INTERNATIONAL STANDARD

ISO/IEC 15026-1

First edition
2013-11-01

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 15026-1:2013(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

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

This first edition of ISO/IEC 15026-1 cancels and replaces ISO/IEC TR 15026-1:2010, which has been technically revised.

ISO/IEC 15026 consists of the following parts, under the general title *Systems and software engineering — Systems and software assurance*:

— *Part 1: Concepts and vocabulary*

— *Part 2: Assurance case*

— *Part 3: System integrity levels*

— *Part 4: Assurance in the life cycle*

The IEEE Computer Society collaborated with ISO/IEC JTC 1 in the development of the international standards of ISO/IEC 15026. *IEEE Std 1228-1994 and IEEE Standard for Safety Plan* were used as base documents in the development of this standard.

Introduction

Software and systems assurance and closely related fields 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 ISO/IEC 15026-2 to ISO/IEC 15026-4. It supports shared concepts, issues and terminology applicable across a range of properties, application domains, and technologies.

Systems and software engineering — Systems and software assurance —

Part 1: Concepts and vocabulary

1 Scope

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

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

2 Applicability

2.1 Audience

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 requirements for specific properties in such a way as to be more certain of those properties and their requirements. ISO/IEC 15026 uses concepts and terms consistent with ISO/IEC 12207 and ISO/IEC 15288 and generally consistent with the ISO/IEC 25000 series, but the potential users of ISO/IEC 15026 need to understand differences from concepts and terms to which they may be accustomed. This part of ISO/IEC 15026 attempts to clarify these differences.

2.2 Field of applicability

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

3 Terms and definitions

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

NOTE These are intended to be uniform through all parts of ISO/IEC 15026.

3.1 Terms related to assurance and properties

3.1.1
assurance
grounds for justified confidence that a claim has been or will be achieved

3.1.2
claim
true-false statement about the limitations on the values of an unambiguously defined property—called the claim's property—and limitations on the uncertainty of the property's values falling within these limitations during the claim's duration of applicability under stated conditions

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

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

— 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;

— limitations on conditions associated with the claim;

— condition-related uncertainty.

Note 3 to entry: The term "limitations" is used to fit the many situations that can exist. Values can be a single value or multiple single values, a range of values, or multiple ranges of values, and can be multi-dimensional. The boundaries of these limitations are sometimes not sharp, e.g. they may involve probability distributions and may be incremental.

3.1.3
assurance case
reasoned, auditable artefact created that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s)

Note 1 to entry: An assurance case 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);

— justification of the choice of top-level claim and the method of reasoning.

3.1.4
dependability
collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance

Note 1 to entry: Dependability is used only for general descriptions in non-quantitative terms.

Note 2 to entry: ISO/IEC 25010[99] 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.[64] and[69]), and many more address the qualities within it. IEC 60050-191 offers related definitions.[63]

[SOURCE: IEC 60300-1:2003]

3.2 Terms related to product and process

3.2.1
process
set of interrelated or interacting activities which transforms inputs into outputs

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

3.2.2
process view
description of how a specified purpose and set of outcomes may be achieved by employing the activities and tasks of existing processes

[SOURCE: ISO/IEC 15288:2008, D.3]

3.2.3
product
result of a process

Note 1 to entry: Results could be components, systems, software, services, rules, documents, or many other items.

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

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

3.2.4
system
combination of interacting elements organized to achieve one or more stated purposes

Note 1 to entry: A system may be considered as a product or as the services it provides.

Note 2 to entry: 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.

[SOURCE: ISO/IEC 15288:2008]

3.2.5
requirement
statement that translates or expresses a need and its associated constraints and conditions

Note 1 to entry: Requirements exist at different tiers and express the need in high-level form (e.g. software component requirement).

[SOURCE: ISO/IEC/IEEE 29148:2011]

3.2.6
system element
member of a set of elements that constitutes a system

Note 1 to entry: 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.

[SOURCE: ISO/IEC 15288:2008]

3.3 Terms related to integrity level

3.3.1
integrity level
claim of a system, product, or element that includes limitations on a property's values, the claim's scope of applicability, and the allowable uncertainty regarding the claim's achievement

Note 1 to entry: Generally, the intention is that maintaining limitations on a property's values related to the relevant items will result in maintaining system risks within limits.

Note 2 to entry: Adapted from ISO/IEC 15026:1998.

3.3.2
integrity level requirements
set of specified requirements imposed on aspects related to a system, product, or element and associated activities in order to show the achievement of the assigned integrity level (that is, meeting its claim) within the required limitations on uncertainty; this includes the evidence to be obtained

Note 1 to entry: Since an integrity level is defined as a claim, the two phrases "achievement of the assigned integrity level" and "meeting its claim" are equivalent.

Note 2 to entry: In ISO/IEC 15026:1998, 3.3.1 and 3.3.2 are referred to as the "integrity level" and "integrity requirements" respectively. The latter has been changed to "integrity level requirements" both for increased clarity and because this is common usage in safety.

Note 3 to entry: IEEE Std 1012:2004 defines "integrity level" as "a value representing project-unique characteristics (e.g. software complexity, criticality, risk, safety level, security level, desired performance, reliability) that define the importance of the software to the user." That is, an integrity level is a value of a property of the target software. Since both a claim and a statement that a property has a particular value can be regarded as a proposition of a system or software, the two definitions of integrity levels have significantly the same meaning.

