ISO/DIS 26262
Global training
Agenda

Learning objectives
Introduction
I. Normative references
II. History
III. Scope of the standard
IV. Vocabulary – part 1
V. Management of Functional Safety – part 2
VI. Concept phase – part 3
VII. Product development : system level – part 4
VIII. Product development : hardware level – part 5
IX. Product development : software level – part 6
X. Product & operation – part 7
XI. Supporting processes – part 8
XII. ASIL – oriented and safety analysis – part 9
XIII. Guideline – part 10
General learning objectives

At the end of the session, attendees should be able:

- to know the origin of the ISO standard
- to understand the application field of the ISO standard
- to know the scope of this standard
- to acquire the new concepts introduced by the standard
- to have an overview of methods allowing to analyse and cope with the identified risks
Introduction of the Automotive Safety Standard

ISO 26262 was prepared by Technical Committee ISO/TC 22, Road Vehicle, Subcommittee SC3 Electrical and Electronic Equipment.

ISO 26262 consists of the following parts, under the general title « Road vehicle – functional safety ».

- Part 1 : Vocabulary
- Part 2 : Management of functional safety
- Part 3 : Concept phase
- Part 4 : Product development system level
- Part 5 : Product development hardware level
- Part 6 : Product development software level
- Part 7 : Production & Operation
- Part 8 : Supporting process
- Part 9 : ASIL oriented and safety oriented analyses
- Part 10 : Guideline
Introduction of the Automotive Safety Standard

1. Vocabulary

2. Management of functional safety

3. Concept phase

4. Product development: system level

5. Product development: hardware level

6. Product development: software level

7. Production and operation

7-5 Operation, service (maintenance and repair), and decommissioning

8. Supporting processes

8-5 Interfaces within 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 analyses

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 analyses

10. Guideline on ISO 26262 (informative)

MAJ 07/03/2010
Introduction of the Automotive Safety Standard

This Standard is the *adaptation* of *IEC 61508* to comply with needs specific to the application sector of Electric & Electronic (E/E) systems within road vehicles.

This standard:

- provides an automotive safety lifecycle and supports tailoring the necessary activities during these lifecycle phases
- provides an automotive specific risk-based approach for determining risk classes (Automotive Safety Integrity Level ASIL)
- uses ASIL for specifying the item’s necessary safety requirements for achieving an acceptable residual risk
- provides requirements for validation & confirmation measures to ensure a sufficient and acceptable level of safety being achieved
I – Normative references

- ISO 9001- 2000, *Quality management systems – Requirements*
- ISO 16949, *Quality management systems – Particular requirements for the application of ISO 9001- 2000 for automotive production and relevant service part organizations*
- ISO 3779, *Road vehicles – Vehicle Identification Number (VIN)*
- ISO 3883, *Road vehicles – Types – Terms and definitions*
II - History

First definition...

**Risk**
Combination of the probability of occurrence of harm and the severity of that harm

**Functional safety**
Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems

**Safety**
Absence of unreasonable risks
Objectives of this standard:

- **Comparability with existing IEC 61508** shall remain due to product liability aspects.

- All normative sections should have a Safety Integrity Level dependency.

- Adaptation of the safety lifecycle to typical automotive development and operation phases is needed.

- Distinction between management, development and support processes.
II - History

Objectives of this standard?

- Standard shall support implementation of development processes and safety assessments.
- Standard should refer to milestones and prototypes/samples of typical automotive development processes.
- Standard shall include requirements on manufacture/supplier relation and distributed development processes.
Objectives of this standard?

- **Hazard analysis and risk assessment** shall be adapted for typical automotive use cases.

- **Emphasis on verification / validation process**, including Application of HIL-tests, LabCars, fleet tests and user oriented tests during validation shall be considered.

- Support of probabilistic target values for random hardware failures.
II - History

**Workteam**

Convenor: Ch. Jung,
Secretary: E. Fritzsche, FAKRA

Germany: BMW, Bosch, Continental, Daimler, VW
France: PSA, Renault, Continental, Valeo
Austria: (MagnaSteyr, ARC Seibersdorf Research GmbH)
Italy: Fiat Group, Centro Ricerche Fiat, TRW
Japan: Honda, Nissan, Toyota, Denso, Hitachi
Sweden: Volvo Cars, AB Volvo, Delphi,
UK: Landrover, MIRA
USA: TRW, GM, Delphi
Belgium: Nissan Europe, Toyota Europe
Canada: Critical Systems Labs
II - History

- **IEC 61508**
  - **Initial work of individual companies**
  - **OEMs Suppliers Technical Services**
  - **FAKRA BNA MISRA**
  - **Initiatives within national standardization bodies**
  - **First drafts of requirement specifications**
    - **RESPONSE Automotive SPICE**
    - **ISO TC22 SC3 WG16**

- **History**
  - **2002**
  - **2003**
  - **2004**
  - **2005**
  - **2011**
II - History

This target date planner shows you the three main development tracks for project managing the development of an ISO standard. It will help you choose the track and then set the target dates you need to meet for your standards to be delivered to the market on time. The times shown are the maximum for each stage and can be shortened whenever possible.

**Approval**

Approval at DIS and FDIS stages requires two thirds of P members of the TC to vote yes and not more than a quarter of all votes cast to be negative.

100% approval at DIS can mean straight to publication if the committee agrees.

---

**Decision**

DIS is approved and can be communicated outside the Working Group.
III – Scope of the standard

This standard is applicable to safety related systems, that include one or more E/E systems, and that are installed in series production passenger cars with a max gross weight up to 3,5 t but not in vehicle for drivers with disabilities.

ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems including interaction of these systems. It does not address hazards as electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, and similar hazards unless directly caused by malfunctioning behaviour of E/E safety related systems.

Additional requirements for vehicles for the transport of hazardous goods are not covered by this Standard.
### IV – Vocabulary

#### 1. Vocabulary

#### 2. Management of functional safety

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2-5</td>
<td>Overall safety management</td>
<td>2-6</td>
</tr>
<tr>
<td>2-7</td>
<td>Safety management after release for production</td>
<td></td>
</tr>
</tbody>
</table>

#### 3. Concept phase

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3-5</td>
<td>Item definition</td>
</tr>
<tr>
<td>3-6</td>
<td>Initiation of the safety lifecycle</td>
</tr>
<tr>
<td>3-7</td>
<td>Hazard analysis and risk assessment</td>
</tr>
<tr>
<td>3-8</td>
<td>Functional safety concept</td>
</tr>
</tbody>
</table>

#### 4. Product development: system level

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4-5</td>
<td>Initiation of product development at the system level</td>
</tr>
<tr>
<td>4-6</td>
<td>Specification of the technical safety requirements</td>
</tr>
<tr>
<td>4-7</td>
<td>System design</td>
</tr>
<tr>
<td>4-8</td>
<td>Item integration and testing</td>
</tr>
<tr>
<td>4-10</td>
<td>Functional safety assessment</td>
</tr>
<tr>
<td>4-11</td>
<td>Release for production</td>
</tr>
<tr>
<td>4-8</td>
<td>Safety validation</td>
</tr>
</tbody>
</table>

#### 5. Product development: hardware level

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5-5</td>
<td>Initiation of product development at the hardware level</td>
</tr>
<tr>
<td>5-6</td>
<td>Specification of hardware safety requirements</td>
</tr>
<tr>
<td>5-7</td>
<td>Hardware design</td>
</tr>
<tr>
<td>5-8</td>
<td>Hardware architectural metrics</td>
</tr>
<tr>
<td>5-9</td>
<td>Evaluation of violation of the safety goal due to random HW failures</td>
</tr>
<tr>
<td>5-10</td>
<td>Hardware integration and testing</td>
</tr>
</tbody>
</table>

#### 6. Product development: software level

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6-5</td>
<td>Initiation of product development at the software level</td>
</tr>
<tr>
<td>6-6</td>
<td>Specification of software safety requirements</td>
</tr>
<tr>
<td>6-7</td>
<td>Software architectural design</td>
</tr>
<tr>
<td>6-8</td>
<td>Software unit design and implementation</td>
</tr>
<tr>
<td>6-9</td>
<td>Software unit testing</td>
</tr>
<tr>
<td>6-10</td>
<td>Software integration and testing</td>
</tr>
<tr>
<td>6-11</td>
<td>Verification of software safety requirements</td>
</tr>
</tbody>
</table>

#### 8. Supporting processes

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8-5</td>
<td>Interfaces within distributed developments</td>
</tr>
<tr>
<td>8-6</td>
<td>Specification and management of safety requirements</td>
</tr>
<tr>
<td>8-7</td>
<td>Configuration management</td>
</tr>
<tr>
<td>8-8</td>
<td>Change management</td>
</tr>
<tr>
<td>8-9</td>
<td>Verification</td>
</tr>
<tr>
<td>8-10</td>
<td>Documentation</td>
</tr>
<tr>
<td>8-11</td>
<td>Qualification of software tools</td>
</tr>
<tr>
<td>8-12</td>
<td>Qualification of software components</td>
</tr>
<tr>
<td>8-13</td>
<td>Qualification of hardware components</td>
</tr>
<tr>
<td>8-14</td>
<td>Proven in use argument</td>
</tr>
</tbody>
</table>

#### 9. ASIL-oriented and safety-oriented analyses

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9-5</td>
<td>Requirements decomposition with respect to ASIL tailoring</td>
</tr>
<tr>
<td>9-6</td>
<td>Criteria for coexistence of elements</td>
</tr>
<tr>
<td>9-7</td>
<td>Analysis of dependent failures</td>
</tr>
<tr>
<td>9-8</td>
<td>Safety analyses</td>
</tr>
</tbody>
</table>

#### 10. Guideline on ISO 26262 (Informative)

Introduction à la norme ISO 26262

MAJ 07/03/2010
Main terms ...

