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<br>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)

  - Develop and maintain the configuration management status information, for system elements, baselines, and releases. (6.3.5.3.d.1)
  - Capture, store and report configuration management data. (6.3.5.3.d.2)
- Information management process (6.3.6)
  - Define the items of information that will be managed. (6.3.6.3.a.2)
  - Designate authorities and responsibilities for information management. (6.3.6.3.a.3)
  - Define information maintenance actions. (6.3.6.3.a.5)
  - Maintain information items and their storage records, and record the status of information. (6.3.6.3.b.2)
  - Dispose of unwanted, invalid or unvalidated information. (6.3.6.3.b.5)
- Quality assurance process (6.3.8)
  - Create records and reports related to quality assurance activities. (6.3.8.3.d.1)
  - Maintain, store, and distribute records and reports. (6.3.8.3.d.2)
  - Identify incidents and problems associated with product, service, and process evaluations. (6.3.8.3.d.3)
- Business or mission analysis process (6.4.1)
  - Define the business or mission analysis strategy. (6.4.1.3.a.2)
  - Define the mission, business, or operational problem or opportunity. (6.4.1.3.b.2)
  - Maintain traceability of business or mission analysis. (6.4.1.3.e.1)
- Stakeholder needs and requirements definition process (6.4.2)
  - Prepare for stakeholder needs and requirements definition. (6.4.2.3.a)
  - Define stakeholder needs. (6.4.2.3.b)
  - Define context of use within the concept of operations and the preliminary life cycle concepts. (6.4.2.3.b.1)
  - Identify stakeholder needs. (6.4.2.3.b.2)
  - Develop the operational concept and other life cycle concepts. (6.4.2.3.c)
  - Identify the stakeholder requirements and functions that relate to critical quality characteristics, such as assurance, safety, security, environment, or health. (6.4.2.3.d.2)
  - Define stakeholder requirements, consistent with life cycle concepts, scenarios, interactions, constraints, and critical quality characteristics. (6.4.2.3.d.3)
  - Analyze the complete set of stakeholder requirements. (6.4.2.3.e.1)
  - Define critical performance measures that enable the assessment of technical achievement. (6.4.2.3.e.2)
  - Obtain explicit agreement on the stakeholder requirements. (6.4.2.3.f.1)

  - Maintain traceability of stakeholder needs and requirements. (6.4.2.3.f.2)
- System requirements definition process (6.4.3)
  - Prepare for system requirements definition. (6.4.3.3.a)
  - Define system requirements. (6.4.3.3.b)
  - Define each function that the system is required to perform. (6.4.3.3.b.1)
  - Define necessary implementation constraints. (6.4.3.3.b.2)
  - Identify system requirements that relate to risks, criticality of the system, or critical quality characteristics. (6.4.3.3.b.3)
  - Define system requirements and rationale. (6.4.3.3.b.4)
  - Analyze the complete set of system requirements. (6.4.3.3.c.1)
  - Obtain explicit agreement on the system requirements. (6.4.3.3.d.1)
  - Maintain traceability of the system requirements. (6.4.3.3.d.2)
- Architecture definition process (6.4.4)
  - Define the system context and boundaries in terms of interfaces and interactions with external entities. (6.4.4.3.c.1)
  - Identify architectural entities and relationships between entities that address key stakeholder concerns and critical system requirements. (6.4.4.3.c.2)
  - Select, adapt, or develop models of the candidate architectures of the system. (6.4.4.3.c.4)
  - Maintain the architecture definition and evaluation strategy. (6.4.4.3.f.5)
  - Maintain traceability of the architecture. (6.4.4.3.f.6)
- Design definition process (6.4.5)
  - Assess alternatives for obtaining system elements. (6.4.5.3.c)
  - Identify any candidate non-developmental-items (NDI) that may be considered for use. (6.4.5.3.c.1)
  - Map design characteristics up to the system elements. (6.4.5.3.d.1)
  - Capture design and rationale. (6.4.5.3.d.2)
  - Maintain traceability of design. (6.4.5.3.d.3)
- System analysis process (6.4.6)
  - Define the scope, objectives, and level of fidelity of the system analysis. (6.4.6.3.a.3)
  - Maintain traceability of system analysis results. (6.4.6.3.c.1)
- Implementation process (6.4.7)
  - Record objective evidence that the system element meets system requirements. (6.4.7.3.b.3)
  - Record implementation results and any anomalies encountered. (6.4.7.3.c.1)

  - Maintain traceability of the implemented system elements. (6.4.7.3.c.2)
- Integration process (6.4.8)
  - Perform check of the interfaces, selected functions, and critical quality characteristics. (6.4.8.3.b.3)
  - Record integration results and any anomalies encountered. (6.4.8.3.c.1)
  - Maintain traceability of the integrated system elements. (6.4.8.3.c.2)
- Verification process (6.4.9)
  - Define the verification strategy. (6.4.9.3.a.4)
  - Identify system constraints from the verification strategy to be incorporated in the system requirements, architecture, or design. (6.4.9.3.a.5)
  - Record verification results and any anomalies encountered. (6.4.9.3.c.1)
  - Record operational incidents and problems and track their resolution. (6.4.9.3.c.2)
  - Maintain traceability of the verified system elements. (6.4.9.3.c.4)
- Transition process (6.4.10)
  - Demonstrate proper installation of the system. (6.4.10.3.b.4)
  - Demonstrate the installed system is capable of delivering its required functions. (6.4.10.3.b.7)
  - Demonstrate the functions provided by the system are sustainable by the enabling systems. (6.4.10.3.b.8)
  - Record transition results and any anomalies encountered. (6.4.10.3.c.1)
  - Record operational incidents and problems and track their resolution. (6.4.10.3.c.2)
  - Maintain traceability of the transitioned system elements. (6.4.10.3.c.3)
- Validation process (6.4.11)
  - Identify and plan for the necessary enabling systems or services needed to support validation. (6.4.11.3.a.6)
  - Record validation results and any anomalies encountered. (6.4.11.3.c.1)
  - Record operational incidents and problems and track their resolution. (6.4.11.3.c.2)
  - Maintain traceability of the validated system elements. (6.4.11.3.c.4)
- Operation process (6.4.12)
  - Define an operation strategy. (6.4.12.3.a.1)
  - Identify system constraints from operation to be incorporated in the system requirements, architecture, or design. (6.4.12.3.a.2)
  - Identify or define training and qualification requirements for personnel needed for system operation. (6.4.12.3.a.5)
  - Monitor system operation. (6.4.12.3.b.3)
  - Record results of operation and any anomalies encountered. (6.4.12.3.c.1)
  - Record operational incidents and problems and track their resolution. (6.4.12.3.c.2)

- Maintain traceability of the operations elements. (6.4.12.3.c.3)

