TECHNICAL SPECIFICATION

ISO/IEC TS 15504-10

First edition
2011-11-15

Information technology — Process assessment —

Part 10: Safety extension

Technologies de l'information — Évaluation des procédés —

Partie 10: Extension de sécurité

Reference number
ISO/IEC TS 15504-10:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 The process dimension 2
4.1 Safety Management process 2
4.2 Safety Engineering process 5
4.3 Safety Qualification process 7
5 Life-cycle guidance 9
Annex A (informative) **Work Product Characteristics** 17
Annex B (informative) **Process Reference Model** 22
Bibliography 25

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.

In other circumstances, particularly when there is an urgent market requirement for such documents, the joint technical committee may decide to publish an ISO/IEC Technical Specification (ISO/IEC TS), which represents an agreement between the members of the joint technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/IEC TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/IEC TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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 TS 15504-10 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

ISO/IEC 15504 consists of the following parts, under the general title *Information technology — Process assessment*:

— *Part 1: Concepts and vocabulary*

— *Part 2: Performing an assessment*

— *Part 3: Guidance on performing an assessment*

— *Part 4: Guidance on use for process improvement and process capability determination*

— *Part 5: An exemplar Process Assessment Model*

— *Part 6: An exemplar system life cycle process assessment model* [Technical Report]

— *Part 7: Assessment of organizational maturity* [Technical Report]

— *Part 9: Target process profiles* [Technical Specification]

— *Part 10: Safety extension* [Technical Specification]

The following part is under preparation:

— *Part 8: An exemplar process assessment model for IT service management* [Technical Report]

Introduction

The published ISO/IEC 15504 process assessment models for systems and software do not currently provide a sufficient basis for performing a process capability assessment of processes with respect to the development of complex safety-related systems.

This part of ISO/IEC 15504 provides a general framework in which assessments can take place. However, additional guidance and processes are needed to support the use of the existing process assessment models for systems and software when applied to safety-related systems development in order to make consistent judgment regarding process capability or improvement priorities.

Developing safety-related systems requires specialized processes, techniques, skills and experience. Process amplifications are needed in the area of safety management, safety engineering and the safety qualification. This part of ISO/IEC 15504 presents these amplifications (a safety extension) as three process descriptions. This part of ISO/IEC 15504 also provides additional informative components concerning additional life-cycle verification activities related to the methods and techniques selected relevant to safety requirements adopted and tailoring guidance for users intending to use the safety extension as part of a process assessment.

This part of ISO/IEC 15504, as a standalone document, can be used in conjunction with ISO/IEC 15504-5 and/or ISO/IEC TR 15504-6 process assessment models by experienced assessors with minimal support from safety domain experts.

This part of ISO/IEC 15504 is developed independent of any specific safety standards that define safety principles, methods, techniques and work products. However, elements of relevant safety standards can be mapped to the safety extension and the safety extension is intended to be extendable to include specific safety standards requirements.

NOTE According to the purpose of ISO/IEC 15504, this part is to be considered independent of any domain-specific standard. Consequently, technical engineering solutions and methods as well as specific working products required by any domain-specific safety standard are not explicitly mapped on the safety engineering process and the other processes defined in this part of ISO/IEC 15504. At assessment time, these technical engineering solutions and methods, as well as specific working products, are to be considered by the assessor as project-specific solutions/choices or project requirements related to specific corresponding processes.

Information technology — Process assessment —

Part 10:
Safety extension

1 Scope

This part of ISO/IEC 15504 is a safety extension that defines additional processes and guidance to support the use of the exemplar process assessment models for system and software (ISO/IEC 15504-5 and ISO/IEC TR 15504-6) when applied to assessment of processes in the development of (functional or non-functional) safety-related systems in order to make consistent judgment regarding process capability and/or improvement priorities.

This part of ISO/IEC 15504 is not intended to provide the state of the art for developing or verifying functional or non-functional safety-related systems or components.

NOTE The aim of this part of ISO/IEC 15504 is not to provide a way to verify the compliance with one or more domain-specific safety standards, nor to extend ISO/IEC 15504 in order to use it as a safety standard against which to verify compliance. The aim is to provide assessors with the necessary means and information for measuring the capability of processes and also defining possible process improvement actions when the software/system under development is safety-related.

2 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 document (including any amendments) applies.

ISO/IEC 15504-1:2004, *Information technology — Process assessment — Part 1: Concepts and vocabulary*