

**National Academy of Sciences  
Briefing on ISO 26262**



**Joe Miller  
November 16, 2010**



# Contents



- 1) What are the basic features of the ISO standard and how will functional safety be certified?**
- 2) How does the ISO functional safety standard apply the principles of IEC 61508 to automotive electronics? Are there any major differences?**
- 3) How will the ISO standard impact the way electronic systems in autos will be developed in the future?**
- 4) How will lifecycle aspects of functional safety be treated given the new standard?**
- 5) Do you expect that all car manufacturers will apply this standard?**

# What are the basic features of the ISO standard and how will functional safety be certified?

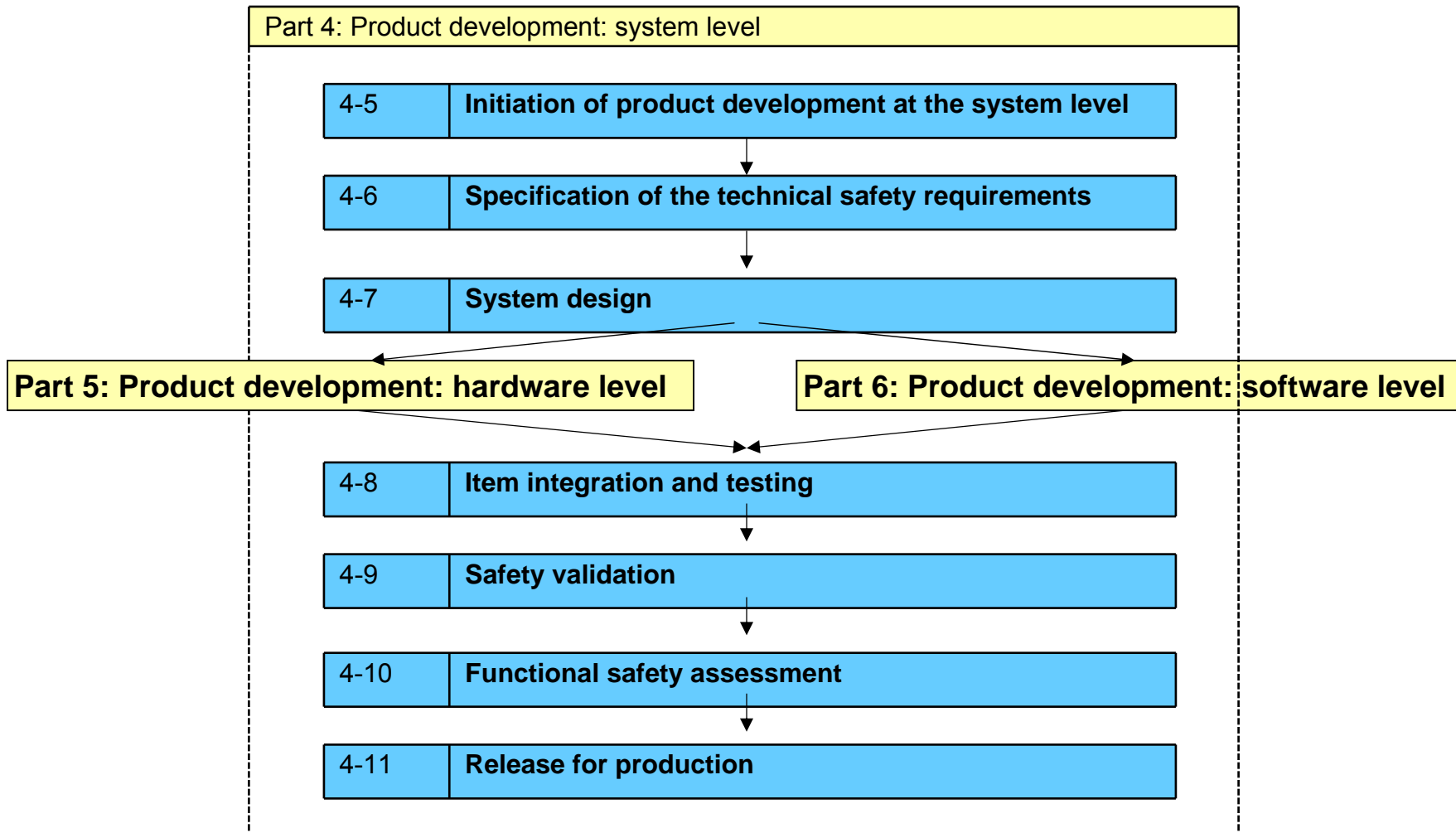


- 1) **Safety Goals and concepts; includes ASIL.**
- 2) **Product Development at the System level.**
  - 1) **Hardware Development.**
  - 2) **Software development.**
- 4) **production and operations**
- 5) **Not Certified**
  - 1) **Confirmation Review**
  - 2) **Audit**
  - 3) **Functional Safety Assessment**
  - 4) **Required Independence**

