DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 15026-1

ISO/IEC JTC **1**/SC **7**

Secretariat: **BIS**

Voting begins on:
2018-02-01

Voting terminates on:
2018-04-26

Systems and software engineering — Systems and software assurance —

Part 1:
Concepts and vocabulary

Ingénierie des systèmes et du logiciel — Assurance des systèmes et du logiciel —

Partie 1: Concepts et vocabulaire

ICS: 35.080

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 15026-1:2018(E)

© ISO/IEC 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Applicability ... **1**
2.1 Audience ... 1
2.2 Field of applicability ... 1

3 Normative references ... **1**

4 Terms and definitions ... **1**
4.1 Terms related to assurance and properties ... 2
4.2 Terms related to product and process ... 3
4.3 Terms related to integrity level ... 4
4.4 Terms related to conditions and consequences ... 6
4.5 Terms related to organization ... 8

5 Organization of this International Standard ... **8**

6 Basic concepts ... **8**
6.1 Introduction ... 8
6.2 Assurance ... 9
6.3 Stakeholders ... 9
6.4 System and product ... 9
6.5 Property ... 10
6.5.1 Properties as behaviors ... 10
6.6 Uncertainty and confidence ... 10
6.7 Conditions and initiating events ... 11
6.8 Consequences ... 11

7 Using multiple parts of this document (all parts) ... **12**
7.1 Introduction ... 12
7.2 Initial usage guidance ... 12
7.3 Relationships among parts of this document (all parts) ... 12
7.4 Authorities ... 13

8 This document (all parts) and the assurance case ... **13**
8.1 Introduction ... 13
8.2 Justification of method of reasoning ... 14
8.3 Means of obtaining and managing evidence ... 15
8.4 Certifications and accreditations ... 15

9 This document (all parts) and integrity levels ... **15**
9.1 Introduction ... 15
9.2 Risk analysis ... 16

10 This document (all parts) and the life cycle ... **16**
10.1 Introduction ... 16
10.2 Assurance activities in the life cycle ... 17

11 Summary ... **18**

Bibliography ... **19**

© ISO/IEC 2018 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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.

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 editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO 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).

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

For an explanation on 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 the following URL: 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 IEEE Computer Society Systems and Software Engineering Standards Committee, under the Partner Standards Development Organization cooperation agreement between ISO and IEEE..

This second edition cancels and replaces the first edition (ISO/IEC 15026-1:2013), which has been technically revised.

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

— Definitions of terms introduced in ISO/IEC 15026-3:2015 are added. Definitions of terms whose definitions are modified in ISO/IEC 15026-3:2015 are updated.

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

© ISO/IEC 2018 – All rights reserved

Introduction

Software and systems assurance and closely related fields share concepts but have differing vocabularies and perspectives. This document provides a unifying set of underlying concepts and an unambiguous use of terminology across these various fields. It provides a basis for elaboration, discussion, and recording agreement and rationale regarding concepts and the vocabulary used uniformly across this document (all parts).

This document clarifies concepts needed for understanding software and systems assurance and, in particular, those central to the use of Part 2, Part 3 and Part 4 of this document. It supports shared concepts, issues and terminology applicable across a range of properties, application domains, and technologies.

© ISO/IEC 2018 – All rights reserved

Systems and software engineering — Systems and software assurance —

Part 1: Concepts and vocabulary

1 Scope

This document defines assurance-related terms and establishes an organized set of concepts and relationships to establish a basis for shared understanding across user communities for assurance. It provides information to users of the other parts of this document including the combined use of multiple parts. The essential concept introduced by this document (all parts) is the statement of claims in an assurance case and the support of those claims through argumentation and evidence. These claims are in the context of assurance for properties of systems and software within life cycle processes for the system or software product.

Assurance for a service being operated and managed on an ongoing basis is not covered in this document (all parts).

2 Applicability

2.1 Audience

A variety of potential users of this document (all parts) exists including developers and maintainers of assurance cases and those who wish to develop, sustain, evaluate, or acquire a system that possesses requirements for specific properties in such a way as to be more certain of those properties and their requirements. This document (all parts) uses concepts and terms consistent with ISO/IEC/IEEE 12207 and ISO/IEC/IEEE 15288 and generally consistent with the ISO/IEC 25000 series, but the potential users of this document (all parts) need to understand differences from concepts and terms to which they may be accustomed. This document attempts to clarify these differences.

2.2 Field of applicability

The primary purpose of this document is to aid users of the other parts of this document by providing context, concepts, and explanations for assurance, assurance cases, and integrity levels. While essential to assurance practice, details regarding exactly how to measure, demonstrate, or analyse particular properties are not covered. These are the subjects of more specialized standards of which a number are referenced and included in the Bibliography.

3 Normative references

There are no normative references in this document.

4 Terms and definitions

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

© ISO/IEC 2018 – All rights reserved