BS ISO/IEC 15026-3:2015

BSI Standards Publication

Systems and software engineering — Systems and software assurance

Part 3: System integrity levels

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO/IEC 15026-3:2015. It supersedes BS ISO/IEC 15026-3:2011 which is withdrawn.

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

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

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

Published by BSI Standards Limited 2015

ISBN 978 0 580 84227 6

ICS 35.080

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2015.

Amendments/corrigenda issued since publication

Date	Text affected

BS ISO/IEC 15026-3:2015

INTERNATIONAL STANDARD

ISO/IEC 15026-3

Second edition
2015-12-01

Systems and software engineering — Systems and software assurance —

Part 3: System integrity levels

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

Partie 3: Niveaux d'intégrité du système

Reference number
ISO/IEC 15026-3:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

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

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

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information Technology*, Subcommittee SC 7, *Software and systems engineering*.

This second edition cancels and replaces the first edition (ISO/IEC 15026-3:2011), 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 ISO/IEC 15026 series.

INTERNATIONAL STANDARD **ISO/IEC 15026-3:2015(E)**

Systems and software engineering — Systems and software assurance —

Part 3: System integrity levels

1 Scope

This part of ISO/IEC 15026 specifies the concept of integrity levels with corresponding integrity level requirements that are required to be met in order to show the achievement of the integrity level. It places requirements on and recommends methods for defining and using integrity levels and their corresponding integrity level requirements. It covers systems, software products, and their elements, as well as relevant external dependences.

This part of ISO/IEC 15026 is applicable to systems and software and is intended for use by the following:

a) definers of integrity levels such as industry and professional organizations, standards organizations, and government agencies;

b) users of integrity levels such as developers and maintainers, suppliers and acquirers, system or software users, assessors of systems or software and administrative and technical support staff of systems and/or software products.

One important use of integrity levels is by suppliers and acquirers in agreements; for example, to aid in assuring safety, financial, or security characteristics of a delivered system or product.

This part of ISO/IEC 15026 does not prescribe a specific set of integrity levels or their integrity level requirements. In addition, it does not prescribe the way in which integrity level use is integrated with the overall system or software engineering life cycle processes. It does, however, provide an example of use of this part of ISO/IEC 15026 in Annex A.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC/IEEE 12207, *Systems and software engineering — Software life cycle processes*

ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*

3 Terms and definitions

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

3.1
adverse consequence
consequence (3.3) that results in a specified level of loss

Note 1 to entry: An adverse consequence results from the *system-of-interest* (3.23) being in a *dangerous condition* (3.4) combined with the environment of the *system* (3.21) being in its worst-case state (relative to the adverse consequence).

Note 2 to entry: Harm in ISO Guide 51 is an instance of an adverse consequence. The concept of adverse consequences is introduced in order to cover not only harm in the safety context but also other losses such as loss of assets in the security context.

3.2
claim
proposition representing a requirement of the *system-of-interest* (3.23) that enables the system-of-interest to achieve *tolerable risk* (3.25) if it were met

Note 1 to entry: A claim is consistent with claims in the other parts of ISO/IEC 15026 series but issues of claims here are restricted to achievement of a tolerable risk.

Note 2 to entry: A safety goal required in ISO 26262 is an instance of a claim.

3.3
consequence
outcome of an event affecting objectives

[SOURCE: ISO Guide 73:2009, 3.5.1.3]

3.4
dangerous condition
state of a *system* (3.21) which, in combination with some states of the environment, will result in *adverse consequence* (3.1)

Note 1 to entry: A hazardous situation in ISO/IEC Guide 51 and IEC 61508–4 is an instance of a dangerous condition. A concept of dangerous conditions is introduced in order to cover not only hazardous situations in the safety context but also errors in the reliability, integrity, confidentiality, or dependability contexts and other states of a system which can lead to adverse consequences.

Note 2 to entry: Occurrences of failures in the context of reliability or as defined in IEC 61508–4 often, but not always, lead to dangerous conditions.

Note 3 to entry: A dangerous condition therefore has attributes, at least, a) the associated adverse consequences, b) the trigger events that lead to the dangerous condition, and c) the trigger events that lead to the adverse consequences from the dangerous condition.

3.5
design authority
person or organization that is responsible for the design of the product

[SOURCE: ISO/IEC 15026–1]

3.6
initial risk
estimated *risk* (3.16) before applying *risk reduction measures* (3.18)

3.7
integrity level
required degree of confidence that the *system-of-interest* (3.23) meets the associated *integrity level claim* (3.10)

Note 1 to entry: The words “integrity level” forms an indivisible label. This International Standard does not pronounce on, nor depend on, a concept of integrity by itself.

Note 2 to entry: An integrity level is different from the *likelihood* (3.13) that the integrity level claim is met but they are closely related.

Note 3 to entry: The word “confidence” implies that the definition of integrity levels can be a subjective concept.

Note 4 to entry: In this part of ISO/IEC 15026, integrity levels are defined in terms of risk and hence, cover safety, security, financial and any other dimension of risk that is relevant to the system-of-interest.

3.8
integrity level assurance authority
independent person or organization responsible for certifying compliance with the *integrity level requirements* (3.11)

[SOURCE: ISO/IEC 15026–1]

3.9
integrity level definition authority
person or organization responsible for defining *integrity levels* (3.7) and *integrity level requirements* (3.11)

3.10
integrity level claim
claim (3.2) representing a requirement for a *risk reduction measure* (3.18) identified in the *risk treatment* (3.20) process of the *system-of-interest* (3.23)

Note 1 to entry: In general, it is described in terms of requirements that, when met, would avoid, control or mitigate the *consequences* (3.3) of *dangerous conditions* (3.4) and provide *tolerable risk* (3.25).

Note 2 to entry: The claim that can be regarded as an integrity level claim in IEC 61508 is that an E/E/PE safety-related system satisfactorily performs the specified safety functions under all the stated conditions.

