Requirements Engineering and Management with ISO 26262 and Automotive SPICE

October 25, 2012
Milan
10th Workshop on Automotive Software & Systems

Fabio Bella
Kugler Maag Cie

KUGLER MAAG CIE
besser mit uns

Agenda

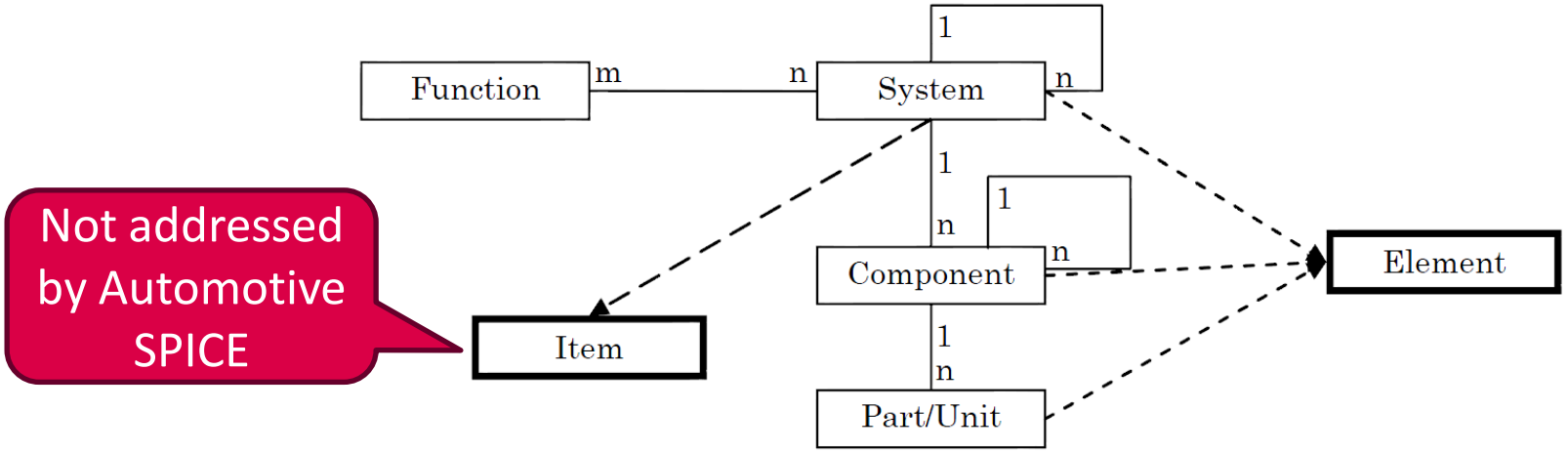
- Introduction
- Requirements engineering according to Automotive SPICE
- Requirements engineering according to ISO 26262
- Mapping of requirements-related work products of ISO 26262 and A-SPICE
- Requirements engineering and management with ISO 26262 and A-SPICE
- Conclusions

Introduction (1/2)

Situation with respect to regulation of requirements-related activities in the Automotive sector

- ISO 26262 regulates areas that are already partially addressed by Automotive SPICE
- In the case of requirements management and engineering, extensive overlaps but also great differences between the two standards exist
- In general, many companies have already structured their requirements-related processes to cope with expectations of Automotive SPICE
- **What has to be considered when implementing ISO 26262 expectations with respect to requirements management and engineering in a context, which is already aligned to Automotive SPICE?**

Introduction (2/2)