- Maintenance process (6.4.13)
  - Define a maintenance strategy. (6.4.13.3.a.1)
  - Identify and plan for the necessary enabling systems or services needed to support maintenance. (6.4.13.3.a.4)
  - Perform maintenance. (6.4.13.3.b)
  - Review incident and problem reports to identify future corrective, adaptive, perfective and preventive maintenance needs. (6.4.13.3.b.1)
  - Perform preventive maintenance by replacing or servicing system elements prior to failure, according to planned schedules and maintenance procedures. (6.4.13.3.b.5)
  - Perform failure identification actions when a non-compliance has occurred in the system. (6.4.13.3.b.6)
  - Identify when adaptive or perfective maintenance is required. (6.4.13.3.b.7)
  - Record maintenance and logistics results and any anomalies encountered. (6.4.13.3.d.1)
  - Record operational incidents and problems and track their resolution. (6.4.13.3.d.2)
  - Identify and record trends of incidents, problems, and maintenance and logistics actions. (6.4.13.3.d.3)
  - Maintain traceability of the maintenance elements. (6.4.13.3.d.4)
  - Provide key information items that have been selected for baselines. (6.4.13.3.d.5)
  - Monitor customer satisfaction with system and maintenance support. (6.4.13.3.d.6)

- Disposal process (6.4.14)
  - Define a disposal strategy for the system, to include each system element and any resulting waste products. (6.4.14.3.a.1)
  - Return the environment to its original state or to a state that specified by agreement. (6.4.14.3.c.2)
  - Archive information gathered through the lifetime of the system to permit audits and reviews in the event of long-term hazards to health, safety, security and the environment, and to permit future system creators and users to build a knowledge base from past experiences. (6.4.14.3.c.3)

## 6.5 Guidance and recommendations

### 6.5.1 General

This subclause provides guidance and recommendations with respect to some of the activities and tasks of the processes in ISO/IEC/IEEE 15288 identified in 6.4. Necessary extensions to the activities and tasks are provided. Any special interpretation, if necessary, is also given.

In the following, each subclause is dedicated to a system life cycle process that has some activity or task that implements the system assurance process view. At the end of the paragraphs, except for the first paragraph in each subclause which is general, the numbering of the activity or task in ISO/IEC/IEEE 15288 enclosed by angle brackets is given, followed by the numbering of the outcome of

this process view enclosed by square brackets. This means the paragraph is guidance about the activity or task to achieve the outcome.

EXAMPLE At the end of the second paragraph of 6.5.2, there is a mark "<a)1), a)2), b)1)>; outcome [d)]". This means the paragraph is guidance about the tasks a)1), a)2) and b)1) of the acquisition process, and the guidance is for achieving the outcome d) of this process view.

### 6.5.2 Acquisition process

The purpose of the acquisition process is to obtain a product or service in accordance with the acquirer's requirements (ISO/IEC/IEEE 15288:2015, 6.1.1.1). This process should help ensure that all requirements for achieving the assurance claim and for showing the achievement is passed to the supplier through the agreement.

The project should submit a request for proposal (RFP) with the consideration of avoiding misunderstandings in interpretation so as to obtain a feasible assurance claim. <a)1), a)2), b)1)>; outcome [d)]

The primary stakeholders should endeavour to ensure that the agreement includes achievement of the assurance claim. <c)1)>; outcome [d)]

The variables relevant to the elements being acquired and influencing achievement of the assurance claim should be referred to in the agreement, as well as the values of those variables. The project should derive the requirements for the elements being acquired from the assurance claim and incorporate them into the request for the supply of the element. <c)1)>; outcome [d)]

In addition, the project should incorporate the following considerations into the negotiations and the agreement with the supplier:

a) confidence that the product development environment has appropriate resources in place to protect the integrity of the product and the assurance claim during development;

b) confidence that the system development lifecycle model chosen by the supplier is appropriate to the nature of the assurance claim;

c) confidence that the development lifecycle is conducted using well documented, repeatable processes that are monitored in accordance with a quality management plan appropriate to the nature of the assurance claim. <c)1)>; outcome [c), d)]

The agreement should enable fulfilment of the requirements that are necessary for achievement of the assurance claim. <c)1)>; outcome [d)]

NOTE 1 For instance, the agreement usually includes such requirements as guarding against counterfeit parts, tampering, elements with vulnerabilities, and revealing of confidential information. The confidential information includes information about vulnerabilities that makes certain that what is received is what is expected.

The project should consider a multi-stage agreement when appropriate. <a)1)>; outcome [d)]

The project should revisit the approaches to showing achievement of the assurance claim if the relationship between the acquirer and the supplier changes or if the acquirer's requirements change. <c)3)>; outcome [f)]

NOTE 2 The relationship between the acquirer and the supplier changes when a new supplier participates, or mergers and acquisitions (M&A) take place with respect to a supplier. The acquirer's requirements often have to change in order to ensure that the supplier does not refuse to provide required information, enable a new threat, or undermine existing safeguards for the system-of-interest.

NOTE 3 This action invokes change management carried out as a part of the configuration management process.

Independent reporting of issues regarding the assurance claim should be required in the contract. <c)1)>; outcome [f)]

### 6.5.3 Supply process

The purpose of the supply process is to provide an acquirer with a product or service that meets agreed requirements (ISO/IEC/IEEE 15288:2015, 6.1.2.1). This process should help ensure that all requirements for achieving the assurance claim and for showing the achievement is passed to the acquirer through the agreement.

The primary stakeholders should endeavour to ensure that the agreement includes achievement of the assurance claim from the technical and resources aspects. The variables relevant to the elements being supplied and influencing achievement of the assurance claim should be referred to in the agreement, as well as the values of those variables. <c)1)>; outcome [d)]

The agreement should enable fulfilment of the requirements that are necessary for achievement of the assurance claim. <c)>; outcome [d)]

The project should incorporate the following considerations into the negotiations and the agreement with the acquirer, in order to achieve the assurance claim which offsets the resource available to the project:

a) confidence that there is a means to fulfil major requirements in a practical manner from technical and other aspects;

b) consideration of a multistage agreement, in the case that the precise cost estimation is difficult to achieve;

c) consideration of stepwise commencement of operations of the system, should there be a possibility of missing the deadline due to unexpected reason. <c)1)>; outcome [c), d)]

Independent reporting of issues regarding the assurance claim should be required in the contract. <c)1)>; outcome [f)]

The project should provide information that is necessary to select the assurance claim. <c)1)>; outcome [a)]

### 6.5.4 Life cycle model management process

The purpose of the life cycle model management process is to define, maintain, and assure availability of policies, life cycle processes, life cycle models, and procedures for use by the organization with respect to the scope of ISO/IEC/IEEE 15288 (ISO/IEC/IEEE 15288:2015, 6.2.1.1).

The primary stakeholders should endeavour to ensure that the implemented life cycle model is feasible from the aspect of achievement of the assurance claim, and will be so through evolution of the life cycle model. <a), c)>; outcome [d)]

### 6.5.5 Quality management process

The purpose of the quality management process is to assure that products, services and implementations of the quality management process meet organizational and project quality objectives and achieve customer satisfaction (ISO/IEC/IEEE 15288:2015, 6.2.5.1).

The quality management process should be consistent with the requirements for achieving assurance with the required degree of confidence. <a)1)>; outcome [d)]

The quality management process should document the justification for the requirements for achieving the assurance to the extent of the required degree of confidence. <b)1)>; outcome [f)]

NOTE Often the justification for those requirements are established by an authority such as a standards organization, industry organization or organizations responsible for contract management within a company.

