TECHNICAL SPECIFICATION

ISO/IEC TS 5723

First edition
2022-07

Trustworthiness — Vocabulary

Reference number
ISO/IEC TS 5723:2022(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

Published in Switzerland

Contents

Page

Foreword

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

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

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

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

Introduction

Recent times have seen an increase in the complexity of integrating technology bringing together various viewpoints. Some examples of this are the convergence of operational technologies (OT) and information technologies (IT) as seen in the Internet of Things (IoT), the rise of big data and artificial intelligence (AI).

The complexity as well as the criticality, from both a safety and a mission point of view, have given rise to the need to communicate both the trustworthiness of products, services and technologies, and the trustworthiness of organizations that are providing these. Having a common understanding of the characteristics that can be used to describe trustworthiness and a common way of defining the vocabulary and characteristics will allow stakeholders to make a judgement as to whether a product, service or technology meets the stakeholder expectations.

This document is primarily intended for use horizontally in an IT domain. It is applicable to all domains in which IT is used.

The terms and definitions in subclause 3.2 are extracted from the ISO and the IEC vocabulary repositories. Where multiple definitions are given, those that best fit the current context of trustworthiness have been selected. For some characteristics, multiple definitions have been retained for different domains.

The terms and definitions in subclause 3.3 are provided for completeness.

Trustworthiness — Vocabulary

1 Scope

This document provides a definition of trustworthiness for systems and their associated services, along with a selected set of their characteristics.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

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

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

3.1 Trustworthiness

3.1.1
trustworthiness
ability to meet *stakeholders'* (3.3.8) expectations in a *verifiable* (3.3.12) way

Note 1 to entry: Depending on the context or sector, and also on the specific product or service, data, technology and process used, different characteristics apply and need verification to ensure stakeholders' expectations are met.

Note 2 to entry: Characteristics of trustworthiness include, for instance, *accountability* (3.2.1), *accuracy* (3.2.2), *authenticity* (3.2.3), *availability* (3.2.4), *controllability* (3.2.5), *integrity* (3.2.7, 3.2.8), *privacy* (3.2.9), *quality* (3.2.10, 3.2.11), *reliability* (3.2.12, 3.2.13), *resilience* (3.2.14, 3.2.15), *robustness* (3.2.16), *safety* (3.2.17), *security* (3.2.18), *transparency* (3.2.19, 3.2.20) and *usability* (3.2.21).

Note 3 to entry: Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as to organizations.

Note 4 to entry: *Verifiability* (3.3.12) includes *measurability* (3.3.5) and demonstrability by means of *objective evidence* (3.3.7).

3.2 Selected trustworthiness characteristics

3.2.1
accountability
state of being *accountable* (3.3.1)

Note 1 to entry: Accountability relates to an allocated responsibility. The responsibility can be based on regulation or agreement or through assignment as part of delegation.

Note 2 to entry: For *systems* (3.3.10), accountability is a property that ensures that actions of an entity can be traced uniquely to the entity (see ISO 7498-2:1989, 3.3.3).

Note 3 to entry: In a governance context, accountability is the obligation of an individual or organization to account for its activities, for completion of a deliverable or task, accept the responsibility for those activities, deliverables or tasks, and to disclose the results in a transparent manner (see ISO/TS 21089:2018, 3.3.1).

[SOURCE: ISO/IEC 38500:2015, 2.3, modified — Note 2 to entry and Note 3 to entry have been added.]

3.2.2
accuracy
measure of closeness of results of observations, computations, or estimates to the true values or the values accepted as being true

[SOURCE: ISO 17572-1:2022, 3.1]

3.2.3
authenticity
property that an entity is what it claims to be

[SOURCE: ISO/IEC 27000:2018, 3.6]

3.2.4
availability
property of being accessible and usable on demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.2.5
controllability
property of a *system* (3.3.10) that allows a human or another external agent to intervene in the system's functioning

Note 1 to entry: Such a system is heteronomous.

[SOURCE: ISO/IEC 22989:2022, 3.5.6, modified — The admitted term "controllable" has been removed and "an AI system" has been changed to "a system".]

3.2.6
information security
preservation of confidentiality, *integrity* (3.2.7, 3.2.8) and *availability* (3.2.4) of information

Note 1 to entry: In addition, other properties, such as *authenticity* (3.2.3), *accountability* (3.2.1), non- repudiation, and *reliability* (3.2.12, 3.2.13) can also be involved.

[SOURCE: ISO 27000:2018, 3.28]

3.2.7
integrity
<data> property whereby data have not been altered in an unauthorized manner since they were created, transmitted, or stored

[SOURCE: ISO/IEC 29167-19:2019, 3.3, modified — The domain has been added.]

3.2.8
integrity
<systems> property of *accuracy* (3.2.2) and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36, modified — The domain has been added.]

3.2.9
privacy
freedom from intrusion into the private life or affairs of an individual

[SOURCE: ISO/IEC 2382:2015, 2.22, modified — The section “when that intrusion results from undue or illegal gathering and use of data about that individual" has been removed from the definition and the Note to entry has been removed.]

3.2.10
quality
<data> degree to which the characteristics of data satisfy stated and implied needs when used under specified conditions

[SOURCE: ISO/IEC 25024:2015, 4.11, modified — “data” is removed from the term and the domain has been added.]

3.2.11
quality
<system> degree to which a set of inherent characteristics of an object fulfils requirements

Note 1 to entry: An object can be a product, process or service.

