COURSE 2

ISO26262

ISO 26262, titled "Road vehicles – Functional safety", is an international standard for functional safety of electrical and/or electronic systems in production automobiles defined by the International Organization for Standardization (ISO) in 2011 [3].

Overview

Functional safety features form an integral part of each automotive product development phase, ranging from the specification, to design, implementation, integration, verification, validation, and production release. The standard ISO 26262 is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/Electronic Systems. ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic and electrical safety-related systems.

The first edition, published on 11 November 2011, is intended to be applied to electrical and/or electronic systems installed in "series production passenger cars" with a maximum gross weight of 3500 kg. It aims to address possible hazards caused by the malfunctioning behaviour of electronic and electrical systems.

Although entitled "Road vehicles – Functional safety" the standard relates to the functional safety of Electrical and Electronic systems as well as that of systems as a whole or of their mechanical subsystems [3].

Like its parent standard, IEC 61508, ISO 26262 is a risk-based safety standard, where the risk of hazardous operational situations is qualitatively assessed and safety measures are defined to avoid or control systematic failures and to detect or control random hardware failures, or mitigate their effects.

Goals of ISO 26262:

- Provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases.
- Covers functional safety aspects of the entire development process (including such activities as requirements specification, design, implementation, integration, verification, validation, and configuration).
- 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.
- Provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved [3].

Background

Increasing complexity throughout the automotive industry is resulting in increased efforts to provide safety-compliant systems [4]. For example, modern automobiles use by-wire systems such as throttle-by-wire. This is when the driver pushes on the accelerator and a sensor in the pedal sends a signal to an electronic control unit.

This control unit analyses several factors such as engine speed, vehicle speed, and pedal position. It then relays a command to the throttle body. It is a challenge of the automotive industry to test and validate systems like throttle-by-wire. The goal of ISO 26262 is to provide a unifying safety standard for all automotive E/E systems.

The Draft International Standard (DIS) of ISO 26262 was published in June 2009. Since the publication of the draft, ISO 26262 has gained traction in the automotive industry. Because a public draft standard is available, lawyers treat ISO 26262 as the technical state of the art. The technical state of the art is the highest level of development of a device or process at a particular time. According to German law, car producers are generally liable for damage to a person caused by the malfunction of a product. If the malfunction could not have been detected by the technical state of the art, the liability is excluded [German law on product liability] [4].

Implementing ISO 26262 allows leveraging a common standard to measure how safe a system will be in service. It also provides the ability to reference specific parts of your system because of a common vocabulary provided by the standard. This falls in line with other safety-critical application areas; a common standard provides a way to measure how safe your system is.

The difference between IEC61508 and ISO 26262

➢ IEC 61508	➢ ISO 26262
1. Framework standard	1. IEC 61508 Automotive Sector adaptation
2. Implied context of Process/Automation industries (where validation is done after install)	2. Applies to vehicles with ≥ 4 wheels (carrying passengers, goods)
3. Safety Integrity Levels, “SIL” ✓ SIL 1 – SIL 4; ✓ Measure of the reliability of safety functions (Includes a quantitative target for the probability of a dangerous failure); ✓ No exact mapping between SIL’s and ASIL’s.	3. Automotive SIL, “ASIL” ✓ ASIL A-D; ✓ Based on the violation of a safety goal (Provides requirements to achieve acceptable level of risk); ✓ No exact mapping between SIL’s and ASIL’s (Loose mapping).
4. Focus on safety functions	4. Focus on safety goals
	5. Adds required work products

Parts of ISO 26262

ISO 26262 covers the entire product development lifecycle of electrical / electronic automotive products. The standard is composed of 10 parts, as shown below [6]:

Part 1 defines the language of ISO 26262 – terms, abbreviations, acronyms, etc.

Part 2 is an over-arching guide focusing on the management of safety requirements, both from a project and organizational point of view.

Part 3 focuses on what ISO 26262 calls the ‘concept phase’. This phase is concerned with initial project definition, establishing the safety requirements and criteria for the project and initiating the safety cycle.

Part 4 is concerned with systems levels development – that is, detailed requirements analysis, system synthesis, functional and logical allocation, and system evaluation, validation and verification.