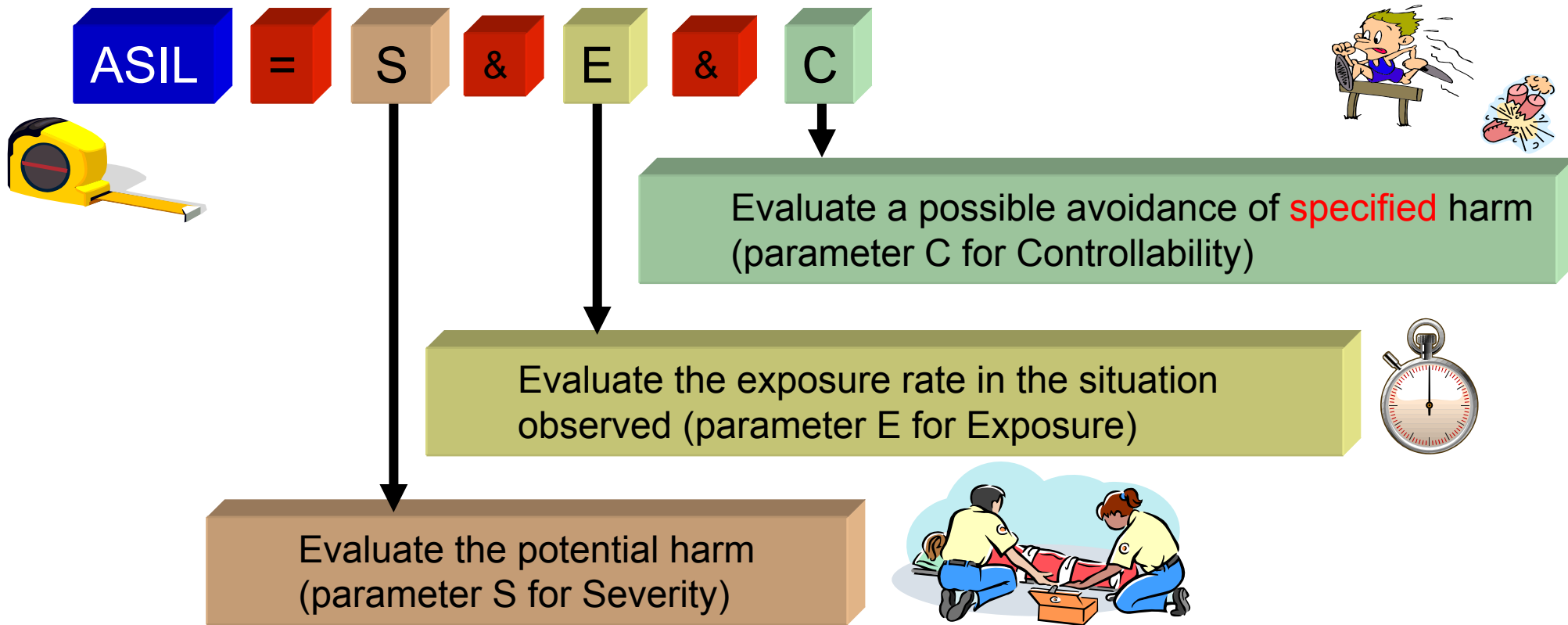
# Safety Goals and Concepts



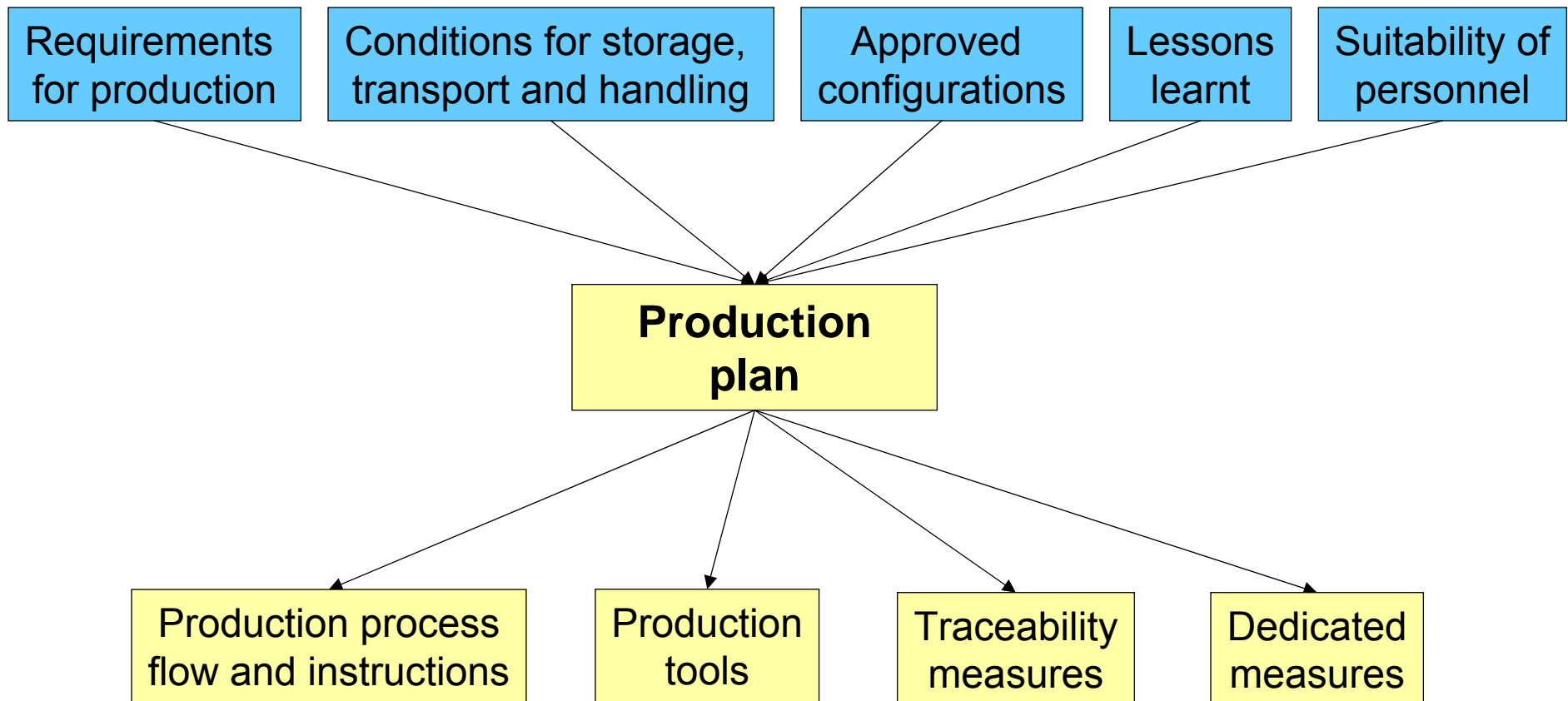
# Product Development at the System level



