PD ISO/IEC TR 15026-1:2010

Incorporating corrigendum September 2012

BSI Standards Publication

Systems and software engineering — Systems and software assurance

Part 1: Concepts and vocabulary

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™

Full document details: PD ISO/IEC/TR 15026-1:2010

National foreword

This Published Document is the UK implementation of ISO/IEC TR 15026-1:2010, incorporating corrigendum September 2012. Together with BS ISO/IEC 15026-2:2011, BS ISO/IEC 15026-3:2011 and BS ISO/IEC 15026-4:2012 it supersedes BS ISO/IEC 15026:1998, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/15, Software and systems engineering.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2013.
Published by BSI Standards Limited 2013.

ISBN 978 0 580 81151 7

ICS 35.080

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 September 2010.

Amendments/corrigenda issued since publication

Date	Text affected
30 April 2013	Implementation of ISO/IEC corrigendum September 2012: Subclause 6.4 updated

Documents
Document Sharing Hub

Full document details: PD ISO/IEC/TR 15026-1:2010

TECHNICAL REPORT

ISO/IEC TR 15026-1

First edition
2010-08-15

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

Reference number
ISO/IEC TR 15026-1:2010(E)

Documents
Document Sharing Hub
© ISO/IEC 2010

Full document details: PD ISO/IEC/TR 15026-1:2010

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 2010

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

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/IEC/TR 15026-1:2010

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Terms and definitions 1

3 Document purpose and audience 4

4 Organization of report 4

5 Basic concepts 4
5.1 Introduction 4
5.2 Stakeholders 4
5.3 System and Product 6
5.4 Uncertainty 6
5.5 Assurance 6

6 How to use multiple parts of ISO/IEC 15026 7
6.1 Introduction 7
6.2 Initial usage concerns 7
6.3 Internal structure of parts 8
6.4 Relationships among parts of ISO/IEC 15026 9
6.5 Authorities 9
6.6 Mitigation of ambiguity 9

7 Assurance Case 10
7.1 Introduction 10
7.2 Claims 13
7.3 Arguments 23
7.4 Evidence 34
7.5 Management and life cycle of assurance case 39
7.6 Decision making using the assurance case 40

8 ISO/IEC 15026 and integrity levels 42
8.1 Introduction 42
8.2 Defining integrity levels 43
8.3 Establishing integrity levels 44
8.4 Planning and performing 45
8.5 Conditions and their initiating or transitioning events 46
8.6 Issues 46
8.7 Outcomes 48
8.8 Summary 48

9 ISO/IEC 15026 and life cycle processes: 15288/12207 49
9.1 Introduction 49
9.2 Technical processes 50
9.3 Transition, Operation, Maintenance and Disposal 55
9.4 Organization processes 56

10 Summary 57

Annex A (informative) **Frequently asked questions** 58

Annex B (informative) **Difficulties with terms and concepts** 59

Annex C (informative) **ISO/IEC 15026 relationships to standards** 61

Annex D (informative) **Phenomena** 64

Documents
Document Sharing Hub

© ISO/IEC 2010 – All rights reserved

Full document details: PD ISO/IEC/TR 15026-1:2010

Annex E (informative) **Security** **68**
Annex F (informative) **Selected Related Standards** **79**
Bibliography **85**

Tables

Table 1 — Examples of Stakeholders 5
Table 2 — Some time- and resource-related properties 21
Table 3 — Example ways of showing something is true 24
Table 4 — Communities with different viewpoints and approaches to reasoning 25
Table 5 — Relationship aspects that are possible bases for or relevant to arguments 30
Table D-1 — Some kinds and sources of phenomena 64

List of Figures

Figure 1 — Fragment of Structure 11
Figure 2 — Claim 16
Figure 3 — Argument Context 23
Figure 4 — Simple State Model 28
Figure 5 — Simplified "cause and effect" chains 28
Figure 6 — System and Environment 42
Figure 7 — Two actors cause transitions 47
Figure 8 — Life cycle process groups 49
Figure C-1 — Some relationships among standards 63

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

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.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard (“state of the art”, for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

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 TR 15026-1, which is a Technical Report of type 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*

— *Part 2: Assurance case*

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

ISO/IEC 15026:1998, IEEE Std 1228-1994 and IEEE Standard for Safety Plan were used as base documents in the development of ISO/IEC TR 15026-1.

Documents
Document Sharing Hub

© ISO/IEC 2010 – All rights reserved

Full document details: PD ISO/IEC/TR 15026-1:2010

Introduction

Within software and systems assurance and closely related fields, many specialties and subspecialties share concepts but have differing vocabularies and perspectives. This part of ISO/IEC 15026 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 all parts of ISO/IEC 15026.

This part of ISO/IEC 15026 clarifies concepts needed for understanding software and systems assurance and, in particular, those central to the use of subsequent parts of ISO/IEC 15026. This part of ISO/IEC 15026 supports intellectual mastery of software and systems assurance primarily at the level of shared concepts, issues and terminology applicable across a range of properties, application domains, and technologies.

The appreciation of the contents of this part of ISO/IEC 15026 might undergo change as work proceeds on the other parts of ISO/IEC 15026. A revision of this part of ISO/IEC 15026 reflecting any such changes is expected to be later published as an International Standard.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

Systems and software engineering — Systems and software assurance —

Part 1:
Concepts and vocabulary

1 Scope

This part of ISO/IEC 15026 defines terms and establishes an extensive and organized set of concepts and their relationships, thereby establishing a basis for shared understanding of the concepts and principles central to ISO/IEC 15026 across its user communities. It provides information to users of the subsequent parts of ISO/IEC 15026, including the use of each part and the combined use of multiple parts.

Coverage of assurance for a service being operated and managed on an ongoing basis is not covered in ISO/IEC 15026.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
assurance
grounds for justified confidence that a claim has been or will be achieved

2.2
assurance case
representation of a claim or claims, and the support for these claims

NOTE An assurance case is reasoned, auditable artefact created to support the contention its claim or claims are satisfied. It contains the following and their relationships:

- one or more claims about properties;
- arguments that logically link the evidence and any assumptions to the claim(s);
- a body of evidence and possibly assumptions supporting these arguments for the claim(s).

2.3
approval authority
entity with the authority to decide that the assurance case and the extent of assurance it provides are satisfactory

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

NOTE 2 In two-party situations, 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, e.g. the purchase of off-the-shelf products developed by a single-party, the independence of the approval authority can be a relevant issue to the acquirer.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/IEC/TR 15026-1:2010

2.4
claim
statement of something to be true including associated conditions and limitations

NOTE 1 The statement of a claim does not mean that the only possible intent or desire is to show it is true. Sometimes claims are made for the purpose of evaluating whether they are true or false or undertaking an effort to establish what is true.

NOTE 2 In its entirety, a claim conforming to ISO/IEC 15026-2 is an unambiguous declaration of an assertion with any associated conditionality giving explicit details including limitations on values and uncertainty. It could be about the future, present, or past.

2.5
design authority
person or organization that is responsible for the design of the product

2.6
failure
termination of the ability of an item to perform a required function or its inability to perform within previously specified limits

2.7
fault isolation
ability of a subsystem to prevent a fault within the subsystem from causing consequential faults in other subsystems

2.8
integrity assurance authority
independent person or organization responsible for assessment of compliance with the integrity-level-related requirements

NOTE Adapted from ISO/IEC 15026:1998, in which the definition is "The independent person or organization responsible for assessment of compliance with the integrity requirements."

2.9
integrity level
denotation of a range of values of a property

NOTE 1 Generally, the intention is that meeting these values related to the relevant items will result in maintaining system risks within limits.

NOTE 2 Adapted from ISO/IEC 15026:1998.

2.10
organization
person or a group of people and facilities with an arrangement of responsibilities, authorities and relationships

[ISO/IEC 15288:2008]

NOTE 1 This definition and notes are taken from ISO/IEC 15288:2008. The definition in ISO/IEC 15288:2008 was adapted from ISO 9000:2005.

NOTE 2 A body of persons organized for some specific purpose, such as a club, union, corporation, or society, is an organization.

NOTE 3 An identified part of an organization (even as small as a single individual) or an identified group of organizations can be regarded as an organization if it has responsibilities, authorities and relationships.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

2.11
process
set of interrelated or interacting activities which transforms inputs into outputs

[ISO/IEC 15288:2008 and ISO/IEC 12207:2008]

NOTE This definition does not preclude the existence of a null process, activity or transformation, or of null inputs or outputs.

