
**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

Withhold

Withdrawn



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Foreword	v
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

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

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/IEC 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*