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

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order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn.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again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.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)	-

Work Products	
Inputs	Outputs
S-09 Safety plan	S-01 Hazard analysis report [Outcome: 1, 7]
17-03 Customer requirements [ISO/IEC 15504-5]	15-08 Risk analysis report [Outcome: 1, 7] [ISO/IEC 15504-5]
S-10 Safety policy	S-16 Safety requirements [Outcome: 4, 7]
S-17 Safety standard	S-06 Safety integrity requirements [Outcome: 5]
S-15 Safety regulations	13-22 Traceability record [Outcome: 5, 7] [ISO/IEC 15504-5]
13-16 Change request [ISO/IEC 15504-5]	14-04 Test log [Outcome: 3, 8] [ISO/IEC 15504-5]
	15-05 Evaluation report [Outcome: 9] [ISO/IEC 15504-5]
	S-04 Safety demonstration [Outcome: 3, 6, 7, 9]
	S-18 Safety Validation results [Outcome: 3, 6, 8]
	S-02 Hazard log [Outcome: 2, 3]
	13-04 Communication record [Outcome: 3, 7, 9] [ISO/IEC 15504-5]

4.3 Safety Qualification process

Process ID	SAF.3		
Process Name	Safety Qualification		
Process Purpose	The purpose of the Safety Qualification process is to assess the suitability of external resources when developing a safety-related software or system.		
Process Outcomes	As a result of the successful implementation of the Safety Qualification process: 1) Safety qualification strategy for external resources is developed. 2) Safety qualification plan is developed and executed. 3) Safety qualification documentation is written. 4) Safety qualification report is produced.		
Base Practices	**SAF.3.BP.1**: **Develop a safety qualification strategy.** Develop a qualification strategy. The qualification strategy shall consider the quality requirements of the external resources (reflecting the safety requirements determined for the safety-related software or system). The qualification strategy includes criteria for selecting qualification methods. [Outcome 1] **SAF.3.BP.2**: **Plan the safety qualification of external resources.** Plan the qualification acitivities for the external resources. Select the appropriate qualification method for each external resources. [Outcome 2] NOTE 1: The process of external resources selection is not in the scope of the qualification process. NOTE 2: For the safety qualification it may be helpful to define a classification scheme for external resources. Every class may have a set of qualification methods assigned to it. Examples of external resources are as follows:		

	- core engineering tools - automatic code generators, compilers and linkers; - engineering support tools - test, build and configuration management tools; - management support tools - documentation and project management tools. A classification of these resources based on the impact on software could be: - Core engineering tools are software tools, which have direct impact on the generated source code or binary code and therefore can inject defects into the target software. - Engineering support tools are software tools, which do not have direct impact on the generated source code or binary code, but either they do support the generation of source code or binary code or their mal-function may prevent the detection of defects in the target software. - Management support tools are software tools, which do not have any impact on the generated source code or binary code. NOTE 3: Qualification methods may include - Increased confidence from use - Evaluation of the development process; - Demonstration that the development was based on a safety standard - Validation of the tool - Development in compliance with safety standard - Certification **SAF.3.BP.3: Qualify the external resources.** Execute qualification according to the qualification methods chosen. [Outcome 2] . **SAF.3.BP.4: Record the safety qualification results.** Record the results of the safety qualification and disseminate the results from the qualification to interested parties. [Outcome 3] NOTE 4: The qualification documentation incudes: - Unique identification and version number of the external resources - Configuration of external resources - Qualification method used - Result of qualification **SAF.3.BP.5: Maintain and update the safety qualification results.** Maintain and update the safety qualification results and documentation throughout the usage of the external resources. [Outcome 4]
Specific Practices (for Levels 2-5)	-

Work Products	
Inputs	Outputs
S-09 Safety plan	S-14 Safety qualification strategy [Outcome: 1]
17-03 Customer requirements [ISO/IEC 15504-5]	S-12 Safety qualification plan [Outcome: 2]
S-10 Safety policy	S-13 Safety qualification results [Outcome: 3, 4]
S-17 Safety standard	S-11 Safety qualification documentation [Outcome: 3]
S-15 safety regulations	S-04 Safety demonstration [Outcome: 3, 4]
S-03 Qualification requirements on external resources	
S-04 Safety demonstration	

5 Life-cycle guidance

In comparison to an assessment in a non-safety-related development environment a process assessment of a safety-related development environment provides additional process evidence. This evidence is related both to the specific, additional processes described in clause 4 of this part of ISO/IEC 15504 and also to the particular approach to carrying out systems and software engineering life-cycle processes that is required to address safety-related software/systems issues.

