INTERNATIONAL STANDARD

ISO/ IEC/IEEE 15026-3

Third edition
2023-10

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/IEEE 15026-3:2023(E)

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

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

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

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.

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 or www.iec.ch/members_experts/refdocs).

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

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

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

This third edition cancels and replaces the second edition (ISO/IEC 15026-3:2015), which has been technically revised.

The main changes are as follows:

— removal of duplicate terminological entries already included in ISO/IEC/IEEE 15026-1:2019 except for a few essential terms which are included in this edition for ease of reference;

— updates to normative references to the current edition of each reference.

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

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

Systems and software engineering — Systems and software assurance —

Part 3: System integrity levels

1 Scope

This document specifies the concept of integrity levels with the corresponding integrity level requirements for achieving the integrity levels. Requirements and recommended methods are provided for defining and using integrity levels and their corresponding integrity level requirements. This document covers systems, software products, and their elements, as well as relevant external dependences.

This document is applicable to systems and software and is intended for use by:

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 document 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 document in Annex A.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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*

ISO/IEC/IEEE 15026-1, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC/IEEE 15026-1 and the following apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp/ui

— IEC Electropedia: available at https://www.electropedia.org

— IEEE Standards Dictionary Online: available at https://dictionary.ieee.org

3.1
integrity level
degree of confidence that the system-of-interest meets the associated *integrity level claim* (3.4)

Note 1 to entry: A definition of "integrity" consistent with its use in "integrity level" has not been agreed in the relevant communities. Hence, no separate definition of "integrity" is included in this document.

Note 2 to entry: An integrity level is different from the likelihood 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 is a subjective concept.

Note 4 to entry: In this document, 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.

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.3.1, modified — Note 1 to entry has been revised to be more accurate and clearer; the reference to ISO/IEC 25010 has been removed; in note 4 to entry, "economic" has been replaced by "financial".]

3.2
integrity level assurance authority
independent person or organization responsible for certifying compliance with the *integrity level requirements* (3.5)

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.5.4, modified — The term has been changed from "integrity assurance authority" to "integrity level assurance authority".]

3.3
integrity level definition authority
person or organization responsible for defining integrity levels and integrity level requirements

3.4
integrity level claim
proposition representing a requirement on a risk reduction measure identified in the risk treatment process of the system-of-interest.

Note 1 to entry: In general, an integrity level claim is described in terms of requirements that, when met, would avoid, control or mitigate the consequences of dangerous conditions, and provide tolerable risk.

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.

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.3.4, modified — Notes 1 and 2 to entry have been revised to be more accurate and clearer.]

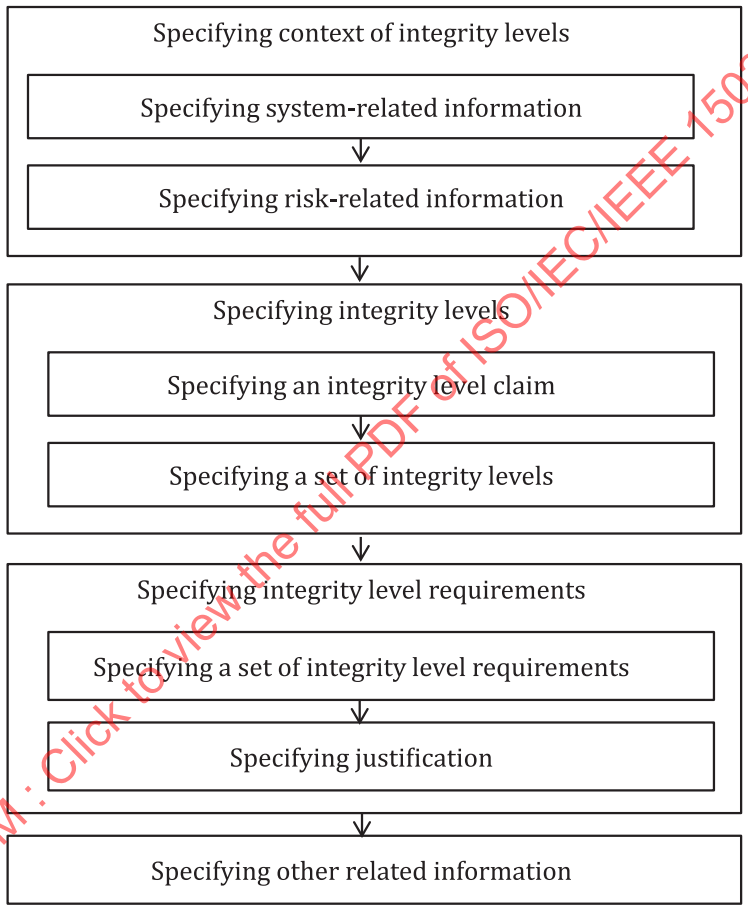
3.5
integrity level requirements
set of requirements that, when met, will provide a level of confidence in the associated *integrity level claim* (3.4) commensurate with the associated *integrity level* (3.1)

