DRAFT INTERNATIONAL STANDARD ISO/IEC 30754

Attributed to ISO/IEC JTC 1 by the Central Secretariat

Voting begins on
2016-04-06

Voting terminates on
2016-07-06

FAST-TRACK PROCEDURE

Information technology — Software trustworthiness — Governance and management — Specification

Titre manque

ICS 35.080

This draft International Standard is submitted for JTC 1 national body vote under the "fast-track" procedure.

In accordance with Resolution 30 of the JTC 1 Berlin Plenary 1993, the proposer of this document recommends assignment of JTC1 to JTC 1.

The procedures used to develop this document are described in the ISO/IEC Directives, Part 1 - Consolidated JTC 1 Supplement.

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

NOTE FROM ITTF

This draft International Standard is submitted for JTC 1 national body vote under the “fast-track” Procedure.

In accordance with Resolution 30 of the JTC 1 Berlin Plenary 1993, the proposer of this document recommends assignment of ISO/IEC 30754 to JTC 1.

“FAST-TRACK” PROCEDURE

1 Any P-member and any Category A liaison organization of ISO/IEC JTC 1 may propose that an existing standard from any source be submitted directly for vote as an enquiry draft (DIS). The criteria for proposing an existing standard for the fast-track procedure are a matter for each proposer to decide.

2 The proposal shall be received by the ITTF, which will take the following actions.

2.1 Settle the copyright and/or trademark situation with the organization having originated the proposed document, so that it can be freely copied and distributed to national bodies without restriction.

2.2 Assess in consultation with the JTC 1 secretariat which subcommittee (SC) is competent for the subject covered by the proposed document and ascertain that there is no evident contradiction with other International Standards.

2.3 Distribute the proposed document as an enquiry draft (DIS).

3 The period for combined enquiry voting (DIS) and the conditions for approval shall be as specified in Annex F.2.3 of the JTC 1 Supplement

4 At the end of the voting period, the comments received, whether editorial only or technical, will be dealt with by a working group (WG) appointed by the secretariat of the relevant SC.

5 If, after the deliberations of this WG, the conditions of approval are met, the draft standard shall progress to the approval stage (FDIS). If not, the proposal has failed and any further action shall be decided upon by the subcommittee to which the document was attributed.

In either case the WG shall prepare a full report which will be circulated by the ITTF.

6 If the proposed standard is accepted and published, its maintenance will be handled by JTC 1.

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC DIS 30754 was prepared by British Standards Institution (BSI) for Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Relationships with other publications

This Standard is intended to be used as a stand alone specification, or it can be used as a companion and complement to other relevant standards, by any organization that is looking for trustworthiness and confidence in its software.

This Standard contains requirements that define the principles required to achieve software trustworthiness but does not specify how to implement those principles. Annex A includes an example of the principles that can deliver the requirements of this Standard mapped again the lifecycle.

Use of this document

It has been assumed in the preparation of this Standard that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is “shall”.

Commentary, explanation and general informative material is presented in smaller italic type and does not constitute a normative element.

The word “should” is used to express recommendations, the word “may” is used to express permissibility and the word “can” is used to express possibility, e.g. a consequence of an action or event.

Spelling conforms to The Shorter Oxford English Dictionary.

Contractual and legal considerations

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

Compliance with this Standard cannot confer immunity from legal obligations.

0 Introduction to Software Trustworthiness

0.1 Aims

The aim of ISO/IEC 30754 is to provide a specification for software trustworthiness.

0.2 Objectives

This specification is intended to be widely applicable to software in its many guises from embedded equipment through consumer devices to industrial control systems. It aims to provide a consensus specification for software trustworthiness, either as a stand-alone document, or as a companion and complement to other relevant standards, by collating good practice from the five main facets of trustworthiness that currently typically operate in isolation (safety, reliability, availability, resilience and security).

By helping to improve software trustworthiness within organizations, this specification could result in significant savings for the economy and reduce the risk major disruptions to a range sectors.

NOTE See *Risk and Responsibility in a Hyperconnected World*, WEF[1]

The requirements of ISO/IEC xx754 can enable an organization to, for example:

- improve controls;
- improve operational effectiveness and efficiency;
- improve organizational learning.

These in turn can result in:

- improved stakeholder confidence and trust;
- increased likelihood of achieving objectives;
- reduced risk;
- enhanced business reputation.

0.3 Claims of Conformance

0.3.1 General

An organization may claim conformance with ISO/IEC 30754.

0.3.2 Form of Claims

All claims are required to include a reference to ISO/IEC 30754.

0.3.3 Basis of Claim

A claim of conformance can be made on the basis of:

a) a first-party conformity assessment performed by the organization (self assessment);

b) a second-party conformity assessment performed by, for example, a trade association; or
c) a third-party conformity assessment performed by an organization, such as a certification body, that is independent of both the organization and any linked trade association.