### 6.5.6 Project planning process

The purpose of the project planning process is to produce and coordinate effective and workable plans. The project plans should include the means to ensure adequate resources to achieve the assurance claim and show the achievement (ISO/IEC/IEEE 15288:2015, 6.3.1.1).

NOTE 1 Achievement of the assurance claim and the argument showing the achievement can be documented as an assurance case with the structure and format provided by ISO/IEC 15026-2.

The assurance objectives should be communicated to as many stakeholders of the project as possible, including top management, customers and suppliers. <a)1)>; outcome [d)]

The development method, environment and tools should be determined in consideration of the assurance claim and the required degree of confidence in achievement of the assurance claim, according to an analysis of the workflow and information processed by the system. <a)2)>; outcome [d)]

NOTE 2 Each of the development methodologies, such as process-oriented, data-oriented, and object-oriented methods, has its own suitability to different applications.

The primary stakeholders should endeavour to ensure that personnel have sufficient skills and authority which adequately cover all the requirements related to the assurance claim, and which address achieving the assurance claim and showing the achievement. <b)4)>; outcome [d)]

NOTE 3 This action invokes the human resource management process, task 6.2.4.3.a.1: Identify skill needs based on current and expected projects.

The project plan should include planning to achieve assurance claim, to help ensure that project progress enables to achieve the assurance claim in a timely manner, and to deal with the potential effects from vulnerabilities and weaknesses that can affect achievement of the assurance claim. <a)3), a)4), b)1)>; outcome [d)]

The project should clarify the tasks and responsibility with respect to the assurance claim. <a)4), b)4)>; outcome [d)]

The project should incorporate decision points and milestones to manage cost, schedule, and performance risks associated with uncertain, ambiguous and emerging requirements that contribute to achieving the assurance claim. These decision points should be at the relevant points in the project so that important decisions and requirements from stakeholders are not postponed, regardless of their complexity. <b)3)>; outcome [d)]

The project objectives should include assurance objectives. <a)1)>; outcome [a), d)]

The assurance objectives should include constraints caused by the laws, regulations and standards. The activities and tasks for obtaining necessary licenses or certifications should be included in the project plan. <a)1)>; outcome [c)]

EXAMPLE 1 If the assurance claim is related to safety, obtaining required safety certifications can be reflected in project planning.

NOTE 4 The assurance objectives are determined by the considerations of:

a) the dangers, adverse consequences, harm, threats, and hazards that are to be managed or affected by the system, and

b) the tolerable values of the variables related to the assurance claim and maximum acceptable uncertainties of them.

The project should specify responsibilities for reporting and management of issues for the assurance claim. <b)4)>; outcome [d)]

The project should determine the ancillary actions required for showing achievement of the assurance claim, and calculate the cost, timescales and resources necessary for their completion. The goal for these ancillary actions should be given quantitatively whenever possible. Quantitative estimation is

preferable for evaluation of achievement in the operation process. The evaluation of achievement should be continued throughout the life cycle as needed. <a)3), a)4), a)5)>; outcome [f)]

EXAMPLE 2 In the nuclear industry, safety monitoring is continued throughout the life cycle.

Care should be taken when the project uses commercial off-the-shelf (COTS) items because their effect to achievement of the assurance claim and its demonstration is often beyond control of the project. Where customization is required, particular attention should be given to ensuring that the assurance claim is not invalidated. <a)3), a)4), a)5)>; outcome [d)]

NOTE 5 Evaluation of the use of COTS and bespoke products can be done in the design definition process.

### 6.5.7 Project assessment and control process

The purpose of the project assessment and control process is to assess if the plans are aligned and feasible; determine the status of the project, technical and process performance, and direct execution to help ensure that the performance is according to plans and schedules, within projected budgets, to satisfy technical objectives (ISO/IEC/IEEE 15288:2015, 6.3.2.1).

The primary stakeholders should endeavour to ensure that the project plan is feasible from the aspect of achievement of the assurance claim, and will be so through replanning of the project. <a), c)>; outcome [d)]

### 6.5.8 Decision management process

The purpose of the decision management process is to provide a structured, analytical framework for objectively identifying, characterizing and evaluating a set of alternatives for a decision at any point in the life cycle and select the most beneficial course of action (ISO/IEC/IEEE 15288:2015, 6.3.3.1). The decision management process should help ensure that the consequences of achieving the assurance claim and showing the achievement are considered whenever a decision is made.

The project should include decisions related to the assurance claim as a category of decision types in the decision management strategy. <a)1)>; outcome [d)]

Decision criteria for trade-offs and other decisions should protect the assurance claim and should involve the stakeholders relevant to the assurance claim. <a), b)>; outcome [d)]

The decision management strategy should help ensure that any effects on achieving the assurance claim and showing the achievement are included in the evaluation of consequences and associated risks of alternative actions in decisions affecting policies, procedures, plans, personnel, environment, products, services, and critical supporting infrastructure. <a)1)>; outcome [d), f)]

Once a decision relevant to the assurance claim has been made, its effect should be reflected in the approaches to showing their achievement. <c)3)>; outcome [f)]

### 6.5.9 Risk management process

The purpose of the risk management process is to identify, analyze, treat and monitor the risks continually. The risk management process is a continual process for systematically addressing risk throughout the life cycle of a system product or service. It can be applied to risks related to the acquisition, supply, development, maintenance or operation of a system (ISO/IEC/IEEE 15288:2015, 6.3.4.1).

NOTE 1 The source of the paragraph above is ISO/IEC/IEEE 15288. The word “supply” is added to the last sentence.

The risk management strategy should include determination of the required degree of confidence in achievement of the assurance claim. <a)1)>; outcome [b)]

Managing risks that are related to the assurance claim should be thoroughly integrated throughout the risk management process in priority setting, decision making, establishing and maintaining the risk profile, and risk treatment. <a), b), c), d), e)>; outcome [d)]

The assurance information can be used as a framework for organizing and addressing the risks related to the assurance claim. <a)1), b)1), b)2), c)1), c)2), c)3)>; outcome [d)]

When establishing a risk profile, emphasis should be given to causal factors and conditions for their occurrence, warning signs and indications of emerging risks relating to achievement of the assurance claim. <b)2)>; outcome [b), d)]

Practices to analyse and mitigate adverse effects on achievement of the assurance claim should be developed and used when suppliers of off-the-shelf or bespoke products make changes to these products without providing detailed information about those changes. <c)1), c)2), c)3), c)4)>; outcome [d)]

The risk that the required degree of confidence is not achieved should be taken into consideration. <c)>; outcome [d)]

The possibilities of failing to achieve the assurance claim and failing to show this achievement to an acceptable extent should be realistically considered, including the risks of having to redevelop parts of the system. <c)4)>; outcome [d)]

The project should evaluate the potential for not being able to achieve the assurance claim in a timely manner, resulting in a risk to the system certification or accreditation or resulting in the system not being used as intended. <c)1, c)2)>; outcome [d)]

Contingency action in the event that the assurance claim cannot be achieved in a timely manner should be identified, planned, and approved by the relevant stakeholders. <c)4)>; outcome [d)]

Careful attention should be given to difficulties in provision of needed evidence for achievement of the assurance claim, in ensuring prompt reporting and assessment of reports, and in maintenance of complete records. <c)4)>; outcome [e)]