**Item**
System or array of systems or a function to which ISO 26262 is applied

**Safety**
Absence of unreasonable risk

**Functional safety**
Absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems

**Safety case**
Argument that the safety goals for an item are complete and satisfied by evidence compiled from work products of the safety activities during development

NOTE Safety case can be extended to cover safety issues beyond the scope of this standard.
Main terms …

Exposure
state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis

Severity
measure of the extent of harm to an individual in a specific situation

Automotive Safety Integrity Level (ASIL)
one of four levels to specify the item’s or element’s necessary requirements of ISO 26262 and safety measures for avoiding an unreasonable residual risk with D representing the most stringent and A the least stringent level

Safety goal
Top-level safety requirement as a result of the hazard analysis and risk assessment
IV – Vocabulary

Main terms …

**Random hardware fault**
Failure that may occur unpredictably during the lifetime of a hardware element and that follows a probability distribution

NOTE: Random hardware failure rates can be predicted with reasonable accuracy.

**Systematic fault**
Failure of an element or item that is caused in a deterministic way during development, manufacturing, or maintenance

NOTE: Systematic failures can be prevented by applying design measures or production process changes on this element or item.
Main terms …

**Fault**
abnormal condition that can cause an element or an item to fail

**Hazard**
Potential source of harm

**Failure**
Termination of the ability of an element or an item to perform a function as required

**ASIL decomposition**
Apportioning of safety requirements redundantly to sufficiently independent elements with the objective of reducing the ASIL of the elements
V – Management of Functional Safety

1. Vocabulary

2. Management of functional safety

3. Concept phase

4. Product development: system level

5. Product development: hardware level

6. Product development: software level

7. Production and operation

8. Supporting processes

9. ASIL-oriented and safety-oriented analyses

10. Guideline on ISO 26262 (informative)
**Objectives**

The objective of this clause is to define the requirements on the organizations that are responsible for the safety lifecycle, or that perform safety activities in the item’s safety lifecycle.

This clause serves as a prerequisite to all the ISO 26262 activities in the item’s safety lifecycle.
V – Management of Functional Safety

ASIL cotation

Requirement specification
Safety goals and Functional safety concept

Validation e.g. vehicle driving tests

Vehicle integration

Architecture and system design
Technical Safety concept

Verification e.g. HIL test

System integration

HW & SW component design
Measures for fault avoidance and mitigation

Verification e.g. Module testing

Module / Component integration

Implementation

Safety analysis

e.g. System FMEA
RBD, FTA,
State transition diagrams

e.g. Component FMEA
Detailed FTA
V – Management of Functional Safety

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

4-11 Release for production

5 Hardware level
6 Software level

Part 2

Product development

Other technologies
Controllability
External measures

Operation planning
Production planning

7-6 Operation and decommissioning
7-5 Production

Concept phase

After SOP

Back to appropriate lifecycle phase

MAJ 07/03/2010

Introduction à la norme ISO 26262
V – Management of Functional Safety

Requirements to perform this part (global)

- Safety culture needed
- Quality management (ISO 9001 / ISO TS 16949)
- Training & Qualification (knowledge areas: safety practices, methodology expertise, functional safety process…)
- Application of safety lifecycle (tailoring of lifecycle: combining per splitting sub-phases, performing an activity in an added phase or sub-phase…)
Requirements during development phase...

- Safety responsibilities (project manager, appointed, role & mission, safety manager…)
  - The role of the safety manager can be filled by the project manager
  - The tasks of the safety manager can be tailored according to the size of the project and the ASIL.
  - Functional safety management tasks include the timely and professional delivery of safety activity results
Requirements during development phase…

Planning for all safety management activities.

*Safety manager* shall plan the activities, shall create a safety plan & safety planning

The safety plan shall either be:

a) a plan referenced in the overall project plan; or
b) included in the overall project plan, such that the safety activities are distinguishable.

Each of the activities in the *safety plan* should be described according to the following:

- Objective
- Required work products from other activities, such as described in prerequisites
- Person in charge of safety activities
- Starting point in time and duration
- Documentation of the respective work products
V – Management of Functional Safety

Requirements during development phase...

In developing the safety plan, the specific activities shall be tailored according to the ASIL and the constraints of the project.

- Safety case (compiled progressively during the development phase)

The safety case shall be comprehensive and complete with regard to the work products defined in the safety plan.
### Requirements during development phase...

#### Confirmation measures for ensuring functional safety

<table>
<thead>
<tr>
<th></th>
<th>Functional safety audit</th>
<th>Confirmation review</th>
<th>Functional safety assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject</strong></td>
<td>Implementation of the processes required for functional safety</td>
<td>Work product</td>
<td>Item as described in the item definition (see ISO°26262-3, Clause°5)</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Audit report°</td>
<td>Confirmation review report°</td>
<td>Assessment report on functional safety of the item</td>
</tr>
<tr>
<td><strong>Responsibility of the Auditor/Reviewer/Safety Assessor</strong></td>
<td>Adequate evaluation of the processes against the definition of the activity, referenced or listed in the safety plan.</td>
<td>Adequate evaluation of the compliance of the work product with the respective requirements of ISO°26262</td>
<td>Adequate evaluation of the achieved functional safety level</td>
</tr>
<tr>
<td><strong>Timing during lifecycle</strong></td>
<td>During implementation of the required processes</td>
<td>After completion of the corresponding safety activity</td>
<td>Progressively during development, or in a single block</td>
</tr>
<tr>
<td><strong>Scope and depth</strong></td>
<td>Determined by the auditor</td>
<td>Planned prior to the review, in accordance with the safety plan</td>
<td>Review of processes and safety measures required for functional safety</td>
</tr>
</tbody>
</table>

° can be included in a functional safety assessment report
## V – Management of Functional Safety

### Requirements during developpement phase…

<table>
<thead>
<tr>
<th>Confirmation measures</th>
<th>applies to ASIL of the</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirmation review of the hazard analysis &amp; risk assessment, of the item that is dealt with in accordance with ISO°26262 (see ISO°26262-3, Clause 7 and if applicable, ISO 26262-8, Clause 5) - independent from the developers of the item</td>
<td>I3</td>
<td>For all ASILs, and including hazards rated as QM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirmation review of the safety plan (see Clause 6) - independent from the developers of the item / project management</td>
<td>-</td>
<td>I1</td>
<td>I2</td>
<td>I3</td>
<td></td>
</tr>
<tr>
<td>Confirmation review of the integration and testing plan (see ISO°26262-4, Clause 5) - independent from the developers of the item / project management</td>
<td>I0</td>
<td>I1</td>
<td>I2</td>
<td>I3</td>
<td></td>
</tr>
<tr>
<td>Confirmation review of the validation plan (see ISO°26262-4, Clause 5) - independent from the developers of the item / project management</td>
<td>I0</td>
<td>I1</td>
<td>I2</td>
<td>I3</td>
<td></td>
</tr>
<tr>
<td>Confirmation review of the safety analyses (FMEA, FTA) (see ISO°26262-9, 8.4.8)</td>
<td>I1</td>
<td>I1</td>
<td>I2</td>
<td>I3</td>
<td></td>
</tr>
<tr>
<td>Confirmation review of the qualification of software tools (see ISO°26262-8, Clause 11) - independent from the person performing the qualification of the software tool</td>
<td>-</td>
<td>I0</td>
<td>I1</td>
<td>I1</td>
<td></td>
</tr>
<tr>
<td>Confirmation review of the proven in use arguments (analysis, data and credit), of the candidates. See ISO°26262-8, Clause 14. - independent from the supplier of the argument</td>
<td>I0</td>
<td>I1</td>
<td>I2</td>
<td>I3</td>
<td></td>
</tr>
<tr>
<td>Confirmation review of the completeness of the safety case (see 6.4.5) - independent from authors of safety case</td>
<td>I0</td>
<td>I1</td>
<td>I2</td>
<td>I3</td>
<td></td>
</tr>
<tr>
<td>Audit of functional safety processes (see 6.4.6) - independent from the persons working in accordance with the processes required for functional safety</td>
<td>-</td>
<td>I0</td>
<td>I2</td>
<td>I3</td>
<td></td>
</tr>
<tr>
<td>Functional safety assessment (see 6.4.6.7) - independent from the supplier of the safety case</td>
<td>-</td>
<td>I0</td>
<td>I2</td>
<td>I3</td>
<td></td>
</tr>
</tbody>
</table>

The confirmation measures shall be performed according to their **ASIL** and following table.
V – Management of Functional Safety

Requirements during development phase...