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.3.2, modified — Note 1 to entry has been removed.]

4 Defining integrity levels

4.1 Users 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 users of this clause are organizations which develop specifications defining a set of integrity levels. The 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 that 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

↓ represents flow of processes (iteration of processes is not shown for simplicity)

Figure 1 — Defining integrity levels

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) 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 Assurance cases work together with integrity levels by providing justified arguments for integrity level related definitions and means to demonstrate achievement of integrity levels. Their significance increases in an area where the body of relevant experience is less substantial or less well understood.

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 defined:

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 the ISO 26262 series. The definition of target classes of systems of IEC 61508 and the ISO 26262 series pertain to “electrical/electronic/programmable electronic (E/E/PE) systems that 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 3500 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 to clarify the scope of applicability of the integrity levels being defined:

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.

NOTE 1 While in general a risk is a negative or positive effect of uncertainty (ISO Guide 73), this document focuses on risks that are negative effects.

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

— a 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 types of events that lead to the condition. The following event types should be taken into account:

— random failures;

— systematic failures;

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

— failures caused by interactions between elements of the environment and the system (e.g. failures caused by a threat agent).

Likelihood of a dangerous condition should also be considered.

Risk criteria specify the meaning of system-related risks and are used to specify the tolerable risk. Risk criteria are defined to be consistent with applicable contractual, legal and regulatory constraints, which can be bases for the tolerable risk. Prior to specifying risk criteria, the categories for which risks will be evaluated are defined. These risk categories 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, for example, an inherent safety by design, and safety- or security-related functions, but also organizational supports or social frameworks to treat risks, for example, a contingency plan for operators, warnings in user's manuals, and safety- or security-related standards or regulations for developers. A structure of risk reduction measures should be assumed in order to clarify which parts are 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:

— a 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 are undefined or not 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 2 IEC 61508 assumes that a safety-related system can be recognized independently.

NOTE 3 The 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 4 IEC 61508 gives three sets of integrity levels, each of which corresponds to a demand mode to perform functional safety mechanisms.

4.4 Specifying integrity level claim and integrity levels

4.4.1 Key concepts

Figure 2 depicts the relationship among key concepts in this document. 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 satisfaction of the integrity level claims shall 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 consequences. The risk treatment process shall result in tolerable risk, where risk is characterized by its adverse consequence, which has attributes of severity and likelihood.

