INTERNATIONAL STANDARD

ISO/IEC 15026-3

First edition
2011-12-15

Systems and software engineering — Systems and software assurance —

Part 3: **System integrity levels**

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

Partie 3: Niveaux d'intégrité du système

Reference number
ISO/IEC 15026-3:2011(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

Tables

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 15026-3 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 15026-3 cancels and replaces ISO/IECI 15026:1998, which has been technically revised.

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*

The following part is under preparation:

- *Part 4: Assurance in the life cycle*

Systems and software engineering — Systems and software assurance —

Part 3: System integrity levels

1 Scope

This part of ISO/IEC 15026 specifies the concept of integrity levels with corresponding integrity level requirements that are required to be met in order to show the achievement of the integrity level. It places requirements on and recommends methods for defining and using integrity levels and their integrity level requirements. It covers systems, software products, and their elements, as well as relevant external dependences.

This part of ISO/IEC 15026 is applicable to systems and software and is intended for use by:

a) definers of integrity levels such as industry and professional organizations, standards organizations, and government agencies;

b) users of integrity levels such as developers and maintainers, suppliers and acquirers, users, and assessors of systems or software and for the administrative and technical support of systems and/or software products.

One important use of integrity levels is by suppliers and acquirers in agreements; for example, to aid in assuring safety, economic, or security characteristics of a delivered system or product.

This part of ISO/IEC 15026 does not prescribe a specific set of integrity levels or their integrity level requirements. In addition, it does not prescribe the way in which integrity level use is integrated with the overall system or software engineering life cycle processes. It does, however, provide an example of use of this part of ISO/IEC 15026 in Annex B.

2 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 document (including any amendments) applies.

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

3 Terms and definitions

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

NOTE While a definition is included for "integrity level", 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 part of ISO/IEC 15026. For the definition of "integrity" used in ISO/IEC JTC 1 SC 7, see ISO/IEC 25010:2011, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*.

4 Integrity level framework

4.1 Integrity level specification

An integrity level specification includes two kinds of related requirements defined as follows:

a) **"Integrity level"**—A claim of a system, product, or element. This claim includes limitations on a property's values, the claim's scope of applicability, and the allowable uncertainty regarding the claim's achievement. A label designated for an integrity level is called an integrity level's label.

b) **"Integrity level requirements"**—A 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.

Definers of integrity levels need to justify explicitly the assertion that meeting an integrity level's corresponding integrity level requirements suffices to achieve the integrity level within its allowable uncertainty. This justification can be reflected in, but not necessarily included in, a source for users (e.g., a standard).

NOTE 1 In ISO/IEC 15026:1998, a) and b) 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 2 "Integrity level" is sometimes referred as "integrity level claim" to distinguish it from "integrity level requirement".

NOTE 3 See 8.2 and 8.2.4 for a detailed explanation of "required limitations."

NOTE 4 See ISO/IEC TR 15026-1 for further explanation of the use of evidence.

NOTE 5 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 value can be regarded as a proposition of a system or software, the two definitions of integrity levels have significantly the same meaning.

NOTE 6 Integrity level claims in this part of ISO/IEC 15026 can cover behaviours or conditions of the system or product or values of a property, in which case they can play roles of both "requirements" and "measures". For an acquisition of a system or product, an integrity level claim can be used for representing an agreement between the acquirer and the supplier. In this case the integrity level claim plays the role of a requirement. In the activity of accepting a system or product in the acquisition process, the integrity level claim is used for confirming that the delivered system or product complies with the agreement, i.e., the delivered system or product is measured by an integrity level claim.

NOTE 7 Integrity levels and standards utilizing them have a significant history especially in safety. Integrity levels in safety-related standards are defined in multi-level sets addressing varying degrees of stringency and/or uncertainty of their achievement with higher levels providing higher stringency and lower uncertainty. One example safety standard is IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems. Elsewhere, similar schemes are used with different labels, e.g., "conformance classes."

To complete the integrity level framework, the next clause describes a process for using integrity levels that also provides the background for understanding the needs and motivations addressed during their definition.

4.2 Process for using integrity levels

A risk-based approach is used within this part of ISO/IEC 15026 to determine the integrity level assigned to the system or product. From this system or product integrity level, integrity levels are derived for elements of the system or product. Figure 1 shows an overview of the activities required to use integrity levels. Inputs and outputs for each activity are shown in Table A.1 in Annex A. In addition to the main feedback loops shown in Figure 1, feedback can occur among all these activities.

NOTE 1 ISO/IEC 16085:2006 defines “risk” as “The combination of the probability of an event and its consequence.”

