ISO/IEC 15504 – Part 10
Safety Extension

Giuseppe Lami
Istituto di Scienza e Tecnologie dell'Informazione
Consiglio Nezionale delle Ricerche
Pisa

ISO/IEC 15504 – Part 10

talk overview

- Foundation of the draft
- Status
- Structure of the ISO/IEC 15504 Part 10
- Relationship with existing safety-related standards
- Conclusions

ISO/IEC 15504 – Part 10

Editorial Team

Giuseppe Lami – Italy (project editor)

Klaudia Dussa-Zieger – Germany (co-editor)

Jonathan Earthy – UK (co-editor)

Mika Johansson – Finland (co-editor)

ISO/IEC 15504 – Part 10

Foundations

- The ISO/IEC 15504 standard does provide a general framework in which assessments can take place.
- Developing safety related systems requires specialised processes, techniques, skills and experience.
- The scope of the ISO/IEC 15504 Part 10 is to develop 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 Parts 5 and 6) when applied to the assessment of safety related systems developments
- The aim is to make consistent judgment regarding process capability and/or improvement priorities.

ISO/IEC 15504 – Part 10

Content structure

- Target document: single Technical Report Type 2 **as ISO/IEC TR 15504 Part 10**
- Two main parts:
  - Core processes definition
    - Safety management process
    - Safety engineering process
    - Tool qualification process
  - Specific guidance on how safety-related issues have to be addressed in the system and software lifecycle processes.

ISO/IEC 15504 – Part 10

Status

- Core processes definition completed
- Lifecycle guidance: not defined yet. This part will be defined after discussions at the Lima meeting.

ISO/IEC 15504 – Part 10 – clause 4.1

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	1. Safety principles and criteria are established to satisfy safety functions. 2. The scope of the safety activities for the project is defined 3. Safety activities are planned and implemented covering safety engineering, supporting safety verification, validation, and independent assessment activities. 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 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

ISO/IEC 15504 – Part 10 – clause 4.2

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	1. Hazards related to product are identified and analysed ; 2. Hazard log is established and maintained ; 3. Assurance case for the product lifecycle is established and maintained; 4. Safety requirements are defined; 5. Safety integrity requirements are defined and allocated to software elements; 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 ;

ISO/IEC 15504 – Part 10 – clause 4.3

Process Name	Tool Qualification
Process Purpose	The purpose of the Tool Qualification process is to assess the suitability of (software) tool for use when developing a safety-related software or system.
Process Outcomes	As a result of the successful implementation of the Tool Qualification process: 1) tool qualification strategy is developed 3) tool qualification plan is developed and executed 4) tool documentation is written 5) tool qualification report is produced

ISO/IEC 15504 – Part 10 – clause 4.4

Process Name	COTS and Reuse component Qualification process
Process Purpose	
Process Outcomes	

Under balloting among the editorial team members

ISO/IEC 15504 – Part 10 – clause 5

- Purpose:
  - to define the impact of the safety extension on the existing ISO/IEC 15504 processes.
  - To provide specific guidance on how safety-related issues have to be addressed in the system and software lifecycle processes.

Processes in clauses 4.x **+**
guidance in clause 5 **=**

a sufficient basis for performing a process capability assessment of processes with respect to the development of complex safety critical systems

ISO/IEC 15504 – Part 10 vs. Existing safety standards

- The Safety Extension aims at being independent of any specific safety standards that define safety principles, methods, techniques and work products;
- Elements of relevant safety standards will be able to be mapped to the Safety Extensions
  and
  Safety Extensions will be extendable to be able to include specific safety standards requirements.

ISO/IEC 15504 Part 10 vs. ISO 26262

QUESTION	ISO/IEC 15504 Part	ISO/IEC 26262
Does it provide a Life Cycle for safety critical system/software? Model	No	Yes
Does it address the way risk evaluation and hazard analysis are to	No	Yes
Does it defines safety-specific	Yes	At some extent
Does it make sense talking about “compliance with it”?	No	Yes
Does it make sense using it for process capability determination?	Yes	No
Does it provide an approach for risk classification?	No	Yes
Does it address the SIL (ASIL)	No	Yes

ISO/IEC 15504 Part 10 vs. ISO 26262

- Can some relations be found between ISO/IEC 15504 Part 10 and ISO/IEC 26262?
  - Being compliant with ISO/IEC 26262 is a way to cover the processes in the ISO/IEC 15504 l

Capability	Yes
Capability level 1	Yes
Capability level 2	at some extent
Capability level 3	probably not

Conclusions

- ISO/IEC 15504 Part 10 aims at allowing the use of SPICE in organisations developing safety critical systems by assuring that all the process activities can be considered in the assessment and then evaluated according to the SPICE's PAM.
- Three core processes have been defined so far
  (+ 1 aadditonal in the next WD?)
- ISO/IEC 15504 Part 10 stays at a different level respect the ISO/IEC 26262: the first addresses the process level while the other the project level

