IEEE STANDARDS ASSOCIATION

IEEE Standard—
Adoption of ISO/IEC 15026-2:2011

Systems and Software Engineering—
Systems and Software Assurance—
Part 2: Assurance Case

IEEE Computer Society

Sponsored by the
Software & Systems Engineering Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

11 October 2011

IEEE Std 15026-2™-2011

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

IEEE Standard—
Adoption of ISO/IEC 15026-2:2011

Systems and Software Engineering—
Systems and Software Assurance—
Part 2: Assurance Case

Sponsor

Software & Systems Engineering Standards Committee
of the
IEEE Computer Society

Approved 10 September 2011

IEEE-SA Standards Board

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

Abstract: ISO/IEC 15026-2:2011 is adopted by this standard. ISO/IEC 15026-2:2011 specifies minimum requirements for the structure and contents of an assurance case to improve the consistency and comparability of assurance cases and to facilitate stakeholder communications, engineering decisions, and other uses of assurance cases.

An assurance case includes a top-level claim for a property of a system or product (or set of claims), systematic argumentation regarding this claim, and the evidence and explicit assumptions that underlie this argumentation. Arguing through multiple levels of subordinate claims, this structured argumentation connects the top-level claim to the evidence and assumptions.

Assurance cases are generally developed to support claims in areas such as safety, reliability, maintainability, human factors, operability, and security, although these assurance cases are often called by more specific names, e.g. safety case or reliability and maintainability (R&M) case.

ISO/IEC 15026-2:2011 does not place requirements on the quality of the contents of an assurance case and does not require the use of a particular terminology or graphical representation. Likewise, it places no requirements on the means of physical implementation of the data, including no requirements for redundancy or co-location.

Keywords: adoption, argument, assurance case, claim, dependability, evidence, IEEE 15026-2, 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 © 2011 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 11 October 2011. 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 978-0-7381-6799-2 STD97161
Print: ISBN 978-0-7381-6800-5 STDPD97161

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.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

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 or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The 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 this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, 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 herein 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 five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, 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 this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her 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.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received 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 interpretation requests except in those cases where the matter has previously received formal consideration. 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 interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

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

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.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

Introduction

This introduction is not part of IEEE Std 15026-2-2011, IEEE Standard—Adoption of ISO/IEC 15026-2:2011, Systems and Software Engineering—Systems and Software Assurance—Part 2: Assurance Case.

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 15026-2:2011. 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 16085:2006 is identical to ISO/IEC 16085:2006

— IEEE Std 15026-1™-2011 is identical to ISO/IEC TR 15026-1:2010

It should be noted that IEEE is currently processing a standard that will be identical to the following ISO/IEC standard:

— ISO/IEC/IEEE 15289 will be identical to ISO/IEC 15289 when the former is approved.

It should also be noted that IEEE is currently planning adoptions of the other parts of the 15026 series, namely, ISO/IEC 15026-3 and ISO/IEC 15026-4, after they are published as ISO/IEC standards.

It should further be noted that IEEE is currently planning to adopt ISO/IEC 25010:2011.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard 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.

Copyright © 2011 IEEE. All rights reserved.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

Updating of IEEE documents

Users of IEEE standards 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 Standards Association web site at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA web site at http://standards.ieee.org.

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.

Interpretations

Current interpretations for this and all other standards can be accessed at the following URL: http://standards.ieee.org/findstds/interps/index.html.

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 with respect to the existence or validity of any patent rights in connection therewith. 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.

Copyright © 2011 IEEE. All rights reserved.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, 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
Edward Addy
Johann Amsenga
H. Stephen Berger
Juris Borzovs
Pieter Botman
Lyle Bullock
Juan Carreon
Sue Carroll
Keith Chow
Paul Croll
Geoffrey Darnton
David Deighton
Sourav Dutta
Andrew Fieldsend
David Friscia
David Fuschi
Ignacio Marin Garcia
Lewis Gray
Ron Greenthaler
Randall Groves
Jon Hagar
John Harauz
Mark Henley
Richard Hilliard