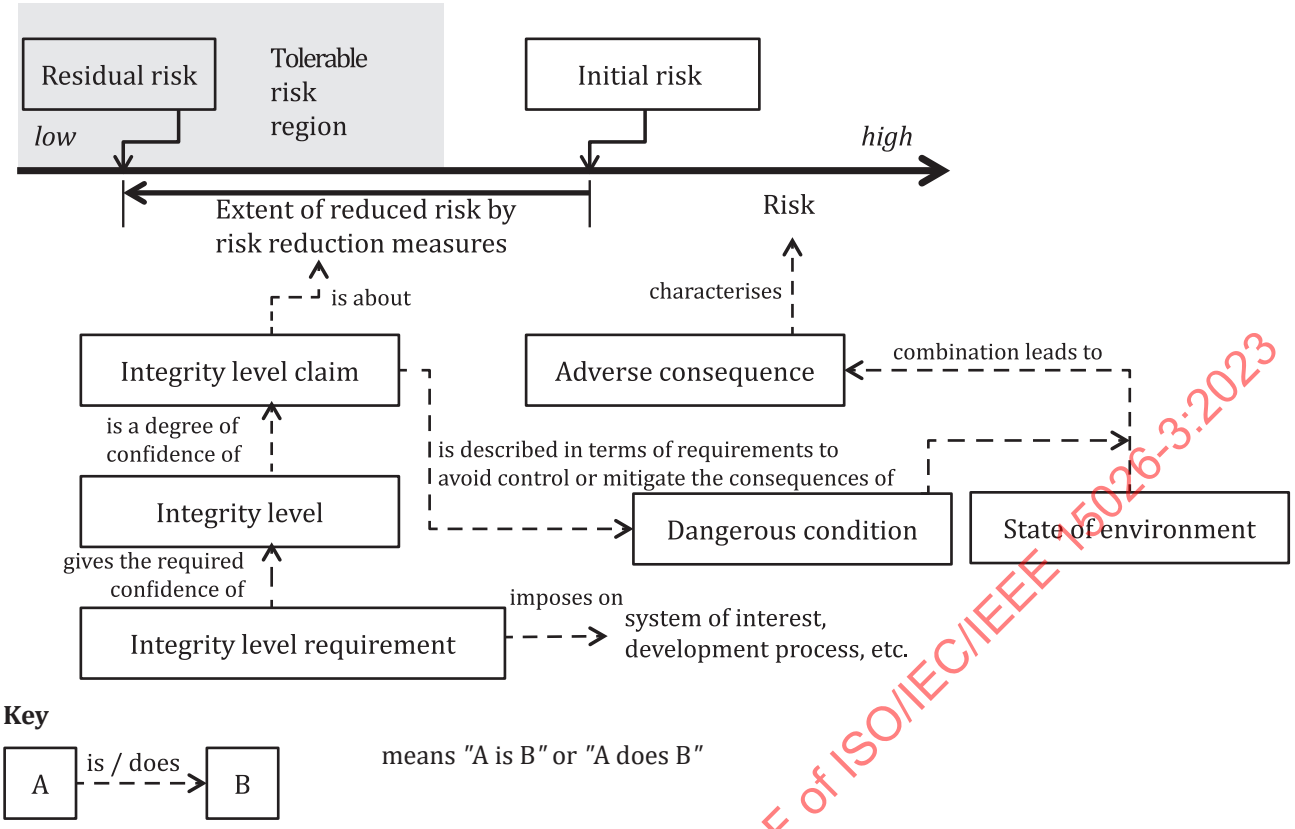


Figure 2 — Relations among key concepts

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.

4.4.2 Specifying an integrity level claim

An integrity level claim is a proposition on a risk reduction measure 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) a statement shall be a proposition on a system in the target class of systems and on the risk reduction measures taken for the system;

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 can be obtained 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 one or more adverse consequences and also to consider means to eliminate or avoid adverse consequence (Figure 3). Therefore, integrity level claims are typically defined in terms of dangerous conditions:

— a claim that a dangerous condition is controlled;

— a claim that a dangerous condition is avoided;

— a combination of the statements above.