The risk profile should include information necessary for obtaining the degree of confidence. This includes the tolerable risk, potential adverse consequences, dangerous conditions, risk sources, and the residual risk. <b)2)>; outcome [b)]

In order to determine the required degree of confidence, the risk management strategy can include the following actions:

a) determine risk criteria and the tolerable risk of the system-of-interest; <a)1)>; outcome [b)]

b) analyse risks of the system-of-interest and record the result to the risk profile; <b)2), c)>; outcome [b)]

c) give a structure of the risk reduction measures, including the one implemented by the system-of-interest; <c)4)>; outcome [b)]

d) evaluate risks and record the result to the risk profile; <c)3)>; outcome [b)]

e) determine the required degree of confidence in achievement of the assurance claim with acceptable risk and emphasize the consequence of risks to support the decision on required degree of confidence in achievement of the assurance claim. <d)2)>; outcome [b)]

### 6.5.10 Configuration management process

The purpose of configuration management (CM) is to manage and control system elements and configurations over the life cycle. CM also manages consistency between a product and its associated configuration definition (ISO/IEC/IEEE 15288:2015, 6.3.5.1). CM is concerned with assurance information in the following two ways:

— Descriptions in configuration management are part of assurance information.

— Assurance information itself is managed by the configuration management process.

The configuration management strategy should determine means to extract information relevant to the assurance claim from the configuration management process and to incorporate it into the assurance information. Maintenance should include this action. The configuration management strategy should also provide protection of configuration item data and meta-data, both in repositories and under modification. <a)1)>; outcome [d)]

The project should identify the assurance information and periodically combine it into an identified configuration to constitute an organized version of the assurance information. Review and audit of the configuration management process should recommend corrective and preventive actions against accidental or unauthorized modifications of the assurance information. <a)1), b)1), c)1), c)2), c)3), c)4)>; outcome [a), b), c), e), f)]

The configuration management strategy should facilitate the achievement of the assurance claim and its demonstration. At a minimum, the following should be addressed:

— employing rigor and protective measures that are commensurate with the criticality of the system, the data, the mission and the assurance argument, and are flexible enough to enable a wide variety of threats to be addressed;

— adjusting granularity within the configuration management process to support the approach to showing achievement of the assurance claim. <a)1)>; outcome [d)]

The Configuration management process should be tailored if it is necessary for this facilitation. <a)1)>; outcome [d)]

The project should establish and maintain required confidentiality, integrity, availability, authentication, accountability (including non-repudiation), and auditability of the assurance information. <a)1)>; outcome [d)]

The primary stakeholders should endeavour to ensure consistency of integrity and security of the configuration with the assurance information <a)1)>; outcome [d)]

Access control, distribution control, storage, and protection should be maintained throughout the product or service life cycle. <d)1), d)2)>; outcome [d)]

The arguments and supporting evidence should be built, collected, and maintained throughout the life cycle and are typically derived from multiple sources. <b)3), c)2)>; outcome [e), f)]

The primary stakeholders should endeavour to ensure consistency of integrity and security of the configuration with the approach to showing achievement of the assurance claim. <c)2), d)1)>; outcome [f)]

### 6.5.11 Information management process

The purpose of the information management process is to generate, obtain, confirm, transform, retain, retrieve, disseminate and dispose of information, to designated stakeholders (ISO/IEC/IEEE 15288:2015, 6.3.6.1). The information management process provides the relevant stakeholders including regulatory or approval authorities with the assurance information.

The defined items of information that will be managed should include the assurance information. <a)2)>; outcome [a), b), c), e), f)]

NOTE 1 ISO/IEC 15026-2 provides a structure for this information.

When an assurance claim concerns “safety” or “security”, the assurance information should provide an argument covering the full required scope for the safety or security. <a)2)>; outcome [f)]

The project should collect, organize, and analyse the following information in addition to the assurance information:

— information and evidence not necessarily directly related to the system-of-interest, including information about prior versions of the system-of-interest, information about similar systems, assurance patterns, templates or exchangeable assurance information elements relevant to the system-of-interest, and arguments to mitigate risks and justifications for using that argument,

— information concerning the validity and integrity of the assurance information, and

— information and reports about failure, human errors, faults, weaknesses, and incidents as regards the assurance claim.

The information in the first item above should be generated for both successes and failures. <a)2), a)4)>; outcome [f)]

The project should plan for independent reporting regarding the assurance claim. In particular, the following should be specified:

— documentation of reports and issues regarding the assurance claim, and

— coordination of reporting and dissemination of information regarding the assurance claim.

The reporting of dissemination of information regarding the assurance claim should be coordinated not only throughout the organization but the customers and suppliers should be involved as needed. <a)2), a)5)>; outcome [a), f)]

The project should preserve integrity and validity of assurance information and, in order to do so, should conduct management and control the information. This includes:

— protecting assurance information from malicious and non-malicious actions,

— limiting access to sensitive information such as information about threat and hazard,

— maintaining the required confidentiality, and

— responding to incidents involving the assurance information. <b)2), b)5)>; outcome [e), f)]

Whenever a change is made in the information related to the assurance claim, the part of the agreement that is relevant to the change and the relationship between the change and the relevant part of the agreement should be clarified. <b)2)>; outcome [e), f)]

NOTE 2 This action invokes change management in the configuration management process and the agreement processes.

### 6.5.12 Quality assurance process

The purpose of the quality assurance process is to help ensure the effective application of the organization's quality management process to the project (ISO/IEC/IEEE 15288:2015, 6.3.8.1).

Quality assurance is relative to quality requirements, while assurance as provided in this document is relative to the assurance claim. The primary stakeholders should sort out output of the quality assurance process that can be used as evidence of achievement of the assurance claim, so that they can also be used for this process view. <d)>; outcome [e), f)]

### 6.5.13 Business or mission analysis process

The purpose of the business or mission analysis process is to define the business or mission problem or opportunity, characterize the solution space, and determine potential solution class(es) that could address a problem or take advantage of an opportunity (ISO/IEC/IEEE 15288:2015, 6.4.1.1).

The primary stakeholders should endeavour to ensure that the approach to showing the achievement of the assurance claim is reconciled in the context of the business to be conducted with the system. <a)2), b)2)>; outcome [e), f)]

### 6.5.14 Stakeholder needs and requirements definition process

The purpose of the stakeholder needs and requirements definition process is to define the stakeholder requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment. It identifies stakeholders, or stakeholder classes, involved with the system throughout its life cycle, and their needs, expectations, and desires. It analyses and transforms these into a common set of stakeholder requirements. As a subset of stakeholder requirements, critical properties required for achievement of the assurance claim are identified and documented. (ISO/IEC/IEEE 15288:2015, 6.4.2.1).

The assurance claim should be selected by analysis of the complete set of stakeholder requirements. The project should aid this selection from the technical point of view by, for instance, identifying additional risks, consequences and related uncertainties, and compliance requirement. <d)2)>; outcome [a)]

NOTE 1 As stakeholders define their requirements, some will emerge as requiring high confidence in their achievement because they are associated with important consequences, risks, regulations or other mandates (e.g. anti-tamper, security), relating to properties of the system. Requirements requiring high confidence can be used to identify the assurance claim.

