COURSE 4

Part 6 - Product Development: Software Level

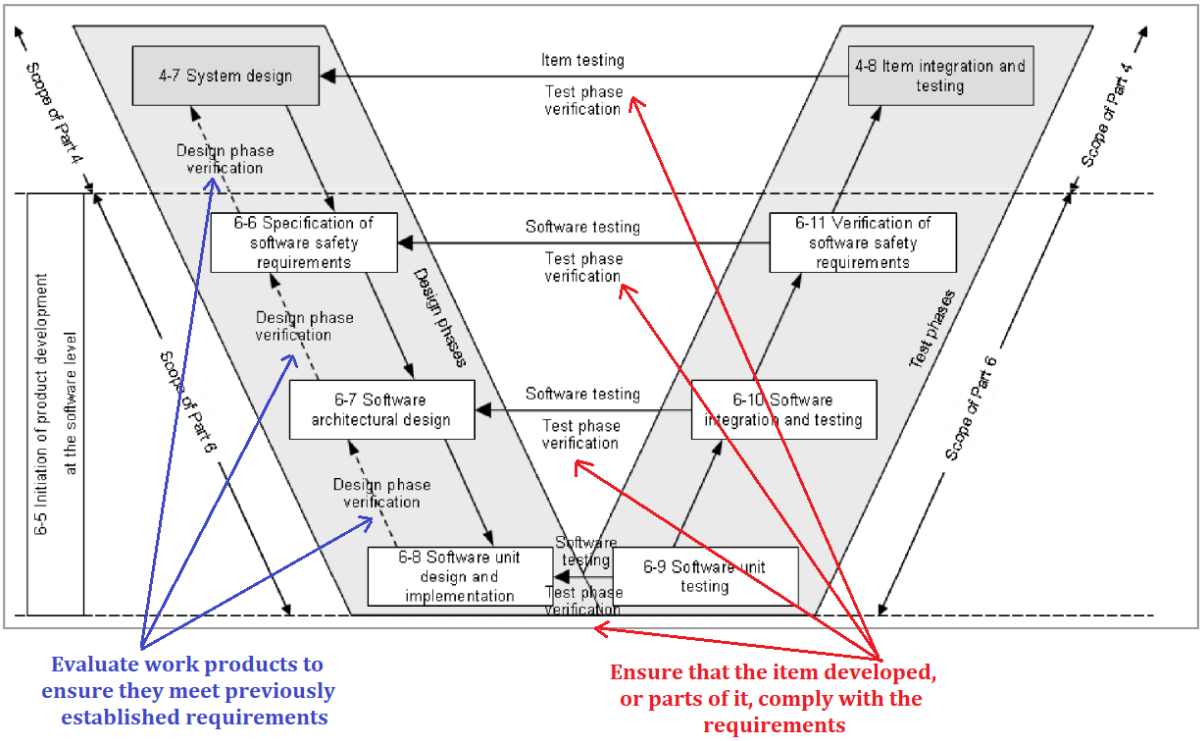
Overview

A. Planning

- Software development activities for functional safety.
- Supporting processes.
- Methods to achieve requirements of assigned ASIL.
- Guidelines and tools.
- Coordination with product development at hardware level.

B. Lists requirements to be satisfied for each phase of the software development lifecycle

- Dependent on ASIL.



Part 7 - Production and Operation

- Specifies requirements on production, operation, service, and decommissioning.
- Production objectives.
  - ✓ Develop a production plan for safety-related products.
  - ✓ Ensure that the required functional safety is achieved during the production process.
- Planning.
  - ✓ Includes planning for safety-related special characteristics.

e.g., temp. range for specific processes, material characteristics, configuration …

- ✓ Considers requirements for production, conditions for storage, transport, and handling of hardware elements, approved configurations, …
- ✓ Describes, as applicable production process flow and instructions, production tools and means, …

➢ Requirements for production

- ✓ Implementation of the planned production process, analysis of process failures and monitoring of corrective measures, …

Part 8 - Supporting Processes

➢ Objective

- ✓ Consolidate common requirements to maintain consistency.

➢ Supporting Processes.