3.11
integrity level requirement
set of requirements that, when met, will provide a level of confidence in the associated *integrity level claim* (3.10) commensurate with the associated *integrity level* (3.7)

3.12
level of risk
magnitude of a *risk* (3.16) or combination of risks, expressed in terms of the combination of *consequences* (3.3) and their *likelihood* (3.13)

[SOURCE: ISO Guide 73:2009, 3.6.1.8]

3.13
likelihood
probability of something happening

3.14
property-of-interest
any property that, if lost, is considered a negative effect

Note 1 to entry: The concept of property-of-interest is introduced in order to characterize negative effects of *consequences* (3.3).

Note 2 to entry: In the safety context, human lives and health are instances of properties-of-interest.

Note 3 to entry: Assets in the security context, e.g. defined in ISO/IEC 15408-1, are instances of properties-of-interest.

3.15
residual risk
risk (3.16) remaining after *risk treatment* (3.20)

[SOURCE: ISO Guide 73:2009, 3.8.1.6]

3.16
risk
effect of uncertainty on objectives

[SOURCE: ISO Guide 73:2009, 1.1]

Note 1 to entry: An effect is a deviation from the expected: positive and/or negative. In this International Standard, the focus is on negative deviations leading to *adverse consequences* (3.1).

Note 2 to entry: Risk is often characterized by reference to potential events and *consequences* (3.3), or a combination of them.

Note 3 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated *likelihood* (3.13) of occurrence. In this International Standard, risk is characterized as the combination of the severity of the adverse consequence and the likelihood of an adverse consequence occurring.

Note 4 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

3.17
risk criteria
terms of reference against which the significance of a *risk* (3.16) is evaluated

[SOURCE: ISO Guide 73:2009, 3.3.1.3]

3.18
risk reduction measure
steps taken to reduce or mitigate *risk* (3.16)

Note 1 to entry: A typical risk reduction measure is a safety-related system in IEC 61508 series.

3.19
risk source
element that, alone or in combination, has the intrinsic potential to give rise to *risk* (3.16)

[SOURCE: ISO Guide 73:2009, 3.5.1.2]

Note 1 to entry: A hazard in ISO Guide 73:2009 is an instance of a risk source.

Note 2 to entry: A fault, an error, or a failure in the context of reliability can be a risk source. The definitions of those terms can be found in IEC 61508–4.

Note 3 to entry: A threat in the context of security, a *threat agent* (3.24), and an adverse action defined in ISO/IEC 15408-1 can be a risk source.

3.20
risk treatment
process to eliminate *risk* (3.16) or reduce it to a tolerable level

[SOURCE: ISO Guide 73:2009, 3.8.1, modified]

3.21
system
combination of interacting elements organized to achieve one or more stated purposes

[SOURCE: ISO/IEC/IEEE 15288]

3.22
system element
member of a set of elements that constitutes a *system* (3.21)

[SOURCE: ISO/IEC/IEEE 15288]

3.23
system-of-interest
system (3.21) whose life cycle is under consideration in the context of ISO 15026

[SOURCE: ISO/IEC/IEEE 15288]

3.24
threat agent
entity that can adversely act on *property-of-interest* (3.14)

[SOURCE: ISO/IEC 15408-1:2009, 3.1.71, modified]

3.25
tolerable risk
level of risk (3.12) that is accepted in a given context based on the current values of society

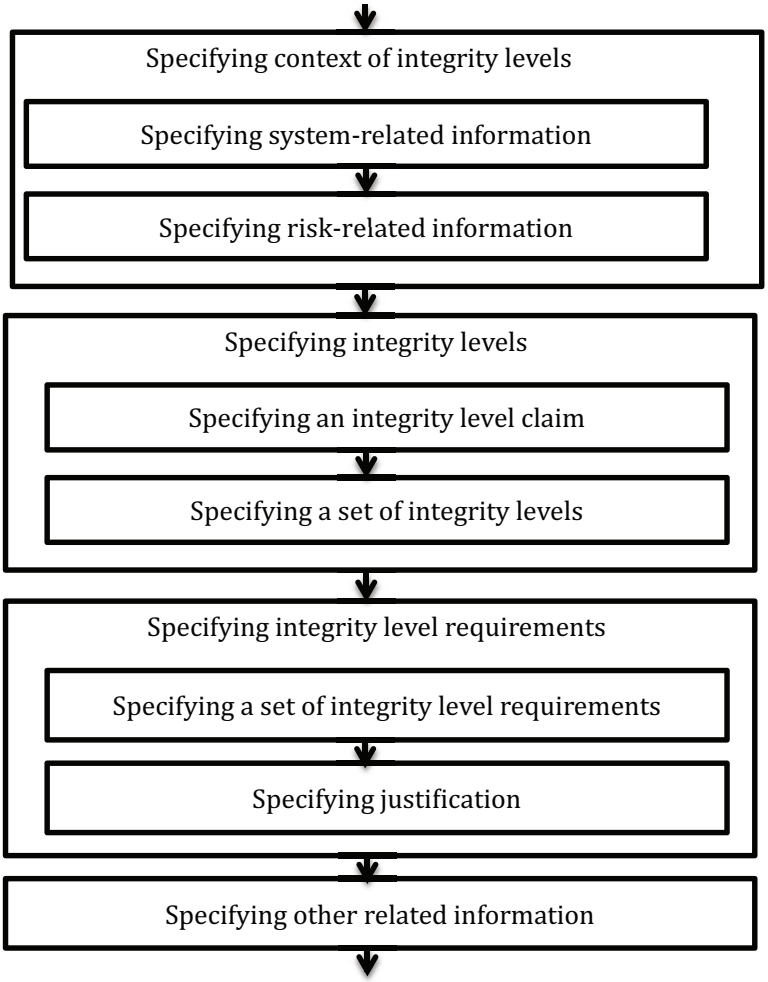
[SOURCE: ISO/IEC Guide 51:2014, 3.15]

Note 1 to entry: A tolerable risk is sometimes called acceptable risk, e.g. ISO/IEC/IEEE 16085, and ISO 14971. The general risk management standards ISO Guide 73 and ISO 31000 use both phrases without explicit definitions.

4 Defining integrity levels

4.1 Expected readers of this Clause

This Clause explains the process of defining a set of integrity levels for a specific system domain and general requirements for related-products, such as integrity levels, integrity level claims, and integrity level requirements. Thus, the expected readers of this Clause are organizations which develop specifications defining a set of integrity levels. Those organizations, which are called integrity level definition authorities, include international or domestic standardization organizations, any other standardization organizations, arbitrary industry organizations, or a department in an organization which is responsible for the organization's policy or standard for contract management. Figure 1 shows the overview of the process of defining integrity levels.