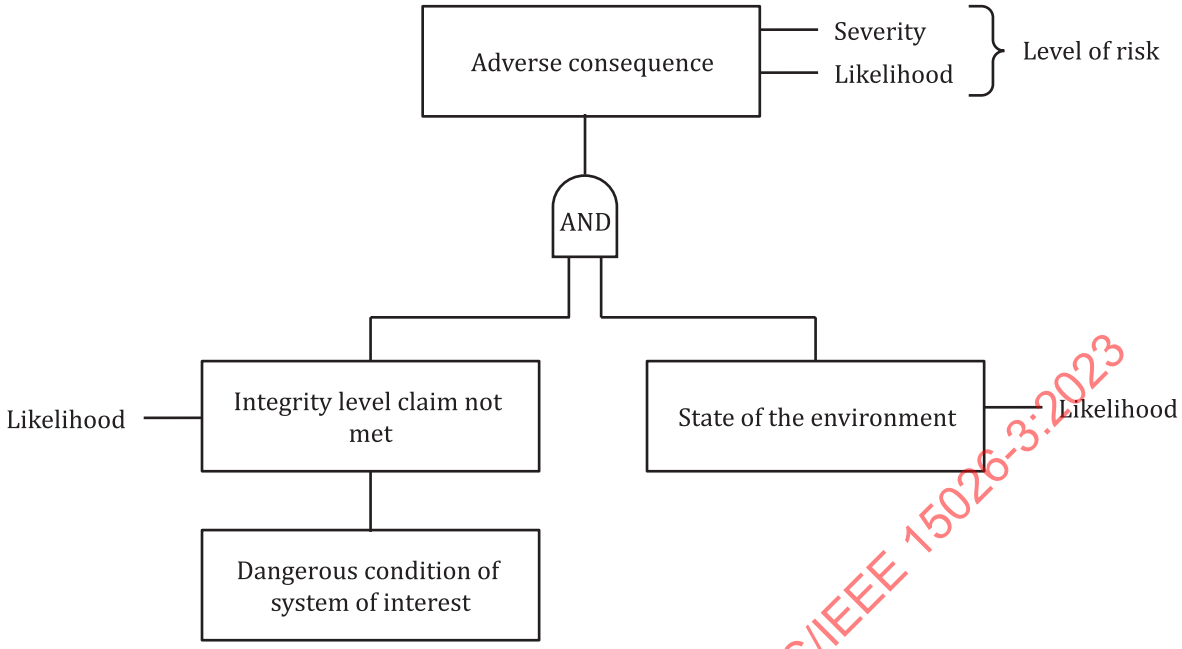


Figure 3 — Relationship between adverse consequence, state of the environment and integrity level claim

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

— a claim that risk sources are removed;

— a claim that the adverse consequences are mitigated;

— a 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 proposition 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 an integrity level claim combining removal of risk source and mitigation of the adverse consequence can be found in ISO 26262. In this example, ISO 26262 requires that a safety goal, which is defined for each hazard of an item, be satisfied.

4.4.3 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 defined 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) The integrity levels shall be defined based on a combination of the following:

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

2) the 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) The set of integrity levels shall be given in accordance with 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".

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 an 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 specifies what evidence is required to show that the requirement is satisfied.

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

Typical integrity level requirements specify the following:

— 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;

— the necessary test coverage criteria for testing;

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

— the provision of quantitative data;

— system or software life cycle processes;

— specific system development process models;

— specific methodologies to be used in development processes;

— specific tools to be used in system development processes;

— 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 depend on the risk that was used to define the integrity levels.

4.6 Specifying the 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 Clauses 6, 7 and 9. The process guideline shall contain the following processes:

a) determining system integrity levels;

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

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

5 Using integrity levels

5.1 Users of this clause

The framework of integrity levels is used to share common understandings of risks of systems among relevant stakeholders, especially between developers and users of the system. Developers can include development branches in an organization, system-integrators, and vendors. Usually, developers have a role in the determination of the required integrity level and the preparation of evidence demonstrating conformance with the integrity level requirements. The role of these developers 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 document, such third-party person or organization is called an integrity level assurance authority, who is expected to approve the design of the system based on the objective evidence produced to demonstrate conformance with the integrity level requirements.

Figure 4 shows the integrity level related products provided by the integrity level definition authority and the products established by a user of the set of integrity levels.