2.12
process view
description of how a specified purpose and set of outcomes can be achieved by employing the activities and tasks of existing processes

NOTE This definition is adapted from the description of the process view concept in ISO/IEC 15288:2008, D.3.

2.13
product
result of a process

[ISO/IEC 15288:2008 and ISO 9000:2005]

NOTE 1 Results could be components, systems, software, services, rules, documents, or many other items.

NOTE 2 "The result" could in some cases be many related individual results. However, claims usually relate to specified versions of a product.

2.14
system
combination of interacting elements organized to achieve one or more stated purposes

[ISO/IEC 15288:2008]

NOTE 1 A system may be considered as a product or as the services it provides.

NOTE 2 In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g. aircraft system. Alternatively, the word "system" may be substituted simply by a context-dependent synonym, e.g. aircraft, though this may then obscure a system principles perspective.

NOTE 3 Notes 1 and 2 are also taken from ISO/IEC 15288:2008.

2.15
system element
member of a set of elements that constitutes a system

[ISO/IEC 15288:2008]

NOTE 1 A system element is a discrete part of a system that can be implemented to fulfil specified requirements. A system element can be hardware, software, data, humans, processes (e.g. processes for providing service to users), procedures (e.g. operator instructions), facilities, materials, and naturally occurring entities (e.g. water, organisms, minerals), or any combination.

NOTE 2 Note 1 is also taken from ISO/IEC 15288:2008.

2.16
systematic failure
failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

3 Document purpose and audience

The primary purpose of this part of ISO/IEC 15026 is to aid users of the other parts of ISO/IEC 15026. For each topic, it first briefly covers what might be needed by engineers and technical mangers new to the topic of assurance cases or integrity levels. Lists of aspects or examples are provided for concreteness and as reminders or checklists. 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.

If a decision is made to use any parts of ISO/IEC 15026, then understanding certain concepts and terms is essential. This part of ISO/IEC 15026 provides context, concepts, and explanations to aid users in doing this as well as aiding in the usage of the other parts.

A variety of potential users of ISO/IEC 15026 exists including developers and maintainers of assurance cases and those who wish to develop, sustain, evaluate, or acquire a system that possesses specific properties of interest in such a way as to be surer of those properties. Users of this International Standard can benefit from knowing the included terms, concepts, and principles. For example, while ISO/IEC 15026 uses terms consistent with ISO/IEC 12207 and ISO/IEC 15288 and generally consistent with the ISO/IEC 25000 series, the users of ISO/IEC 15026 need to know any differences from that to which they are accustomed. The remainder of this part of ISO/IEC 15026 attempts to clarify issues of the concepts of interest to users of ISO/IEC 15026.

4 Organization of report

Clause 5 of this part of ISO/IEC 15026 covers basic concepts such as stakeholders, product, assurance, and uncertainty. Clause 6 covers some issues of which users of the future ISO/IEC 15026-2, ISO/IEC 15026-3, and ISO/IEC 15026-4 need to be initially aware. Clauses 7, 8, and 9 cover terms, concepts, and topics particularly relevant to users of ISO/IEC 15026-2, ISO/IEC 15026-3, and ISO/IEC 15026-4, respectively, although users of one part can also benefit from some of the information in the clauses oriented to other parts. Clause 8 is for users of ISO 15026:1998, as well as of the future ISO/IEC 15026-3.

Those who have curiosity or initial questions about ISO/IEC 15026 could find it useful to take an early look at Annex A on page 58, the Frequently asked questions annex. Other annexes cover pitfalls with terminology (Annex B), ISO/IEC 15026's relationships to several other standards (Annex C), phenomena (Annex D) as a way of helping ISO/IEC 15026 users to think about possibilities, security (Annex E), and some related standards (Annex F). Annex E gives special attention to security because it is an area expected to be relatively new to many initial users of ISO/IEC 15026. However, ISO/IEC 15026 can be used for both positive concerns, such as high performance, as well as negative concerns, such as security. A bibliography is included at the end.

5 Basic concepts

5.1 Introduction

This clause covers the terms and concepts fundamental to ISO/IEC 15026: stakeholders, systems and products, uncertainty, and assurance.

5.2 Stakeholders

5.2.1 Introduction

Through their life cycle systems and software have multiple stakeholders who affect or are affected by the system and system-related activities. Stakeholders might benefit from, incur losses from, impose constraints on, or otherwise have a “stake” in the system.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

5.2.2 Kinds of stakeholders

A given system will typically have stakeholders from several of the categories in Table 1.

Table 1 — Examples of Stakeholders

Product's larger environment
Regulators
Standards bodies
Specific communities (such as government or the banking industry)
National (possibly multi-national) and international laws, regulations, treaties, and agreements
Enforcement personnel and organizations
Competitors
Entities about whom the product contains information (e.g. customers and suppliers)
Evaluators, regulators, certifiers, accreditors, and auditors
Attackers
The general public
Organizational
Sources of relevant policies (e.g. safety, security, personnel, procurement, and marketing policies)
Decision makers regarding acquisition and usage (including request for proposal writers and issuers as well as makers of decisions to acquire or use)
Authorized units within an organization
Directly related to product
Product developers and maintainers
Integrators of the system or software into a larger product (e.g. OEMs or enterprise-wide application developers)
Those involved in product transition (e.g. trainers and installers)
Product operators and administrators
End users
Others involved throughout the product's systems life cycle (e.g. sustainers and disposers)
System into which product is incorporated
Other systems interacting with the product or using the product's services
Suppliers of services or consumables to product
Product owners and custodians
Project management
Owners and custodians of elements in the system (e.g. data)

In addition, stakeholders can include non-users whose performance, results, or interests might be affected, e.g., entities whose software is executing on the same or networked computers.

A different but important kind of stakeholder is an attacker, who certainly imposes constraints or has interests involved with the system, as in, "Both we and the enemy have a stake in keeping within the laws of war." However, some in the security community and elsewhere use the term "stakeholders" in such a way as to exclude attackers. Attackers can be of many kinds and have a variety of motivations and capabilities. The issue of how hostile or malicious in intention or detrimental in action an entity would need to be to qualify as an attacker is unclear.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

A given system or project might involve more or less of the stakeholders in Table 1. Stakeholder roles and relative importance can be difficult to establish, for example, who—system funders, customers, beneficiaries, attackers, benefit gainers or loss sufferers—is more important or should have more influence on which decisions, including the importance to assurance-related decisions and importance as users of assurance-related artefacts. The existence and characteristics of potential or actual attackers can strongly influence decisions.

5.2.3 Stakeholder interests and assets

Stakeholder interests include any benefit, loss, or advantage, e.g., one says, “In the national interests” or “not in the interest of the organization” or “not in my interest.” Interests include the wealth and reputations of persons about whom information is kept. Assets may also be of many kinds, including real estate, facilities, equipment, people, wealth, information or data, an executing process, or anything else that is of value to stakeholders.[1] Assets within the system and its immediate environment do not necessarily include everything that might be relevant. Examples of those assets about which the contents of the system could facilitate positive or adverse actions of any kind include shareholder value, facilities, infrastructure, spies, soldiers, and other valued objects, processes, or conditions. The relevant stakeholders whose interests are of concern usually include the system’s owners and users, but developers and operators need to identify relevant stakeholder interests and assets and their value or relative importance to the development and operation of the system.

5.3 System and Product

To be consistent with ISO/IEC 15288 and 12207, ISO/IEC 15026, Systems and software assurance, uses the term “system” throughout. Users of this standard who are more familiar with using the term “product” should note that “system” includes products and services that are the results of processes as well as software, and system or software elements or components. While primarily motivated by concern for systems produced (at least in part) by human-controlled or artificial processes, this is not a restriction on its use. This standard can be used in reducing uncertainty about a system’s dependence on natural phenomena.

5.4 Uncertainty

Uncertainty is used in ISO/IEC 15026 as an inclusive term. It covers lack of certainty whether the uncertainty can be modelled probabilistically or not. This definition allows the term “uncertainty” to be applied to anything. Certain communities restrict the application of this term to predictions of future events, to physical measurements already made, or to unknowns. While these limited usages may be convenient within those communities, ISO/IEC 15026 users span many communities.

5.5 Assurance

While ISO/IEC 15026 uses a specific definition for the term as being grounds for justified confidence, for clarity ISO/IEC 15026 seldom uses the term “assurance” alone.