Key

↓ flow of processes

NOTE Iteration of processes is not shown for simplicity.

Figure 1 — Overview of the process of defining integrity level

4.2 Appropriate area to define integrity levels

Not all areas are suitable for definition and use of integrity levels. Integrity levels shall be defined for an area only if a substantial body of relevant experience exists for the area that is well understood by those performing the definition. Integrity levels can be used for areas where levels of risks (e.g. high, medium, low risk) can be clearly defined. Each level of risk provides a basis for a different required degree of confidence that the integrity level claim is met.

NOTE When dealing with risks of a system in an area where a substantial body of relevant experience does not exist, then the use of an assurance case is appropriate.

4.3 Specifying context of integrity levels

4.3.1 Specifying system-related information

The following information about systems in the target area shall be specified by the integrity level definition authority in order to clarify the scope of applicability of the integrity levels being specified:

a) definition of the target class of systems;

b) assumptions on the environment.

NOTE Examples of a definition of a target class of systems can be found in IEC 61508 and ISO 26262. The definition of target classes of systems of IEC 61508 and ISO 26262 pertain to "electrical/electronic/programmable electronic (E/E/PE) systems are used to carry out safety functions" and "safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg", respectively.

4.3.2 Specifying risk-related information

The following information about risks related to systems in the target area shall be specified by the integrity level definition authority in order to clarify the scope of applicability of the integrity levels being specified:

a) property-of-interest;

b) possible adverse consequences;

c) possible dangerous conditions and the states of the environment that together with the dangerous condition will result in an adverse consequence;

d) risk criteria;

e) tolerable risks;

f) assumptions on the structure of risk reduction measures.

Information about properties-of-interest gives a definition of negative effects. An adverse consequence can have the following attributes but is not restricted to:

— description of the event that leads to the consequence;

— likelihood of the occurrence of the event;

— severity of the consequence;

— controllability of the event;

— exposure (time) to the event.

Dangerous conditions can be classified by the type of events that leads to the condition. The following event types should be taken into account:

a) random failures;

b) systematic failures;

c) failures caused by interactions between system elements without any faults of those system elements;

d) failures caused by interactions between elements of the environment and the system (for example, failures caused by a threat agent).

Likelihood of a dangerous condition should also be considered.

A risk criterion specifies the meaning or method of measurement of system-related risks and is used to specify the tolerable risk. A risk criterion shall be consistent with governing requirements such as legal, regulatory, or contractual requirements, which can be bases for the tolerable risk. Prior to specifying risk criteria, the categories for which risks will be evaluated are defined. These may include human health and safety, environmental protection, legal and regulatory compliance, security, cost, project schedule, reputation, and performance. A scale of severity and likelihood is defined for the applicable categories. Stakeholders usually cooperate and agree on risk criteria.

Risk reduction measures include not only parts of a system used to mitigate risks, e.g. an inherent safety by design, and safety-related or security-related functions, but also organizational supports or social frameworks to treat risks, e.g. a contingency plan for operators, warnings in user's manuals, and safety-related or security-related standards or regulations for manufacturers. A structure of risk reduction measures should be assumed in order to clarify which parts is the responsibility of the target class of systems. A typical structure is a multi-layered protection structure for safety. Assumptions on the structure of risk reduction measure are characterized by the following criteria:

— multi-layered structure to mitigate risks, over the environments and the target systems;

— parts of a system, which relates to risk reduction measures, including parts that might not be defined or recognized independently;

— risk reduction measures which contain human elements;

— detectability of loss of the function of risk reduction measure;

— frequency of demand to perform a risk reduction measure.

NOTE 1 IEC 61508 series assumes that a safety-related system can be recognized independently.

NOTE 2 ISO 26262 series assumes that a driver plays a part of the safety-related mechanism and includes aspects such as controllability of an event.

NOTE 3 IEC 61508 series gives three sets of integrity levels accordingly, each of which corresponds to a demand mode to perform the functional safety mechanism.

4.4 Specifying integrity levels

Figure 2 depicts the relation among key concepts in this part of ISO 15026. The goal of the framework of integrity levels is to achieve tolerable risk relative to the system-of-interest and its environment. An integrity level claim is a requirement on a risk reduction measure identified in the risk treatment process of the system of interest. The integrity level claims, when satisfied, shall eliminate, avoid, control, or mitigate any dangerous conditions of the system of interest. The dangerous conditions in combination with specific states of the environment result in adverse conditions. The risk treatment process shall result in tolerable risk, where risk is characterized by its adverse consequence, which has attributes of severity and likelihood.

The integrity level is the degree of confidence to which the system of interest meets its integrity level claims. Integrity level requirements are those requirements that when satisfied will provide the necessary degree of confidence.

