

AS/NZS ISO/IEC 15026.3:2022
ISO/IEC 15026-3:2015



Australian/New Zealand Standard™

Systems and software engineering — Systems and software assurance

Part 3: System integrity levels



AS/NZS ISO/IEC 15026.3:2022

This Joint Australian/New Zealand Standard™ was prepared by Joint Technical Committee IT-015, Software and Systems Engineering. It was approved on behalf of the Council of Standards Australia on 11 May 2022 and by the New Zealand Standards Approval Board on 4 May 2022.

This Standard was published on 27 May 2022.

The following are represented on Committee IT-015:

- Australian Computer Society
- Australian Digital Health Agency
- Australian Society for Technical Communication (NSW)
- Department of Defence (Australian Government)
- Engineers Australia
- Griffith University
- Institute of IT Professionals New Zealand
- IT Service Management Forum Australia
- NSW Business Chamber
- Systems Engineering Society of Australia
- Universities New Zealand
- University of New South Wales
- University of Southern Queensland
- University of Technology Sydney

This Standard was issued in draft form for comment as DR AS/NZS ISO/IEC 15026.3:2022.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

www.standards.govt.nz

ISBN 978 1 76113 773 0

Australian/New Zealand Standard™

Systems and software engineering — Systems and software assurance

Part 3: System integrity levels

Originated as AS/NZS 15026:1999.
Revised and redesignated as AS/NZS ISO/IEC 15026.3:2013.
Second edition 2022.

COPYRIGHT

© ISO/IEC 2022 — All rights reserved

© Standards Australia Limited/the Crown in right of New Zealand, administered by the New Zealand Standards Executive 2022

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth) or the Copyright Act 1994 (New Zealand).

Preface

This Standard was prepared by the joint Standards Australia/Standards New Zealand Committee IT-015, Software and Systems Engineering, to supersede AS/NZS ISO/IEC 15026.3:2013.

The objective of this document is to specify the concept of integrity levels with corresponding integrity level requirements that need to be met in order to show the achievement of the integrity level. It places requirements on, and recommends methods for, defining and using integrity levels and their corresponding integrity level requirements. It covers systems, software products, and their elements, as well as relevant external dependences.

This document applies 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; and
- (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 e.g. 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 nor does it 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.

This document is identical with, and has been reproduced from, ISO/IEC 15026-3:2015, *Systems and software engineering — Systems and software assurance — Part 3: System integrity levels*.

As this document has been reproduced from an International document, the following apply:

- (i) In the source text “this part of ISO/IEC 15026” should read “this document”.
- (ii) A full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface	ii
Foreword	iv
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Defining integrity levels	5
4.1 Expected readers of this Clause	5
4.2 Appropriate area to define integrity levels	6
4.3 Specifying context of integrity levels	7
4.3.1 Specifying system-related information	7
4.3.2 Specifying risk-related information	7
4.4 Specifying integrity levels	8
4.4.1 Specifying an integrity level claim	9
4.4.2 Specifying a set of integrity levels	10
4.5 Specifying integrity level requirements	11
4.5.1 Specifying a set of integrity level requirements	11
4.5.2 Specifying the justification between integrity levels and their integrity level requirements	11
4.6 Specifying integrity level determination process	11
5 Using integrity levels	12
5.1 Expected readers of this clause	12
5.2 Purpose for using integrity levels	13
5.3 Outcomes of using integrity levels	13
6 System integrity level determination	13
6.1 General	13
6.2 Purpose of the system integrity level determination process	13
6.3 Outcome of the system integrity level determination process	14
6.4 Activities of the system integrity level determination process	14
7 Assigning system element integrity levels	15
7.1 Purpose of the assigning system element integrity levels process	15
7.2 Outcome of the assigning system element integrity levels process	15
7.3 Activities of the assigning system element integrity levels process	15
8 Meeting integrity level requirements	16
8.1 General	16
8.2 Purpose of meeting integrity level requirements	16
8.3 Outcome of meeting integrity level requirements	16
8.4 Activities of meeting integrity level requirements	17
9 Agreement and approval authorities	18
Annex A (informative) An example of use of ISO/IEC 15026-3	19
Bibliography	23

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

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

This second edition cancels and replaces the first edition (ISO/IEC 15026-3:2011), which has been technically revised.

ISO/IEC 15026 consists of the following parts, under the general title *Systems and software engineering — Systems and software assurance*:

- *Part 1: Concepts and vocabulary*
- *Part 2: Assurance case*
- *Part 3: System integrity levels*
- *Part 4: Assurance in the life cycle*

The IEEE Computer Society collaborated with ISO/IEC JTC 1 in the development of the ISO/IEC 15026 series.

Australian/New Zealand Standard

Systems and software engineering — Systems and software assurance

Part 3: System integrity levels

1 Scope

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

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

- a) definers of integrity levels such as industry and professional organizations, standards organizations, and government agencies;
- b) users of integrity levels such as developers and maintainers, suppliers and acquirers, system or software users, assessors of systems or software and administrative and technical support staff of systems and/or software products.

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

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

2 Normative references

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

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

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

3 Terms and definitions

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

3.1

adverse consequence

consequence ([3.3](#)) that results in a specified level of loss

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

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

3.2 claim

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

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

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

3.3 consequence

outcome of an event affecting objectives

[SOURCE: ISO Guide 73:2009, 3.5.1.3]

3.4 dangerous condition

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

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

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

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

3.5 design authority

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

[SOURCE: ISO/IEC 15026-1]

3.6 initial risk

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

3.7 integrity level

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

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

Note 2 to entry: An integrity level is different from the *likelihood* (3.13) that the integrity level claim is met but they are closely related.

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

Note 4 to entry: In this part of ISO/IEC 15026, integrity levels are defined in terms of risk and hence, cover safety, security, financial and any other dimension of risk that is relevant to the system-of-interest.

3.8**integrity level assurance authority**

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

[SOURCE: ISO/IEC 15026-1]

3.9**integrity level definition authority**

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

3.10**integrity level claim**

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

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

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

3.11**integrity level requirement**

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

3.12**level of risk**

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

[SOURCE: ISO Guide 73:2009, 3.6.1.8]

3.13**likelihood**

probability of something happening

3.14**property-of-interest**

any property that, if lost, is considered a negative effect

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

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

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

3.15**residual risk**

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

[SOURCE: ISO Guide 73:2009, 3.8.1.6]

3.16**risk**

effect of uncertainty on objectives

[SOURCE: ISO Guide 73:2009, 1.1]

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

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

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

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

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

3.17**risk criteria**

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

[SOURCE: ISO Guide 73:2009, 3.3.1.3]

3.18**risk reduction measure**

steps taken to reduce or mitigate *risk* (3.16)

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

3.19**risk source**

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

[SOURCE: ISO Guide 73:2009, 3.5.1.2]

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

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

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

3.20**risk treatment**

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

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

3.21**system**

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

[SOURCE: ISO/IEC/IEEE 15288]