Generally, one needs grounds for justifiable confidence prior to depending on a system, especially a system involving complexity, novelty, or technology with a history of problems (e.g., software). The greater the degree of dependence, the greater the need for strong grounds for confidence. The appropriate valid arguments and evidence to establish a rational basis for justified confidence for the relevant claims for the system’s properties need to be made. These properties may include such aspects as future costs, behaviour, and consequences. Throughout the life cycle, adequate grounds need to exist for justifying decisions related to ensuring the design and production of an adequate system and to be able to place reliance on that system.

---

[1] The set of stakeholders whose interests are to be preserved or increased excludes adversaries and possibly others whose interests one might desire to limit, hinder, endanger, or harm. Note, however, that there may be overriding legal requirements to protect such excluded stakeholders, such as trespassers, thieves and enemy soldiers.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

Nevertheless, decision makers need to obtain sufficient confidence that is adequately justified. Professionals that use this International Standard need to supply adequate grounds for such confidence and have its adequacy correctly judged by decision makers.

NOTE This need can sometimes lead to including the kinds of evidence that the relevant decision makers find most convincing.

Assurance is a term whose usage varies, but all usage relates to placing limitations on or reducing uncertainty in such things as measurements, observations, estimations, predictions, information, inferences, or effects of unknowns with the ultimate objective of achieving and/or showing a claim. Such a reduction in uncertainty may provide an improved basis for justified confidence. Even if the estimate of a parameter's value remains unchanged, the effort spent in reducing uncertainty about its value can often be cost-effective since the resulting reduced uncertainty improves the basis for decision-making.

The term "assurance" may relate to different scopes – from the consequences in the world at large to system elements and their constituents as well as their interactions – and to any property of a system. Kinds and examples of properties are covered in 7.2.7.

Assurance may relate to (1) would the system or software as specified meet real-world needs and expectations, to (2) would or does the as-built and operated system meet the specifications, or to both (1) and (2). Specifications may be representations of static and/or dynamic aspects of the product. One may speak of an external specification, a specification related to the product-environment boundary, or a top-level specification that may contain some internal design. Specifications often include descriptions of capability, functionality, behaviour, structure, service, and responsibility including time- and resource-related aspects as well as limitations on frequency or seriousness of deviations by the product and related uncertainties. ISO/IEC 15288 and ISO/IEC 12207 as well as the IEEE standards on requirements divide these concerns into "functional" and "non-functional" ones.

Specifications may be prescriptions and/or constraints (e.g. for and on product behaviours) as well as include measures of merit and directions regarding tradeoffs. Generally, specifications place some limitations on when they apply such as on the environment and its conditions (e.g. temperature) and possibly the conditions of the product (e.g. age or amount of wear).

6 How to use multiple parts of ISO/IEC 15026

6.1 Introduction

This clause covers issues regarding use of this International Standard. The topics covered are Initial usage concerns, Internal structure of parts of ISO/IEC 15026, Relationships among parts of ISO/IEC 15026, Authorities, and Mitigation of ambiguity.

6.2 Initial usage concerns

The decision to use one or more parts of ISO/IEC 15026 involves understanding their purpose, scope, and requirements and considering their fit with the user's organizations, policies, processes, practices, personnel, standards and other governing documents. The decision to use ISO/IEC 15026 can be the result of risk assessments, needs for information for decision making (e.g., decisions to launch or acquire a product), customer direction, organizational practices, or regulatory requirements.

When conformance is not required, the decision regarding use might include deciding to conform but not claim conformance, to use the standard as guidance, or to conform to or use only portions as guidance.

Decisions concerning their voluntary use need to analyse the feasibility of doing so, including existing organizational readiness (e.g., need and relevant competencies), riskiness of the situation, cost/benefit (including the amount of value affected by decisions it would support), the advantages of taking a more systematic approach to system-related engineering and management activities and decisions, and the alternative approaches available. On one hand, assurance cases are simply aids for good risk management,

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

but on the other hand, they can involve a significant change in thinking and can influence every system-related activity.

The properties and/or claims covered when using ISO/IEC 15026 are entirely up to the users of the standard who are responding to their own needs and outside requirements. Any property or claim may be selected, regardless of its importance or related risk. However, ISO/IEC 15026-2 is intended to be used for high assurance situations and not low assurance ones, and the other parts are expected to also find their primary use among higher assurance situations.

ISO/IEC 15026 or its parts can be used alone or with other standards or guidance. They can be mapped to most life cycle standards, and can use any set of well-defined qualities or properties. Annex C begins to address these issues.

NOTE Many more or less process-oriented standards exist that are useful for their specificity in the detail and methods they contain. Many of these are usable in conjunction with parts of ISO/IEC 15026.

While ISO/IEC 15026-3 will be generally backwards compatible with ISO/IEC 15026:1998, transitioning to ISO/IEC 15026-3 will require dealing with some differences. ISO/IEC 15026-3 will open up new engineering and decision options, because it takes not only a standalone perspective but also one that includes relating integrity levels to an assurance case. ISO/IEC 15026-3 will concentrate more on the system itself and its integrity levels rather than on external risk analysis and also includes the creation of integrity levels. Clause 8 discusses integrity levels.

Occasionally user confusion exists concerning "should". Within ISO/IEC 15026, "should" is used "to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) ["should not"] a certain possibility or course of action is deprecated but not prohibited" ([129] page 65). No documented justification is required for doing otherwise.

A final sometimes misunderstood point is that maliciousness and subversion are concerns even when no security-related system property is involved. Malicious developers might have an effect on successful achievement of almost any property.

6.3 Internal structure of parts

The parts of ISO/IEC 15026 are:

— ISO/IEC 15026-1: Concepts and vocabulary: initially a Technical Report and then revised to be an International Standard and possibly a guidance document.

— ISO/IEC 15026-2: Assurance case: will include requirements on the content and structure of the assurance case.

— ISO/IEC 15026-3: System integrity levels: will relate integrity levels to the assurance case and include requirements for their use with and without an assurance case (revision of ISO/IEC 15026:1998).

— ISO/IEC 15026-4: Assurance in the life cycle: addresses concurrent development and maintenance of the system and its assurance case, including project planning for assurance considerations.

The future ISO/IEC 15026-2, ISO/IEC 15026-3 and ISO/IEC 15026-4 have a number of aspects designed to facilitate their use. The main purpose of their structure and layout is to provide separately identifiable individual requirements or small sets of related requirements to facilitate traceability regarding conformance. This structure may make a casual or initial reading less smooth, but eases the repeated readings and references during use.

The parts have limited introductory and explanatory material but are self-contained and intended to be usable by knowledgeable persons as standalone documents.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

6.4 Relationships among parts of ISO/IEC 15026

While each of ISO/IEC 15026-2, ISO/IEC 15026-3 and ISO/IEC 15026-4 will provide a separation of concerns and may be used alone, they may be used together as they form a related set. This part of ISO/IEC 15026 provides background, concepts, and vocabulary that are applicable to all three and particularly relates Clause 7 to ISO/IEC 15026-2, Clause 8 to ISO/IEC 15026-3, and Clause 9 to ISO/IEC 15026-4.

The assurance case is relevant to some extent in all parts. ISO/IEC 15026-2 concentrates on the contents and structure of the assurance case. ISO/IEC 15026-3 relates integrity levels to their role in assurance cases, and ISO/IEC 15026-4 provides details on integrating the assurance case into the system life cycle processes. ISO/IEC 15026-4 includes assurance-related concerns across the life cycle and concerns that extend beyond those directly related to the assurance case, including project planning for assurance-related considerations.

6.5 Authorities

Parts of ISO/IEC 15026 involve "authorities" as shown in Clause 3, Terms and definitions. For example, ISO/IEC 15026-3 includes obtaining agreements between the design authority and integrity assurance authority.

NOTE For example, a new system needs the approval authorities of acquirers to take charge of analysing the process of creating assurance cases with the design authority and the integrity assurance authority of the suppliers.

However, the "approval authority" for the assurance case is not necessarily the judge of conformance to a part of ISO/IEC 15026. To the extent possible claims of conformance to parts are judged on aspects that are more straightforward and more difficult to dispute than the quality of artefacts and decisions judged in the context of the system or project. In practice, contracts can explicitly call for the acquirer to be the approval authority or the approver of conformance to parts of ISO/IEC 15026.

Conflict of motivations, competence, diligence, and trustworthiness of any authority are potential issues. Therefore, parts of ISO/IEC 15026 calling for identification of an authority provide descriptions of their degree of independence. This allows decision makers, including potential users of systems, to consider these descriptions in deciding the degree of confidence they should have in any approval.