- **Safety assessment** shall consider:
  - Confirmation plan
  - Recommendations from the functional safety assessment, if available
  - Results from the functional safety audits and confirmation reviews

One or more persons shall be appointed to carry out a functional safety assessment and shall provide a judgement of functional safety
Requirements for compliance

When claiming compliance with ISO 26262, each requirement shall be complied with, unless one of the following applies:
1) Tailoring in accordance with ISO 26262-2 has been planned and shows that the requirement does not apply.
2) A rationale is available that the non-compliance is acceptable and the rationale has been assessed in accordance with ISO 26262-2.
Information marked as a "NOTE" is only for guidance in understanding, or for clarification of, the associated requirement and shall not be interpreted as a requirement itself.
Interpretation of tables

- Tables may be normative or informative depending on their context.
- The different methods listed in a table contribute to the level of confidence that the corresponding requirement shall apply.
- Each method in a table is either a consecutive entry (marked by a sequence number in the leftmost column, e.g., 1, 2, 3) or an alternative entry (marked by a number followed by a letter in leftmost column, e.g., 2a, 2b, 2c).
- For consecutive entries all methods are recommended in accordance with the ASIL.
- For alternative entries an appropriate combination of methods shall be applied in accordance with the ASIL, independently of whether they are listed in the table or not. If methods are listed with different degrees of recommendation for an ASIL the higher one should be preferred.
- For each method, the degree of recommendation to use the corresponding method depends on the ASIL and is categorized as follows:
  - ”++” The method is highly recommended for this ASIL.
  - “+” The method is recommended for this ASIL.
  - “o” The method has no recommendation for or against its usage for this ASIL.
VI – Concept phase

Objectives

The objective of this part is:
- to define & describe the item
- to develop an adequate understanding of the item
- to select the applicable safety lifecycle
- to identify and categorize the potential hazard of the item
- to formulate the safety goals
- to define the preliminary architecture element
VI – Concept phase

Item definition

➢ Information needed:
  o purpose and content of the item
  o functional requirements of the item
  o further requirement for the item regarding the environmental conditions in which the item is used
  o boundary of the item
  o interfaces with other items
  o requirements from other items
  o allocation & distribution of functions among the items involved
VI – Concept phase

Initiation of the safety lifecycle

- Determination of the development category

It shall be determined whether the item is a modification of an existing item or if it is a new development

  - In case of a new development, the entire safety lifecycle shall be applied
  - In case of a modification, the relevant lifecycle sub-phases and activities shall be determined

- Impact analysis & adapted safety lifecycle

  - In case of a modification of the item, an impact analysis shall be conducted to determine the areas affected by the modification
VI – Concept phase

Hazard risk analysis

- The hazard analysis and risk assessment sub-phase comprises three steps:
  a) Situation analysis and hazard identification: The goal of the situation analysis and hazard identification is to identify the potential unintended behaviours of the item that could lead to a hazardous event.
  b) Hazard classification: The hazard classification schema comprises the determination of the severity (S), the probability of Exposure (E) and the Controllability (C) associated with the considered hazard of the item.
  c) ASIL determination: Determining the required automotive safety integrity level.
a) Situation analysis & hazard identification

- The operational situations and operating modes in which an item's malfunctioning behaviour is able to trigger hazards shall be described; both for cases when the item is correctly used and when it is incorrectly used in a **foreseeable way**.
- A list of **operational situations** to be evaluated shall be prepared.
- The failure modes and hazards shall be detailed.
- The consequences of hazardous events shall be identified for relevant operational situations and operating modes.
a) Situation analysis & hazard identification

The operational situation addresses the limits within which the item is expected to behave in a safe manner. For example, a normal passenger road vehicle is not expected to travel cross country at high speed. Example: Operational situations include visibility, road surface traction, road surface unevenness, road surface bank angle change, road surface pitch change, objects in the path of the vehicle, objects on a trajectory intersecting the path of the vehicle, relative velocity of the vehicle and the object it is approaching, relative to the distance (gap).

Only the item **without any safety mechanism** shall be evaluated during situation analysis and hazard identification (i.e. safety mechanisms intended to be implemented or that have already been implemented in predecessor systems shall not be considered as a means for providing risk reduction).
b) Hazard classification

- Estimation of potential severity

The severity of potential harm shall be estimated. The severity shall be assigned to one of the severity classes S0, S1, S2 or S3 in accordance with the following table:

<table>
<thead>
<tr>
<th>Class</th>
<th>S0</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>No injuries</td>
<td>Light and moderate injuries</td>
<td>Severe and life-threatening injuries (survival probable)</td>
<td>Life-threatening injuries (survival uncertain), fatal injuries</td>
</tr>
</tbody>
</table>

The severity class can be based on a combination of injuries, and this can lead to a higher evaluation of S than would result from just looking at single injuries.
## VI – Concept phase

### Examples of severity categorisation

<table>
<thead>
<tr>
<th>Class</th>
<th>S0</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>No injuries</td>
<td>light and moderate injuries</td>
<td>Severe injuries, possibly life-threatening, survival probable</td>
<td>Life-threatening injuries (survival uncertain) or fatal injuries</td>
</tr>
<tr>
<td>Reference for single injuries (from AIS scale)</td>
<td>AIS 0</td>
<td>more than 10% probability of AIS 1-6 (and not S2 or S3)</td>
<td>more than 10% probability of AIS 3-6 (and not S3)</td>
<td>more than 10% probability of AIS 5-6</td>
</tr>
<tr>
<td>Informative examples</td>
<td>-Pushing over roadside infrastructure, e.g. post or fence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Light collision</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Light grazing damage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Damage while entering or leaving a parking space</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Leaving the road without collision or rollover</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-Side collision, e.g. crashing into a tree (impact to passenger cell), $15 &lt; \Delta v &lt; 25$ km/h</td>
<td>$\Delta v &lt; 15$ km/h</td>
<td>$15 &lt; \Delta v &lt; 25$ km/h</td>
<td>$\Delta v &gt; 25$ km/h</td>
<td></td>
</tr>
<tr>
<td>Side collision with a passenger car (impact to passenger cell)</td>
<td>$\Delta v &lt; 15$ km/h</td>
<td>$15 &lt; \Delta v &lt; 35$ km/h</td>
<td>$\Delta v &gt; 35$ km/h</td>
<td></td>
</tr>
<tr>
<td>Rear/front collision between two passenger cars</td>
<td>$\Delta v &lt; 20$ km/h</td>
<td>$20 &lt; \Delta v &lt; 40$ km/h</td>
<td>$\Delta v &gt; 40$ km/h,</td>
<td></td>
</tr>
<tr>
<td>Other collisions</td>
<td>-Scrape collision with little vehicle to vehicle overlap (&lt; 10%)</td>
<td></td>
<td></td>
<td>-Roof or side collision with considerable deformation</td>
</tr>
<tr>
<td>Under riding a truck</td>
<td>Without deformation of the passenger cell</td>
<td></td>
<td></td>
<td>With deformation of the passenger cell</td>
</tr>
<tr>
<td>Pedestrian/bicycle accident</td>
<td>E.g. during a turning manoeuvre inside built-up area</td>
<td></td>
<td></td>
<td>Outside built-up area</td>
</tr>
</tbody>
</table>
VI – Concept phase

AIS : Abbreviated Injury Scale

AIS 0: no injuries.

AIS 1: light injuries such as skin-deep wounds, muscle pains, whiplash etc.

AIS 2: moderate injuries such as deep flesh wounds, concussion with up to 15 minutes of unconsciousness, uncomplicated long bone fractures, uncomplicated rib fractures etc.

AIS 3: severe but not life-threatening injuries such as skull fractures without brain injury, spinal dislocations below the fourth cervical vertebra without damage to the spinal cord, more than one fractured rib without paradoxical breathing etc.

AIS 4: severe injuries (life-threatening, survival probable) such as concussion with or without skull fractures with up to 12 hours of unconsciousness, paradoxical breathing.

AIS 5: critical injuries (life-threatening, survival uncertain) such as spinal fractures below the fourth cervical vertebra with damage to the spinal cord, intestinal tears, cardiac tears, more than 12 hours of unconsciousness including intracranial bleeding.

AIS 6: extremely critical or fatal injuries such as fractures of the cervical vertebrae above the third cervical vertebra with damage to the spinal cord, extremely critical open wounds of body cavities (thoracic and abdominal cavities) etc.
b) Hazard classification

- Estimation of the probability of exposure

The probability of exposure of each operational situations shall be estimated. The probability of exposure shall be assigned to one of the probability classes E0, E1, E2, E3 and E4 in accordance with following table

<table>
<thead>
<tr>
<th>Class</th>
<th>E0</th>
<th>E1</th>
<th>E2</th>
<th>E3</th>
<th>E4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>incredible</td>
<td>Very low probability</td>
<td>Low probability</td>
<td>Medium probability</td>
<td>High probability</td>
</tr>
</tbody>
</table>

The number of vehicles equipped with the item shall not be considered when estimating the probability of exposure

The hazard analysis and risk assessment is performed for individual vehicles equipped with the item.
## Introduction à la norme ISO 26262

### Part 3: Concept phase

#### Illustration

<table>
<thead>
<tr>
<th>Class</th>
<th>E1</th>
<th>E2</th>
<th>E3</th>
<th>E4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Very low probability</td>
<td>Low probability</td>
<td>Medium probability</td>
<td>High probability</td>
</tr>
<tr>
<td>Definition of duration/probability of exposure</td>
<td>Not specified</td>
<td>&lt; 1% of average operating time</td>
<td>1% - 10% of average operating time</td>
<td>&gt; 10% of average operating time</td>
</tr>
</tbody>
</table>

Class of probability of exposure regarding duration/probability of exposure in driving situations.
### Illustration

#### Class of probability of exposure regarding duration/probability of exposure in driving situations

<table>
<thead>
<tr>
<th>Class</th>
<th>E1</th>
<th>E2</th>
<th>E3</th>
<th>E4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Very low probability</td>
<td>Low probability</td>
<td>Medium probability</td>
<td>High probability</td>
</tr>
<tr>
<td>Definition of frequency</td>
<td>Situations that occur less often than once a year for the great majority of drivers</td>
<td>Situations that occur a few times a year for the great majority of drivers</td>
<td>Situations that occur once a month or more often for an average driver</td>
<td>All situations that occur during almost every drive on average</td>
</tr>
<tr>
<td>Informative examples</td>
<td>Stop at railway crossing, which requires the engine to be restarted Towing Jump start</td>
<td>Pulling a trailer, driving with a roof rack Driving on a mountain pass with an unsecured steep slope Driving situation with a deviation from the desired path Snow and ice</td>
<td>Fuelling Overtaking Tunnels Hill hold Car wash Wet roads Congestion</td>
<td>Starting Shifting gears Accelerating Braking Steering Using indicators Parking Driving backwards</td>
</tr>
</tbody>
</table>
b) Hazard classification

- Estimation of controllability

The controllability by the driver or other traffic participants shall be estimated. The controllability shall be assigned to one of the controllability classes C0, C1, C2 and C3 in accordance with following table.