In this clause the influence of the safety extension on the assessment of the processes in the ISO/IEC 15504-5 and ISO/IEC TR 15504-6 is described in a tabular format. The tables provided in this clause give the assessors, for each process contained in ISO/IEC 15504-5 and ISO/IEC TR 15504-6, an indication of additional issues to be taken into account at assessment time. The issues are provided by means of sentences indicating specific relationships between ISO/IEC 15504-5 and ISO/IEC TR 15504-6 processes and the ISO/IEC TS 15504-10 processes as well as highlighting relevant aspects to be considered to improve the completeness of the data gathering phase of the assessment. In this way, an assessor can use the table to check whether, in assessing a ISO/IEC 15504-5 or ISO/IEC TR 15504-6 process, some relevant aspects related to the safety development environment have been missed.

Table 1 — ISO/IEC 15504-5 processes assessment in a safety-related context

ISO/IEC 15504-5 process	Related Safety process	Effect of safety context	Notes
ENG.1: Requirements Elicitation	SAF.2	Elicitation includes data and information necessary to define safety requirements as well as to identify hazards and risks.	
ENG.2: System Requirements Analysis	SAF.2	System safety requirements and system safety integrity requirements are derived from the relevant regulations and standards as well as the outcomes of the hazard analysis and risk analysis. Safety requirements are integrated and harmonized with the overall (system) requirements specifications.	
ENG.3: System Architectural Design	SAF.2	The system architecture and functional decomposition satisfies the system safety requirements. Traceability between system elements and system safety requirements and system safety integrity requirements is defined and maintained. Impact on safety of external and internal interfaces	

		of the system is analyzed.	
ENG.4: Software Requirements Analysis	SAF.2	Software safety requirements are specified and the impact on the achievement of other software requirements is analyzed. Impact of operating environment on software safety requirements is analyzed.	
ENG.5: Software Design	SAF.2	Design solutions meet software safety requirements. The safety-related software design features are analyzed to ensure their testability.	
ENG.6: Software Construction	SAF.2	Safety requirements of a software unit are implemented and tested. Regression test set is created and maintained to ensure that safety features of software are not affected by changes.	Specific testing techniques can be aimed at showing that no other functionality is implemented. Specific test coverage measures can be required.
ENG7: Software Integration	SAF.2	Regression test set is created and maintained to ensure that safety features of software are not affected by changes.	
ENG8: Software Testing	SAF.2	Safety requirements for the entire software are tested. Regression test set is created and maintained to ensure that safety features of software are not affected by changes.	
ENG9: System Integration	SAF.2	Regression test set is created and maintained to ensure that safety features of software are not affected by changes.	
ENG10: System Testing	SAF.2	System safety features are tested. Regression test set is created and maintained to ensure that safety features of software are not affected by changes.	
ENG11: Software Installation	SAF.2	No safety-specific effects	Special care is to be made for software and parameters installation into the target system.
ENG.12: Software and System Maintenance	SAF.2	Change requests are analyzed for their impact on safety. Risks associated with the maintenance activities are assessed. Safety-related verification and validation activities are performed as appropriate with respect to	

		changes made.	
ACQ.1: Acquisition Preparation	SAF.1, SAF.3	Additional safety-related obligations and requirements are stated in the acquisition requirements in order to communicate these to the potential suppliers. Acquisition strategy contains supplier and acquirer responsibilities with respect to these requirements.	
ACQ.2 Supplier Selection	SAF.1	The capability required to meet the obligations and requirements described in ACQ.1 is defined and suppliers with that capability are selected. An agreement defining the supplier's responsibility with respect to system safety is negotiated.	
ACQ.3 Contract Agreement	SAF.1, SAF.2	A contract defining the acquirer's and the supplier's expectations, responsibilities and liabilities with respect to system safety is put in place with the selected supplier(s).	
ACQ.4 Supplier Monitoring	SAF.1	The supplier's performance of safety-related activities is known to the acquirer.	
ACQ.5 Customer Acceptance	SAF.1	The acquirer accepts the system as meeting the agreed safety requirements.	This process may include negotiation.
SPL.1: Supplier Tendering	SAF.1	The scope of proposal requests includes the development of safety-related systems. Safety requirements, safety integrity requirements are analyzed and required safety activities, competencies, skills and infrastructures are estimated.	
SPL.2: Product Release	SAF.2, SAF.3	The release documentation includes the demonstration of compliance with safety requirements.	
SPL.3: Product Acceptance support	SAF.1, SAF.2, SAF.3	The product is handed to the customer with relevant safety information. The product is adapted to work safely in the operational environment. Training related to safety is conducted as specified in the contract	Training on safety may range from an introduction to safety features to qualification of staff.
OPE.1: Operational Use	SAF.1, SAF.2	The safe operation of the product is ensured for the duration of its intended usage and in its operational environment. Product use is monitored and analyzed to identify emerging safety issues.	
OPE.2: Customer Support	SAF.1	The customer/user raises safety-related problems occurred in use of the product.	

