FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/
IEC/IEEE
FDIS
15026-3**

ISO/IEC JTC **1**/SC **7**

Secretariat: **BIS**

Voting begins on:
**2023-08-02**

Voting terminates on:
**2023-09-27**

# 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/IEEE FDIS 15026-3:2023(E)



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

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

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

Published in Switzerland

# Contents

Page

# Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 or www.iec.ch/members_experts/refdocs).

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

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

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

This third edition cancels and replaces the second edition (ISO/IEC 15026-3:2015), which has been technically revised.

The main changes are as follows:

— removal of duplicate terminological entries already included in ISO/IEC/IEEE 15026-1:2019 except for a few essential terms which are included in this edition for ease of reference;

— updates to normative references to the current edition of each reference.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

# Systems and software engineering — Systems and software assurance —

# Part 3: System integrity levels

## 1 Scope

This document specifies the concept of integrity levels with the corresponding integrity level requirements for achieving the integrity levels. Requirements and recommended methods are provided for defining and using integrity levels and their corresponding integrity level requirements. This document covers systems, software products, and their elements, as well as relevant external dependences.

This document 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, 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 document 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 document in Annex A.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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/IEEE 12207, *Systems and software engineering — Software life cycle processes*

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

ISO/IEC/IEEE 15026-1, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

## 3 Terms and definitions

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

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

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

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

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

**3.1**
**integrity level**
degree of confidence that the system-of-interest meets the associated *integrity level claim* (3.4)

Note 1 to entry: A definition of "integrity" consistent with its use in "integrity level" has not been agreed in the relevant communities. Hence, no separate definition of "integrity" is included in this document.

Note 2 to entry: An integrity level is different from the likelihood 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 is a subjective concept.

Note 4 to entry: In this document, 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.

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.3.1, modified — Note 1 to entry has been revised to be more accurate and clearer; the reference to ISO/IEC 25010 has been removed; in note 4 to entry, "economic" has been replaced by "financial".]

**3.2**
**integrity level assurance authority**
independent person or organization responsible for certifying compliance with the *integrity level requirements* (3.5)

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.5.4, modified — The term has been changed from "integrity assurance authority" to "integrity level assurance authority".]

**3.3**
**integrity level definition authority**
person or organization responsible for defining integrity levels and integrity level requirements

**3.4**
**integrity level claim**
proposition representing a requirement on a risk reduction measure identified in the risk treatment process of the system-of-interest.

Note 1 to entry: In general, an integrity level claim is described in terms of requirements that, when met, would avoid, control or mitigate the consequences of dangerous conditions, and provide tolerable risk.

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.

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.3.4, modified — Notes 1 and 2 to entry have been revised to be more accurate and clearer.]

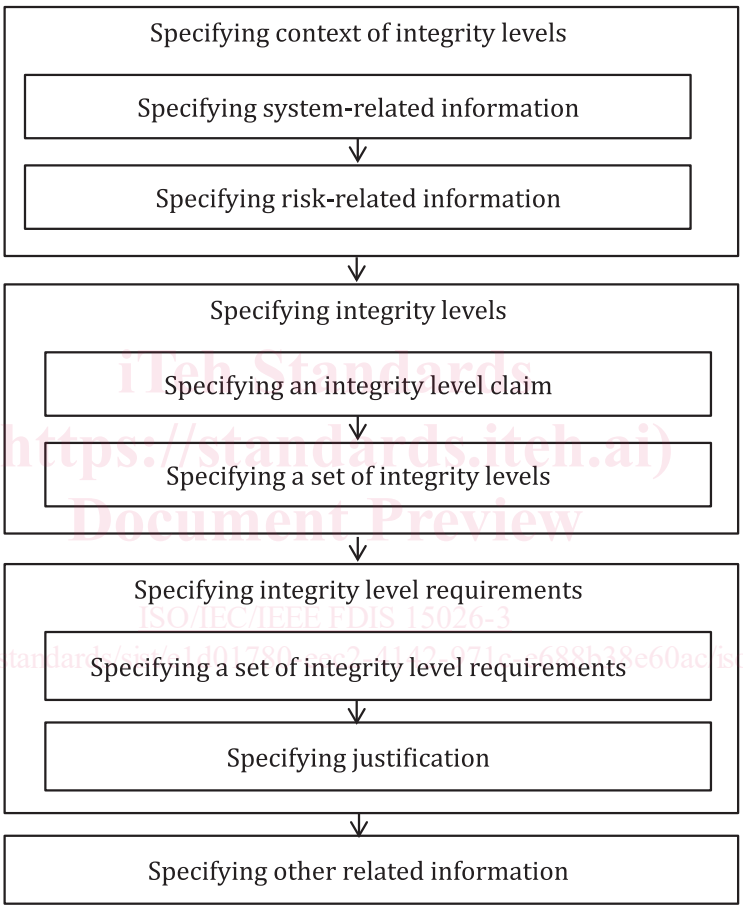
**3.5**
**integrity level requirements**
set of requirements that, when met, will provide a level of confidence in the associated *integrity level claim* (3.4) commensurate with the associated *integrity level* (3.1)

