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.

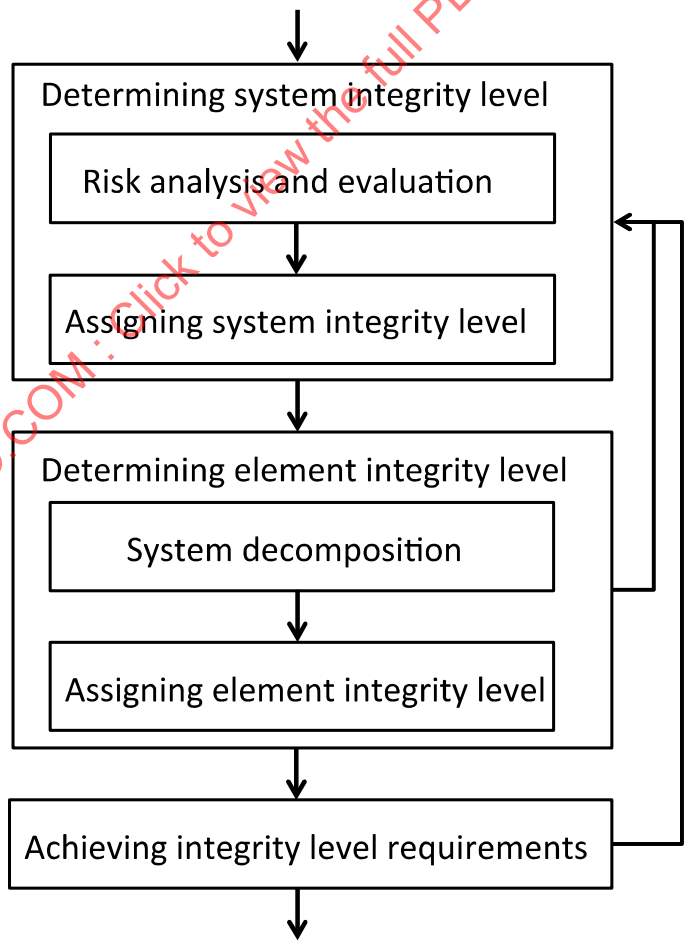

Figure 1 — Overview of activities for integrity level determination

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.

This justification in turn results from a thorough understanding of the scope of applicability and accompanying analysis. Analysis is performed in order to produce specifications for integrity levels and to ensure their needed applicability, suitability, accuracy, completeness, and allowable uncertainty that will be associated with their use. This includes addressing the aspects listed in 6.3.1.

Any risk analyses should conform to the requirements of 8.2.3 Risk analyses.

NOTE Use of integrity levels can contribute to providing grounds for confidence with stakeholders and limitations on uncertainty. However, this part of ISO/IEC 15026 specifies neither the requirements to be met in order to achieve the grounds for a stated degree of confidence nor specific limitations on uncertainty.

6.6 Three required work products

Integrity levels are usually defined once and used many times. As explained in 4.1, integrity level specifications include two kinds of related requirements and the justification relating these two requirements. Thus, three unambiguous work products consistent with the framework in 4.1 shall be documented for each integrity level.

a) "Integrity level"—What the integrity level fulfils or claims: namely a requirement or claim that the system, product, or element meets:

   1) A range of target values for a property, e.g., a quality characteristic such as reliability or occurrences of dangerous failures.

   2) A limit on scope of applicability—typically, within a specified scope under specified conditions.

   3) Specified limitations on uncertainty.

b) "Integrity level requirements"—What the integrity level imposes on:

   1) What is done and how, when, etc., including requirements related to organization, processes, activities, tasks, methods, means and resources including personnel and tools, work environment, communication, management or coordination, record keeping, and other aspects of performance.

   2) The system, product or element, including requirements on associated material, services, and artefacts including any software.

   3) The obtained evidence, which may include limitations on allowable remaining uncertainty associated with evidence, e.g., uncertainty remaining after a test is passed.

c) Justification of "integrity level requirements"—A justification showing that meeting the integrity level requirements supports meeting the integrity level claim within the required limitations on uncertainty.

The following three clauses further explain these work products.

6.6.1 Specifying an integrity level claim

Specifying an integrity level claim is essential to defining its meaning and thus should be unambiguous.

To ensure the coverage of conditions of use, the scope of applicability of an integrity level shall include the potential presence for a system, product, or element of:

a) Random failures and dangerous behaviours and events.

b) Systematic failures unless documented justification is provided for doing otherwise.

c) Failures and dangerous events and behaviours resulting from maliciousness, including treating these failures as systematic failures unless documented justification is provided for doing otherwise,

6.6.2 Specifying integrity level requirements

Meeting an integrity level requirement shows the achievement of limitations on the values of a property, under certain conditions, and within a particular uncertainty.

Evidence required by each integrity level's corresponding integrity level requirements is essential to defining and specifying them and evaluating their achievement. To have an acceptably established specification, integrity level requirements shall:

a) Be consistent with the justification or source relating the integrity level to its integrity level requirements (6.6.3). This includes assuring the integrity level's use is within the scope of applicability supported by the justification including the dependencies involved and the method for assigning integrity levels to system or product elements.

b) Require evidence imposed by the integrity level requirements to show the meeting of all the integrity level requirements including the achievement of any limitations on uncertainty.

