



DPC: 24/30495604 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 27 August 2024

Origin: International

Latest date for receipt of comments: 20 October 2024

Project No. 2024/01895

Responsible committee: IST/15 Software and systems engineering

Interested committees:

Title: Draft BS EN ISO/IEC/IEEE 15026-1 BS EN ISO/IEC/IEEE 15026-1 Systems and software engineering - Systems and software assurance. Part 1: Concepts and vocabulary.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 20 October 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC/IEEE DIS 15026-1

Systems and software engineering — Systems and software assurance —

Part 1: Concepts and vocabulary

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

Partie 1: Concepts et vocabulaire

ICS: 35.080; 01.040.35

ISO/IEC JTC 1/SC 7

Secretariat: **BIS**

Voting begins on:
2024-08-27

Voting terminates on:
2024-11-19

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC/IEEE DIS 15026-1:2024(en)



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

© IEEE 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or IEEE at the respective address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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

Email: stds.ipr@ieee.org
Website: www.ieee.org

Contents

Page

Foreword.....iv

Introduction.....v

1 Scope.....1

2 Normative references.....1

3 Terms and definitions.....1

3.1 Terms related to assurance.....2

3.2 Terms related to system life cycles.....4

3.3 Terms related to integrity level.....6

3.4 Terms related to risks and dependability.....6

4 Organization of this document.....10

5 Basic concepts.....10

5.1 General.....10

5.2 Assurance.....10

5.3 Stakeholders.....11

5.4 System and product.....11

5.5 Property.....11

5.5.1 General.....11

5.5.2 Properties as behaviours.....12

5.6 Uncertainty and confidence.....12

5.7 Conditions and initiating events.....12

5.8 Consequences.....13

6 Using multiple parts of ISO/IEC/IEEE 15026.....13

6.1 General.....13

6.2 Initial usage guidance.....13

6.3 Relationships among parts of ISO/IEC/IEEE 15026.....14

6.4 Authorities.....14

7 ISO/IEC/IEEE 15026 (all parts) and the assurance case.....15

7.1 General.....15

7.2 Justification of method of reasoning.....15

7.3 Means of obtaining and managing evidence.....16

7.4 Certifications and accreditations.....17

8 ISO/IEC/IEEE 15026 (all parts) and integrity levels.....17

8.1 General.....17

8.2 Risk analysis.....17

9 ISO/IEC/IEEE 15026 (all parts) and the life cycle.....18

9.1 General.....18

9.2 Assurance activities in the life cycle.....19

10 Summary.....19

Bibliography.....20

IEEE notices and abstract.....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.

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

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 contained in its standards.

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

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information Technology*, Subcommittee SC 7, *Software and systems engineering*, in cooperation with the Systems and Software Engineering Standards Committee of the IEEE Computer Society, under the Partner Standards Development Organization cooperation agreement between ISO and IEEE.

This second edition cancels and replaces ISO/IEC 15026-1:2019, which has been technically revised.

The main changes compared to the previous edition are as follows:

- definitions of terms introduced in other parts of ISO/IEC 15026 are added or modified;
- definitions of terms whose definitions were sourced from ISO/IEC 15288 and ISO/IEC/IEEE 24774 updated.

A list of all parts in the ISO/IEC/IEEE 15026 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Software and systems assurance and closely related fields share concepts but have different vocabularies and perspectives. This document provides a unifying set of underlying concepts and an unambiguous use of terminology across these various fields. It provides a basis for elaboration, discussion and recording agreement and rationale regarding concepts and the vocabulary used uniformly across ISO/IEC/IEEE 15026 (all parts).

This document clarifies concepts needed for understanding software and systems assurance and, in particular, those central to the use of ISO/IEC 15026-2, ISO/IEC 15026-3 and ISO/IEC 15026-4. It supports shared concepts, issues and terminology applicable across a range of properties, application domains and technologies.