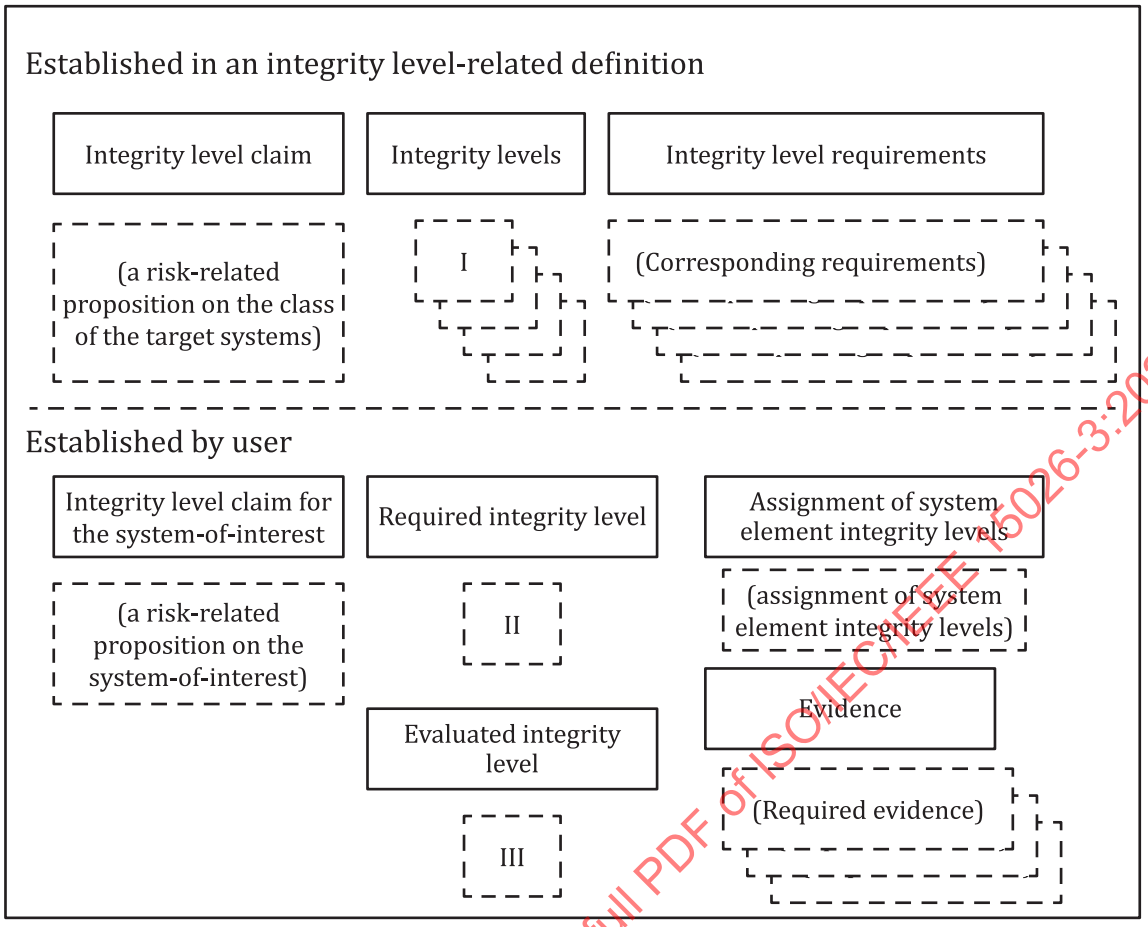


Figure 4 — Integrity level related-products with their sources

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

As a result of the successful usage of integrity levels:

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

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

c) system elements with lower integrity levels than the system integrity level are identified; 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

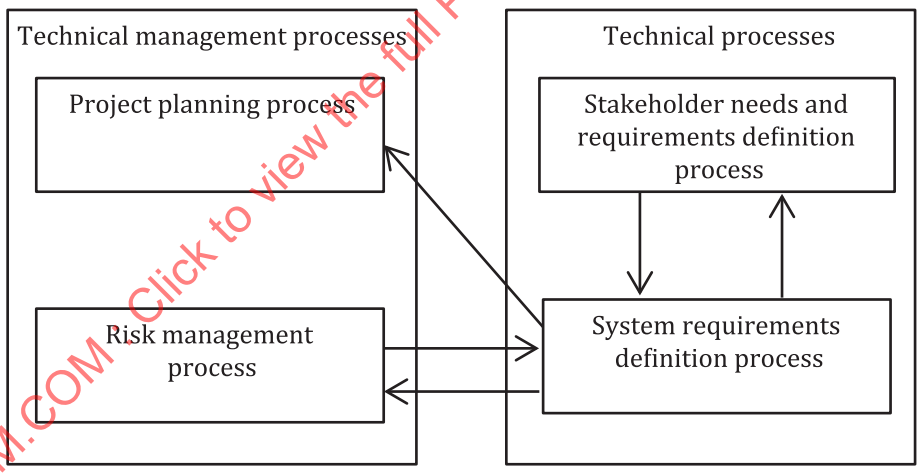
Determination of the system integrity level is typically done early in the development lifecycle of a system since the integrity level requirements need to be input to the project planning process. Integrity level determination should be done as part of the process to define stakeholder requirements.

A system integrity level shall be determined 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 and ISO/IEC/IEEE 12207.