NOTE 1 In some situations, user justifications can be required of their interpretation and application of the integrity level requirements (particularly if selection among alternatives is possible) and of their evidence showing the meeting of integrity level requirements. This is also relevant in 6.8 Information provided for users.

c) Cover relevant aspects of the characteristics and behaviour of infrastructure upon which achievement of the claim depends including any mechanism implementing a connection with external elements (or entities).

d) Cover the integration of subordinate elements within a system, product, or element consistent with achieving the integrity level of the super-ordinate system, product, or element.

e) Include the required scope of assignment of integrity levels to internal system elements and other elements depended upon.

f) Span over time including tracking the performance of the system, product, or element in order to detect and, if practicable, to avoid exceeding required limitations.

NOTE 2 Before transition and operation, such requirements may be met by the system or product providing necessary support and included in documentation, training, human interfaces, other aids, trials, and, if warranted, agreements. This span of time generally includes development.

g) Require the meeting of the requirements of Clause 10.

h) Show that the stringency, thoroughness, rigor, and other quality characteristics required of evidence and accompanying information are appropriate to requirements deriving from the justification for integrity level requirements.

Use of alternative means for meeting integrity level requirements is covered in 10.2. However, integrity level requirements may prohibit or restrict alternative means. Integrity level requirements should include detection of warnings for and indications of the need for action throughout the life cycle.

6.6.3 Justification of match between integrity level claim and its requirements

6.6.3.1 General

For each integrity level documented justification shall be provided or a source or sources shall be identified and justified that shows—throughout the scope of applicability and within the required limitations on uncertainty—that:

a) Meeting the integrity level requirements shows the achievement of the integrity level claim.

b) Meeting the requirements for evidence shows the meeting of integrity level requirements.

The documented justification includes coverage of all entities upon which achievement of the integrity level depends. The documentation is agreed upon and approved in accord with Clause 11.

NOTE 1 A single justification may show that meeting the requirements for evidence shows the achievement of the claim.

NOTE 2 Restrictions and assumptions included in or implied by the justification of the integrity level requirements are consistent with the integrity level's scope of applicability. This includes requirements on engineering done during integrity level use (6.8), for example design restrictions and limitations on methods used to assign integrity levels to system elements and external dependences.

6.6.3.2 Using assurance case in justification

An assurance case may be used in this justification. Some restrictions can arise from the nature of the argument, particularly restrictions on engineering such as the method of assigning integrity levels to system elements during design. The assurance case establishes required evidence. A single general assurance case structure might cover one or multiple integrity levels. Thus, when an assurance case is used, achievement of an integrity level equates to a claim in the assurance case and its integrity level requirements derive from the need to ensure the scope of the argument, the consistency of claims within it, and the achievement of the evidence required by the assurance case.

Ensuring applicability of argumentation shall cover ensuring conformance to the integrity level claims and the applicability conditions to those claims as well as any requirements to assure assumptions. This includes any limitations on the scope of the dependencies and methods for assigning integrity levels to the system or product elements that are included in the justification.

The integrity level requirements should include a set of evidence required by all or a portion of an assurance case (or set of assurance cases) as well as evidence that the conditions on its matching claim and any other assumptions are met.

NOTE 1 For example, an approach might take the form of a general assurance case for the area of applicability and normal approaches to design, implementation, operation, maintenance, and disposal. It might have a top-level claim concerning a property of widespread importance (e.g., safety), useful limitations on property values and uncertainty under specified conditions, and an argument that cover the needs of the area of applicability.

NOTE 2 Some think of an integrity level, including justifications of its integrity level requirements and evidence, as similar in purpose to a general, pre-packaged, reusable assurance case. Conversely, integrity levels can be used to support a claim within an assurance case where the claim matches an integrity level.

6.7 Maintaining integrity level specification

Maintaining the usefulness and usability of the integrity level claim, corresponding integrity level requirements, and the validity and adequacy of the justification matching them is the main motivation for updating an integrity level specification and associated justification. The integrity level specification and its associated justification shall be maintained including assessing the possible need for updating whenever a potentially significant change occurs or a previous oversight is discovered in the integrity level's area of applicability. A significant change includes newly discovered or worsening (e.g., the factors or their adverse consequences become larger, more frequent, more likely, of longer duration, less predictable, expected sooner, or more costly) factors such as the following.

a) Risk dimensions with significant potential relevance.

b) Dangerous conditions.

c) Initiating events.

d) Sources of danger.

e) Sources or degree of uncertainty.

f) Consequences.

g) Deficiencies in capability.

h) Mitigation mechanisms.

i) Interfaces, interactions, connections, or dependencies of an applicable system with its environment.

NOTE "Dangerous conditions" are further explained in Clause 8 and in ISO/IEC TR 15026-1

6.8 Information provided for users

6.8.1 Requirements

Specifications for integrity levels shall include or be accompanied by information allowing users to:

a) Understand the set of integrity levels and its corresponding integrity level requirements.

b) Establish that the scope of applicability of an integrity level (or set of integrity levels) covers the scope of use.

c) Judge the feasibility and merit of use.

d) Perform activities in accordance with the integrity level justifications, in particular, assignment of integrity levels to systems, products, and elements. From the integrity level(s) assigned to a system or product, these activities derive the integrity levels assigned to the system elements and external elements it depends on.

e) Establish whether integrity level requirements have been met.

f) Perform the activities and/or use methods related to associated uncertainties.

g) Identify the approval authority for the integrity level specification, including justification, and accompanying materials and aids.

