INTERNATIONAL STANDARD

ISO/IEC 15026-3

Second edition
2015-12-01

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 15026-3:2015(E)

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

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

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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information Technology*, Subcommittee SC 7, *Software and systems engineering*.

This second edition cancels and replaces the first edition (ISO/IEC 15026-3:2011), 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*

— *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 ISO/IEC 15026 series.

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 corresponding 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 the following:

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, system or software users, assessors of systems or software and administrative and technical support staff 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, financial, 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 A.

2 Normative references

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

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

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

3 Terms and definitions

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

3.1
adverse consequence
consequence (3.3) that results in a specified level of loss

Note 1 to entry: An adverse consequence results from the *system-of-interest* (3.23) being in a *dangerous condition* (3.4) combined with the environment of the *system* (3.21) being in its worst-case state (relative to the adverse consequence).

Note 2 to entry: Harm in ISO Guide 51 is an instance of an adverse consequence. The concept of adverse consequences is introduced in order to cover not only harm in the safety context but also other losses such as loss of assets in the security context.

3.2
claim
proposition representing a requirement of the *system-of-interest* (3.23) that enables the system-of-interest to achieve *tolerable risk* (3.25) if it were met

Note 1 to entry: A claim is consistent with claims in the other parts of ISO/IEC 15026 series but issues of claims here are restricted to achievement of a tolerable risk.

Note 2 to entry: A safety goal required in ISO 26262 is an instance of a claim.

3.3
consequence
outcome of an event affecting objectives

[SOURCE: ISO Guide 73:2009, 3.5.1.3]

3.4
dangerous condition
state of a *system* (3.21) which, in combination with some states of the environment, will result in *adverse consequence* (3.1)

Note 1 to entry: A hazardous situation in ISO/IEC Guide 51 and IEC 61508–4 is an instance of a dangerous condition. A concept of dangerous conditions is introduced in order to cover not only hazardous situations in the safety context but also errors in the reliability, integrity, confidentiality, or dependability contexts and other states of a system which can lead to adverse consequences.

Note 2 to entry: Occurrences of failures in the context of reliability or as defined in IEC 61508–4 often, but not always, lead to dangerous conditions.

Note 3 to entry: A dangerous condition therefore has attributes, at least, a) the associated adverse consequences, b) the trigger events that lead to the dangerous condition, and c) the trigger events that lead to the adverse consequences from the dangerous condition.

3.5
design authority
person or organization that is responsible for the design of the product

[SOURCE: ISO/IEC 15026–1]

3.6
initial risk
estimated *risk* (3.16) before applying *risk reduction measures* (3.18)

3.7
integrity level
required degree of confidence that the *system-of-interest* (3.23) meets the associated *integrity level claim* (3.10)

Note 1 to entry: The words “integrity level” forms an indivisible label. This International Standard does not pronounce on, nor depend on, a concept of integrity by itself.

Note 2 to entry: An integrity level is different from the *likelihood* (3.13) 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 part of ISO/IEC 15026, integrity levels are defined in terms of risk and hence, cover safety, security, financial and any other dimension of risk that is relevant to the system-of-interest.

3.8
integrity level assurance authority
independent person or organization responsible for certifying compliance with the *integrity level requirements* (3.11)

[SOURCE: ISO/IEC 15026–1]

3.9
integrity level definition authority
person or organization responsible for defining *integrity levels* (3.7) and *integrity level requirements* (3.11)

3.10
integrity level claim
claim (3.2) representing a requirement for a *risk reduction measure* (3.18) identified in the *risk treatment* (3.20) process of the *system-of-interest* (3.23)

Note 1 to entry: In general, it is described in terms of requirements that, when met, would avoid, control or mitigate the *consequences* (3.3) of *dangerous conditions* (3.4) and provide *tolerable risk* (3.25).

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

3.11
integrity level requirement
set of requirements that, when met, will provide a level of confidence in the associated *integrity level claim* (3.10) commensurate with the associated *integrity level* (3.7)

3.12
level of risk
magnitude of a *risk* (3.16) or combination of risks, expressed in terms of the combination of *consequences* (3.3) and their *likelihood* (3.13)

[SOURCE: ISO Guide 73:2009, 3.6.1.8]

3.13
likelihood
probability of something happening

3.14
property-of-interest
any property that, if lost, is considered a negative effect

Note 1 to entry: The concept of property-of-interest is introduced in order to characterize negative effects of *consequences* (3.3).