Systems and software engineering — Systems and software assurance —

Part 1: Concepts and vocabulary

1 Scope

This document defines assurance-related terms and establishes an organized set of concepts and relationships to form a basis for shared understanding across user communities for assurance. It provides information to users of the other parts of ISO/IEC/IEEE 15026 including the combined use of multiple parts. The essential concept introduced by ISO/IEC/IEEE 15026 (all parts) is the statement of claims in an assurance case and the support of those claims through argumentation and evidence. These claims are in the context of assurance for properties of systems and software within life cycle processes for the system or software product.

Assurance for a service being operated and managed on an ongoing basis is not covered in ISO/IEC/IEEE 15026 (all parts).

A variety of potential users of ISO/IEC/IEEE 15026 (all parts) exists including developers and maintainers of assurance cases and those who wish to develop, sustain, evaluate or acquire a system that possesses requirements for specific properties in such a way as to be more certain of those properties and their requirements. ISO/IEC/IEEE 15026 (all parts) uses concepts and terms consistent with ISO/IEC/IEEE 12207 and ISO/IEC/IEEE 15288 and generally consistent with the ISO/IEC 25000 series, but the potential users of ISO/IEC/IEEE 15026 (all parts) need to understand the differences from concepts and terms to which they may be accustomed. This document attempts to clarify these differences.

The primary purpose of this document is to aid users of the other parts of ISO/IEC/IEEE 15026 by providing context, concepts and explanations for assurance, assurance cases and integrity levels. While essential to assurance practice, details regarding exactly how to measure, demonstrate or analyse particular properties are not covered. These are the subjects of more specialized standards of which a number are referenced and included in the Bibliography.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

ISO, IEC and IEEE maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>
- IEEE Standards Dictionary Online: available at <http://dictionary.ieee.org>

3.1 Terms related to assurance

3.1.1

assurance

grounds for justified confidence that a *claim* ([3.1.10](#)) has been or will be achieved

Note 1 to entry: By definition, assurance is about a claim.

Note 2 to entry: The claim can be a conjunction of more than one claim.

3.1.2

assurance argument

artefact that links tangible evidence and assumptions to provide a convincing and valid argument of a claim under a given context

3.1.3

assurance case

auditable artefact that provides a convincing and sound argument for a claim on the basis of tangible evidence under a given context

Note 1 to entry: An argument is valid if and only if it is necessary that if all of the premises are true, then the conclusion is true. An argument is sound if and only if it is valid and contains only true premises.

3.1.4

assurance case report

auditable artefact that provides the claim of an *assurance case* ([3.1.3](#)) and a complete index of the argument and evidence of the assurance case such that the assurance case of interest can be assembled from the index

Note 1 to entry: An assurance case report is mapped to the report field. An assurance case report is an introduction to the assurance case. Its content varies from one case to another. For simple and/or small assurance cases a report can be superfluous. For larger or more complex assurance cases the report can include a system description, some of the argument and its supporting evidence e.g. the higher-level arguments and their supporting evidence.

Note 2 to entry: Assurance case reports are often issued as periodic updates to the assurance case at pre-agreed points such as at the end of a life cycle stage. They report on results of assurance activities done so far, an assessment of overall progress and a review of assurance activities' performance. Assurance case reports can be used at decision gates for stage exit/entry by suppliers and for project monitoring by acquirers.

3.1.5

assurance claim

claim for which *assurance* ([3.1.1](#)) is considered

3.1.6

assurance information

information including a claim about a system, evidence supporting the claim, an argument showing how the evidence supports the achievement of the claim, and the context for these items

Note 1 to entry: The sub-claims included in the argument of assurance information can be about the life cycle of the *system-of-interest* ([3.2.10](#)) when, for example, the top-level claim implies continuous achievement of some property.

Note 2 to entry: ISO/IEC/IEEE 15026-2 specifies assurance cases that documents assurance information.