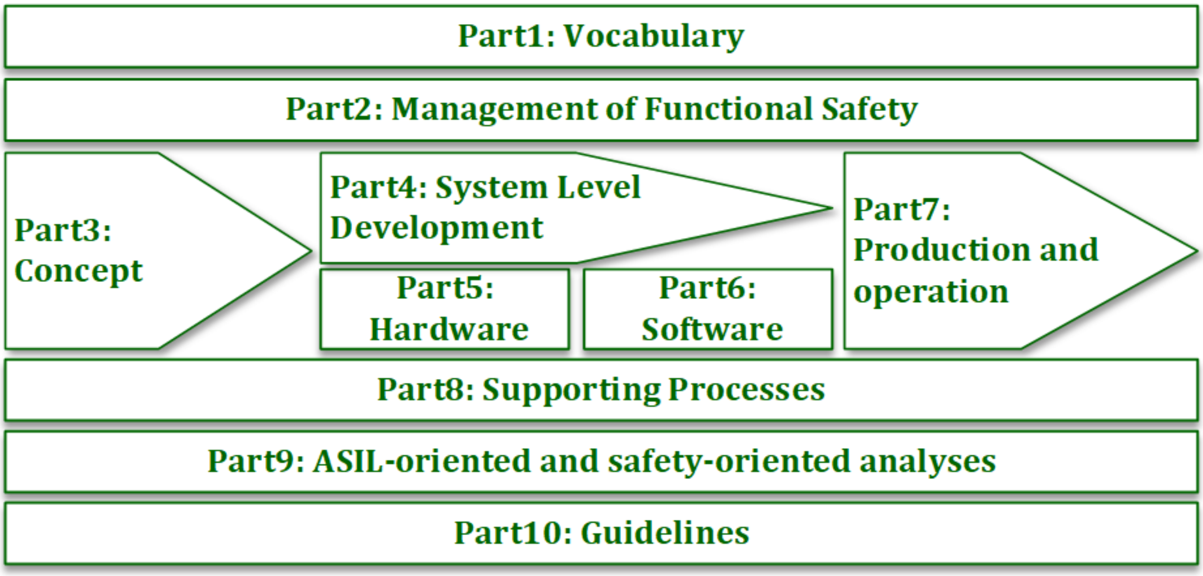

Part1: Vocabulary
Part2: Management of Functional Safety
Part3: Concept
Part4: System Level Development
Part5: Hardware
Part6: Software
Part7: Production and operation
Part8: Supporting Processes
Part9: ASIL-oriented and safety-oriented analyses
Part10: Guidelines

Fig. 3.1. The parts of ISO 26262 [6]

Part 5 covers the hardware aspects of system design and implementation.

Part 6 focuses on the software aspects of system design and implementation.

Part 7 details requirements for system production, operation, installation, servicing, decommission, etc.

Part 8 defines requirements for processes that support the development effort, including charge management, documentation standard, tool qualification, verification and validation, etc.

Part 9 gives requirements and guidance with respect to safety analyses; in particular, all aspects related to ASIL-oriented requirements.

Part 10 gives guidance on applying ISO 26262.

ISO 26262 assumes you are already working to a define development process. The standard applies additional constrains to your process, focussed on the system safety aspects.

ISO 26262 uses a classic 'V-model' framework to organise its requirements. The V-model in a standard way to describe the relationship between your development artefacts [6].

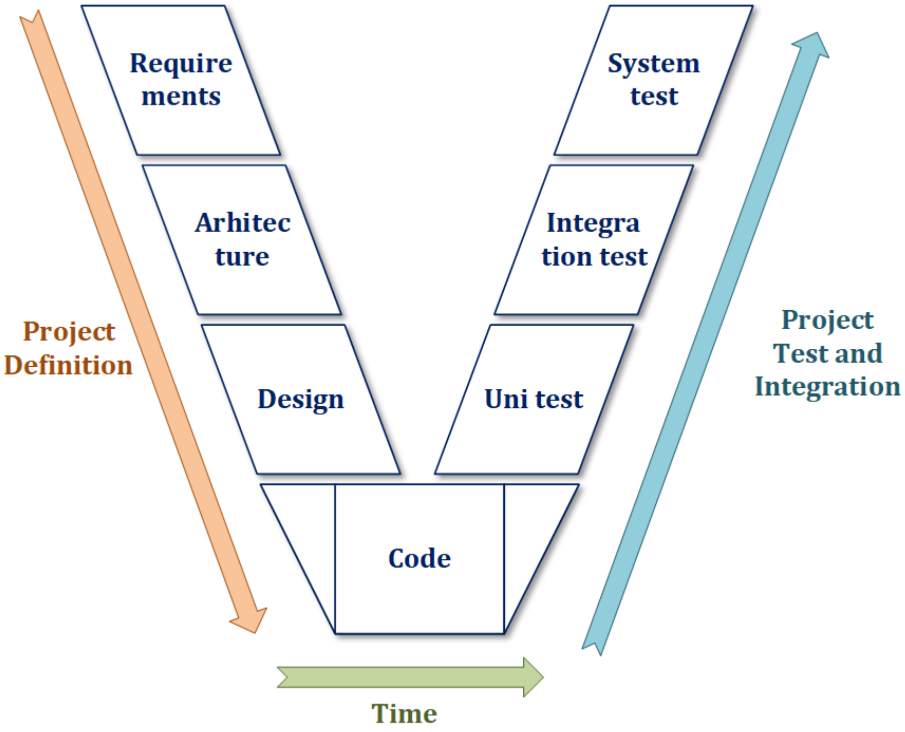
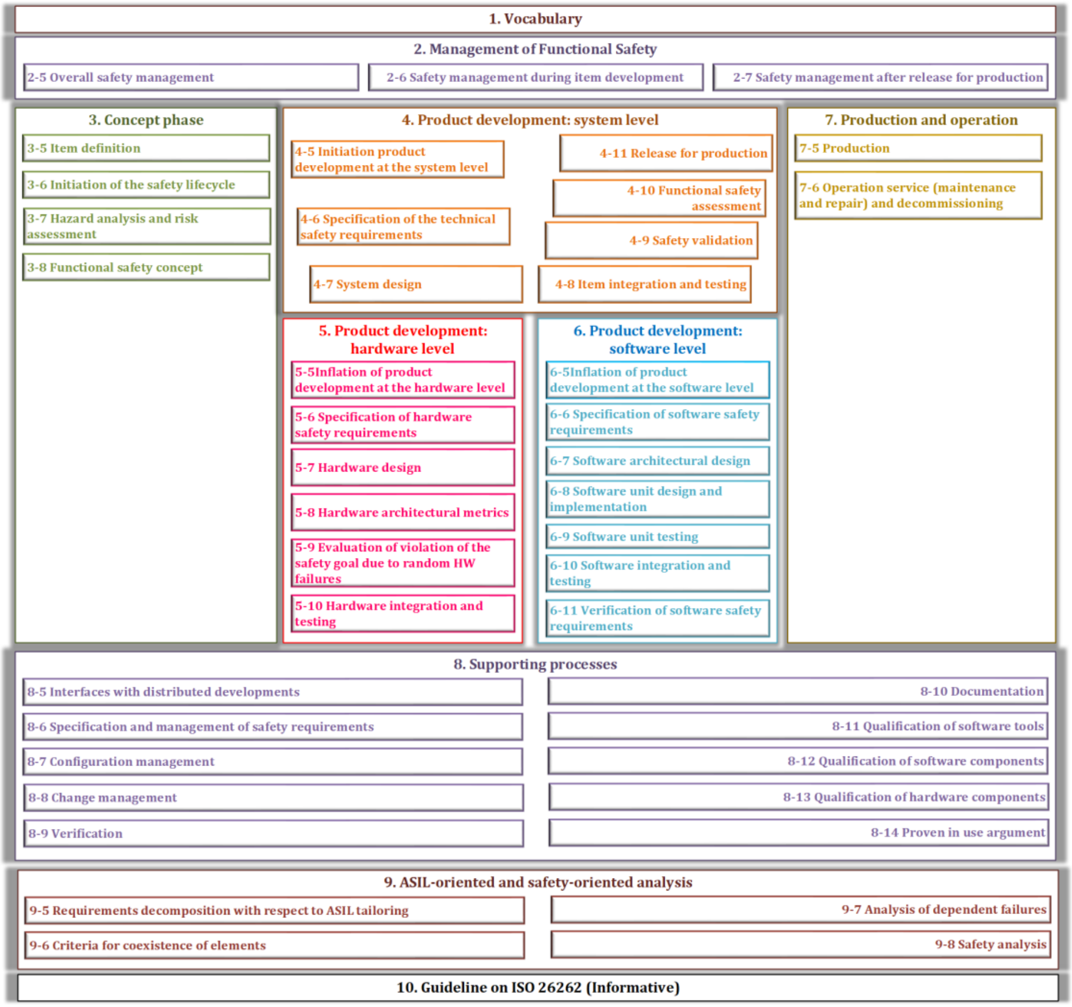