The project should prioritize sub-claims of the assurance claim in order to select the critical sub-claims, when not all sub-claims can be achieved and to pursue the next best measure is the only choice. <e)1), e)2)>; outcome [d), f)]

NOTE 2 The assurance claim can be formed as conjunction of sub-claims, so that the achievement of all sub-claims entails the achievement of the assurance claim. The sub-claims created by this action and the justification and rationale for their selection can be documented as part of the assurance information and maintained for later investigation when necessary.

The documentation of prioritization and maintenance of its rationale is done as a part of maintaining stakeholder requirements traceability to the sources of stakeholder need. <f)2)>; outcome [d), f)]

The project should provide support to stakeholders as required, so as to help achievement of the assurance claim. <d)2)>; outcome [d)]

NOTE 3 Some stakeholders do not have a technical background and need technical assistance in defining stakeholder requirements or in negotiation to resolve conflicting stakeholder requirements. Explicit interpretation of the stakeholder's requirements and the technical application of those requirements would be necessary to ensure a common understanding among both technical and non-technical stakeholders.

The stakeholders should agree that they all share the responsibility for the definition of stakeholder requirements. When requested, they should provide necessary information such as their own needs. If the system analyst has responsibility for eliciting requirements, other stakeholders should be responsible for cooperating and collaborating with the analyst. <d)2)>; outcome [d)]

Although essential requirements are defined and confirmed under the Stakeholder requirements definition process, they are subject to change as a result of resolving conflicts between requirements of different stakeholders and limitations from the system considerations when conducting the activities of the System requirements definition process. The activities and tasks of these two processes are, therefore, conducted iteratively. Due to cost, schedule, and other constraints or changes in stakeholder needs, requirements will evolve. As agreements on changes in requirements are made, impacts on the ability to achieve agreements related to the critical properties should also be addressed, although an agreement should be respected and should not be changed too easily, even if no legal or financial action results. <all activities>; outcome [d)]

NOTE 4 Refer to ISO/IEC/IEEE 29148:2018, Clause 5, for more discussion of the iterative nature of these activities and tasks.

Among stakeholders, those who need to share an understanding of the risks of the system-of-interest should be identified. <a)>; outcome [d)]

The source (typically a standard) that provides the set of degrees of confidence should be identified. <b)2)>; outcome [b)]

NOTE 5 The set of degrees of confidence can be a set of integrity levels as defined in ISO/IEC 15026-3.

The stakeholder needs should entail the determination of the required degree of confidence. <b)2)>; outcome [b)]

NOTE 6 The required degree of confidence determined here can be integrity level as provided in ISO/IEC 15026-3.

The specified set of stakeholder requirements should yield the required degree of confidence in achievement of the assurance claim. <d)2)>; outcome [d)]

Simultaneously with the selection of the assurance claim, the project should preliminarily define means for showing achievement of the assurance claim paying particular attention to trade-offs related to stakeholder tolerance for risks. Stakeholders should identify their tolerance for failure, degradation, and compromise or loss, e.g. degraded modes of operation. The project also should identify any cultural, social, and organizational context of the system that can affect achievement of the assurance claim or showing the achievement. <d)2), f)1)>; outcome [f)]

NOTE 7 This activity is aided by using experience and records regarding previous versions of the system-of-interest, systems similar to it, assurance patterns/templates or exchangeable assurance information elements relevant to the system-of-interest, operational environments of the system, or known intentions or predictions regarding the use of the system in its environment.

The primary stakeholders should endeavour to ensure that decisions necessary in the later stages of the life cycle are based on the stakeholder requirements defined in this process. <e)1)>; outcome [d)]

NOTE 8 This action invokes the decision management process.

The primary stakeholders should endeavour to ensure the involvement of all relevant stakeholders (e.g. those stakeholders familiar with the business need for the critical property and knowledge of the critical property) in requirements definition to keep the introduction of additional stakeholder requirements to a minimum in later stages of the life cycle. <f)1)>; outcome [d)]

NOTE 9 Collaboration is essential in defining the purpose of the system product (e.g. new business enabled by the new system). The project personnel have the system or software development technology knowledge but no detailed image of the use of the system, while the acquirers, customers, or users understand what the use of the system would be without the technical skill to build it.

The primary stakeholders should endeavour to ensure that the approach to achieving the assurance claim is reconciled in the context of the business or concept of operations to be conducted with the software. <c)>; outcome [d)]

Stakeholder needs and requirements are a key input to the risk management process. Stakeholder needs and requirements related to risks, tolerability of risks, required degree of confidence in achievement of the assurance claim and requirements that, when met, will provide the required degree of confidence in achievement of the assurance claim should be identified and provided as input to the risk management process. <d)2)>; outcome [d)]

The following actions help achievement of the assurance claim by improving communication between stakeholders and reducing the likelihood of misunderstanding between stakeholders.

a) During the analysis of the stakeholder requirements, the fact that each stakeholder has their own circumstance and set of values should be taken into account. <a)>; outcome [d)]

   The project should work across the set of technology-knowledgeable stakeholders to determine the feasibility of requirements across the lifecycle. The full life cycle should be considered to determine the requirements feasibility and avoid modifications that drive undesirable changes in costs,

schedule and/or performance later in the lifecycle when more technical detail about the system is known.

b) The stakeholder requirements should be stated as simply as possible in order to make the achievement of the critical properties easier to be shown. <b)>; outcome [d)]

c) The project should try to minimize both the number of work items that are necessary but not listed in the stakeholder requirements and any duplication of work items in the stakeholder requirements. <d)3)>; outcome [d)]

The assurance claim should include claim that necessary standards relevant to the critical properties are considered in the stakeholder requirements. <b)1), b)2)>; outcome [a)]

### 6.5.15 System requirements definition process

The purpose of the system requirements definition process is to transform the stakeholder, user-oriented view of desired capabilities into a technical view of a solution that meets the operational needs of the user (ISO/IEC/IEEE 15288:2015, 6.4.3.1).

The required values for the variables used in the assurance claim should be defined in the system requirements definition process. The following items should be explicitly specified in the system requirements, in so far as they are related to the assurance claim:

— the functional boundary of the system;

— the functions;

— implementation constraints;

— the critical performance measures;

— system requirements in terms of values for variables pertaining to the assurance claim;

— the priority among the system requirements;

— the maintenance of traceability of the system requirements. <b)2), b)3), b)4)>; outcome [d)]

EXAMPLE If functional safety is chosen as the critical property, the part of system requirements required to be specified in this process view would be “safety lifecycle requirements,” as described in IEC 61508-1.

The constraints for the system environment required to achieve the assurance claim and to show the achievement should be identified by performing analysis of risks or consequences. This analysis should be facilitated by the following information for each sub-claim of the assurance claim:

— risks associated with the system not achieving the assurance claim;

— allowed values of variables related to the sub-claim;

— allowable degree of uncertainty related to the sub-claim and its achievement;

— applicable conditions related to the sub-claim. <c)1)>; outcome [a), e), f)]

Before the assurance claim is selected and validated, the project should review the system requirements related to the assurance claim and determine:

— whether they are consistent with stakeholder requirements, and

— whether they have adequately captured those critical properties the violation of which has severe consequences and for which stakeholders require high confidence. <a), b)>; outcome [a), d)]

The project should document the assurance claim and their relationships to stakeholder and system requirements that justify them. <c)1)>; outcome [a), d)]

The system requirements should be unambiguous and well examined, so that the risk of misunderstanding about the assurance claim is reduced. <b)4)>; outcome [d)]

NOTE See ISO/IEC/IEEE 29148 for additional guidance on the characteristics of good requirements.