Werner Hoelzl
Glenn Hoffman
Robert Holibaugh
Bernard Homes
Peter Hung
Atsushi Ito
Cheryl Jones
Piotr Karocki
Dwayne Knirk
Thomas Kurihara
Susan Land
J. Dennis Lawrence
David Leciston
Daniel Lindberg
Greg Luri
Faramarz Maghsoodlou
Wayne W. Manges
L. Tajerian Martinez
Edward McCall
Kathryn Moland
James Moore
Michael S. Newman
Mirko Palazzo
William Petit
Ulrich Pohl
Iulian Profir

Gerald Radack
Annette Reilly
Robert Robinson
Randall Safier
Bartien Sayogo
Robert Schaaf
Maud Schlich
Richard Schrenker
Stephen Schwarm
Gil Shultz
Carl Singer
James Sivak
Luca Spotorno
Friedrich Stallinger
Thomas Starai
Elena Strange
Walter Struppler
Marcy Stutzman
Anusheel Tandon
Theodore Urbanowicz
David Walden
Paul Work
Oren Yuen
Janusz Zalewski
Wenhao Zhu

Copyright © 2011 IEEE. All rights reserved.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

When the IEEE-SA Standards Board approved this standard on 10 September 2011, it had the following membership:

Richard H. Hulett, *Chair*
John Kulick, *Vice Chair*
Robert Grow, *Past Chair*
Judith Gorman, *Secretary*

Masayuki Ariyoshi
William Bartley
Ted Burse
Clint Chaplin
Wael Diab
Jean-Philippe Faure
Alex Gelman
Paul Houzé
Jim Hughes
Joseph L. Koepfinger*
David Law
Thomas Lee
Hung Ling
Oleg Logvinov
Ted Olsen
Gary Robinson
Jon Rosdahl
Sam Sciacca
Mike Seavey
Curtis Siller
Phil Winston
Howard Wolfman
Don Wright

*Member Emeritus

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

Satish Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Catherine Berger
IEEE Standards Project Editor

Malia Zaman
IEEE Standards Program Manager, Technical Program Development

Copyright © 2011 IEEE. All rights reserved.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

IEEE Standard—
Adoption of ISO/IEC 15026-2:2011

Systems and Software Engineering— Systems and Software Assurance— Part 2: Assurance Case

IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

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.

Copyright © 2011 IEEE. All rights reserved.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

INTERNATIONAL STANDARD

ISO/IEC 15026-2

First edition
2011-02-15

Systems and software engineering — Systems and software assurance —

Part 2: **Assurance case**

Ingénierie du logiciel et des systèmes — Assurance du logiciel et des systèmes —

Partie 2: Cas d'assurance

Reference number
ISO/IEC 15026-2:2011(E)

© ISO/IEC 2011

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

Contents

Page

© ISO/IEC 2011 – All rights reserved

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

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 15026-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

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*

System integrity levels and assurance in the life cycle will form the subjects of future parts.

© ISO/IEC 2011 – All rights reserved

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

Introduction

The purpose of this part of ISO/IEC 15026 is to ensure the existence of types of assurance case content and restrictions on assurance case structure, thereby improving consistency and comparability among instances of assurance cases and facilitating stakeholder communications, engineering decisions, and other uses of assurance cases.

Existing standards addressing different application areas and topics related to assurance cases might use differing terminology and concepts when addressing common themes. This part of ISO/IEC 15026 is based on experience drawn from these many specialized standards and guidelines. It is applicable to any property of a system or product.

NOTE It is intended that ISO/IEC TR 15026-1 will be transformed into an International Standard.

In addition to concepts and terminology, ISO/IEC TR 15026-1 provides background and a list of related standards that could be useful in understanding and using this part of ISO/IEC 15026. Assurance cases are generally developed to support claims in areas such as safety, reliability, maintainability, human factors, operability, and security, although these assurance cases are often called by more specific names, e.g. safety case or reliability and maintainability (R&M) case.