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.3.2, modified — Note 1 to entry has been removed.]

# 4 Defining integrity levels

## 4.1 Users 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 users of this clause are organizations which develop specifications defining a set of integrity levels. The 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 that 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**

↓ represents flow of processes (iteration of processes is not shown for simplicity)

**Figure 1 — Defining integrity levels**

## 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) 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 Assurance cases work together with integrity levels by providing justified arguments for integrity level related definitions and means to demonstrate achievement of integrity levels. Their significance increases in an area where the body of relevant experience is less substantial or less well understood.

## 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 defined:

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 the ISO 26262 series. The definition of target classes of systems of IEC 61508 and the ISO 26262 series pertain to “electrical/electronic/programmable electronic (E/E/PE) systems that 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 3500 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 to clarify the scope of applicability of the integrity levels being defined:

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.

NOTE 1 While in general a risk is a negative or positive effect of uncertainty (ISO Guide 73), this document focuses on risks that are negative effects.

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

— a 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 types of events that lead to the condition. The following event types should be taken into account:

— random failures;

— systematic failures;

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

— failures caused by interactions between elements of the environment and the system (e.g. failures caused by a threat agent).

Likelihood of a dangerous condition should also be considered.

Risk criteria specify the meaning of system-related risks and are used to specify the tolerable risk. Risk criteria are defined to be consistent with applicable contractual, legal and, regulatory constraints, which can be bases for the tolerable risk. Prior to specifying risk criteria, the categories for which risks will be evaluated are defined. These risk categories may include: human health and safety; environmental protection; legal and regulatory compliance; security; cost; project schedule; reputation; and performance. A scale of severity and likelihood is defined for the applicable categories. Stakeholders usually cooperate and agree on risk criteria.

Risk reduction measures include not only parts of a system used to mitigate risks, for example, an inherent safety by design, and safety- or security-related functions, but also organizational supports or social frameworks to treat risks, for example, a contingency plan for operators, warnings in user's manuals, and safety- or security-related standards or regulations for developers. A structure of risk reduction measures should be assumed in order to clarify which parts are the responsibility of the target class of systems. A typical structure is a multi-layered protection structure for safety. Assumptions on the structure of risk reduction measure are characterized by the following criteria:

— a multi-layered structure to mitigate risks, over the environments and the target systems;

— parts of a system, which relates to risk reduction measures, including parts that are undefined or not recognized independently;

— risk reduction measures which contain human elements;

— detectability of loss of the function of risk reduction measure;

— frequency of demand to perform a risk reduction measure.



NOTE 2 IEC 61508 assumes that a safety-related system can be recognized independently.

NOTE 3 The ISO 26262 series assumes that a driver plays a part of the safety-related mechanism and includes aspects such as controllability of an event.

NOTE 4 IEC 61508 gives three sets of integrity levels, each of which corresponds to a demand mode to perform functional safety mechanisms.

## 4.4 Specifying integrity level claim and integrity levels

### 4.4.1 Key concepts

Figure 2 depicts the relationship among key concepts in this document. The goal of the framework of integrity levels is to achieve tolerable risk relative to the system-of-interest and its environment. An integrity level claim is a requirement on a risk reduction measure identified in the risk treatment process of the system-of-interest. The satisfaction of the integrity level claims shall avoid, control or mitigate any dangerous conditions of the system-of-interest. The dangerous conditions in combination with specific states of the environment result in adverse consequences. The risk treatment process shall result in tolerable risk, where risk is characterized by its adverse consequence, which has attributes of severity and likelihood.