<table>
<thead>
<tr>
<th>Class</th>
<th>C0</th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Controllable in general</td>
<td>Simply controllable</td>
<td>Normally controllable</td>
<td>Difficult to control or uncontrollable</td>
</tr>
</tbody>
</table>

The evaluation of possibilities of the avoidance of a specific harm, that is the controllability, is an estimation of the probability that the driver or other endangered persons are able to gain control of the hazardous event that is arising and are able to avoid the specific harm.
## VI – Concept phase

### Illustration

<table>
<thead>
<tr>
<th>Class</th>
<th>C0</th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Controllable in general</td>
<td>Simply controllable</td>
<td>Normally controllable</td>
<td>Difficult to control or uncontrollable</td>
</tr>
<tr>
<td>Definition</td>
<td>Controllable in general</td>
<td>99% or more of all drivers or other traffic participants are usually able to avoid a specific harm.</td>
<td>90% or more of all drivers or other traffic participants are usually able to avoid a specific harm.</td>
<td>Less than 90% of all drivers or other traffic participants are usually able, or barely able, to avoid a specific harm.</td>
</tr>
<tr>
<td>Informative examples</td>
<td>Unexpected increase in radio volume</td>
<td>Situations that are considered distracting Unavailability of a driver assisting system</td>
<td>When starting the vehicle with a locked steering column, the car can be brought to stop by almost all drivers early enough to avoid a specific harm to persons nearby. Faulty adjustment of seats while driving can be controlled by almost all drivers by bringing the vehicle to a stop.</td>
<td>Driver can normally avoid departing from the lane in case of a failure of ABS during emergency braking. Driver is normally able to avoid departing from the lane in case of a motor failure at high lateral acceleration (motorway exit). Driver is normally able to bring the vehicle to a stop in case of a total lighting failure at medium or high speed on an unlighted country road without departing from the lane in an uncontrolled manner. Driver is normally able to avoid hitting an unlit vehicle on an unlit country road.</td>
</tr>
</tbody>
</table>

**Examples of possibly controllable hazards by the driver or by the endangered individuals**

- Unexpected increase in radio volume
- Situations that are considered distracting
- Unavailability of a driver assisting system
- When starting the vehicle with a locked steering column, the car can be brought to stop by almost all drivers early enough to avoid a specific harm to persons nearby.
- Faulty adjustment of seats while driving can be controlled by almost all drivers by bringing the vehicle to a stop.
- Driver can normally avoid departing from the lane in case of a failure of ABS during emergency braking.
- Driver is normally able to avoid departing from the lane in case of a motor failure at high lateral acceleration (motorway exit).
- Driver is normally able to bring the vehicle to a stop in case of a total lighting failure at medium or high speed on an unlighted country road without departing from the lane in an uncontrolled manner.
- Driver is normally able to avoid hitting an unlit vehicle on an unlit country road.
c) ASIL classification

An ASIL shall be determined for each hazardous event using the estimation parameters severity (S), probability of exposure (E) and controllability (C) in accordance with following table.

The work product of the ASIL determination shall include: the operational situations and operating modes with severity, probability of exposure, controllability and the resulting ASIL.
c) ASIL classification

Scenario 1

- Hazard
  - Exposure y + Controlability x → Accident z
  - ASIL A

Scenario 2

- Exposure v + Controlability u → Accident w
  - ASIL B
  - ASIL = max (ASIL A, ASIL B)
Introduction à la norme ISO 26262

MAJ 07/03/2010

51/134

acceptable

not acceptable

Probability of exposition to driving situation where accident can potentially happen

Risk Reduction external to technical system: e.g. driver controls situation

Probability per hour (runtime)

Always

Sometimes

Rarely

Very rarely

Extreme improbable

Severity of possible accident

Safety class (ASIL)

Tolerable Risk

Lower than tolerable risk

Residual Risk

Severity

Low

Important

Hazardous

(Catastrophically)

ASIL level (A to D)

Reliability of system and absence of systematic faults safety class (ASIL)
Evaluation of exposure in mutually exclusive operational situations

During hazard analysis and risk assessment, having established the list of operational situations and having estimated the values of the S, E and C parameters for each situation, it shall be ensured that the chosen level of detail of the list of operational situations does not lead to an inappropriate lowering of the ASIL of the corresponding safety goals.

Applies to ASIL A, B, C and D: A *safety goal* shall be formulated for each hazardous event evaluated in the hazard analysis.

*An ASIL shall be assigned to each safety goal.*
*A safe state should be assigned to each safety goal.*
VI – Concept phase

Example 1

**Safety goal** “do not let valve1 closed when speed is higher than 100 km/h”. ASIL C

Safe state: valve1 open.

Example 2

**Safety goal** “No lock of steering during driving”. ASIL D
VI – Concept phase

**Functional Safety Concept**

➢ To comply with the safety goals, the functional safety concept specifies the *basic safety mechanisms* and *safety measures* in the form of functional safety requirements.

➢ To specify safety mechanisms the functional safety concept addresses the following:

  • Fault detection and failure mitigation;
  • Transitioning to a safe state;
  • Fault tolerance mechanisms, where a fault does not lead directly to the violation of the safety goals and which maintains the system in a safe state (with or without degradation);
  • Fault detection and driver warning in order to reduce the risk exposure time to an acceptable interval (repair request, stop request); and
  • Arbitration logic to select the most appropriate control request from multiple requests generated simultaneously by different functions.
Functional Safety Concept

If the functional safety requirements are allocated to elements of other technologies then the following shall apply:

- the functional safety requirements implemented by other technologies shall be derived and allocated to the corresponding elements
- the functional safety requirements relating to the interfaces with other technologies shall be specified
- the implementation of functional safety requirements by other technologies shall be ensured through specific measures
VI – Concept phase

Functional Safety Concept

Illustration

⇒ L, SW et Batt = Significant failures

⇒ sensor, logic et warning = monitoring
VI – Concept phase
ASIL decomposition

Objectives

The objective of this clause is to provide rules and guidance for decomposing safety requirements into redundant safety requirements to allow ASIL tailoring at the next level of detail.

Sub-phases of ASIL decomposition and criticality analysis
General

Starting from safety goals, the safety requirements are derived and detailed during the development phases. The ASIL, as an attribute of the safety goal, is inherited by each subsequent safety requirement. The functional and technical safety requirements are allocated to architectural elements, starting with preliminary architectural assumptions and ending with the hardware and software elements.

The method of ASIL tailoring during the design process given in ISO 26262 is called "ASIL decomposition". During the allocation process, benefit can be obtained from architectural decisions and the existence of independent architectural elements. This offers the opportunity:

• to implement safety requirements redundantly by these independent architectural elements; and
• to assign a potentially lower ASIL to these redundant safety requirements.

If there is no independence between the elements, the ASIL of the safety goal is inherited by each requirement and element.
VI – Concept phase

ASIL decomposition

Classification scheme of ASILs when decomposing safety requirements
VI – Concept phase

ASIL decomposition

Example

Safety goal : Not to open the door while the vehicle speed is higher than 15 km/h :

ASILC.

1: The DSC will send the accurate vehicle speed information to the PSDM \(\Rightarrow\) ASILC.

2: The PSDM will allow the powering of the actuator only if the vehicle speed is below 15 km/h \(\Rightarrow\) ASIL B(C).

3: The switch will be in an open state if the vehicle speed is above 15 km/h \(\Rightarrow\) ASIL A(C).
VI – Concept phase

To sum up this part…

Operational situation(s) → Scenario(s) + S / E / C quotation → max (ASIL) → ASIL classification → Safety goal

Defined from safe state

Σ FSR = Functional Safety Concept

Verication of FSC
# VII – Product development: system level

## 1. Vocabulary

| 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 of product development of the system level | 4-6 Specification of the technical safety requirements | 4-7 System design | 4-8 Item integration and testing |

## 5. Product development: hardware level

| 5-5 Initiation of product development at the hardware level | 5-6 Specification of hardware safety requirements | 5-7 Hardware design | 5-8 Hardware architectural metrics |

## 6. Product development: software level

| 6-5 Initiation 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 |

## 8. Supporting processes

| 8-5 Interfaces within 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 analyses

| 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 analyses |

## 10. Guideline on ISO 26262 (informative)

**Intervention à la norme ISO 26262**

**MAJ 07/03/2010**

**Part 4**
The objective of this part is:

- to develop the **technical safety concept**
- to design a system that fulfils the functional requirements
- to verify the system design against the technical safety requirements
- to check the integration and testing
- to provide evidence that the safety related requirements are appropriate
VII – Product development: system level

Where are we in the STD?

Part 4: Product development: system level

4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design

Part 5: Product development: hardware level

Part 6: Product development: software level

4-8 Item integration and testing
4-9 Safety validation
4-10 Functional safety assessment
4-11 Release for production
**VII – Product development : system level**

**Specification of technical safety concept**

The first objective of this sub-phase is to *develop the technical safety concept*. The technical safety requirements specification refines the functional safety concept considering the functional concept and the preliminary architectural design.