3.4 Terms related to conditions and consequences

3.4.1
consequence
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

Note 1 to entry: It could yield a benefit, a loss, or neither.

3.1.8
risk
combination of the probability of an event and its consequence

Note 1 to entry: The term "risk" is generally used only when there is at least the possibility of negative consequences.

Note 2 to entry: In some situations, risk arises from the possibility of deviation from the expected outcome or event.

Note 3 to entry: See ISO/IEC Guide 51 for issues related to safety.

[SOURCE: ISO/IEC 16085]

3.4.2
adverse consequence
undesirable consequence associated with a loss

3.4.3
desirable (or positive) consequence
consequence associated with a benefit or gain or avoiding an adverse consequence

3.4.4
error
erroneous state of the system

3.4.5
fault
defect in a system or a representation of a system that if executed/activated could potentially result in an error

Note 1 to entry: Faults can occur in specifications when they are not correct.

3.4.6
attack
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) or an adverse consequence

3.4.7
violation
behaviour, act, or event deviating from a system's desired property or claim of interest

Note 1 to entry: In the area of safety, the term "violation" is used to refer to a deliberate human contravention of a procedure or rule.

3.4.8
failure
termination of the ability of a system to perform a required function or its inability to perform within previously specified limits; an externally visible deviation from the system's specification

3.4.9
systematic failure
failure related in a deterministic way to a certain cause that can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

3.5 Terms related to organization

3.5.1
organization
person or a group of people and facilities with an arrangement of responsibilities, authorities and relationships

Note 1 to entry: A body of persons organized for some specific purpose, such as a club, union, corporation, or society, is an organization.

Note 2 to entry: 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.

[SOURCE: ISO/IEC 15288:2008]

3.5.2
approval authority
person (or persons) and/or organization (or organizations) responsible for approving activities, artefacts, and other aspects of the system during its life cycle

Note 1 to entry: 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 to entry: 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, for example, 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.

3.5.3
design authority
person or organization that is responsible for the design of the product

3.5.4
integrity assurance authority
independent person or organization responsible for certifying compliance with the integrity level requirements

Note 1 to entry: 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."

4 Organization of this International Standard

Clause 5 of this International Standard covers basic concepts such as assurance, stakeholders, systems and products, uncertainty, and consequence. Clause 6 covers some issues of which users of 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 for other parts. A Bibliography is included at the end. References to numbered items in the Bibliography are shown in brackets throughout.

5 Basic concepts

5.1 Introduction

This clause covers the concepts and vocabulary fundamental to all parts of ISO/IEC 15026.

5.2 Assurance

ISO/IEC 15026 uses a specific definition for assurance as being grounds for justified confidence. Generally, stakeholders need 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 in the relevant claims about 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.

Assurance is a term whose usage varies among the communities who use the term. However, 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 property'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.

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 system. Specifications often include descriptions of capability, functionality, behaviour, structure, service, and responsibility including time-related and resource-related aspects as well as limitations on frequency or seriousness of deviations by the product and related uncertainties.

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).

5.3 Stakeholders

Through their life cycle systems and software have multiple stakeholders who affect or are affected by the system and the system life cycle processes. Stakeholders might benefit from, incur losses from, impose constraints on, or otherwise have a "stake" in the system, and therefore are those that provide the requirements for the system. Stakeholders can include non-users whose performance, results, or other requirements 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. This International Standard includes the attacker as a stakeholder; however, some in the security community and elsewhere exclude attackers from their use of the term "stakeholders."

The relevant stakeholders whose requirements are of concern include not only the system's owners and users, but also developers and operators who need to identify requirements for the development and operation of the system. Depending on conditions and consequences, the various stakeholders require grounds for justified confidence in properties of the system for which they identified requirements.

5.4 System and Product

To be consistent with ISO/IEC 15288 and ISO/IEC 12207, ISO/IEC 15026 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 standard can be used in reducing uncertainty about a system's dependence on natural phenomena as well.

5.5 Property

ISO/IEC 15026 relates assurance to requirements of a property of a system or software product. A property might include a condition, a characteristic, an attribute, a quality, a trait, a measurement, or a consequence. A property might be invariant, or dependent on time, situation, or history. In ISO/IEC 15026, a property is expected to be relevant directly or indirectly to a system or systems and thus have related requirements.

Properties may have requirements 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, a system's future behaviour and consequences (see 5.8) often become principal issues in its assurance.

Many of the properties with requirements are qualities of the system. Several standards and reports provide lists and definitions of qualities that could be the subject of assurance including ISO/IEC 9126-1, ISO/IEC 25010 and the related series, ISO/IEC 2382-14, ISO 9241, ISO/TR 18529, and ISO/TS 25238.

This use of the term "property" derives from, is consistent with, and subsumes the broad use of the term "property" in ISO/IEC 25010 where it is used spanning properties that are inherent or not, internal, external, and in use or context.

Producers and other stakeholders may prioritize properties such as efficiency and reliability and perform trade-off studies between them and their related requirements. A number of techniques have been created for addressing these trades, such as those in [25], [64], [122], [157], and [40]. The specifying of a top-level claim for a property is sometimes the result of analyses including trade-off studies.

5.5.1 Properties as behaviours

Often the property is specified as behaviour. 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 constraint.

These kinds of properties can be stated as conditions or constraints that must be true of the system.[1)] 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.