Fig. 3.2. A classic V-model [6]



1. Vocabulary

2. Management of Functional Safety
2-5 Overall safety management
2-6 Safety management during item development
2-7 Safety management after release for production

3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept

4. Product development: system level
4-5 Initiation product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-8 Item integration and testing
4-9 Safety validation
4-10 Functional safety assessment
4-11 Release for production

5. Product development: hardware level
5-5Inflation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Hardware architectural metrics
5-9 Evaluation of violation of the safety goal due to random HW failures
5-10 Hardware integration and testing

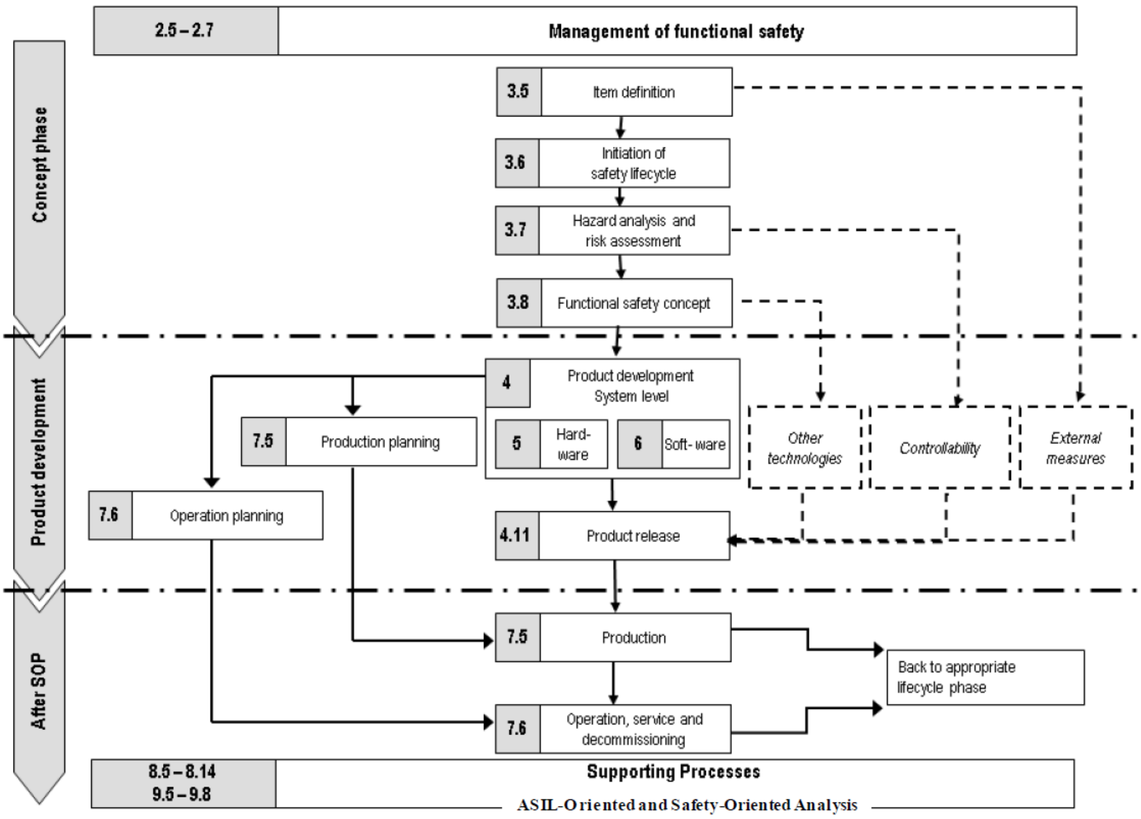
6. Product development: software level
6-5Inflation of product development at the software level
6-6 Specification of software safety requirements
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements

7. Production and operation
7-5 Production
7-6 Operation service (maintenance and repair) and decommissioning

8. Supporting processes
8-5 Interfaces with distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Qualification of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument

9. ASIL-oriented and safety-oriented analysis
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analysis

10. Guideline on ISO 26262 (Informative)


2.5 – 2.7
Management of functional safety
Concept phase
3.5
Item definition
3.6
Initiation of safety lifecycle
3.7
Hazard analysis and risk assessment
3.8
Functional safety concept
Product development
4
Product development System level
5
Hard-ware
6
Soft- ware
7.5
Production planning
7.6
Operation planning
Other technologies
Controllability
External measures
4.11
Product release
After SOP
7.5
Production
7.6
Operation, service and decommissioning
Back to appropriate lifecycle phase
8.5 – 8.14
9.5 – 9.8
Supporting Processes
ASIL-Oriented and Safety-Oriented Analysis

Part 1: Vocabulary

ISO 26262 specifies a vocabulary (a Project Glossary) of terms, definitions, and abbreviations for application in all parts of the standard [7]. Of particular importance is the careful definition of *fault*, *error*, and *failure* as these terms are key to the standard's definitions of functional safety processes, particularly in the consideration that "A *fault* can manifest itself as an *error* ... and the *error* can ultimately cause a *failure*" [7].

Item

Within this standard, *item* is a key term. *Item* is used to refer to a specific system or array of systems that implements a function at the vehicle level to which the ISO 26262 Safety Life Cycle is applied. That is, the *item* is the highest identified object in the process and is thereby the starting point for product-specific safety development under this standard.

Element

System or part of a system, including components, hardware, software, hardware parts, and software units - effectively, anything in a system that can be distinctly identified and manipulated.

Fault

Abnormal condition that can cause an *element* or an *item* to fail.

Error

Discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretically correct value or condition.

Failure

Termination of the ability of an *element* to perform a function as required.

Note: Since an element's specification defines its required function, the standard recognizes incorrect specification as a potential source of failure.

Malfunctioning Behaviour

Failure or unintended behaviour of an *item* with respect to its design intent.

Hazard

Potential source of harm caused by malfunctioning behaviour of the *item*.

Functional Safety

Absence of unreasonable risk due to *hazards* caused by malfunctioning behaviour of Electrical/Electronic systems.

Note: In contrast to the formal vocabularies defined for other Functional Safety standards, Fault Tolerance is not explicitly defined within this standard -- it is assumed impossible to comprehend all possible faults in a system. Functional Safety *rather than Fault Tolerance is the objective of the standard. ISO 26262 does not use the (IEC 61508) terms SFF and hardware fault tolerance. The terms* single point faults metric *and* latent faults metric *are used instead* [8].

Failure types

- *Random Hardware Failures*
  - ✓ failure that may occur unpredictably during the lifetime of a hardware element and that follows a probability distribution.
- *Systematic Failures*
  - ✓ failure of an element or item that is caused in a deterministic way during development, manufacturing, or maintenance;
  - ✓ all software faults and a subset of hardware faults are systematic.

Safety Mechanism

- Activity or technical solution to detect / avoid / control failures or mitigate their harmful effects.
- Implemented by an E/E function or element or in other technologies.
- The safety mechanism is either
  - ✓ able to switch to or maintain the item in a safe state or
  - ✓ able to alert the driver such that the driver is expected to control the effect of the failure.

Work product

- Information or data.
- The result of one or more system safety process activities.
- Format appropriate to the work product’s content.
  - ✓ Data files, models, source code, etc.
  - ✓ May include currently existing documents.
  - ✓ Several work products may be in one document.

Confirmation measures

- Ensure the sufficient completion of work products and proper execution of the safety lifecycle.
- Provide for the evaluation of the system safety activities and work products.
- Used to determine the adequacy of achievement of the functional safety goals.

Safety case

- Communicates a clear, comprehensive and defensible argument (supported by evidence) that a system is acceptably safe to operate in a particular context.
- Includes references to safety requirements and supporting evidence.
- AND a "safety argument" that describes how the safety requirements have been interpreted, allocated, decomposed, etc., and fulfilled as shown by the supporting evidence.