This part gives a list of recommendations:

- The response of the system or elements to stimuli shall be specified for each *technical safety requirement* in combination with each possible operating mode and system state.
- The technical safety concept shall specify functional, safety-related and/or other relevant dependencies between systems or elements.
VII – Product development : system level

Specification of technical safety concept

Example

The ECU in charge of the Adaptive Cruise Control (ACC) switches off the ACC functionality when the brake system ECU reports that the Vehicle Stability Control functionality is unavailable.

We have as well:

- Control of latent faults (Safety mechanisms dedicated to detect and control latent faults shall be specified)
- Redundancy (If redundancy is used the type of redundancy used shall be specified)
VII – Product development : system level

System design

The first objective of this subphase is to develop the system design and the technical safety concept that comply with the functional requirements and the technical safety requirements specification of the item. The second objective of this sub-phase is to verify the system design against the technical safety requirements.

Requirements for architecture

If requirements with different ASIL are allocated to one architectural element this element shall be developed according to the highest ASIL.

If a separation between safety-related elements and other elements is not possible, each element of the item and their interactions shall be treated as safety-related.
System design

Avoidance of systematic faults:
- Measures for avoidance of systematic faults shall be specified
- Deductive and inductive analysis dedicated to causes and effects of systematic failures shall be applied according to following table

<table>
<thead>
<tr>
<th>Method</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
</tbody>
</table>
| Deductive analysis | o    | +    | ++   | ++ 
| Inductive analysis | ++   | ++   | ++   | ++ |

a. Deductive analysis methods include FTA, reliability block diagrams.
b. Inductive analysis methods include FMEA, ETA, Markov modelling.
System design

- Usage of well-trusted design principles:
  
  a) Re-use of well-trusted safety architecture;
  b) Re-use of well-trusted design principles or designs for elements, hardware and software components;
  c) Re-use of well-trusted mechanisms for the detection and control of failures;
  d) Re-use of well-trusted or standardised interfaces.
**System design**

- Measures for control of random hardware failures during operation. Applies to ASIL (B, C and D:
  - The target values for both metrics of part 5 clause 8, shall be specified for final evaluation at the item level
  - One of the alternative procedures of part 5 clause 9 shall be chosen and the target values for final validation at item level shall be specified.
  - Appropriate targets for failure rates and diagnostic coverage should be specified at element level in order to comply with the target values of the metrics in part 5 clause 8 and the procedures in part 5 clause 9.
VII – Product development : system level

System design

- Verification and system design :

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>B</td>
</tr>
<tr>
<td></td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>D</td>
</tr>
<tr>
<td>1a System design inspection&lt;sup&gt;a&lt;/sup&gt;</td>
<td>+</td>
</tr>
<tr>
<td>1b System design walkthrough&lt;sup&gt;a&lt;/sup&gt;</td>
<td>++</td>
</tr>
<tr>
<td>2a Simulation&lt;sup&gt;b&lt;/sup&gt;</td>
<td>+</td>
</tr>
<tr>
<td>2b System prototyping and vehicle tests&lt;sup&gt;b&lt;/sup&gt;</td>
<td>+</td>
</tr>
<tr>
<td>3 Safety analyses&lt;sup&gt;c&lt;/sup&gt;</td>
<td>+</td>
</tr>
</tbody>
</table>

<sup>a</sup> Methods 1a and 1b serve as check of complete and correct detailing and implementation of the technical safety requirements into system design.

<sup>b</sup> Methods 2a and 2b can be used advantageously as a fault injection technique.

<sup>c</sup> For conducting safety analyses, see ISO 26262-9: —, Clause 8.
Item integration & testing

The first objective of the system integration and testing is to integrate the parts of a system and, if applicable, systems of other technologies and external measures or systems step by step into the entire system. The integrated system has to comply with each safety requirement in accordance with its specification and ASIL classification.

The second objective of the system integration and testing is to verify that the system design is correctly realised by the entire system.
### Item integration & testing

- **Table 3- Methods for deriving test cases for item integration testing**

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Analysis of requirements</td>
<td>++</td>
</tr>
<tr>
<td>1b Analysis of external and internal interfaces</td>
<td>+</td>
</tr>
<tr>
<td>1c Generation and analysis of equivalence classes for hardware software integration</td>
<td>+</td>
</tr>
<tr>
<td>1d Analysis of boundary values</td>
<td>+</td>
</tr>
<tr>
<td>1e Knowledge or experience based error guessing</td>
<td>+</td>
</tr>
<tr>
<td>1f Analysis of functional dependencies</td>
<td>+</td>
</tr>
<tr>
<td>1g Analysis of common limit conditions, sequences, and sources of common cause</td>
<td>+</td>
</tr>
<tr>
<td>1h Analysis of environmental conditions and operational use cases</td>
<td>+</td>
</tr>
<tr>
<td>1i Analysis of field experience</td>
<td>+</td>
</tr>
</tbody>
</table>
VII – Product development : system level

Item integration & testing

➢ Table 4 — Correctness of implementation of system design specification and technical safety requirements

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Requirements-based testa</td>
<td>++</td>
</tr>
<tr>
<td>1b Fault injection testb</td>
<td>+</td>
</tr>
<tr>
<td>1c Back-to-back testc</td>
<td>+</td>
</tr>
</tbody>
</table>

a A requirements-based test denotes a test against functional and non-functional requirements.
b A fault injection test uses special means to introduce faults into the test object during runtime. This can be done within the software via a special test interface or specially prepared hardware. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety mechanisms are not invoked.
c A back-to-back test compares the responses of the test object with the responses of a simulation model to the same stimuli, to detect differences between the behaviour of the model and its implementation.
### Table 5 - Correctness of functional performance of safety mechanisms

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>Back-to-back test</td>
<td>+</td>
</tr>
<tr>
<td>Performance test</td>
<td>+</td>
</tr>
</tbody>
</table>

*a* A back-to-back test compares the responses of the test object with the responses of a simulation model to the same stimuli, to detect differences between the behaviour of the model and its implementation.

*b* A performance test can verify the performance concerning e.g. task scheme, timing, power output in the context of the whole test object, and can verify the ability of the hardware to run with the intended control software.

### Table 6 - Consistency and correctness of implementation of external and internal interfaces

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>Test of external interfaces</td>
<td>+</td>
</tr>
<tr>
<td>Test of internal interfaces</td>
<td>+</td>
</tr>
<tr>
<td>Interface consistency check</td>
<td>+</td>
</tr>
</tbody>
</table>

*a* Interfaces tests of the test object include tests of analogue and digital inputs and outputs, boundary tests and equivalent-class tests to completely test the specified interfaces, compatibility, timings and other specified ratings for the test object. Internal interfaces of an ECU are tested by static tests for the compatibility of software and hardware as well as dynamic tests of SPI- or I²C-communications or any other interface between elements of an ECU.


Table 7 — Effectiveness of diagnostic coverage of hardware fault detection mechanisms

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Fault injection testa</td>
<td>++</td>
</tr>
<tr>
<td>1b Error guessing testb</td>
<td>++</td>
</tr>
</tbody>
</table>

- a A fault injection test uses special means to introduce faults into the test object during runtime. This can be done within the software via a special test interface or specially prepared hardware. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety mechanisms are not invoked.
- b An error guessing test uses expert knowledge and data collected through lessons learned to anticipate errors in the test object. Then a set of tests along with adequate test facilities is designed to check for these errors. Error guessing is an effective method given a tester who has previous experience with similar test objects.

Table 8 — Level of robustness

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Resource usage testa</td>
<td>++</td>
</tr>
<tr>
<td>1b Stress testb</td>
<td>++</td>
</tr>
</tbody>
</table>

- a A resource usage test can be done statically e.g. by checking for code sizes or analyzing the code regarding interrupt usage, in order to verify that worst-case scenarios do not run out of resources, or dynamically by runtime monitoring.
- b A stress test verifies the test object for correct operation under high operational loads or high demands from the environment. Therefore, tests under high loads on the test object, or with exceptional interface loads, or values (bus loads, electrical shocks etc.), as well as tests with extreme temperatures, humidity or mechanical shocks, can be applied.
Item integration & testing

- Table 11 — Consistency and correctness of implementation of external and internal interfaces

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Test of external interfaces</td>
<td>+</td>
</tr>
<tr>
<td>1b Test of internal interfaces</td>
<td>+</td>
</tr>
<tr>
<td>1c Interface consistency check</td>
<td>o</td>
</tr>
<tr>
<td>1d Communication test</td>
<td>++</td>
</tr>
<tr>
<td>1e Test of interaction/communication</td>
<td>++</td>
</tr>
</tbody>
</table>

a An interface test of the system includes tests of analogue and digital inputs and outputs, boundary tests, and equivalent-class tests, to completely test the specified interfaces, compatibility, timings, and other specified characteristics of the system. Internal interfaces of the system are tested by static tests, (e.g. match of plug connectors), as well as by dynamic tests concerning bus communications or any other interface between elements of the system.

b A communication and interaction test includes tests of the communication between the elements of the system as well as between the system under test and other vehicle systems during runtime against functional and non-functional requirements.
### Table 12 — Effectiveness of diagnostic failure coverage of safety mechanisms at item level

<table>
<thead>
<tr>
<th>Test methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Fault injection testa</td>
<td>+</td>
</tr>
<tr>
<td>1b Error guessing testb</td>
<td>+</td>
</tr>
<tr>
<td>1c Test derived from field experiencec</td>
<td>o</td>
</tr>
</tbody>
</table>

- **a** A fault injection test uses special means to introduce faults into the item. This can be done within the item via a special test interface, specially prepared elements, or communication devices. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety measures are not invoked.
- **b** An error guessing test uses expert knowledge and data collected through lessons learned to anticipate errors in the item. Then a set of tests along with adequate test facilities is designed to check for these errors. Error guessing is an effective method given a tester who has previous experience with similar items.
- **c** A test derived from field experience uses the experience and data gathered from the field. Erroneous system behaviour or newly discovered operational situations are analysed and a set of tests is designed to check the system with respect to the new findings.
Safety validation

The first objective is 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.