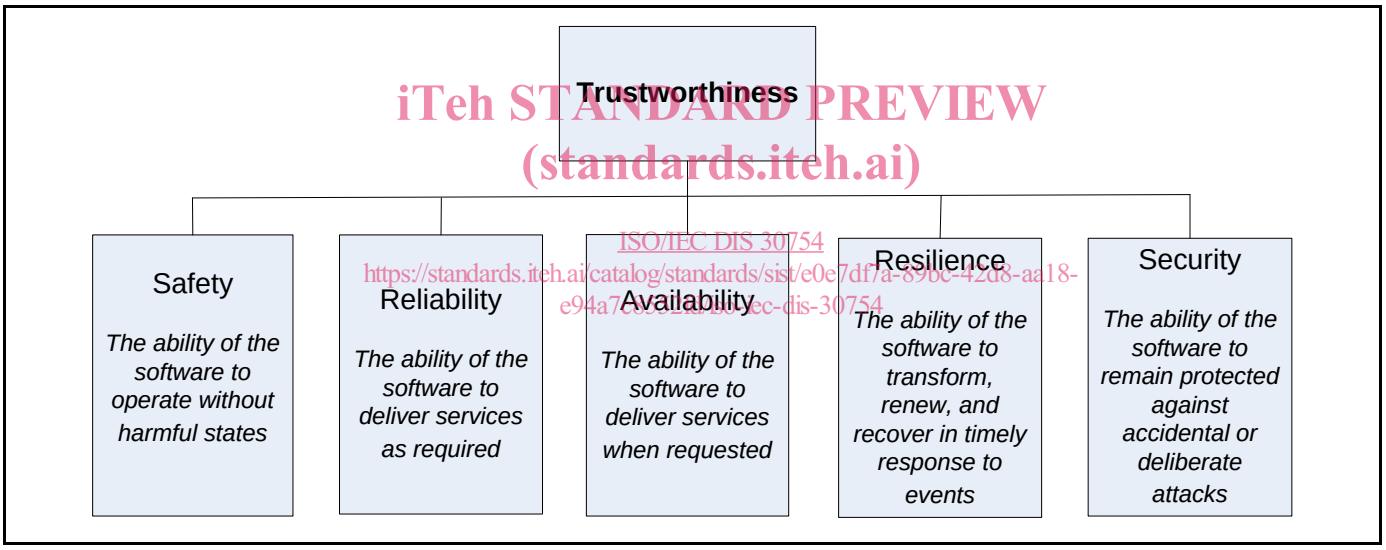
0.4 Context

0.4.1 Approach

ISO/IEC 30754 is intended for any organization that seeks to establish or improve confidence in its software trustworthiness. It is applicable to all organizations regardless of their size, type and the nature of their business.

For this specification, software trustworthiness is identified as consisting of five Facets, as described in Figure 1.

Figure 1 – Facets of trustworthiness



It is important that organizations review every software implementation to see which aspects apply and derive a set of principles and techniques to suit the context and intended use.

For each of these Facets of Trustworthiness there will be objectives, of varying complexity.

A common set of implied objectives apply to most software implementations, not least because of legal and regulatory requirements.

'Safety' aims to provide assurance that:

- the stated requirements are accurate and appropriate;
- safety issues are considered via safety requirements;
- the architecture and design are consistent with and reflect the stated requirements;
- technical defects are absent;
- application defects are absent;

- the stated requirements are identifiable in the low-level code and that all low-level code implements at least one stated requirement;
- the test data sets reflect the stated requirements;
- the test data sets cover the low-level code to a specified degree.

'Reliability' aims to provide assurance that:

- all the patterns of use are reflected in the stated requirements;
- there are no technical defects;
- the test data sets reflect patterns of use;
- there are no application defects.

'Availability' aims to provide assurance that:

- the stated requirements are accurate and appropriate;
- the architecture and design are consistent with and reflect the stated requirements;
- technical defects are absent;
- application defects are absent;
- the test data sets reflect the stated requirements.

'Resilience' aims to provide assurance that:

- the stated requirements are accurate and appropriate;
- the architecture and design are consistent with and reflect the stated requirements;
- technical defects are absent;
- application defects are absent;
- the test data sets reflect the stated requirements.

'Security' aims to provide assurance that:

- the security requirements consider all security issues;
- the architecture and design satisfy the security requirements;
- there are no security defects in the code;
- the test data reflects the security requirements.

0.4.2 Organizational Controls

In order to deliver trustworthy software, an organization requires a set of underpinning controls that apply to all activities.

The software management system aims to provide assurance that:

- all personnel are appropriately qualified;

- adequate resources are allocated;
- all necessary communication takes place;
- activity proceeds in a series of measured steps;
- specific steps are performed independently;
- activity proceeds in a timely manner;
- all verification processes are completed within the specified criteria.