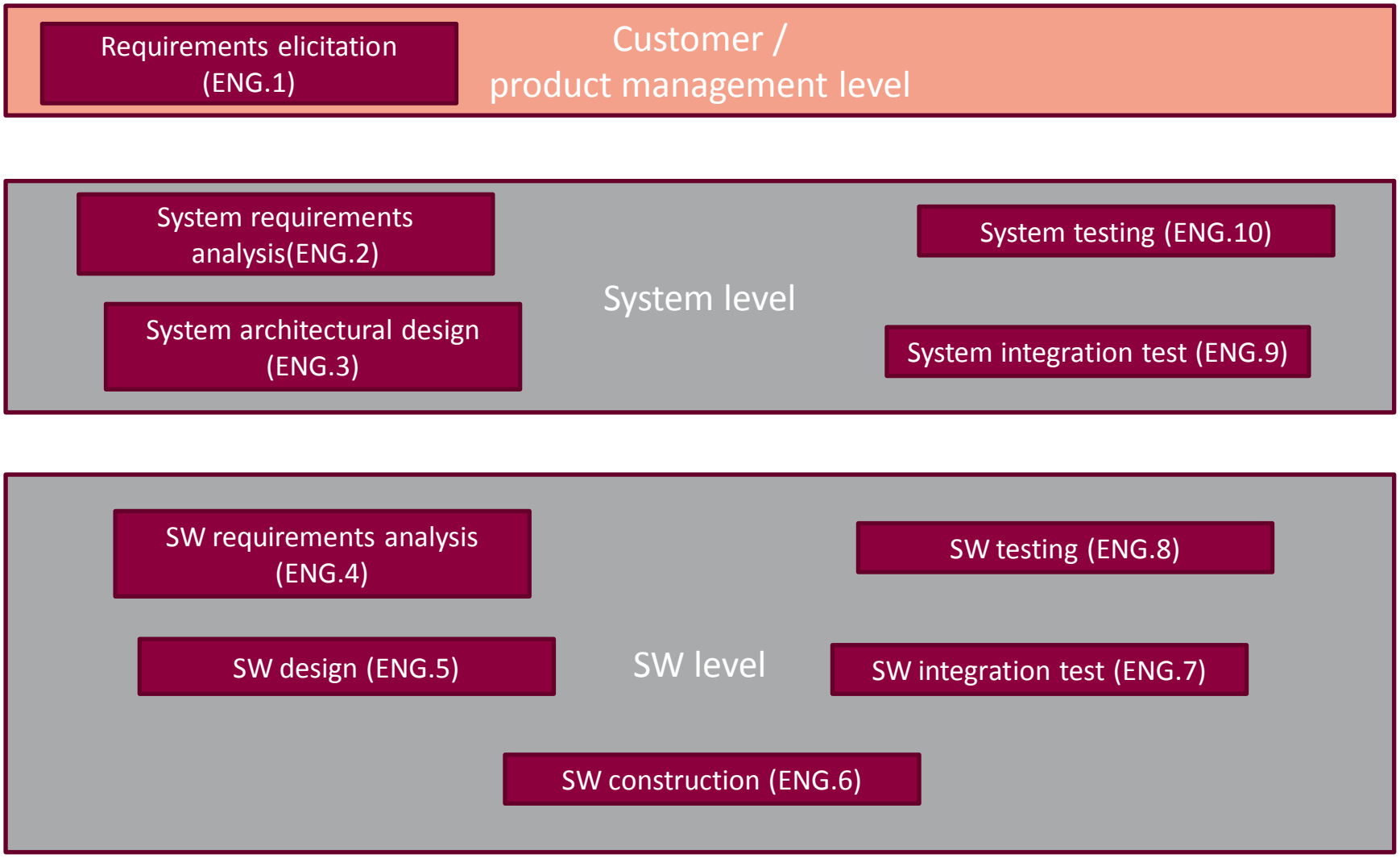
Source: ISO / DIS 26262-10

- As an example, with functional safety to be addressed as an item characteristic, many companies must widen their focus from the system they deliver to the whole item, which has to be safe
- As a result, the role of the customer becomes fundamental when eliciting (safety) requirements to properly understand hazardous events at item level and their consequences in terms of safety requirements to be met by individual systems of the item

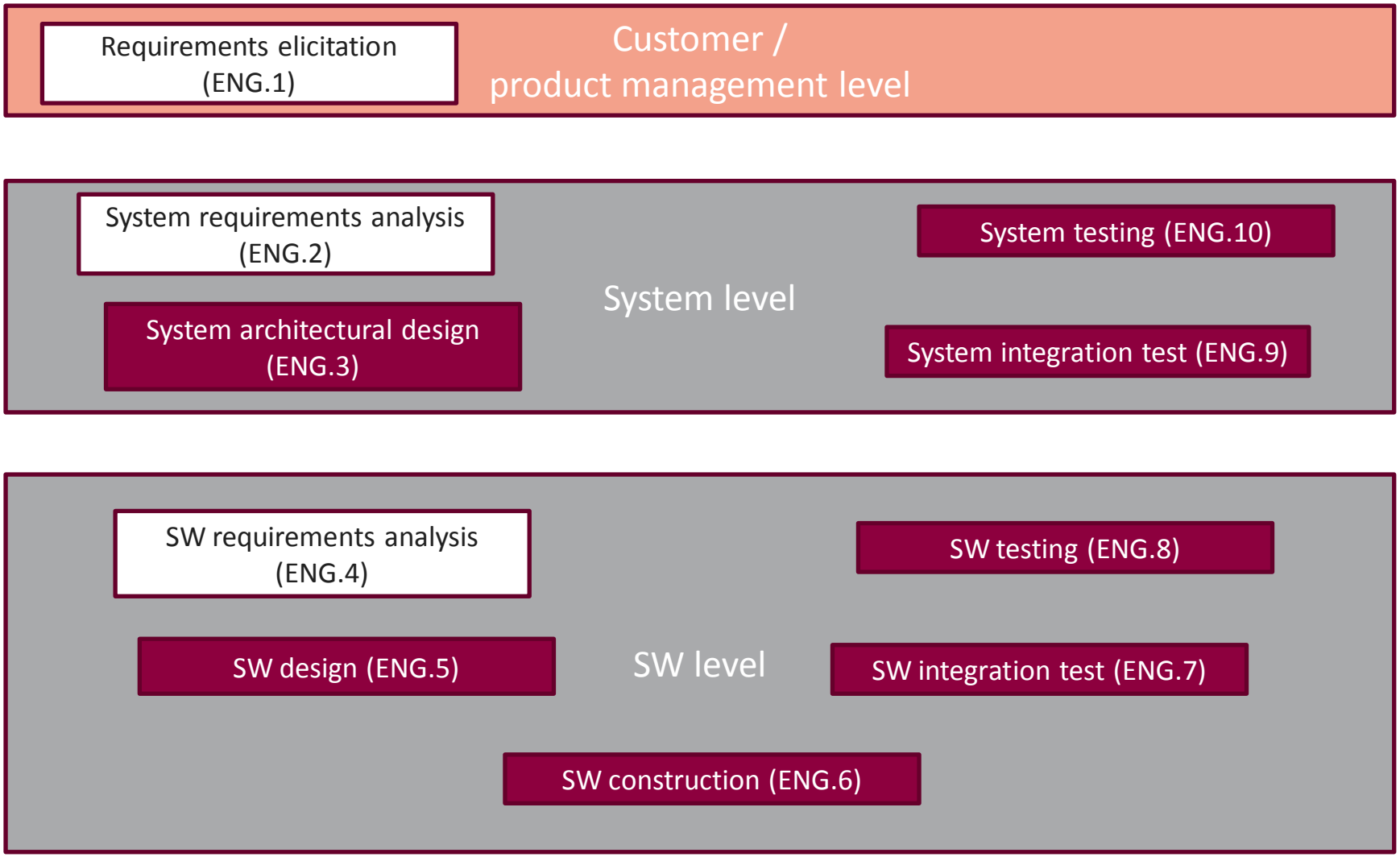
Agenda

- Introduction
- Requirements engineering according to Automotive SPICE
- Requirements engineering according to ISO 26262
- Mapping of requirements-related work products of ISO 26262 and A-SPICE
- Requirements engineering and management with ISO 26262 and A-SPICE
- Conclusions

Automotive SPICE – Engineering process group (ENG)



Automotive SPICE – Engineering process group (ENG)



