INTERNATIONAL STANDARD

ISO/IEC/IEEE 15026-1

First edition
2019-03

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

Reference number
ISO/IEC/IEEE 15026-1:2019(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Institute of Electrical and Electronics Engineers, Inc
3 Park Avenue, New York
NY 10016-5997, USA

Email: stds.ipr@ieee.org
Website: www.ieee.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.

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 ISO documents should be noted. This document was drafted in accordance with the rules given in the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information Technology*, Subcommittee SC 7, *Software and systems engineering*, in cooperation with the Systems and Software Engineering Standards Committee of the IEEE Computer Society, under the Partner Standards Development Organization cooperation agreement between ISO and IEEE.

This first edition cancels and replaces ISO/IEC 15026-1:2013, which has been technically revised.

The main changes compared to the previous edition are as follows:

— definitions of terms introduced in ISO/IEC 15026-3:2015 are added;

— definitions of terms whose definitions are modified in ISO/IEC 15026-3:2015 are updated.

A list of all parts in the ISO/IEC/IEEE 15026 series can be found on the ISO website.

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.

Introduction

Software and systems assurance and closely related fields share concepts but have different vocabularies and perspectives. This document 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 ISO/IEC/IEEE 15026 (all parts).

This document clarifies concepts needed for understanding software and systems assurance and, in particular, those central to the use of ISO/IEC 15026-2, ISO/IEC 15026-3 and ISO/IEC 15026-4. It supports shared concepts, issues and terminology applicable across a range of properties, application domains and technologies.

Systems and software engineering — Systems and software assurance —

Part 1: Concepts and vocabulary

1 Scope

This document defines assurance-related terms and establishes an organized set of concepts and relationships to form a basis for shared understanding across user communities for assurance. It provides information to users of the other parts of ISO/IEC/IEEE 15026 including the combined use of multiple parts. The essential concept introduced by ISO/IEC/IEEE 15026 (all parts) 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/IEEE 15026 (all parts).

A variety of potential users of ISO/IEC/IEEE 15026 (all parts) 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/IEEE 15026 (all parts) uses concepts and terms consistent with ISO/IEC/IEEE 12207 and ISO/IEC/IEEE 15288 and generally consistent with the ISO/IEC 25000 series, but the potential users of ISO/IEC/IEEE 15026 (all parts) need to understand the differences from concepts and terms to which they may be accustomed. This document attempts to clarify these differences.

The primary purpose of this document is to aid users of the other parts of ISO/IEC/IEEE 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.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

ISO, IEC and IEEE maintain terminological databases for use in standardization at the following addresses:

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

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

— IEEE Standards Dictionary Online: available at http://dictionary.ieee.org

3.1 Terms related to assurance and properties

3.1.1
assurance
grounds for justified confidence that a *claim* (3.1.4) has been or will be achieved

3.1.2
assurance case
reasoned, auditable artefact created that supports the contention that its top-level *claim* (3.1.4) (or set of claims) is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s)

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); and

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

3.1.3
attribute
inherent property or characteristic of an entity that can be distinguished quantitatively or qualitatively by human or automated means

Note 1 to entry: ISO 9000 distinguishes two types of attributes: a permanent characteristic existing inherently in something; and an assigned characteristic of a *product* (3.2.3), *process* (3.2.1), or *system* (3.2.4) (e.g., the price of a product, the owner of a product).

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.2]

3.1.4
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* (3.1.5)

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.

3.1.5
condition
measurable qualitative or quantitative *attribute* (3.1.3) that is stipulated for a *requirement* (3.2.5) and that indicates a circumstance or event under which a requirement applies

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.6]

3.1.6
constraint
externally imposed limitation on the *system* (3.2.4), its design, or implementation or on the *process* (3.2.1) used to develop or modify a system

Note 1 to entry: A constraint is a factor that is imposed on the solution by force or compulsion and may limit or modify the design.

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.7]

3.1.7
dependability
<of an item> ability to perform as and when required

Note 1 to entry: Dependability includes availability, reliability, recoverability, maintainability, and maintenance support performance, and, in some cases, other characteristics such as durability, safety and security.

Note 2 to entry: Dependability is used as a collective term for the time-related quality characteristics of an item.

[SOURCE: IEC 60050-192:2015, 192-01-22]

3.2 Terms related to product and process

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

Note 1 to entry: The definition for this term can also be found in ISO 9000 and ISO/IEC/IEEE 12207.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.30, modified — Note 1 to entry has been added.]

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* (3.2.1)

Note 1 to entry: The process view concept is introduced in ISO/IEC/IEEE 15288:2015, Annex E and ISO/IEC/IEEE 12207:2017, Annex E.

3.2.3
product
result of a *process* (3.2.1)

Note 1 to entry: There are four agreed generic product categories: hardware (e.g., engine mechanical part); software (e.g., computer program); services (e.g., transport); and processed materials (e.g., lubricant). Hardware and processed materials are generally tangible products, while software or services are generally intangible.

Note 2 to entry: Results could be components, *systems* (3.2.4), software, services, rules, documents, or many other items.