This part of ISO/IEC 15026 uses the terminology and concepts consistent with ISO/IEC 12207:2008, ISO/IEC 15288:2008, and ISO/IEC 15289:2006. This part of ISO/IEC 15026 does not presume or require that it is applied in conjunction with ISO/IEC 12207:2008 or ISO/IEC 15288:2008.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

Systems and software engineering — Systems and software assurance —

Part 2: **Assurance case**

1 Scope

This part of ISO/IEC 15026 specifies minimum requirements for the structure and contents of an assurance case. An assurance case includes a top-level claim for a property of a system or product (or set of claims), systematic argumentation regarding this claim, and the evidence and explicit assumptions that underlie this argumentation. Arguing through multiple levels of subordinate claims, this structured argumentation connects the top-level claim to the evidence and assumptions.

This part of ISO/IEC 15026 does not place requirements on the quality of the contents of an assurance case. Rather, it places requirements on the existence of the contents and structure of an assurance case. While several notations and slightly varying terminologies are currently used in practice, this part of ISO/IEC 15026 does not require the use of a particular terminology or graphical representation. Likewise, it places no requirements on the means of physical implementation of the data, including no requirements for redundancy or co-location.

2 Conformance

An assurance case conforms to this part of ISO/IEC 15026 if it meets the requirements of Clause 6 and Clause 7.

3 Normative references

The following referenced documents are indispensable for the application of this document.

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

ISO/IEC 15289, *Systems and software engineering — Content of systems and software life cycle process information products (Documentation)*

4 Terms and definitions

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

5 Use of this part of ISO/IEC 15026

System- or product-related needs and requirements, interactions of the system or product with its environment, and real-world events and conditions can result in an objective to obtain assurance that the system or product achieves certain claims. To meet this objective, assurance cases support these claims concerning selected

© ISO/IEC 2011 – All rights reserved

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

properties of the system or product. While these properties may be selected for any reason, one commonly selects them because they are risk-related and high confidence is needed in their realization in a system or product. The results of developing an assurance case are the values and their uncertainties established for each top-level claim's property. The uncertainties regarding the truth or falsehood of these claims are an essential conclusion of the assurance case.

Stakeholders can evaluate the assurance case to determine the extent of achievement of the top-level claim by the system or product and whether this achievement is shown within the allowable uncertainty or risk and any related consequences. The results regarding the top-level claim and its support along with related uncertainties and consequences constitute a basis for rationally managing risk, achieving grounds for appropriate confidence, and aiding in decision making.

Generally, stakeholders can make better decisions about a system or product when the uncertainties of conclusions regarding these properties are reduced. While an assurance case is useful for decision-making by knowledgeable stakeholders (e.g., developers and service providers), often the primary motivation for an assurance case is to support crucial decisions by stakeholders without this background, such as those involved in certification, regulation, acquisition, or audit of the system.

How the assurance case is used and the amount of effort devoted to its formulation can vary greatly due to the stringency of the properties selected, the applicable duration of the claim, the degree of uncertainty, the scope of the assumptions made, and the risk or consequences involved. Thus, the content needed in an assurance case varies depending on the stakeholder and evaluation context. For example, depending on the system requirements and the property specified by the top-level claim, an assurance case could be used for validation or verification purposes.

This part of ISO/IEC 15026 is intended to be utilized while developing and maintaining assurance cases. When developing a new system or product or making a major change, the development of the assurance case should be integral within processes, plans, engineering, activities, and decisions related to the development of the system or product of interest.

In order to provide the needed flexibility and cover the many areas where assurance cases are utilized, this part of this International Standard uses a general approach and calls for a mapping between it and the contents of any conforming assurance case. The requirements for this mapping are in 7.2.

NOTE 1 The term “uncertainty” is used as a general term to mean "lack of certainty." Different communities restrict the application of this term to limited usage, e.g., to predictions of future events, to physical measurements already made, or to unknowns, but in this International Standard the term applies to any uncertainty.

NOTE 2 Selecting the top-level claim and the properties it involves is not restricted by this part of ISO/IEC 15026 but may be specified in stakeholder requirements or established by an approval authority for the system or product. Top-level claims might be a portion of the total requirements and specification but might be something internal to the system, related to something the system depends upon, or only indirectly related to the primary system of interest.

NOTE 3 Limitations of a system’s or product’s assurance case should be reflected in the guidance; transition, operations, and maintenance documentation; training; operator and user aids; data collection capabilities; and services included in or accompanying the system or product. Knowledge of these limitations allows avoidance and recognition of violations of relevant assumptions or the conditions related to the top-level claims.

