

Australian/New Zealand Standard™

**Systems and software engineering—
Systems and software assurance**

Part 3: System integrity levels



AS/NZS ISO/IEC 15026.3:2013

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 6 May 2013 and on behalf of the Council of Standards New Zealand on 29 April 2013.

This Standard was published on 24 May 2013.

The following are represented on Committee IT-015:

Australian Computer Society
Australian Society for Technical Communication, NSW
Charles Sturt University
Department of Defence, Australia
Griffith University
Quantitative Enterprise Software Performance
La Trobe University
National Association of Testing Authorities Australia
National ICT Australia
New Zealand Organisation for Quality
NSW Business Chamber
Systems Engineering Society of Australia
University of Auckland
University of Technology, Sydney
Vendor Interests, New Zealand

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.saiglobal.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

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

Australian/New Zealand Standard™

**Systems and software engineering—
Systems and software assurance**

Part 3: System integrity levels

Originated as AS/NZS 15026:1999.
Jointly revised and redesignated as AS/NZS ISO/IEC 15026.3:2013.

COPYRIGHT

© Standards Australia Limited/Standards New Zealand

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 (Australia) or the Copyright Act 1994 (New Zealand).

Jointly published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001 and by Standards New Zealand, Private Bag 2439, Wellington 6140.

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-015, Software and Systems Engineering, to supersede AS/NZS 15026:1999, *Information technology—System and software integrity levels*.

The objective of this Standard is to specify the concept of integrity levels with corresponding integrity level requirements that are required to be met in order to show 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 Standard is identical with, and has been reproduced from ISO/IEC 15026-3:2011, *Systems and software engineering—Systems and software assurance—Part 3: System integrity levels*.

As this Standard is reproduced from an International Standard, the following applies:

- (a) In the source text ‘this part of ISO/IEC 15026’ should read ‘this Australian/New Zealand Standard’.
- (b) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

<i>Reference to International Standard</i>	<i>Australian/New Zealand Standard</i>
ISO/IEC TR	SA/SNZ TR
15026 Systems and software engineering— Systems and software assurance	15026 Systems and software engineering— Systems and software assurance
15026-1 Part 1: Concepts and vocabulary	15026.1 Part 1: Concepts and vocabulary

The terms ‘normative’ and ‘informative’ have been used in this Standard to define the application of the annex to which they apply. A ‘normative’ annex is an integral part of a Standard, whereas an ‘informative’ annex is only for information and guidance.

CONTENTS

1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Integrity level framework	2
4.1	Integrity level specification	2
4.2	Process for using integrity levels	3
5	Using this Part 3	4
5.1	Uses of this part of ISO/IEC 15026	4
5.2	Documentation	5
5.3	Personnel and organizations	5
5.4	Overview of this part of ISO/IEC 15026	5
6	Defining integrity levels	6
6.1	Purpose for using this part of ISO/IEC 15026	6
6.2	Outcomes of using this part of ISO/IEC 15026	6
6.3	Prerequisites for defining integrity levels	6
6.3.1	Establish appropriateness of area for use of integrity levels	6
6.3.2	Establish purpose and preliminary scope	7
6.4	Consistency with use requirements	7
6.5	Analysis of scope of applicability	7
6.6	Three required work products	8
6.6.1	Specifying an integrity level claim	8
6.6.2	Specifying integrity level requirements	9
6.6.3	Justification of match between integrity level claim and its requirements	9
6.7	Maintaining integrity level specification	10
6.8	Information provided for users	11
6.8.1	Requirements	11
6.8.2	Guidance and recommendations	11
7	Using integrity levels	11
7.1	Purpose for using this part of ISO/IEC 15026	11
7.2	Outcomes of using this part of ISO/IEC 15026	12
7.3	Prerequisites for use of integrity levels	12
7.3.1	Determine scope of covered risks	12
7.3.2	Establish applicability of integrity levels to the scope of their use	13
7.3.3	Decide role of integrity levels in life cycle	13
7.3.4	Establish approach to risk analysis	13
8	System or product integrity level determination	13
8.1	Introduction	13
8.2	Risk	14
8.2.1	Introduction	14
8.2.2	Risk criterion	14
8.2.3	Risk analyses	15
8.2.4	Risk evaluation	17
8.3	Assignment of system or product integrity level	17
8.4	Independence from internal architecture	18
8.5	Maintaining system or product integrity level	18
8.5.1	Introduction	18
8.5.2	System changes	18

	<i>Page</i>
8.5.3 Risks becomes known	18
8.5.4 Requirements change	18
8.6 Traceability of system or product integrity level assignments	19
9 Assigning system element integrity levels	19
9.1 General.....	19
9.2 Architecture and design.....	19
9.2.1 General.....	19
9.2.2 Failure handling mechanisms	19
9.3 Assignment	20
9.4 Scope of assignments.....	20
9.5 Special considerations.....	20
9.5.1 Cycles and recursion	20
9.5.2 Special situations and requirements regarding integrity levels.....	20
9.5.3 Behaviours other than failure.....	21
9.6 Maintaining the assignment of integrity levels.....	21
9.6.1 General.....	21
9.6.2 Changing integrity level assignments.....	21
10 Meeting integrity level requirements	22
10.1 Requirements related to evidence	22
10.1.1 Related information	22
10.1.2 Organization of evidence	22
10.1.3 Interpretation of evidence	22
10.2 Alternatives	22
10.3 Achieving integrity level claim	23
10.4 Corrective actions.....	23
11 Agreements and approvals.....	23
11.1 Authorities.....	23
11.2 Specific approvals and agreements related to integrity level definition	24
11.3 Specific approvals and agreements related to integrity level use	24
11.4 Documentation.....	25
Annex A (normative) Inputs and outputs for integrity level framework	26
A.1 Table for Clause 4 Integrity level framework	26
Annex B (informative) An example of use of ISO/IEC 15026-3	27
B.1 Introduction.....	27
B.2 Overview	27
B.3 Defining integrity levels (Clause 6).....	27
B.4 Using a framework of integrity levels (Clauses 7 and 8)	29
B.5 System element integrity levels (Clause 9).....	31
B.6 Using integrity levels according to this part of ISO/IEC 15026.....	31
Bibliography	32
Tables	
Table A.1 — Inputs and outputs for activities in Figure 1	26
Table B.1 — Integrity levels for examples	28
Table B.2 — Integrity level claims' ranges of property values for examples	28
Table B.3 — Examples of integrity level requirements and associated evidence.....	29

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 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*