Note 3 to entry: The "result" could in some cases be many related individual results. However, *claims* (3.1.4) usually relate to specified versions of a product.

Note 4 to entry: The definition for this term can also be found in ISO 9000 and ISO/IEC/IEEE 12207.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.32, modified—Notes 2 to 4 to entry have been added.]

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

Note 1 to entry: A system is sometimes considered as a *product* (3.2.3) or as the services it provides.

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" is substituted simply by a context-dependent synonym, e.g., aircraft, though this potentially obscures a system principles perspective.

Note 3 to entry: A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment.

Note 4 to entry: The definition for this term can also be found in ISO/IEC/IEEE 12207.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.46, modified — Note 4 to entry has been added.]

3.2.5
requirement
statement which translates or expresses a need and its associated *constraints* (3.1.6) and *conditions* (3.1.5)

Note 1 to entry: Requirements exist at different levels in the *system* (3.2.4) structure.

Note 2 to entry: A requirement is an expression of one or more particular needs in a very specific, precise and unambiguous manner.

Note 3 to entry: A requirement always relates to a system, software or service, or other item of interest.

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.19]

3.2.6
system element
member of a set of elements that constitutes a *system* (3.2.4)

EXAMPLE Hardware, software, data, humans, *processes* (3.2.1) (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials, and naturally occurring entities or any combination.

Note 1 to entry: A system element is a discrete part of a system that can be implemented to fulfill specified *requirements* (3.2.5).

Note 2 to entry: The definition for this term can also be found in ISO/IEC/IEEE 12207.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.47, modified — Note 2 to entry has been added.]

3.3 Terms related to integrity level

3.3.1
integrity level
degree of confidence that the *system-of-interest* (3.3.12) meets the associated *integrity level claim* (3.3.4)

Note 1 to entry: While a definition of “integrity level” is given, existing definitions and the relevant communities do not agree on a definition of “integrity” consistent with its use in “integrity level”. Hence, no separate definition of “integrity” is included in this document. For the definition of “integrity” used in ISO/IEC JTC 1/SC 7, see ISO/IEC 25010:2011, 4.1.6.2.

Note 2 to entry: An integrity level is different from the *likelihood* (3.3.6) that the integrity level claim is met but they are closely related.

Note 3 to entry: The word “confidence” implies that the definition of integrity levels can be a subjective concept.

Note 4 to entry: In this document, integrity levels are defined in terms of *risk* (3.4.2) and hence cover safety, security, economic and any other dimension of risk that is relevant to the system-of-interest.

3.3.2
integrity level requirements
set of *requirements* (3.2.5) that, when met, will provide a level of confidence in the associated *integrity level claim* (3.3.4) commensurate with the associated *integrity level* (3.3.1)

Note 1 to entry: An integrity level requirement is different from any requirement in ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207.

3.3.3
initial risk
estimated *risk* (3.4.2) before applying *risk reduction measures* (3.3.9)

3.3.4
integrity level claim
proposition representing a *requirement* (3.2.5) on a *risk reduction measure* (3.3.9) identified in the *risk treatment* (3.3.11) *process* (3.2.1) of the *system-of-interest* (3.3.12)

Note 1 to entry: In general, it is described in terms of requirements to avoid, control or mitigate the *consequences* (3.4.1) of *dangerous conditions* (3.4.11), so as to provide a *tolerable risk* (3.3.15) if it is met.

Note 2 to entry: The proposition that can be regarded as an integrity level claim in IEC 61508 is that an E/E/PE safety-related *system* (3.2.4) satisfactorily performing the specified safety functions under all the stated conditions.

3.3.5
level of risk
magnitude of a *risk* (3.4.2) or combination of risks, expressed in terms of the combination of *consequences* (3.4.1) and their *likelihood* (3.3.6)

[SOURCE: ISO Guide 73:2009, 3.6.1.8]

3.3.6
likelihood
chance of something happening

[SOURCE: ISO Guide 73:2009, 3.6.1.1, modified — NOTEs 1 and 2 have been removed.]

3.3.7
residual risk
risk (3.4.2) remaining after *risk treatment* (3.3.11)

[SOURCE: ISO Guide 73:2009, 3.8.1.6, modified — NOTEs 1 and 2 have been removed.]

3.3.8
risk criteria
terms of reference against which the significance of a *risk* (3.4.2) is evaluated

[SOURCE: ISO Guide 73:2009, 3.3.1.3, modified — NOTEs 1 and 2 have been removed.]

3.3.9
risk reduction measure
measure to reduce or mitigate *risk* (3.4.2)

Note 1 to entry: A typical risk reduction measure is a safety-related *system* (3.2.4) in the IEC 61508 series.

3.3.10
risk source
element which alone or in combination has the intrinsic potential to give rise to *risk* (3.4.2)

Note 1 to entry: A hazard in ISO Guide 73 is an instance of a risk source.

Note 2 to entry: A *fault* (3.4.6), an *error* (3.4.5) or a *failure* (3.4.9) in the context of reliability can be a risk source. The definitions of those terms can be found in IEC 61508-4.