NOTE 4 The text often refers to a single assurance case or to a single top-level claim; however, a system or product may have multiple assurance cases, and an assurance case may have multiple top-level claims.

6 Structure and contents of an assurance case

6.1 General

This part of ISO/IEC 15026’s description of assurance case structure and contents uses the term “components” for the main parts of an assurance case and describes the relationships among these components. The following general requirements apply:

a) The components of an assurance case shall be unambiguous, identifiable, and accessible.

© ISO/IEC 2011 – All rights reserved

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

NOTE Ambiguity may be avoided by associating a component with information on its context, such as: definitions of the terms used, the environment of the system or product, and the identities of entities responsible for a component’s development or maintenance.

b) Each component shall be uniquely identified and shall be able to have its origin identified, its history ascertained, and its integrity assured.

c) For each component, the component's contents, the information related to it, and the other components with which it has relationships shall be identifiable and accessible."

NOTE For each component, its description and needed other components, e.g., evidence for claims and related information such as test case results, are identifiable and accessible.

d) An assurance case shall contain the auxiliary contents required by ISO/IEC 15289 for this type of documentation.

NOTE This part of ISO/IEC 15026 places no restrictions on how these auxiliary contents are included and no requirement that the assurance case be a separate document.

6.2 Overall structure

The five principal components of an assurance case are claims, arguments, evidence, justifications, and assumptions.

Figure 1 describes the structure of assurance cases. It is not normative.

Claims

A claim is a proposition to be assured about the system of concern. It may be accompanied with auxiliary information such as the range of some date mentioned in the proposition or the uncertainty of the proposition.

Justifications, Arguments, Evidence and Assurance Cases

Justifications, arguments, evidence and assurance cases are defined mutually recursively in this figure.

Given a claim c, a justification j of c is a reason why c has been chosen.

Comment: Therefore, a justification is defined relative to a claim c. An argument (defined below) is also defined relative to a claim, but it is different from justification because a justification is a reason for the choice of a claim, while an argument is a reason why a claim is true.

Given a claim c and a set es of evidence, an argument that assures c using es is defined to be a reason why the truth of c is deduced from the main part of evidence in the set es.

Evidence is either a fact, a datum, an object, a claim or an assurance case. A claim is called an assumption if it appears in an assurance case as evidence. The main part of the evidence is defined according to the form of the evidence; if the evidence is either a fact, datum, object or a claim, its main part is itself; but if the evidence is an assurance case a_0, its main part is the claim of a_0.

Comment: It will be clarified below in this figure that the evidence of an assurance case is used by an argument of that assurance case to assure that its claim holds.

Comment: A claim appearing as evidence is called an assumption because such evidence is a proposition without any reason why it is true. When a reason for its truth is provided, it is expected that an assurance case, whose argument is that reason, is constructed and provided as the evidence instead of providing only the claim as evidence.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

An assurance case is defined to be a quadruple of a claim c, a justification j of c, a set es of evidence and an argument g which assures c using es. Let a = (c, j, es, g) be an assurance case; c is defined to be the claim of a; similarly, j is defined to be the justification of a, es to be the set of evidence of a, and g to be the argument of a.

Comment: The definition of assurance cases depends on that of arguments, the definition of arguments depends on that of evidence, and the definition of evidence depends on that of assurance cases. These definitions, however, are not circular, but mutually recursive with each other.

Comment: For mathematically oriented readers, the following recursive definition of the set of assurance cases might help. The set A of assurance cases and the set E of evidence are defined by the following recursive equations.

$$A_0 = C \times \{ j_0 \in J(c_0) \mid c_0 \in C \} \times \wp_f(E) \times \{ g_0 \in G(c_0, es_0) \mid c_0 \in C, es_0 \in \wp_f(E) \}$$

$$A = \{ (c, j, es, g) \in A_0 \mid j \in J(c), g \in G(c, es) \}$$

$$E = F + D + O + C + A$$

where

$J(c)$ is the set of all justifications for a claim c;
C is the set of claims;
$\wp_f(E)$ is the set of all finite subsets of E (finite powerset of E);
$G(c_0, es_0)$ is the set of arguments which assures a claim c_0 using a set es_0 of evidence;
F is the set of facts, D is the set of data;
O is the set of objects;
$M \times N$ is the direct product of M and N, for any sets M and N; and
$M + N$ is the discriminated union (direct sum) of M and N for any sets M and N.

