INTERNATIONAL STANDARD

ISO/IEC/IEEE 15026-4

First edition
2021-05

Systems and software engineering — Systems and software assurance —

Part 4: Assurance in the life cycle

Ingénierie du logiciel et des systèmes — Assurance du logiciel et des systèmes —
Partie 4: Assurance du cycle de vie

Reference number
ISO/IEC/IEEE 15026-4:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 ISO documents should be noted. This document was drafted in accordance with the rules given in the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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.

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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.

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 first edition cancels and replaces ISO/IEC 15026-4:2012, which has been technically revised.

The main changes compared to the previous edition are as follows:

— References to the life cycle processes standards (ISO/IEC 15288:2008 and ISO/IEC 12207:2008, respectively) are changed to refer to their updated versions (ISO/IEC/IEEE 15288:2015 and ISO/IEC/IEEE 12207:2017, respectively).

— Outcomes of the process views are changed to make the link to their purpose clearer.

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

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.

Introduction

Many specialized standards and guidelines address specific application areas and topics related to assurance and use different concepts and terminology when addressing common themes. ISO/IEC/IEEE 15026-1 provides terminology and concepts used in ISO/IEC 15026 (all parts).

ISO/IEC 15026-2 provides minimum requirements for the structure and contents of assurance cases that treat claims regarding properties of a system or software product selected for special treatment. The results of performing the life cycle activities and tasks referenced in this document can be recorded in the form of the assurance case described in ISO/IEC 15026-2.

ISO/IEC 15026-3 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.

ISO/IEC 15026-2, ISO/IEC 15026-3 and this document all use the concepts and vocabulary defined in ISO/IEC/IEEE 15026-1; however, any part may be applied independently of the others and the use of one does not require the use of any others.

Systems and software engineering — Systems and software assurance —

Part 4: Assurance in the life cycle

1 Scope

This document provides guidance and recommendations for assurance of a selected claim about the system-of-interest by achieving the claim and showing the achievement. The guidance and recommendations are given in a system assurance process view on top of ISO/IEC/IEEE 15288 and a software assurance process view on top of ISO/IEC/IEEE 12207.

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 15026-1, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

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

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC/IEEE 15026-1, ISO/IEC/IEEE 15288, and ISO/IEC/IEEE 12207 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

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

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

3.1
assurance
grounds for justified confidence that a claim has been or will be achieved

Note 1 to entry: By definition, assurance is about a claim.

Note 2 to entry: The claim can be a conjunction of more than one claim.

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.1.1, modified — Notes 1 and 2 to entry have been added.]

3.2
assurance argument
artefact that links tangible evidence and assumptions to provide a convincing and valid argument of a claim under a given context

3.3
assurance claim
claim for which *assurance* (3.1) is considered

3.4
assurance information
information including a claim about a system, evidence supporting the claim, an argument showing how the evidence supports the achievement of the claim, and the context for these items

Note 1 to entry: The sub-claims included in the argument of assurance information can be about the life cycle of the system of interest when, for example, the top-level claim implies continuous achievement of some property.

Note 2 to entry: ISO/IEC 15026-2 specifies assurance cases that documents assurance information.

3.5
assurance objective
purpose of achievement of the *assurance claim* (3.3)

Note 1 to entry: Assurance objectives determine the required degree of integrity level and permissible uncertainty in the *assurance information* (3.4).

3.6
critical property
property that is agreed by primary stakeholders as having serious consequence

4 Conformance

The assurance guidance and recommendations referenced in this document are to be understood in the context of the processes, activities and tasks of ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207.

Conformance may be claimed to this document with respect to the system assurance process view and/or the software assurance process view. Thus, conformance to this document shall be achieved in either or both of the following ways.

a) achieving the required outcomes of the system assurance process view, in addition to conforming to ISO/IEC/IEEE 15288;

b) achieving the required outcomes of the software assurance process view, in addition to conforming to ISO/IEC/IEEE 12207.