- ✓ Interfaces within distributed developments.
- ✓ Specification and management of safety requirements.
- ✓ Configuration management.
- ✓ Change management.
- ✓ Verification.
- ✓ Documentation.
- ✓ Qualification of software tools.
- ✓ Qualification of software components.
- ✓ Qualification of hardware components.
- ✓ Proven in use argument.

8.5. Interfaces Within Distributed Developments

➢ Objective

- ✓ Describe procedures and allocate responsibilities within distributed developments (e.g., vehicle manufacturer and supplier) for items and elements.

➢ Supplier selection criteria

- ✓ Evaluate the supplier's capability to develop and produce items of comparable complexity and ASIL according to ISO 26262.
- ✓ Supplier's quality management system, experience, capability in developing products of comparable complexity and ASIL, …

8.6. Specification and Management of Safety Requirements

➢ Objectives

- ✓ Ensure correct specification of safety requirements with respect to attributes and characteristics.
- ✓ Support consistent management of safety requirements throughout the safety lifecycle.

➢ Clause includes requirements for

- ✓ Notations for the specification of safety requirements.
- ✓ Attributes and characteristics of safety requirements.
- ✓ Properties for the collection of safety requirements.
- ✓ Management of safety requirements.

8.7. Configuration Management

- ➢ Objective
  - ✓ Ensure unique identification and reproducibility of work products at any time.
  - ✓ Ensure traceability of relationships and differences between earlier and current versions.
- ➢ Clause includes requirements for
  - ✓ Compliance with the requirements of ISO TS 16949, 4.2.3 and ISO 12207, 6.2.
  - ✓ Work products listed in ISO 26262 are subject to configuration management.
  - ✓ Tools subject to configuration management.

8.8. Change Management

- ➢ Objective
  - ✓ The analysis and management of changes to safety-related work products occurring throughout the safety lifecycle.
- ➢ Involves
  - ✓ Systematically planning, controlling, monitoring, implementing, and documenting changes, while maintaining consistency of all work products.
- ➢ Clause includes requirements for
  - ✓ Planning and initiating change management.
  - ✓ Change requests.
  - ✓ Impact analysis of the change requests.
  - ✓ Deciding on a change request.
  - ✓ Carrying out and documenting the change.

8.9. Verification

- ➢ Objective
  - ✓ Ensure that all work products.
    - are correct, complete, and consistent.
    - meet the requirements of ISO 26262.
- ➢ Clause includes requirements for
  - ✓ Planning of verification.
  - ✓ Specification of verification.
    - Selection and specification of verification methods, specification of test cases, …

- ✓ Execution of verification.
  - Verification shall be executed as planned and specified
- ✓ Evaluation of verification.
  - Requirements on the evaluation of the verification results.

8.10. Documentation

- ➢ Objectives
  - ✓ Develop a documentation management strategy so that every phase of the entire safety lifecycle can be executed effectively and can be reproduced.
- ➢ Clause includes requirements for
  - ✓ Availability of documentation.
  - ✓ Content of documentation.

8.11. Qualification of Software Tools

- ➢ Objective
  - ✓ Provide evidence of SW tool suitability for use in developing a safety-related item or element.
    - Confidence in correct execution of activities and tasks required by ISO 26262.
- ➢ Clause includes
  - ✓ Planning of qualification of a software tool
  - ✓ Classification of a software tool
    - Tool impact (Possible violation of safety requirement if tool is malfunctioning or producing erroneous output (TI0 – no possibility, TI1 – possibility).
    - Tool detection (Possibility of preventing or detecting that the software tool is malfunctioning or producing erroneous output (TD1 – TD4).
    - Tool confidence level (Based on tool impact and tool detection determinations (TCL1 – TCL4).
- ➢ Methods for qualifying software tools
  - ✓ For TCL2, TCL3, and TCL4.
  - ✓ Increased confidence from use.
  - ✓ Evaluation of the development process.
  - ✓ Validation of the software tool.
  - ✓ Development in compliance with a safety standard.
- ➢ Description of each method for qualification.
- ➢ Verification requirements of the qualification of software tools.
- ➢ Work Products – software tool classification analysis, software tool qualification plan, software tool documentation, software tool qualification report.

