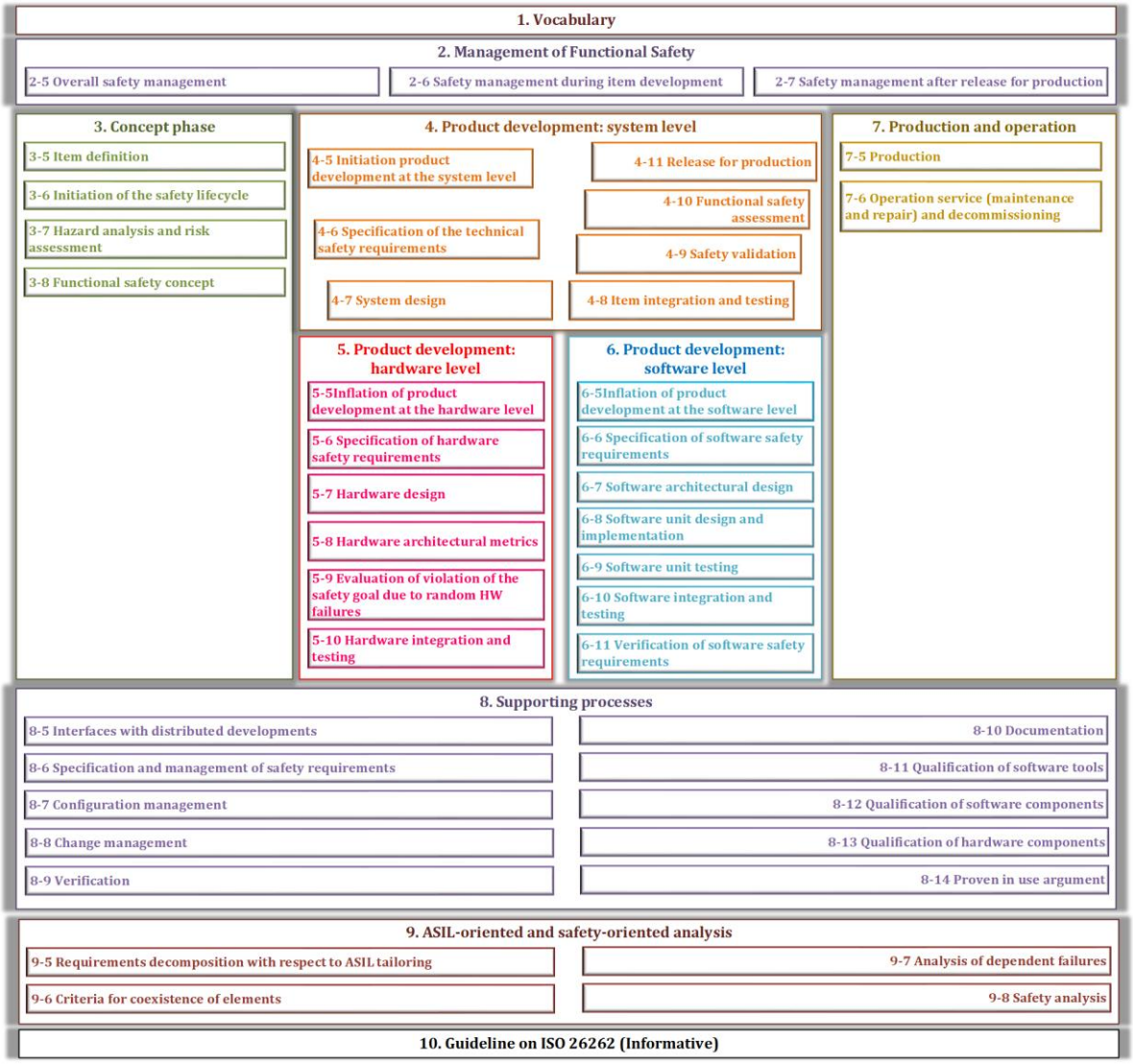
COURSE 3

ISO26262



Part 2 - Management of functional safety

ISO 26262 provides a standard for functional safety management for automotive applications, defining standards for overall organizational safety management as well as standards for a safety life cycle for the development and production of individual automotive products. The ISO 26262 safety life cycle described in the next section operates on the following safety management concepts [3]:

Hazardous Event

A *hazardous event* is a relevant combination of a vehicle-level *hazard* and an operational situation of the vehicle with potential to lead to an accident if not controlled by timely driver action.

Safety Goal

A *safety goal* is a top-level safety requirement that is assigned to a system, with the purpose of reducing the risk of one or more *hazardous events* to a tolerable level.

