DAIMLER

Implementation of requirements from ISO 26262 in the development of E/E components and systems

Challenges & Approach

Automotive Electronics and Electrical Systems Forum 2008
May 6, 2008, Stuttgart, Germany

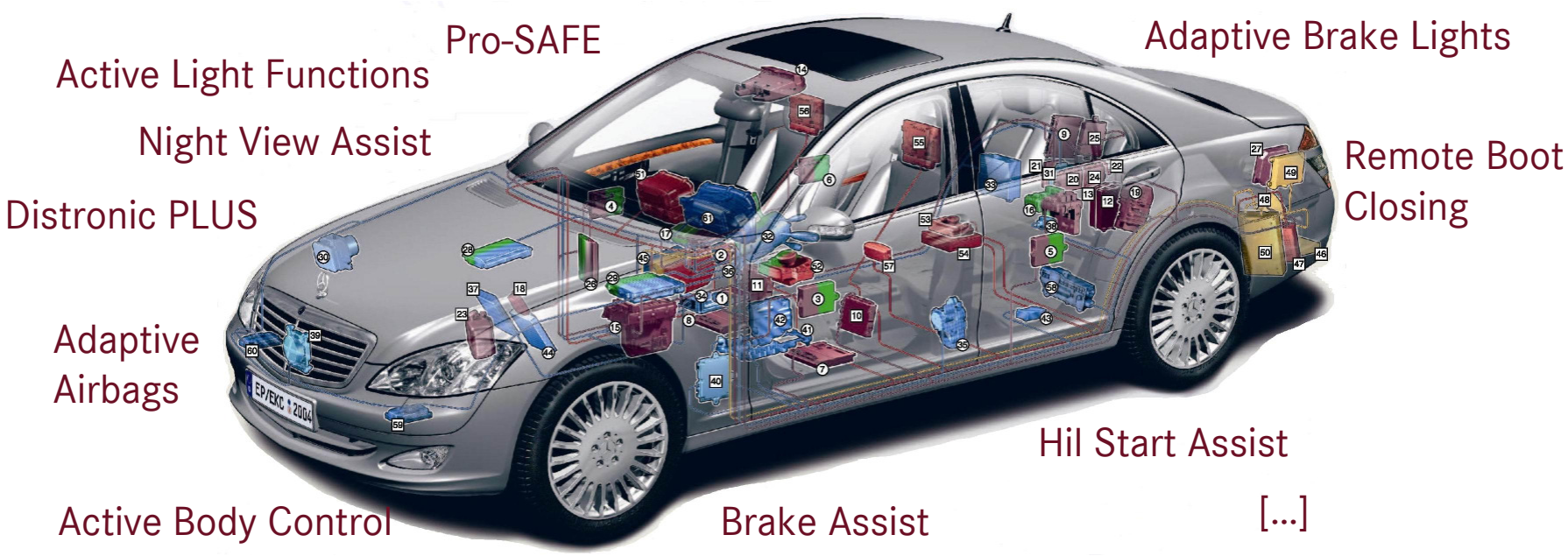
Dr. Axel Dold (Daimler AG, Research & Development GR/ESP) / 06.05.2008

Outline

- Introduction
- Overview of ISO 26262
- Challenges for Daimler
- Implementation Approach
- Summary / Outlook

Current Situation
Trends in Automotive Electric/Electronics (E/E)

- Increasing functionality and complexity of software-based car functions
- Increasing risks from systematic faults and random hardware faults
- Most of the new car functions are safety-related



Development of software-based vehicle functions
Current and future general conditions

- German legislature requires, that safe cars are developed according to state-of-the-art technology
- Based on the IEC 61508, a new upcoming standard (ISO 26262) is derived to comply with needs specific to the application sector of E/E systems within road vehicles
- When published as an ISO standard (expected in 2011), the new standard must be applied to every new car platform development project
- Additional requirements to development and supporting processes must be met (e.g. safety management, document management), and suitable methods must be applied (e.g. hazard analysis and risk assessment, safety analysis methods)

ISO 26262
Upcoming automotive standard for functional safety

Objective:

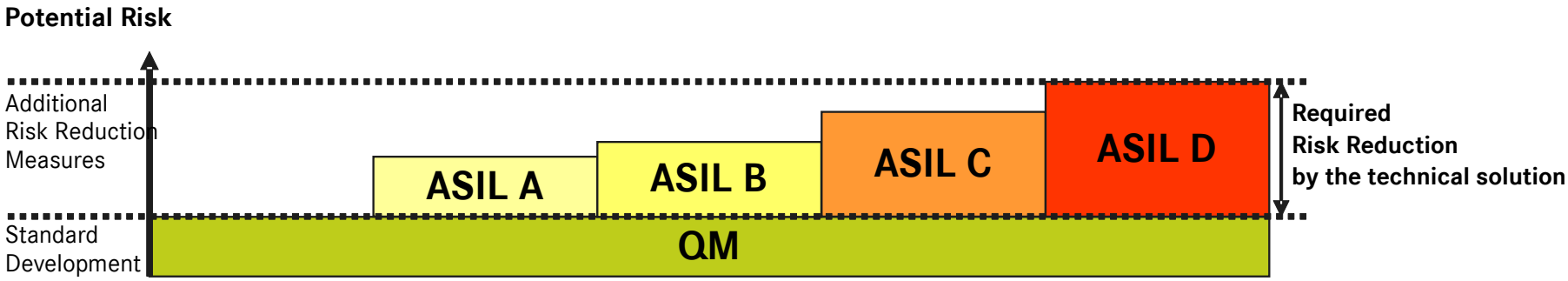
- To achieve a comparable acceptable residual risk for each of the vehicle functions independent of the potential (initial) risk
- State-of-the-art technology for the development of safety-related systems address:
  - ⇒ Prevention of systematic faults
  - ⇒ Detection, controlling and handling of the remaining relevant faults / failures
  - ⇒ Definition of all necessary activities, to ensure and accomplish the required functional safety of the E/E systems

Basic Idea:

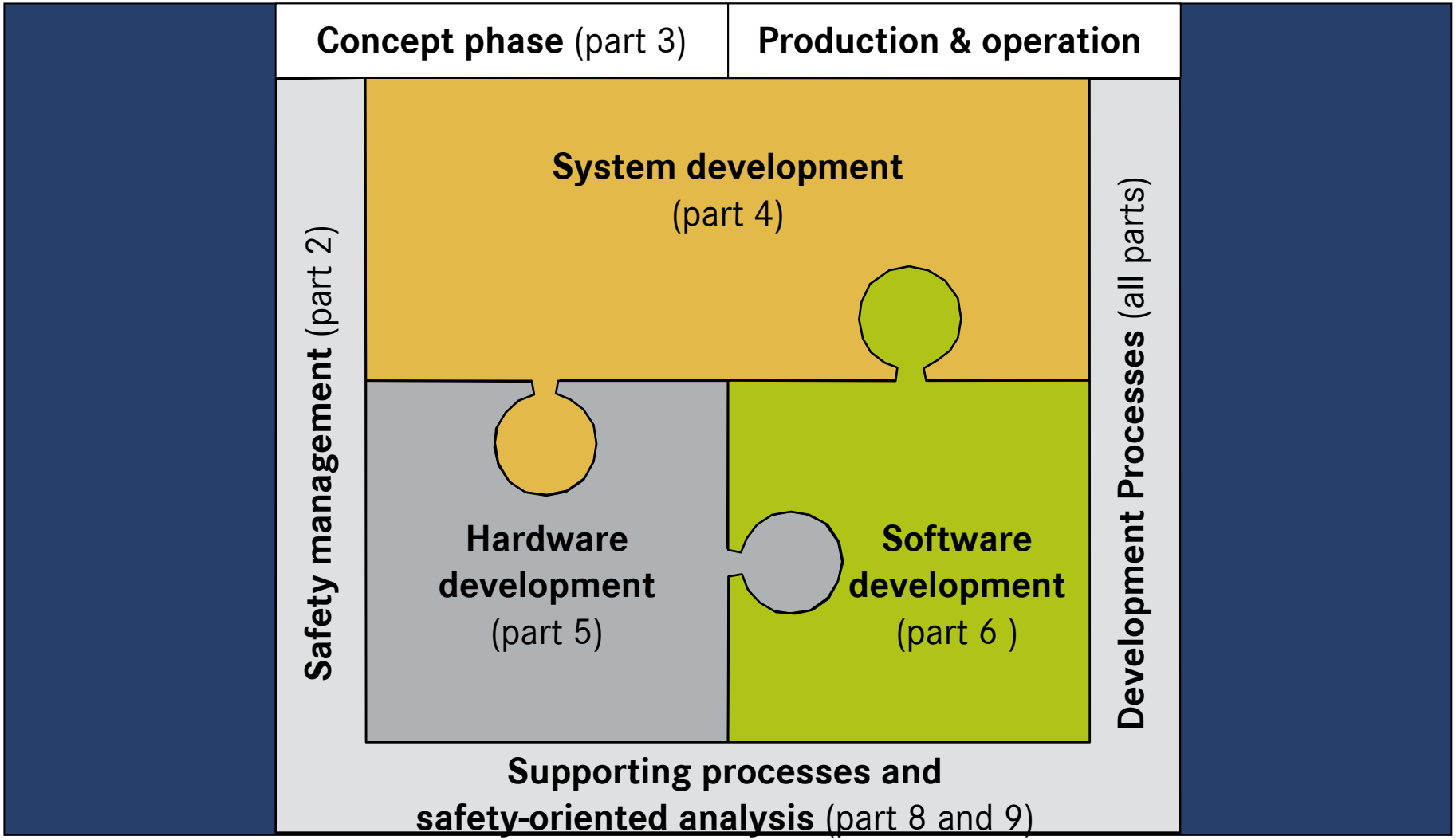
- Identify potential hazards and risks of a vehicle function
- Define acceptable risk goals and establish safety requirements
- Define and implement measures to avoid or reduce risks
- Validate that (safety) goals are met