The system requirements should reflect the risk reduction measures established by the risk management process. <b)3)>; outcome [d)]

The system requirements should also capture the necessary degree of confidence in achievement of the assurance claim, and the requirements, when met, that will provide the required degree of confidence in achievement of the assurance claim. <b)3)>; outcome [b), d)]

The explicit agreement on the system requirements and its traceability should be provided whenever it is necessary to show the achievement of the assurance claim. <d)1), d)2)>; outcome [e)]

### 6.5.16 Architecture definition process

The purpose of the architecture definition process is to generate system architecture alternatives, to select one or more alternative(s) that frame stakeholder concerns and meet system requirements, and to express this in a set of consistent views (ISO/IEC/IEEE 15288:2015, 6.4.4.1).

Each architecture alternative should enable the system to achieve the assurance claim <c)1), c)2), c)4)>; outcome [d)].

Information produced in this process and required as evidence of achievement of the assurance claim or required for showing achievement of the assurance claim should be provided. <c)1), c)2), c)4)>; outcome [e), f)]

The architecture definition and evaluation strategy, as well as traceability of the architecture, should be provided whenever it is necessary to show the achievement of the assurance claim. <f)5), f)6)>; outcome [e)]

### 6.5.17 Design definition process

The purpose of the design definition process is to provide sufficient detailed data and information about the system and its elements to enable the implementation consistent with architectural entities as defined in models and views of the system architecture (ISO/IEC/IEEE 15288:2015, 6.4.5.1).

The project should evaluate the use of off-the-shelf and bespoke products as elements according to the project needs. <c)>; outcome [d)]

NOTE The effect of use of COTS and bespoke products can be done in the project planning process.

The map of design characteristics to the system elements, design document and its rationale, and traceability of design should be provided whenever it is necessary to show the achievement of the assurance claim. <d)2), d)3)>; outcome [e)]

### 6.5.18 System analysis process

The purpose of the system analysis process is to provide a rigorous basis of data and information for technical understanding to aid decision-making across the life cycle (ISO/IEC/IEEE 15288:2015, 6.4.6.1).

The degree of confidence in achievement of the assurance claim identified in outcome b) of this process view should be considered in the definition of level of fidelity of system analysis, assuming the result of system is used in the argument f) of this process view. <a)3)>; outcome [b)]

The traceability of system analysis results should be provided whenever it is necessary to show the achievement of the assurance claim. <c)1)>; outcome [e)]

### 6.5.19 Implementation process

The purpose of the implementation process is to realize a specified system element (ISO/IEC/IEEE 15288:2015, 6.4.7.1).

The objective evidence that the system element meets system requirements, implementation results and encountered anomalies, as well as traceability of the implemented system elements, should be provided whenever it is necessary to show the achievement of the assurance claim. <b)3), c)1), c)2)>; outcome [e)]

### 6.5.20 Integration process

The purpose of the integration process is to synthesize a set of system elements into a realized system (product or service) that satisfies system requirements, architecture, and design (ISO/IEC/IEEE 15288:2015, 6.4.8.1).

The project should check that the result of integration achieves the assurance claim. <b)3)>; outcome [d)]

Recorded integration results and encountered anomalies, as well as traceability of the integrated system elements, should be provided whenever it is necessary to show the achievement of the assurance claim. <c)1), c)2)>; outcome [e)]

### 6.5.21 Verification process

The purpose of the verification process is to provide objective evidence that a system or system element fulfils its specified requirements and characteristics (ISO/IEC/IEEE 15288:2015, 6.4.9.1). The verification plan should be consistent with the strategy for achieving the assurance claim and showing the achievement.

The primary stakeholders should endeavour to ensure that the verification plans, activities and decisions contribute to achieving the assurance claim with confidence to the required degree. The effect of reliability of means and tools to the uncertainty of achieving the assurance claim should be considered. <a)4), a)5)>; outcome [b)]

The verification plan should be consistent with the plans for achieving the assurance claim and for showing the achievement. In particular, it includes:

— identification of verification criteria,

— measurement criteria,

— means to resolve problems related to the assurance claim, and

— means to let the assurance information reflect the resolution of the problems. <a)4)>; outcome [d), e), f)]

Recorded verification results and encountered anomalies, operational incidents and problems and their resolution, and traceability of the verified system elements should be provided whenever it is necessary to show the achievement of the assurance claim. <c)1), c)2), c)4)>; outcome [e)]

### 6.5.22 Transition process

The purpose of the transition process is to establish a capability for a system to provide services specified by stakeholder requirements in the operational environment (ISO/IEC/IEEE 15288:2015, 6.4.10.1).

The assurance claim should be demonstrated with respect to the result of installation. <b)4), b)7), b)8)>; outcome [d)]

Recorded transition results and encountered anomalies, operational incidents and problems and their resolution, and traceability of the transitioned system elements should be provided whenever it is necessary to show the achievement of the assurance claim. <c)1)>; outcome [e)]

### 6.5.23 Validation process

The purpose of the validation process is to provide objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment (ISO/IEC/IEEE 15288:2015, 6.4.12.1).

The validation plan should be sufficient to obtain confidence in achievement of the assurance claim to the required degree. <a)6)>; outcome [b)]

Recorded validation results and encountered anomalies, operational incidents and problems and their resolution, and traceability of the validated system elements should be provided whenever it is necessary to show the achievement of the assurance claim. <c)1)>; outcome [e)]

### 6.5.24 Operation process

The purpose of the operation process is to use the system to deliver its services a capability for a system to provide services (ISO/IEC/IEEE 15288:2015, 6.4.12.1). The operation plan should include plans for achieving the assurance claim and showing the achievement.

The operation plan should provide for regular audits of operation records to verify that there is no evidence that the system or the demonstration of the achievement of the assurance claim have been unknowingly subverted. <a)1), a)2), a)5)>; outcome [e), f)]

The plan should include adequate measures that prevent harm or loss of sensitive information related to the assurance claim even if the control of the system is lost or transferred. <a)1)v)>; outcome [d)]

The project should establish reporting systems and procedures for investigation and disposition of incidents related to the assurance claim. Examples of such incidents are:

— attempted violations and violations of the assurance claim,

— product vulnerabilities or weakness that can contribute to violations, and

— new sources of danger potentially resulting in violation of the assurance claim throughout the life cycle. <c)2)>; outcome [d)]

Appropriate safeguards should be put in place for required confidentiality when communicating the plan and reporting the incidents above. <b)3)>; outcome [d)]

The operation plan should conform to the operational restrictions that derive the assumptions of the argument showing achievement of the assurance claim. The operation plan should also prescribe that violations of those operational restrictions are reported, recorded, and resolved. The operation plan should also contain training information on how to establish and maintain compliance with those operational restrictions. <a)1)>; outcome [d)]

Results of operation and any anomalies encountered, operational incidents and problems and their resolution, and traceability of the operations elements should be provided whenever it is necessary to show the achievement of the assurance claim. <c)1), c)2), c)3>; outcome [e)]

The operation plan should cope with changes in operational conditions even if it is not encompassed in the assurance claim; for that purpose, the plan should prescribe the means to modify the approach to showing achievement of the claim and the related assurance information so as to reflect the changes. <a)1), c)2)>; outcome [d)]

The operation plan should include assessment of effects of changes in the system or its operational environment on the usability related to the assurance claim and on assumptions of the assurance argument. <a)1)>; outcome [d)]

### 6.5.25 Maintenance process

The purpose of the maintenance process is to sustain the capability of the system to provide a service (ISO/IEC/IEEE 15288:2015, 6.4.13.1). The maintenance plans should include plans for continual achievement of the assurance claim throughout the life cycle.