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[135] including access control mechanisms and policies and restrictions on information overtly or covertly communicated,

5.6 Uncertainty and confidence

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. Uncertainty can include vague notions that may be modelled without the use of probability. 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.

The degree of confidence that can be or is justifiably engendered based on a specific assurance case may vary by individual or organization and the situation. The less uncertainty about an assurance case’s claims, the higher the degree of justified confidence. However, the conversion of an amount of uncertainty into a degree of justified confidence in suitability for certain applications is not straightforward or well understood. For this and other reasons, consequences are sometimes directly included within the assurance case. While this closes a logical gap, it does not remove the decision maker’s act of judgement regarding the merited degree of confidence.

5.7 Conditions and initiating events

The assurance case needs to cover all the conditions that could have a significant negative effect on the conclusion and uncertainty of the top-level claim. The potentially relevant universe of conditions and events can be hard to initially identify[2] and ascertaining which ones might have a significant effect can be difficult without at least initially including them in the assurance case.

Historically, the one condition that has received the most attention is system failure. A substantial volume of checklists, practice, and literature exists concerning system failure (e.g,[2],[71] and[14] Chapter 18 page 475-524). While much of this work has been done in the communities addressing safety, security, or human error, system failure can result in less achievement of a positive property or consequence as well as negative properties or losses.

The dangerousness of system behaviours can differ by the conditions of its environment. These behaviours and conditions often need combining during analysis to establish whether adverse consequences will result or not. The actual conditions of its environment might or might not be known within the system depending on its sensors or inputs and their processing.

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

The designers of the system might or might not be cognizant of all the initiating events for a condition within the environment; however, dangerous conditions may need to be dealt with even though not all of their initiating events are known or recognizable.

5.8 Consequences

Outside the system, much of the reasoning is based on conditions that could lead to adverse consequences and their initiating events or preconditions. Inside the system reasoning is based on conditions that can lead to dangerous system behaviours and the initiating events or preconditions for these conditions.

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:

A consequence is desirable or undesirable from a stakeholder's perspective, viewpoint or interests. A consequence may occur anywhere in the system's life cycle.

In complex socio-technical systems, explanations of mishaps or claim violations cannot be limited to "component" failures. Adverse consequences can result from normal behaviour variability and unintended or unanticipated interactions.[57][54] Regardless of how they arise, dangerous conditions and adverse consequences are subjects for mitigation.

Attackers can possess capabilities, resources, motivations, and intentions that enable them to initiate and carry malicious efforts to violate a claim. Violators use their capabilities to take advantage of system-provided and/or environment-provided opportunities called vulnerabilities, i.e. "weaknesses... that could be exploited or triggered by a threat source"[150].[2)]

A 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.

Several standards or reports mention consequences associated with systems within a specific domain. Examples include ISO 14620,[79] ISO 19706,[81] and ISO/TS 25238.[121] Risk management standards also address consequences, for example ISO/IEC 16085[91]and ISO 31000.

6 Using multiple parts of ISO/IEC 15026

6.1 Introduction

ISO/IEC 15026 or its parts can be used alone or with other standards or guidance. The parts of ISO/IEC 15026 can be mapped to most life cycle standards and can use any set of well-defined qualities or properties.

6.2 Initial usage guidance

The properties and/or claims covered when using ISO/IEC 15026 are entirely up to the users of the standard who are responding to the system's stakeholders' needs and requirements. Any property or claim may be selected for an assurance case, regardless of its importance or related risk; however, the parts of ISO/IEC 15026 are designed primarily for those properties that one or more primary stakeholders deem as critical. ISO/IEC 15026-4 uses the term "critical properties" for these stakeholder priorities and requirements.

While ISO/IEC 15026-3 is 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

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".

includes relating integrity levels to an assurance case. ISO/IEC 15026-3 concentrates 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.

6.3 Relationships among parts of ISO/IEC 15026

The parts of ISO/IEC 15026 are:

— ISO/IEC 15026-1, *Concepts and vocabulary*, explains concepts and terms as a basis for all Parts of this International Standard.

— ISO/IEC 15026-2, *Assurance case*, includes requirements on the content and structure of the assurance case.

— ISO/IEC 15026-3, *System integrity levels*, relates integrity levels to the assurance case and includes requirements for their use with and without an assurance case (revises ISO/IEC 15026:1998).

— ISO/IEC 15026-4, *Assurance in the life cycle*, gives assurance-related guidance and recommendations for specific activities throughout system and software life cycle processes.

While ISO/IEC 15026-2, ISO/IEC 15026-3, and ISO/IEC 15026-4 provide a separation of assurance topics and may be used alone, they may be used together because they form a related set. This part of ISO/IEC 15026 provides background, concepts, and vocabulary that are applicable to all three and specific introductions to coverage of ISO/IEC 15026-2, ISO/IEC 15026-3, and ISO/IEC 15026-4.

The assurance case is relevant to a greater or lesser extent in all parts, although ISO/IEC 15026-4 discusses achieving the claim and showing the achievement of the claim whether or not such "showing" is contained in an artefact specifically called an "assurance case."

ISO/IEC 15026-2 concentrates on the contents and structure of the assurance case. ISO/IEC 15026-3 relates integrity levels and assurance cases by describing how integrity levels and assurance cases can work together, especially in the definition of specifications for integrity levels or by using integrity levels within a portion of an assurance case. This relationship is governed by the degree of risk and dependencies in the system.