8.12. Qualification of Software Components

- Objectives
  - ✓ To enable the re-use of existing software components as part of items, systems, or elements developed in compliance with ISO 26262 without completely re-engineering the software components.
  - ✓ To show their suitability for re-use.
- Required information to treat a software component as qualified
  - ✓ Specification of the software component.
  - ✓ Evidence that the software component complies with its requirements.
  - ✓ Evidence that the software component is suitable for its intended use.
- Requirements on the verification of the qualification of a software component.

8.13. Qualification of Hardware Components

- Objectives
  - ✓ To show the suitability of intermediate level hardware components and parts for their use as part of items, systems, or elements, developed in compliance with ISO 26262.
    - Concerning their functional behaviour and their operational limitations.
  - ✓ Provide relevant information regarding
    - Failure modes and their distribution.
    - Diagnostic capability with regard to the safety concept for the item.

8.14. Proven in use

- Objective
  - ✓ Provide guidance for proven in use argument
    - Alternate means of compliance with ISO 26262 requirements.
    - May be used in case of reuse of existing items or elements when field data is available.
- Proven in use credit does not eliminate need for integration safety lifecycle activities.
- Considers:
  - ✓ Service period for the item/element.
  - ✓ Changes to the candidate for a future application.
- Requirements on analysis of field data
  - ✓ Configuration management and change control applied to candidate.
  - ✓ Target values for proven in use.
  - ✓ Field problems need to be recorded and retrievable.

Part 9 - Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis

Automotive Safety Integrity Level refers to an abstract classification of inherent safety risk in an automotive system or elements of such a system. ASIL classifications are used within ISO 26262 to express the level of risk reduction required to prevent a specific hazard, with ASIL D representing the highest and ASIL A the lowest. The ASIL assessed for

a given hazard is then assigned to the safety goal set to address that hazard and is then inherited by the safety requirements derived from that goal.

ASIL Assessment Overview

The determination of ASIL is the result of *hazard analysis and risk assessment*. In the context of ISO 26262, a hazard is assessed based on the relative impact of hazardous effects related to a system, as adjusted for relative likelihoods of the hazard manifesting those effects. That is, each hazardous event is assessed in terms of severity of possible injuries within the context of the relative amount of time a vehicle is exposed to the possibility of the hazard happening as well as the relative likelihood that a typical driver can act to prevent the injury.

ASIL Assessment Process

At the beginning of the safety life cycle, hazard analysis and risk assessment is performed, resulting in assessment of ASIL to all identified hazardous events and safety goals.

A. Requirements decomposition with respect to ASIL tailoring

- Objectives
  - ✓ Decomposing safety requirements into redundant safety requirements (not necessarily identical) to allow ASIL tailoring at the next level of detail.
    - In this decomposition, the relevant safety goal is only violated if both elements fail simultaneous.
- Some Requirements
  - ✓ ASIL decomposition is performed considering each allocated safety requirement of the element.
  - ✓ Initial safety requirements are implemented by sufficiently independent elements and redundant safety requirements are derived for each of these elements.

B. Criteria for coexistence of elements

- Objectives Provide criteria for coexistence within the same element of
  - ✓ safety-related sub-elements with non-safety-related ones.
  - ✓ safety-related sub-elements assigned different ASILs.
- Requirements
  - ✓ A non-safety-related sub-element coexisting in the same element with safety-related sub-element(s) shall only be treated as a QM sub-element, if it has no functional dependency with any of the safety requirements allocated to the element and it does not interfere with any other safety-related sub-elements of the element.
  - ✓ In the case of coexistence in the same element of safety-related sub-elements with different ASILs, a sub-element shall only be treated as a lower ASIL sub-element if it is shown that it does not interfere with any other sub-element assigned a higher ASIL, for each of the safety requirements allocated to the element.

C. Analysis of Dependent Failures

- Objective
  - ✓ Identify any single event or single cause that could bypass or invalidate the independence or freedom from interference between elements of an item required to comply with its safety goals.
- Requirements
  - ✓ Identification of potential for dependent failures from safety analyses
  - ✓ Evaluation for dependent failures in order to determine if a reasonably foreseeable cause exists which will cause the dependent failures to occur and violate a safety goal.
  - ✓ Resolution of dependent failures in change requests to mitigate the root cause in the sub-phases of the safety lifecycle for which analysis of dependent failure is applied.