The maintenance plan should provide for evaluation of the effect of changes of the system or system elements on information related to the assurance claim. <a)1)>; outcome [d)]

The plan should include provision for the controlled update and release of artefacts related to the assurance claim. <a)1)>; outcome [d)]

The maintenance plan should include assessment of the effects of changes in the system or its operational environment, e.g. on usability, that can impact the assurance claim. This assessment should include ongoing measurement of the critical properties when maintenance changes are made. <a)1), b)1), b)7)>; outcome [d)]

NOTE 1 Effect of changes to assurance claim is assessed by invoking change management activities of the configuration management process. This includes examination of the plan as well as the result of change.

Implication of change should be disseminated widely and should be clear, concise and comprehensible. <b)>; outcome [d)]

NOTE 2 Such information can be disseminated by means of formal reports to management personnel, safety newsletters, bulletins, and training. This is accomplished by invoking the information management process.

The maintenance plan should provide measures to prevent replacement, retirement, or disposal of parts or components of the system from compromising achievement of the assurance claim. <a)1), a)4)>; outcome [d)]

The maintenance plan should have provisions for informing the risk management strategy of risk information related to the assurance claim and guidance related to modifications, workarounds, and other risks related to maintenance. <a)1), d)2), d)5)>; outcome [d)]

In order to maintain the achievement of the assurance claim, a risk assessment or analysis of effects related to the assurance claim of these changes should be performed. <b)1), b)5), b)6), b)7)>; outcome [d)]

All proposed product changes, including changes to requirements not related to the assurance claim, design, and components, should undergo analyses of impact related to the assurance claim.

The maintenance plan should include resources for updating the assurance argument and assurance information as required, including new evidence. <b)1), b)7)>; outcome [e), f)]

Maintenance and logistics results and any anomalies encountered, operational incidents and problems ant their resolution, trends of incidents and problems in maintenance and logistics actions, and traceability of the maintenance elements should be provided whenever it is necessary to show the achievement of the assurance claim. <d)1), d)2), d)3), d)4)>; outcome [e)]

### 6.5.26 Disposal process

The purpose of the disposal process is to end the existence of a system element or system for a specified intended use, appropriately handle replaced or retired elements, and to properly attend to identified critical disposal needs (e.g. per an agreement, per organizational policy, or for environmental, legal, safety, security aspects) (ISO/IEC/IEEE 15288:2015, 6.4.14.1).

The primary stakeholders should examine whether the result of the disposal process is relevant to the assurance claim and, if there is anything relevant, should endeavour to ensure that the disposal process contributes to achievement of the assurance claim. <a)1), c)2), c)3)>; outcome [d)]

NOTE An example of the result that can be relevant to the assurance claim is the data stored in the systems. The assurance claim can require that such data be scrapped appropriately so as to keep security and privacy of the users.

# 7 Software assurance process view

## 7.1 General

This clause provides the software assurance process view. 7.2 provides its purpose; 7.3 provides its outcomes; 7.4 identifies the processes, activities and tasks that implement the process view; and 7.5 provides guidance about and recommendations for some of the processes that implement the process view. Since all processes of ISO/IEC/IEEE 12207 are applied iteratively and recursively in the life cycle, the guidance and recommendations should also be applied iteratively and recursively.

NOTE 1 ISO/IEC/IEEE 12207:2017, E.6 describes the process view for software assurance (information security). Although its process view name is identical to the process view being defined in this clause, the two process views are defined independently of each other and their purposes are completely different.

NOTE 2 See ISO/IEC/IEEE 24748-1 for more information about life cycle models and the iteration and recursion of processes.

NOTE 3 Performance of the software 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.

## 7.2 Purpose

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

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

## 7.3 Outcomes

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

a) the assurance claim for the software 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 software 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.

## 7.4 Processes, activities and tasks that implement the software assurance process view

Table 1 shows the ISO/IEC/IEEE 12207 life cycle processes that should be applied in order to achieve outcomes of the software assurance process view.

The processes, activities, and tasks of ISO/IEC/IEEE 12207 that should be used to achieve the outcomes provided in 7.3 are provided in the list below with their respective ISO/IEC/IEEE 12207:2017 subclause numbers. Table 1 shows the processes that contain activities or tasks listed below. Guidance and recommendations with respect to some of these tasks are given in 7.5.

NOTE The five processes which are discussed in 7.5 are marked with an asterisk (*) in the following list.

- 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, as necessary. (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 or if its priority has changed. (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)
  - Select the software system elements to be uniquely identified as configuration items subject to configuration control. (6.3.5.3.b.1)

- Perform configuration change management. (6.3.5.3.c)
- Perform release control. (6.3.5.3.d)
- Develop and maintain the CM status information for software system elements, baselines, and releases. (6.3.5.3.e.1)
- Capture, store and report configuration management data. (6.3.5.3.e.2)

— Information management process (6.3.6)

- Define the items of information that will be managed. (6.3.6.3.a.2)
- Designate authorities and responsibilities for information management. (6.3.6.3.a.3)
- Define information maintenance actions. (6.3.6.3.a.5)
- Maintain information items and their storage records, and record the status of information. (6.3.6.3.b.2)
- Dispose of unwanted, invalid or unvalidated information. (6.3.6.3.b.5)

— Quality assurance process (6.3.8)

- Create records and reports related to quality assurance activities. (6.3.8.3.d.1)
- Maintain, store, and distribute records and reports. (6.3.8.3.d.2)
- Identify incidents and problems associated with product, service, and process evaluations. (6.3.8.3.d.3)

— Business or mission analysis process (6.4.1)

- Define the business or mission analysis strategy. (6.4.1.3.a.2)
- Define the mission, business, or operational problem or opportunity. (6.4.1.3.b.2)
- Maintain traceability of business or mission analysis. (6.4.1.3.e.1)

— Stakeholder needs and requirements definition process (6.4.2)

- Prepare for stakeholder needs and requirements definition. (6.4.2.3.a)
- Define stakeholder needs. (6.4.2.3.b)
- Define context of use within the concept of operations and the preliminary life cycle concepts. (6.4.2.3.b.1)
- Identify stakeholder needs. (6.4.2.3.b.2)
- Develop the operational concept and other life cycle concepts. (6.4.2.3.c)
- Identify the stakeholder requirements and functions that relate to critical quality characteristics, such as assurance, safety, security, environment, or health. (6.4.2.3.d.2)
- Define stakeholder requirements, consistent with life cycle concepts, scenarios, interactions, constraints, and critical quality characteristics. (6.4.2.3.d.3)
- Analyze the complete set of stakeholder requirements. (6.4.2.3.e.1)
- Define critical performance measures that enable the assessment of technical achievement. (6.4.2.3.e.2)
- Obtain explicit agreement on the stakeholder requirements. (6.4.2.3.f.1)

