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)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Tables

List of Figures

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.

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.

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.

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.

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

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.

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.

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.

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,

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.

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 a greater or lesser 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.

While ISO/IEC 15026-3 supports its use with a ISO/IEC 15026-2-conformant assurance case, it also supports use of integrity levels without an assurance case or with an assurance case that is not entirely conformant to ISO/IEC 15026-2. However, users of ISO/IEC 15026-3 require ISO/IEC 15026-2, as parts of it are required related to integrity levels. In addition, ISO/IEC 15026-3 places a subset of the requirements in ISO/IEC 15026-2 on any assurance cases used with integrity levels, and some are also requirements ISO/IEC 15026-3 places on all risk analyses.

ISO/IEC 15026-4 addresses integrating the assurance case into the system life cycle processes and the concurrent development and maintenance of the system and its assurance case. While more extensive, its requirements are consistent with the assurance case life cycle requirements in ISO/IEC 15026-2, although it can be used with an assurance case that is not conformant to ISO/IEC 15026-2. ISO/IEC 15026-3 makes many points about what can be included in an integrity level's imposed requirements on development and maintenance or as evidence within an assurance case. 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

