

IEEE Standard Adoption of ISO/IEC 15026-3—Systems and Software Engineering—Systems and Software Assurance—Part 3: System Integrity Levels

IEEE Computer Society

Sponsored by the
Software & Systems Engineering Standards Committee

Currently in preview, click buy full version

IEEE Standard Adoption of ISO/IEC 15026-3—Systems and Software Engineering—Systems and Software Assurance—Part 3: System Integrity Levels

Sponsor

Software & Systems Engineering Standards Committee
of the
IEEE Computer Society

Approved 14 June 2013

IEEE-SA Standards Board

Abstract: 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 are specified in this adoption of ISO/IEC 15026-3:2011. It places requirements on and recommends methods for defining and using integrity levels and their integrity level requirements, including the assignment of integrity levels to systems, software products, their elements, and relevant external dependences.

This standard is applicable to systems and software and is intended for use by the following:

- Definers of integrity levels such as industry and professional organizations, standards organizations, and government agencies;
- 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 standard 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.

This standard 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. ISO/IEC TR 15026-1 provides additional information and references to aid users of IEEE Std 15026-3.

Keywords: adoption, argument, assurance case, claim, dependability, evidence, IEEE 15026-3, integrity level, property, reliability, safety, security software assurance, software engineering, system assurance, systems engineering

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

Copyright © 2013 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 12 July 2013. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-8436-4 STD98243
Print: ISBN 978-0-7381-8437-1 STDPD98243

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Notice and Disclaimer of Liability Concerning the Use of IEEE Documents: IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. 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 IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon any IEEE Standard document.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied "AS IS."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE standard is subjected to review at least every ten years. If a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Translations: The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official Statements: A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. Announcements, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on Standards: Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions or changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important to ensure that any response to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE working group at <http://standards.ieee.org/develop/wg/>.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Photocopies: Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Notice to users

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at <http://standards.ieee.org/index.html> or contact the IEEE at the address listed previously. For more information about the IEEE Standards Association or the IEEE standards development process, visit IEEE-SA Website at <http://standards.ieee.org/index.html>.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at <http://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE standard was completed, the Life Cycle Processes Working Group had the following membership:

James W. Moore, *IEEE Computer Society Liaison to ISO/IEC JTC 1/SC 7*

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Ed Addario	Werner Hoelzl	Robert Robinson
Edward Addy	Glenn Hoffman	Helmut Sandmayr
T. Scott Ankrum	Robert Holibaugh	Bartien Sayogo
Chris Bagge	Bernard Homes	Robert Schaaf
Charles Barest	Peter Hung	Hans Schaefer
Juris Borzovs	Atsushi Ito	Maud Schlich
Pieter Botman	Mark Jaeger	David Schultz
Lyle Bullock	Cheryl Jones	Stephen Schwarm
Juan Carreon	Piotr Karocki	Gil Shultz
Sue Carroll	Dwayne Knick	Carl Singer
Lawrence Catchpole	Ronald Knudsen	James Sivak
Keith Chow	Thomas Kurihara	Michael Smith
Geoffrey Darnton	George Kyle	Kapil Sood
Thomas Dineen	Sumit Lind	Friedrich Stallinger
Teresa Doran	J. Dennis Lawrence	Thomas Starai
Antonio Doria	David Leciston	Walter Struppler
Harriet Feldman	Greg Luri	Gerald Stueve
Andrew Fieldsend	Wayne Manges	Marcy Stutzman
Eva Freund	William McBride	Thomas Tullia
David Friscia	Edward McCall	Vincent Tume
David Fuschi	James W. Moore	John Vergis
Gregg Giesler	Michael S. Newman	David Walden
Ron Greenthaler	Chris Osterloh	Stephen Webb
Randall Groves	William Petit	M. Karen Woolf
John Harau	Ulrich Pohl	Jian Yu
David Herrell	Iulian Profir	Oren Yuen
Richard Hilliard	Annette Reilly	Janusz Zalewski

When the IEEE-SA Standards Board approved this standard on 14 June 2013, it had the following membership:

John Kulick, *Chair*
David J. Law, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi
Peter Balma
Farooq Bari
Ted Burse
Wael William Diab
Stephen Dukes
Jean-Philippe Faure
Alexander Gelman

Mark Halpin
Gary Hoffman
Paul Houzé
Jim Hughes
Michael Janezic
Joseph L. Koepfinger*
Oleg Logvinov

Ron Petersen
Gary Robinson
Jon Walter Rosdahl
Adrian Stephens
Peter Sutherland
Yatin Trivedi
Phil Winston
Yu Yuan

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Catherine Berger
IEEE Standards Senior Program Manager, Document Development

Malia Zanin
IEEE Standards Program Manager, Technical Program Development

Introduction

This introduction is not part of IEEE Std 15026-3-2013, IEEE Standard Adoption of ISO/IEC 15026-3—Systems and Software Engineering—Systems and Software Assurance—Part 3: System Integrity Levels.

The IEEE Software and Systems Engineering Standards Committee (S2ESC) has undertaken a long-term program to harmonize its standards with those of ISO/IEC JTC 1/SC 7, the international standards committee for software and systems engineering. In areas of overlap, one organization sometimes adopts the relevant standard from the other organization, or the two organizations cooperate to produce a single joint standard. In this case, S2ESC has chosen to adopt a relevant document from SC 7.

This IEEE standard is an adoption of ISO/IEC 15026-3:2011. References to some ISO/IEC standards should be considered as references to the identical IEEE standard:

- ISO/IEC/IEEE 12207:2008 is identical to ISO/IEC 12207:2008
- ISO/IEC/IEEE 15288:2008 is identical to ISO/IEC 15288:2008
- ISO/IEC/IEEE 15289:2011 is identical to ISO/IEC 15288:2011
- ISO/IEC/IEEE 16085:2006 is identical to ISO/IEC 16085:2006
- IEEE Std 15026-1™-2011 is identical to ISO/IEC TR 15026-1:2010
- IEEE Std 15026-2™-2011 is identical to ISO/IEC 15026-2:2011
- ISO/IEC/IEEE 42010:2011 is identical to ISO/IEC 42010:2011

It should also be noted that IEEE is currently planning to ballot a portion of the other part of the 15026 series, namely, ISO/IEC 15026-4.

Errata

The following editorial corrections are made in the adopted document:

Page 5, Subclause 5.4, first line: Change “5.4” to “Clause 6”.

Page 6, Subclause 6.1, fourth line: Change “acheivement” to “achievement”.

Contents of IEEE Std 15026-3-2013

ISO/IEC 15026-3:2011..... 1

Currently in preview, click buy full version

IEEE Standard Adoption of ISO/IEC 15026-3—Systems and Software Engineering—Systems and Software Assurance—Part 3: System Integrity Levels

IMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

**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



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*