AS/NZS ISO/IEC 15026.4:2013
ISO/IEC 15026-4:2012

AS/NZS ISO/IEC 15026.4:2013

Australian/New Zealand Standard™

Systems and software engineering—Systems and software assurance

Part 4: Assurance in the life cycle

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

Full document details: AS NZS ISO IEC 15026.4-2013

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-015, Software and Systems Engineering. It was approved on behalf of the Council of Standards Australia on 2 May 2013 and on behalf of the Council of Standards New Zealand on 29 April 2013.
This Standard was published on 24 May 2013.

The following are represented on Committee IT-015:

Australian Computer Society
Australian Society for Technical Communication, NSW
Charles Sturt University
Department of Defence, Australia
Griffith University
Quantitative Enterprise Software Performance
La Trobe University
National Association of Testing Authorities Australia
National ICT Australia
New Zealand Organisation for Quality
NSW Business Chamber
Systems Engineering Society of Australia
University of Auckland
University of Technology, Sydney
Vendor Interests, New Zealand

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.saiglobal.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR AS/NZS ISO/IEC 15026.4.

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15026.4-2013

Australian/New Zealand Standard™

Systems and software engineering—Systems and software assurance

Part 4: Assurance in the life cycle

First published as AS/NZS ISO/IEC 15026.4:2013.

COPYRIGHT

© Standards Australia Limited/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Australia) or the Copyright Act 1994 (New Zealand).

Jointly published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001 and by Standards New Zealand, Private Bag 2439, Wellington 6140.

ISBN 978 1 74342 450 6

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

AVA Documents Document Sharing Hub

Full document details: AS NZS ISO IEC 15026.4-2013

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-015, Software and Systems Engineering.

The objective of this Standard is to provide guidance and recommendations for conducting selected processes, activities and tasks for systems and software products requiring assurance claims for properties selected for special attention, and called 'critical properties'. It also specifies a property-independent list of processes, activities and tasks, in the context of a defined life cycle model, to achieve the claim and show the achievement of the claim.

This Standard is identical with, and has been reproduced from ISO/IEC 15026-4:2012, *Systems and software engineering—Systems and software assurance*—Part 4*: Assurance in the life cycle.*

As this Standard is reproduced from an International Standard, the following applies:

(a) In the source text 'this part of ISO/IEC 15504' should read 'this Australian/New Zealand Standard'.

(b) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian/New Zealand Standard*	
ISO/IEC		SA/SNZ TR	
15026	Systems and software engineering—Systems and software assurance	15026	Systems and software engineering—Systems and software assurance
15026-1	Part 1: Concepts and vocabulary	15026.1	Part 1: Concepts and vocabulary
		AS/NZS ISO/IEC	
15288	Systems and software engineering—System life cycle processes	15288	Systems and software engineering—System life cycle processes
12207	Systems and software engineering—Software life cycle processes	12207	Information technology—Software life cycle processes

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15026.4-2013

CONTENTS

1 Scope 1
2 Conformance 1
3 Normative references 1
4 Terms and definitions 2
5 Key concepts for and use of this part of ISO/IEC 15026 2
5.1 Life cycle approach 2
5.2 Assurance claims 2
5.3 Using this part of ISO/IEC 15026 3
5.3.1 Use for an agreement 3
5.3.2 Use for regulation 3
5.3.3 Use for development 3
6 Process view purposes and required outcomes 3
6.1 Systems assurance process view 3
6.1.1 Purpose 4
6.1.2 Required outcomes 4
6.2 Software assurance process view 4
6.2.1 Purpose 4
6.2.2 Required outcomes 4
7 Assurance guidance and recommendations for selected processes 4
7.1 Introduction 4
7.2 Acquisition process 5
7.2.1 Relevant activities and tasks 5
7.2.2 Assurance guidance and recommendations 5
7.3 Supply process 6
7.3.1 Relevant activities and tasks 6
7.3.2 Assurance guidance and recommendations 6
7.4 Project planning process 7
7.4.1 Relevant activities and tasks 7
7.4.2 Assurance guidance and recommendations 7
7.5 Decision Management process 8
7.5.1 Relevant activities and tasks 9
7.5.2 Assurance guidance and recommendations 9
7.6 Risk Management process 9
7.6.1 Relevant activities and tasks 10
7.6.2 Assurance guidance and recommendations 11
7.7 Configuration management process 11
7.7.1 Relevant activities and tasks 11
7.7.2 Assurance guidance and recommendations 12
7.8 Information Management process 13
7.8.1 Relevant activities and tasks 13
7.8.2 Assurance guidance and recommendations 13
7.9 Stakeholder Requirements Definition process 14
7.9.1 Relevant activities and tasks 15
7.9.2 Assurance guidance and recommendations 15
7.10 Requirements Analysis process 17
7.10.1 Relevant activities and tasks 18
7.10.2 Assurance guidance and recommendations 19