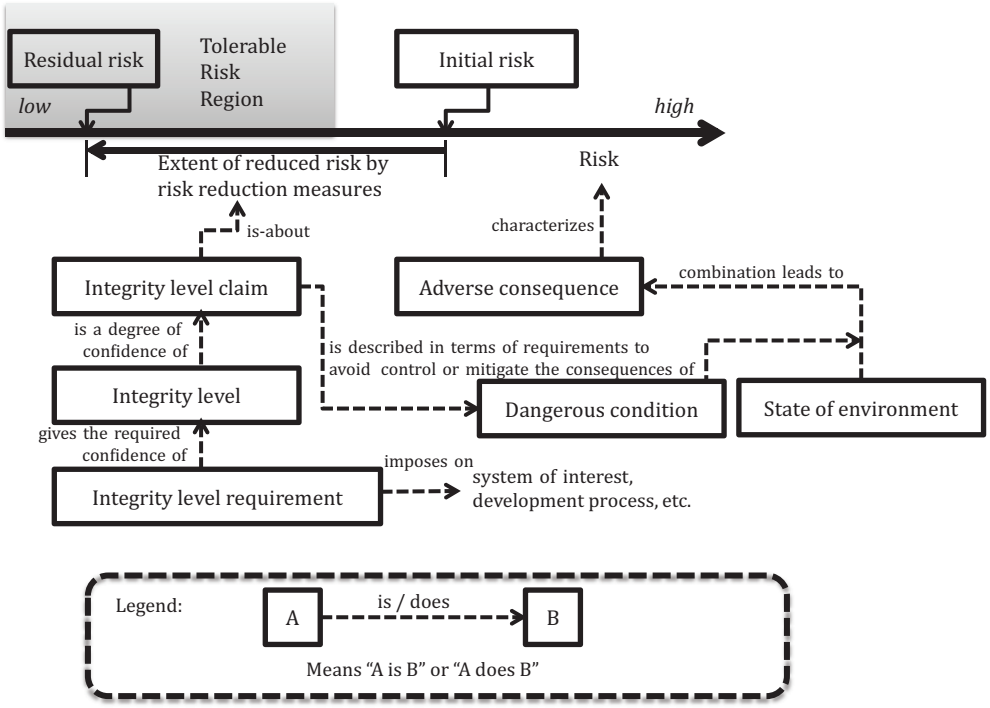


Figure 2 — Relations among key concepts in this part of ISO 15026

4.4.1 Specifying an integrity level claim

An integrity level claim is a statement about a property of a system such that if the claim is true, then tolerable risk is achieved. An integrity level claim shall be a statement satisfying the following conditions:

a) statement shall be a proposition on a system in the target class of systems and on their risk related issues;

b) any assumptions on the environment or the conditions of a system that are prerequisite to the integrity level claim being valid shall be stated.

Achieving tolerable risks is executed during the risk treatment process. As means of risk treatment can have several different options, claims can vary according to those means. The concept of a dangerous condition is introduced to capture potential situations that lead to adverse consequence and also to consider means to eliminate or avoid adverse consequence. Therefore, integrity level claims are typically defined in terms of dangerous conditions, as follows:

— claim stating to control a dangerous condition;

— claim stating to avoid a dangerous condition;

— combination of the statements above.

Another type of integrity level claim can be considered for other risk reduction measures, including dealing with risk sources and adverse consequences, as follows:

a) claim stating to remove risk sources;

b) claim stating to mitigate the adverse consequences;

c) combination of the statements above.

For defining a set of integrity levels, precise claims are not necessary. For example, a claim may just state that an assumed risk reduction measure performs in an expected way.

NOTE 1 Typical options of risk treatment can be found in ISO 31000.

NOTE 2 A claim can be a statement of an arbitrary combination of the risk treatment options above.

NOTE 3 The predicate that can be regarded as an integrity level claim in IEC 61508 is one regarding an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions.

NOTE 4 An example of the last type above is the corresponding proposition in ISO 26262 that a safety-goal, which is defined for each hazard of an item, is satisfied.

4.4.2 Specifying a set of integrity levels

An integrity level is assigned to a system-of-interest or a system element, and corresponds to the worst-case risk associated with the system. Integrity levels are usually expressed as a set of levels, for example, 1, 2, and 3 or a, b, and c. The integrity level of a system should be determined based on the worst risk in all the categories of risk associated with the system. The set of integrity levels shall satisfy the following requirements:

a) each integrity level in a set of integrity levels shall have a unique identifier;

b) integrity levels shall be determined based on the following:

   1) level of the worst-case risk associated with the system of interest;

   2) required likelihood that the integrity level claims are met necessary to achieve tolerable risk (taking into account the likelihood that the environment is in a state pre-requisite to the dangerous condition resulting in an adverse consequence);

c) set of integrity levels shall be given as graded degrees of the likelihood.

Likelihood that an integrity level claim is satisfied should be expressed in terms of "reliability of mitigating function" or "limit on rate of dangerous condition".

NOTE 1 A typical expression of likelihood is a range of probability.

NOTE 2 IEC 61508 uses the terms "probability of a dangerous failure on demand of the safety function" and "frequency of a dangerous failure of the safety function".

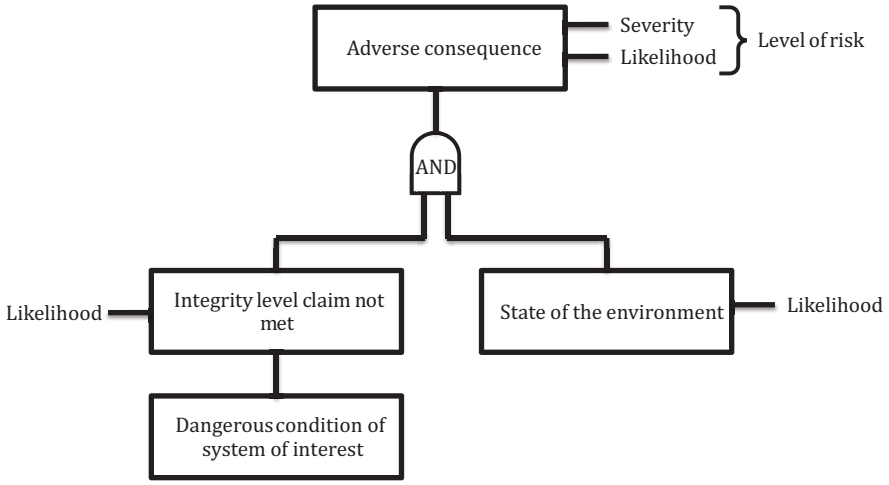


Figure 3 — Relationship between adverse consequence, state of the environment and integrity level claim (informative)

4.5 Specifying integrity level requirements

4.5.1 Specifying a set of integrity level requirements

A set of integrity level requirements is associated with a set of integrity levels and defined as those requirements that provide appropriate level of confidence that the integrity level claim is met. A set of integrity level requirements shall satisfy the following attributes:

a) each integrity level requirement defines the required evidence necessary to show that the requirement is satisfied;

b) each integrity level requirement is defined such that compliance with the requirement can be demonstrated objectively.