- Deduce the required ASIL  
(ASIL for Automotive Safety Integrity Level)



- Evaluate item:



# Production and Operations

- Assure conformance of Production Plan to ISO 26262
  - Production process flow
  - Production tools
  - Implementation of traceability measures
- Ensure that required functional safety is achieved during the production process
- Include to plan the safety-related special characteristics,
  - e.g. temperature range for specific processes, material characteristics, expiration date, fastening torque, production tolerance, and configuration
- Planning of operation, service (maintenance and repair), and decommissioning
- Field monitoring process
- Activities addressing safety issues before disassembly



# Confirmation Measures (Property Comparison)

Confirmation activity	Confirmation review	Functional safety audit	Functional safety assessment
Result	<i>Confirmation review report<sup>a</sup></i>	<i>Functional safety audit report<sup>a</sup></i>	<i>Functional safety assessment report</i>
Subject for evaluation	Work product	Implementation of the processes required for functional safety.	Item as described in the “Item definition” (see ISO°26262-3, Clause°5).
Responsibility of the persons that perform the confirmation measure	Evaluation of the compliance of the work product with the corresponding requirements of ISO 26262.	Evaluation of the implementation of the required processes.	Evaluation of the achieved functional safety. Provision of a recommendation for acceptance, a conditional acceptance or a rejection.
Timing during lifecycle	After completion of the corresponding safety activity. Completion before the release for production.	During the implementation of the required processes.	Progressively during development, or in a single block. Completion before the release for production.
Scope and depth	Planned prior to the review, in accordance with the safety plan.	Implementation of the processes against the definitions of the activities referenced or specified in the safety plan.	The work products required per the safety plan, the implementation of the required processes and a review of the implemented safety measures that can be assessed during the item development.