		Customer support contributes to the safe operation of the product.	
PIM.1: Process Establishment	SAF.1, SAF.2,SAF.3	A standard set of safety processes is established, along with an indication of each process's applicability. Implementation and tailoring guidance is established for safety processes.	
PIM.2: Process Assessment	SAF.1, SAF.2, SAF.3	Adaptability of the standard processes to the process requirements from applicable domain-specific safety standards is taken into account. According to the assessment purpose, the SAF.1, SAF.2 and SAF.3 processes can be in the scope of the assessment.	
PIM.3: Process Improvement	SAF.1, SAF.2, SAF.3	Safety-related improvement objectives have higher priority	
MAN.1: Organizational Alignment	SAF.1	Safety of products and services is to be addressed in the definition of the organization's business goals and the process framework. Safety culture is to be promoted and verified at organization level.	
MAN.2: Organizational Management	SAF.1	Safety management practices and management infrastructures should be taken into account as part of the organization management process.	In particular, when a domain-specific safety standard is adopted, the organization management should provide the necessary support for accomplishment with the applicable clauses.
MAN.3: Project Management	SAF.1	Estimations, life-cycle definition, planning, allocation of responsibilities, tracking and controlling, taking corrective actions and reporting for safety-related and non safety-related activities are to be performed in an integrated manner in order to avoid any possible conflicts or missing responsibility. Safety organizational structure (in particular independence of roles) is an important aspect.	
MAN.4: Quality Management	SAF.1	The quality management system incorporates safety management activities, resources and responsibilities avoiding conflicts and lacks.	

MAN.5: Risk Management	SAF.1, SAF.2	Safety-related hazard and risks identification and risk analysis, evaluation, treatment and monitoring are integrated into the overall risk management strategy avoiding conflicts and omissions.	
MAN.6: Measurement	SAF.1, SAF.2, SAF.3	Safety-related measurements and analysis data are managed by this process and are taken into account in the measurements strategy avoiding conflicts and lacks.	
RIN1:Human Resources Management	SAF.1	Needed safety-related skills and competencies are identified. The competence of staff is developed and evaluated; new staff is recruited based on the needs.	See RIN.2 for competence development.
RIN.2: Training	SAF.1	The organization and project have to be provided with individuals who possess the needed safety-related skills, knowledge, qualifications, certifications and authorizations to perform their roles effectively. These may be domain-specific.	
RIN3:Knowledge Management	SAF.1, SAF.2	Relevant knowledge about safety is managed. This includes organizational, legislative, generic technical and domain specific technical knowledge.	
RIN4:Infrastructure	SAF.1, SAF.2, SAF.3	Infrastructure requirements for safety related processes are identified. The risks associated with deficiencies are managed.	
REU.1: Asset Management	SAF.1, SAF.3	Safety attributes (e.g. safety integrity requirements) are included in the reuse asset classification scheme. Criteria for safety-related reuse asset acceptance, certification and retirement are defined.	
REU.2: Reuse Program Management	SAF.1, SAF.3	The reuse program management process takes into account the identified safety attributes and ensures the suitability of safety-related reuse products through the safety qualification process.	See REU.1
REU.3: Domain Engineering	SAF.3	Safety and safety integrity requirements are incorporated into the criteria for domain definitions, models, and architectures. Domain-specific assets reflect the safety-related criteria. Changes to the domain models and architectures are evaluated with respect to the safety-related criteria.	See REU.1
SUP.1: Quality Assurance	SAF.1, SAF.2, SAF.3	Safety-related products, processes and activities are covered by the quality assurance process. Verification of adherence to applicable safety standards is part of this process.	Quality assurance is typically independent of the development project.
SUP.2: Verification	SAF.2	The performance of safety-related verification activities and the identification and record of possible	