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub
Full document details: AS NZS ISO IEC 15026.4-2013

Page

7.11 Verification process 19
7.11.1 Relevant activities and tasks 20
7.11.2 Assurance guidance and recommendations 20
7.12 Operation process 20
7.12.1 Relevant Activities and Tasks 21
7.12.2 Assurance guidance and recommendations 21
7.13 Maintenance process 21
7.13.1 Relevant activities and tasks 21
7.13.2 Assurance guidance and recommendations 22

Bibliography 23

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15026.4-2013

INTRODUCTION

In its entirety, ISO/IEC 15026 consists of multiple parts:

a) ISO/IEC TR 15026-1, *System and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

NOTE ISO/IEC TR 15026-1 is intended to be replaced by an International Standard.

b) ISO/IEC 15026-2, *System and software engineering — Systems and software assurance — Part 2: Assurance case*

c) ISO/IEC 15026-3, *System and software engineering — Systems and software assurance — Part 3: System integrity levels*

d) ISO/IEC 15026-4, *System and software engineering — Systems and software assurance — Part 4: Assurance in the life cycle*

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 TR 15026-1 provides terminology and concepts used in all parts of ISO/IEC 15026.

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 part of ISO/IEC 15026 can be recorded in the form of the assurance case described in ISO/IEC 15026-2.

ISO/IEC 15026-3 addresses the assignment of integrity levels for selected elements of a system. Where ISO/IEC 15026-2 is applicable, it can bring useful structure, aid, and direction to defining claims and showing their achievement through the use of integrity levels and accompanying integrity level requirements.

ISO/IEC 15026-2, ISO/IEC 15026-3 and ISO/IEC 15026-4 all use the concepts and vocabulary defined in ISO/IEC TR 15026-1; however, any part can be applied independently of the others and the use of one does not require the use of any others.

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15026.4-2013

NOTES

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15026.4-2013

AUSTRALIAN/NEW ZEALAND STANDARD

Systems and software engineering—Systems and software assurance

Part 4: Assurance in the life cycle

1 Scope

This part of ISO/IEC 15026 gives guidance and recommendations for conducting selected processes, activities and tasks for systems and software products requiring assurance claims for properties selected for special attention, called critical properties. This part of ISO/IEC 15026 specifies a property-independent list of processes, activities and tasks to achieve the claim and show the achievement of the claim. This part of ISO/IEC 15026 establishes the processes, activities, tasks, guidance and recommendations in the context of a defined life cycle model and set of life cycle processes for system and/or software life cycle management.

NOTE The stakeholders determine which of the system or software properties are selected for special attention and require assurance claims. This part of ISO/IEC 15026 uses the term “critical” to distinguish those properties from other requirements.

2 Conformance

Conformance may be claimed to this part of ISO/IEC 15026 with respect to the systems assurance process view and/or the software assurance process view. Thus, conformance to this part of ISO/IEC 15026 can be achieved in either or both of the following ways:

a) Demonstrating that the required outcomes of the systems assurance process view (6.1.2) have been achieved, in addition to conforming to the Agreement, Project, and Technical processes of ISO/IEC 15288.

b) Demonstrating that the required outcomes of the software assurance process view (6.2.2) have been achieved, in addition to conforming to the Agreement, Project, Technical, and Software Specific processes of ISO/IEC 12207:2008.

A claim of conformance is relevant only to specific claims regarding designated systems or software.

Conformance to ISO/IEC 15026 Part 2 can assist in achieving the outcomes required by the two process views in this part of ISO/IEC 15026.

NOTE Parties to an agreement may choose to incorporate selected portions of this part of the International Standard into the terms of the agreement. However, compliance with the agreement does not justify a claim of conformance to this part of the International Standard. A claim of conformance can only be justified as explained above.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced documents (including any amendments) applies.

ISO/IEC TR 15026-1, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 15026.4-2013

This part requires activities and tasks in the context of complete sets of life cycle processes that comprise life cycle models for projects. The two sets of life cycle processes are provided in:

ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*

ISO/IEC 12207:2008, *Systems and software engineering — Software life cycle processes*

The assurance guidance and recommendations referenced in this part of ISO/IEC 15026 are to be understood in terms of their being in the context of the processes, activities and tasks of ISO/IEC 15288 and ISO/IEC 12207.

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC TR 15026-1, ISO/IEC 15288:2008, and ISO/IEC 12207:2008 apply.

5 Key concepts for and use of this part of ISO/IEC 15026

5.1 Life cycle approach

It is presumed that the user of this International Standard is using a defined life cycle model and set of life cycle processes for system and/or software life cycle management. Across the life cycle, the systems and software process views in Clause 6 use the guidance and recommendations in Clause 7 for the performance of specific processes, activities, and tasks in order to achieve and show the achievement of assurance claims. Since all processes of ISO/IEC 15288 and ISO/IEC 12207 are applied iteratively and recursively in the life cycle, the guidance and recommendations for assurance are also applied iteratively and recursively. In that way, the achievement of assurance can be checked during each iteration or recursion.

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

5.2 Assurance claims

When system or software product requirements call for assurance of one or more critical properties of the system or software product, the overall claims for assurance regarding these properties' values are referred to in ISO/IEC 15026 as assurance claims. Commonly, such critical properties are in areas where substantial risk or consequences are involved such as reliability and maintainability, safety, security, or human factors.

NOTE The material in this clause is adopted from ISO/IEC 15026-2.

Achieving assurance claims normally includes all the considerations involved in achieving stringent requirements. A requirement is defined in ISO/IEC 29148 as “statement which translates or expresses a need and its associated constraints and conditions” and a claim is defined in ISO/IEC TR 15026-1 as “statement of something to be true including associated conditions and limitations.” This part of ISO/IEC 15026 considers requirements to be statements of values for variables and claims to be statements of requirements to be true.

While assurance claims can be derived from a number of sources, they are normally motivated by potential real-world adverse consequences related to the intended uses of the system and justified as deriving from system or software requirements. Each assurance claim is fully and unambiguously specified including:

a) “Assurance claims” — that is, the top-level claims, including

   1) Values for the variables of the critical property required for its achievement.

   2) Limitations on allowable uncertainties regarding this achievement.

   3) Conditions and/or durations of applicability under which it applies.

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 15026.4-2013

4) The set of versions or instances of the system or software product covered by the claims.

c) “Justification for assurance claims” — that is, the justification for selecting and specifying these particular assurance claims.

d) “Body of information showing achievement of assurance claims” or more succinctly as the “information showing [or assuring] the achievement of assurance claims”.

This last item includes the evidence, the rationale or argument showing how the evidence supports the claims, and any assumptions underlying this rationale. Normally, this rationale has multiple levels of derived claims internal to it, e.g., claims about system elements at each level of decomposition that need to be true in order for the assurance claims about the system or software product to be true. The body of information also includes information on the validity, integrity, relevance, and significance of the evidence.