ASPICE requirements-related processes

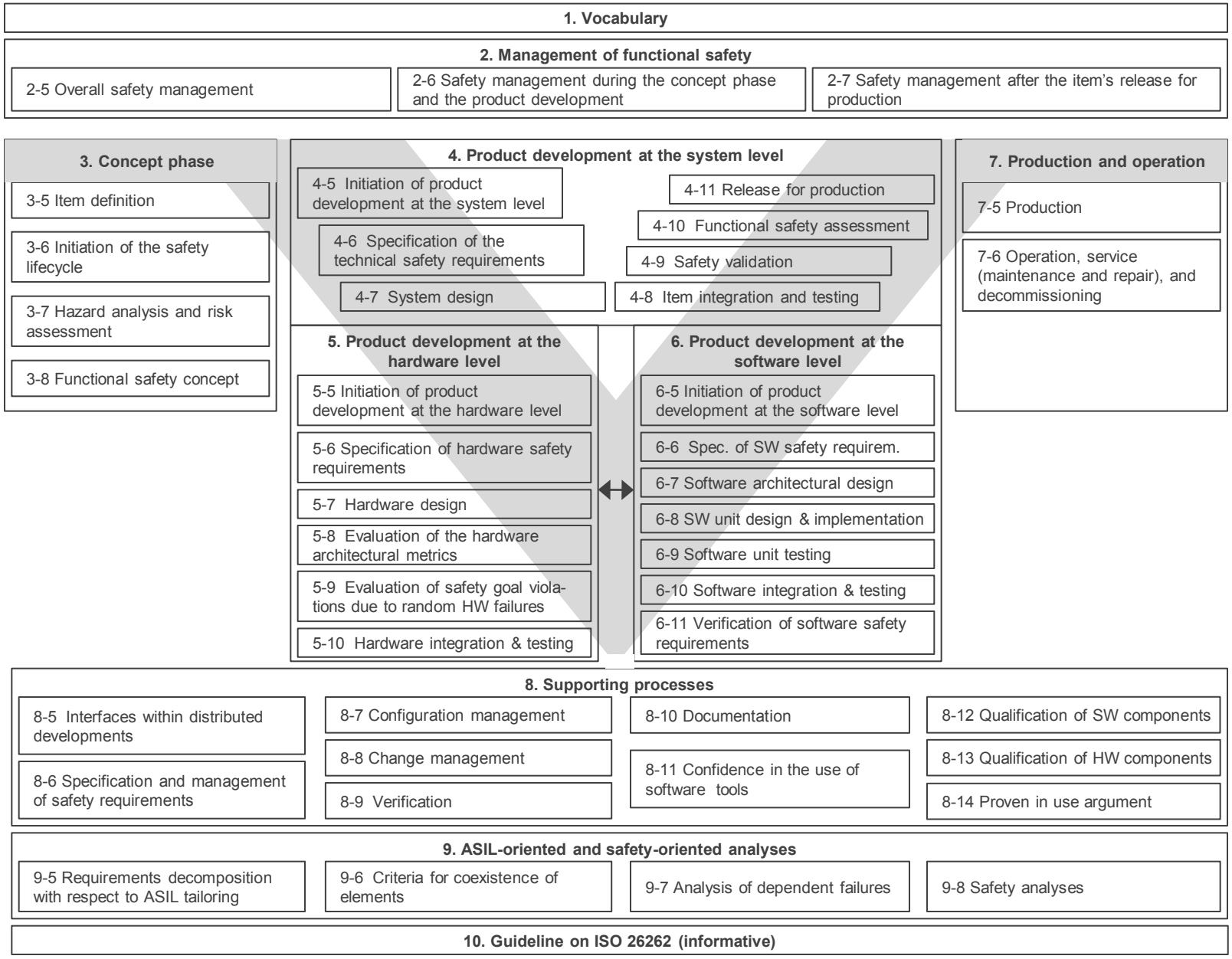
- **ENG.1 Requirements elicitation**:
  The purpose of the Requirements elicitation process is to gather, process, and track evolving customer needs and requirements throughout the life of the product and/or service so as to establish a requirements baseline that serves as the basis for defining the needed work products.
  → *Customer requirements*
- **ENG.2 System requirements analysis**:
  The purpose of the System requirements analysis process is to transform the defined customer requirements into a set of desired system technical requirements that will guide the design of the system.
  → *System requirements*
- **ENG.4 Software requirements analysis**:
  The purpose of the Software requirements analysis process is to establish the software requirements for the system.
  → *Software requirements*
- No dedicated process exist to analyze *hardware requirements*