If the risks or the risk treatment are not well understood or if the dependency structure of the whole system or the choice of suitable claims is unclear, then using an assurance case is the better choice than using integrity levels. This particularly is the case when facing new kinds of risks or using a new kind of risk treatment. In these situations, justifying the choice of the top-level claim for the assurance case is important.

When the risks and their treatment are well understood, however, developers need not justify the choice of the top-level claim and need only select the proper claims for their context from a known set—an integrity level from a set of integrity levels. In these situations, the generic arguments created by the definers of the integrity level provide the justification that meeting the integrity level requirements will adequately show the meeting of the integrity level. Such a justification (e.g. a generalized assurance case) is usually created one time by a separate organization and used by multiple projects.

ISO/IEC 15026-4 includes assurance-related guidance and recommendations for activities across the life cycle processes including activities that extend beyond those directly related to an assurance case, e.g. project planning for assurance-related considerations.

6.4 Authorities

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

7 ISO/IEC 15026 and the assurance case

7.1 Introduction

ISO/IEC 15026-2 covers the structure and content of an assurance case. It describes the five principal components of an assurance case: claims, arguments, evidence, justifications, and assumptions. The purpose of an assurance case is to improve assurance communications by informing stakeholders' decision-making and supplying grounds for needed stakeholder confidence. The most common use 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. Usually, an assurance case addresses the reasons to expect and confirm successful production of the system, including the possibilities and risks identified as difficulties or obstacles to developing and sustaining that system.

Unlike logical proofs of the deduction of the claims from the evidence, which covers the absolute truth or Platonic truth aspects, assurance cases deal with the dialectic aspects of the system where the truth is always relative or even subjective. In other words, logical proofs are described under a fixed logical theory, but assurance cases may be rebutted on the basis that the underlying logical theory is inappropriate. The need for assurance case arises when one realizes the properties of the systems in the real world can never be completely formalized in a logical theory, but there is always something which is not covered by any logical formalization.

NOTE When the top-level claim is about safety, security, dependability or RAM (reliability, availability and maintainability), assurance cases associated with these claims are called safety cases, security cases, dependability cases or RAM cases, respectively. See,[139],[142],[143],[146],[154],[155],[168],[74],[22],[23] and[24] in the Bibliography.

Considered as an artefact, an assurance case has quality-related aspects such as 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[164] covers a substantial list of quality-related characteristics for assurance cases. The quality-related aspects of an assurance case are not covered in ISO/IEC 15026-2 or any part of ISO/IEC 15026.

Any substantive modifications in the system, changes in the environment, or changes in the assurance case's top-level claims will necessitate recorded changes to the assurance case. 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 [[139], p. 5].

NOTE An assurance case's claim(s) on the values of properties could 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.

7.2 Justification of method of reasoning

An argument has an associated justification for the validity or merit of its method of reasoning. The method of argument can be an additional source of uncertainty.

A variety of bases for argumentation and analysis in the assurance case might be used, and these vary in their applicability, power, resulting accuracy and uncertainty, and ease of use. Subjects of and

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

Examples of methods of reasoning include:

- Quantitative:
  - Deterministic (e.g. formal proofs).
  - Non-deterministic formal systems for reasoning:
    - Probabilistic,
    - Game theoretic (e.g. minimax), or
    - 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.

Complex products and situations—and any involving humans—are beyond the current state of the art to "quantitatively" create precise and accurate predictions. Subjective judgements are used in the absence of affordable, suitable, more objective methods and techniques or where needed to supplement or evaluate the results of such techniques. Supplementing quantitative techniques with expert review and judgement is widely used and generally accepted. As with other forms of argumentation, subjective judgements take the form of a claim and its support. While sometimes necessary or advantageous, use of subjective judgement within the assurance case can lead to additional uncertainties, so, generally, (just as with assumptions) the less critical the judgement is the better.

The patterns of occurrences of "natural" events and common, non-malicious human behaviours are usually described probabilistically. However, possibilities for intelligent, malicious actions whose probability is not determinable or not knowable is particularly a concern if the intelligent, malicious adversary deliberately violates any probability estimates one could make regarding their behaviour, e.g. to achieve surprise. This distinction is central to the difference in reasoning between safety and security.

7.3 Means of obtaining and managing evidence

For any property, many means of obtaining evidence exist. Among these are human experience, history, observations, measurements, tests, evaluation and compliance results, analyses, defects, and inferences. The evidence should achieve the objectives claimed in the assurance argument (MoD DefStan 00-42 Part 3, section 9.1[139]).

The body of evidence can become quite large and may need to be organized and managed by some framework providing permanence and traceability of the evidence in order to provide users confidence in its source, contents and validity. One guidebook[150] indicates:

- Evidence should be uniquely identified so that arguments can uniquely reference the evidence.
- Evidence should be verifiable and auditable.
- Evidence should be protected and controlled by configuration management.
- Evidence needs to be accompanied by the metadata needed to properly use it within the assurance case.

This last point is simply a restatement of what testing is supposed to achieve related to the assurance case.

7.4 Certifications and accreditations

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 evidence. It should not only give coherent confidence to stakeholders, but also contain enough information to be used by certifiers and accreditors.