ISO 26262
Automotive Safety Integrity Levels

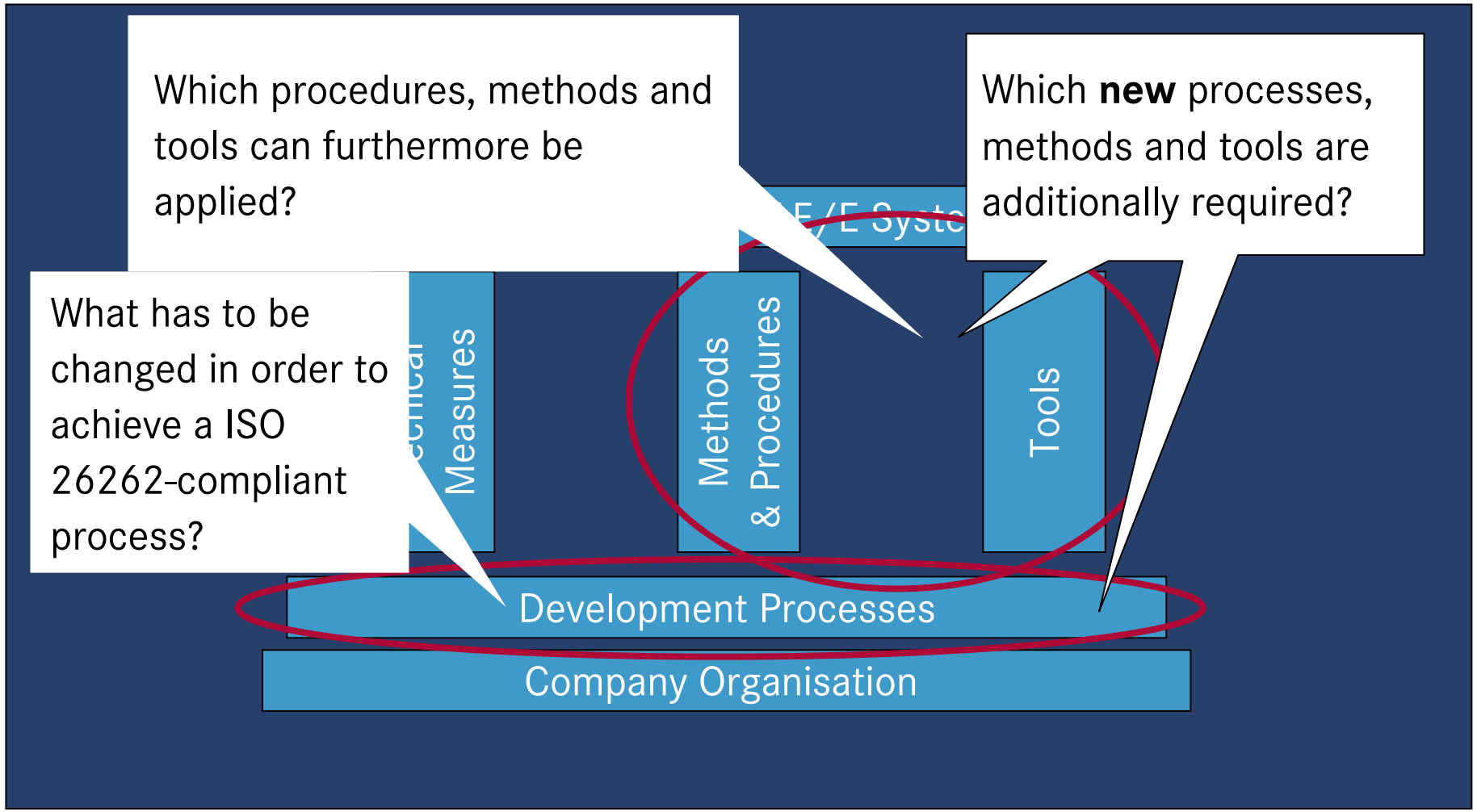
- The technical risk reduction measures to achieve an acceptable residual risk are classified into 4 classes
  - Automotive Safety Integrity Level (ASIL): A,B,C,D
- **Important Remark**: The ASIL always refers to a specific safety requirement