Typical integrity level requirements include the following:

— requirements on the necessary quality attributes of the requirements and design specification documents obtained from the technical processes in ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207;

— requirements on the necessary test coverage criteria for testing;

— requirements on the specific analyses to be performed on a system and its elements;

— requirements related to providing quantitative data;

— requirements on system life cycle processes;

— requirements on specific system development process models;

— requirements on specific methodologies to be used in development processes;

— requirements on specific tools to be used in system development processes;

— requirements on evidence to be used to support claims based on usage history.

4.5.2 Specifying the justification between integrity levels and their integrity level requirements

The documented justification of the adequacy of each set of integrity level requirements is a subjective decision made by the integrity level definition authority. The necessary level of confidence and the set of integrity level requirements that provide that level of confidence will depend on the risk class that was used to define the integrity levels.

4.6 Specifying integrity level determination process

The integrity level definition authority shall define a process guideline for the determination of a system integrity level, system element integrity levels, and achievement of required integrity levels in accordance with Clause 6, Clause 7, and Clause 9. The process guideline shall contain the following aspects:

a) process for determining system integrity levels;

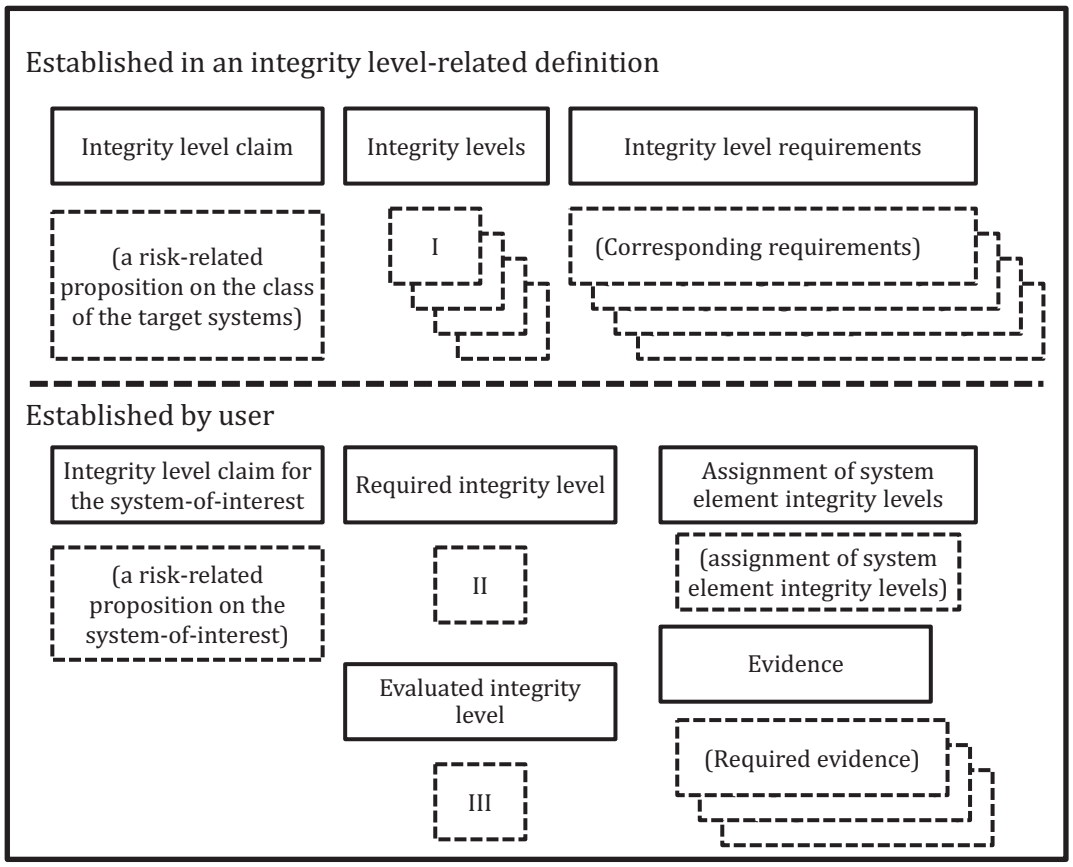
b) process for assigning integrity levels to system elements, including definition of the pre-requisite conditions for allowing a system element to have a lower integrity level than the system integrity level;

c) processes for maintaining integrity levels during the design change process for the system.

5 Using integrity levels

5.1 Expected readers of this clause

The framework of integrity levels is used to share common understandings of risks of systems among related stakeholders, especially between manufacturers and users of the system. Manufacturers can include development branches in an organization, system-integrators, and vendors. Usually, those manufacturers have a role in the determination of the required integrity level and the preparation evidence demonstrating compliance with the integrity level requirements. The role of those manufacturers is called the design authority. The users also vary according to the characteristics of the target class of systems. Agreement that tolerable risk has been achieved is often based on the result of a certification by some third party organization. In this part of ISO 15026, such third party person or organization is called an integrity level assurance authority, which is expected to approve the design of the system based on the objective evidence produced to demonstrate compliance with the integrity level requirements.



NOTE Solid lined square represents a class of products while a dashed line square represents an instance of a product.

Figure 4 — Integrity level related-products with their responsible person or organizations (informative)

Figure 4 shows the list of integrity level related products where the products in the top half of the figure will be provided by the integrity level definition authority and the products in the bottom half will be established by a user of the set of integrity levels.

5.2 Purpose for using integrity levels

The use of integrity levels contributes to providing grounds for stakeholder confidence and support for their decision-making. An integrity level also provides a common language to share understandings of risks in a system-of-interest among several stakeholders.

5.3 Outcomes of using integrity levels

The following are results of the successful usage of integrity levels:

a) sufficient integrity level claims that achieve tolerable risk for the system are defined;

b) integrity level requirements are defined to guide project planning, and provide an agreement between the design authority and the integrity assurance authority on the acceptance criteria for the system;

c) system elements with lower integrity levels than the system integrity level are identified, their integrity levels are defined, and the architectural features of the system that justifies that their lower integrity level are documented at a sufficient level of detail to justify that the lower integrity level elements cannot prevent or impede performance of higher integrity level elements;

d) objective evidence providing adequate confidence that the integrity level claims were satisfied with the necessary level of confidence are produced.

6 System integrity level determination

6.1 General

Determination of the system integrity level is typically done early in the development lifecycle of a system since the integrity level requirements need to be input to the project planning process. Integrity level determination should be done as part of the process to define stakeholder requirements.