The aviation and nuclear power industries have long histories of standards and certifications, and the security community in ISO/IEC JTC 1/SC 27 has been working on the topic of assurance for many years. Security examples include the Common Criteria, FIPS 140 for cryptology, and ISO/IEC 27002, *Information technology–Code of Practice for Information Security Management,* combined with ISO/IEC 27001 (formerly with UK standard BS 7799-2:2002) form a basis for an Information Security Management System (ISMS) certification of an operational system. The UK Ministry of Defence and Civil Aviation Authority have also produced standards of interest including assurance-case-based standards for reliability, maintainability, and safety—e.g,[139],[142],[143],[22] and.[23] Many standards are listed in the Bibliography.

The safety community (e.g. commercial aviation) has used certification (designated agent or licensure) of key personnel as part of its approaches. A number of safety and computer security certifications exist from management-oriented ones to technical ones about specific products, e.g. certifications from the International Information Systems Security Certification Consortium (ISC) and the SANS Institute.

8 ISO/IEC 15026 and integrity levels

8.1 Introduction

Integrity levels are suitable for use for certain levels of risk or to support an assurance case and impose criteria especially on the project, evidence collected, and system. An integrity level can be viewed as a representation of the degree of confidence that is used to reach agreement among stakeholders of a system about risks related to that system.

ISO/IEC 15026-3 first establishes an integrity level framework. The remainder of the standard covers defining integrity levels, using integrity levels, determining system or product integrity levels using risk analyses, assigning system element integrity levels, meeting integrity level requirements using evidence, and agreements and approvals involving authorities (see 6.4).

Integrity level requirements reflect what is required to achieve and show that the system or system element has (or had or will have) the properties claimed by its integrity level. A system's integrity level states what would be adequate in terms of properties of the entire system. Thus, showing the properties has a basic role in showing the meeting of larger claims involving the system and its environment including desirable or undesirable consequences. If such larger claims are not made, then achieving and showing system element integrity levels supplies a basic part of showing the top-level claim regarding the system itself.

In practice, integrity levels are often discussed in terms emphasizing the evidence needed to meet the integrity level requirements and thereby provide evidence for the arguments supporting claims regarding properties of the system itself. However, the quality of the arguments justifying meeting integrity level requirements as showing the achievement of its related integrity level is also important because of the affect of that quality on uncertainties. Argument-, evidence- and assumption-related uncertainties are a part of establishing integrity level requirements.

NOTE Integrity levels and standards utilizing them have a significant history especially in safety. Integrity levels in safety-related standards are defined in multi-level sets addressing varying degrees of stringency and/or uncertainty of their achievement with higher levels providing higher stringency and lower uncertainty. One example safety standard is IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related* systems.[70] Elsewhere, similar schemes are used with different labels, e.g. "conformance classes."

8.2 Risk analysis

Risk analysis establishes the required integrity level for the entire system. Risk analysis is an ongoing and iterative process that should balance what is not yet knowable with what needs to be known. The integrity levels resulting from risk analysis are a translation of the values of consequences into the occurrences and timings of conditions or behaviours of the system. This translation is propagated to the integrity levels internal to the system and of its dependences as they are also in terms of occurrences

and timings. Thus, integrity levels are a codification of what is needed to be done and shown for various ranges and severities of limitations on property values and their associated uncertainties.

ISO/IEC 15026 does not cover risk analysis in detail. Many standards and guidance documents exist that offer guidelines for risk analysis and can aid in the identification of potential adverse consequences. IEC 61508[70] and IEC 31010 ed. 1.0 (2009-11-27), *Risk management--Risk management techniques,* provide approaches to risk analysis. As safety-specific terminology is used in IEC 300-3-9, the terms "hazard" and "harm" should be interpreted as "dangerous condition" and "adverse consequence," respectively. IEC 60300, *Dependability management*,[64] also provides guidance.

Other specialized standards include ISO 13849[78] on machinery, ISO 14620[79] on space systems, ISO 19706[81] on fire, ISO/TS 25238[121]on health informatics, ISO/IEC 27005[110] on information security, and UK CAP 760[24] on air traffic and airports. Also of possible interest are the more general risk management standards ISO/IEC 16085[91]and ISO 31000.

9 ISO/IEC 15026 and the life cycle

9.1 Introduction

ISO/IEC 15026-4, *Assurance in the life cycle*, provides a *process view* for systems and software assurance by providing a statement of purpose and a set of outcomes suitable for systems and software assurance. The concept of a process view is formulated and described in an annex of ISO/IEC 15288, *Systems and software engineering — System life cycle processes*. Like a process, the description of a process view includes a statement of purpose and outcomes. Unlike a process, the description of a process view does not include activities and tasks. Instead, the description includes guidance and recommendations explaining how the outcomes can be achieved by employing the activities and tasks of the various processes in ISO/IEC 15288 and ISO/IEC 12207, *Systems and software engineering — Software life cycle processes*.

All of the life cycle processes are described in both ISO/IEC 15288 and ISO/IEC 12207 although the processes in ISO/IEC 12207 are specialized to software and, in some cases, have different names reflecting that specialization. ISO/IEC 12207 contains processes not contained in ISO/IEC 15288 related to software implementation processes; support processes, and reuse processes.