D. Safety Analyses

- Objectives
  - ✓ To examine the influence of faults and failures on items or elements regarding their architecture, functions and behaviour.
  - ✓ Provide information on conditions and causes that could lead to violation of a safety goal or safety requirement.
  - ✓ Contribute to the identification of new functional or non-functional hazards not previously considered during hazard analysis and risk assessment.
- Requirements
  - ✓ Carried out according to the ASIL assigned to the item or element.
  - ✓ Performed according to national, international or other appropriate standards or guidelines.
  - ✓ Provide measures and apply them to faults or failures that could potentially violate the safety goals or safety requirements.
  - ✓ Implement the above measures as part of the product development.
  - ✓ The results of the safety analyses are used to determine the need for additional safety-related test cases.
  - ✓ The results of the safety analyses are documented and reviewed.

Each *hazardous event* is classified according to the *severity* (S) of *injuries* it can be expected to cause:

Severity Classifications (S):

S0 No Injuries

S1 Light to moderate injuries

S2 Severe to life-threatening (survival probable) injuries

S3 Life-threatening (survival uncertain) to fatal injuries

Risk Management recognizes that consideration of the severity of a possible injury is modified by how likely the injury is to happen; that is, for a given hazard, a hazardous event is considered a lower risk if it is less likely to happen. Within the *hazard analysis and risk assessment* process of this standard, the likelihood of an injurious hazard is further classified according to a combination of *exposure* (E) (the relative expected frequency of the operational conditions in which the injury can possibly happen) and *control* (C) (the relative likelihood that the driver can act to prevent the injury).

Exposure Classifications (E):

E0 Incredibly unlikely

E1 Very low probability (injury could happen only in rare operating conditions)

E2 Low probability

E3 Medium probability

E4 High probability (injury could happen under most operating conditions)

Controllability Classifications (C):

C0 Controllable in general

C1 Simply controllable

C2 Normally controllable (most drivers could act to prevent injury)

C3 Difficult to control or uncontrollable

In terms of these classifications, an "Automotive Safety Integrity Level D" hazardous event (abbreviated "ASIL D") is defined as an event having reasonable possibility of causing a life-threatening (survival uncertain) or fatal injury, with the injury being physically possible in most operating conditions, and with little chance the driver can do something to prevent the injury. That is, *ASIL D* is the combination of S3, E4, and C3 classifications. For each single reduction in any one classification from its maximum value (excluding reduction of C1 to C0), there is a single level reduction in the ASIL from *D*. [For example, a hypothetical uncontrollable (C3) fatal injury (S3) hazard could be classified as ASIL A if the hazard has a very low probability (E1).] The ASIL level below *A* is the lowest level, *QM*. *QM* refers to the standard's consideration that below ASIL A, there is no safety relevance and only standard Quality Management processes are required.

These Severity, Exposure, and Control definitions are informative, not prescriptive, and effectively leave some room for subjective variation or discretion between various automakers and component suppliers. In response, the Society for Automotive Safety Engineers (SAE) is drafting J2980 – *Considerations for ISO26262 ASIL Hazard Classification* to provide more explicit guidance for assessing Exposure, Severity and Controllability for a given hazard.