Source: Automotive SPICE®, PAM Vers. 2.5

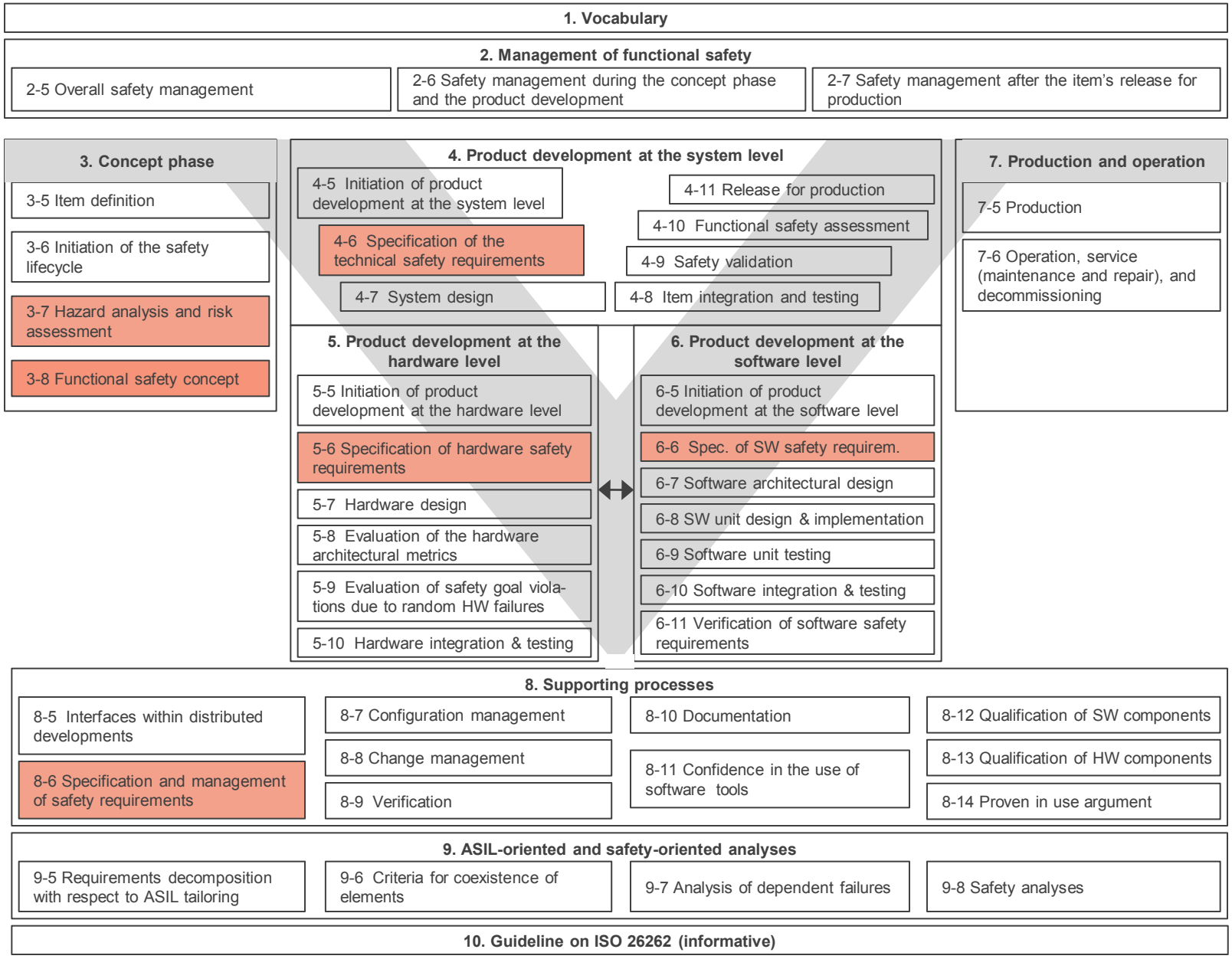
Agenda

- Introduction
- Requirements engineering according to Automotive SPICE
- Requirements engineering according to ISO 26262
- Mapping of requirements-related work products of ISO 26262 and A-SPICE
- Requirements engineering and management with ISO 26262 and A-SPICE
- Conclusions

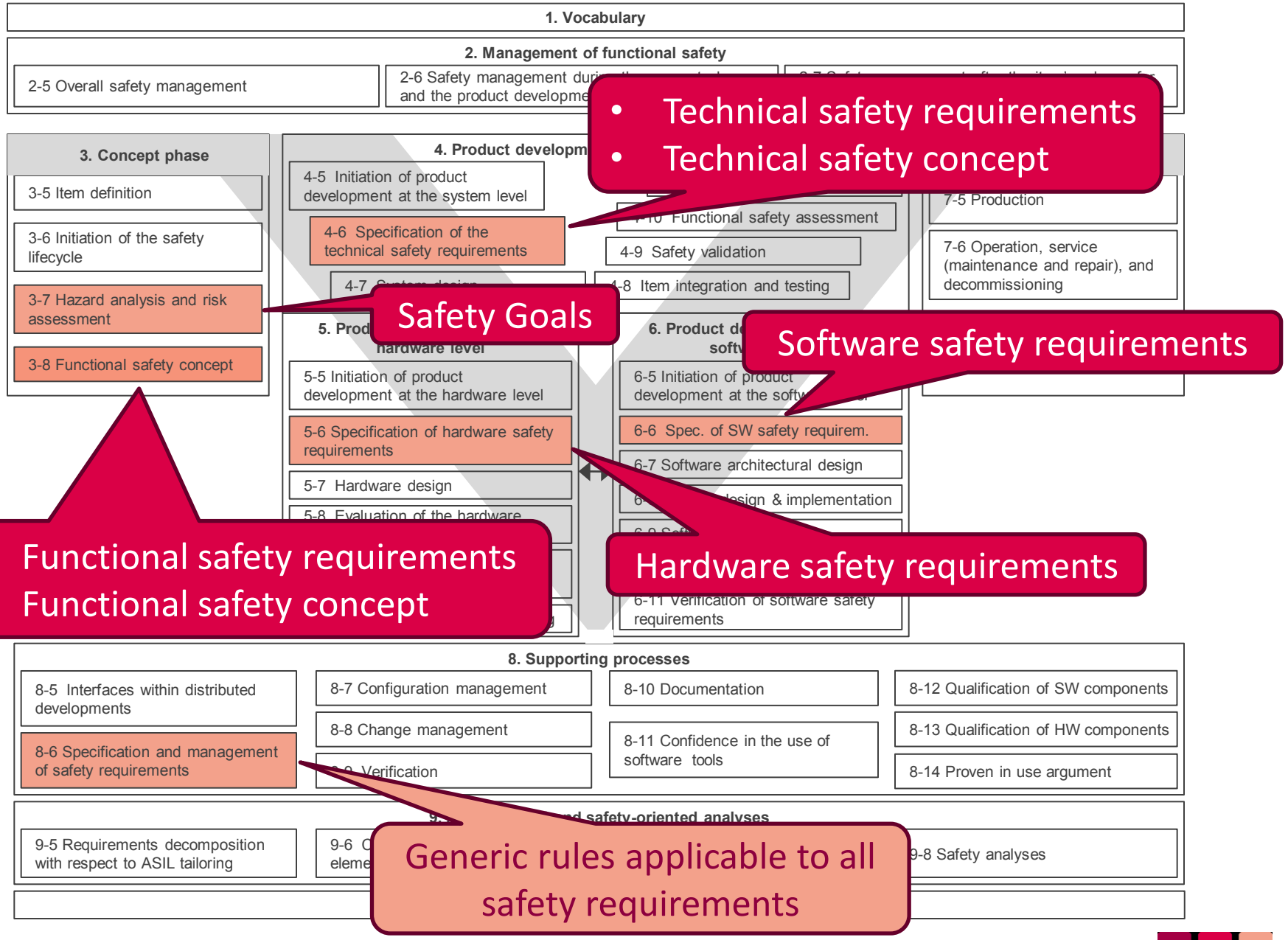
ISO 26262 Overview



ISO 26262 Overview



ISO 26262 Overview



Technical safety requirements

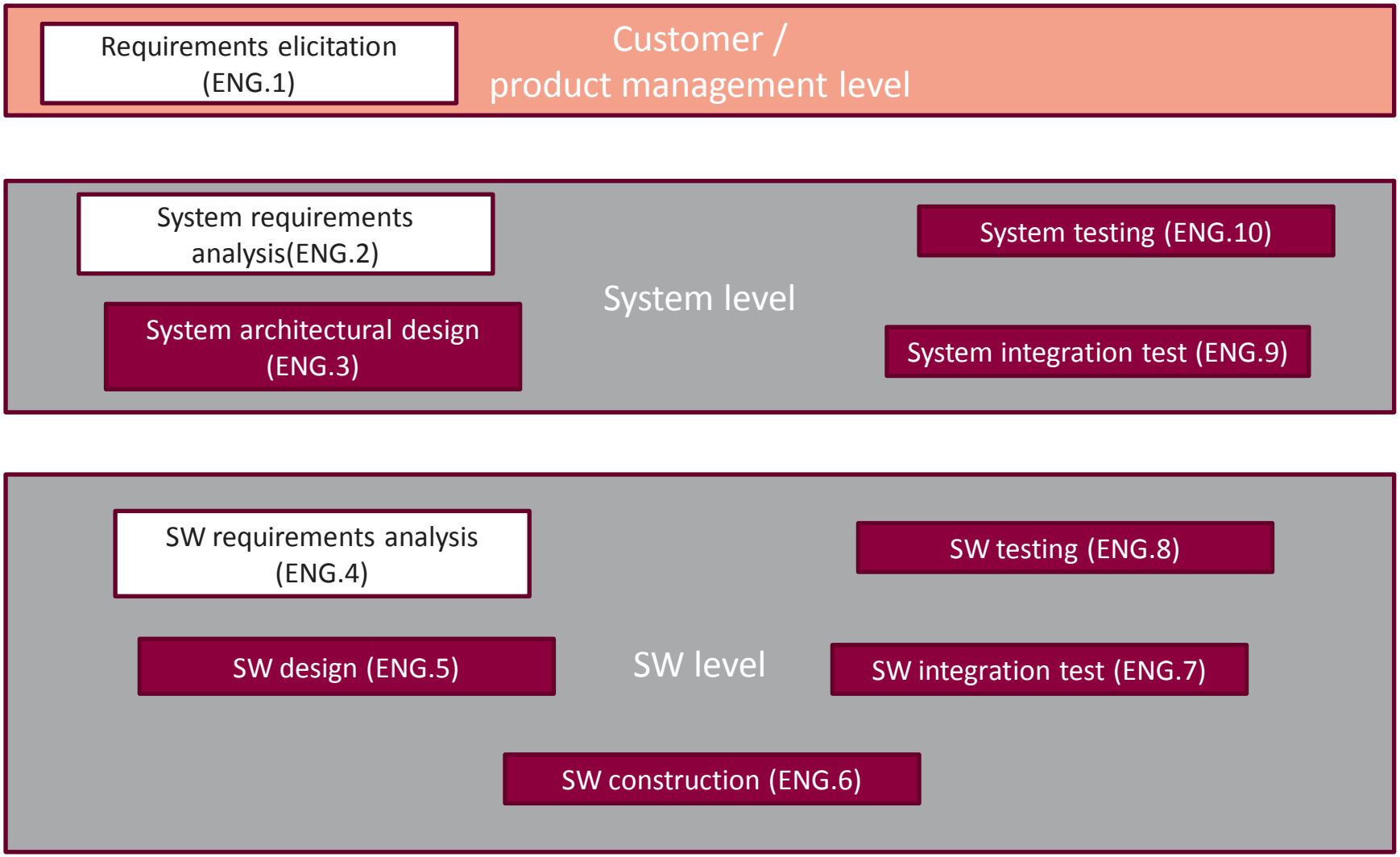
Requirements at the item / system level including safety mechanisms:

- Detection, indication and control of faults in the system itself and in external devices interacting with the system
- Measures to achieve or maintain a safe state
- Fault tolerant time interval and emergency operation time
- Measures to prevent faults from being latent (6.4.4: ASIL (A), (B), C, D)
- Tests before and after a period of operation (pre-drive checks, post-drive checks)
- Multiple point fault detection interval

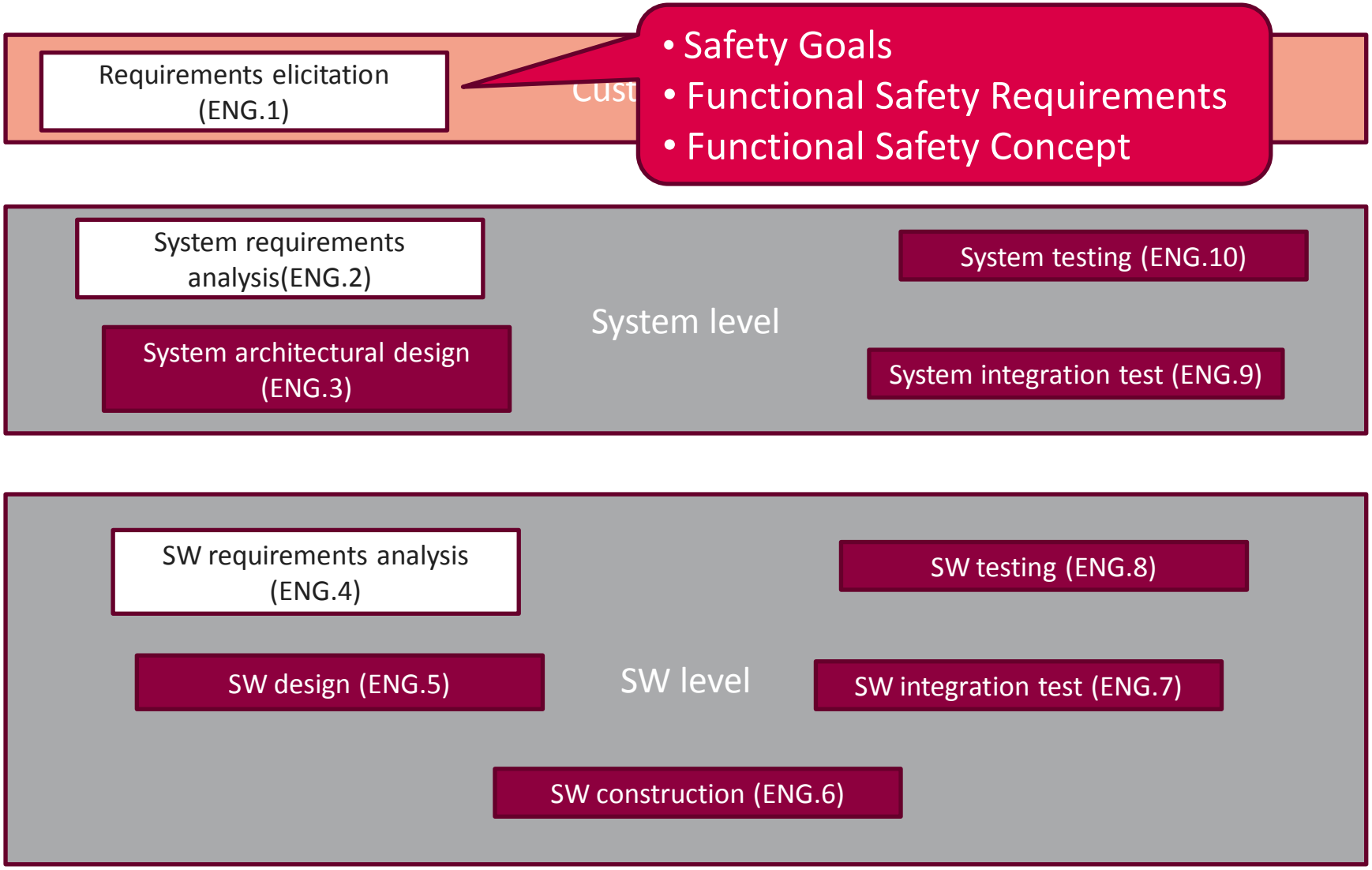
Agenda

- Introduction
- Requirements engineering according to Automotive SPICE
- Requirements engineering according to ISO 26262
- Mapping of requirements-related work products of ISO 26262 and A-SPICE
- Requirements engineering and management with ISO 26262 and A-SPICE
- Conclusions

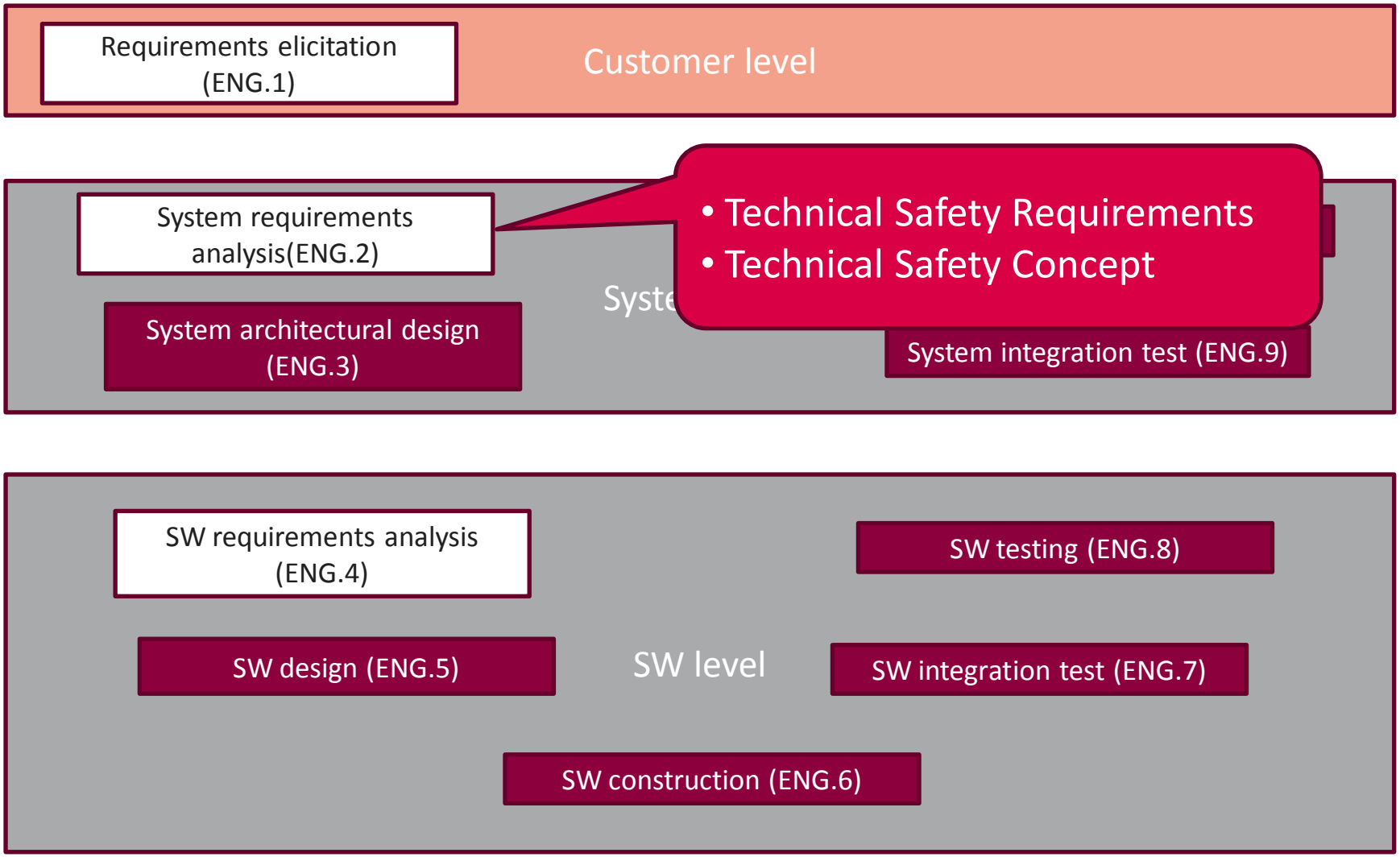
Automotive SPICE – Engineering process group (ENG)



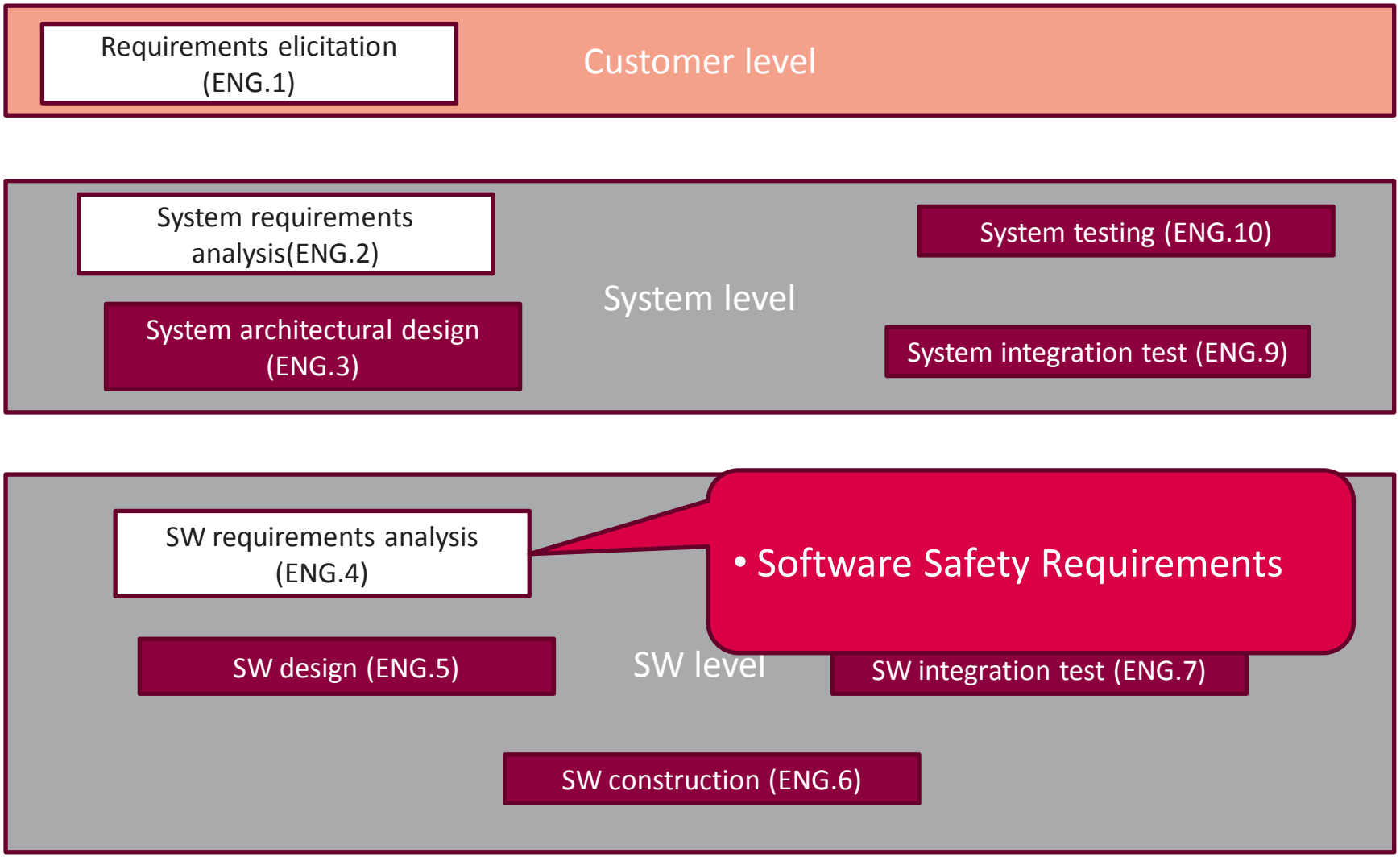
Automotive SPICE – Engineering process group (ENG)