The processes, activities, tasks, and the guidance and recommendations all have to be performed in the context of a life cycle model. The multi-part Technical Report ISO/IEC/TR 24748, *Systems and software engineering – Life cycle management* is intended to facilitate the joint usage of the process content of the two life cycle process standards. ISO/IEC/TR 24748 provides unified and consolidated guidance on the life cycle management of systems and software. Its purpose is to help ensure consistency in system concepts and life cycle concepts, models, stages, processes, process application, iteration and recursion of processes during the life cycle, key points of view, adaptation and use in various domains. ISO/IEC 24748-1 illustrates the use of a life cycle model for systems in the context of ISO/IEC 15288 and provides a corresponding illustration of the use of a life cycle model for software in the context of ISO/IEC 12207.

ISO/IEC 15026-4 gives the user the freedom to choose whether they use a specific artefact called an "assurance case" or document the assurance-related information in other documents. The point is to achieve the top-level claim and then to show the achievement of the claim for the value of a critical property for a relevant stakeholder. Life cycle processes, activities and tasks need to reflect both realizing an adequate system and being sure that the system is adequate by showing that achievement to the required confidence of the stakeholders.

Users of ISO/IEC 15026-4 may require risk assessment and risk management, measurement, and requirements processes that are more fully elaborated than the treatments provided in ISO/IEC 15288 and ISO/IEC 12207. Three International Standards, ISO/IEC 16085, *Risk management*, ISO/IEC 15939, *Measurement*, and ISO/IEC/IEEE 29148, *Requirements engineering*, are designed to be used with ISO/IEC 15288 and ISO/IEC 12207 to provide more detail for these three processes. Other standards that provide useful requirements and guidance for selected processes are ISO/IEC/IEEE 15289 for

documentation resulting from the execution of life cycle processes and ISO/IEC/IEEE 16326 for the project management process.

ISO/IEC 15026 is intended to be compatible with these life cycle process standards. The goals of assurance, the selection of claims to be assured, assurance-related planning, and the construction and maintenance of the assurance case have influences within all life cycle processes.

9.2 Assurance activities in the life cycle

The execution of a planned and systematic set of assurance activities is needed to provide grounds for confidence in system properties. These activities are designed to ensure that both processes and systems conform to their requirements, standards and guidance, and defined procedures[145]. "Processes" in this context, include all of the activities involved in the design, development, and sustainment of the system. For software, "software products" include the software itself, the data associated with it, its documentation, and supporting and reporting paperwork produced as part of the software process (e.g. test results and assurance arguments) as well as whatever else is needed to complete the assurance case. The "requirements" include requirements for the properties that should be exhibited, ultimately based on requirements to limit, reduce, or manage property-related costs and losses. The "standards and guidance" may be technical, defining the technologies that can be used in the system or software, or they may be non-technical, defining aspects of the process that are further delineated by the "procedures" that make satisfaction of the system's requirements possible.

Management of life cycle activities includes handling both the activities directly involving the assurance-related information and the effect that the assurance-related information has on other activities. This management is best performed when the top-level claims are considered from the beginning of concept development, used to influence all activities and systems[140] and Appendix B in [22], and became an integral part of the overall engineering process. These activities could all be done only if the system and the body of information showing achievement of those claims were being developed concurrently.

This parallel nature of development rationale and argument is but one of the advantages of concurrent development of the system and its assurance case. The development process and the system can be aimed not only at achieving the claim but doing so in a way that can be shown to be adequate by the assurance case. The assurance case influences the system by causing it to be developed in such a way that an argument is more practical to construct. This often results in a simpler system (at least internally), a system whose system elements can be used in isolation to show certain sub-claims, and an arrangement of system elements such that reasoning about the composition is both within the state of the art and practical. Concurrent processes can include requirements covering more conditions and events as well as adequate resilience, methods being used that produce few faults, and validation or verification being targeted to what needs to be shown and showing that adequately.

10 Summary

This International Standard has been written to provide users of all parts of ISO/IEC 15026 an adequate understanding of the concepts and terminology used in ISO/IEC 15026 that previously may not have been shared across the communities served. The explanations of what is covered in each part of ISO/IEC 15026 should provide a basis for selecting and using those parts as well as a rationale behind the organization of the ISO/IEC 15026 series of standards itself.

Bibliography

[1] Abran A., & Moore J.W. (Executive editors); Pierre Bourque, Robert Dupuis, Leonard Tripp (Editors). Guide to the Software Engineering Body of Knowledge. 2004 Edition. Los Alamitos, California: IEEE Computer Society, Feb. 16, 2004. Available at http://www.swebok.org

[2] Adamski A., & Westrum R. Requisite imagination: The fine art of anticipating what might go wrong." In: [55], p. 193-220, 2003

[3] Adelard. The Adelard Safety Case Development Manual. Available at http://www.adelard.com/web/hnav/resources/ascad

[4] Alexander I *Systems Engineering Isn't Just Software*. 2001. Available at http://easyweb.easynet.co.uk/~iany/consultancy/systems_engineering/se_isnt_just_sw.htm.

[5] Allen J.H., Barum S., Ellison R.J., McGraw G., Mead N.R. *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley, 2008

[6] Altman W., Ankrum T., Brach W. *Improving Quality and the Assurance of Quality in the Design and Construction of Nuclear Power Plants: A Report to Congress*. U.S. Nuclear Regulatory Commission: Office of Inspection and Enforcement, 1987

[7] Anderson J.P. *Computer Security Technology Planning Study Volume I*, ESDTR-73-51, Vol. I, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA 01730, Oct. 1972.