ISO 26262
Overview (Baseline 11)

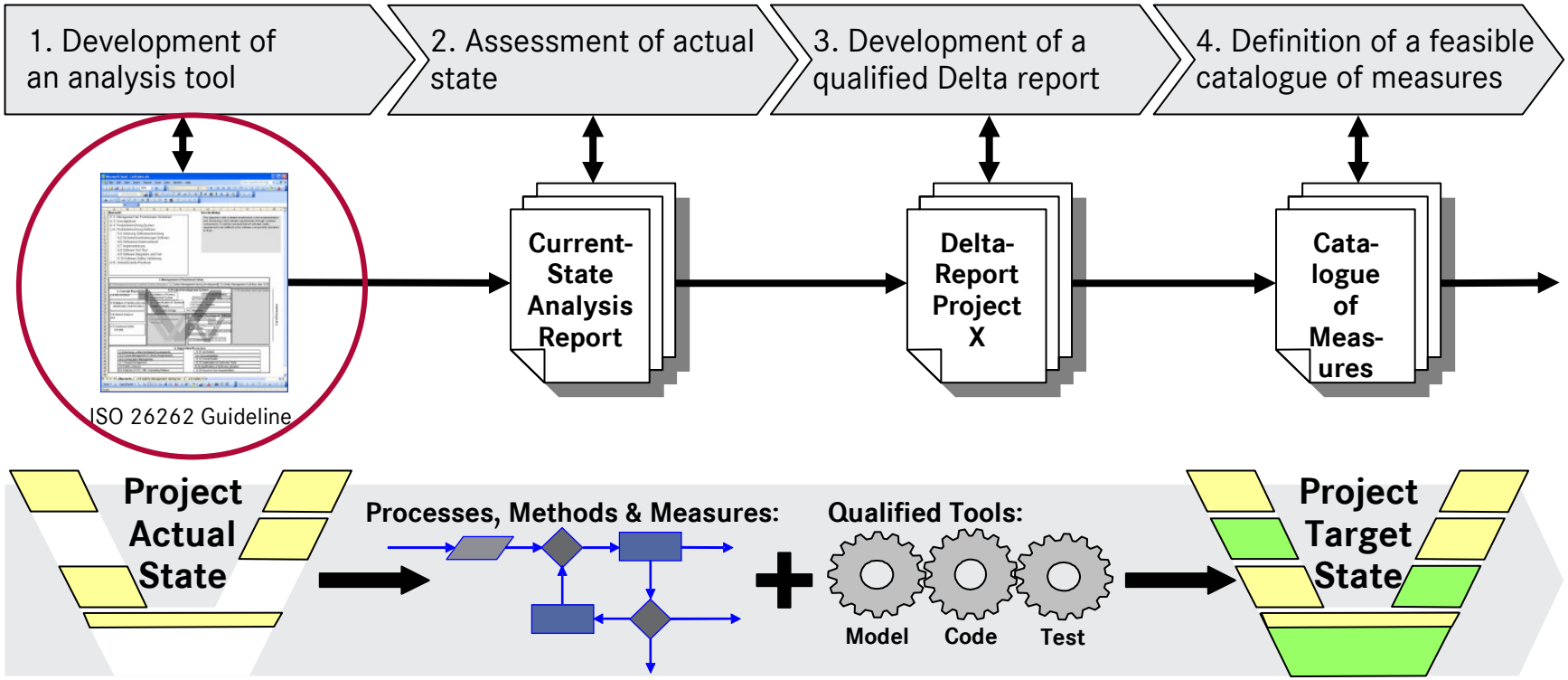


ISO 26262 – The new safety standard
Challenges for Daimler

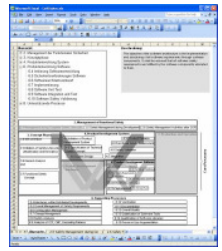


ISO WD 26262
Gap analysis in pilot projects

Generation of an assessment view (of the standard) to assess the (current) processes and applied methods / tools for selected pilot projects



ISO 26262
Development of a process guideline



Elaboration of the requirements of ISO 26262:

- Analysis of the interrelationship and dependencies
- Determination of valid process variants

Adaptation to Daimler development context and needs:

- Mapping to existing development processes
- Restriction of the variability

Documentation of the remaining variants:

- Separation into obligatory, optional and variable phases within the development processes
- Compilation of applicable methods and procedures for each sub phase resp. development step

ISO WD 26262
Requirements to software development methods

Example from part 6 „SW Development“:
Requirements to methods for informally verifying the software architectural design

Methods and Measures		According to req.	ASIL			
			A	B	C	D
1a	Inspection of software architectural design	6.4.20	++	++	++	++
1b	Walkthrough of software architectural design	6.4.20	++	+	o	o
1c	Model Inspection	6.4.20	++	++	++	++
1d	Model Walkthrough	6.4.20	++	+	o	o