In this part of 15026, a system is assumed to have the following structure in order to introduce the process for assigning an integrity level to a system. First, a system has several interfaces, each of which is a boundary between the system and its environment. Any influence on the system and from the system is represented by this concept, e.g., operations by users, interactions with other systems, and attacks by malicious persons.

A system consists of system elements, which are units associated with an integrity level for purposes of this part of ISO/IEC 15026. Several ways exist to choose what parts of the system are system elements. Decomposing a system into elements is accomplished before or during the assignment of integrity levels described in this part of ISO/IEC 15026. A system element can be seen as a system and thus a system-element relation can be found at each layer of system decomposition.

NOTE 2 A “system element” is sometimes referred to as an “element” if the context is understood.

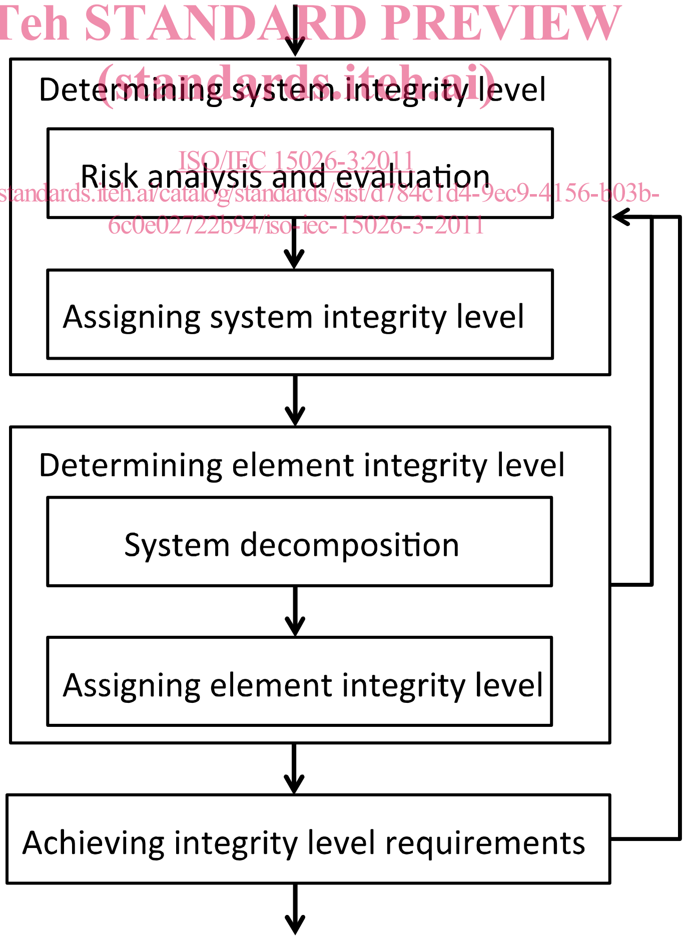
Determining system integrity level
Risk analysis and evaluation
Assigning system integrity level
Determining element integrity level
System decomposition
Assigning element integrity level
Achieving integrity level requirements

Figure 1 — Overview of activities for integrity level determination

In order to determine the system or product integrity level, a risk criterion measure for the target system is established to determine which factor (i.e., event, condition of the system, situation of the environment, etc.) is considered as a risk. Based on the criterion, risks related to the system or product are analyzed and evaluated to establish limitations on the timing and occurrence of adverse consequences and the conditions that lead to them. These limitations are preferably established by limiting the occurrence of the initiating events for these conditions. Once these limitations are established, limitations on behaviours of the system or product are derived that, if met, would meet the limitations on adverse consequences, conditions, and initiating events within limitations on allowable uncertainties.

NOTE 3 As it is the more common context in which integrity levels are used, this part of ISO/IEC 15026 speaks in terms of limiting losses (e.g. adverse consequences, dangers, or risks) but is equally applicable in terms of achieving benefits.

NOTE 4 An “adverse consequence” is a consequence associated with a loss.

NOTE 5 The phrase “initiating event” and related concepts are explained in ISO/IEC TR15026 Part 1.

For systems with behaviours that can lead to adverse consequences, limitations on the values of the properties reflect the required limitations on the occurrence, timing, and/or allowable uncertainties regarding these behaviours. For example, for systems, products, or their elements that perform a mitigating function, the properties of interest include their being invoked reliably and the availability and reliability of their services.

To assign an integrity level to a system, product, or element is in effect to assign integrity levels to the system, product, or element interfaces related to the consequences of interest. Different behaviours of the system or product can result in different severities of risk as can behaviours associated with each external interface, e.g., as a result of interfacing with different entities. The same is true for interfaces between internal system elements.