6.8.2 Guidance and recommendations

Information should be provided to aid users of the integrity levels including:

a) Insight and aid regarding risk analysis and evaluation to the extent practicable.

b) Guidance on the determination of the integrity level to assign to a system or product—for example, the situations under which to assign a specific integrity level to a particular external interface of a system or product.

c) Information to facilitate engineering consistent with the justification of integrity level requirements.

d) Guidance to facilitate the meeting of the requirements of Clause 10.

7 Using integrity levels

7.1 Purpose for using this part of ISO/IEC 15026

An integrity level assigned to a system or product states a claim concerning the behaviours and conditions of that system or product, such that, the objective for using integrity levels is met if this claim is true. Generally, this objective would limit or manage the risks associated with the system or product acceptably. The derived integrity level for each system element states a claim regarding those of its behaviours upon which the integrity level claim of the system or product depends. Each assigned integrity level has integrity level requirements that when met show the achievement of the integrity level claim of the system element to within the allowed uncertainty.

NOTE The use of integrity levels normally contributes to providing grounds for stakeholder confidence and support for their decision making.

7.2 Outcomes of using this part of ISO/IEC 15026

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

a) The integrity level claim, i.e., limitations on property values, conditions of applicability, and limitations on uncertainty.

b) Integrity level requirements for each integrity level used.

c) Justification or source that:

   1) Meeting the corresponding integrity level requirements suffices to show the achievement of the integrity level claim.

   2) Obtaining the required evidence suffices to show the meeting of the integrity level requirements.

NOTE Outcomes a), b) and c) should result from defining integrity levels (see 5.4). While this part of ISO/IEC 15026 may be used with integrity levels that were not defined in conformance with 6, a), b) and c) are always required.

d) Unique identification including version, date, number, instance or instances, and tag information for a system, product, or element for which conformance is claimed.

e) Assignment of an integrity level to the system or product.

f) Assignments of integrity levels to the system elements upon which the system or product depends for achievement of the assigned integrity level or set of integrity levels of the system or product and justification of these assignments to system elements.

g) The activities performed regarding associated uncertainties and their results.

h) The qualifications of the methods and tools used and justifications of their use.

i) The evidence required by the integrity level requirements of the assigned integrity levels, or acceptably showing the achievement of the integrity level or these integrity level requirements by other approved means. Evidence is properly obtained, its integrity preserved, and its required availability provided.

j) Outcomes of current and any related preceding agreement and approval activities.

k) Records showing conformance to the normative requirements of this part of ISO/IEC 15026 regarding using integrity levels.

l) The relevant work products that can confirm the meeting of the assigned integrity level requirements.

7.3 Prerequisites for use of integrity levels

7.3.1 Determine scope of covered risks

The determination of the scope to which this part of ISO/IEC 15026 is applied shall properly reflect the stakeholders and their interests. It shall also reflect prior decisions allocating a scope to the risks covered under this part of ISO/IEC 15026 and the scope of risks to be covered elsewhere. This allocation can be done by risk dimensions (e.g., safety, economic, security) or otherwise. The following apply:

a) The result of the scope decision shall be clearly defined, agreed upon and approved in accord with Clause 11, and documented.

b) The scope of coverage under this part of ISO/IEC 15026 shall correspond with achieving the intended purpose of its use.

c) The scope shall cover maliciousness unless a sensible justification is documented and agreed upon and approved in accord with Clause 11.

d) All adverse consequences and risks relevant to the system or product should be determined to be assigned responsibility somewhere—inside or outside the scope of activities covered by this part of ISO/IEC 15026.

e) Whenever relevant risks or other conditions are discovered that no one has the responsibility to analyse, those risks shall be assigned to relevant persons and/or organizations and shall be identified to those with agreement and approval authority in accord with Clause 11.

7.3.2 Establish applicability of integrity levels to the scope of their use

The integrity level or set of integrity levels used from an identified source or sources shall be applicable to the situation and system or product to which the integrity level or set of integrity levels is assigned, including applicability for each:

a) Integrity level claim.

b) Integrity level requirement.

c) Justification of the integrity level requirements establishing support for the claim. This includes the dependencies and method for assigning integrity levels to system or product elements that are included in the justification.

The scope, nature, and limitations of all of these require applicability to the situation and system or product including the arguments, assumptions, and evidence used in the justification. In addition, the materials accompanying these should fit the intended scope of use.

7.3.3 Decide role of integrity levels in life cycle

Users of this part of ISO/IEC 15026 should establish the intended role of integrity levels within their system or product life cycle. The process described in this part of ISO/IEC 15026 is presented as distinct from the overall life cycle processes. The intention of this part of ISO/IEC 15026 is to encourage but not require that integrity level use be integrated with the system or software life cycle processes.

7.3.4 Establish approach to risk analysis

The approach to risk analysis and evaluation should fit the situation. Risk analysis might be being performed for other reasons already, and this analysis is to be augmented as necessary. Standards or guidelines can exist for use within a relevant scope. In addition, risk analysis could involve use of assurance cases.

8 System or product integrity level determination

8.1 Introduction

Determining the integrity level of the system or product involves the following activities:

a) A risk criterion measure is defined that specifies a measure or scale to be used.

NOTE 1 “Risk criteria” is defined in ISO/IEC 16085:2006 *Systems and software engineering — Life cycle processes — Risk management* as “The terms of reference by which the significance of risk is assessed” and includes the following note: “Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic and environmental aspects, the concerns of stakeholders, priorities and other inputs to the assessment.”