Automotive Safety Integrity Level

An *Automotive Safety Integrity Level* (ASIL) represents an automotive-specific risk-based classification of a *safety goal* as well as the validation and confirmation measures required by the standard to ensure accomplishment of that goal.

Safety Requirement

Safety requirements include all *safety goals* and all levels of requirements decomposed from the safety goals down to and including the lowest level of functional and technical safety requirements allocated to hardware and software components.

Functional Safety Management requires:

- Planning, coordinating, and documenting activities related to functional safety
- Implementing management plan for all phases of the safety lifecycle, including:
  1. Overall project-independent functional safety management activities.
  2. Safety management during development.
  3. Safety management after Start of Production (SOP).

1. *Overall project-independent functional safety management activities*
   - Objectives
     - ✓ Define responsibilities of persons, departments and organisations in charge of each phase during the overall safety lifecycle.
     - ✓ Define management activities during the complete safety lifecycle.
   - Management plan to incorporate:
     - ✓ Safety culture.
     - ✓ Quality management.
     - ✓ Continuous improvement.
     - ✓ Training and qualification.
     - ✓ Application of the lifecycle.
2. *Safety management during development*
   - Objectives
     - ✓ To define responsibilities of the persons, departments and organisations in charge of functional safety for each phase during development.
     - ✓ Includes activities to ensure functional safety of the item.
     - ✓ Includes activities for confirmation of functional safety measures.
     - ✓ Define management activities during the development phases
   - Management plan to incorporate:
     - ✓ Allocation of safety responsibilities and duties.
     - ✓ All safety management activities during development.
     - ✓ Safety case.
     - ✓ Confirmation measures for assessment of functional safety.
3. *Safety management after Start of Production*
   - Objectives
     - ✓ To define responsibilities of persons, departments and organisations in charge of functional safety after SOP.
     - ✓ Relates to general activities necessary to ensure the required functional safety of the item.
   - Requirements
     - ✓ Organizational measures to achieve functional safety.
     - ✓ Management of functional safety after SOP.

- ✓ Field monitoring and collection of data.
- ✓ Malfunction survey.
- ✓ Malfunction analysis.
- ✓ Malfunction solution.

Parts 3-7 - Safety Life Cycle

Processes within the ISO 26262 *safety life cycle* identify and assess hazards (safety risks), establish specific safety requirements to reduce those risks to acceptable levels, and manage and track those safety requirements to produce reasonable assurance that they are accomplished in the delivered product. These safety-relevant processes may be viewed as being integrated or running in parallel with a managed requirements life cycle of a conventional Quality Management System:

- An *item* (a particular automotive system product) is identified and its top-level system functional requirements are defined.
- A comprehensive set of *hazardous events* are identified for the *item*.
- An *ASIL* is assigned to each *hazardous event*.
- A *safety goal* is determined for each *hazardous event*, inheriting the ASIL of the hazard.
- A vehicle level *functional safety concept* defines a *system architecture* to ensure the *safety goals*.
- *Safety goals* are refined into lower-level *safety requirements*.

(In general, each safety requirement inherits the ASIL of its parent safety requirement/goal. However, subject to constraints, the inherited ASIL may be lowered by decomposition of a requirement into redundant requirements implemented by sufficiently independent redundant components.)

- "Safety requirements" are allocated to *architectural components* (subsystems, hardware components, software components).

(In general, each component should be developed in compliance with standards and processes suggested/required for the highest ASIL of the safety requirements allocated to it.)

- The architectural components are then developed and validated in accord with the allocated safety (and functional) requirements.

Part 3 - Concept Phase

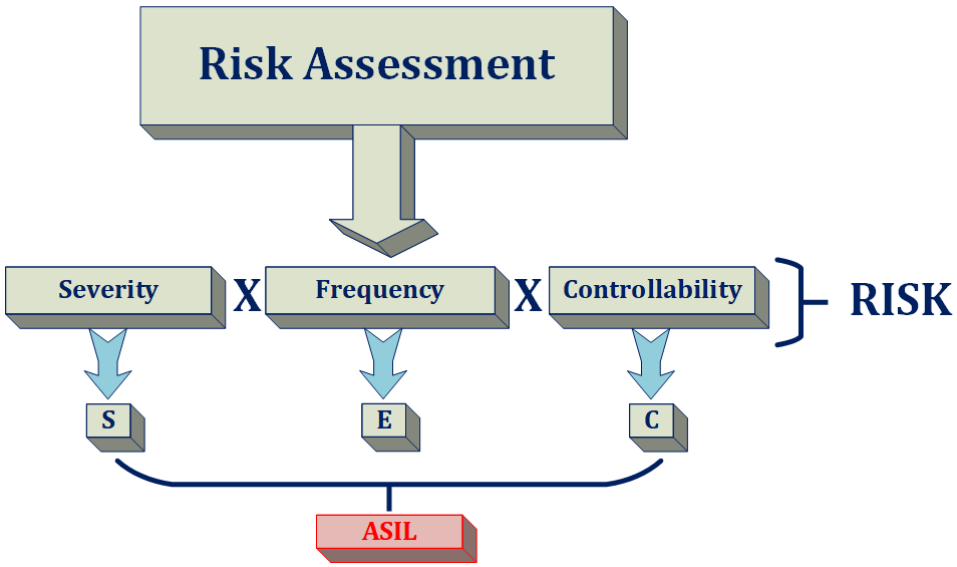
A. Identify relevant safety lifecycle steps