NOTE 6 Different integrity levels may be assigned to different interfaces. External interfaces of a system or product are accessible on its boundary and are implemented by the system or product elements. Likewise, integrity levels can be assigned to an element of an external system upon which the system or product depends and mechanisms connecting external system elements.

NOTE 7 In this part of ISO/IEC 15026, elements of external systems upon which the system or product depends are sometimes referred to more briefly as “external elements” and included when “elements” are referred to unless otherwise indicated. “External elements” include external services and external mechanisms for connection or service delivery.

The integrity levels for internal elements as well as for external elements upon which the system or product integrity level(s) depend derive from the integrity levels assigned to system or product interfaces. Each integrity level has a corresponding set of integrity level requirements that must be met regarding the system and related aspects and activities as well as regarding related evidence. This evidence is obtained in order to justify that the integrity levels are met within allowable uncertainty.

5 Using this Part 3

5.1 Uses of this part of ISO/IEC 15026

The intended uses of this part of ISO/IEC 15026 are for the definition of an integrity level or a set of integrity levels, the use of integrity levels during the system or product life cycle, and the assignment of integrity levels to a system or product and its elements. Integrity levels are used most commonly during design, implementation, verification, and maintenance processes in order to assure the system or product has property values that limit related risks during operations, e.g., a certain degree of reliability.

NOTE 1 The term “design” in this part of ISO/IEC 15026 includes designs from all the system or software life-cycle processes, e.g., architectural design in ISO/IEC 15288:2008 and system architectural design, software architectural design, and software detailed design in ISO/IEC 12207:2008.

NOTE 2 If this part of ISO/IEC is applied to software only, the system integrity level and the integrity levels of the non-software elements are only required in order to determine the integrity levels of the software elements.

Although the definition, determination, and application of integrity levels is accomplished within the context of applying risk management, this part of ISO/IEC 15026 covers risk analysis and evaluation only at a high level and does not cover technical and specialized risk analyses. Additional information is needed to augment the high-level requirements on risk analyses included in this part of ISO/IEC 15026 and can be found in items in the Bibliography.

Users of this part of ISO/IEC 15026 should read all its clauses because understanding the definition of integrity levels and understanding the use of integrity levels require an understanding of each other. Aspects of defining integrity levels map to their use and the needs of their users. Knowing their use can provide clarifying motivations for defining them and the resulting work products. Understanding the requirements for their use requires understanding their definition.

This part of ISO/IEC 15026 can be used alone or with other parts of ISO/IEC 15026. It can be used with a variety of technical and specialized risk analysis and development approaches such as those referenced in ISO/IEC 15026-1. ISO/IEC 15026-1 provides additional information and references to aid users of this part of ISO/IEC 15026.

Assurance cases are covered by ISO/IEC 15026-2. This part of ISO/IEC 15026 does not require the use of assurance cases but describes how integrity levels and assurance cases can work together, especially in the definition of specifications for integrity levels or by using integrity levels within a portion of an assurance case.

If the risks or the risk treatment are not well understood or if the dependency structure of the whole system or the choice of suitable claims is unclear, then an assurance case is the better choice. This particularly is the case when facing new kinds of risks or using a new kind of risk treatment. In these situations, justifying the choice of the top-level claim for the assurance case is important.

When the risks and their treatment are well understood, however, developers need not justify the choice of the top-level claim and need only select the proper claims for their context from a known set—an integrity level from a set of integrity levels. In these situations, the generic arguments created by the definers of the integrity level provide the justification that meeting the integrity level requirements will adequately show the meeting of the integrity level. Such a justification (e.g., a generalized assurance case) is usually created one time by a separate organization and used by multiple projects.

5.2 Documentation

Results, artefacts, and the performance of activities covered by this part of ISO/IEC 15026 shall be documented and this documentation's integrity preserved. Requirements for documentation of attempted and actual agreements and approvals are included in 11.4.

5.3 Personnel and organizations

The personnel and organizations performing activities covered in this part of ISO/IEC 15026 shall be competent, and organizations shall be properly concerned with the intentions and trustworthiness of their personnel. Organizations should ensure these requirements are met by taking actions corresponding to the severity of the risks involved and by following any governing requirements. Evidence of competency may be part of an assurance case.

5.4 Overview of this part of ISO/IEC 15026

Clauses 5, 5.4, and 11 relate to the definition of integrity levels. Clauses 5, 7, 8, 9, 10, and 11 relate to the use of integrity levels. The purpose and outcomes for using this part of ISO/IEC 15026 appear in 6.1 and 6.2 for defining integrity levels and 7.1 and 7.2 for using integrity levels. Prerequisites for defining and using integrity levels are covered in 6.3 and 7.3, respectively. The authorities to be identified and their agreements and approvals are covered in Clause 11. Annex A contains the inputs and outputs for the integrity level framework illustrated in Figure 1. Annex B provides a notional example covering aspects of Clauses 5.4, 7, 8, and 9.