6.6 Mitigation of ambiguity

Clarity is needed for assurance cases, integrity levels, and defining processes. The requirements for unambiguous language within the documents it requires are explicit in ISO/IEC 15026. For example, each portion of the assurance case needs to be clear and unambiguous to its developers, reviewers, and users. Unambiguous does not necessarily imply precise or deterministic properties or measures, but rather that those properties or measures can be evaluated. Unambiguous also does not imply lack of uncertainty in measurement.

Definitions need to be clear. The variety of definitions that exist among the relevant audiences of the systems and software communities and their specialties and subspecialties and within ISO publications means that multiple-word terms or phrases often need to be used. Definitions of single words are unlikely to be shared across the relevant audiences and communities, and even within a single audience segment the term may be ambiguous or used in varying ways.

Thus, for lack of ambiguity to be achieved, terms need to be adequately defined and authors, reviewers, and users of the assurance cases, integrity levels, and defining processes need to have a shared understanding of the underlying concepts and context.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

7 Assurance Case

7.1 Introduction

An assurance case is a means to provide grounds for confidence and to aid decision making. The assurance case has one or more top-level claims in which confidence is needed and has supporting arguments connecting the top-level claims with multiple levels of sub-claims. The sub-claims are in turn supported by evidence and, where appropriate, assumptions.

NOTE This part of ISO/IEC 15026 often refers to a single top-level claim. However, this is not a comprehensive prescription; an assurance case may have multiple top-level claims.

The most common purpose of an assurance case is to provide assurance about system properties to parties not closely involved in the system's technical development processes. Such parties may be involved in the system's certification or regulation, acquisition, or audit. More broadly stated the purpose of an assurance case is to inform stakeholders' decision-making and to supply grounds for needed stakeholder confidence. Different stakeholders seek to achieve their own goals such as developing a suitably trustworthy system or deciding whether or not to use a system in light of the risks.

NOTE In addition, an assurance case can be created simply to ascertain reality or even what claim is (or possibly was or will be) true.

Usually, an assurance case addresses the reasons to expect and confirm successful production of the system, including concern for the possibilities and risks identified as difficulties or obstacles to developing and sustaining that system. Assurance cases include claims about a system, normally that it satisfies relevant requirements, and supporting arguments for these claims that are in turn supported by evidence or assumptions including their relationships. To convince stakeholders successfully, the possibilities and risks they perceive and their doubts should be addressed whether the developers believe these perceptions to be merited or not.

The assurance case provides a multi-level structure of claims, sub-claims and connecting arguments that are ultimately based on evidence and assumptions that provide a reasoned, auditable argument supporting a claim. Together they show the truth or achievement of the top-level claim(s) or their falsehood or non-achievement. Figure 1 shows the major kinds of components of an assurance case.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

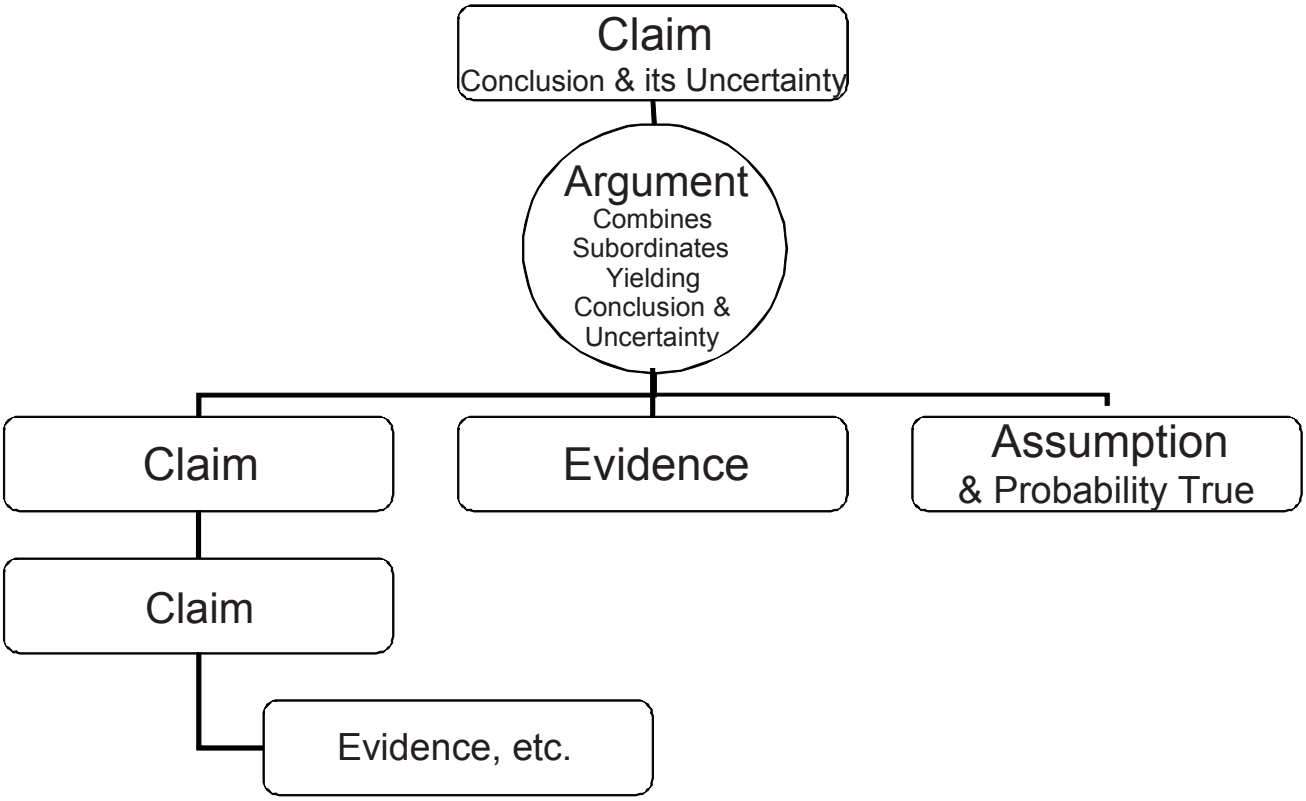

Figure 1 — Fragment of Structure

Best first considered with the initial system concept and requirements, the assurance case subsequently reflects experienced or postulated possibilities and risks; avoidance and mitigation strategies related to its claims; and an assurance argument referring to associated and supporting evidence. This evidence can come from design and construction activities, quality results from reviews, process fidelity records, standards conformance results, personnel qualification records, mathematical proof checkers, analyses, verification and validation activities, tests and trials, and eventually in-service and field data.

Any substantive modifications in the system or the assurance case's top-level claims will necessitate recorded changes to the assurance case. Such changes can also be generated by changes in the environment. Thus, an assurance case usually contains a progressively expanding body of evidence built up during development and later life cycle activities that responds as required to all relevant changes [[147], p. 5].

The users of ISO/IEC 15026-2 select the assurance case's purpose and the system and its required properties to be covered by the claim. The assurance case's argument should be supported by evidence and, where appropriate, assumptions.

A combined assurance case for multiple properties may be produced. Thus, the claim's property is possibly composed from multiple properties, and these possibly include consequences.

NOTE 1 An assurance case's claim(s) properties required could perhaps include the system's entire set of requirements for a property of interest. One example might have a top-level claim composed of (1) required limitations on consequences (2) functionality and properties of the system itself (e.g. that this functionality cannot be bypassed). The qualities defined in the ISO/IEC 25000-series include qualities related to functionality and constraints. The Common Criteria v. 3.1 Revision 2 [30] is also interested in both.

NOTE 2 Industry and agency standards and guides that are explicitly about assurance cases are included in the Bibliography. Standards or standards-related entries include [147], [150], [151], [155], [156], [157], [165], [166], [181], [182], [183], [197], [198], and [199].

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

NOTE 3 A safety case is an assurance case that is targeted at establishing safety claims. Another kind of assurance case used regularly is the Reliability, Availability and Maintainability or RAM Case. RAM assurance cases are the topic of [147]. Another approach to RAM cases is documented in the SAE JA1000 Reliability Program Standard [181].

Assurance case content includes relationships, specifications, definitions, justifications, real-world consequences, conditionalities, and uncertainties. Contents may include background information and links providing traceability. Contents need to be sufficient for all relevant stakeholders to be able to comprehend and evaluate the argument or case presented. Depending on the stakeholder and the anticipated evaluation context, contents may need to be scaled up or down accordingly, always conforming to ISO/IEC 15026.