The software technical infrastructure aims to provide assurance that:

- all information, designs, algorithms and other such artefacts are retained for future use and analysis;
- the design and coding artefacts are adequately documented;
- all past and present versions of the software are available at any time and that future versions will similarly be available;
- all appropriate test data sets can be applied to the corresponding version and any future versions of the software;
- regression testing can be applied in order to ensure that the software changes only in the required manner.

0.4.3 Challenges

Software problems are generally characterised as a one of three types:

- **Weaknesses**, which are generic classes of potential deficiency in software, such as buffer overflows.
- **Vulnerabilities**, which can be:
  - the existence of a generic weakness in a particular platform, such as a buffer overflow occurring in a specific operating system or application;
  - interactions between multiple software elements that bypass intended controls;
  - accidental actions of software developers that result in defects and errors;
  - deliberate actions of software developers that bypass intended controls, such as trap doors that permit unauthorised access to the system.
- **Susceptibilities**, which are the confirmed presence of one or more vulnerability within an implemented system, such as the presence of an operating system with a buffer overflow defect.

Susceptibilities in systems stem from:

- initial implementation;
- changes to software, such as from adding new facilities or the correction of detected errors ('patching');

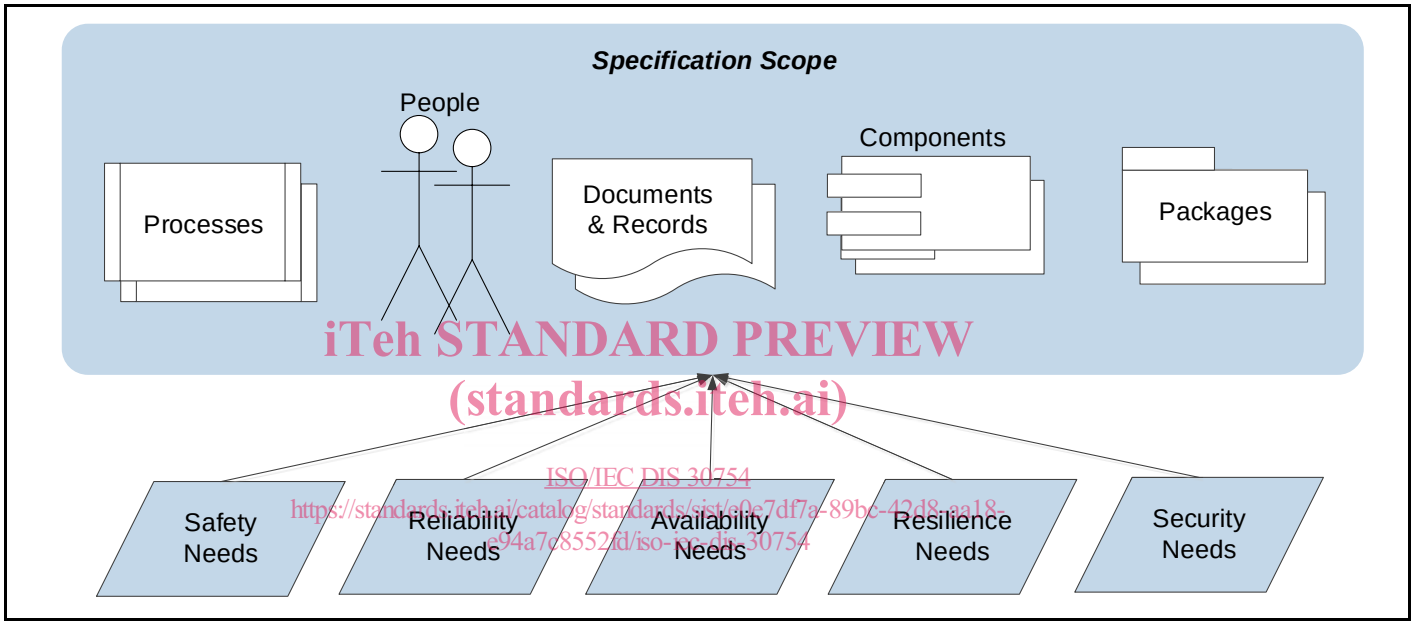
- use of utility programs, which may be capable of circumventing security measures in the controlling or application software.

For the application of these terms specifically to software, see Clause 3.

