



ISO/IEC JTC 1/SC 27 **N 8119**

ISO/IEC JTC 1/SC 27/WG 3 **N 38119**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: other

TITLE: SC 7 LS Officer presentation

SOURCE: 39th SC 27/WG 3 meeting

DATE: 2009-11-02

PROJECT:

STATUS: This document was made available at the 39th SC 27/WG 3 meeting held in Redmond, US, 2nd – 6th May 2009. It is circulated within SC 27 for information.

ACTION: FYI

DUE DATE:

DISTRIBUTION: P-, O-, and L- Members
W. Fumy, SC 27 Chairman, M. De Soete, SC 27 Vice Chair
E. Humphreys, K. Naemura, M. Bañón, M.C. Kang, K. Rannenber, WG-Conveners

MEDIUM: Server

NO. OF PAGES: 1 + 28

ISO/IEC 15026

Presentation to
SC27 Interim Meeting
2-6 November 2009
Redmond, Washington, USA

Overview

- Introduction
 - General
 - Status in standards process
 - Editors
- Four Parts
- Final Comments

Presentation reflects current versions, and presenter's current understanding and intentions

INTRODUCTION

2-7 November 2009

General

- General title: *Systems and software engineering — Systems and software assurance*
- Development in: JTC1 SC7 WG7
- Prior version of ISO/IEC 15026:1998 was on *Software integrity levels*
- Initial work on this version began in 2007
- Four Parts

Status of Parts

- Part 1: Concepts and vocabulary
 - TR (in publication) an IS is planned for later
- Part 2: Assurance case
 - Ballot in on CD4; likely FCD next
- Part 3: System integrity levels
 - Comment period for WD2 ended; possibly CD1 next
- Part 4: Assurance in the life cycle
 - WD1 out for comment (Due 15 Jan. 2010)

Note on scope and motivation

- Potentially covers any system or product properties selected
- Inspired by
 - Safety, R&M, security, maintainability, human factors, and others
 - Stringent requirements
 - Needs for confidence and decision making, e.g. acceptability for shipment or use

Editors

- Samuel Redwine, Jr.
 - Editor ISO/IEC 15026
- Dr. Yoshiki Kinoshita
 - Co-editor for ISO/IEC 15026 Parts 2 and 4
- Dr. Toshinori Takai
 - Co-editor for ISO/IEC 15026 Part 3
- Dr. Karen Richter
 - Co-editor for ISO/IEC 15026 Parts 1, 2, 3, & 4

ISO/IEC 15026 *Systems and software engineering — Systems and software assurance*

PART 1: CONCEPTS AND VOCABULARY

Purpose

- Aid users of Parts 2-4
- Inform other interested parties, e.g. reviewers of Parts 2-4

Scope

- Shared concepts, issues and terminology applicable across a range of properties, application domains, and technologies
- Clarifies concepts central to the use of Parts 2-4 of ISO/IEC 15026.
- The TR will be revised and republished as an IS after the other three parts have been completed.

Contents

- Terms and definitions covering parts
- Basic concepts
- Using, particularly using multiple parts
- Assurance cases
- Integrity levels
- ISO/IEC 15026 and life cycle processes:
ISO/IEC15288/12207
- Numerous annexes

ISO/IEC 15026 *Systems and software engineering — Systems and software assurance*

PART 2: ASSURANCE CASE

Background

- Assurance: grounds for justified confidence that a claim has been or will be achieved
- A claim conforming to ISO/IEC 15026 Part 2 is an unambiguous true-false statement including limitations on values of a property under specified conditions and its associated uncertainty.

Background cont'd.

- An assurance case is reasoned, auditable artefact created to support the contention its claim or claims are satisfied. It contains the following and their relationships:
 - One or more claims about properties.
 - Arguments that logically link the evidence and any assumptions to the claim(s).
 - A body of evidence and possibly assumptions supporting these arguments for the claim(s).

Scope

- Concerned with structure and principal components of an assurance case
- Does not address “quality” of engineering and contents
- Brief

ISO/IEC 15026 *Systems and software engineering — Systems and software assurance*

PART 3: SYSTEM INTEGRITY LEVELS

Background

- **integrity level:** denotation of a range of values of a property
 - A claim regarding a system or system element
- **Integrity requirements** are associated with an integrity level to assure its achievement by imposing requirements on:
 - system, product, or element
 - its development, maintenance, and possibly other life cycle processes including means and actors
 - require evidence to be obtained regarding these

Scope

- Places requirements and offers guidance and recommendations on the specification, assignment, and application of integrity levels and their integrity requirements for systems and products and their elements and dependencies.
 - This includes software
- Does not prescribe:
 - Specific set of integrity levels or integrity requirements
 - How to integrate integrity levels into life cycle

Content

- Risk analysis and evaluation
 - High-level and general
 - Nature of output required to establish system integrity level
- Assigning integrity levels including to elements
- Integrity requirements and relationship to integrity level
- Agreements and approvals

ISO/IEC 15026 *Systems and software engineering — Systems and software assurance*

PART 4: ASSURANCE IN THE LIFE CYCLE

Background

- WD1 out for comment until January 15
- WD1's scope is designed to facilitate comment not to reflect final scope
- Most content derived from existing sources
- Motivated by inclusion of assurance case in life cycle

Scope

- Encompasses the relevant processes, activities, and tasks in order to develop, maintain and provide grounds for confidence and decision-making related to high assurance systems and software and achieving and showing the achievement of the claims being assured.
- It applies across a wide range of situations needing high assurance.

Content

- WD1's content is designed to facilitate comment
- Required purpose and outcomes
- Required activities and tasks with related guidance and recommendations
- Structure parallels ISO/IEC 15288 and 12207, but use of them is not required if life cycle used can be mapped to Part 4
- Almost all guidance and recommendations derived from existing sources

CONCLUSION

ISO/IEC 15026

- Is concerned with grounds for confidence in systems and products
- Is motivated by risks, uncertainty, and adverse consequences and difficult requirements as well as the needs of decision making, e.g. decision to use
- Has four parts covering assurance cases, integrity levels, and life cycle that can be used separately or together as well as with other standards

SC Life cycle standards

- ISO/IEC 15288:2008 Systems engineering
-- System life cycle processes
- ISO/IEC 12207:2008 Information
technology -- Software life cycle processes

Final remarks

- I am interested in
 - Assurance
 - Security
- Supplied some comments on 27034 and 29193
- Here all week