NOTE 2 A risk criterion measure may be stated in terms of adverse consequence multiplied by its probability of occurrence or in other terms (e.g., maximum loss) and may be a combination of component measures.

b) Required limitations on allowable risk criterion values are established. The required limitations are obtained as a result of risk analysis and evaluation.

c) The integrity level assignment(s) to the system or product derive from these limitations and are such that meeting them implies meeting these limitations on occurrence and timing within limitations on uncertainty. Thus, the system or product integrity level corresponds to allowable risk criterion values.

NOTE 3 Within the safety community this might be stated as, “Integrity Requirement is expressed using a risk criterion measure that is mapped to integrity levels (which are normally a quantisation of the risk criterion measure). The limitation on the risk criterion for the system or product maps to a particular integrity level for the system or product. (This, in turn, will correspond to integrity level requirements—or obligations.)”

8.2 Risk

8.2.1 Introduction

For performance of a risk analysis, information is needed about the system or product, its environment and stakeholder requirements and the risk dimensions and related properties relevant to the system or product. Examples of related properties include integrity, availability, reliability, and confidentiality as well as properties related to safe and economical use. Any risks identified by the risk analysis are analyzed with the system or product interfaces, and an integrity level is assigned to the system or product and its interfaces. These system or product integrity levels reflect the required values of the associated risk criterion.

NOTE The ultimate operational goal of the approach to risks and uncertainty in ISO/IEC 15026 is benefiting (or at least protecting) stakeholders and improving their decision-making. Achieving lower uncertainty in engineering terms leads to better grounds for confidence and bases for decision-making. In general, while uncertainty relates to engineering, stakeholder confidence is a subjective state that can be idiosyncratic or even irrational. Therefore, to ensure the proper use of engineering results, the uncertainties referred to in this part of ISO/IEC 15026 generally have more objective values than the subjective degree of confidence a stakeholder might derive from integrity level use.

8.2.2 Risk criterion

8.2.2.1 Specification of risk criterion

A risk criterion specifies the meaning or method of measurement of system- or product-related risk and is used to specify limitations on risk. This risk criterion shall:

a) Be established along with the risk-related measurement scale.

b) Have the limitations required on its value specified.

c) Be consistent with governing requirements such as legal, regulatory, or contractual requirements, including the limitations identified in b).

These risk criterion specifications and any related justifications are agreed upon and approved in accord with Clause 11.

8.2.2.2 Methods for risk criterion calculations

The methods used for risk criteria calculation provide results that can be compared against the risk criterion specifications. The more demanding the situation, the more reliable, robust, and fitting to the situation the methods used for risk criterion calculation should be. When assessing calculation methods the following shall be documented:

a) The methods and tools used for risk criterion calculations.

b) Approaches used for and the results of method and tool assessments.

Multiple methods for risk criterion calculations may be specified for differing circumstances. Additional methods chosen should have results consistent with, or more pessimistic than, others.

NOTE The methods used for risk criterion calculation should have a logical justification reflecting their intended use This includes the correspondence of their reliability and robustness to the related consequences, the degree of novelty, the stringency of the claims and limitations on uncertainty, and the relevant state of the art.

8.2.3 Risk analyses

8.2.3.1 General

Fundamentally, risk analysis is performed to answer three questions: what can go wrong, when, and with what consequences. Ultimately the concern is adverse consequences. The risk analysis can cover multiple risk dimensions such as safety, economic, and security. The scope, determined in accord with 7.3.1, can establish the dimensions to be covered. Relevant aspects include the capabilities of the system or product, the relationships of the system or product with its environment, and the analyzability of the system or product.

The system or product integrity level corresponds to allowable risk criterion values. The occurrence and timing of conditions or behaviours (including failure) can affect this value either directly or because its functionality includes mitigation of consequences of initiating events within the environment or dangerous conditions. Dangerous conditions are conditions associated with the system or product that could lead to adverse consequences.

NOTE 1 The outcomes of both risk analysis and risk evaluation (see 8.2.4) can result in changes to the system or product design to eliminate or reduce risks. Such changes could require the risk analysis and/or evaluation activities to be repeated.

NOTE 2 Risk analyses and evaluation should include the history of the same or similar situations and include efforts to evaluate the degree of completeness of the results. Over time, these efforts should build an improved understanding and representation of the situation. Records should be kept even if those records are not immediately needed.

8.2.3.2 Required occurrences of risk analysis

Risk analysis and/or evaluation shall be performed:

a) Initially, before the first assignment of an agreed upon or approved system or product integrity level.

b) Whenever aspects of the situation that affect risk are identified as potentially worsening or as not having been previously identified or analysed, including those listed in 6.7, unless effect analysis shows risk analysis to be unnecessary.

c) Whenever a system or product interface with a dependency on its environment changes, unless documented justification is provided for doing otherwise.

After establishment of the system or product design, confirmation should be obtained that the integrity levels assigned to the system or product interfaces reflect the required risk criterion values.

8.2.3.3 Identification of possible adverse consequences

System-related adverse consequences shall be identified and evaluated.

NOTE In addition to external adverse consequences, system elements can cause “internal” adverse consequences (e.g. corruption of information).

8.2.3.4 Identification of dangerous conditions

The following shall be agreed upon and approved in accord with Clause 11:

a) The relevant conditions, behaviours, and events and the relations among them.

b) Justification for their identification as relevant (or in some cases not relevant).

Conditions associated with the system or product that could lead to adverse consequences (dangerous conditions) should be identified together with their initiating events.

NOTE 1 An identified condition might allow, facilitate, cause, prevent avoidance or mitigation of, change, or contribute to adverse consequences or to the transition to another (more) dangerous condition.