<sup>a</sup> can be included in functional safety assessment report

# Required confirmation measures

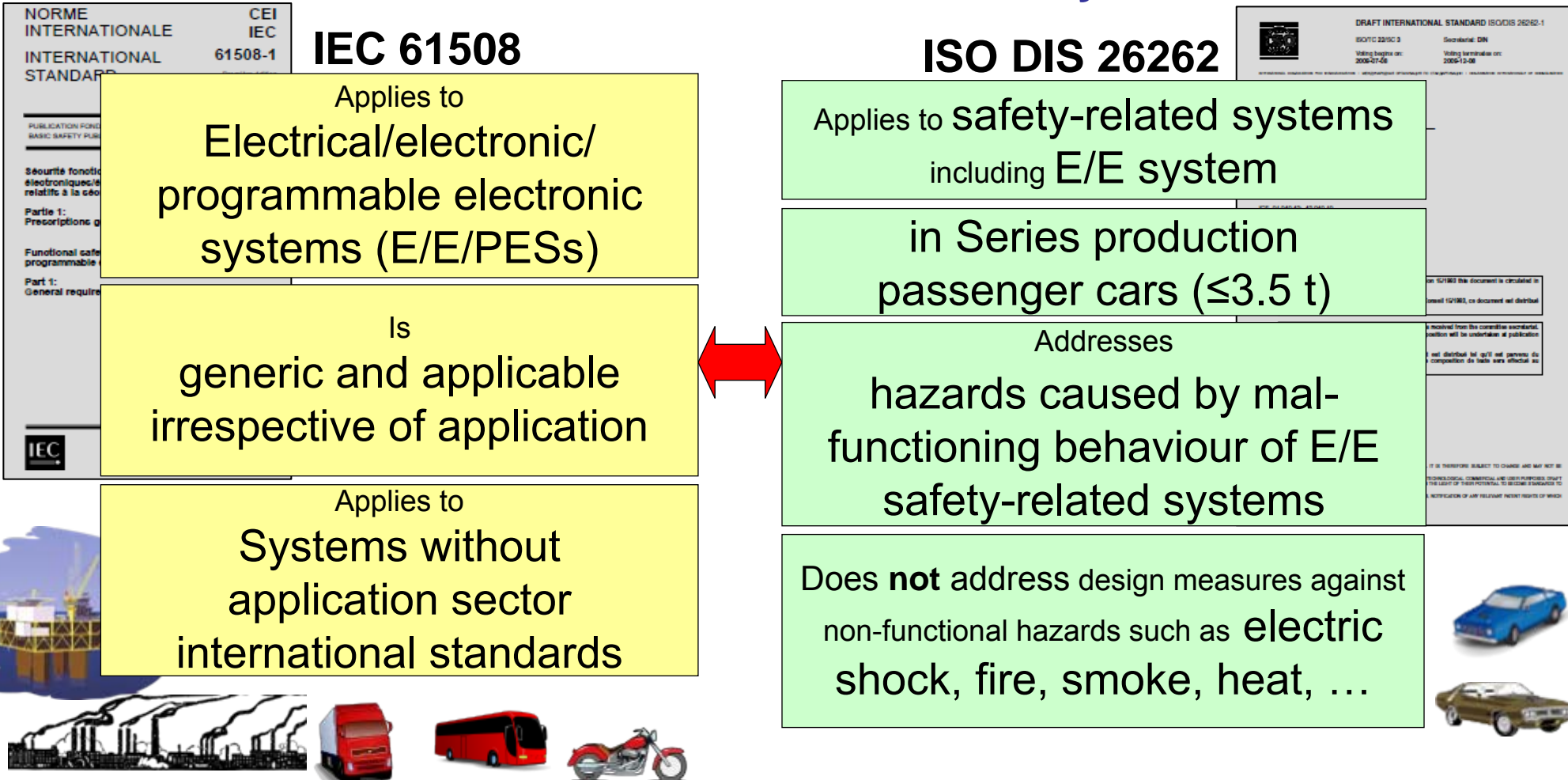
- -: no requirement regarding this confirmation measure;
- I0: the confirmation measure should be performed;
- I1: the confirmation measure shall be performed;
- I2: the confirmation measure shall be performed, by a person from a different team, i.e. not reporting to the same direct superior; and
- I3: the confirmation measure shall be performed, by a person from a different department or organization, i.e. independent from the relevant department, regarding management, resources, and responsibility for release for production.

Confirmation measure	A	B	C	D	
Confirmation review of safety plan (see Clause 6) - independent from the developers of the item / project management	-	I1	I2	I3	highest ASIL among safety goals of the item
Confirmation review of integration and testing plan (see ISO°26262-4, Clause 5) -independent from the developers of the item / project management	I0	I1	I2	I2	highest ASIL among safety goals of the item
Confirmation review of validation plan (see ISO°26262-4, Clause 5) -independent from the developers of the item / project management	I0	I1	I2	I2	highest ASIL among safety goals of the item
...	...	...	...	...	...

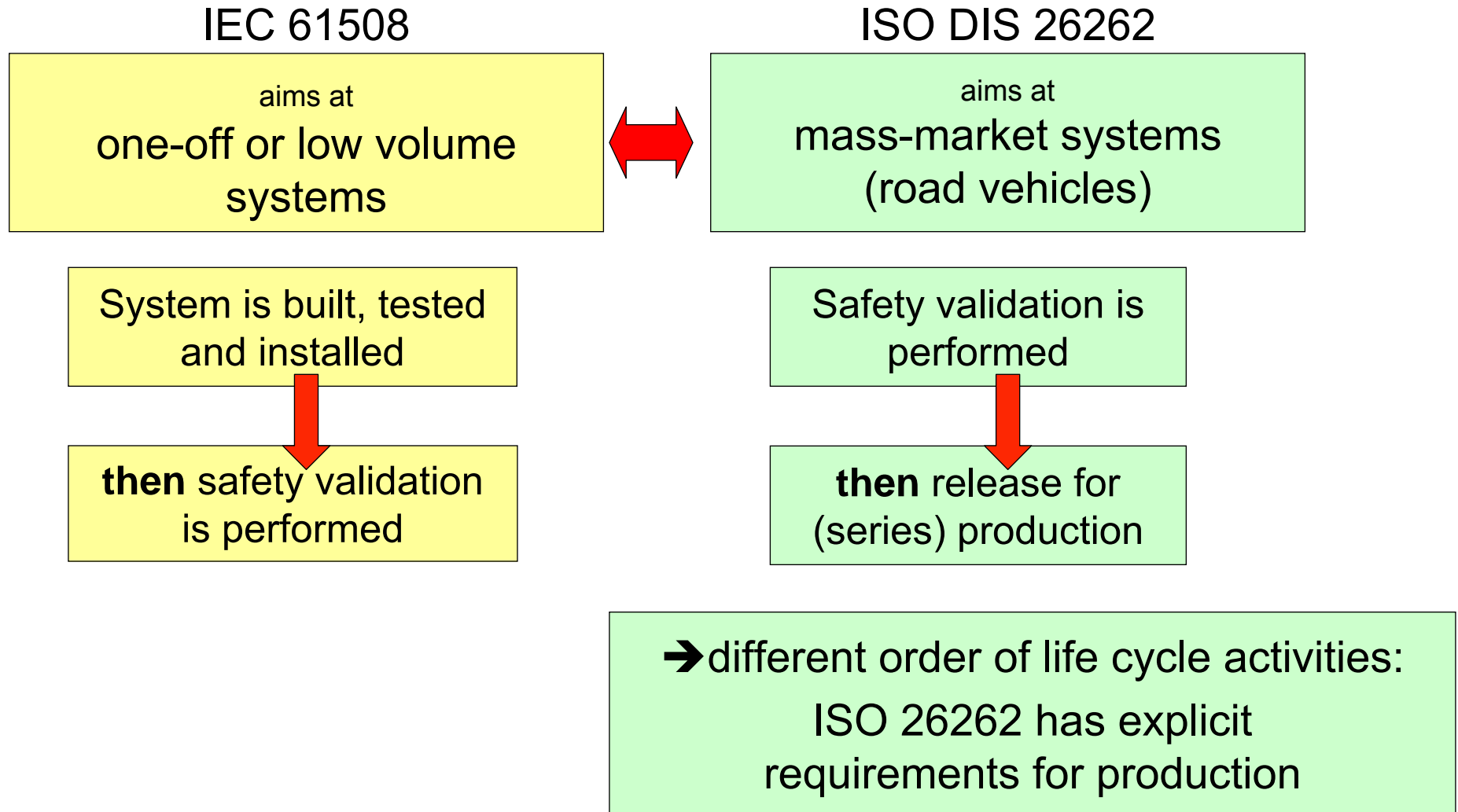
- 1) What are the basic features of the ISO standard and how will functional safety be certified?
- 2) ***How does the ISO functional safety standard apply the principles of IEC 61508 to automotive electronics? Are there any major differences?***
- 3) How will the ISO standard impact the way electronic systems in autos will be developed in the future?
- 4) How will lifecycle aspects of functional safety be treated given the new standard?
- 5) Do you expect that all car manufacturers will apply this standard?

# Aim and Scope of ISO 26262 vs. IEC61508

- ISO 26262: developed by automotive industry on basis of IEC 61508 to avoid risks in relation with use of E/E Systems



# Major differences - Aims



# Major differences - Structure and content

## IEC 61508

Normative:

- Part 1: General requirements
- Part 2: Requirements for E/E/PES systems
- Part 3: Software requirements
- Part 4: Definition and abbreviations

Informative:

- Part 5: Examples of methods for the determination of SILs
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

## ISO DIS 26262

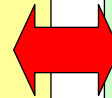
Part 1: Vocabulary

Normative:

- Part 2: Management of functional safety
- Part 3: Concept phase
- Part 4: Product dev.: system level
- Part 5: Product dev.: hardware level
- Part 6: Product dev.: software level
- Part 7: Production and operation
- Part 8: Supporting processes
- Part 9: ASIL-oriented and safety-oriented analyses

Informative:

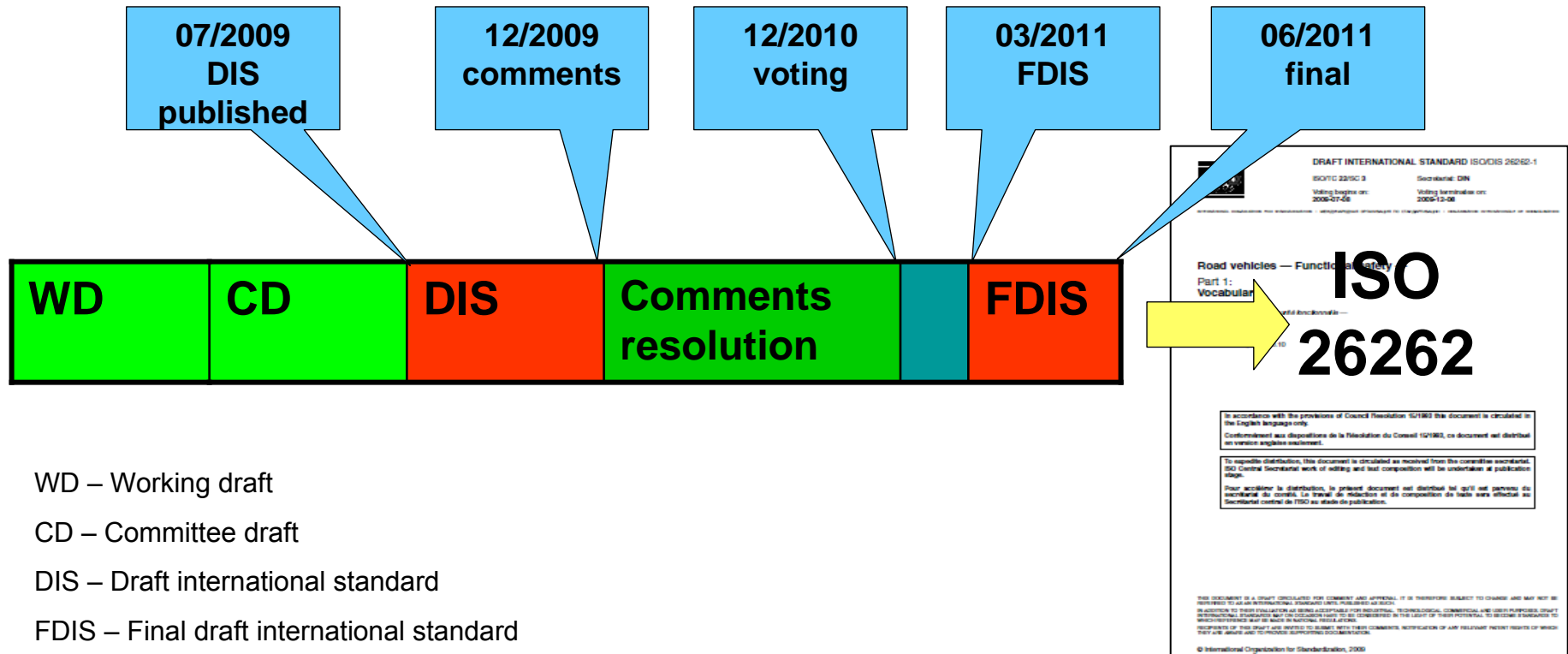
- Part 10: Guideline on ISO 26262



- 1) What are the basic features of the ISO standard and how will functional safety be certified?
- 2) How does the ISO functional safety standard apply the principles of IEC 61508 to automotive electronics? Are there any major differences?
- 3) ***How will the ISO standard impact the way electronic systems in autos will be developed in the future?***
- 4) How will lifecycle aspects of functional safety be treated given the new standard?
- 5) Do you expect that all car manufacturers will apply this standard?

# ISO 26262 - Roadmap

## ■ Estimated roadmap for release



WD – Working draft

CD – Committee draft

DIS – Draft international standard

FDIS – Final draft international standard

# Major differences - Work Products

IEC 61508

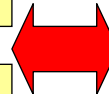
ISO DIS 26262

Specifies  
Requirements

Specifies  
Requirements

Only indirectly  
(Work products)

Specifies  
Work products (>100\*)



(\*tailoring by combine / split)

## Create, foster and sustain a Safety Culture

Establish and maintain  
Organisation specific rules and  
processes

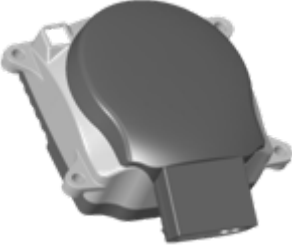

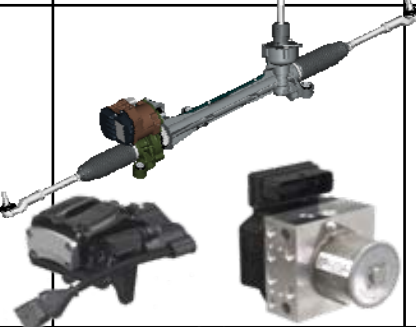
Deal with  
functional safety anomalies

- Communicate to safety manager
- Analysis
- Evaluation

Ensure  
Documentation

Ensure  
Continuous improvement process

# Major differences – ASIL per ISO 26262

ASIL	Example		Sample Ranking	Sample requirement: Diagnostic coverage / process reqt.	Highly recommended reqs. in tables of part 4, 5, 6
A	<b>Cruise control</b> , failure to decelerate		S1, C2, E4	none / <u>some</u>	~ 50
	<b>Follow to Stop</b> deceleration outside design limits		S1, C3, E4	90% single point, 60% latent / <u>more</u>	~ 80
C	<b>Passenger Airbag</b> wrong deployment		S2, C3, E4	97% single point, 80% latent / <u>even more</u>	~ 130
D	<b>Electric Steering</b> , Wrong assist		S3, C3, E4	99% single point, 90% latent / <u>most</u>	~ 150
	<b>EPB</b> , lock rear wheels <b>SCS</b> , wrong intervention				

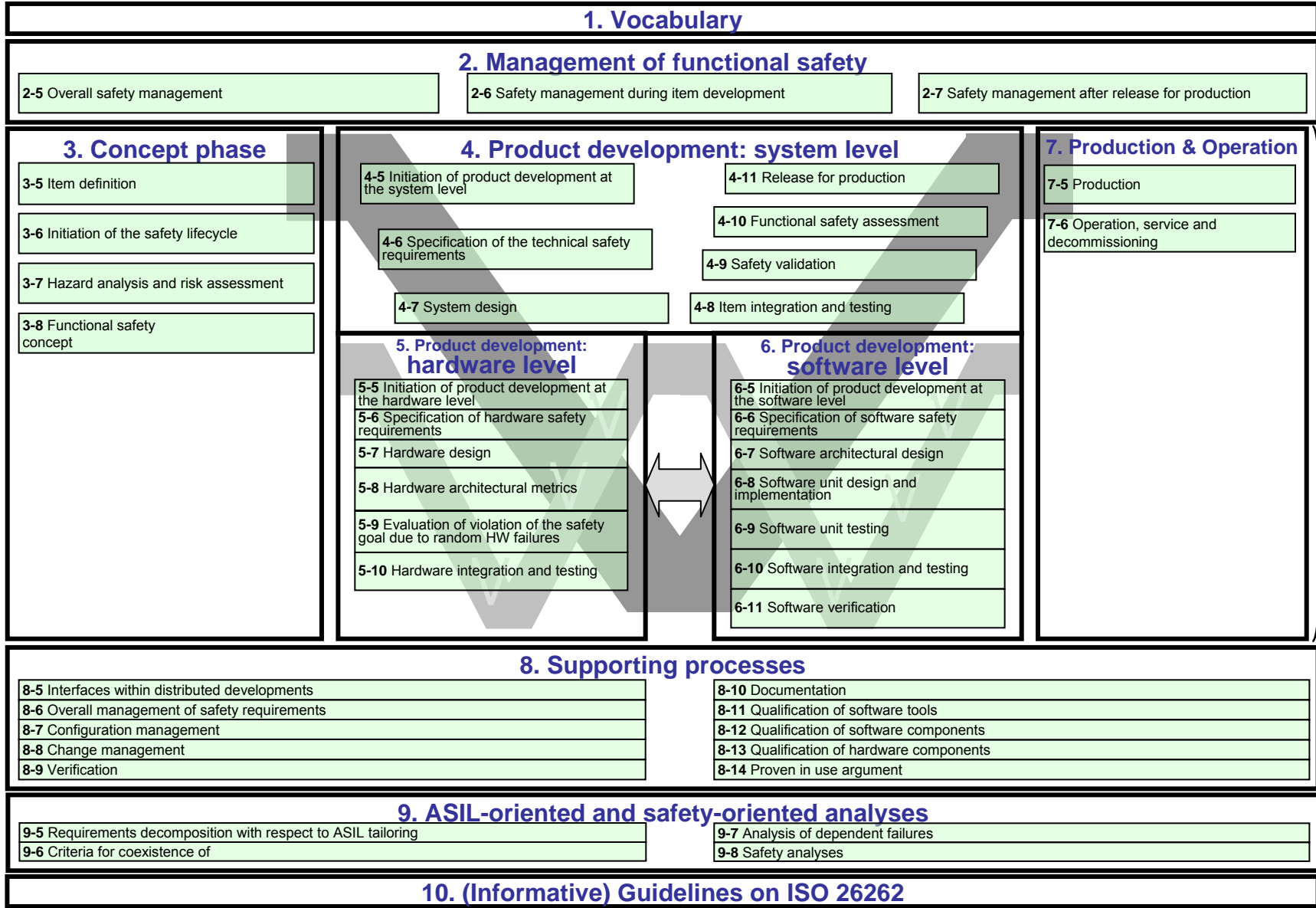
**Higher ASIL increases effort**

- 1) What are the basic features of the ISO standard and how will functional safety be certified?
- 2) How does the ISO functional safety standard apply the principles of IEC 61508 to automotive electronics? Are there any major differences?
- 3) How will the ISO standard impact the way electronic systems in autos will be developed in the future?
- 4) ***How will lifecycle aspects of functional safety be treated given the new standard?***
- 5) Do you expect that all car manufacturers will apply this standard?

# General structure ISO 26262



ISO 26262 affects all areas



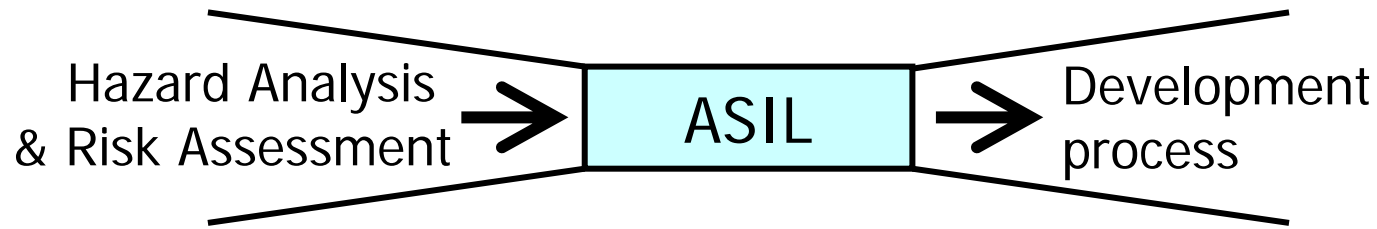
Management

Core processes

Support

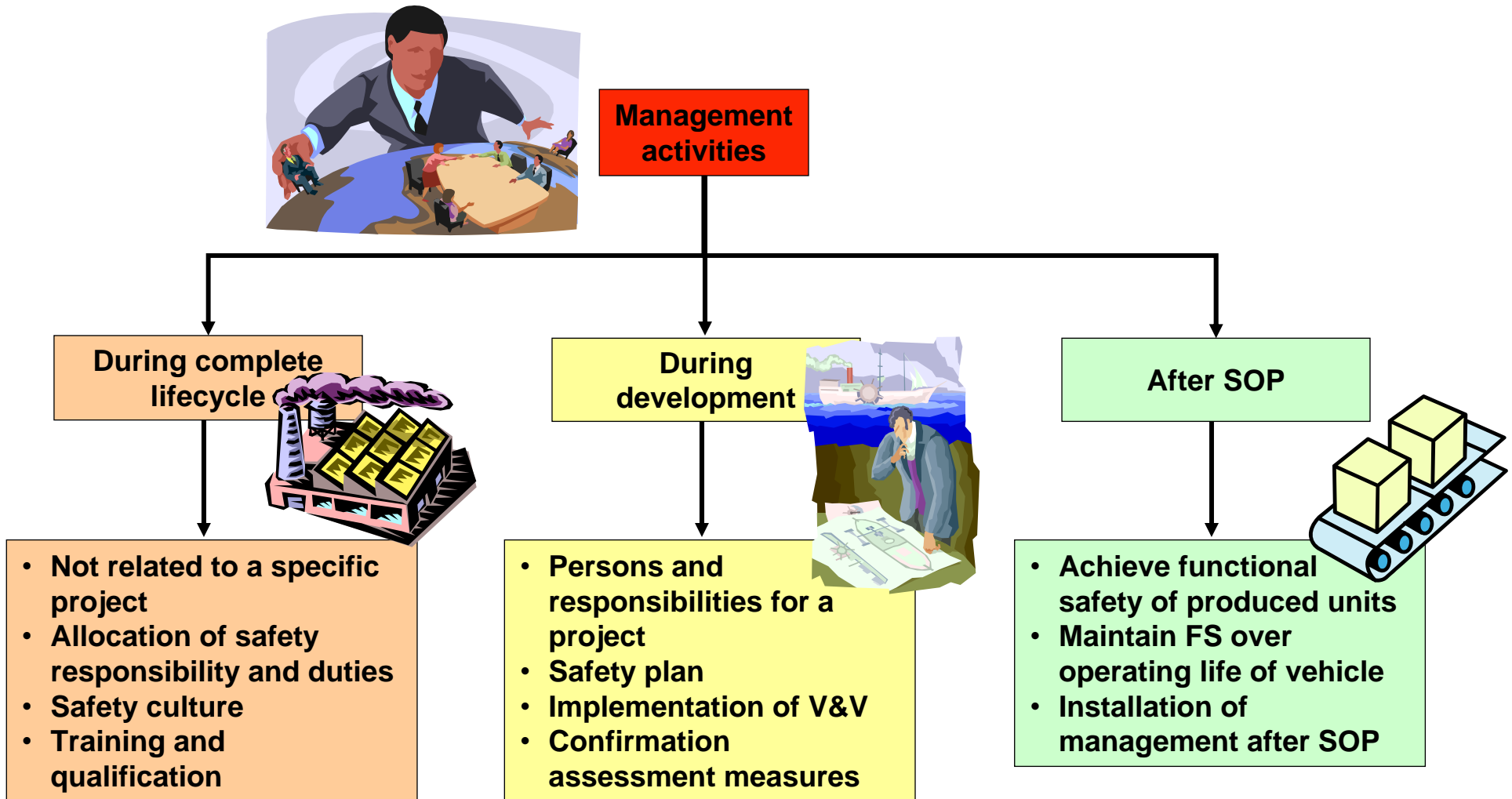
# Requirements-oriented safety approach

Dealing with hazards in an appropriate way



- Result of Hazard Analysis and Risk Assessment:
  - Identification of the need for (and amount of) requirements regarding functional safety: Safety Goals and Automotive Safety Integrity Level (ASIL)
- Demonstrate (ASIL-adjusted) compliance with safety requirements by measures taken in
  - procedures,
  - architecture,
  - design, ...

# Safety Management for all phases



- 1) What are the basic features of the ISO standard and how will functional safety be certified?
- 2) How does the ISO functional safety standard apply the principles of IEC 61508 to automotive electronics? Are there any major differences?
- 3) How will the ISO standard impact the way electronic systems in autos will be developed in the future?
- 4) How will lifecycle aspects of functional safety be treated given the new standard?
- 5) *Do you expect that all car manufacturers will apply this standard?*

# Opinion concerning Application of ISO 26262



- 1) Vehicle manufacturer's (VMs) and suppliers have participated in the development of ISO 26262 from Europe, Japan, and the US for about 5 years**
- 2) There have been tutorials and papers on its application including examples**
- 3) It can be expected that a tailored application of the standard will continue to expand rapidly, particularly with respect to new developments and modification of products already in production.**
- 4) It can be expected that there will be joint developments with VMs and suppliers as prescribed in the standard**
- 5) In addition, suppliers will develop Safety Elements out of Context (SEooC). This will reduce the burden to VMs when the assumptions of the SEooC are met**