The second objective is to provide evidence that the safety goals are correct, complete and fully achieved at vehicle level.
Safety validation

- The following methods and measures shall be used or carried out, depending on the ASIL level
  - reproducible tests with specified test procedures, test cases, and pass/fail criteria;
  - EXAMPLE: positive tests of functions and safety requirements, black box, simulation, tests under boundary conditions, fault injection, durability tests, stress tests, highly accelerated life testing (HALT), simulation of external influences
  - analyses (e.g. FMEA, FTA, ETA, simulation);
  - long-term tests, such as vehicle driving schedules and captured test fleets;
  - user tests under real-life conditions, panel or blind tests, expert panels;
  - reviews.
**Functional safety assessment**

The objective of the requirements in this Clause is to assess functional safety, that *is achieved* by the item.

For each step of the safety lifecycle in ISO 26262-2 Figure 2, the specific topics to be addressed by the functional safety assessment shall be identified.

The functional safety assessment shall be conducted in accordance with ISO 26262-2 clause 6.4.6.7.
VII – Product development : system level

B.1 System functions
B.1.1 Detailed presentation of the system, components and functional attributes
B.1.2 Overview of electrical components
B.1.3 Hazard analysis and risk assessment of functions

B.2 Hardware
B.2.1 Block diagram of functions
B.2.2 Layout and circuit diagram
B.2.3 Interfaces

B.3 Safety concept
B.3.1 Basic principles of the safety concept
B.3.2 Definition of the safe state(s), or degradation principle
B.3.3 Function of the safety concept
B.3.4 Evidence of safe operation under fault conditions (fault tolerance)
B.3.5 Interaction between the safety concept and other systems/functions
B.3.6 Allocation of functional safety requirements to
  — E/E system;
  — Systems of other technologies;
  — External risk reduction measures;

B.4 Safety analysis and safety data
B.4.1 Fault analysis (FMEA; FTA, etc.)
B.4.2 Internal monitoring functions
B.4.3 Qualification of reliability data

B.5 Safety design process for the lifecycle phases
B.5.1 Project management
B.5.2 Documentation
B.5.3 Specification phase
B.5.4 Design and development phase
B.5.5 Integration phase
B.5.6 Planning of general validation / safety validation
B.5.7 Results of general validation / safety validation

B.6 Software development
B.6.1 Software safety concept
B.6.2 Software structure
B.6.3 Software tests and documentation
B.6.4 Development tools used
B.6.5 Identification and follow-up monitoring of software changes (version control)
B.6.6 Protection of implemented software against unauthorised changes

B.7 Verification and test
B.7.1 Verification of system functions under fault-free conditions
B.7.2 Verification of system functions under the influence of faults

B.8 Documentation and safety case
B.8.1 Completeness
B.8.2 Consistency
B.8.3 Continuity

B.9 Summary and assessment

Example of an agenda for an assessment of functional safety for ASIL D
VII – Product development: system level

Release for production

The objective of this clause is 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 release documentation of functional safety for release for production shall include the following information:
- the name and signature of the person in charge of release;
- the version/s of the released item;
- the configuration of the released item;
- references to associated documents;
- the release date.
VII – Product development : system level

To sum up this part...

Operational situation(s) → Scenario(s) + S / E / C quotation → max (ASIL) → ASIL classification → Safety goal

Defined from safe state

Functional Safety Requirement 1

Σ TSR = Technical Safety Concept

Technical Safety Requirement 1

…

Technical Safety Requirement i

Σ FSR = Functional Safety Concept

ASIL decomposition

Part 4
VIII – Product development: hardware level

Part 5

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 of 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

5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Hardware architecture 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

6-5 Initiation 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
7-5 Operation, service (maintenance and repair), and decommissioning

8. Supporting processes

8-5 Interfaces within 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 analyses

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 analyses

10. Guideline on ISO 26262 (informative)
The objective of the initiation of the product development for the hardware is to determine and plan the functional safety activities during the individual sub-phases of hardware development.
VIII – Product development: hardware level

Initiation of product development

Informative reference phase model for development of a safety-related item
VIII – Product development : hardware level

Specification of hardware safety requirements

The first objective of this clause is to make available a consistent and complete hardware specification that will be applied to the hardware of the item or element under consideration. The requirements of this specification are hardware safety requirements.

The second objective is to verify that the hardware safety requirements are consistent with the technical safety concept.

A further objective of this phase is to detail the hardware-software interface (HSI) requirements
VIII – Product development : hardware level

Specification of hardware safety requirements

➢ The hardware safety requirements specification shall include:
  o The hardware safety requirements of safety mechanisms dedicated to *control failures external* to the element under consideration with their relevant attributes
  o The hardware safety requirements of safety mechanisms dedicated to *control internal failures* of the hardware of the item or element, with their relevant attributes
  o The hardware safety requirements of safety mechanisms dedicated to *detect and signal internal or external failures*
  o The hardware safety requirements that describe the characteristics needed to *ensure the effectiveness* of the above safety mechanism
Specification of hardware safety requirements

This includes for instance the functional behaviour required for an ECU in case of an external failure, such as an open-circuit in the input of the ECU.

These attributes may be for instance timing and detection abilities of a watchdog.

This includes for instance the allocated time of reaction for the hardware part of a safety mechanism, so as to be consistent with the fault-tolerant time.
VIII – Product development: hardware level

Specification of hardware safety requirements

- Verification of the hardware safety requirements

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Walkthrough of hardware safety requirements</td>
<td>++</td>
</tr>
<tr>
<td>1b Inspection of hardware safety requirements</td>
<td>+</td>
</tr>
</tbody>
</table>

Part 5
**Hardware design**

The first objective of this clause is to design the hardware with respect to the system design specification and the hardware safety requirements.

The second objective of this clause is to verify the hardware design against the system design specification and the hardware safety requirements.
Hardware design

- In order to avoid common design faults, lessons learned, if applicable, shall be used.
- Non-functional causes for failure of a safety-related hardware part shall be considered during hardware detailed design, including the following influences, if applicable: temperature, vibrations, water, dust, EMI, noise factor, cross-talks originating either from other hardware parts of the hardware component or from its environment.
- The hardware detailed design shall ensure that hardware parts are used within their environmental and operational specifications.
**Hardware design**

*Safety analysis* of architectural design and hardware failures shall be conducted at appropriate levels: system or component, to identify new functional or non-functional hazards not already considered during hazard analysis and risk assessment and to identify the safety-related hardware elements.

For each safety-related hardware element the safety analysis shall identify:
- Safe faults
- Single point faults or residual faults
- Dual point faults (either perceived, detected or latent)
## Verification of hardware design

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Hardware design inspection(^a)</td>
<td>+</td>
</tr>
<tr>
<td>1b Hardware design walkthrough (^a)</td>
<td>++</td>
</tr>
<tr>
<td>2 Safety analyses</td>
<td></td>
</tr>
<tr>
<td>3a Emulation by simulation(^b)</td>
<td>o</td>
</tr>
<tr>
<td>3b Development by prototype hardware</td>
<td>o</td>
</tr>
</tbody>
</table>

\(^a\) Methods 1a and 1b serve as a check of the complete and correct implementation of the technical safety requirements in the hardware design.

\(^b\) Methods 3a and 3b serve as a check of particular points of hardware design for which analytical methods 1 and 2 are not considered sufficient. It can be used among other as a fault injection technique.
VIII – Product development: hardware level

Hardware architectural metric

Single Point

Failure with safety mechanism (included covered rate)

« Safety » failure

\[ \frac{\text{ASIL C : } N = 3\%}{+} \quad \frac{\text{ASIL D : } N = 1\%}{< N\%} \]
Assessment criteria for probability of violation of safety goals

The objective of the requirements in this clause is to make available criteria that can be used in a rationale that the residual risk of safety goal violation, due to random hardware failures of the item, is sufficiently low.

NOTE ‘Sufficiently low’ means “comparable to accepted risks on similar items already in use”.
Assessment criteria for probability of violation of safety goals

Two alternative methods:

- The first method consists of using a probabilistic metric to evaluate violation of the considered safety goal (using for instance quantified FTA) and compares the result of this quantification with a target value.

- The second method consists of the individual evaluation of each residual and single point fault and of each dual point failure leading to the violation of the considered safety goal. This analysis method can also be considered to be a cut-set analysis.