Safety Lifecycle for given item is adapted based on:

- ➢ "New development"
  - ✓ Consider all safety lifecycle steps relevant.
- ➢ "Modification" of an existing component/system
  - ✓ Tailor safety lifecycle following an impact analysis of the modifications.
  - ✓ Impact analysis considers the "proven in use argument" if original component/system was not developed based on ISO 26262.

B. Perform a Hazard Analysis

Determine ASIL



Severity	S0	S1	S2	S3
	No injury	Light and moderate injury	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Exposure	E0	E1	E2	E3	E4
	Incredible	Very low probability	Low probability	Medium probability	High probability

Controllability	C0	C1	C2	C3
	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

C. Identify Safety Goals

- Safety Goals are top-level safety requirement as a result of the hazard analysis and risk assessment.
- A safety goal is to be determined for each hazardous event evaluated in the hazard analysis.
- ASIL determined for the hazardous event is to be assigned to the corresponding safety goal.
- Potential hazard may have more than one safety goal.
- If similar safety goals are determined, they can be combined into one safety goal that will be assigned the highest ASIL of the similar goals.

Part 4 - Product Development: System Level

4.6. Specification of the Technical Safety Requirements

- Objective is to develop the technical safety requirements, which refine the functional safety concept considering the preliminary architectural design.
- To verify through analysis that technical safety requirements comply to the functional safety requirements.
- To bring item-level functional safety requirements into system-level technical safety requirements, down to the allocation to hardware and software elements.

4.7. System Design

- To develop the system design and the technical safety concept that comply with the functional requirements and the technical safety requirements specification.
- Verify the System design and technical safety concept comply with Technical safety requirements specification.
- Need to have bidirectional traceability between System design and Technical safety requirements specification.

4.8. Item integration and testing

- To integrate the different parts that compose the system, included other technologies and/or external entities, and to test the obtained product to comply with each safety requirement and to verify that the design has been correctly implemented.
- The integration and testing are carried out from software-hardware integration and going through integration of systems up to vehicle integration, with specific tests performed at each integration phase.

4.9. Safety Validation

- To provide evidence of due compliance with the functional safety goals and that the safety concepts are appropriate for the functional safety of the item.
- To provide evidence that the safety goals are correct, complete and fully achieved at vehicle level.
- The validation plan shall include:

1. The configuration of the item.
2. The specification of test cases and acceptance criteria.
3. The required environmental conditions.

4.10. Functional safety assessment

- To assess the functional safety that is achieved by the item.

4.11. Release for Production

- To specify the criteria for the release for production at the completion of the item development.
- The release for production confirms that the item complies with the requirements for functional safety at vehicle level.
- The documentation shall include

a) the name and signature of the person in charge of release;

b) the version/s of the released item;

c) the configuration of the released item;

d) references to associated documents;

e) the release date.

Part 5 - Product Development: Hardware Level

Overview

- Identify relevant safety lifecycle steps for item hardware engineering.
- Identify Hardware safety requirements.
- Design hardware, protecting for safety concerns.
- Assess architectural constraints.
- Evaluate probability of violation of a safety goal.
- Hardware safety integration and test [9].

Establish Target Safety Goal Metrics

- Single Point Fault: fault leads directly to the violation of the safety goal.
- Residual Fault: portion of a fault, not covered by a safety mechanism, that by itself leads to the violation of a safety goal.
- Dual/Multiple Point Fault: combination of two/multiple independent faults that leads directly to the violation of a safety goal.
- Latent Fault: multiple point fault whose presence is not detected by a safety mechanism nor perceived by the driver.
- Safe Faults: fault whose occurrence will not significantly increase the probability of violation of a safety goal [9].

ASIL	Single Point Fault Metric	Latent Multiple Point Fault Metic
B	> 90%	> 60%
C	>97%	>80%
D	>99%	>90%