[SOURCE: ISO 9000:2015, 3.6.2, modified — Original Note 1 to entry and Note 2 to entry have been removed; a new Note 1 to entry has been added and the domain of “<system>” has been added.]

3.2.12
reliability
<cybersecurity> property of consistent intended behaviour and results

[SOURCE: ISO/IEC 27000:2018, 3.55, modified — The domain has been added.]

3.2.13
reliability
<system> ability of an item to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration can be expressed in units appropriate to the item concerned (e.g. calendar time, operating cycles, distance run, etc.) and the units should always be clearly stated.

Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

[SOURCE: IEC 60050-192:2015, 192-01-24, modified — The domain has been changed, the phrase "of an item" has been added at the beginning of the definition and Note 3 to entry has been removed.]

3.2.14
resilience
<governance> ability to anticipate and adapt to, resist, or quickly recover from a potentially disruptive event, whether natural or man-made

[SOURCE: ISO 15392:2019, 3.21, modified — The domain has been added.]

3.2.15
resilience
<system> *capability* (3.3.2) of a *system* (3.3.10) to maintain its functions and structure in the face of internal and external change, and to degrade gracefully when this is necessary

3.2.16
robustness
ability of a *system* (3.3.10) to maintain its level of performance under a variety of circumstances

[SOURCE: ISO/IEC 22989:2022, 3.5.12, modified — “any” has been changed to “a variety of”.]

3.2.17
safety
property of a *system* (3.3.10) such that it does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered

[SOURCE: ISO/IEC/IEEE 12207:2017, 3.1.48, modified — "expectation that a system" has been changed to "property of a system such that it".]

3.2.18
security
resistance to intentional, unauthorized act(s) designed to cause harm or damage to a *system* (3.3.10)

[SOURCE: ISO/IEC 23643:2020, 3.16]

3.2.19
transparency
<information> open, comprehensive, accessible, clear and understandable presentation of information

[SOURCE: ISO 16759:2013, 3.8.4, modified — The domain has been added.]

3.2.20
transparency
<systems> property of a *system* (3.3.10) or process to imply openness and *accountability* (3.2.1)

[SOURCE: ISO/IEC 27036-3:2013, 3.3, modified — The domain has been added.]

3.2.21
usability
extent to which a *system* (3.3.10) product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

Note 1 to entry: The "specified" users, goals and context of use refer to the particular combination of users, goals and context of use for which usability is being considered.

Note 2 to entry: The word "usability" is also used as a qualifier to refer to the design knowledge, competencies, activities and design attributes that contribute to usability, such as usability expertise, usability professional, usability engineering, usability method, usability evaluation, usability heuristic.

[SOURCE: ISO 9241-11:2018, 3.1.1]

3.3 Selected supporting definitions

3.3.1
accountable
answerable for actions, decisions, and performance

[SOURCE: ISO/IEC 38500:2015, 2.2]

3.3.2
capability
measure of capacity and the ability of an entity (*system* (3.3.10), person or organization) to achieve its objectives

[SOURCE: ISO/IEC 19770-1:2017, 3.10, modified — Note 1 to entry and domain <asset management> have been removed.]

3.3.3
constituent system
independent *system* (3.3.10) that forms part of a *system of systems (SoS)* (3.3.11)

Note 1 to entry: Constituent systems can be part of one or more SoS. Each constituent system is a useful system by itself, having its own development, management, utilization, goals, and resources, but interacts within the SoS to provide the unique *capability* (3.3.2) of the SoS.

[SOURCE: ISO/IEC/IEEE 21839:2019, 3.1.1]

3.3.4
dependability
<of an item> ability to perform as and when required

Note 1 to entry: Dependability includes *availability* (3.2.4), *reliability* (3.2.12, 3.2.13), recoverability, maintainability, and maintenance support performance, and, in some cases, other characteristics such as durability, *safety* (3.2.17) and *security* (3.2.18).

Note 2 to entry: Dependability is used as a collective term for the time-related *quality* (3.2.10, 3.2.11) characteristics of an item.

[SOURCE: IEC 60050-192:2015, 192-01-22]

3.3.5
measurability
ability to assess an attribute of an entity against a *metric* (3.3.6)

Note 1 to entry: The word "measurable" is the adjective form of measurability.

3.3.6
metric
defined measurement method and measurement scale

[SOURCE: ISO/IEC 14102:2008, 3.4]

3.3.7
objective evidence
data supporting the existence or verity of something

Note 1 to entry: Objective evidence can be obtained through observation, measurement, test, or other means.

[SOURCE: ISO 9000:2005, 3.8.1]

3.3.8
stakeholder
any individual, group, or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

[SOURCE: ISO/IEC 38500:2015, 2.24]

3.3.9
socio-technical system
system (3.3.10) that includes a combination of technical and human or natural elements

[SOURCE: INCOSE SEBoK]

3.3.10
system
combination of interacting elements organized to achieve one or more stated purposes

[SOURCE: ISO/IEC/IEEE 21840:2019, 3.1.8]

3.3.11
system of systems
set of *systems* (3.3.10) and system elements that interact to provide a unique *capability* (3.3.2) that none of the *constituent systems* (3.3.3) can accomplish on its own

Note 1 to entry: System elements can be necessary to facilitate interaction of the constituent systems in the system of systems.

[SOURCE: ISO/IEC/IEEE 21840:2019, 3.1.10]

3.3.12
verifiable
can be checked for correctness by a person or tool

[SOURCE: ISO/IEC/IEEE 15289:2019, 3.1.29]