		safety-related detected defects is incorporated into this process	
SUP.3: Validation	SAF.2	Software safety validation activities are incorporated into and harmonized with the other software validation activities.	Software safety validation should be aligned with system safety validation (see Table 2 - TEC.8)
SUP.4: Joint Review	SAF.1	Safety aspects (e.g. compliance with domain-specific safety standards, safety evaluation of work products) may be included in the scope of joint reviews when required/necessary.	
SUP.5: Audit	SAF.1	Safety audits by an independent party are included into the audit strategy when required by specific safety standards or when necessary	
SUP.6: Product Evaluation	SAF.2, SAF.3	Safety evaluation is carried out when a product is used in an environment or application with different potential hazards, or with a different set of users. Stated and implied needs are derived from hazard analysis, incident analysis or context of use analysis.	
SUP.7: Documentation	SAF.1, SAF.2, SAF.3	Recorded information associated with development of safety-related system (e.g. safety case, qualification, safety requirements) is part of the documentation process.	
SUP.8: Configuration Management	SAF.1, SAF.2, SAF.3	Safety-related items are under configuration management to guarantee their integrity and availability.	
SUP.9: Problem Resolution Management	SAF.1, SAF2	Problems related to safety are included in the problem resolution management.	Investigation and diagnosis of the cause of problems related to safety include specific techniques (e.g. fault tree analysis)
SUP.10: Change Request Management	SAF,1, SAF.2	The analysis of changes identifies the impact on safety.	Particular attention should be paid to verification and validation activities for safety-related changes.

Table 2 — ISO/IEC TR 15504-6 processes assessment in a safety-related context

ISO/IEC TR 15504-6 process	Related Safety process	Safety influence description	Title/Notes
AGR.1: Acquisition	SAF.1	The acquisition relationship, including level of assurance and need to perform safety processes, are supervised.	Table 1 ACQ.1-5 contain more details of acquirer's responsibilities with respect safety
AGR.2: Supply	SAF.2	The need for safety processes is identified and the supplier's capability to meet safety requirements is demonstrated.	Table 1 SPL.1-3 contain more details of supplier's responsibilities with respect safety
ENT.1: Life Cycle Model Management	SAF.1	Safety processes are defined, maintained and their availability is assured.	
ENT.2: Project Portfolio Management	SAF.1	Participation in safety-related/critical projects is decided. The necessary levels of investment are made available.	
ENT.3: Infrastructure Management	SAF.1, SAF.3	Enabling infrastructure and services for safety activities are provided throughout the life cycle.	
ENT.4: Human Resource Management	SAF.1	Sufficient people with the required skills to perform safety-related activities are provided.	
ENT.5: Quality Management	SAF.1	The quality management system addresses safety management activities, resources and responsibilities.	
PRJ.1: Project Planning	SAF.1	Project planning determines the activities, schedule, products and resources needed to address safety.	
PRJ.2: Measurement	SAF.1, SAF.2	Measurements related to safety are defined, collected and analyzed in order to support decisions and demonstrate the achievement of product safety.	
PRJ.3: Project Assessment and Control	SAF.1, SAF.2	Monitor project status and direct project plan execution to ensure that safety requirements are met (this includes re-planning as appropriate to address identified deviations and variations).	
PRJ.4: Decision Management	SAF.1, SAF.2	When safety is a required system quality decision management will be guided by safety criteria.	
PRJ.5: Risk Management	SAF.1, SAF.2	Where risks include safety risks, they are identified, analyzed and treated continuously.	

PRJ.6: Configuration Management	SAF.1, SAF.2, SAF.3	Safety-related items are under configuration management to guarantee their integrity and availability.	
PRJ.7: Information Management	SAF.1, SAF.2, SAF.3	Required safety-related information is provided to all designated processes and parties throughout the life cycle.	
TEC.1: Stakeholder Requirements Management	SAF.2	The stakeholders, their effect on system safety, their need for health and safety and the societal risk with respect to the system of interest are detailed.	
TEC.2: Requirements Analysis	SAF.2	The safety requirements for the system of interest with appropriate integrity and traceability requirements are defined and analyzed.	Safety requirements may include performance, properties, constraints, functions.
TEC.3: Architectural Design	SAF.2, SAF.3	A system architecture and a functional decomposition that satisfy the system safety requirements are developed.	
TEC.4: Implementation	SAF.2, SAF.3	Components of the system with specified safety properties are produced.	
TEC.5: Integration	SAF.2, SAF.3	Components to realise the system consistent with the architectural design and the safety requirements are brought together.	
TEC.6: Verification	SAF.1	The fulfilment of safety requirements is verified.	
TEC.7: Transition	SAF.1	System is put into service taking account of operational safety requirements and management. Collection of qualification data related to installation.	
TEC.8: Validation	SAF.2	Objective evidence that the services provided by a system when in use comply with safety requirements achieving its intended use is provided.	
TEC.9: Operation	SAF.1, SAF.2	In-service feedback and incident reports are collected and analysed in terms of safety. Corrective actions maintain safety performance.	
TEC.10: Maintenance	SAF.1	Maintenance actions maintain safety performance.	
TEC.11: Disposal	SAF.1, SAF.2, SAF.3	The system is deactivated, disabled and removed from use in accord with the safety requirements.	
TLR.1: Tailoring	SAF.1	System life-cycle processes are adapted according to safety management requirements	