Figure 1 — Structure of assurance cases (informative)

The following requirements apply to the structure of an assurance case:

a) An assurance case shall have one or more top-level claims that are the ultimate goals of its argumentation.

NOTE Multiple top-level claims are equivalent to their conjunction.

b) An argument shall be supported by one or more claims, evidence, or assumptions.

NOTE 1 An argument is used to show how the components directly underlying it relate to a claim or set of claims. The set of underlying components for an argument comprises a collection of evidence, assumptions, or lower-level claims.

NOTE 2 Since one argument cannot directly support another argument; a lower-level argument should attach to a lower-level claim that in turn attaches to the higher-level argument.

c) A claim shall be supported either by just one argument, or by one or more claims, evidence, or assumptions.

NOTE Every claim in an assurance case requires support, which can take different forms. Therefore, a claim is never a bottom component of an assurance case. One (and only one) argument can be used to support a claim. Alternatively, a claim can be supported (directly, and not via an argument) by some collection of evidence, assumptions, or lower-level claims.

d) A claim, argument, evidence, or assumption shall not support itself either directly or indirectly.

NOTE A single claim, argument, evidence, or assumption may be used to support multiple components.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

6.3 Claims

6.3.1 Form of claim

A claim shall be a true-false statement that states the limitations on the values of an unambiguously defined property—called the claim's property, limitations on the uncertainty of the property's value meeting the limitations on it, and limitations on conditions under which the claim is applicable.

6.3.2 Claim contents

As indicated in the following list, a claim shall have the required contents and may have the optional contents:

a) Claim's property (required).

b) Limitations on the value of the property associated with the claim (e.g., on its range) (required).

c) Limitations on the uncertainty of the property value meeting its limitations (required).

d) Limitations on duration of claim's applicability (optional).

e) Duration-related uncertainty (optional).

f) Limitations on conditions under which the claim is applicable (required).

g) Condition-related uncertainty (optional).

h) If a property in a claim applies to some subset of systems, products, or their elements, their identification including relevant versions or instances (conditionally required).

i) Consequences or risks if they are relevant to claim (conditionally required).

NOTE 1 The term "limitations" is used to fit the many situations that can exist. Values can be a single value or multiple single values, a range of values or multiple ranges of values, or multi-dimensional. The boundaries of these limitations sometimes involve probability distributions, are incremental, or have other fuzzy aspects.

NOTE 2 Uncertainties also may be associated with the duration of applicability and the stated conditions. Particular claims need not include all possible uncertainties and commonly include only one. Where accurate, uncertainties may be zero.

6.3.3 Coverage of conditions

The conditions, including any specified durations, covered by the combination of assurance case components supporting a claim shall together cover the conditions, including any specified duration, for which the claim is applicable.

6.3.4 Justification of the choice of top-level claims

Because the choice of a top-level claim and its property is critical in order to meet the objective of an assurance case and drives the assurance case's formulation, a top-level claim shall have a justification for its choice.

NOTE Justification for the top-level claim serves as a means for communicating risk among stakeholders of the system and for recording agreement.

© ISO/IEC 2011 – All rights reserved

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

6.4 Arguments

6.4.1 Argument characteristics

An argument is used to show how the components directly underlying it relate to a claim or set of claims. An argument can be particularly useful if it is in the form of an engineering calculation or logic proof and not in the form of an assurance case.

An argument has the following characteristics:

a) The argument shall be stated in a manner that uses the components directly below it.

b) The argument shall reach a conclusion or conclusions that relate to each claim it supports.

c) The argument shall establish the uncertainties of each conclusion it reaches.

d) The argument shall contain the information needed to establish its effect on uncertainty.

6.4.2 Justification of argument's method of reasoning

An argument shall have an associated justification for the validity or merit of its method of reasoning (e.g., calculating or arguing).