To users of ISO/IEC 15026, the practicality of evaluation is a central concern of assurance cases. Evaluation addresses the issues of establishing estimates of a property's values and their uncertainty by predicting, measuring including testing, and analysing them. Assurance cases address the question of the uncertainty a property does or does not (or did or did not, or will or will not) meet its related claim (or claims).

The assurance case is central to the rational use of systems. Where uncertainty and consequence are serious concerns, an assurance case needs to exist whether written or not—otherwise an essential element needed to provide grounds for confidence (assurance) is missing. These consequences could be either positive or negative (e.g. risk).

Considered as an artefact, an assurance case has quality issues that concern the overall case, claims, arguments, evidence, and assumptions. Among these quality-related aspects are the nature of content, its form or structure (e.g. method of argumentation or modularity), semantic issues such as completeness, creation and maintenance including tool support, usability and presentation, integrity, validity, understandability, and having clearly stated conclusions with explicit degrees of uncertainty. One article [176] covers a substantial list of quality-related characteristics for assurance cases.

The success of an assurance case depends not only on its characteristics as a standalone artefact, but also on the project processes and the more particular assurance case methods, practices, techniques, and tools. Important practices include the assurance case being considered from the earliest stage in an effort; being planned, designed, developed, and maintained concurrently with the system; and being used to influence all activities and systems [148] and Appendix B in [197].

The approach to assurance or the assurance strategy should appear in any feasibility study and be further elaborated to accompany any operational concept document, and a description of the proposed assurance case would normally appear in a proposal document during acquisition.

The assurance case provides an audit trail of the relevant engineering concerns. It provides a justification for why certain activities have been undertaken and how they were judged successful. As a living, top-level control document, its status is continually tracked and typically summarized in Assurance Case Reports at predefined intervals or milestones. The assurance case usually remains with the system throughout its life cycle through disposal.

While certification and regulatory authorities do not always consider everything relevant, every aspect having potential significant consequences for meeting the top-level claim or for the confidence of key stakeholders has a potential place in a full assurance case. It should not only give coherent confidence to developers, sustainers, and acquirers, but also be directly usable by certifiers and accreditors.

Activities called "assurance activities" overlap with other project activities including those directed towards evaluations of both the system and the processes used to develop and sustain it. Activities directly creating, maintaining, and evaluating the assurance case need to be planned and performed and include:

- Create top-level assurance claim from requirements.
- Establish degree of uncertainty needed for information to be used in decision making.
- Establish structure of the argument with sub-claims, including their relationships.
- Create portions of the assurance argument tailored for the desired limitation on uncertainty.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

- Compile portions of the argument and supporting evidence.
- Verify.
- Validate.
- Use as input to certification.

This clause's major subclauses cover Claims, Arguments, Evidence including assumptions, Management and life cycle of assurance case, and Decision making using the assurance case.

7.2 Claims

7.2.1 Introduction

Selecting the top-level claim and the properties it involves are not restricted by ISO/IEC 15026, although their statement is. Top-level claims are often a portion of the total requirements and specification but may be something internal to the system, related to something the system depends upon or not directly related to the primary system of interest. This subclause includes coverage of motivations for claims, their form and scope, and example properties they might involve.

7.2.2 Motivations for a claim

7.2.2.1 Kinds of questions to answer

While the nominal question that the assurance case answers is: (Was, Is, or Will) the claim shown (be) within the required uncertainty limitations? This question might be stated as: Will it be good enough for what we require and are we sure enough about that answer? However, several other kinds of questions might readily be asked:

a) What is the chance that the claim's property will meet its limitations?

b) How lenient would limitations on the property's value need to be to allow us to be sure enough that its values will fall within limitations?

c) What can be shown about the claim's property from the evidence?

In addition, several other more open kinds of questions might be asked:

d) What, if anything, can we be sure (enough) about regarding this situation or system?

e) What if anything can be ascertained about this situation or system?

f) Finally, for each of a) through e), one can also ask, for how long and under what conditions?

These questions represent different motivations or starting places for using an assurance case.

Assurance cases can be used to address verification and validation concerns by answering the following questions:

a) If the assurance case's top-level claim is met, will this result in meeting real-world intention(s), need(s), and expectation(s)?

b) Will or does the system as designed, implemented, transitioned, and operated meet the top-level claim?

These two questions need to be dealt with by any approach to the life cycle of a system where risk, consequences, or uncertainty are issues. Dealing with these questions aids not only gauging feasibility, suitability, and desirability of development, production, transition, and operations, but also corrective action,

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

learning, and improvement. These questions may be dealt with separately or together, and assurance cases used for one alone, both together in a single assurance case, or both separately as long as the ISO/IEC 15026-2 requirements for such a combination are met.

Risk management combines degrees of uncertainties regarding achievement of questions a) and b) to establish the comprehensive, net or residual potential consequences or risk.

7.2.2.2 Categories of requirements

ISO/IEC 25030 provides a categorization for requirements that, while only for software, has relevance to other aspects of systems as well as to the system as a whole. These categories include functionality, quality (both internal and external), development requirements, and quality in use.

Examples of measures of internal quality are given in ISO/IEC 9126-3 (to be replaced by ISO/IEC 25022). Examples of measures of external quality are given in ISO/IEC 9126-2 (to be replaced by ISO/IEC 25023). Examples of quality in use measures are given in ISO/IEC 25010. Many come from life cycle processes that usually follow development, such as manufacturability, marketability, training, maintainability and test equipment, usability, interoperability, use in extreme environments, legal compliance, cost of operation, and mission accomplishment (not all from ISO/IEC 25010).

Producers and other stakeholders may prioritize properties such as efficiency and reliability and perform trade-off studies between them. Additionally, achieving a quality such as safety might affect speed or other characteristics making them less desirable. Specifying the system's external behaviour is a system design activity and, as such, can be fraught with tradeoffs, including ones among properties or qualities. A number of techniques have been created for addressing these trades, such as those in [25], [70], [131], [169], and [42]. The specifying of a top-level claim is sometimes the result of analyses including trade-off studies.

The need fulfilled by a top-level claim and its assurance case can be small compared to the concerns related to the total system. Will the ground at the site support the planned structure? Will a sub-function on a new airplane be at least as safe as the same sub-function on similar prior airplanes? Is a tool adequately trustworthy? Assurance cases may be used for either large or small requirements or needs.

7.2.3 Form of a claim

A claim takes the form of a true-false statement concerning a property that may be a combination of other properties. The term "property" is used quite generally – a property is a descriptive aspect that may have a claim concerning it, at least in principle, evaluated as true or false. Subclause 7.2.7 explains properties in detail.

This usage of the term "property" derives from, is consistent with, and subsumes the broad use of the term "property" in ISO/IEC CD 25010 where it is used spanning properties including properties that are inherent or not, internal, external, and in use or context. In principle, one could apply ISO/IEC 15026 to claims regarding any property of any importance.

A claim is a true-false statement that concerns 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. Uncertainties also may be associated with the duration of applicability and the stated conditions. Thus, a claim potentially contains the following components:

- Claim's property.
- 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.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

- Limitations on conditions associated with the claim.
- Condition-related uncertainty.

NOTE 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 but rather involve probability distributions, are incremental or have other fuzzy aspects.

Each of these components may have details within it. In particular, the property might include consequences or its worth – how valuable or costly it is or would be. Limitations on a property's values may be fixed (held constant). This might be done for the sake of exploring or analysing what values of other components of the claim (and possibly other properties) would be consistent with these fixed limitations – for example, the property of possessing a certain strength for what duration.

Each of the following can be stated about each of these components within the claim:

- What is required.
- What is planned to be established.
- What is actually shown or established.
- What is possibly or actually contradicted.

NOTE Some subset of them is established within the context of interest at a given moment – e.g., what is required has been specified, what is planned has been determined, or what has actually been shown is known.