Annex A
(informative)

Work Product Characteristics

Work product characteristics listed in this Annex can be used when reviewing potential inputs and outputs of process implementation. The characteristics are provided as guidance for the attributes to look for, in a particular sample work product, to provide objective evidence supporting the assessment of a particular process. A documented process and assessor judgment is needed to ensure that the process context (application domain, business purpose, development methodology, size of the organization, etc.) is considered when using this information. Work products are defined using the schema in Table B.1. Work products and their characteristics should be considered as a starting point for considering whether, given the context, they are contributing to the intended purpose of the process, not as a check-list of what every organization must have.

The characteristics of work products mentioned in clauses 4.1, 4.2, and 4.3 having the identifier in the format S-xx are provided in this Annex A. For the characteristics of the others refer to ISO/IEC 15504-5 and ISO/IEC TR 15504-6.

Table A.1 — Work product identification

Work product Identifier #	An identifier number for the work product which is used to reference the work product.
Work product name	Provides an example of a typical name associated with the work product characteristics. This name is provided as an identifier of the type of work product the practice or process might produce. Organizations may call these work products by different names. The name of the work product in the organization is not significant. Similarly, organizations may have several equivalent work products which contain the characteristics defined in one work product type. The formats for the work products can vary. It is up to the assessor and the organizational unit coordinator to map the actual work products produced in their organization to the examples given here.
Work product characteristics	Provides examples of the potential characteristics associated with the work product types. The assessor may look for these in the samples provided by the organizational unit

WP ID	WP Name	WP Characteristics
S-01	Hazard analysis report	- Identifies the hazards analysed - Record the results of the analysis: -assumptions made -context-related elements considered in the analysis -constraints -classification/evaluation of the effects of hazards
S-02	Hazard log	- Identifies what hazard were identified - Describes hazards
S-03	Qualification requirements on external resources	- identifies the external resources under safety qualification - identifies the quality (reliability, availability, maintainability, ...) requirements for each external resource under safety qualification - identifies applicable sources of qualification requirements definition - defines measurable qualification requirements on the external resources under qualification
S-04	Safety demonstration	- Provides documentation or references to: - Hazard and risk analysis results - review minutes - test records - implementation design - validation test results - safety audit reports - project safety planning and management - safety log - external resources qualification results - Pre-existing resources safety qualification results
S-05	Safety criteria	- Defines the expectations for safety: -establishes the limits of acceptable risk associated with a hazard

		-establishes safety targets
S-06	Safety integrity requirements	- identifies safety-related functional requirements - provides an evaluation of the conditions under which the probability the safety-related functional requirements - provides the evaluation of the probability the safety-related functional requirements are satisfactorily performed under the defined conditions
S-07	Safety life-cycle model	- provides high level description of activities to be performed for safety - provides the sequencing of the safety life-cycle phases - identifies dependences among safety life-cycle phases - identifies required inputs and outputs at each safety life-cycle phase - identifies the key decision points (milestones) in the model - identifies the safety control points in the model
S-08	Safety log	- Registers the safety assessment evidences and results over the product life cycle - Identifies what evidences have been used - Identifies time and place of the assessment - Identifies responsible and involved persons for the safety assessment
S-09	Safety plan	- Provides project-related safety objectives and goals - Describes activities and tasks required to ensure safety/comply with safety requirements - Supports the integration of safety engineering with other processes - References to related work products - Provides methods for and scheduling of activities for assessing/verifying compliance to safety requirements - References to any regulatory requirements and standards - identifies safety criteria - Describes safety monitoring and control activities - Provides target timeframe to achieve safety requirements - Indicates methods to achieve safety requirements and goals