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



Key

↓ represents flow of processes

Figure 5 — Processes in ISO/IEC/IEEE 15288 related to the system integrity level determination process

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

As a result of successful implementation of the system integrity level determination process:

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

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

c) a 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) the integrity level claims are identified;

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

f) integrity level requirements associated with the 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 shall be implemented by applying the following processes of ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207. Activities shown below each process are derived from ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207 but are specific to determination of system integrity levels.

a) The stakeholder needs and requirements 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) determine a standard in which a set of integrity levels is defined;

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

b) The system requirements definition process, with invocations of the risk management process, provides for the following activities:

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

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

   3) analyse risks of the system-of-interest and record the result in the risk profile;

   4) give a structure of the risk reduction tasks, including those implemented by the system-of-interest;

   5) evaluate risks and record the result in the risk profile;

   6) determine the required system integrity level;

   7) 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, each work product should be agreed among relevant stakeholders. The required system integrity level shall be used by the project planning processes.

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

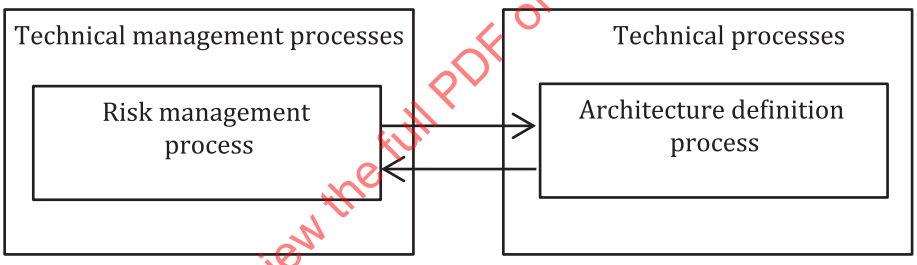
a) a set of system elements is identified;

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

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

7.3 Activities of the assigning system element integrity levels process

The assigning system element integrity levels process shall be implemented by applying the systems architecture definition process in ISO/IEC/IEEE 15288 or the architecture definition process of ISO/IEC/IEEE 12207 with invocations of the risk management process. (Figure 6).



Key

↓ represents flow of processes

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

The activities are derived from ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207, 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 relevant 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) for each system element identify integrity level requirements 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.

8 Meeting integrity level requirements

8.1 General

Meeting integrity level requirements is a process to ensure achievement of the determined system integrity level and the assigned system element integrity levels, i.e. satisfaction of all integrity level requirements associated with them. 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.

8.2 Purpose of meeting integrity level requirements

The purpose of the meeting integrity level requirements process is to reach agreement among relevant stakeholders that the residual risk of the implementation of the system-of-interest is evaluated to be within tolerable risk with a level of confidence commensurate with the associated integrity level.

8.3 Outcome of meeting integrity level requirements

As a result 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;

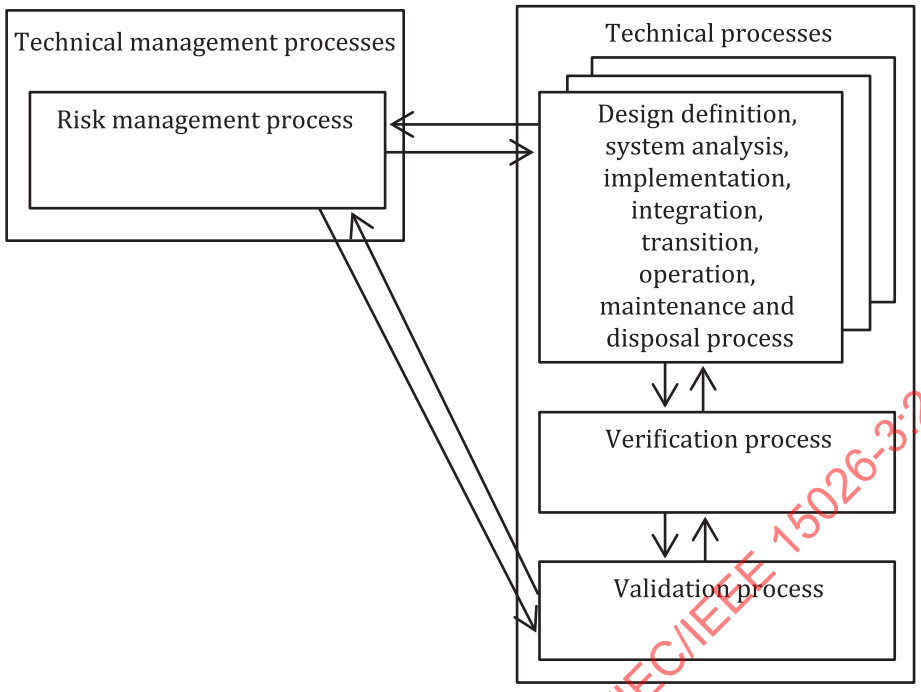
c) among the relevant stakeholders, especially between the design authority and the integrity level assurance authority, agreement that the required integrity level is achieved.

