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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15504-1 and the following apply.

3.1
hazard
potential source of physical injury or damage to the health of people or damage to property or the environment

[ISO/IEC Guide 51:1999]

3.2
external resource
resource not developed under project control

NOTE Resources not developed under project control include: tools, libraries, COTS, re-use components.

3.3
safety demonstration
body of evidence and rationale that shows an item is justified as being safe within allowed limits on risk

NOTE 1 For example, this might include that an item was designed and integrated correctly to approved standards by competent people in accordance with approved procedures with sufficient mitigation, and tested sufficiently.

NOTE 2 For more information about safety case and assurance case in general, see ISO/IEC 15026.

3.4
safety criteria
limits of acceptable risk associated with a hazard

NOTE These limits may be defined as imposed safety targets or developed from analysis or development policy.

3.5
safety-related incident
incident having an impact on safety

3.6
safety integrity requirement
likelihood of a safety-related system satisfactorily performing the required safety functions under stated conditions

3.7
safety life cycle
project or product life cycle in which safety processes are performed

3.8
safety requirement
requirement that is needed to ensure the safety of the product

4 The process dimension

In this section the definitions of processes needed to support process assessments are defined.

The performance of one or more of the processes in this part of ISO/IEC 15504 is not intended to cover the requirements of any other safety standard. The achievement of a certain capability level in one or more of those processes does not imply the compliance with any other domain specific safety standard.

4.1 Safety Management process

Process ID	SAF.1		
Process Name	Safety Management		
Process Purpose	The purpose of the Safety Management Process is to ensure that products, services and life-cycle processes meet safety objectives.		
Process Outcomes	As a result of the successful implementation of the Safety Management process: 1) Safety principles and safety criteria are established. 2) The scope of the safety activities for the project is defined. 3) Safety activities are planned and implemented. 4) Tasks and resources necessary to complete the safety activities are sized and estimated. 5) Safety organization structure (responsibilities, roles, reporting channels, interfaces with		

	other projects or OUs …) is established. 6) Safety activities are monitored, safety-related incidents are reported, analysed, and resolved. 7) Agreement on safety policy and requirements for supplied products or services is achieved. 8) Supplier's safety activities are monitored.
Base Practices	**SAF.1.BP.1: Define safety objectives and criteria.** The limits of acceptable risk associated with a hazard are defined externally as imposed safety targets or developed from analysis or development policy. Safety targets and/or acceptable levels of risk are determined. [Outcome1] **SAF.1.BP.2: Define Safety Life Cycle.** The Safety Life Cycle is defined, which is appropriate to the context, complexity, safety criteria and targets for the project. [Outcome 2] NOTE 1: Assure Functional safety throughout the product life cycle. For this reason, the safety management includes and reflects all phases of the product life cycle. **SAF.1.BP.3: Perform safety planning.** Safety engineering and management activities are to be implemented in order to meet and verify that safety requirements are identified, their dependencies are determined, their implementation planned, and the resource needs are identified. [Outcome 3] **SAF.1.BP.4: Define safety activities integration.** Safety activities integration with product development, project life cycle and support process is determined. [Outcome 3, 5] NOTE 2: Examples of integration between development life cycle and safety activities can be found in IEC 61508 and ISO 26262. NOTE 3: Safety activities integration is supported by traceability of safety requirements during the development life cycle. **SAF.1.BP.5: Define skills requirements definition and allocate responsibility.** Skills needs for carrying out planned safety activities are identified and responsibilities, authorities, and independence of involved roles are defined and allocated accordingly. [Outcome 3, 4, 5] **SAF.1.BP.6: Implement planned safety activities.** The activities defined in the safety planning are implemented. [Outcome 3] **SAF.1.BP.7: Monitor the deployment of the safety activities.** Monitor the deployment of the safety activities and act to correct deviations: safety activities of the project are monitored, and safety-related incidents identified in work products, and safety activities are reported, analyzed, managed to closure and further prevented. [Outcome 6] **SAF.1.BP.8: Define and agree safety policy and safety requirements with suppliers.** Methods and techniques to monitor supplier's safety activities are agreed with the customer. Define an agreement on how the supplier assures safety of the supplied

	product. [Outcome 7] **SAF.1.BP.9: Monitor the safety activities of the supplier**. Supplier's safety activities to meet the safety requirements are monitored and reported. [Outcome 8] **SAF.1.BP.10: Implement an escalation mechanism.** Develop and maintain the escalation mechanism that ensures that safety issues may be escalated to appropriate levels of management to resolve them. [Outcome 6]
Specific Practices (optional for Levels 2-5)	-