THANKS FOR YOUR ATTENTION

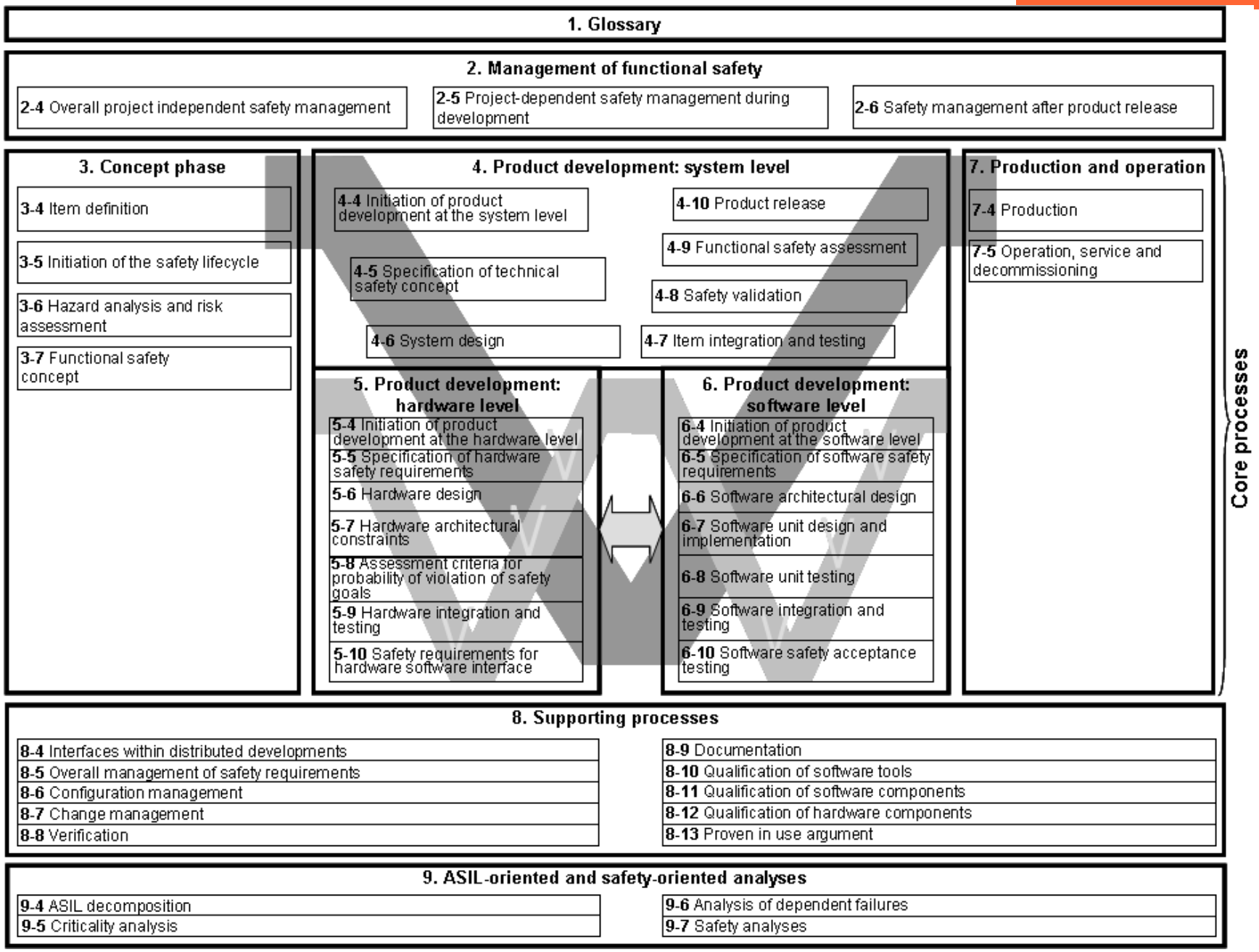
Giuseppe Lami, Phd

giuseppe.lami@isti.cnr.it

ISO/IEC 15504 – Part 10 vs. ISO/IEC 26262

AUTOMOTIVE SPIN ITALIA

  - Provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases;
  - Provides an automotive specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs);
  - Uses ASILs for specifying the item's necessary safety requirements for achieving an acceptable residual risk; and
  - Provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved.
- Functional safety is influenced by the development process (including such activities as requirements specification, design, implementation, integration, verification, validation and configuration), the production and service processes and by the management processes.
- Safety issues are intertwined with common function-oriented and quality-oriented development activities and work products. This International Standard addresses the safety-related aspects of the development activities and work products.


1. Glossary
2. Management of functional safety
2-4 Overall project independent safety management
2-5 Project-dependent safety management during development
2-6 Safety management after product release
3. Concept phase
3-4 Item definition
3-5 Initiation of the safety lifecycle
3-6 Hazard analysis and risk assessment
3-7 Functional safety concept
4. Product development: system level
4-4 Initiation of product development at the system level
4-5 Specification of technical safety concept
4-6 System design
4-7 Item integration and testing
4-8 Safety validation
4-9 Functional safety assessment
4-10 Product release
5. Product development: hardware level
5-4 Initiation of product development at the hardware level
5-5 Specification of hardware safety requirements
5-6 Hardware design
5-7 Hardware architectural constraints
5-8 Assessment criteria for probability of violation of safety goals
5-9 Hardware integration and testing
5-10 Safety requirements for hardware software interface
6. Product development: software level
6-4 Initiation of product development at the software level
6-5 Specification of software safety requirements
6-6 Software architectural design
6-7 Software unit design and implementation
6-8 Software unit testing
6-9 Software integration and testing
6-10 Software safety acceptance testing
7. Production and operation
7-4 Production
7-5 Operation, service and decommissioning
Core processes
8. Supporting processes
8-4 Interfaces within distributed developments
8-5 Overall management of safety requirements
8-6 Configuration management
8-7 Change management
8-8 Verification
8-9 Documentation
8-10 Qualification of software tools
8-11 Qualification of software components
8-12 Qualification of hardware components
8-13 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-4 ASIL decomposition
9-5 Criticality analysis
9-6 Analysis of dependent failures
9-7 Safety analyses