The rationale often includes several different kinds of 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. These are combined to achieve an overall conclusion and an estimate of the remaining uncertainty regarding the achievement of the assurance claims.

The body of information composing and organizing these three items is an element (or elements) of the system or software product and, as such, is maintained and updated throughout the system life cycle, to include development as well as maintenance. As a system element, all the processes, activities, and tasks regarding a system element apply to it, such as configuration management, verification, and validation.

5.3 Using this part of ISO/IEC 15026

This part of ISO/IEC 15026 can be used for an agreement between an acquirer and supplier, for regulation purposes, or for assessment of internal development processes to improve achieving and showing the achievement of assurance claims for the system or software product. Its use is, however, not limited to these three purposes.

5.3.1 Use for an agreement

This part of ISO/IEC 15026 can be used for an agreement between an acquirer and a supplier concerning achieving and showing the achievement of an assurance claim about the value of variables for a critical property of the system or software product being acquired. The acquirer and supplier relationship can occur at different levels of the supply chain (prime-supplier, internal to one organization, etc.).

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

5.3.2 Use for regulation

An authoritative body can use this part of ISO/IEC 15026 for regulation for assuring some critical property of a system or software product. The need for such regulation can arise to assure or certify a critical property of a system or software product, to clarify their assurance in the condition of trade, or to do some other action.

5.3.3 Use for development

This part of ISO/IEC 15026 can be used for an internal assessment by a developer in improving its processes for achieving and showing the achievement of assurance claims for critical properties of systems and software products it develops.

6 Process view purposes and required outcomes

6.1 Systems assurance process view

The following clauses define the purpose and required outcomes of the systems assurance process view.

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 15026.4-2013

6.1.1 Purpose

The purpose of the Systems Assurance Process View is to achieve the assurance claims regarding the system properties selected for special attention and to provide a body of information showing the achievement of those claims. The Systems Assurance Process View covers the system of interest including any constituent software.

6.1.2 Required outcomes

The following outcomes shall result from the successful implementation of the Systems Assurance Process View:

a) A subset of requirements for the achievement of critical properties is defined.

b) Assurance claims, their justification, and the body of information showing the achievement of the assurance claims for the critical properties are established as an element of the system.

c) A strategy for achieving these assurance claims and showing their achievement is defined.

d) The extent of achievement of the assurance claims is communicated to affected stakeholders.

6.2 Software assurance process view

The following clauses define the purpose and required outcomes of the software assurance process view.

6.2.1 Purpose

The purpose of the Software Assurance Process View is to achieve the assurance claims regarding the software properties selected for special attention and to provide a body of information showing the achievement of those claims.

6.2.2 Required outcomes

The following outcomes shall result from the successful implementation of the Software Assurance Process View:

a) A subset of requirements for achievement of the critical properties for application of this process view is defined.

b) Assurance claims, their justification, and the body of information showing achievement of the assurance claims for the critical properties are established as an element of the system.

c) A strategy for achieving these assurance claims and showing their achievement is defined.

d) The extent of achievement of the assurance claims is communicated to affected stakeholders.

7 Assurance guidance and recommendations for selected processes

7.1 Introduction

Clause 7 cites the activities and tasks from the Agreement, Project, and Technical categories of processes in ISO/IEC 15288:2008 and in ISO/IEC 12207:2008 that require extension or special interpretation when a defined level of assurance is to be demonstrated. The numbers of those activities and tasks correspond to the numbers in the parent standards (ISO/IEC 15288 and ISO/IEC 12207). Assurance-claim-related guidance and recommendations are provided for performing these activities and tasks to achieve the outcomes of the process views. This guidance and recommendations assume and depend upon the full application of ISO/IEC 15288 and ISO/IEC 12207 as indicated in Clause 3. The processes and activities not cited in this clause are considered adequate as defined in ISO/IEC 15288:2008 and ISO/IEC 12207:2008 to achieve the claims for the critical properties.

Accessed by MONASH UNIVERSITY LIBRARY on 13 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 15026.4-2013