[8] Anderson R.J. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley and Sons, Second Edition, 2008

[9] Ankrum T.S., & Kromholz A.H. Structured Assurance Cases: Three Common Standards," Ninth IEEE International Symposium on High-Assurance Systems Engineering (HASE'05), pp. 99-108, 2005

[10] Armstrong J.M., & Paynter S.P. *The Deconstruction of Safety Arguments through Adversarial Counter-argument*. School of Computing Science, Newcastle University CS-TR-832, 2004

[11] Atchison B., Lindsay P., Tombs D. *A Case Study in Software Safety Assurance Using Formal Methods*. Technical Report No. 99-31. Sept. 1999

[12] ATSIN Number 17 Issued 9. Lapses and Mistakes. Air Traffic Services Information Notice, Safety Regulation Group, ATS Standards Department. UK Civil Aviation Authority, August 2002

[13] Bahill A.T., & Gissing B. Re-evaluating Systems Engineering Concepts Using Systems Thinking. *IEEE Trans. Syst. Man Cybern. C*. 1998 November, **28** (4) pp. 516–527

[14] Berg C.J. *High-Assurance Design: Architecting Secure and Reliable Enterprise Applications*. Addison Wesley, 2006

[15] Bernstein Lawrence, & Yuhas C. M. Trustworthy Systems through Quantitative Software Engineering. Wiley-IEEE Computer Society Press, 2005. About reliability not security

[16] Bishop M., & Engle S. *The Software Assurance CBK and University Curricula*. Proceedings of the 10th Colloquium for Information Systems Security Education, 2006

[17] Bishop M. *Computer Security: Art and Practice*. Addison-Wesley, 2003

[18] Bishop P., & Bloomfield R. *A Methodology for Safety Case Development*. Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-critical Systems Symposium, Birmingham. 1998

[19] Bishop P., & Bloomfield R. *The SHIP Safety Case Approach*. SafeComp95, Belgirate, Italy. Oct 1995

[20] Buehner M.J., & Cheng P.W. Causal Learning. In: *The Cambridge Handbook of Thinking and Reasoning*, (Morrison R., & Holyoak K.J. eds.). Cambridge University Press, 2005, pp. 143–68.

[21] Cannon J.C. *Privacy*. Addison Wesley, 2005

[22] CAP 670 Air Traffic Services Safety Requirements. UK Civil Aviation Authority Safety Regulation Group, 2012

[23] CAP 730 Safety Management Systems for Air Traffic Management A Guide to Implementation. UK Civil Aviation Authority Safety Regulation Group, 12 September 2002

[24] CAP 760 Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases For Aerodrome Operators and Air Traffic Service Providers, 10 December 2010

[25] Chung L. et al. *Non-Functional Requirements in Software Engineering*. Kluwer, 1999

[26] Clark D.D., & Wilson D.R. *A Comparison of Commercial and Military Computer Security Policies*, Proc. of the 1987 IEEE Symposium on Security and Privacy, IEEE, pp. 184-196, 1987

[27] CNSS. National Information Assurance Glossary, CNSS Instruction No. 4009, 26 April 2010. Available at http://www.cnss.gov/full-index.html

[28] Committee on Information Systems Trustworthiness. *Trust in Cyberspace, Computer Science and Telecommunications Board*. National Research Council, 1999

[29] Committee on National Security Systems (CNSS) Instruction 4009: National Information Assurance (IA) Glossary. Revised May 2003. Available at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[30] Common Criteria Recognition Arrangement (CCRA). Common Criteria v3.1 Revision 2. NIAP September 2007. Available at http://www.commoncriteriaportal.org.

[31] Common Weaknesses Enumeration. MITRE, 2012. Available at http://cwe.mitre.org

[32] Cooke N.J., Gorman J.C., Winner J.L. Team Cogitation. p. 239-268 In: [43]

[33] Courtois P.-J. *Justifying the Dependability of Computer-based Systems: With Applications in Nuclear Engineering*. Springer, 2008

[34] Cranor L., & Garfinkel S. *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly, 2005

[35] Dayton-Johnson. Jeff. Natural disasters and adaptive capacity. OECD Development Centre Research programme on: Market Access, Capacity Building and Competitiveness. Working Paper No. 237 DEV/DOC(2004)06, August 2004

[36] Department of Defense Directive 8500.1 (6 February 2003). Information Assurance (IA), Washington, DC: US Department of Defense, ASD(NII)/DoD CIO, April 23, 2007. Available at http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.

[37] Department of Defense Strategic Defense Initiative Organization. Trusted Software Development Methodology, SDI-S-SD-91-000007, vol. 1, 17 June 1992

[38] Department of Homeland Security National Cyber Security Division's "Build Security In" (BSI) web site, 2012, http://buildsecurityin.us-cert.gov

[39] Dependability Research Group. *Safety Cases*. University of Virginia, Available at: http://dependability.cs.virginia.edu/info/Safety_Cases

[40] Despotou G., & Kelly T. *Extending the Safety Case Concept to Address Dependability*, Proceedings of the 22nd International System Safety Conference, 2004

[41] Dowd M., McDonald J., Schuh J. *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*. Addison-Wesley, 2006

[42] Dunbar K., & Fugelsang J. Scientific Thinking and Reasoning. In: [59], p. 705–727

[43] Durso F.T., Nickerson R.S., Dumais S.T., Lewandowsky S., Perfect T.J. eds. *Handbook of Applied Cognition* 2nd edition . Wiley, 2007