NOTE 2 An undesirable event, dangerous condition, or transition between conditions can have an associated uncertainty of occurrence. Sequences of conditions and/or events can lead to an immediate precondition for an adverse consequence followed by an actual adverse consequence. The precondition for an adverse consequence can be a combination of the "conditions" identified from analyses that might need to occur simultaneously or with certain timing.

In this context, dangerous conditions are associated with a system or product if:

a) The failure of the system or product could lead to the dangerous condition.

b) Operation of the system or product within the scope of applicability of the integrity level claim or its involvement in other life cycle processes could lead to a dangerous condition.

c) The system or product performs a mitigating function for an initiating event in the environment that could lead to the dangerous condition.

d) Behaving or operating as specified leads to the dangerous condition, but as a result of deliberate decisions made with awareness that this can happen.

NOTE 3 Failures can vary in their potential adverse consequences; some could be insignificant. However, in identifying these variations all failures need to be considered as well as the range of events and conditions that might occur. Conditions and events in the environment affected by a system or product can in turn affect its future situation.

Unanticipated dangerous conditions can occur and initiating events can be unknown. Dangerous conditions should be considered regardless of how those dangerous conditions arise.

8.2.3.5 Consideration of system or product architecture

The system or product architecture (when available) shall be taken into account during dangerous condition and event identification to ensure that failure modes, behaviours, conditions, characteristics specific to the technologies used, and interactions with the environment are considered.

NOTE 1 As this is an investigative technique, it does not conflict with the requirement in 8.4 that the integrity level of the system or product not depend on its internal architecture.

NOTE 2 In part, analysts and designers often deal with the results of risk analyses and identified potential adverse consequences and dangerous conditions while creating or later changing a system design or its operation or maintenance procedures.

8.2.3.6 Consequence analysis

Consequence analysis is used to estimate the severity of a dangerous condition as it relates to the occurrence of adverse consequences. Measures that might mitigate the adverse consequence of the initiating event(s) or dangerous conditions should be identified. For related discussion, see 7.3.4.

8.2.3.7 Occurrence and timing analyses

Occurrence, timing, and uncertainty analysis are used to estimate the likelihood of each consequence, dangerous condition, or initiating event.

Timing for conditions (e.g., occurrence and duration) or event occurrence (e.g., frequency) shall be estimated meeting any requirements on the uncertainty of the result. This estimate should use multiple sources including relevant historical data, results synthesized by analytical or engineering techniques (see ISO/IEC 15026-1 for relevant references), and estimations deriving from expert judgment.

NOTE The results of analyses may be expressed in quantitative or qualitative terms such as terms for ranges of frequency (e.g. Frequent, Probable, Occasional, Remote, Improbable, or Incredible) as long as the requirements for comparisons with the risk criterion are met.

8.2.3.8 Using assurance cases in determining the integrity level of the system or product

When an assurance case or partially completed assurance case is available during risk analysis, it might be useful for establishing limitations associated with the system or product during risk analysis and for confirmation of the identification of the properties in integrity level claims.

NOTE In relating assurance cases and integrity levels, their respective claims can be mapped to each other.

8.2.4 Risk evaluation

The results from risk analysis and evaluation includes required limitations on the occurrence, timing, and value of consequences, conditions, and associated uncertainties from which system or product requirements can be derived.

The following shall be performed:

a) Establish the required limitations on the occurrence and timing of behaviours and/or conditions of the system or product and the associated allowable uncertainties regarding conformance to these limitations.

b) Consider the possibility of behaviours or conditions associated with the system or product, rather than the system or product or its elements failing to meet specifications, as causing the risk criterion not to be met.

Risk evaluation and its results are agreed upon and approved in accord with Clause 11.

NOTE Nothing in this part of ISO/IEC 15026 should be interpreted as requiring or allowing the assignment of integrity levels such that the risk criterion associated with the system or product is not met.

8.3 Assignment of system or product integrity level

The required limitations on the occurrence, timing, and value of consequences and conditions and the associated uncertainties resulting from risk analysis and evaluation shall be used to establish the required limitations on occurrence and timing of behaviours of the system or product. An integrity level can be assigned to the entire system or product and thereby to all relevant interfaces or a distinct integrity level can be assigned to each interface. In the latter case the integrity level also applies to the system or product element implementing that interface.

The integrity level or levels assigned shall have integrity level claims that meet the derived limitations on the system or product behaviours. To achieve this, at least one of the following is required:

a) Meeting the system or product assigned integrity level implies meeting the required limitations on the system or product behaviours.

b) The system or product integrity level is consistent with meeting the required limitations on the system or product behaviours but does not imply them. Other methods are then used to provide the information needed to show that the actual behaviours of the system or product meet the required limitations on

behaviours within the required limitations on uncertainty. These other methods and their results and documentation are agreed upon and approved in accord with Clause 11.

NOTE Some system, product, or element interfaces might have no integrity-level-related dependence or reliance upon them by external entities. While such interfaces need not be assigned an integrity level, these interfaces should be assigned at least the lowest integrity level.

8.4 Independence from internal architecture

The system or product integrity level or those required at its external interfaces shall not depend upon the internal architecture of the system or product. For this purpose, the system or product should be regarded as a black box.

8.5 Maintaining system or product integrity level

8.5.1 Introduction

The reasons for re-establishing integrity levels are in three categories: (1) the system has changed (2) an unidentified risk has become known and (3) user requirements have changed.