Remark: From each group of methods at least one suitable method must be selected according to the ASIL classification

ISO WD 26262
Daimler-specific selection of suitable methods

Selection of the most suitable methods for Daimler for the informal verification of the SW architectural design

Methods and Measures		According to req.	ASIL			
			A	B	C	D
1a	Inspection of software architectural design	6.4.20	++	++	++	++
1b	Walkthrough of software architectural design	6.4.20	++	+	o	o
1c	Model Inspection	6.4.20	++	++	++	++
1d	Model Walkthrough	6.4.20	++	+	o	o

ISO WD 26262
ASIL-based method selection

The selected methods are documented within the ISO 26262 guideline:

Methods and Measures		ASIL			
		A	B	C	D
1a	Inspection of software architectural design	++	++	++	++
1c	Model Inspection	++	++	++	++

For a specific project, the suitable methods can be selected based on the ASIL classification:

Methods and Measures		ASIL			
		A	B	C	D
1a	Inspection of software architectural design	++	++	++	++
1c	Model Inspection	++	++	++	++

ISO WD 26262

Results of the analysis in the pilot projects

Many requirements of the upcoming standard addressing the development and supporting processes are already mapped into internal quality standards

⇒ Processes must be partially adapted and evaluated according to the additional requirements (e.g. change management, development interface agreement with supplier)