[44] Ellsworth P.C. Legal Reasoning. In: [59], p. 685–704

[45] Ericsson K.A., Charness N., Feltovich P.J., Hoffman R.R. eds. *The Cambridge Handbook of Expertise and Expert Performance*. Cambridge University Press, 2006

[46] Fenton N., Littlewood B., Neil M., Strigini L., Sutcliffe A., Wright D. Assessing dependability of safety critical systems using diverse evidence. *IEE Proc. Softw.* 1998 **145** (1) pp. 35–39

[47] Gasser M. Building a Secure Computer System. Van Nostrand Reinhold, 1988. Available at http://deke.ruc.edu.cn/wshi/readings/cs02.pdf

[48] Gray J.W. *Probabilistic Interference*. Proceedings of the IEEE Symposium on Research in Security and Privacy. IEEE, p. 170-179, 1990

[49] Greenwell W., Strunk E., Knight J. *Failure Analysis and the Safety-Case Lifecycle*. IFIP Working Conference on Human Error, Safety and System Development (HESSD) Toulouse, France. Aug 2004

[50] Greenwell W.S., Knight J.C., Pease J.J. *A Taxonomy of Fallacies in System Safety Arguments*. 24th International System Safety Conference, Albuquerque, NM, August 2006

[51] Hall A., & Chapman R. Correctness by Construction: Developing a Commercial Secure System. *IEEE Softw.* 2002 Jan/Feb, **19** (1) pp. 18–25

[52] Herrmann D.S. *Software Safety and Reliability*. IEEE Computer Society Press, 1999

[53] Hoglund G., & McGraw G. *Exploiting Software: How to break code*. Addison-Wesley, 2004

[54] Hollnagel E., Woods D.D., Leveson N. eds. *Resilience Engineering: Concepts and Precepts*. Ashgate Pub Co, 2006

[55] Hollnagel E. ed. *Handbook of cognitive task design*. Lawrence Erlbaum Associates, 2003

[56] Hollnagel E. Human Error: Trick or Treat?. In: [43], p. 219–238

[57] Hollnagel E. *Barriers and Accident Prevention*. Ashgate, 2004

[58] Hollnagel E. Human Factors: From Liability to Asset. Presentation, 2007. Available at www.vtt.fi/liitetiedostot/muut/Hollnagel.pdf

[59] Holyoak K.J., & Morrison R.G. eds. *The Cambridge Handbook of Thinking and Reasoning*. Cambridge University Press, 2005

[60] Howard M., & LeBlanc D.C. *Writing Secure Code*. Microsoft Press, Second Edition, 2002

[61] Howard M., & Lipner S. *The Security Development Lifecycle*. Microsoft Press, 2006

[62] Howell C. Assurance Cases for Security Workshop (follow-on workshop of the 2004 Symposium on Dependable Systems and Networks), June, 2005

[63] IEC 60050-191, *International Electrotechnical Vocabulary, Chapter 191: Dependability and Quality of Service*

[64] IEC 60300*Dependability management [several parts]*

[65] IEC 60300-3-15 ed1.0 (2009-06) Dependability management - Part 3-15 – Application guide - Engineering of system dependability

[66] IEC 60300-3-2 ed.2.0 (2004-11), *Dependability management – Part 3-2: Application guide - Collection of dependability data from the field*

[67] IEC 60812 ed2.0 (2006-01), *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*

[68] IEC 61025 ed2.0 (2006-12), *Fault tree analysis (FTA)*

[69] IEC 61078 ed2.0 (2006-01), *Analysis techniques for dependability - Reliability block diagram and Boolean methods*

[70] IEC 61508 ed2.0, *Functional safety of electrical/electronic/programmable electronic safety-related systems* [several parts]

[71] IEC 61508-7 ed2.0 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

[72] IEC 61511 ed1.0, *Functional safety - Safety instrumented systems for the process industry sector* [several parts]

[73] IEC 61882 ed1.0 (2001-05), *Hazard and operability studies (HAZOP studies) - Application guide*

[74] IEC CD 62741 ed.1.0, *Reliability of systems, equipment, and components. Guide to the demonstration of dependability requirements. The dependability case*

[75] STD IEEE 1228-1994, *IEEE Standard for Software Safety Plans*

[76] INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING INCOSE. Guide to Systems Engineering Body of Knowledge (G2SEBoK). Available at http://g2sebok.incose.org/

[77] ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

[78] ISO 13849, *Safety of machinery — Safety-related parts of control systems* [three parts]

[79] ISO 14620, *Space systems — Safety requirements* [three parts]

[80] ISO 14625:2007, *Space systems — Ground support equipment for use at launch, landing or retrieval sites — General requirements*

[81] ISO 19706:2011, *Guidelines for assessing the fire threat to people*

[82] ISO 20282, *Ease of operation of everyday products* [four parts]

[83] ISO 2394:1998, *General principles on reliability for structures*

[84] ISO 28003:2007, *Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems*

[85] ISO 9241-400:2007, *Ergonomics of human — system interaction — Part 400: Principles and requirements for physical input devices*

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

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

[88] ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security* [three parts]

[89] ISO/IEC TR 15443, *Information technology — Security techniques — Security assurance framework* [two parts]

[90] ISO/IEC 15939:2007, *Systems and software engineering — Measurement process*