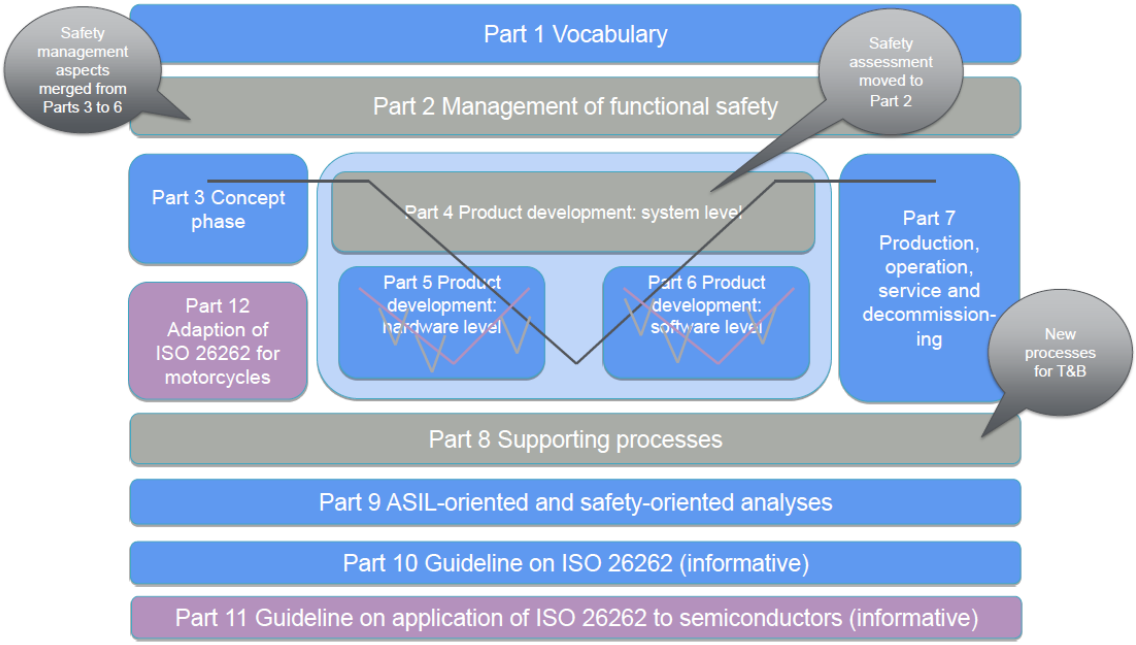
Future Development

First edition of ISO26262 was publish in 2011. In 2018 the 2nd Edition was published. Some updates were necessary considering the following [15]:

Specific requirements to adapt ISO 26262 to

- ✓ Extend scope to other types of vehicles (motorcycles, trucks, buses);
  - ❑ Motorcycles ISO/PAS 19695 and new Part 12 in Edition 2.

- ✓ Give additional guidance on semiconductor devices;
  - ❑ ISO/PAS 19451 and new Part 11 in Edition 2.
- ✓ Address ADAS-related hazards caused by "normal operation" of the sensors;
  - ❑ Currently will be developed as a separate PAS (ISO/PAS 21448).
- ✓ Other challenges include
  - ✓ Addressing highly distributed architectures.
  - ✓ Moves towards highly automated vehicles.
  - ✓ Cybersecurity.



A. **Trucks and buses**

Unlike motorcycles, truck and bus requirements are integrated into the main. Parts of the standard e.g.

- ➢ Some specific requirements for hazard analysis and risk assessment
  - ✓ Management of variants in performing the analysis;
  - ✓ Integration of truck and bus examples in the tables of Annex B;
- ➢ New supporting processes for
  - ✓ Development of a base vehicle for an application out of scope of ISO 26262;
  - ✓ Integration of safety elements developed out of scope of ISO 26262.

B. **Motorcycles**

Requirements of Parts 2 through 9 apply to motorcycles, however some tailoring is required [16]. Requirements in Part 12 supersedes the corresponding requirements in the other parts.

The major adaptation of requirements in the case of motorcycles applies to the development of the hazard analysis and risk assessment and the determination of the S, E, and C parameters.

- ✓ Introduction of Motorcycle Safety Integrity Level.
- ✓ MSIL is mapped to the ASIL.
- ✓ Safety goals are assigned to the mapped ASIL.

MSIL	ASIL
QM	QM
A	QM
B	A
C	B
D	C

C. **Guidelines for Semiconductor**

- ➢ A necessary extension of ISO 26262 to provide guidelines for semiconductors used in automotive application.
  - ✓ Informative Part.
- ➢ Semiconductor components can be developed as
  - ✓ Part of the item –safety analysis performed per Part 5 requirements.
  - ✓ Safety Element out of Context (SEooC) –development is based on assumptions to be verified at integration.
- ➢ Guidelines on semiconductor components.
- ➢ Guidelines on semiconductor technologies.