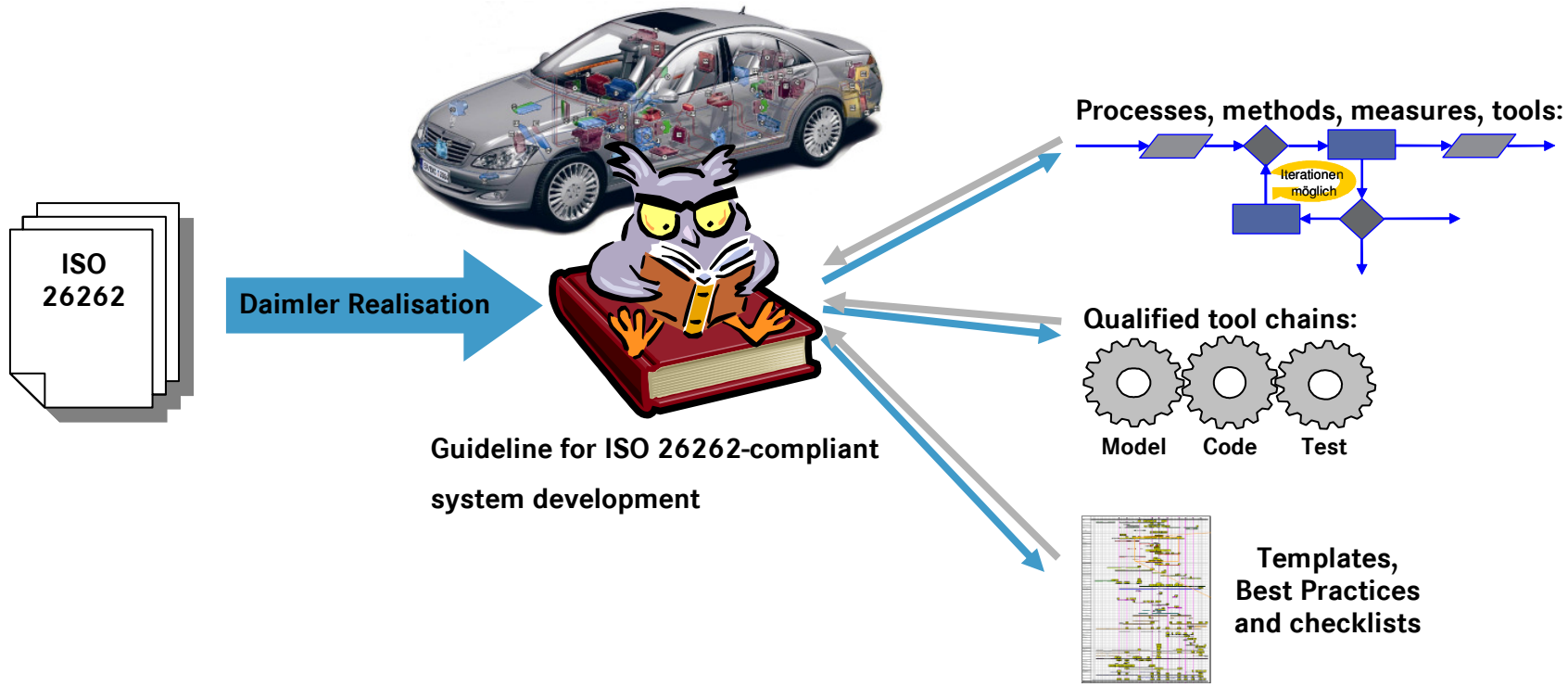
⇒ The modified / adapted processes and methods must be incorporated into internal quality standards

Requirements to the management of functional safety:

- Developing, piloting, and accomplishing new processes, methods and tools:
  - Document structures / management for safety-related work products
  - Integrated safety analysis methods for systems and software must be established (e.g. FMEA, FTA)

Implementation of ISO 26262
Guidelines for system, hardware and software development

Documentation of all safety activities and corresponding methods and tools for the E/E system developers including templates, examples and process instructions.



Implementation of ISO 26262
Summary

- The upcoming safety standard faces a great challenge for the automotive industry:
  - Requirements must be implemented efficiently under consideration of the internal context and constraints
  - Specific requirements comprise the safety-related activities and technical risk mitigation measures
- There is no discrepancy between mature development processes and the ISO 26262 concerning organisational requirements and supporting processes
- Safety must be an integral part of current and future process improvement activities
- For software development suitable methods and measures have to be developed / adapted and qualified tools must be provided