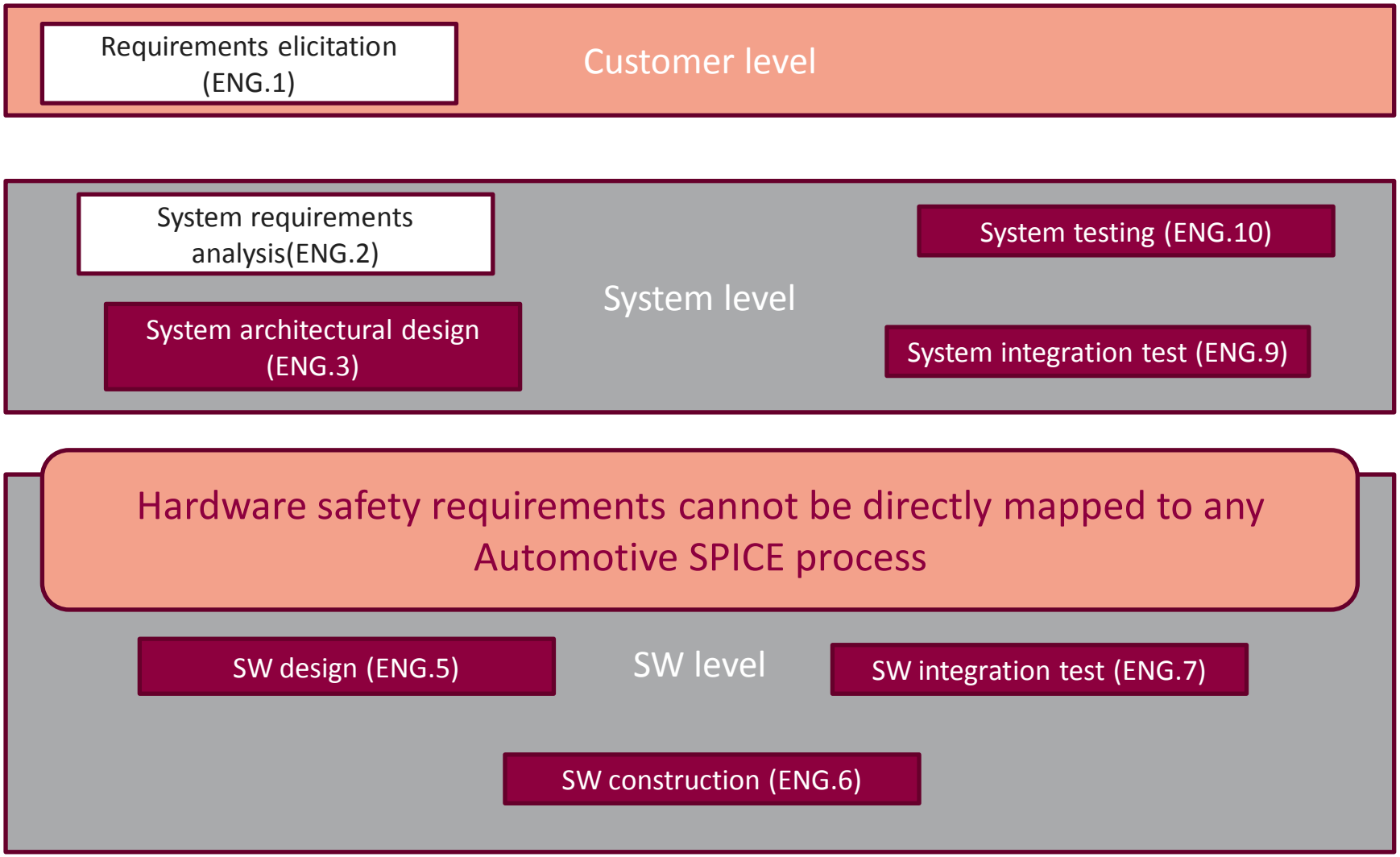
Automotive SPICE – Engineering process group (ENG)



Automotive SPICE – Engineering process group (ENG)



Automotive SPICE – Engineering process group (ENG)



Agenda

- Introduction
- Requirements engineering according to Automotive SPICE
- Requirements engineering according to ISO 26262
- Mapping of requirements-related work products of ISO 26262 and A-SPICE
- Requirements engineering and management with ISO 26262 and A-SPICE
- Conclusions

Requirements engineering and management with ISO 26262 and Automotive SPICE (1/3)

- Since Automotive SPICE does not explicitely address hardware development, to specify and analyze hardware safety requirements additional processes are required

- Other safety requirements such as safety goals, functional and technical safety requirements can be processed within the scope of processes already implemented and aligned to Automotive SPICE

- Safety requirements do not relate to nominal performance of the system under development; they can be integrated into existing requirements specifications, however, they need to be classified accordingly

Requirements engineering and management with ISO 26262 and Automotive SPICE (2/3)

- Safety goals, functional safety requirements and functional safety concept are often delivered by the customer; in any case a strong cooperation between customer and supplier(s) is required to understand all possible hazardous events at item level and derive technical safety requirements for the system to be developed by the supplier

- Safety goals are required to calculate hardware metrics; without clearly defined and agreed safety goals, it could become difficult or even impossible to fulfill ISO 26262 requirements with respect to hardware metrics

Requirements engineering and management with ISO 26262 and Automotive SPICE (3/3)

Additional ISO 26262 expectations apply with respect to methods for requirements engineering and management

Table 1 — Specifying safety requirements

Methods		ASIL			
		A	B	C	D
1a	Informal notations for requirements specification	++	++	+	+
1b	Semi-formal notations for requirements specification	+	+	++	++
1c	Formal notations for requirements specification	+	+	+	+

Table 2 — Methods for the verification of safety requirements

Methods		ASIL			
		A	B	C	D
1a	Verification by walk-through	++	+	o	O
1b	Verification by inspection	+	++	++	++
1c	Semi-formal verification[a]	+	+	++	++
1d	Formal verification	o	+	+	+

[a] Method 1c can be supported by executable models.

Source ISO 26262-8

Agenda

- Introduction
- Requirements engineering according to Automotive SPICE
- Requirements engineering according to ISO 26262
- Mapping of requirements-related work products of ISO 26262 and A-SPICE
- Requirements engineering and management with ISO 26262 and A-SPICE
- Conclusions

Conclusions (1/2)

- Even if Automotive SPICE and ISO 26262 uses different terminology they do not contradict each other

- Implementation of ENG.1, 2 and 4 of Automotive SPICE is a sound basis for requirements engineering and management

- To deal with ISO 26262, processes need to be extended to cope with hardware (safety) requirements

Conclusions (2/2)

- During requirements elicitations, additional information about safety goals, functional safety requirements and concept has to be provided by the customer (if no customer is available, assumptions must be made → SEooC)

- Safety requirements can be integrated into available requirements specifications but they must be distinguished from the nominal performance of the system under development

- ISO 26262 states additional expectations regarding methods for requirements engineering and management

If you wish to deepen the subject…

KUGLER MAAG CIE GmbH
Leibnizstr. 11
70806 Kornwestheim, Germany
information@kuglermaag.com
www.kuglermaag.com

… contact me

Fabio Bella
Senior Process Consultant, Manager Italy
Fabio.bella@kuglermaag.com
Mobile +39 345 7019271

Thank you for your attention.
Questions? Comments?

Requirements Engineering and Management with ISO 26262 and Automotive SPICE , Version A

KUGLER MAAG CIE
besser mit uns