3.1
integrity level
claim of a system, product, or element that includes limitations on a property's values, the claim's scope of applicability, and the allowable uncertainty regarding the claim's achievement

Note 1 to entry: Generally, the intention is that maintaining limitations on a property's values related to the relevant items will result in maintaining system risks within limits.

Note 2 to entry: Adapted from ISO/IEC 15026:1998.

3.3.2
integrity level requirements
set of specified requirements imposed on aspects related to a system, product, or element and associated activities in order to show the achievement of the assigned integrity level (that is, meeting its claim) within the required limitations on uncertainty; this includes the evidence to be obtained

Note 1 to entry: Since an integrity level is defined as a claim, the two phrases "achievement of the assigned integrity level" and "meeting its claim" are equivalent.

Note 2 to entry: In ISO/IEC 15026:1998, 3.3.1 and 3.3.2 are referred to as the "integrity level" and "integrity requirements" respectively. The latter has been changed to "integrity level requirements" both for increased clarity and because this is common usage in safety.

Note 3 to entry: IEEE Std 1012:2004 defines "integrity level" as "a value representing project-unique characteristics (e.g. software complexity, criticality, risk, safety level, security level, desired performance, reliability) that define the importance of the software to the user." That is, an integrity level is a value of a property of the target software. Since both a claim and a statement that a property has a particular value can be regarded as a proposition of a system or software, the two definitions of integrity levels have significantly the same meaning.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.4 Terms related to conditions and consequences

ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/sist/e34e78c2-15ab-4d6a-9199-49e39d4eca8d/iso-iec-15026-1-2013

3.4.1
consequence
effect (change or non-change), usually associated with an event or condition or with the system and usually allowed, facilitated, caused, prevented, changed, or contributed to by the event, condition, or system

Note 1 to entry: It could yield a benefit, a loss, or neither.

3.1.8
risk
combination of the probability of an event and its consequence

Note 1 to entry: The term "risk" is generally used only when there is at least the possibility of negative consequences.

Note 2 to entry: In some situations, risk arises from the possibility of deviation from the expected outcome or event.

Note 3 to entry: See ISO/IEC Guide 51 for issues related to safety.

[SOURCE: ISO/IEC 16085]

3.4.2
adverse consequence
undesirable consequence associated with a loss

3.4.3
desirable (or positive) consequence
consequence associated with a benefit or gain or avoiding an adverse consequence

© ISO/IEC 2013 – All rights reserved

3.4.4
error
erroneous state of the system

3.4.5
fault
defect in a system or a representation of a system that if executed/activated could potentially result in an error

Note 1 to entry: Faults can occur in specifications when they are not correct.

3.4.6
attack
malicious action or interaction with the system or its environment that has the potential to result in a fault or an error (and thereby possibly in a failure) or an adverse consequence

3.4.7
violation
behaviour, act, or event deviating from a system's desired property or claim of interest

Note 1 to entry: In the area of safety, the term "violation" is used to refer to a deliberate human contravention of a procedure or rule.

3.4.8
failure
termination of the ability of a system to perform a required function or its inability to perform within previously specified limits; an externally visible deviation from the system's specification

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.4.9
systematic failure
failure related in a deterministic way to a certain cause that can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/iso/[illegible]/iso-iec-15026-1-2013
49e39d4eca8d/iso-iec-15026-1-2013

3.5 Terms related to organization

3.5.1
organization
person or a group of people and facilities with an arrangement of responsibilities, authorities and relationships

Note 1 to entry: A body of persons organized for some specific purpose, such as a club, union, corporation, or society, is an organization.

Note 2 to entry: An identified part of an organization (even as small as a single individual) or an identified group of organizations can be regarded as an organization if it has responsibilities, authorities and relationships.

[SOURCE: ISO/IEC 15288:2008]

3.5.2
approval authority
person (or persons) and/or organization (or organizations) responsible for approving activities, artefacts, and other aspects of the system during its life cycle

Note 1 to entry: The approval authority may include multiple entities, e.g. individuals or organizations. These can include different entitles with different levels of approval and/or different areas of interest.

Note 2 to entry: In two-party situations, approval authority often rests with the acquirer. In regulatory situations, the approval authority may be a third party such as a governmental organization or its agent. In other situations, for example, the purchase of off-the-shelf products developed by a single-party, the independence of the approval authority can be a relevant issue to the acquirer.

© ISO/IEC 2013 – All rights reserved

3.5.3
design authority
person or organization that is responsible for the design of the product

3.5.4
integrity assurance authority
independent person or organization responsible for certifying compliance with the integrity level requirements

Note 1 to entry: Adapted from ISO/IEC 15026:1998, in which the definition is: "The independent person or organization responsible for assessment of compliance with the integrity requirements."

4 Organization of this International Standard

Clause 5 of this International Standard covers basic concepts such as assurance, stakeholders, systems and products, uncertainty, and consequence. Clause 6 covers some issues of which users of ISO/IEC 15026-2, ISO/IEC 15026-3 and ISO/IEC 15026-4 need to be initially aware. Clauses 7, 8, and 9 cover terms, concepts, and topics particularly relevant to users of ISO/IEC 15026-2, ISO/IEC 15026-3 and ISO/IEC 15026-4, respectively, although users of one part can also benefit from some of the information in the clauses for other parts. A Bibliography is included at the end. References to numbered items in the Bibliography are shown in brackets throughout.

5 Basic concepts

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5.1 Introduction

This clause covers the concepts and vocabulary fundamental to all parts of ISO/IEC 15026.

ISO/IEC 15026-1:2013
https://standards.iteh.ai/catalog/standards/sist/e34e78c2-15ab-4d6a-9199-49e39d4eca8d/iso-iec-15026-1-2013

5.2 Assurance

ISO/IEC 15026 uses a specific definition for assurance as being grounds for justified confidence. Generally, stakeholders need grounds for justifiable confidence prior to depending on a system, especially a system involving complexity, novelty, or technology with a history of problems (e.g. software). The greater the degree of dependence, the greater the need for strong grounds for confidence. The appropriate valid arguments and evidence to establish a rational basis for justified confidence in the relevant claims about the system's properties need to be made. These properties may include such aspects as future costs, behaviour, and consequences. Throughout the life cycle, adequate grounds need to exist for justifying decisions related to ensuring the design and production of an adequate system and to be able to place reliance on that system.

Assurance is a term whose usage varies among the communities who use the term. However, all usage relates to placing limitations on or reducing uncertainty in such things as measurements, observations, estimations, predictions, information, inferences, or effects of unknowns with the ultimate objective of achieving and/or showing a claim. Such a reduction in uncertainty may provide an improved basis for justified confidence. Even if the estimate of a property's value remains unchanged, the effort spent in reducing uncertainty about its value can often be cost-effective since the resulting reduced uncertainty improves the basis for decision-making.

Assurance may relate to (1) would the system or software as specified meet real-world needs and expectations, to (2) would or does the as-built and operated system meet the specifications, or to both (1) and (2). Specifications may be representations of static and/or dynamic aspects of the system. Specifications often include descriptions of capability, functionality, behaviour, structure, service, and responsibility including time-related and resource-related aspects as well as limitations on frequency or seriousness of deviations by the product and related uncertainties.

Specifications may be prescriptions and/or constraints (e.g. for and on product behaviours) as well as include measures of merit and directions regarding tradeoffs. Generally, specifications place some

 © ISO/IEC 2013 – All rights reserved