Note 2 to entry: In the safety context, human lives and health are instances of properties-of-interest.

Note 3 to entry: Assets in the security context, e.g. defined in ISO/IEC 15408-1, are instances of properties-of-interest.

3.15
residual risk
risk (3.16) remaining after *risk treatment* (3.20)

[SOURCE: ISO Guide 73:2009, 3.8.1.6]

3.16
risk
effect of uncertainty on objectives

[SOURCE: ISO Guide 73:2009, 1.1]

Note 1 to entry: An effect is a deviation from the expected: positive and/or negative. In this International Standard, the focus is on negative deviations leading to *adverse consequences* (3.1).

Note 2 to entry: Risk is often characterized by reference to potential events and *consequences* (3.3), or a combination of them.

Note 3 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated *likelihood* (3.13) of occurrence. In this International Standard, risk is characterized as the combination of the severity of the adverse consequence and the likelihood of an adverse consequence occurring.

Note 4 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

3.17
risk criteria
terms of reference against which the significance of a *risk* (3.16) is evaluated

[SOURCE: ISO Guide 73:2009, 3.3.1.3]

3.18
risk reduction measure
steps taken to reduce or mitigate *risk* (3.16)

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

3.19
risk source
element that, alone or in combination, has the intrinsic potential to give rise to *risk* (3.16)

[SOURCE: ISO Guide 73:2009, 3.5.1.2]

Note 1 to entry: A hazard in ISO Guide 73:2009 is an instance of a risk source.

Note 2 to entry: A fault, an error, or a failure in the context of reliability can be a risk source. The definitions of those terms can be found in IEC 61508–4.

Note 3 to entry: A threat in the context of security, a *threat agent* (3.24), and an adverse action defined in ISO/IEC 15408-1 can be a risk source.

3.20
risk treatment
process to eliminate *risk* (3.16) or reduce it to a tolerable level

[SOURCE: ISO Guide 73:2009, 3.8.1, modified]

3.21
system
combination of interacting elements organized to achieve one or more stated purposes

[SOURCE: ISO/IEC/IEEE 15288]

3.22
system element
member of a set of elements that constitutes a *system* (3.21)

[SOURCE: ISO/IEC/IEEE 15288]

3.23
system-of-interest
system (3.21) whose life cycle is under consideration in the context of ISO 15026

[SOURCE: ISO/IEC/IEEE 15288]

3.24
threat agent
entity that can adversely act on *property-of-interest* (3.14)

[SOURCE: ISO/IEC 15408-1:2009, 3.1.71, modified]

3.25
tolerable risk
level of risk (3.12) that is accepted in a given context based on the current values of society

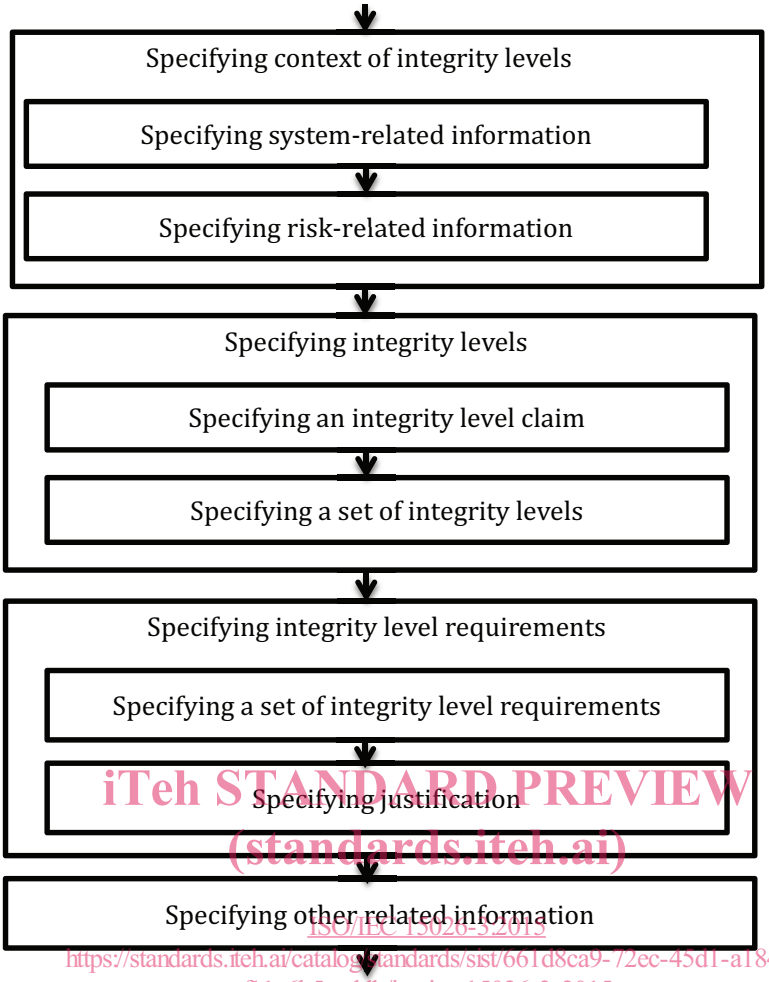
[SOURCE: ISO/IEC Guide 51:2014, 3.15]