8.5.2 System changes

The need for reestablishment of the system or product integrity level shall be assessed and, if necessary, re-established in accordance with this part of ISO/IEC 15026 whenever a system or product change is proposed or implemented.

8.5.3 Risks becomes known

The need to re-establish the integrity level of a system or product shall be assessed and, if necessary, the integrity level re-established in accordance with this part of ISO/IEC 15026 whenever:

a) A risk analysis or evaluation result exists that was not reflected in the latest decision assigning the system or product integrity level.

b) A decision is being made among alternative designs and their required risk criterion values differ.

c) The system or product has newly discovered or suspected opportunities for dangerous conditions, violation of relevant claims, or worsening associated adverse consequences.

d) Faults occur that are not promptly corrected.

e) Newly discovered or suspected dangers or failures exist or are indicated by operational data.

f) The system or product design or functionality changes include mitigating (e.g., eliminating, preventing or avoiding, limiting, reducing, or managing) consequences.

g) The system or product design does not result in meeting the risk criterion.

8.5.4 Requirements change

The need to re-establish the integrity level of a system or product shall be assessed and, if necessary, re-established in accordance with this part of ISO/IEC 15026 whenever the user requirements for the system change.

8.6 Traceability of system or product integrity level assignments

The assignment of the system or product interface integrity levels shall be traceable to their limitations from risk evaluation, the method used, and the actual performance of their determination.

9 Assigning system element integrity levels

9.1 General

A system or product consists of one or more elements. An element can be solely software, solely hardware, composed of other entities, or composed of combinations of these. Elements can be depended upon (used) by multiple elements and can depend upon (use) multiple elements.

Interface behaviour relevant to the achievement of its integrity level depends directly or indirectly on system or product elements that implement that interface. Once integrity levels are established for the interfaces—either uniformly for the system or product or individually—integrity levels need to be established for these elements. These element-related assignments can be complicated by the inability to assign new integrity levels to already existing elements. In addition, the possibility exists for elements to cause “internal” adverse consequences (e.g., physical damage to a system) that affect integrity level assignments.

Assignment of integrity levels to system or product elements depends on the design of the system or product and its elements. Normally the property in an integrity level claim of a system element is the same as that of the elements depending on it. However, this relationship can be affected by the element’s role(s) within the design.

9.2 Architecture and design

9.2.1 General

The architecture and design of the system, product, or element that depend on the system element being assigned an integrity level shall:

a) Be defined in sufficient detail prior to assignment of integrity levels to allow identification of element roles and their interfaces and to provide the needed basis for identification of relevant dependencies.

b) Allow verification of these dependences.

For the approach to integrity levels presented herein to be most effective, the analysability of the system or product and its elements regarding the relevant property or properties should be ensured or confirmed.

NOTE Consideration should be given to the design's capability to implement given assignments of integrity levels.

9.2.2 Failure handling mechanisms

Failure handling mechanisms comprised of one or more system elements can be used to detect system or product element failures and to take action to prevent unallowable consequences. In these cases, the system or product element failure is still a concern if the failure occurs and the failure handling mechanism is ineffective. Examples of failure handling mechanisms include data integrity checks (software), hardware watchdog timers (hardware), and manual recovery (humans). Design features such as redundancy, diversity, and separation (e.g., separation in time or space, partitioning, control of interaction, segregation, barriers, non-interference, guards, or isolation) can affect the integrity levels required of system elements.

NOTE 1 Redundancy can be used to prevent failures from leading to dangerous conditions, provided common mode failures among the redundant elements are avoided (for example by proper diversity among them).

NOTE 2 Design consideration should be given to capabilities for flexibility and adaptability, detection and early warning, damage confinement, diagnosis and repair, providing ongoing situational awareness, making rapid decisions in emergencies, and recovering rapidly, in combination with the environment, from occurrences of dangerous conditions and adverse consequences. See also 9.5.2

9.3 Assignment

Each system element or element interface that is depended upon by system elements also assigned integrity levels or that provide an external interface for the system or product upon which entities depend shall be assigned an integrity level using a method consistent with the:

a) Specifications of integrity levels being used and the justification for their integrity level requirements.

b) Dependencies involved.

c) Requirements in 9.5.2 and 9.5.3.

d) Lower integrity levels allowable only from the use of design features that have been agreed upon and approved in accord with Clause 11 and only within the limits agreed upon and approved. For example, consideration of the degree of benefit provided by a failure handling mechanism and the definition of what constitutes adequate diversity.

NOTE 1 Generally, the combination of the roles of each element and the integrity levels of these elements need to result in achieving the integrity level assigned to an element (its interfaces).. An element with multiple dependencies upon it that are related to a set of integrity levels needs to be assigned the highest integrity level among these except as provided by special considerations and allowances within this part of ISO/IEC 15026.

NOTE 2 Issues that need to be assured by design, implementation, operation, and related evidence are (1) interfacing occurs with the proper entity or entities, (2), these entitles have the proper interfacing behaviours, and (3) integrity is maintained across the connection. These issues often include concerns related to the characteristics and behaviour of a mechanism implementing the connection (e.g., communication infrastructure). Altogether, these issues are sometimes called “interface integrity”.

9.4 Scope of assignments

Assignment of integrity levels shall be performed for a scope consistent with the integrity level requirements corresponding to the set of integrity level specifications and justifications of the integrity level requirements. This scope is agreed upon and approved in accord with Clause 11.