The quality of a claim depends on it being fully specified, so the true-false statement may need to be further defined by references to either internal or external material such as definitions of terms or descriptions of context. Aspects needing supplementary definitions may include limitations on the range of property values (e.g., required degree of achievement or tolerances), its duration of applicability, conditions it requires or on which it depends, properties being combined and relations or measures used in the combination, and limitations on uncertainty. While many terms have well-known meanings and even abbreviations, e.g., kilometres per hour, that do not need explicit definition, many do, and all terms need to be explicitly stated, such as units of measure,

Often the conditions under which the claim is said to be true and its duration of applicability are treated as unvarying constants. However, they could be treated as variables and as having uncertainties. This is particularly true when the purpose of the assurance case is to simply establish what is true. For example, uncertainty may exist about the durability of the system or how long it will continue to possess a quality. Figure 2 gives a simplified view of the claim's components and their relationships.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

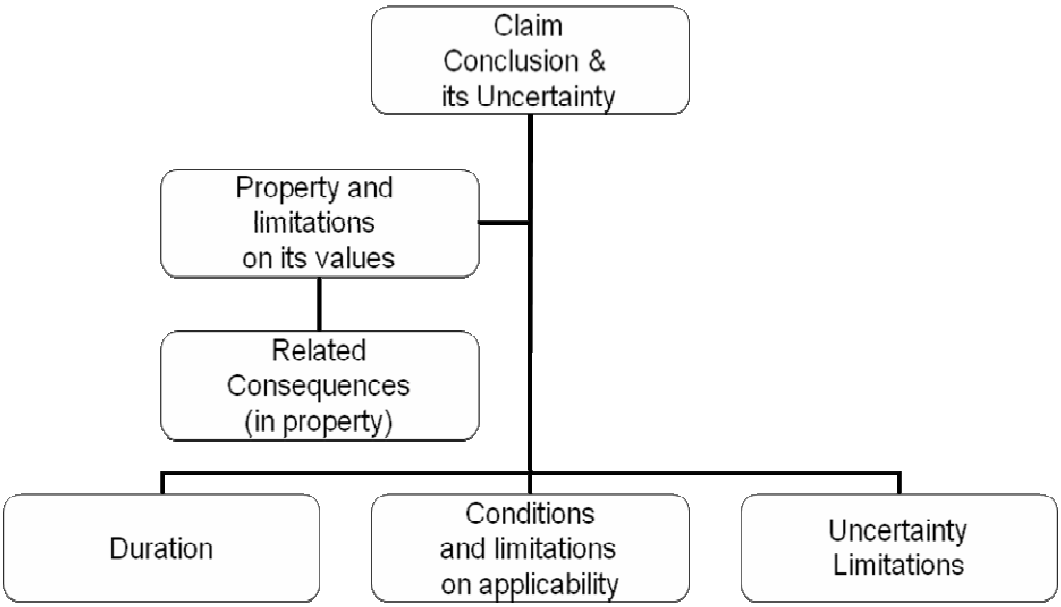

Figure 2 — Claim

In addition to the required limitations on uncertainty, a claim can have several categories of uncertainty associated with it: the uncertainty that is required to be achieved, the uncertainty that is planned to be achieved, and the uncertainty that has already been achieved. The uncertainty about the claim achieved by its supporting argument (and sub-claims, evidence, and assumptions) needs to meet any required limitations on its uncertainty. Finally, uncertainties can exist about uncertainties.

Among the forms in which claims may be stated is in terms of placing limitations on events or the establishment and preservation of conditions. For example, claims might take the forms of:

- For events:
  - Having desired behaviours and events.
  - Limitations on undesirable behaviours and events.
- For conditions:
  - Establishing (and possibly preserving or re-establishing) the preconditions for desired events.
  - Establishing and preserving the conditions that preclude (or limit) undesirable events.

To preclude an event, the relevant condition should imply the negation of the precondition for such an event. Similarly, one speaks of states and state transitions. A state of a system, a possibly relevant condition, can involve many aspects as [[14], p. 13] states, “The total state of a given system is the set of the following states: computation, communication, stored information, interconnection, and physical condition.” If a system contains humans, then the relevant portions of their states are also part of the system state.

7.2.4 Scope of concern

In different situations or activities, concerns for properties can vary in extent and in time. In extent or nature, concerns vary across several echelons of lessening scale from the real world to the individual system element or service, behaviour, or property as well as across their relationships, makeup, contents, and governance. In time, concerns can exist in a context before the conception of a particular system and beyond a system’s life cycle to ultimate consequences and residual obligations. A system-related claim can have a scope of interest that is on one side of or extends across the system environment.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

7.2.4.1 Extent

Recognizing these varying scopes of concern, ISO/IEC 25010 defines three different kinds of quality for a software product:

- Quality in use: the extent to which a software product used by specific users meets their needs to achieve specific goals with effectiveness, productivity, safety and satisfaction in specific contexts of use.
- External software quality: capability of a software product to enable the behaviour of a system to satisfy stated and implied needs when the system is used under specified conditions.
- Internal software quality: Capability of a set of static attributes of a software product to satisfy stated and implied needs when the software product is used under specified conditions.

A somewhat similar sense of expansiveness exists when conceptualizing where the behaviour, events, or conditions of interest occur. These might relate to different scopes of concern, including:

- Real world – concerns regarding funds, lives, real property, natural environment, and other interests of stakeholders, including allies, adversaries, and neutrals or bystanders.
- System-environment interface – user interface, interface with sensor or effector, service offered by the system, service depended upon by the system, intake of consumables, output of system (including by-products), physical support, interaction with test environment/equipment.
- Internal to system:
  - System elements, resources, or assets.
  - Non-computing elements, resources, or assets, possibly containing computing or information sub-elements, resources, or assets.
  - Computing or information elements, resources, or assets – database, stored software, computing hardware.
  - System behaviour – internal operations or operations viewed from an internal perspective.
  - Software behaviour.
  - Enabling functionality – logging, automatic recovery.

Generally, from outside-in (top to bottom of list), the scopes form an ordered layering of extent of concern. These roughly correspond to layers in an assurance case argument that include consideration of consequences and base their argument on behaviour, events, and conditions in the environment as affected by behaviour at the system-environment boundary, which is in turn the result of behaviour internal to the system. Ultimately, concern is usually driven by real-world effects: benefits, costs, and consequences. However, everything down to the internal details of the system may be relevant in building an argument.

7.2.4.2 Duration of applicability

The duration of applicability of a claim might be stated in calendar time, as a time interval or intervals, as during a life cycle process or processes, as during certain activities, as under certain conditions, or in some combinations of ways. The duration of applicability might result from what is required or what is achievable. While the duration of applicability is usually a constant, it may have required, planned, and supported values and should at least be tacitly consistent with the other corresponding values. The duration of applicability also may have associated uncertainty, but this is not a requirement.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

7.2.5 Consequence

In practice, claims can extend beyond the boundaries of the system or its behaviours. In particular, claims can place limitations on consequences of a system's behaviour and/or system-related events, activities, and/or conditions – especially on the values of consequences. One may refer to:

- **Consequence:** Any effect (change or non-change), usually associated with an event or condition or with the system and usually allowed, facilitated, caused, prevented, changed, or contributed to by the event, condition, or system. It could yield a benefit, a loss, or neither.
- **Adverse consequence:** Consequence associated with a loss.
- **Desirable (or positive) consequence:** Associated with a gain or avoiding an adverse consequence.

A consequence has value or is desirable or undesirable from a stakeholder's perspective, viewpoint or interests. A consequence may occur anywhere in the system's life cycle or beyond. Certain effects within a system may be treated as consequences such as wear from use and damage from mishaps. For example, "The publishing of the concept for the system induced enquires for both investment and purchase," or, "The system was retired and disposed of long ago, but liability remains and new liability claims continue to occur."

7.2.6 Claim violation

7.2.6.1 Violation-related terms

The following three terms in ISO/IEC 15026 are widely used:

- Fault: A defect in a representation of a system or a system that if followed and/or executed/activated could potentially result in an error. It is incorrect and usually thought of in terms of a static representation or a static instance of the system. Faults can occur in specifications when they are not correct. (See 7.2.7.3.1.)
- Error: An erroneous state of the system.
- Failure: An externally visible deviation from the system's specification.

Under the same conditions, exercising a fault might or might not result in an error. Likewise, an error might or might not result in a failure. At a certain time, a fault, error, or failure can be known or unknown.

Usage is less uniform for the following four terms also used in ISO/IEC 15026:

- External mistake (e.g. human error): External entity's or entities' non-malicious action or inaction, or non-malicious input to or interaction with the system that has the potential to result in a fault or/and error (and thereby possibly in failure) or an adverse consequence either not intended or not intended to be adverse.
- Attack: A malicious action or interaction with the system or its environment that has the potential to result in a fault or an error (and thereby possibly in a failure).
- Adverse consequence, as defined above.
- Violation: A behaviour, act, or event deviating from a system's desired property or claim of interest. Examples might include violation of a performance standard, a speed limit, limitations on tolerances, confidentiality, laws, or a claim of suitability.

Human errors (including organizational ones) can be intended or unintended, planned or unplanned, and in agreement or disagreement with a plan, reflecting a mistaken plan, a cognitive lapse in enacting a plan, or a non-cognitive slip.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

7.2.6.2 Violation-related concepts

NOTE In the area of safety the term "violation" is used to refer to a deliberate human contravention of a procedure or rule.