5 Key concepts

5.1 Process view

It is presumed that the user of this document is using a defined life cycle model. This document provides two process views: the system assurance process view on top of ISO/IEC/IEEE 15288 and the software assurance process view on top of ISO/IEC/IEEE 12207.

NOTE See ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207 for a description and examples of process views.

According to the description in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207, a process view includes

— name,

— purpose,

— outcomes, and

— identification and description of the processes, activities and tasks that implement the process view, and references to the sources for these processes, activities and tasks in other standards.

5.2 Assurance claim and assurance information

A claim for which system or software assurance is considered, is called an assurance claim. The system assurance process view in Clause 6 and the software assurance process view in Clause 7 can be used to achieve the assurance claim, and to provide assurance information that shows the achievement. Commonly, such an assurance claim is in area where substantial risks or consequences are involved such as reliability and maintainability, safety, security, or human factors.

While the assurance claim can be derived from a number of sources, it is normally motivated by potential real-world adverse consequences associated with the capability of the system, the intended use of the system, and the outcomes produced by the system.

The body of information showing that the system-of-interest achieves the assurance claim is called assurance information, which includes:

a) the assurance claim,

b) the required degree of confidence in achievement of the assurance claim,

c) justification of selection of the assurance claim,

d) evidence of achievement of the assurance claim, adequate for the required degree of confidence, and

e) an argument about how the evidence in d) supports achievement of the assurance claim a).

The item b) includes the required integrity level of the system with respect to the assurance claim. Items c), d), e) should be adequate for the required degree of confidence in b). The item e) should reflect satisfaction of the assurance claim (item a) commensurate with the required degree of confidence.

NOTE Assurance case as specified by ISO/IEC 15026-2 can be used as a structured approach to compile these items of assurance information.

The argument often includes several different kinds of sub-arguments, e.g. arguments based on design rationale, use of defensive design techniques, verification and validation results, performance of similar systems or products, conformance to standards, or field data. An argument consisting of different kinds of sub-arguments gains more confidence in achievement of the assurance claim.

The assurance information is maintained and updated throughout the system life cycle, in accordance with the change of the system during maintenance and redevelopment. The assurance information is a configuration element of the system-of-interest and associated with all the system life cycle processes. In particular, the assurance information needs to be controlled within the configuration management process which activates the verification process and the validation process, which in turn provides the contents.

5.3 Using this document

5.3.1 General

This document can be used for establishing an agreement between an acquirer and a supplier, for regulatory purposes, or for assessment of internal development processes. This document clarifies what it means both to achieve the assurance claim and to demonstrate that the assurance claim is achieved. Its use is, however, not limited to these three purposes.

5.3.2 Use for an agreement

This document can be used for establishing an agreement between an acquirer and a supplier concerning achieving the assurance claim and showing the achievement. The acquirer and supplier relationship can be at different levels of the supply chain (prime-supplier, internal to one organization, etc.).

NOTE An agreement can range in formality from a written contract to a verbal understanding.

5.3.3 Use for regulation

An authoritative body can use this document for regulation about, for certification about or just for clarification of assurance required in the condition of trade.

5.3.4 Use for development

This document can be used for an internal assessment by a developer in improving its processes for achieving the assurance claim and showing the achievement.

6 System assurance process view

6.1 General

This clause provides the system assurance process view. 6.2 provides its purpose; 6.3 provides its outcomes; 6.4 identifies the processes, activities and tasks that implement the process view; and 6.5 provides guidance about and recommendations for the identified processes. Since all processes of ISO/IEC/IEEE 15288 are applied iteratively and recursively in the life cycle, the guidance and recommendations should also be applied iteratively and recursively.

NOTE 1 See ISO/IEC/IEEE 24748-1 for more information about life cycle models and the iteration and recursion of processes.

NOTE 2 Performance of the system assurance process view is affected crucially by the quality of assurance claim, which in turn reflects the quality of requirements. See ISO/IEC/IEEE 29148 for guidance on requirement engineering.