0.4.4 Tailoring

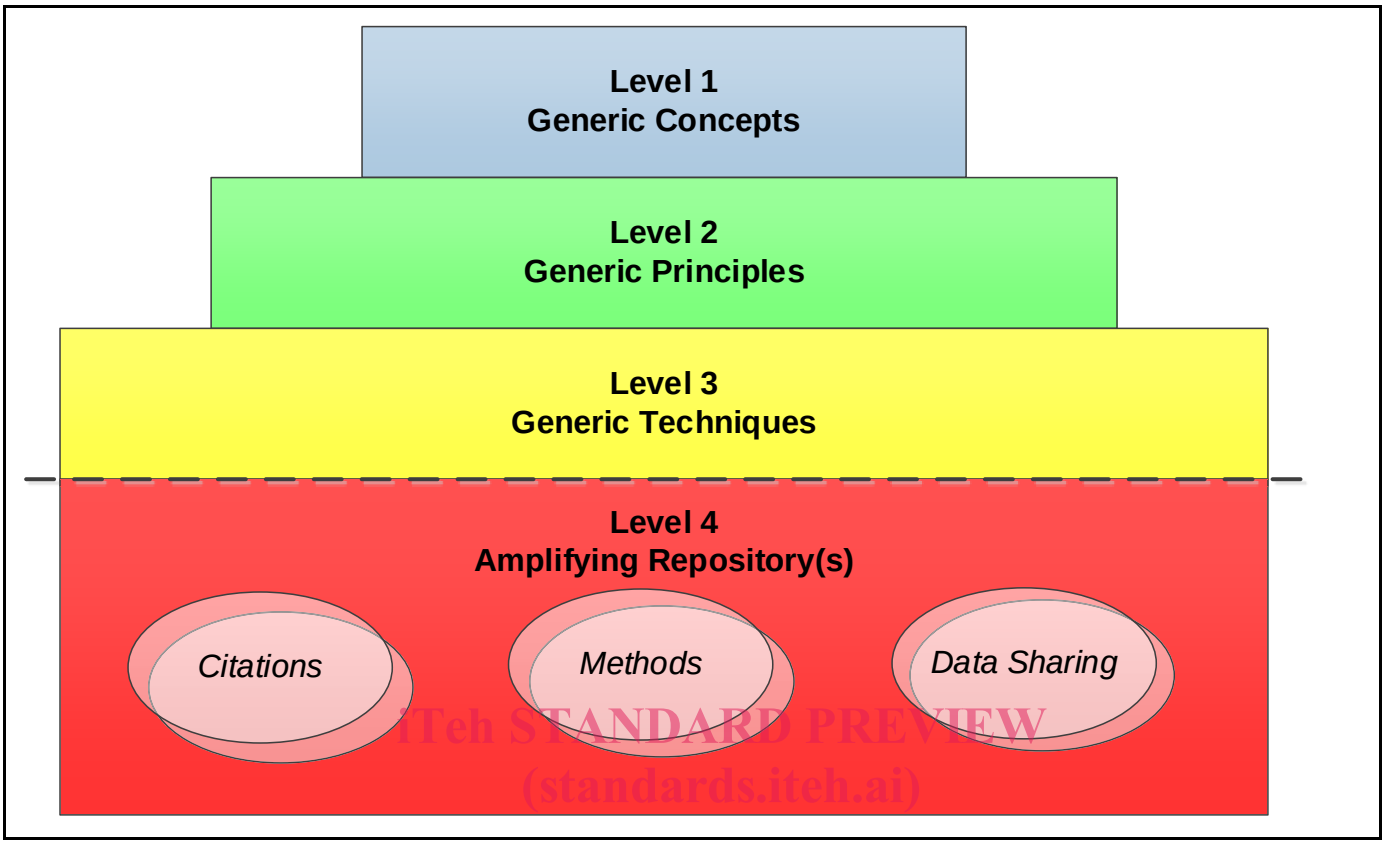
ISO/IEC 30754 is scoped to include all aspects that contribute to trustworthiness of software, as illustrated in Figure 2.

Figure 2 – Aspects of trustworthiness



This is achieved by using the appropriate elements of the framework of decomposed as shown in Figure 3 and detailed in Clauses **5** and **6** and the Annexes.

Figure 3 – Trustworthy Software Framework



This comprehensive Trustworthy Software Framework (TSF) provides a domain- and implementation-agnostic way to reference the large existing body of knowledge, including functional safety, information security, and systems and software engineering and therefore acts as a collation of good practice for software trustworthiness.

When used as a stand-alone document for organizations with no current approach to software trustworthiness, this specification will facilitate the deployment of the TSF for software in its many guises from embedded equipment through consumer devices to industrial control systems.

For organizations that already address software trustworthiness though the lens of one or more of the five main facets of trustworthiness that typically operate in isolation (safety, reliability, availability, resilience and security), this specification provides a companion and complement to other relevant standards, and reviewing the concepts, principles and techniques in this specification alongside practices and Management Systems derived from individual facets allows the identification of gaps and enhancements.

This document does not specify how any technique should be applied to a specific domain of application. This information is available in other standards, such as ISO/IEC 15408 and ISO/IEC 27001 for information security, and IEC61508 for functional safety.

0.4.5 Categorization

For the purposes of this standard, the software audience can be divided into three groups:

