# Part 2: Management of functional safety

ISO 26262 is intended to be applied to **safety-related systems** that include one or more (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg.

ISO 26262 addresses possible **hazards** caused by malfunctioning behavior of E/E safety-related systems, including interaction of these systems.

It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behavior of E/E safety-related systems.

Mal Function

This part of ISO 26262 specifies the requirements for functional safety management for automotive applications, including the following:

* Requisitos relacionados às organizações project-independent requirements with regard to the organizations involved (overall safety management see 5 below), and
* Requisitos relacionados com as actividades de gestão no Ciclo de Vida da Segurança project-specific requirements with regard to the management activities in the safety lifecycle (i.e. management during the **concept phase** and **product development**, and after the **release for production**).

# 4 Requirements for compliance

## 4.1 General requirements

When claiming compliance with ISO 26262, each requirement **shall** be complied with, unless one of the following applies:

1. tailoring of the safety activities in accordance with this part of ISO 26262 has been planned and shows that the requirement does not apply, or
2. A rationale is available that the non-compliance is acceptable and the rationale has been assessed in accordance with this part of ISO 26262.

Information marked as a “**NOTE**” or “**EXAMPLE**” is only for guidance in understanding, or for clarification of the associated requirement, and **shall** not be interpreted as a requirement itself or as complete or exhaustive.

* The results (product) of safety activities are given as work products.

(**1.142 work product** result of one or more associated requirements of ISO 26262. **(An implementation of an ISO26262 requirement)** NOTE a reference (document) can be an independent document containing the complete information of a work product or a list of references to the complete information of a work product.)

* “Prerequisites” are information which **shall** be available as work products of a previous phase.

Given that certain requirements of a clause are ASIL-dependent or may be tailored, certain work products may not be needed as prerequisites. ???

* “Further supporting information” is information that can be considered, but which in some cases is not required by ISO 26262 as a work product of a previous phase and which may be made available by external sources that are different from the persons or organizations responsible for the functional safety activities.

## 4.2 Interpretations of tables

Tables are **normative** or **informative** depending on their context.

The different methods listed in a table contribute to the level of confidence in achieving compliance with the corresponding requirement. Each method in a table is either

1. a consecutive entry (marked by a sequence number in the leftmost column, e.g. 1, 2, 3), or
2. An alternative entry (marked by a number followed by a letter in the leftmost column, e.g. 2a, 2b, 2c).

For consecutive (1, 2, 3) entries, all methods **shall** be applied as recommended in accordance with the ASIL.

If methods other than those listed are to be applied, a rationale **shall** be given that these fulfil the corresponding requirement.

For alternative entries (1a, 1b, 1c) , an appropriate combination of methods **shall** be applied in accordance with the ASIL indicated, independent of whether they are listed in the table or not.

If methods are listed with different degrees of recommendation for an ASIL, the methods with the higher recommendation **should** be preferred.

A rationale **shall** be given that the selected combination of methods complies with the corresponding requirement.

NOTE a rationale based on the methods listed in the table is sufficient. However, this does not imply a bias for or against methods not listed in the table.

For each method, the degree of recommendation to use the corresponding method depends on the ASIL and is categorized as follows:

“++” indicates that the method is highly recommended for the identified ASIL;

“+” indicates that the method is recommended for the identified ASIL;

“o” indicates that the method has no recommendation for or against its usage for the identified ASIL.

## 4.3 ASIL-dependent requirements and recommendations

The requirements or recommendations of each subclause **shall** be complied with for ASIL A, B, C and D, if not stated otherwise.

These requirements and recommendations refer to the ASIL of the safety goal. (?)

If ASIL decomposition has been performed at an earlier stage of development, in accordance with ISO 26262-9:2011, Clause 5, the ASIL resulting from the decomposition **shall** be complied with.

If an ASIL is given in parentheses in ISO 26262, the corresponding subclause **shall** be considered as a recommendation rather than a requirement for this ASIL. This has no link with the parenthesis notation related to ASIL decomposition.

# 5 Overall safety management

## 5.1 Objective

The objective of this clause (5) is to define the requirements for the **organizations** that are responsible for the safety lifecycle, or that perform safety activities in the safety lifecycle.

This clause (5) serves as a *prerequisite* (see above) to the activities in the ISO 26262 safety lifecycle.

## 5.2 General

## 5.2.1 Overview of the safety lifecycle

The ISO 26262 safety lifecycle (see Figure 2 in pdf) encompasses the principal safety activities during the

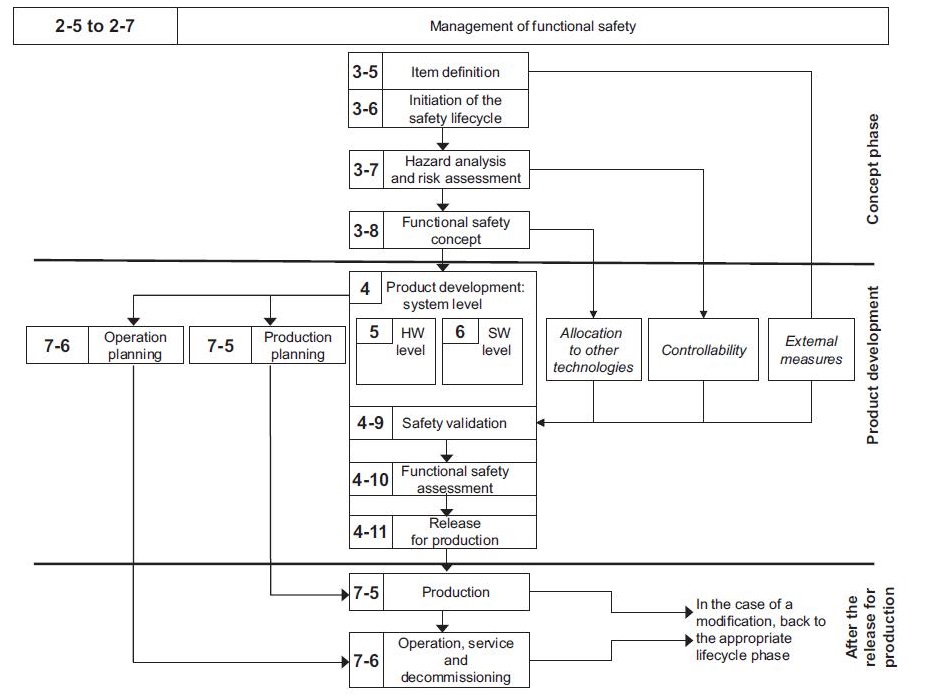
* concept phase
* product development
* production
* operation
* service
* decommissioning.

**🡪Planning, coordinating and documenting and tracking the safety activities of all phases of the safety lifecycle are key management tasks. 🡨**

Figure 2 represents the **reference safety lifecycle model**. Tailoring of the safety lifecycle, including iterations of subphases, is allowed.

NOTE 1 The activities during the concept phase and the product development, and after the release for production are described in detail in ISO 26262-3 (concept phase), ISO 26262-4 (product development at the system level), ISO 26262-5 (product development at the hardware level), ISO 26262-6 (product development at the software level) and ISO 26262-7 (production and operation).

NOTE 2 Table A.1 provides an overview of the objectives, prerequisites and work products of the particular phases of the management of functional safety.



NOTE Within the figure, the specific clauses of each part of ISO 26262 are indicated in the following manner: “m-n”, where “m” represents the number of the part and “n” indicates the number of the clause, e.g. “3-6” represents Clause 6 of ISO 26262-3.

**Figure 2 — Safety lifecycle**

## 5.2.2 26BExplanatory remarks on the safety lifecycle

ISO 26262 specifies requirements with regard to specific phases and subphases of the **safety lifecycle**, but also includes requirements that apply to several, or all, phases of the safety lifecycle, such as the requirements for the management of functional safety.

The key management tasks are to

* Plan,
* Coordinate
* Documenting and
* Track the activities related to functional safety.

These management tasks apply to all phases of the safety lifecycle.

The requirements for the management of functional safety are given in this part, which distinguishes:

* Overall safety management (project-independent requirements with regard to the organizations involved - see this clause 5);
* Safety management during the **concept phase** and the **product development** (see Clause 6);
* Safety management after the item's release for production (see Clause 7).

The following descriptions explain the definitions of the different phases and subphases of the safety lifecycle, as well as other key concepts:

|  |  |
| --- | --- |
| 2-5 to 2.7 Management of functional safety |  |
| a) 3-5 The subphase: item definition |  |
| What are the functionalities of the item? |  |
| What are the interfaces of the item? |  |
| What are the environmental conditions? |  |
| What are the legal requirements? |  |
| What are the known hazards of the item? |  |
| What are the boundaries of the item? |  |
| Assumptions concerning other items? |  |
| Assumptions concerning other elements? |  |
| Assumptions concerning other systems? |  |
| Assumptions concerning other components? |  |

|  |  |
| --- | --- |
| b) 3-6 The subphase: initiation of the safety lifecycle |  |
| new development | modification of an existing item |
|  | the results of an impact analysis are used to tailor the safety lifecycle (see ISO 26262-3:2011, Clause 6) |

|  |  |
| --- | --- |
| c) 3-7 The subphase: HA&RA | Very Complex Phase. Must be deepened |
| estimates the probability of exposure of the item (E) |  |
| estimates the controllability of the item (C) |  |
| estimates the severity of the hazardous of the item (S) |  |
| ASIL of the hazardous events | X |
| Result: safety goals for the item | SafetyGoals.pdf |
| Safety Goal 1 with ASIL X | Written requirement |
| Safety Goal 2 with ASIL X | Written requirement |

Subsequently, the HA&RA determines the safety goals for the item, with the safety goals being the top level safety requirements for the item.

The ASILs determined for the hazardous events (HE) are assigned to the corresponding safety goals.

During the subsequent phases and sub phases, detailed safety requirements are derived from the safety goals.

These safety requirements inherit the ASIL of the corresponding safety goals.

|  |  |
| --- | --- |
| d) The sub phase: functional safety concept |  |
| Get Safety Goals defined in c) and Specify (by functional safety requirements) a Functional Safety Concept | Result: Functional Safety Concept |

Based on the safety goals, a **functional safety concept** (**see ISO 26262-3:2011, Clause 8**) is specified considering preliminary architectural assumptions.

The **functional safety concept** is specified by **functional safety requirements** that are allocated to the elements of the item.

The **functional safety concept** can also include other technologies or interfaces with external measures, provided that the expected behaviours thereof can be validated (see ISO 26262-4:2011, Clause 9).

The implementation of other technologies is outside the scope of ISO 26262 and the implementation of the external measures is outside the scope of the item development.

|  |  |
| --- | --- |
| e) The phase: product development at the system level (4) | BlackBox for the Product Point of View |
| The Item is developed from the system level perspective | Result: The release for production of an item |
|  |  |

After having specified the functional safety concept (in d), the item is developed from the system level perspective, as given in **ISO 26262-4**.

The system development process is based on the concept of a V-model with the specification of

* The technical safety requirements (4-6)
* the system architecture (4-7)
* the system design and implementation on the left hand branch and the integration, verification, validation (4-7)
* The functional safety assessment on the right hand branch (4-10)
* The hardware-software interface is specified in this phase (5 to 6)

Figure 1 provides an overview of the subphases of the product development at the system level.

***The product development at the system level*** incorporates validation tasks for activities occurring within other safety lifecycle phases, including

* the validation of the aspects of the functional safety concept that are implemented by other technologies;
* the validation of the assumptions concerning the effectiveness and the performance of external measures; and
* the validation of the assumptions concerning human response, including controllability and operational tasks.

The release for production is the final subphase of the product development and provides the item’s release for series production (see ISO 26262-4:2011, Clause 11).

|  |  |
| --- | --- |
| f) The phase: product development at the hardware level (5) | Come from 4-5, 4-6, 4-7 |

Based on the system design specification (4-7), the item is developed from the hardware level perspective (see ISO 26262-5).

The hardware development process is based on the concept of a V-model with the specification of the hardware requirements (5-6) and the hardware design (5-7) and implementation on the left hand branch and the hardware integration and testing (5-10) on the right hand branch.

|  |  |
| --- | --- |
| g) The phase: product development at the software level (6) |  |

Based on the system design specification (4-7), the item is developed from the software level perspective (see ISO 26262-6).

The software development process is based on the concept of a V-model with the specification of the software requirements and the software architectural design and implementation on the left hand branch, and the software integration and testing (6-10), and the verification of the software requirements (6-11) on the right hand branch.

|  |  |
| --- | --- |
| h) Production planning and operation planning (7) | Shall pass through 4-8, 4-9, 4-10, 4-11 and is related to Product Development and not related to Production |

The planning for production (7-5) and planning for operation (7-6), and the specification of the associated requirements, starts during the product development at the system level (see **ISO 26262-4**).

The requirements for production and operation are given in **ISO 26262-7:2011**, Clauses 5 and 6.

|  |  |
| --- | --- |
| i) The phase: production and operation, service and decommissioning (7-5 and 7-6) |  |

This phase addresses the production processes relevant for the functional safety goals of the item, i.e. the safety-related special characteristics, and the development and management of instructions for the maintenance, repair and decommissioning of the item to ensure functional safety after the item's release for production (see ISO 26262-7:2011, Clauses 5 and 6).

|  |
| --- |
| j) Controllability (Product Development Phase) |

In the HA&RA (see ISO 26262-3:2011, Clause 7), credit can be taken for the ability of the driver, or the other persons at risk, to control hazardous situations.

The assumptions regarding the controllability in the HA&RA and the functional and technical safety concept are validated during the safety validation (see Figure 2 and ISO 26262-4:2011, Clause 9).

NOTE the exposure and the severity are factors that depend on the scenario. The eventual controllability through human intervention is influenced by the design of the item and is therefore evaluated during the validation (see ISO 26262-4:2011, 9.4.3.2).

|  |
| --- |
| k) External measures |

The external measures refer to the measures outside the item, as specified in the item definition (see Figure 2 and ISO 26262-3:2011, Clause 5), that reduce or mitigate the risks resulting from the item. External measures can include not only additional in-vehicle devices such as dynamic stability controllers or run-flat tyres, but also devices external to the vehicle, like crash barriers or tunnel fire-fighting systems.

The assumptions regarding the external measures in the item definition, the HA&RA and the functional and technical safety concept are validated during the safety validation (see Figure 2 and ISO 26262-4:2011, Clause 9).

External measures can be considered in the HA&RA. However, if credit is taken from an external measure in the HA&RA, that external measure cannot be considered as a risk reduction in the functional safety concept.

ISO 26262 also applies to those external measures that are in the scope of ISO 26262.

|  |
| --- |
| l) Other technologies |

Other technologies, e.g. mechanical and hydraulic technologies, are those different from electrical and/or electronic technologies that are in the scope of ISO 26262. These can be considered in the specification of the functional safety concept (see Figure 2 and ISO 26262-3:2011, Clause 8), during the allocation of safety requirements (see ISO 26262-3 and ISO 26262-4), or as an external measure.

NOTE If an implementation in another technology is specified as an external measure, then it can be useful to repeat the HA&RA to consider the associated risk reduction, which could potentially result in a reduced ASIL of a corresponding safety goal.

TESTE