Threatening entities – also referred to as sources of danger, threat agents, and attackers – can possess capabilities, resources, motivations, and intentions that enable them to initiate and carry out non-malicious (e.g. mistaken) or malicious efforts to violate a claim. Violators use their capabilities to take advantage of system- and/or environment-provided opportunities called vulnerabilities, i.e., "weaknesses…that could be exploited or triggered by a threat source" [161].[2] Non-malicious and malicious entities use specific methods (e.g., agents and kinds of attacks) that often fall within recognizable patterns referred to as patterns of abuse, failure patterns, accident patterns, and attack patterns.

Systems or their environment often employ countermeasures to limit or reduce the opportunities for and ease of violations and limit or reduce adverse consequences such as the extent and intensity of damage that would result from a violation. Generally, attackers make gains only after further effort while system stakeholders make efforts to limit losses. Their respective gains and losses often differ

7.2.7 Properties

7.2.7.1 Introduction

Properties are a means of description, including specification or definition. A property might include a condition, a characteristic, an attribute, a quality, a trait, a measurement, and a consequence. A property might be invariant, or dependent on time, situation, or history.

NOTE In the use of ISO/IEC 15026, a property is usually expected to be relevant directly or indirectly to a system or systems.

Properties may be of interest for what they were in the past, what they are presently, or what they will be in the future. Generally, the last is the most important in ISO/IEC 15026. As this knowledge involves predicting the future, it is often the most difficult and uncertain to attain. Therefore unsurprisingly, a system's future behaviour and consequences often become principal issues in its assurance.

Many of the properties of interest are qualities of the system. Several standards and reports provide lists and definitions of qualities including ISO/IEC 9126, ISO/IEC 25010 and the related series, ISO/IEC 2382-14, ISO 9241, ISO/TR 18529, and ISO/TS 25238. Several standards or reports mention consequences associated with systems within a specific domain. Examples include ISO 14620 [90], ISO 19706 [104], and ISO/TS 25238 [116]. Risk management standards also address consequences, for example ISO/IEC 16085 [97].

Several general properties have been mentioned and more are listed below. However, a specific system requires specified properties within these general properties. Examples of concern for properties include the integrity of a barrier, the maintainability of a piece of equipment, the availability of a less than three minute response by the fire department, and the early confidentiality of new weapons (e.g. the US F-117 stealth fighter). For information or data, confidentiality may only be relevant to a portion of the system's data and integrity concerns only relevant to certain operations involving certain data. The limitations on uncertainty for each engineering application of a property may vary with the degree of seriousness of the property and that in turn usually reflects the possible consequences in the real world.

Properties may include (but are not limited to) dependability-related qualities such as reliability, availability, integrity, maintainability, correctness, accuracy, safety, confidentiality, accountability, or potential for human error; time- and resource-related ones such as processing speed, schedulability, throughput, and storage capacity; and human and organizational ones such as those related to human factors, as well as more global ones such as profit or mission achievement.

---

[2] For many purposes, the meaningfulness and need to separate vulnerabilities from other weaknesses can be low or non-existent. In addition, a question always exists about the current and future contexts that are relevant for "could be exploited or triggered".

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

7.2.7.2 Specifying properties as behaviours

Often the property is specified as a behaviour. For example, a property could be that a certain erroneous state cannot be reached or that a certain sequence of transitions should (or cannot) occur. During performed operations, behaviour-related properties might be formally specified as a combination of:

- Restriction on allowed system states (sometimes called the “safety property”).
- System states that must be reached; required progress or accomplishment (Liveness property).
- Constraints on flows or interactions; requirements for separation.

These kinds of properties can be stated as conditions or constraints that must be true of the system.[3] In practice, these are non-trivial and modularized, involving time and starting state(s) as well as state transitions related to interaction with the system’s (or software’s) environment.

If the system states are adequately known or modelled, this approach can also be taken at the system-environment interface (or software and its environment). One may also wish to model the environment if affects on and within it or changes in its state are important to overall consequences. This is one way requirements related to the environment’s condition (e.g., a certain condition in the environment would be catastrophic) and combined system-environment behaviour can be addressed. This is not an unusual situation as the situation of interest is often larger than the system.

Many kinds of flows such as of gases, fluids, traffic, or information are of possible interest as well as constraints on them such as non-interference and separations to be maintained. In addition, flow constraints are often convenient or necessary to specify aspects of information security [144] including access control mechanisms and policies, and restrictions on information overtly or covertly communicated,

7.2.7.3 Other types of properties

Properties are everywhere. They include anything objectively measurable and many things that are not. Examples include shape, colour, attractiveness, available opportunities, reusability, buoyancy, hardness, and mechanical strength. ISO/IEC 9126-1, ISO/IEC 26702, and ISO/IEC 25030 list many other product qualities that could be the subject of assurance. Other examples are in the following subclauses.

7.2.7.3.1 Correctness

Two major kinds of correctness are relevant:

- Correctness of the specification (or portion thereof) in terms of meeting needs and expectations of stakeholders and for practical purposes such as being feasible.
- Correctness of artefacts and the system in terms of agreement with the specifications – as well as, by extension, agreement during transition, operation, and the rest of the system’s life cycle.

For the latter point, the system might be considered as having two variants of correctness:

- A system is correct at its external boundary if it would always meet its external behaviour specification under the required conditions. That is, it has no failures.
- A system is correct throughout if it contains no faults and therefore is never, under the required conditions, in an error state. In ISO/IEC 25010 terms, this is an internal quality.

---

[3] If specified formally, this can allow static analysis of conformity of designs and code, potentially adding creditable assurance evidence.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

Being internally correct (correct throughout) implies being correct at the external boundary, an external quality in ISO/IEC 25010 terms. A system can be externally correct, however, without being internally correct if it can tolerate or recover from internal error states and never display incorrect externally visible behaviour.

7.2.7.3.2 Dependability

Dependability is a qualitative “umbrella” term [[14], p. 13]. ISO/IEC 25010 notes that "dependability characteristics include availability and its inherent or external influencing factors, such as: reliability, fault tolerance, recoverability, integrity, security, maintainability, durability, and maintenance support." Several standards address dependability (e.g. [70], [71], and [75]), and many more address the qualities within it. IEC 50 (191) offers related definitions [69].

Thus, dependability includes reliability, safety, maintainability, integrity, availability, plus related survivability; and when addressing security includes confidentiality, accountability (knowing who or what did something), non-repudiation (their not being able to deny it), authenticity, security compliance, and immunity (the degree to which the product is resistant to attack), In addition, interfacing with humans or usability, particularly error-prone and inconvenient interfaces, can also have a significant effect on dependability.

Assets may be categorized by attributes related to the dependability property of interest. Examples include confidentiality (e.g., Top Secret, Secret, Confidential, or Unclassified); degree of integrity (e.g., accurate and up-to-date versus old and with unknown accuracy); or criticality of availability or acceptable degree of unavailability (e.g. outage length 0-1 minute, 1-5 minute, 5-10 minutes, 10-30 minutes, 30 minutes-2 hours, greater than two hours). Ultimately, such categorizations derive from and are surrogates for the values of the stakeholders’ real-world benefits and losses (and sometimes uncertainties) potentially associated with the property’s preservation and violation.

7.2.7.3.3 Time- and resource-related

Time- and resource-related properties include meeting deadlines, efficiency, and storage capacity. These are not only important alone but also important in combination with dependability-related and other properties.

Many relationships and potential tradeoffs can exist among dependability properties and speed, efficiency, or other time- or resource-related properties. An example of a property that is relevant to both types is computational difficulty. Computational difficulty is an issue when one tries to compute something and when one wants to prevent someone else from computing something. The first is of interest in achieving real time performance and the latter in decryption.

Another example spanning the two types is availability and timing-out on whatever the deadline is in the particular measurement of availability. In the end, the issue in availability is not whether the system will eventually respond, but will it respond within a specified (e.g., useful or acceptable) time period.

Table 2 lists several properties related to time and resources. These include rates such as throughput or processor clocking, size, and economic ones. An entry such as “storage capacity” could relate to anything stored from fuel to binary bits. These types of properties are often measures of some aspect of performance and partial measures of merit for a system.