9.5 Special considerations

9.5.1 Cycles and recursion

The network formed by dependency relations can include cycles. If a cycle (or recursion) exists, then:

a) The methods applied shall completely cover all possible numbers of cycles or levels of recursion.

b) Documentation shall be provided for these methods and may be provided with the integrity level definition.

For cycles and recursion, automated tools should be used to perform and/or check the methods used.

9.5.2 Special situations and requirements regarding integrity levels

For the following situations additional requirements or guidance and recommendations apply:

a) If the integrity assurance authority judges potential consequences as catastrophic or severe, then the rigor, completeness and depth of analyses and verification shall be justifiable as corresponding to these consequences.

b) If the state or behaviour (including failure) of any element, in isolation or in combination with states of other elements, will result in non-delivery of a mitigating function—more specifically, not always invoked when required or not available and performing correctly when invoked—analyses shall include occurrences of the need for the mitigation function and the consequences of its non-delivery.

c) If integrity levels are assigned anywhere in the system or product, then at least the corresponding integrity level requirements shall be imposed on the integration of its elements including those that are not assigned integrity levels.

d) Where no integrity level has been shown for an existing system element and the evidence required by the integrity level requirements of the currently assigned integrity level is not available, alternatives in 10.2 apply.

9.5.3 Behaviours other than failure

As with a system or product consideration shall be given to the possibility that behaviours not classified as failures in the documented specification for an element can nevertheless cause the system or product or any element not to meet its assigned integrity level or result in dangerous conditions or adverse consequences. Alternatively, conditions that are not errors might do so as well).

9.6 Maintaining the assignment of integrity levels

9.6.1 General

The assignment of integrity levels shall be maintained. If a system, product, or element design is modified, change occurs in the system or product environment, or new or modified risk analyses or evaluations are performed, integrity levels can need reassignment. Reassignment may include assigning new, higher integrity levels whenever required.

9.6.2 Changing integrity level assignments

More specifically, the need for an increase in the assigned integrity level to a system, product, or element shall be assessed and the integrity level reassigned if necessary, whenever:

a) Risk analysis or risk evaluation indicates an increase in risk, dangerous conditions, adverse consequences or their number of occurrences or gives any other indication that the integrity level of a system element might require an increase.

b) A design modification to a system element could possibly require an increase in the integrity level assigned to that element, e.g., the removal of redundancy or backup.

c) Possible increases in values of the risk criterion of a system or product are identified.

d) The system or product design does not result in meeting the risk criterion.

e) A design of a system element does not result in meeting its required integrity level.

f) The degree of tolerance for relevant risk criterion values decreases or the required limitations on risk criterion values changes in ways that does not weaken it.

Changing integrity level assignments, especially to a higher level may require additional activities, including analyses, that may not have been conducted for the lower level integrity level.

10 Meeting integrity level requirements

10.1 Requirements related to evidence

10.1.1 Related information

Evidence shall include or be accompanied by information covering:

a) Its definition.

b) Its integrity, validity, accuracy; and achievement of required limitations on uncertainty.

c) Identification of the integrity level requirements that the evidence contributes to meeting and the significance and meaning of the evidence in that context.

d) Relevance of the context under which the evidence was collected or generated.

e) The version, versions, or instances of system, product, or element with which it is associated.

f) People and tools that generated the evidence.

g) Associated assumptions.

h) Conformance with relevant standards unless documented justification is provided for doing otherwise.

i) Source and method of origination.

j) Enabling access to the evidence and accompanying information.

k) The history of the evidence.

NOTE 1 Relevant evidence can include evidence about how an integrity level requirement was met and evidence supporting the information listed above.

NOTE 2 Examples of evidence include a record of past achievements of related systems, a result of the verification process, and a report of organizational maturity assessment of operator or maintainer.

10.1.2 Organization of evidence

The set of evidence, the items it includes, and the accompanying information shall be organized, located, and presented to be understandable to and to satisfy the purposes of those who review, approve, or use them.

10.1.3 Interpretation of evidence

Whenever multiple legitimate interpretations exist of evidence related to meeting integrity level requirements, a conservative interpretation of this achievement shall be used. The most pessimistic interpretation should be considered.

10.2 Alternatives

For all integrity levels assigned to a system, product, or element, the corresponding integrity level requirements should be met if practicable. If the full evidence required by the integrity level requirements cannot be obtained, and the integrity level requirements do not disallow alternatives; then:

a) The system, product, or element shall, nevertheless, be shown to meet the assigned integrity level within required limitations on uncertainty by the use of evidence and related analysis.

b) Any alternative means (an assurance case can play a role) shall be documented, have documented justification including a risk analysis of its use, and be agreed upon and approved in accord with Clause 11.

10.3 Achieving integrity level claim

An integrity level claim shall be determined not achieved if the evidence obtained regarding the integrity level requirements:

a) Shows an integrity level requirement is not met.

b) Is incomplete and any alternatives are not successful. See 10.2.

c) Is inconclusive or fails to meet required limitations on uncertainty.

For all the assigned integrity levels, meeting their full set of integrity level requirements and obtaining evidence (including approved alternatives in accord with 10.2) should be:

d) Explicitly included in plans including needed resources and time.

e) Consistent with all plans.

10.4 Corrective actions

Reported integrity-level-related problems shall:

a) Be recorded and related actions tracked.

b) Have needed corrective actions taken in a timely manner corresponding to their severity and effect on risk-criterion values.

c) Not have corrective actions result in violating integrity-level-related restrictions or requirements including those in this part of ISO/IEC 15026 except temporarily during emergency conditions justified with a documented reason (e.g., risk analysis and evaluation) and agreed upon and approved in accord with Clause 11.