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

8.4 Activities of meeting integrity level requirements

The meeting integrity level requirements process shall be implemented by applying several technical processes in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 (Figure 7).

NOTE Evidence that is collected, verified and validated can be produced by many processes. The specifics depend on integrity level requirements defined.



Key

↓ represents flow of processes

Figure 7 — Processes in ISO/IEC/IEEE 15288 related to the process of meeting integrity level requirements

Activities are derived from ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 but are specific to meeting integrity level requirements.

a) The design definition process, system analysis process, implementation process, integration process, transition process, operation process and maintenance process, with invocations of the risk management process, provide the following activities:

   1) for each system element, collect objective evidence that is needed to demonstrate the completeness and correctness of the associated integrity level claim for that system element;

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

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

b) The verification process provides the following activities:

   1) for each system element, collect objective evidence that demonstrates the completeness and correctness of the associated integrity level claim for that system element;

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

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

   4) for each system element, verify that obtained evidence is as specified by the integrity level requirements associated with each system element's integrity level;

5) verify that the obtained evidence is as specified by the integrity level requirements.

c) The validation process, with invocations of the 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.

9 Agreement and approval authorities

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

a) integrity level definition authority;

b) design authority;

c) integrity level assurance authority.

Annex A
(informative)

An example of use of ISO/IEC/IEEE 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. The system therefore has security-related adverse consequences. Since an automatic cleaning machine moves and cleans rooms without direct operation by human beings, the safety property is the most significant.

A.2 Defining integrity levels

A.2.1 Characteristics and assumptions of the target system

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

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

b) assumptions of the environment:

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

   2) the machines can 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.

A.2.2 Properties of interest

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

a) the 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) the serene and silent environment of user’s house.

A.2.3 Possible adverse consequences

Possible adverse consequences are as follows:

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

b) the user's home or furniture are damaged by being hit with a machine in ACM;

c) the users' private information is leaked thought the Internet;

d) a machine in ACM is damaged by being hit with something;

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

f) a machine in ACM makes some noise.

A.2.4 Possible dangerous conditions

The list of possible dangerous conditions is as follows:

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

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

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

d) a machine in ACM breaks down.

A.2.5 Example risk criteria

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)

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 days 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

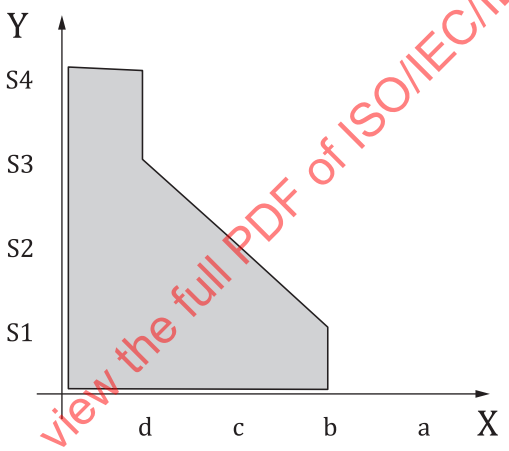
— Likelihood class z: once a year

A.2.6 Example tolerable risk

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 grey area indicates the tolerable risks. For the other risks, i.e. security, availability and noise risks, their tolerable risks should be determined.



Key

X likelihood

Y severity

Figure A.1 — Tolerable risk range

A.2.7 Example risk reduction structure

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) the user's manual states that the use of the machine in ACM is prohibited in the presence of unsupervised children or pets.

Assuming those frameworks to reduce risks, an integrity level claim can be defined as follows:

Under the assumption that the users behave in accordance with the instructions given by the developer, the safety-related functions of a machine in ACM behaves in the expected way.