A system integrity level is a required integrity level for the whole of the system-of-interest. A system integrity level is determined based on information from outcomes of the risk management process. The system integrity level determination process is given as a process view of the risk management process. To determine a system integrity level, information about the system-of-interest is required to determine dangerous conditions.

NOTE 1 Detailed descriptions of the risk management process can be found in ISO/IEC/IEEE 15288, ISO/IEC/IEEE 12207, ISO/IEC/IEEE 16085, and ISO 31000. Although some terminologies are different among those International Standards, their basic ideas are the same.

NOTE 2 Detailed description of the defining stakeholder needs and requirements definition process and the project planning process can be found in ISO/IEC/IEEE 15288.

Figure 5 shows the example processes that relate integrity-level-related processes, including determination of a system integrity level, assignment of system element integrity levels, and meeting integrity level requirements.

6.2 Purpose of the system integrity level determination process

The purpose of the system integrity level determination process is to establish the integrity level of the system consistent with achieving tolerable risk and to share an understanding of these risks among related-stakeholders.

6.3 Outcome of the system integrity level determination process

The following are the results of successful implementation of the system integrity level determination process:

a) stakeholders who need to share an understanding of risk are identified;

b) standard which defines the set of integrity levels used is identified;

c) risk profile is obtained as a result of a preliminary risk assessment processes, including information on each risk containing at least the tolerable risk, potential adverse consequences, dangerous conditions, risk sources, and the residual risk;

d) integrity level claims are identified;

e) required system integrity level is determined and agreed among the related-stakeholders;

f) integrity level requirements associated with the required system integrity level are identified.

The risk profile is obtained by at least one cycle of the set of the risk assessment processes, i.e. risk identification process, risk analysis process and risk evaluation process. After obtaining the first version of the risk profile, a required system integrity level can be determined from the required extent of risk reduction from the estimated risk to achieve the tolerable risk.

6.4 Activities of the system integrity level determination process

The system integrity level determination process can be implemented by applying the following processes in ISO/IEC/IEEE 15288. Activities shown below each process are derived from ISO/IEC/IEEE 15288 but are specific to determination of system integrity levels.

a) Stakeholder Needs & Requirement Definition Process provides for the following activities:

   1) identify stakeholders who need to share an understanding of the risks of the system-of-interest;

   2) give a definition of the system-of-interest;

   3) determine a standard in which a set of integrity levels is defined;

   4) define the integrity level claim in accordance with the stakeholder requirements of the system-of-interest.

b) System Requirements Definition Process, with invocations of Risk Management Process, provides for the following activities:

   1) determine risk criteria and the tolerable risk of the system-of-interest;

   2) analyse risks of the system-of-interest and record the result to the risk profile;

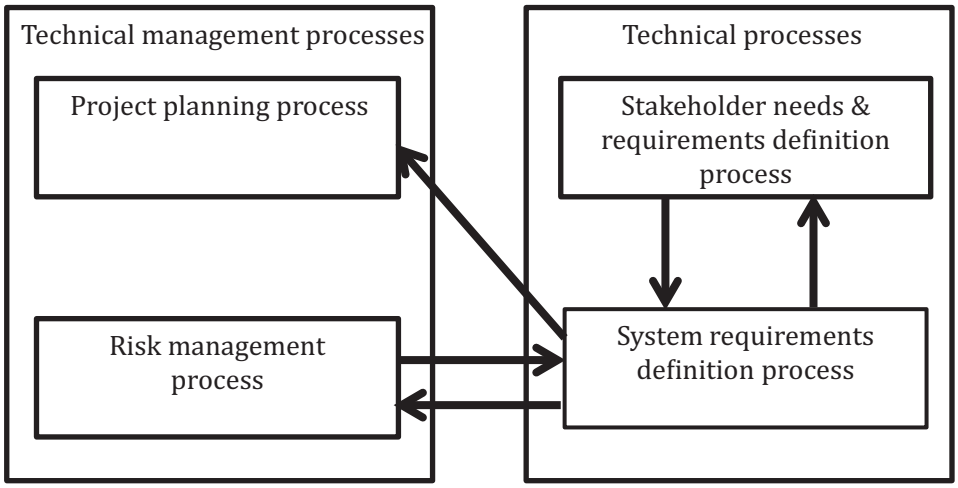
   3) give a structure of the risk reduction measures, including the one implemented by the system-of-interest;

   4) evaluate risks and record the result to the risk profile;

   5) determine the required system integrity level;

   6) specify integrity level requirements associated with the required system integrity level in accordance with the system requirements of the system-of-interest.

The definition of the system-of-interest should be given from the view that the system-of-interest is a part of the overall structure of risk reduction measures. In the above activities, it is not mentioned explicitly but each work product should be agreed on among related stakeholders identified in 1) of a). The required system integrity level can be used by the Project Planning Processes.



Key

flow of processes

Figure 5 — Related processes in ISO/IEC/IEEE 15288 to the system integrity level determination process (informative)

7 Assigning system element integrity levels

7.1 Purpose of the assigning system element integrity levels process

The purpose of the assigning system element integrity level process is to assign an integrity level to a system element consistent with the extent of risk reduction the element contributes within the system.

7.2 Outcome of the assigning system element integrity levels process

The outcome of the assigning system element integrity levels process shall include the following items:

a) set of system elements is identified;

b) for each system element, the related stakeholders are identified and all agree that all related stakeholders are identified;

c) for each system element, the required integrity level for the system element is determined and agreed among the related stakeholders.