NOTE A variety of methods of reasoning can be used within arguments. These methods, including the tools they use, vary in their applicability, power, resulting accuracy and uncertainty, and ease of use. Arguments are used to support or detract from claims. The claims, evidence, and assumptions underlying an argument have uncertainties associated with them, and the argument might affect the uncertainty of the claim using it.

6.5 Evidence

6.5.1 Evidence contents

Evidence shall contain tangible data or information.

NOTE Many kinds of evidence exist. Among these are human experience reports, history, observations, measurements, tests, evaluative and compliance results, correctness of design rationale, analyses, comparison of artefacts, reviews, and defects and other quality assurance and field data. Evidence can already exist, be newly created or collected, or be planned for the future. The evidence should support or detract from the claims in the assurance case. The body of evidence can become quite large and should be organized, located, and presented to be understandable to those who review, approve, or directly use it.

6.5.2 Associated information

Evidence shall contain or have associated with it information regarding its:

a) Definition.

b) Scope of applicability.

c) Uncertainty, including the reliability of its source (e.g., authenticity, trustworthiness, and competence) and the measurement accuracy.

NOTE This information may take any form including one or more assurance cases or portions thereof.

6.5.3 Associated assumptions

Any assumptions related to evidence shall be included in the assurance case.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

6.6 Assumptions

6.6.1 Form of Assumption

An assumption shall take the form of a claim and a reason for it.

6.6.2 Assumption contents

An assumption can have one of three kinds of origins. Two kinds are inherently true given their context and role within the assurance case. These are (1) an assumption implied by the specified conditions restricting the applicability of the claim(s) it supports and (2) an assumption inherent in a method of argumentation, e.g., as a statement of an alternative that is one of a set of alternative assumptions that together cover all the relevant possibilities, such as stating each case in a proof by cases. These two kinds of assumptions have zero uncertainty.

The third kind of an assumption is not inherently true; rather it is a claim not fully warranted by evidence. This third kind of assumption shall:

a) Contain a claim and a reason for it.

b) Contain an indication, identification, or description of the basis of the estimate of the uncertainty regarding the truth of the assumption.

NOTE For best results, such assumptions should have one or more of the following characteristics: have low uncertainty or low risk because they are of low criticality in argumentation, have a weak impact on the argumentation, have a weak effect on critical values or consequences, or are few in number.

6.6.3 Associated evidence

If an assumption is partially warranted or contradicted by evidence, this evidence shall be associated with it.

6.7 Justifications

A top-level claim has a justification for its choice (6.3.4) and an argument has a justification for its method of argumentation (6.4.2).

6.8 Combining assurance cases

If an assurance case incorporates another assurance case, the incorporated assurance case's top-level claim or claims shall each be placed within the original assurance case’s structure at points where claims are allowed.

NOTE A portion of an assurance case may also be a part of other assurance cases.

7 Required outcomes of using Part 2 assurance case

7.1 Outcomes

Application of this part of ISO/IEC 15026 has the following outcomes:

a) An assurance case meeting the requirements of Clause 6 shall be provided as an element of the system.

NOTE As an element of the system, the assurance case is generally expected to be delivered with the system and maintained as the system is maintained.

b) A logical mapping meeting the requirements of 7.2 shall be provided as a part of the assurance case.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

c) Records documenting the fulfilment of the requirements of this part of ISO/IEC 15026 shall be identified and referenced by the assurance case.

d) Identification of the entity or entities asserting conformance shall be provided in the assurance case.

7.2 Mapping to this part of ISO/IEC 15026

An assurance case shall:

a) Include an unambiguous mapping to the components and relationships in Clause 6.

b) Cover all the contents specified in Clause 6 unless documented justification is provided for doing otherwise.

NOTE 1 Because this mapping has to map from assurance cases that are developed within several specialities and utilize many notations, the mapping may take any unambiguous form.

NOTE 2 The mapping may assign a meaning and mapping to a component that is missing if that mapping is unambiguous. For example, if a particular kind of uncertainty is not explicitly specified, then the mapping might state that this is equivalent to it being specified and equalling zero.