The scope of this clause is limited to the random hardware failures of the item. The parts considered in the analyses are the electrical and electronic parts. For electromechanical parts, only the electrical failure modes and failure rate are considered.
For first alternative method

- Table G.1 — Random hardware failure target values

<table>
<thead>
<tr>
<th>ASIL Level</th>
<th>Random hardware failure target values</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>$&lt; 10^{-8} , h^{-1}$</td>
</tr>
<tr>
<td>C</td>
<td>$&lt; 10^{-7} , h^{-1}$</td>
</tr>
<tr>
<td>B</td>
<td>$&lt; 10^{-7} , h^{-1}$</td>
</tr>
<tr>
<td>A</td>
<td>$&lt; 10^{-6} , h^{-1}$</td>
</tr>
</tbody>
</table>
Each **single point fault** is evaluated using criteria on occurrence of the fault. Each residual fault is evaluated using criteria combining occurrence of the fault and efficiency of the safety mechanism.
**VIII – Product development : hardware level**

**Assessment criteria for probability of violation of safety goals**

*Table 5 — Targets of failure rate class and coverage of hardware part regarding residual faults*

<table>
<thead>
<tr>
<th>ASIL of Safety Goal</th>
<th>Diagnostic Coverage wrt. residual faults</th>
<th>Failure rate class 3</th>
<th>Failure rate class 2</th>
<th>Failure rate class 1 + dedicated measuresa</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>&gt;= 99 %</td>
<td>++</td>
<td>++</td>
<td>+</td>
</tr>
<tr>
<td>C</td>
<td>&gt;= 90 %</td>
<td></td>
<td>++</td>
<td>+</td>
</tr>
<tr>
<td>B</td>
<td>&lt; 90 %</td>
<td></td>
<td></td>
<td>+</td>
</tr>
</tbody>
</table>

a The note in requirement 9.4.3.4 gives examples of dedicated measures
Each dual point failure is first evaluated regarding its plausibility. A dual point failure is considered not plausible if both faults leading to the failure are detected or perceived in a sufficiently short time with sufficient coverage. If the dual point failure is plausible, the faults causing it are then evaluated using criteria combining occurrence of the fault and coverage of the safety mechanisms.
VIII – Product development: hardware level

Assessment criteria for probability of violation of safety goals

Table 6 — Targets of failure rate class and coverage of hardware part regarding dual point faults

<table>
<thead>
<tr>
<th>ASIL of Safety Goal</th>
<th>Diagnostic Coverage wrt. latent multiple point faults</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&gt;= 99 %</td>
</tr>
<tr>
<td>D</td>
<td>o</td>
</tr>
<tr>
<td>C</td>
<td>o</td>
</tr>
</tbody>
</table>
Assessment criteria for probability of violation of safety goals

The failure rate class ranking for a hardware part failure rate shall be determined as follows:

- The failure rate corresponding to failure rate class 1 shall be less than the target for ASIL D divided by 100;
- The failure rate corresponding to failure rate class 2 shall be less than ten times the failure rate corresponding to failure rate class 1;
- The failure rate corresponding to failure rate class 3 shall be less than a hundred times the failure rate corresponding to failure rate class 1.
**VIII – Product development : hardware level**

**Evaluation of the diagnostic coverage**

**Generic hardware of an E/E system**

<table>
<thead>
<tr>
<th>Diagnostic technique/measure</th>
<th>See overview of techniques</th>
<th>Maximum diagnostic coverage considered achievable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure detection by on-line monitoring</td>
<td>D.2.1.1</td>
<td>Low</td>
<td>Depends on diagnostic coverage of failure detection</td>
</tr>
<tr>
<td>comparator</td>
<td>D.2.1.2</td>
<td>High</td>
<td>Depends on the quality of the comparison</td>
</tr>
<tr>
<td>Majority voter</td>
<td>D.2.1.3</td>
<td>High</td>
<td>Depends on the quality of the voting</td>
</tr>
<tr>
<td>Dynamic principles</td>
<td>D.2.2.1</td>
<td>Medium</td>
<td>Depends on diagnostic coverage of failure detection</td>
</tr>
<tr>
<td>Analogue signal monitoring in preference to digital on/off states</td>
<td>D.2.2.2</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Self-test by software cross exchange between two independent units</td>
<td>D.2.3.5</td>
<td>Medium</td>
<td>Depends of the quality of the self test</td>
</tr>
</tbody>
</table>
### VIII – Product development: hardware level

#### Hardware integration & testing

Objectives of this sub-phase are to ensure the compliance of the developed hardware with the hardware safety requirements

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a</td>
<td>Analysis of requirements</td>
</tr>
<tr>
<td>1b</td>
<td>Analysis of internal and external interfaces</td>
</tr>
<tr>
<td>1c</td>
<td>Generation and analysis of equivalence classes(a)</td>
</tr>
<tr>
<td>1d</td>
<td>Analysis of boundary values(b)</td>
</tr>
<tr>
<td>1e</td>
<td>Knowledge or experience based error guessing(c)</td>
</tr>
<tr>
<td>1f</td>
<td>Analysis of functional dependencies</td>
</tr>
<tr>
<td>1g</td>
<td>Analysis of common limit conditions, sequences and sources of common cause</td>
</tr>
<tr>
<td>1h</td>
<td>Analysis of environmental conditions and operational use cases</td>
</tr>
<tr>
<td>1i</td>
<td>Standards if existing(d)</td>
</tr>
<tr>
<td>1j</td>
<td>Analysis of significant variants(e)</td>
</tr>
</tbody>
</table>

---

**a** In order to efficiently derive the necessary test cases, analysis of similarities can be conducted.

**b** EXAMPLE values approaching and crossing the boundaries between specified values and out of range values

**c** “Error guessing tests” should be based on data collected through lesson learned process, or expert judgment, or both. It can be supported by FMEA for example.

**d** Existing standards can be ISO 16750 and ISO 11452.

**e** The analysis of significant variants includes worst case analysis.
# IX – Product development: software level

## 1. Vocabulary

| 2-5 Overall safety management | 2-6 Safety management during item development | 2-7 Safety management after release for production |

## 3. Concept phase

<table>
<thead>
<tr>
<th>3-5 Item definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-6 Initiation of the safety lifecycle</td>
</tr>
<tr>
<td>3-7 Hazard analysis and risk assessment</td>
</tr>
<tr>
<td>3-8 Functional safety concept</td>
</tr>
</tbody>
</table>

## 4. Product development: system level

| 4-5 Initiation of product development at the system level |
| 4-6 Specification of the technical safety requirements |
| 4-7 System design |
| 4-8 Item integration and testing |

## 5. Product development: hardware level

| 5-5 Initiation 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

| 6-5 Initiation 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 |

## 8. Supporting processes

| 8-5 Interfaces within 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 |
| 8-11 Qualification of software components |
| 8-13 Qualification of hardware components |
| 8-14 Proven in use argument |

## 9. ASIL-oriented and safety-oriented analyses

| 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 analyses |

## 10. Guideline on ISO 26262 (informative)

Introduction à la norme ISO 26262

MAJ 07/03/2010

107/134
IX – Product development: software level

Objectives

- The objective of this part is:
  - to provide a consistent software requirement specifications
  - to design & analyse the software
  - to evaluate the software architecture of the item
  - to check the integration and testing
IX – Product development: software level

Initiation of product development
IX – Product development : software level

Specification of software safety requirements

The technical safety requirements are divided into hardware and software safety requirements. The specification of the software safety requirements considers constraints of the hardware and the impact of these constraints on the software.

- The software safety requirements shall address each software-based function whose failure could lead to a violation of a technical safety requirement allocated to software.
- The persons responsible for the hardware and software development shall jointly verify the refined hardware software interface specification.

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Informal verification by walkthrough</td>
<td>+</td>
</tr>
<tr>
<td>1b Informal verification by inspection</td>
<td>+</td>
</tr>
<tr>
<td>1c Semi-formal verification</td>
<td>+</td>
</tr>
<tr>
<td>1d Formal verification</td>
<td>o</td>
</tr>
</tbody>
</table>

a Method 1c can be supported by executable models.
Software architectural design

The software architectural design shall exhibit the following properties by use of the principles listed in Table 4:

- modularity;
- encapsulation and;
- minimum complexity.

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a</td>
<td>++</td>
</tr>
<tr>
<td>1b</td>
<td>++</td>
</tr>
<tr>
<td>1c</td>
<td>+</td>
</tr>
<tr>
<td>1d</td>
<td>+</td>
</tr>
<tr>
<td>1e</td>
<td>+</td>
</tr>
<tr>
<td>1f</td>
<td>++</td>
</tr>
<tr>
<td>1g</td>
<td>+</td>
</tr>
</tbody>
</table>

Table 4 — Principles for software architectural design

a In methods 1b, 1c, 1e and 1g "restricted" means to minimise in balance with other design considerations.
b Methods 1d and 1e can, for example, be achieved by separation of concerns which refers to the ability to identify, encapsulate, and manipulate those parts of software that are relevant to a particular concept, goal, task, or purpose.
c Method 1e addresses the limitation of the external coupling of software components.
d Any interrupts used have to be priority-based.
### IX – Product development: software level

Software integration and testing

Table 15 — Methods for software integration testing

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Requirements-based test</td>
<td>++</td>
</tr>
<tr>
<td>1b External interface test</td>
<td>++</td>
</tr>
<tr>
<td>1c Fault injection testa</td>
<td>+</td>
</tr>
<tr>
<td>1d Resource usage testb, c</td>
<td>+</td>
</tr>
<tr>
<td>1e Back-to-back test between model and code, if applicable</td>
<td>+</td>
</tr>
</tbody>
</table>

a This includes injection of arbitrary faults in order to test safety mechanisms (e.g. by corrupting software or hardware components)

b To ensure the fulfillment of requirements influenced by the hardware architectural design with sufficient tolerance, properties such as average and maximum processor performance, minimum or maximum execution times, storage usage (e.g. RAM for stack and heap, ROM for program and data) and the bandwidth of communication links (e.g. data busses) have to be determined.

c Some aspects of the resource usage test can only be evaluated properly when the software integration tests are executed on the target hardware or if the emulator for the target processor supports resource usage tests.

d This method requires a model that can simulate the functionality of the software components. Here, the model and code are stimulated in the same way and results compared with each other.
Objectives

- The first objective of the requirements in this Clause is to develop a production plan for safety-related products.