Work Products	
Inputs	Outputs
S-16 Safety requirements	S-10 Safety policy [Outcome: 1,2]
17-03 Customer requirements [ISO/IEC 15504-5]	S-09 Safety Plan [Outcome: 2, 3, 4, 5]
15-06 Project status report [ISO/IEC 15504-5; ISO/IEC TR 15504-6]	08-12 Project plan [Outcome: 2, 3, 4, 5] [ISO/IEC 15504-5]
S-08 Safety log	14-09 Work breakdown structure [Outcome: 2, 3] [ISO/IEC 15504-5]
13-04 Communication record [ISO/IEC 15504-5]	13-04 Communication record [Outcome: 6, 8] [ISO/IEC 15504-5]
02-00 Contract [ISO/IEC 15504-5]	15-06 Project status report [Outcome: 6, 8] [ISO/IEC 15504-5; ISO/IEC TR 15504-6]
02-01 Commitment/agreement [ISO/IEC 15504-5]	S-08 Safety log [Outcome: 6, 7]
S-17 Safety Standards	13-19 Review record [Outcome: 6] [ISO/IEC 15504-5]
S-10 Safety policy	13-16 Change request [Outcome: 6] [ISO/IEC 15504-5]
08-12 Project plan [ISO/IEC 15504-5]	13-01 Acceptance record [Outcome: 6] [ISO/IEC 15504-5]
S-15 Safety regulation	08-24 Training plan [Outcome: 5] [ISO/IEC 15504-5]
10-01 Life-cycle model [ISO/IEC 15504-5]	S-03 Qualification requirements on External resources [Outcome: 4]
	S-07 Safety life-cycle model [Outcome: 2, 3]
	S-05 Safety criteria [Outcome: 1]
	S-04 Safety demonstration [Outcome: 3]

4.2 Safety Engineering process

Process ID	SAF.2		
Process Name	Safety Engineering		
Process Purpose	The purpose of the Safety Engineering process is to ensure that safety is adequately addressed throughout all stages of the engineering processes.		
Process Outcomes	As a result of the successful implementation of the Safety Engineering process: 1) Hazards related to product are identified and analysed. 2) Hazard log is established and maintained. 3) Safety demonstration for the product life cycle is established and maintained. 4) Safety requirements are defined. 5) Safety integrity requirements are defined and allocated. 6) Safety principles are applied to development processes. 7) Impacts on safety of change requests are analysed. 8) Product is validated against safety requirements. 9) Independent evaluations are performed.		
Base Practices	**SAF.2.BP.1: Identify hazard sources and hazards.** Hazard sources and hazards of relevant operational conditions and for foreseeable misuse are identified. [Outcome 1] **SAF.2.BP.2: Analyze hazards and risks.** For each hazard, analyze likelihood and severity of impact, and evaluate the risk of the hazard. [Outcome 1] **SAF.2.BP.3: Establish and maintain hazard log.** Status of hazards is maintained throughout the whole product life cycle. [Outcome 2] **SAF.2.BP.4: Establish and maintain safety demonstration.** Safety demonstration is created and maintained during the life cycle of the product. Process and product documentation is collected for safety demonstration evidence. [Outcome 3] NOTE 1: A safety case is a way to collect and present information for safety demonstration. **SAF.2.BP.5: Establish and maintain safety requirements.** Establish and maintain throughout the life cycle safety requirements based on the results of hazard and risk analysis and any other applicable sources. [Outcome 4] NOTE 2: Applicable sources can be: legislative requirements, standards, regulations, company policies, customer requirements, customer and end user feedback, verification results, quality assurance findings, validation results, safety validation results, production experiences, commissioning and decommissioning experiences, maintenance and repair experiences, and product field studies. **SAF.2.BP.6: Determine safety integrity requirements.** Safety integrity requirements for each safety requirement based on the risk evaluation of their hazards are determined. [Outcome 5]		

	NOTE 3: The appropriateness of a technique for determining safety integrity requirements depends on legal and safety regulatory requirements, accepted good practices, specific hazards, consequences and risks and the availability of data upon which the hazard and risk analysis is to be based. NOTE 4: Safety integrity requirement may be described i.e. as safety integrity level. **SAF.2.BP.7: Allocate safety requirements and safety integrity requirements.** Safety requirements and safety integrity requirements are allocated to architecture, subsystems and components. [Outcome 5] **SAF.2.BP.8: Apply safety principles to achieve safety integrity requirements.** Principles and methods relevant for achieving the required safety integrity requirements are applied during the product life cycle. [Outcome 6] NOTE 5: Principles and methods may include for example avoidance of common cause failures by designing diversity, or use of formal methods, defensive programming or perspective based inspections. **SAF.2.BP.9: Perform safety impact analysis on changes.** Analyse the impact of the change requests on hazards and risks. Traceability between a change request and the affected safety work products is established. [Outcome 7] **SAF.2.BP.10: Perform safety validations on product.** Safety validations should be based on the outcomes of hazard analysis and risk analysis and performed against safety targets. [Outcome 8] **SAF.2.BP.11: Perform independent assessments.** Assessments of product and processes are performed in preset points during the product life cycle according to the required level of independence. [Outcome 9] NOTE 6: The evaluations may include verification or validation of any work product. NOTE 7: The required level of independence may vary from an independent person to independent organisation.
Specific Practices (optional for Levels 2-5)	-