7.3 Activities of the assigning system element integrity levels process

The assigning system element integrity levels process can be implemented by applying the Architecture Definition process in ISO/IEC/IEEE 15288 with invocations of the Risk Management process. The following activities are derived from ISO/IEC/IEEE 15288 but are specific to the assignment of system element integrity levels:

a) identify system elements from the view of risk reduction measures;

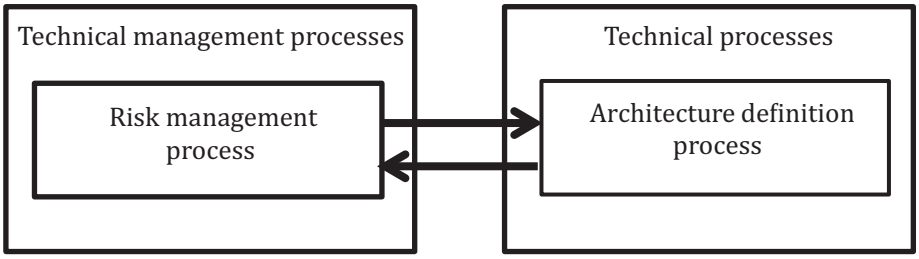
b) for each system element, identify and agree upon related stakeholders;

c) give definitions of the system elements and clarify dependency relations among them from the view of risk reduction measures in accordance with the architectural design of the system-of-interest;

d) determine for each system element a system element integrity level in accordance with the dependency relations;

e) identify for each system element integrity level requirements for the system element based on the system integrity level.

Although in general there are several possibilities to consider how to partition a system into system elements, the identification of the system elements should be based on the view that the system-of-interest is a part of the overall structure of the risk reduction measures.



Key

flow of processes

Figure 6 — Related processes in ISO/IEC/IEEE 15288 to the system element integrity level determination process (informative)

8 Meeting integrity level requirements

8.1 General

Meeting integrity level requirements is a process to make sure that integrity level requirements associated with the determined system integrity level and assigned system element integrity levels are satisfied. The process is based on a collection of evidence that is obtained during technical processes in system and software lifecycle processes. Typical evidence includes review, analysis, and test results obtained during the verification process. Confirming that the required level of risk is achieved can be regarded as a part of the activities in the validation process. The process of meeting integrity level requirements is a part of the validation process.

8.2 Purpose of meeting integrity level requirements

The purpose of the meeting integrity level requirements process is to reach agreement among related stakeholders that the residual risk of the implementation of the system-of-interest is evaluated within tolerable risk.

8.3 Outcome of meeting integrity level requirements

The following are results of meeting the integrity level requirements:

a) objective evidence upon which to base the required level of confidence that the integrity level claims are correct and complete is produced;

b) objective evidence upon which to base the required level of confidence that the integrity level claims are met is produced;

c) among the related stakeholders, especially between the design authority and the integrity level assurance authority, agreement that the required integrity level is achieved.

An assurance case that shows the relation between the data prepared for meeting integrity level requirements and the associated integrity level claim could also be given to share common understanding of risks of the system-of-interest among related stakeholders.

8.4 Activities of meeting integrity level requirements

The meeting integrity level requirements process can be implemented by applying the following processes in ISO/IEC/IEEE 15288. Activities shown below the processes are derived from ISO/IEC/IEEE 15288 but are specific to meeting of integrity level requirements.

a) Design Definition Process, System Analysis Process, Implementation Process, Integration Process, Transition Process, Operation Process and Maintenance Process, with invocations of Risk Management Process, providing the following activities:

   1) for each system element, collect objective evidence that is needed to demonstrate compliance with the integrity level requirements associated with the integrity level for that system element;

   2) collect objective evidence that is needed to demonstrate compliance with the integrity level requirements associated with the system integrity level.

b) Verification Process providing the following activities:

   1) for each system element, collect objective evidence that demonstrates compliance with the integrity level requirements associated with the integrity level for that system element;

   2) collect objective evidence that is needed to demonstrate compliance with the integrity level requirements associated with the system integrity level;

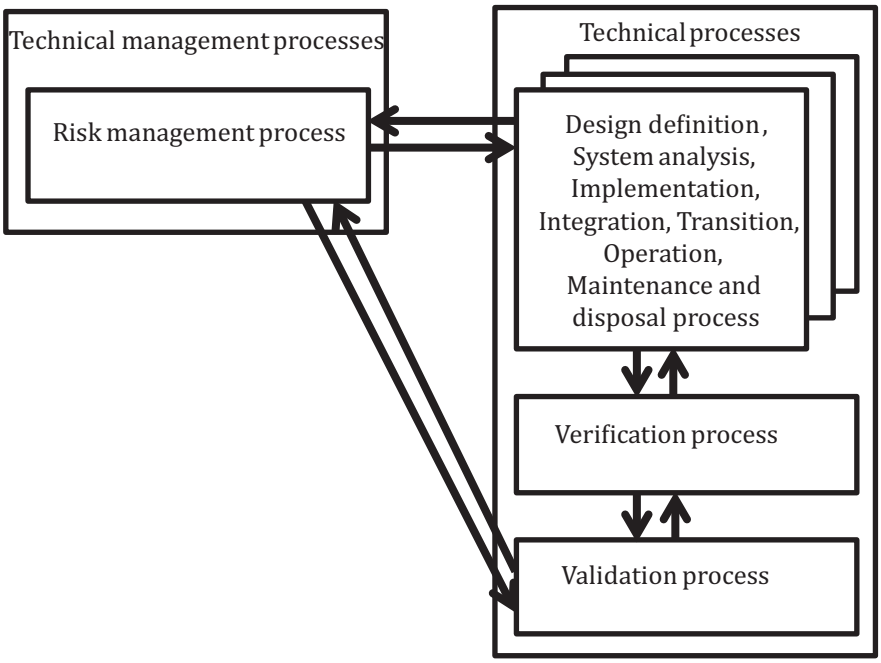
   3) for each system element, verify that obtained evidence satisfies the integrity level requirements associated with each system element's integrity level;

   4) verify that the obtained evidence satisfy the integrity level requirements.

c) Validation Process, with invocations of Risk Management Process, provides the following activities:

   1) for each system element, validate that the obtained evidence and the integrity level requirements associated with the system element integrity level show that the system element integrity level is achieved;

   2) validate that the obtained evidence shows that the required system integrity level is achieved.



Key

flow of processes

Figure 7 — Related processes in ISO/IEC/IEEE 15288 to the process of meeting integrity level requirements (informative)

9 Agreement and approval authorities

The people or organizations fulfilling the following roles shall be identified as follows:

a) integrity level definition authority (3.9);

b) design authority (3.5);

c) integrity level assurance authority (3.8).