- The second objective is to ensure that the required functional safety is achieved during the production process by the relevant product manufacturer or the person or organisation in charge of the process (vehicle manufacturer, supplier, sub-supplier etc.).
Information required

- Production planning
- Control plan (the tests description and criteria for safety-related systems, focus on the systematic faults…)
- Process failures and their potential effects on functional safety shall be analysed and the appropriate measures shall be implemented
- The lessons on the capability, learnt from previously released production plans
- Tools and test equipment concerning the safety-related special characteristics
- The competence of the personnel
The processes concerning operation, repair and maintenance shall be planned.
The *user manual* shall include relevant usage instructions and warnings concerning the item.
The requirements regarding the decommissioning activities shall be developed.
XI – Supporting processes

1. Vocabulary

2. Management of functional safety

3. Concept phase

4. Product development: system level

5. Product development: hardware level

6. Product development: software level

8. Supporting processes

9. ASIL-oriented and safety-oriented analyses

10. Guideline on ISO 26262 (Informative)
**Objective**

The objective of this process is to describe the procedures and allocate associated responsibilities within distributed developments for items and elements.

- 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
XI – Supporting processes

Interfaces within distributed developments

- Supplier selection criteria:
  - Verification of the supplier's quality management system
  - Consideration of the supplier's experience in developing products of comparable complexity and ASIL
  - The supplier's capability in developing products of comparable complexity

- The customer and the supplier shall specify a Development Interface Agreement (DIA)
XI – Supporting processes

**Specification and management of safety requirements**

The first objective is to ensure the correct specification of safety requirements with respect to attributes and characteristics. The second objective is to ensure consistent management of safety requirements throughout the entire safety lifecycle.

Safety requirements constitute all requirements aimed at achieving and ensuring the required degree of functional safety.

During the safety lifecycle, safety requirements are specified and detailed in a hierarchical structure. The structure and dependencies of safety requirements as used in this International Standard are illustrated hereinafter.

In order to support the management of safety requirements, the use of suitable tools for requirements management is recommended.
XI – Supporting processes

Overall management of safety requirements

Structuring of safety requirements
Configuration management

- Configuration management is a well established practice within the automotive industry and is usually applied according to ISO TS 16949, 4.2.3, ISO 10007:2003.
- Each work product of ISO 26262 is managed by configuration management.
- Configuration management shall be maintained throughout the entire safety lifecycle.
Change management

The objective of change management is the analysis and management of changes to safety-related work products occurring throughout the safety lifecycle.

- The change management process shall be planned and initiated, before changes are made to work products.
- A unique identifier shall be assigned for each change request.
- An *impact analysis* on the existing system and its interfaces and connected systems shall be carried out for each change request.
**Verification**

- The first objective of verification is to ensure that the work products are correct, complete and consistent.
- The second objective of verification is to ensure that the work products meet the requirements of ISO 26262.

- The planning of verification shall be carried out for each phase and subphase of the safety lifecycle.
- The specification of verification shall specify and select the methods to be used for the verification.
XI – Supporting processes

**Documentation**

The objective of the documentation is to develop a documentation management strategy, so that every phase of the entire safety lifecycle can be worked through effectively and can be reproduced.

- The documents shall be:
  - precise and concise;
  - structured in a clear manner;
  - easy to understand by their intended audience; and
  - maintainable.
XI – Supporting processes

Qualification of software tools

The objective of the qualification of software tools is to provide evidence of software tool suitability for use when developing a safety-related item or element, such that confidence can be achieved in the correct execution of activities and tasks required by ISO 26262.

The relevant software tool use-cases shall be analysed and evaluated to determine:

- the possibility that a safety requirement, allocated to the safety-related item or element is violated if the software tool is malfunctioning or producing erroneous output, is expressed by the classes of classes of **TI** (Tool Impact)
- the probability of preventing or detecting that the software tool is malfunctioning or producing erroneous output is expressed by the classes of **TD** (Tool error Detection)
XI – Supporting processes

Qualification of software tools

Based on the values determined to the classes of TI and TD the required software tool confidence level shall be determined according to the following list:

• TCL1 shall be selected for TI0;
• TCL1 shall be selected for TI1 and TD1;
• TCL2 shall be selected for TI1 and TD2;
• TCL3 shall be selected for TI1 and TD3; and
• TCL4 shall be selected in all other cases

TCL is an abbreviation for “Tool Confidence Level”, with TCL 4 being the highest level of confidence required and TCL1 being the lowest level of confidence required

Table 2 — Qualification of software tools classified TCL4

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Increased confidence from use</td>
<td>++</td>
</tr>
<tr>
<td>1b Evaluation of the development process</td>
<td>++</td>
</tr>
<tr>
<td>1c Validation of the software tool</td>
<td>+</td>
</tr>
<tr>
<td>1d Development in compliance with a safety standard*</td>
<td>+</td>
</tr>
</tbody>
</table>

* No safety standard is fully applicable to the development of software tools. Instead, a relevant subset of requirements of the safety standard can be selected.
XI – Supporting processes

**Qualification of software components**

- First objective: 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.
- Second objective: to show their suitability for re-use.

The qualification of a software component shall be documented including the following information:

- unique identification and configuration of the software component;
- person or organisation who carried out the qualification;
- the environment used for qualification;
- results of the verification measures applied to qualify the software component; and
- the pre-determined maximum target ASIL of any safety requirement which might be violated if the software component performs incorrectly.
XI – Supporting processes

Qualification of hardware components

- First objective: 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.
- Second objective: to provide relevant information regarding their failure modes and their distribution, and their diagnostic capability with regard to the safety concept for the item.
## Qualification of hardware components

### Table 5 — Qualification, integration and test activities to be conducted depending on the level of HW part or component

<table>
<thead>
<tr>
<th></th>
<th>Basic HW part</th>
<th>Intermediate HW part</th>
<th>Intermediate HW component</th>
<th>Complex HW component</th>
</tr>
</thead>
<tbody>
<tr>
<td>No contribution to a safety requirement</td>
<td>No contribution to a safety requirement</td>
<td>No contribution to a safety requirement</td>
<td>A safety requirement is fully implemented by the HW component</td>
<td></td>
</tr>
<tr>
<td>(resistors, transistors…)</td>
<td>(HS CAN transceiver)</td>
<td>(gray code decoder)</td>
<td>(fuel pressure sensor)</td>
<td>(ECU)</td>
</tr>
<tr>
<td>Standard qualification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qualification in accordance with ISO26262-8:—, Clause 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration/test in accordance with ISO26262-5:—</td>
<td></td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration/test in accordance with ISO26262-4:—</td>
<td></td>
<td></td>
<td>*</td>
<td></td>
</tr>
</tbody>
</table>

* means that the HW element will be integrated in accordance with ISO 26262-4:—, or ISO 26262-5:—, or both ISO 26262-5:— and ISO 26262-4:— depending on "its level".
XI – Supporting processes

Proven in use argument

The objective of this clause is to provide guidance for proven in use argument. Proven in use argument is an alternate means of compliance with ISO 26262 requirements that may be used in case of reuse of existing items or elements when field data is available.

**Targets for demonstration of compliance with safety goal**

<table>
<thead>
<tr>
<th>ASIL</th>
<th>Observable incident rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>&lt; 10^-9/h</td>
</tr>
<tr>
<td>C</td>
<td>&lt; 10^-8/h</td>
</tr>
<tr>
<td>B</td>
<td>&lt; 10^-8/h</td>
</tr>
<tr>
<td>A</td>
<td>&lt; 10^-7/h</td>
</tr>
</tbody>
</table>

**Targets for minimum service period of candidate**

<table>
<thead>
<tr>
<th>ASIL</th>
<th>Minimum service period without observable incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>1.2 · 10^9 h</td>
</tr>
<tr>
<td>C</td>
<td>1.2 · 10^8 h</td>
</tr>
<tr>
<td>B</td>
<td>1.2 · 10^8 h</td>
</tr>
<tr>
<td>A</td>
<td>1.2 · 10^7 h</td>
</tr>
</tbody>
</table>
Proven in use argument

For the application of the proven in use credit to be anticipated, before a proven in use status is obtained, the candidate service period shall demonstrate compliance with the safety goal according to Table 8 with a single sided lower confidence level of 70%.

Table 8 — Limits for observable incident rate (interim period)

<table>
<thead>
<tr>
<th>ASIL</th>
<th>Observable incident rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>&lt; 3 \times 10^{-9}/h</td>
</tr>
<tr>
<td>C</td>
<td>&lt; 3 \times 10^{-8}/h</td>
</tr>
<tr>
<td>B</td>
<td>&lt; 3 \times 10^{-8}/h</td>
</tr>
<tr>
<td>A</td>
<td>&lt; 3 \times 10^{-7}/h</td>
</tr>
</tbody>
</table>
**XI – ASIL oriented and safety analysis**

**Criteria for coexistence of element**

**General**

By default, when an element is composed of several sub-elements, each of those sub-elements is developed in accordance with the measures corresponding to the highest ASIL applicable to this 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.
Introduction à la norme ISO 26262

MAJ 07/03/2010

Description de système ou fonction et ses limites

Système
Définition

Hazard Analysis and Risk Classification

Sécurité des processus
Par exemple : Planification, Qualification, Définition de Responsabilités,

Supporting Processes
Par exemple : Gestion de la configuration, Études de cas, Documentation,

Sécurité des processus
Par exemple : Planification, Qualification, Définition de Responsabilités,

Sécurité des processus
Par exemple : Planification, Qualification, Définition de Responsabilités,

Sécurité des processus
Par exemple : Planification, Qualification, Définition de Responsabilités,

Sécurité des processus
Par exemple : Planification, Qualification, Définition de Responsabilités,

Sécurité des processus
Par exemple : Planification, Qualification, Définition de Responsabilités,

Sécurité des processus
Par exemple : Planification, Qualification, Définition de Responsabilités,