Table 2 — Some time- and resource-related properties

Timing	Throughput
• On time	• Bandwidth
• Meeting Deadline	Speed
• Schedulability	• Rates of Learning and Use
• Delay or Latency	Size
• Response Time	• Storage Capacity
• Sequence	Productivity
• Serializability	Efficiency
• Order Independent	Cost

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

7.2.7.3.4 Human- and organization-related

- An almost unlimited number of properties can be associated with humans and organizations. Among common ones relevant to systems are usability, occupational health and safety, size and reach, physical strength, mission accomplishment, and benefit and loss.
- Normally, existence of a human interface requires concern for human factors within an assurance case because almost every property is affected by it particularly any external quality or a quality in use. Human factors are addressed in several standards, for example [84], [99], and [107].

7.2.7.3.5 Tolerance- and resilience-related

Two common objectives for tolerance and resiliency are:

- Be resilient in response to events or conditions.
- Limit damage or decreases in benefits.

Among the principles sometimes mentioned in connection with resilience are redundancy, diversity, separation, generality, flexibility/adaptability, and restricting dependence. However, a system can have several objectives and activities related to resilience and limiting damage including:

- Forecast events and conditions.
- Maintain readiness.
- Detect events and conditions (desirable and undesirable particularly the latter including precursors, warnings, near misses, and suspicious events).
- Notify and warn.
- Record (e.g. via logs).
- Separation (e.g. by distance, time, barriers, or flow control).
- Continue service, although possibly degraded.
- Damage confinement (including by isolation and risk sharing).
- Diagnosis.
- Repair.
- Put system in a proper state:
- When current state is detected or inferred to be illegitimate (recovery).
- Preventively (e.g. regardless of knowing if needed or if indications exist that might otherwise later experience problem).
- Flexibility and the capability and tactics to successfully adapt and deal with events and conditions.
- Reserves and reserve capacity.
- Characterization, analysis, investigation of root cause or causer.
- Operational "safety" margins.
- Learn and improve.
- Arrangements or agreements with entities in the environment to provide aid (possibly including alliances).

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

The issues also exist concerning the readiness for, response time, speed, capacity, efficiency/cost, and efficacy of these list entries along with doing them when not needed and not doing them when needed. Flexibility and adaptability are often provided, at least in part, by humans.

7.3 Arguments

7.3.1 Introduction

Arguments are the glue that holds the assurance case together by relating its immediate underlying support – sub-claims, evidence, or assumptions – to the claim (or claims) it supports. It yields the combined effect of its evidence, sub-claims, and assumptions into a conclusion.

The term "conclusion" describes the actually shown or established conclusion regarding whether actual property values (did, do, or will) make the true-false statement true or false. The conclusion has its associated uncertainty - that is the uncertainty associated with the claim's property's actual value(s) - meeting it limitations.

The uncertainty regarding the conclusion derives from the uncertainties in the argument's immediate underlying support plus the strength or rigor of the argument and its own effect (plus or minus) on uncertainty. For example, several pieces of evidence that individually would leave much uncertainty about the claim might be combined by an argument into support yielding a claim with low uncertainty.

The resulting uncertainty needs to be within the limitations for uncertainty that were allocated or budgeted to the claim. This required limitation on uncertainty (e.g. it could be in terms of limitation on risk) derives from the uncertainty limitations of claims yet higher in the overall argument structure and ultimately from the limitations associated with the top-level claim. Limitations on the claim in question may be affected by “local” consequences associated with a sub-claim in the assurance case. This might be the situation if the claim relates to a system element whose misbehaviour could have separable consequences of its own.

Figure 3 provides the context for an argument showing how its super-ordinate claim (and sometime claims) is implied by the sub-claims, evidence, and assumptions that lie immediately below it and provide its support.

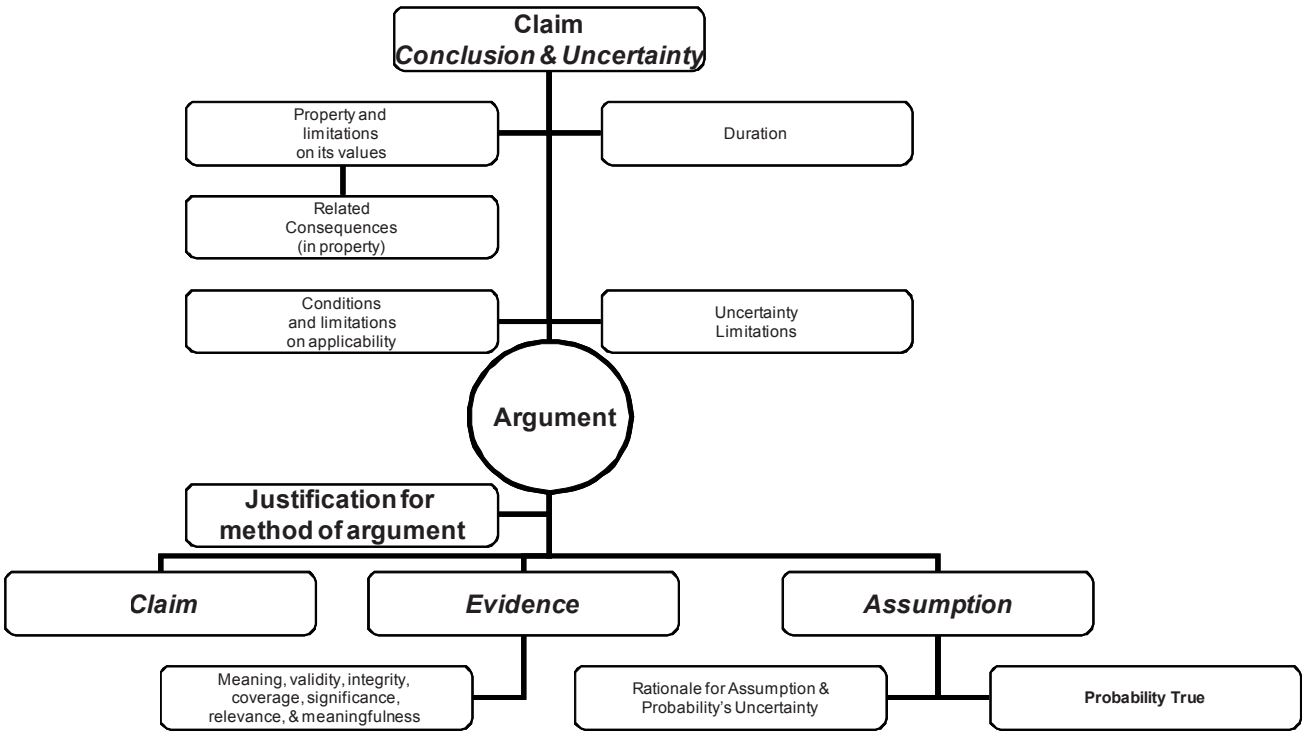

Figure 3 — Argument Context

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010

This subclause briefly discusses the variety of reasoning methods that one might see or consider. This is followed by covering the roles arguments might play in an assurance case, and several issues concerning the bases for and the structures of arguments.

7.3.2 Reasoning Methods

7.3.2.1 Introduction

Many methods of reasoning exist: some are more rigorous than others and may produce stronger results, some are quantitative and some not, and different ones may be appropriate for different situations. Human judgement can frequently play a role. For example, using probability related to occurrence of a natural event contrasts with the need for concern for the possibility of an intelligent, malicious action. Regardless of the method used to reason and decide, it can be difficult to gain adequate information, understand, and structure or model the situation in a way that results in very low uncertainty.

Subjects of and approaches to reasoning differ among communities having differing motivations, mindsets, and often multiple methods of reasoning. Methods of reasoning include:

- Quantitative:
  - Deterministic (e.g., formal proofs).
  - Non-deterministic formal systems for reasoning:
    - Probabilistic.
    - Game theoretic (e.g., minimax).
    - Other uncertainty-based formal systems of reasoning (e.g. fuzzy sets).
- Qualitative (e.g., staff performance evaluations, court judgements, and qualitative statements of event causality).

Some examples of methods of reasoning and their ways of showing something is true (possibly with some uncertainty) are listed in Table 3 — Example ways of showing something is true.

Table 3 — Example ways of showing something is true

Logic
Reduction (e.g. infer by laws of logic, definition, substitution, simplification)
Generalize to collection from arbitrary particular member
Contraposition
Contradiction
Induction
Show existence true by an example
(Show false by counterexample)
By Cases
Probability
Inference (e.g. probability theory)
Induction (e.g. statistics, observations, experiments, tests)
Models
Simulation
Analysis
Agreement among
Multiple methods or instances of showing
Suitable humans

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15026-1:2010