Annex A
(informative)

An example of use of ISO/IEC 15026–3

A.1 General

This example considers the area of automatic cleaning machines for household use. In this context, an automatic cleaning machine provides services for cleaning rooms in the home without human intervention. It is also possible to connect such machines to the Internet to update software, collect usage data or to provide instructions from the user from outside the home. Therefore, the system has security-related adverse consequences. Since an automatic cleaning machine moves and cleans rooms without direct operation by human beings, the safety property would be the most significant.

A.2 Defining integrity levels

The characteristics and the assumptions of the target systems are as follows:

a) definition of the target class of systems: automatic cleaning machines;

b) assumptions of the environment:

   1) machines are home-use, not for industrial factories;

   2) machines may connect to the Internet.

In the following, the class of automatic cleaning machines characterized by the above statements is called ACM. Note that the symbol ACM does not represent any specific type of automatic cleaning machines.

The property-of-interest consists of the following items:

a) health and lives of users; in the following a “user” includes the owner of a machine in ACM, the member of the family of the owner, the guest of the home, and any pets;

b) any household furniture of the user’s home;

c) user’s home;

d) user’s private information;

e) a machine in ACM itself;

f) user’s time that is considered to be obtained with reducing cleaning time by introducing a machine in ACM;

g) serene and silent environment of user’s house.

The list of possible adverse consequences is as follows:

— user is injured or killed by being hit by a machine in ACM;

— user’s home or furniture are damaged by being hit with a machine in ACM;

— users’ private information is leaked through the Internet;

— machine in ACM is damaged by being hit with something;

— machine in ACM does not work during a period that a user has instructed it to work;

— machine in ACM makes some noise.

The list of possible dangerous conditions is as follows:

a) machine in ACM closely approaches the user without intention(near-miss);

b) machine in ACM goes out of control at breakneck speed;

c) network related software used in a machine in ACM has a security vulnerability;

d) machine in ACM breaks down.

The example risk criteria are as follows:

a) Risk leading to injuries of human beings or damages of any household property (safety risk):

   — severity class S1: minor damage of household property;

   — severity class S2: major damage of household property;

   — severity class S3: minor injury to users;

   — severity class S4: severe injury to users;

   — likelihood class a: reasonably possible;

   — likelihood class b: unlikely;

   — likelihood class c: improbable;

   — likelihood class d: extremely improbable.

b) Risk leading to release of private information(security risk):

   — severity class P1: leaking information that contains only logs of a machine in ACM;

   — severity class P2: leaking any other private information (e.g. photos of users, member list of the user's family, etc.).

   The classes of likelihood are the same as in the safety risk case.

c) Risk of loss of user's time(availability risk):

   — availability class T1: outage due to equipment is one day per year;

   — availability class T2: outrage due to equipment is 12 day per year.

d) Risk of threatening user's serene and silent environment(noise risk):

   — severity class E1: noise of infrasound;

   — severity class E2: noise of a frequency within limit of human hearing;

   — likelihood class x: once a week;

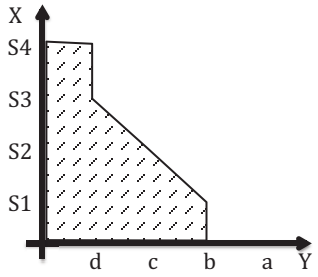
   — likelihood class y: once a month;

   — Likelihood class z: once a year.

An example tolerable risk for the safety risk above can be written as follows:

The risk under (S4, d), (S3, d), (S2, c), and (S1, b) is tolerable.

Figure A.1 shows an intuitive image of the tolerable risk where the gray area indicates the tolerable risks. For the other risks, i.e. security, availability and noise risks, their tolerable risks should be determined.



Key

X severity

Y likelihood

Figure A.1 — Intuitive image of the tolerable risk

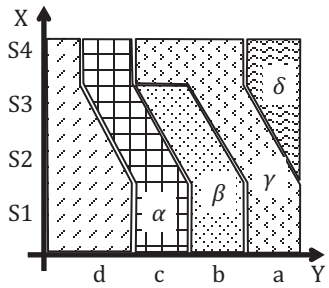
The assumed risk reduction structure is defined with the help of information of the enumerated adverse consequences and the dangerous conditions. For example, to avoid the dangerous condition that a machine in ACM closely approaches the user without intention, the following countermeasures can be considered:

a) safety-related functions of a machine in ACM to avoid such dangerous condition;

b) user's manual should state that the machine in ACM should not be used in the presence of unsupervised children or pets.

Assuming those frameworks to reduce risks, an integrity level claim can be defined as under the assumption that the users behave in accordance with the instructions given by the manufacturer, the safety-related functions of a machine in ACM behaves in the expected way.

In order to define a set of integrity levels, the associated set of risk classes should firstly be obtained from legal, regulatory, or contractual requirements. Example risk classes for safety are illustrated in Figure A.2.



Key

X severity

Y likelihood

Figure A.2 — Example of risk classes for safety

Using these risk classes, a set of the integrity levels for safety in this example is given as follows.

Unique identifier	Corresponding level of risk
ACM-Safety-IL I	α
ACM-Safety-ILII	β
ACM-Safety-IL III	γ
ACM-Safety-IL IV	δ

For the other risks, i.e. security, availability and noise risks, the assumptions of risk reduction measures for those risks and the integrity level claims, risk levels and a set of integrity levels for those risks should be determined. The whole integrity level of a machine in ACM is evaluated as a tuple of integrity levels of safety, security availability, and noise.

Bibliography

[1] IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[2] ISO 26262–10, *Road vehicles — Functional safety — Part 10: Guideline on ISO 26262*

[3] ISO/IEC 25010:2011, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*

[4] ISO/IEC 15408–1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

[5] ISO 14971, *Medical devices — Application of risk management to medical devices*

[6] ISO/IEC Guide 51:2014, *Safety aspects — Guidelines for their inclusion in standards*

[7] ISO Guide 73:2009, *Risk management — Vocabulary*

[8] ISO/IEC 15026–1, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

[9] ISO/IEC/IEEE 16085, *Systems and software engineering — Life cycle processes — Risk management*

[10] ISO 31000, *Risk management — Principles and guidelines*

ICS 35.080
Price based on 23 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™