© ISO/IEC 2011 – All rights reserved

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

Bibliography

[1] Greenwell, William S., John C. Knight, and Jacob J. Pease, "A Taxonomy of Fallacies in System Safety Arguments” 24th International System Safety Conference, Albuquerque, NM, August 2006

[2] IEC 60300 (all parts), *Dependability management*

[3] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[4] IEC 61511 (all parts), *Functional safety — Safety instrumented systems for the process industry sector*

[5] IEC 61882:2001, *Hazard and operability studies (HAZOP studies) — Application guide*

[6] IEEE Std 1228-1994, *IEEE Standard for Software Safety Plans*

[7] ISO/IEC 12207:2008, *Systems and software engineering — Software life cycle processes*

[8] ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*

[9] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

[10] ISO/IEC 15504 (all parts), *Information technology — Process assessment*

[11] ISO/IEC TR 15443 (all parts), *Information technology — Security techniques — A framework for IT security assurance*

[12] ISO/IEC 16085:2006, *Systems and software engineering — Life cycle processes — Risk management*

[13] ISO/TR 18529:2000, *Ergonomics — Ergonomics of human-system interaction — Human-centred lifecycle process descriptions*

[14] ISO/IEC 19770 (all parts), *Information technology — Software asset management*

[15] ISO/IEC 21827:2008, *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)*

[16] ISO/IEC 25010, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality models*[1)]

[17] ISO/IEC 25012:2008, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model*

[18] ISO/IEC 25020:2007, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Measurement reference model and guide*

[19] ISO/IEC 25030:2007, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Quality requirements*

[20] ISO/IEC 25040, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation process*

1) To be published.

© ISO/IEC 2011 – All rights reserved

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

[21] ISO/IEC 25051:2006, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing*

[22] ISO/IEC 26702:2007, *Systems engineering — Application and management of the systems engineering process*

[23] ISO/IEC 27005:2008, *Information technology — Security techniques — Information security risk management*

[24] ISO/IEC Directives, Part 2: *Rules for the structure and drafting of International Standards*, Fifth edition, 2004

[25] KELLY, T. "Arguing Safety – A Systematic Approach to Managing Safety Cases", Doctoral Thesis – University of York: Department of Computer Science. Sept 1998

[26] Ministry of Defence. Defence Standard 00-42 Issue 2, Reliability and Maintainability (R&M) Assurance Guidance. Part 3, R&M Case, 6 June 2003

[27] Ministry Of Defence. Defence Standard 00-55 (PART 1)/Issue 4, Requirements for Safety Related Software in Defence Equipment Part 1: Requirements, December 2004

[28] Ministry of Defence. Defence Standard 00-55 (PART 2)/Issue 2, Requirements for Safety Related Software in Defence Equipment Part 2: Guidance, 21 August 1997

[29] Ministry of Defence. Defence Standard 00-56. Safety Management Requirements for Defence Systems. Part 1. Requirements Issue 4, 01 June 2007

[30] Ministry of Defence. Defence Standard 00-56. Safety Management Requirements for Defence Systems. Part 2 : Guidance on Establishing a Means of Complying with Part 1 Issue 4, 01 June 2007

[31] SafSec Project. SafSec Methodology: Guidance Material: Integration of Safety and Security. Available at: http://www.altran-praxis.com/safSecStandards.aspx

[32] SafSec Project. SafSec Methodology: Standard: Integration of Safety and Security. Available at: http://www.altran-praxis.com/safSecStandards.aspx

[33] Software and Systems Engineering Vocabulary (sevocab). Available at www.computer.org/sevocab/

[34] UK CAA. CAP 670 Air Traffic Services Safety Requirements. UK Civil Aviation Authority Safety Regulation Group, 18 February 2010

[35] UK CAA CAP 760 Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases For Aerodrome Operators and Air Traffic Service Providers, 13 January 2006

© ISO/IEC 2011 – All rights reserved

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.

ICS 35.080

Price based on 10 pages

© ISO/IEC 2011 – All rights reserved

Authorized licensed use limited to: Politechnika Gdanska. Downloaded on December 19,2011 at 11:52:45 UTC from IEEE Xplore. Restrictions apply.