Note 1 to entry: A tolerable risk is sometimes called acceptable risk, e.g. ISO/IEC/IEEE 16085, and ISO 14971. The general risk management standards ISO Guide 73 and ISO 31000 use both phrases without explicit definitions.

4 Defining integrity levels

4.1 Expected readers of this Clause

This Clause explains the process of defining a set of integrity levels for a specific system domain and general requirements for related-products, such as integrity levels, integrity level claims, and integrity level requirements. Thus, the expected readers of this Clause are organizations which develop specifications defining a set of integrity levels. Those organizations, which are called integrity level definition authorities, include international or domestic standardization organizations, any other standardization organizations, arbitrary industry organizations, or a department in an organization which is responsible for the organization's policy or standard for contract management. Figure 1 shows the overview of the process of defining integrity levels.



Key

↓ flow of processes

NOTE Iteration of processes is not shown for simplicity.

Figure 1 — Overview of the process of defining integrity level

4.2 Appropriate area to define integrity levels

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. Integrity levels can be used for areas where levels of risks (e.g. high, medium, low risk) can be clearly defined. Each level of risk provides a basis for a different required degree of confidence that the integrity level claim is met.

NOTE When dealing with risks of a system in an area where a substantial body of relevant experience does not exist, then the use of an assurance case is appropriate.

4.3 Specifying context of integrity levels

4.3.1 Specifying system-related information

The following information about systems in the target area shall be specified by the integrity level definition authority in order to clarify the scope of applicability of the integrity levels being specified:

a) definition of the target class of systems;

b) assumptions on the environment.

NOTE Examples of a definition of a target class of systems can be found in IEC 61508 and ISO 26262. The definition of target classes of systems of IEC 61508 and ISO 26262 pertain to "electrical/electronic/programmable electronic (E/E/PE) systems are used to carry out safety functions" and "safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg", respectively.

4.3.2 Specifying risk-related information

The following information about risks related to systems in the target area shall be specified by the integrity level definition authority in order to clarify the scope of applicability of the integrity levels being specified:

a) property-of-interest;

b) possible adverse consequences;

c) possible dangerous conditions and the states of the environment that together with the dangerous condition will result in an adverse consequence;

d) risk criteria;

e) tolerable risks;

f) assumptions on the structure of risk reduction measures.

Information about properties-of-interest gives a definition of negative effects. An adverse consequence can have the following attributes but is not restricted to:

— description of the event that leads to the consequence;

— likelihood of the occurrence of the event;

— severity of the consequence;

— controllability of the event;

— exposure (time) to the event.

Dangerous conditions can be classified by the type of events that leads to the condition. The following event types should be taken into account:

a) random failures;

b) systematic failures;

c) failures caused by interactions between system elements without any faults of those system elements;

d) failures caused by interactions between elements of the environment and the system (for example, failures caused by a threat agent).

Likelihood of a dangerous condition should also be considered.