11 Agreements and approvals

11.1 Authorities

The following roles shall be identified and communicated to relevant parties:

a) The approval authorities required for a particular use of this standard:

   1) Approval authority for definition of integrity levels (required for definition of integrity levels).

   2) Approval authority for use of integrity levels (required for use of integrity levels).

NOTE 1 Defined in ISO/IEC 15026-1, an approval authority is the person (or persons) and/or organization (or organizations) responsible for approving the activities, artefacts, and other aspects covered by the corresponding contents of this part of ISO/IEC 15026.

b) The integrity assurance authority (for use of integrity levels).

NOTE 2 Defined in ISO/IEC 15026-1, the integrity assurance authority is the person or organization responsible for certifying compliance with the integrity level requirements. The integrity assurance authority may be the same as the approval authority if requirements regarding it are met, e.g., its independence (see 11.4).

c) The design authority (required for use of integrity levels).

NOTE 3 Defined in ISO/IEC 15026-1, the design authority is the person or organization that is responsible for producing the design of the system.

NOTE 4 Authorities are required for production and maintenance and can be required throughout the life cycle.

11.2 Specific approvals and agreements related to integrity level definition

The approval authority for definition of integrity levels shall approve the results of this defining activity including the claim, integrity level requirement(s) and their related justification, and the documentation and other materials for each integrity level: the grouping of integrity levels into sets of integrity levels including their ordering; and the adequacy of the set of integrity levels for their scope of applicability.

11.3 Specific approvals and agreements related to integrity level use

The design authority and integrity assurance authority shall agree regarding the decisions, aspects, and artefacts as follows:

a) Determination of relevant risk dimensions.

b) The specific integrity levels to be used.

c) The suitability of an integrity level for use in the potential presence of systematic failures and any justifications of this use not being required.

d) The decision process for assigning integrity levels.

e) The adequacy of any fault, error, or failure confinement or isolation.

f) Either:

   1) The degree of benefit to be allowed for specific instance of use or alternately specific instance of combined use of architectural or design features.

   2) The decision method for establishing benefit of an architectural or design feature or combinations thereof.

g) Any categorization of architectural or design features.

h) The methods for showing the achievement of the integrity level claim assigned if the full evidence required by the criteria for this integrity level cannot be obtained and where those methods may be used.

i) Decisions that conforming to another standard will result in meeting a portion or aspect of this part of ISO/IEC 15026.

The integrity assurance authority shall approve the following aspects:

j) The risk criterion and all changes to it.

k) Attention given to the possibility of behaviours or alternatively conditions associated with the system or product other than system element failure or system or product failure causing the system or product to not meet the risk criterion and the plans for and results of this attention.

l) Scope or conditions under which this part of ISO/IEC 15026 applies including any change of scope or conditions under which the integrity levels apply. The design authority should be consulted in this approval process.

m) Decisions that a risk is insignificant or that a risk is not to be analysed or evaluated.

n) Selected approaches to integrity level assignment.

o) The integrity level assigned to the system or product.

p) Decision(s) that the risk criterion is met.

The integrity assurance authority and design authority shall jointly approve the following aspects:

q) The scope of the set of system elements assigned integrity levels.

r) The assignments of integrity levels to system elements.

s) Results of risk analyses and evaluations.

t) Any integrity level that does not cover systematic failures and/or maliciousness.

All authorities providing certification or approval for uses of the system or product as well as the awarders of contracts for a made-to-order system or product during the period of performance of their contract should:

u) Be consulted on agreements between and approvals by the design authority and integrity assurance authority and their acceptance sought.

v) Review and, if possible, approve the planned nature of and requirements for the content of artefacts the authorities require related to integrity level claims and integrity level requirements.

11.4 Documentation

Regarding documentation:

a) The agreement or approval of an aspect shall be accompanied by its documentation.

b) Documentation of agreements, approvals, and decisions made during negotiations leading to them shall be approved by those authorities negotiating, agreeing, and/or approving.

c) Documentation shall describe the integrity assurance authority's relationship to and extent of independence from the producer of the system or product and the claimer of conformance to this part of ISO/IEC 15026 if the claimer is different than the producer.

Annex A
(normative)

Inputs and outputs for integrity level framework

A.1 Table for Clause 4 Integrity level framework

Table A.1 — Inputs and outputs for activities in Figure 1

Activities for integrity level determination	Inputs	Intermediate Steps	Outputs
Determining system integrity level	• list of authorities • list of stakeholders • information about the system and its environment • Stakeholder's requirements • role of integrity levels in the lifecycle of the system	• Risk analysis and evaluation • Assigning system integrity level	• list of risks • risk criteria • adverse consequences, dangerous conditions and initiating events for each risk • required limitations on conditions and consequences occurrences and timings • list of interfaces of the system • required limitations on behaviours of system • integrity level claims • system integrity level
Determining element integrity levels	• information about the system and its environment • system integrity level claim	• System decomposition • Assigning element integrity levels	• list of elements of the system • dependency relation among elements • element integrity levels
Achieving integrity level requirements	• information about the system and its environment • set of integrity level assignments for the integrity levels used • integrity level requirements for each integrity level used		• evidence of achievement of integrity level requirements for all integrity level assignments • specifications for any substitutions of integrity level requirements • documented justifications for any substitution of integrity level requirements • any related analysis