  - Maintain traceability of stakeholder needs and requirements. (6.4.2.3.f.2)
- System/software requirements definition process (6.4.3)*
  - Prepare for system/software requirements definition. (6.4.3.3.a)
  - Define system/software requirements. (6.4.3.3.b)
  - Define each function that the software system or element is required to perform. (6.4.3.3.b.1)
  - Define necessary implementation constraints. (6.4.3.3.b.3)
  - Identify requirements that relate to risks, criticality of the software system, or critical quality characteristics. (6.4.3.3.b.4)
  - Define system/software requirements and requirements attributes. (6.4.3.3.b.5)
  - Analyze system/software requirements. (6.4.3.3.c)
  - Analyze the complete set of system/software requirements. (6.4.3.3.c.1)
  - Manage system/software requirements. (6.4.3.3.d)
  - Obtain explicit agreement on the system/software requirements. (6.4.3.3.d.1)
  - Maintain traceability of the system/software requirements. (6.4.3.3.d.2)
- Architecture definition process (6.4.4)
  - Define the system context and boundaries in terms of interfaces and interactions with external entities. (6.4.4.3.c.1)
  - Identify architectural entities and relationships between entities that address key stakeholder concerns and critical software system requirements. (6.4.4.3.c.2)
  - Select, adapt, or develop models of the candidate architectures of the system. (6.4.4.3.c.4)
  - Maintain the architecture definition and evaluation strategy. (6.4.4.3.f.5)
  - Maintain traceability of the architecture. (6.4.4.3.f.6)
- Design definition process (6.4.5)*
  - Identify candidate alternatives for software system elements. (6.4.5.3.c.2)
  - Capture the design and rationale. (6.4.5.3.d.1)
  - Establish traceability between the detailed design elements, the system/software requirements, and the architectural entities of the software system architecture. (6.4.5.3.d.2)
- System analysis process (6.4.6)
  - Define the scope, objectives, and level of fidelity of the analysis. (6.4.6.3.a.3)
  - Maintain traceability of analysis results. (6.4.6.3.c.1)
- Implementation process (6.4.7)
  - Record objective evidence that the software system element meets system requirements. (6.4.7.3.b.6)
  - Record implementation results and anomalies encountered. (6.4.7.3.c.1)

  - Maintain traceability of the implemented system elements. (6.4.7.3.c.2)
- Integration process (6.4.8)
  - Check that the integrated software interfaces or functions run from initiation to an expected termination within an expected range of data values. (6.4.8.3.b.3)
  - Record integration results and anomalies encountered. (6.4.8.3.c.1)
  - Maintain traceability of the integrated system elements. (6.4.8.3.c.2)
- Verification process (6.4.9)*
  - Define the verification strategy. (6.4.9.3.a.1)
  - Identify constraints from the verification strategy to be incorporated in the system/software requirements, architecture, or design. (6.4.9.3.a.2)
  - Review verification results and anomalies encountered and identify follow-up actions. (6.4.9.3.c.1)
  - Record incidents and problems during verification and track their resolution. (6.4.9.3.c.2)
  - Maintain traceability of the verified software system elements. (6.4.9.3.c.4)
- Transition process (6.4.10)
  - Demonstrate proper installation of the software system. (6.4.10.3.b.5.i)
  - Demonstrate the installed or transitioned product is capable of delivering its required functions. (6.4.10.3.b.5.ii)
  - Demonstrate the functions provided by the system are sustainable by the enabling systems. (6.4.10.3.b.5.iii)
  - Record transition results and anomalies encountered. (6.4.10.3.c.1)
  - Record transition incidents and problems and track their resolution. (6.4.10.3.c.2)
  - Maintain traceability of the transitioned system elements. (6.4.10.3.c.3)
- Validation process (6.4.11)
  - Identify and plan for the necessary enabling systems or services needed to support validation. (6.4.11.3.a.5)
  - Record validation results and anomalies encountered. (6.4.11.3.c.1)
  - Record incidents and problems during validation and track their resolution. (6.4.11.3.c.2)
  - Maintain traceability of the validated system elements. (6.4.11.3.c.4)
- Operation process (6.4.12)
  - Define an operation strategy. (6.4.12.3.a.1)
  - Identify system constraints from operation to be incorporated in changes to the system/software requirements, architecture, design, implementation, or transition. (6.4.12.3.a.2)
  - Identify or define training and qualification requirements for personnel needed for system operation. (6.4.12.3.a.5)
  - Monitor system operation. (6.4.12.3.b.3)
  - Record results of operation and anomalies encountered. (6.4.12.3.c.1)

  - Record operational incidents and problems and track their resolution. (6.4.12.3.c.2)
  - Maintain traceability of the operational services and configuration items. (6.4.12.3.c.3)
- Maintenance process (6.4.13)*
  - Define a maintenance strategy. (6.4.13.3.a.1)
  - Identify and plan for the necessary enabling systems or services needed to support maintenance. (6.4.13.3.a.5)
  - Perform maintenance. (6.4.13.3.b)
  - Review stakeholder requirements, complaints, events, incident and problem reports to identify corrective, adaptive, perfective and preventive maintenance needs. (6.4.13.3.b.1)
  - Perform preventive maintenance by replacing, patching, augmenting, or upgrading software system elements, to improve the performance of a software system that is projected to reach unacceptable service levels, e.g. lack of capacity due to increases in demand or stored data, or to avoid unacceptable operating conditions, e.g. running with outdated security software. (6.4.13.3.b.5)
  - Identify when adaptive or perfective maintenance is required. (6.4.13.3.b.6)
  - Record incidents and problems, including their resolutions and significant maintenance and logistics results. (6.4.13.3.d.1)
  - Identify and record trends of incidents, problems, and maintenance and logistics actions. (6.4.13.3.d.2)
  - Maintain traceability of the system elements being maintained. (6.4.13.3.d.3)
  - Provide key artefacts and information items that have been selected for baselines. (6.4.13.3.d.4)
  - Monitor and measure customer satisfaction with system and maintenance support. (6.4.13.3.d.6)
- Disposal process (6.4.14)
  - Define a disposal strategy for the software system, to include each system element and to identify and address critical disposal needs. (6.4.14.3.a.1)
  - Return the environment to its original state or to a state that specified by agreement. (6.4.14.3.c.2)
  - Archive information gathered through the lifetime of the system to permit audits and reviews in the event of long-term hazards to health, safety, security and the environment, and to permit future software system creators and users to build a knowledge base from experience. (6.4.14.3.c.3)

## 7.5 Guidance and recommendations

### 7.5.1 General

This subclause provides guidance and recommendations with respect to some of the activities and tasks of the processes in ISO/IEC/IEEE 12207 identified in 7.4. Necessary extensions to the activities and tasks are provided. Their special interpretation, if necessary, is also given.

The description of notation given in 6.5.1 also applies to this clause.