6.2 Purpose

The purpose of the system assurance process view is to achieve the assurance claim and to provide assurance information to demonstrate that the assurance claim is achieved.

NOTE This process view depends not only on the system-of-interest but also on the assurance claim.

6.3 Outcomes

As a result of the successful implementation of the system assurance process view:

a) the assurance claim for the system is identified;

b) the required degree of confidence in achievement of the assurance claim is identified;

c) justification of selection of the assurance claim is produced;

d) the assurance claim identified by outcome a) has been or will be achieved.

e) evidence of achievement of the assurance claim is produced;

f) an argument about how the evidence in e) supports achievement of the assurance claim a) is produced.

The degree of confidence in outcome b) includes the required integrity level of the system with respect to the assurance claim. Outcomes c), d), e) and f) should be obtained to the extent that the degree of confidence identified by outcome b) is attained.

6.4 Processes, activities and tasks that implement the system assurance process view

Table 1 shows the life cycle processes that should be applied in order to achieve outcomes of the system assurance process view.

Table 1 — Processes that implement the process views in this document

ISO/IEC/IEEE 15288:2015 and ISO/IEC/IEEE 12207:2017 subclause number	ISO/IEC/IEEE 15288:2015 and ISO/IEC/IEEE 12207:2017 subclause title	Used by system assurance process view	Used by software assurance process view
6.1	Agreement processes		
6.1.1	Acquisition process	x	x
6.1.2	Supply process	x	x
6.2	Organizational project-enabling processes		
6.2.1	Life cycle model management process	x	x
6.2.2	Infrastructure management process		
6.2.3	Portfolio management process		
6.2.4	Human resource management process		
6.2.5	Quality management process	x	x
6.2.6	Knowledge management process		
6.3	Technical management processes		
6.3.1	Project planning process	x	x
6.3.2	Project assessment and control process	x	x
6.3.3	Decision management process	x	x
6.3.4	Risk management process	x	x
6.3.5	Configuration management process	x	x
6.3.6	Information management process	x	x
6.3.7	Measurement process		
6.3.8	Quality assurance process	x	x
6.4	Technical processes		
6.4.1	Business or mission analysis process	x	x
6.4.2	Stakeholder needs and requirements definition process	x	x
6.4.3	System requirements definition process System/software requirements definition process	x	x
6.4.4	Architecture definition process	x	x
6.4.5	Design definition process	x	x
6.4.6	System analysis process	x	x
6.4.7	Implementation process	x	x
6.4.8	Integration process	x	x
6.4.9	Verification process	x	x
6.4.10	Transition process	x	x
6.4.11	Validation process	x	x
6.4.12	Operation process	x	x
6.4.13	Maintenance process	x	x
6.4.14	Disposal process	x	x

The processes, activities, and tasks of ISO/IEC/IEEE 15288 that should be used to achieve the outcomes provided in 6.3 are provided in the list below with their respective ISO/IEC/IEEE 15288:2015 subclause numbers. Guidance and recommendations with respect to some of these tasks are given in 6.5.