6 Defining integrity levels

6.1 Purpose for using this part of ISO/IEC 15026

A set of integrity levels is defined for use within a specified scope of applicability for assigning integrity levels to a system or product and to internal and external elements upon which the system or product claim depends. Each integrity level has corresponding integrity level requirements that, if met, would show the acheivement of the integrity level's claim for the system, product, or element to within the allowed uncertainty. Given that the set of integrity levels is used correctly and that the integrity level claim concerning the system or product behaviours is true; the applicable risks are limited or managed acceptably.

6.2 Outcomes of using this part of ISO/IEC 15026

In order to show conformance to this part of ISO/IEC 15026, documentation shall exist that is accurate, available as required, controlled, traceable, and reviewable, whose integrity is preserved, and that covers the following:

a) An analysis showing the suitability of a hierarchical set of integrity levels within its specified scope of applicability.

b) For each integrity level defined, unambiguous:

   1) Designation of its claim, i.e., limitations on property values, scope of applicability, and allowable uncertainty of achievement.

   2) Justification that:

      i) Meeting its integrity level requirements shows the achievement of its claim within the allowable uncertainty.

      ii) Obtaining the required evidence shows the meeting of the integrity level requirements within the allowable uncertainty.

c) Unambiguous specifications and usable requirements and guidance for ensuring the proper use of the set of integrity levels within its scope of applicability. Such use includes activities performed regarding associated uncertainties and their results, the initial assignment of the system or product integrity level, and the assignment of integrity levels to system elements.

d) Identification of the approval authority for integrity level definition and outcomes of the agreement and approval activities for preceding and current agreements.

e) Records showing conformance to the normative requirements of this part of ISO/IEC 15026 for defining integrity levels including clause 5.4.

f) Relevant work products including their history and rationale that can be maintained and revised as needed.

6.3 Prerequisites for defining integrity levels

6.3.1 Establish appropriateness of area for use of integrity levels

6.3.1.1 General

Not all areas are suitable for definition and use of integrity levels. Integrity levels shall be defined for an area only if a substantial body of relevant experience exists for the area that is well understood by those performing the definition.

6.3.1.2 Risks

The following information about risks shall be well understood within a substantial body of relevant experience:

a) Risk-related concerns—potential adverse consequences and their occurrence as well as preconditions for them.

b) Property of interest (which could be a composite property) and limits on its values (across allowable degrees of risk and corresponding integrity levels).

c) Required limitations on the uncertainties involved across allowable degrees of risk and the set of integrity levels.

NOTE Throughout this part of ISO/IEC 15026, use of the word “allowable” is meant to include “acceptable” and “tolerable.” Likewise, “unallowable” includes “unacceptable” and “intolerable.”

6.3.1.3 Environment of the system or product

The following information about the environment of the system or product shall be well understood within a substantial body of relevant experience:

a) Conditions and activities in which the system or product is involved (over the relevant portion of the life cycle).

b) Constraints on the system or product operation and maintenance.

c) Dependence structure of the system or product including its elements and interactions with its environment.

d) Methods of design, implementation, test and evaluation, transition, operation, maintenance, and disposal.

e) Relevant behaviours of the environment, including influences on the system and interactions among system elements.

6.3.1.4 Relevant evidence

A substantial body of evidence should be available so that low enough degrees of uncertainty exist for evidence-based definition to be performed. Knowledge should exist regarding both normal and abnormal situations within the scope of applicability and the immediate or otherwise relevant environment.

NOTE While based on evidence from the past, a definition should satisfy the purpose of future use.

6.3.2 Establish purpose and preliminary scope

An intended purpose and preliminary scope for the integrity levels shall be established in order to ensure the involvement of the needed persons, organizations, expertise, and experience.

6.4 Consistency with use requirements

All the parts of the definition of an integrity level or set of integrity levels shall be consistent with the requirements on their use as covered in Clauses 5, 7, 8 9, 10, and 11. Any accompanying material that does not meet these requirements shall provide documented justification for and be clearly labelled as being otherwise. Related agreements and approvals are obtained in accord with Clause 11.

6.5 Analysis of scope of applicability

The benefit from integrity levels is based, in part, on the applicability allowed by their generality. The scope of applicability depends on the generality of the justification of the corresponding integrity level requirements.