3.1.7

assurance objective

purpose of achievement of the *assurance claim* ([3.1.5](#))

Note 1 to entry: Assurance objectives determine the required degree of *integrity level* ([3.3.1](#)) and permissible uncertainty in the *assurance information* ([3.1.6](#)).

3.1.8**attribute**

inherent property or characteristic of an entity that can be distinguished quantitatively or qualitatively by human or automated means

Note 1 to entry: ISO 9000 distinguishes two types of attributes: a permanent characteristic existing inherently in something; and an assigned characteristic of a product, process, or system (e.g., the price of a product, the owner of a product).

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.2]

3.1.9**basic assumption**

assumption in a collection of claims shared by *assurance cases* (3.1.3) in a specific field

Note 1 to entry: Such a collection corresponds to a set of axioms in formal system in logic.

3.1.10**claim**

true-false statement about the limitations on the values of an unambiguously defined property — called the claim's property — and limitations on the uncertainty of the property's values falling within these limitations during the claim's duration of applicability under stated *conditions* (3.1.11)

Note 1 to entry: Uncertainties may also be associated with the duration of applicability and the stated conditions.

Note 2 to entry: A claim potentially contains the following:

- property of the system-of-interest;
- limitations on the value of the property associated with the claim (e.g., on its range);
- limitations on the uncertainty of the property value meeting its limitations;
- limitations on duration of claim's applicability;
- duration-related uncertainty;
- limitations on conditions associated with the claim; and
- condition-related uncertainty.

Note 3 to entry: 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, and can be multi-dimensional. The boundaries of these limitations are sometimes not sharp, e.g., they can involve probability distributions and can be incremental.

3.1.11**condition**

measurable qualitative or quantitative attribute that is stipulated for a requirement and that indicates a circumstance or event under which a requirement applies

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.6]

3.1.12**constraint**

externally imposed limitation on the system, its design, or implementation or on the process used to develop or modify a system

Note 1 to entry: A constraint is a factor that is imposed on the solution by force or compulsion and may limit or modify the design.

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.7]

3.1.13**critical property**

property that is agreed by primary stakeholders as having serious *consequence* (3.4.3)

3.1.14

dependability <of an item>

ability to perform as and when required

Note 1 to entry: Dependability includes availability, reliability, recoverability, maintainability, and maintenance support performance, and, in some cases, other characteristics such as durability, safety and security.

Note 2 to entry: Dependability is used as a collective term for the time-related quality characteristics of an item.

[SOURCE: IEC 60050-192:2015, 192-01-22]

3.1.15

inference

reasoning step that derives a claim from a list of claims (premises) under a specified context

Note 1 to entry: The claim derived by inference is the conclusion, and the supported claims from which the inference derives the conclusion are the premises.

Note 2 to entry: There are special inferences called obvious inferences. See 5.3.4 EXAMPLE 2.

3.1.16

property

attribute of things

3.1.17

type

set of values, elements or items

3.1.18

undeveloped argument

placeholder argument to be replaced by a concrete argument

3.2 Terms related to system life cycles

3.2.1

approval authority

person (or persons) and/or *organization* (3.2.3) (or organizations) responsible for approving activities, artefacts and other aspects of the *system* (3.2.4) during its life cycle

Note 1 to entry: The approval authority may include multiple entities, e.g., individuals or organizations. These can include different entities with different levels of approval and/or different areas of interest.

Note 2 to entry: In two-party situations, the approval authority often rests with the acquirer. In regulatory situations, the approval authority may be a third party such as a governmental organization or its agent. In other situations, for example, the purchase of off-the-shelf *products* (3.2.3) developed by a single-party, the independence of the approval authority can be a relevant issue to the acquirer.

3.2.2

design authority

person or *organization* (3.2.3) that is responsible for the design of the *product* (3.2.3)

3.2.3

organization

person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives

EXAMPLE Company, corporation, firm, enterprise, manufacturer, institution, charity, sole trader, association, or parts or combination thereof.

[SOURCE: ISO/IEC/IEEE 15288:2023, 3.25]