- Acquisition process (6.1.1)
  - Define a strategy for how the acquisition will be conducted. (6.1.1.3.a.1)
  - Prepare a request for the supply of a product or service that includes the requirements. (6.1.1.3.a.2)
  - Communicate the request for the supply of a product or service to potential suppliers. (6.1.1.3.b.1)
  - Develop an agreement with the supplier that includes acceptance criteria. (6.1.1.3.c.1)
  - Evaluate impact of changes on the agreement. (6.1.1.3.c.3)
  - Negotiate the agreement with the supplier. (6.1.1.3.c.4)
  - Assess the execution of the agreement. (6.1.1.3.d.1)
- Supply process (6.1.2)
  - Negotiate an agreement with the acquirer that includes acceptance criteria. (6.1.2.3.c.1)
  - Negotiate the agreement with the acquirer. (6.1.2.3.c.4)
  - Deliver the product or service in accordance with the agreement criteria. (6.1.2.3.e.1)
- Quality management process (6.2.5)
  - Establish quality management policies, objectives, and procedures. (6.2.5.3.a.1)
  - Define responsibilities and authority for implementation of quality management. (6.2.5.3.a.2)
  - Define quality evaluation criteria and methods. (6.2.5.3.a.3)
  - Provide resources and information for quality management. (6.2.5.3.a.4)
  - Gather and analyze quality assurance evaluation results, in accordance with the defined criteria. (6.2.5.3.b.1)
- Project planning process (6.3.1)
  - Identify the project objectives and constraints. (6.3.1.3.a.1)
  - Define the project scope as established in the agreement. (6.3.1.3.a.2)
  - Define and maintain a life cycle model that is comprised of stages using the defined life cycle models of the organization. (6.3.1.3.a.3)
  - Establish a work breakdown structure based on the evolving system architecture. (6.3.1.3.a.4)
  - Define and maintain the processes that will be applied on the project. (6.3.1.3.a.5)
  - Define and maintain a project schedule based on management and technical objectives and work estimates. (6.3.1.3.b.1)
  - Define roles, responsibilities, accountabilities, and authorities. (6.3.1.3.b.4)
- Decision management process (6.3.3)
  - Define a decision management strategy. (6.3.3.3.a.1)
  - Identify the circumstances and need for a decision. (6.3.3.3.a.2)

- Involve relevant stakeholders in the decision-making in order to draw on experience and knowledge. (6.3.3.3.a.3)
- Select and declare the decision management strategy for each decision. (6.3.3.3.b.1)
- Determine desired outcomes and measurable selection criteria. (6.3.3.3.b.2)
- Identify the trade space and alternatives. (6.3.3.3.b.3)
- Evaluate each alternative, against the criteria. (6.3.3.3.b.4)
- Record, track, evaluate and report decisions. (6.3.3.3.c.3)

— Risk management process (6.3.4)

- Define the risk management strategy. (6.3.4.3.a.1)
- Define and record the context of the risk management process. (6.3.4.3.a.2)
- Define and record the risk thresholds and conditions under which a level of risk may be accepted. (6.3.4.3.b.1)
- Establish and maintain a risk profile. (6.3.4.3.b.2)
- Periodically provide the relevant risk profile to stakeholders based upon their needs. (6.3.4.3.b.3)
- Identify risks in the categories described in the risk management context. (6.3.4.3.c.1)
- Estimate the likelihood of occurrence and consequences of each identified risk. (6.3.4.3.c.2)
- Evaluate each risk against its risk thresholds. (6.3.4.3.c.3)
- Identify recommended alternatives for risk treatment. (6.3.4.3.d.1)
- Implement risk treatment alternatives for which the stakeholders determine that actions should be taken to make a risk acceptable. (6.3.4.3.d.2)
- When the stakeholders accept a risk that does not meet its threshold, consider it a high priority and monitor it continually to determine if any future risk treatment actions are necessary. (6.3.4.3.d.3)
- Once a risk treatment is selected, coordinate management action. (6.3.4.3.d.4)
- Continually monitor all risks and the risk management context for changes and evaluate the risks when their state has changed. (6.3.4.3.e.1)
- Implement and monitor measures to evaluate the effectiveness of risk treatments. (6.3.4.3.e.2)
- Continually monitor for the emergence of new risks and sources throughout the life cycle. (6.3.4.3.e.3)

— Configuration management process (6.3.5)

- Define a configuration management strategy. (6.3.5.3.a.1)
- Identify the system elements and information items that are configuration items. (6.3.5.3.b.1)
- Identify and record requests for change and requests for variance. (6.3.5.3.c.1)
- Coordinate, evaluate, and disposition requests for change and requests for variance. (6.3.5.3.c.2)
- Submit requests for review and approval. (6.3.5.3.c.3)
- Track and manage approved changes to the baseline, requests for change, and requests for variance. (6.3.5.3.c.4)