



TECHNISCHE
UNIVERSITÄT
DRESDEN

Vorlesung Automotive Software Engineering Teil 7 Normen und Standards Einleitung

Sommersemester 2015

Prof. Dr. rer. nat. Bernhard Hohlfeld

Bernhard.Hohlfeld@mailbox.tu-dresden.de

Technische Universität Dresden, Fakultät Informatik

Honorarprofessur Automotive Software Engineering

Normen und Standards Automotive

- AUTOSAR
- OSEK
- Kommunikationsbusse
- ISO 26262
- MISRA-C
- HIS
- Automotive Spice
- CMMI
- Qualitätsstandards
- ASAM



OSEK/ VDX

ASAM

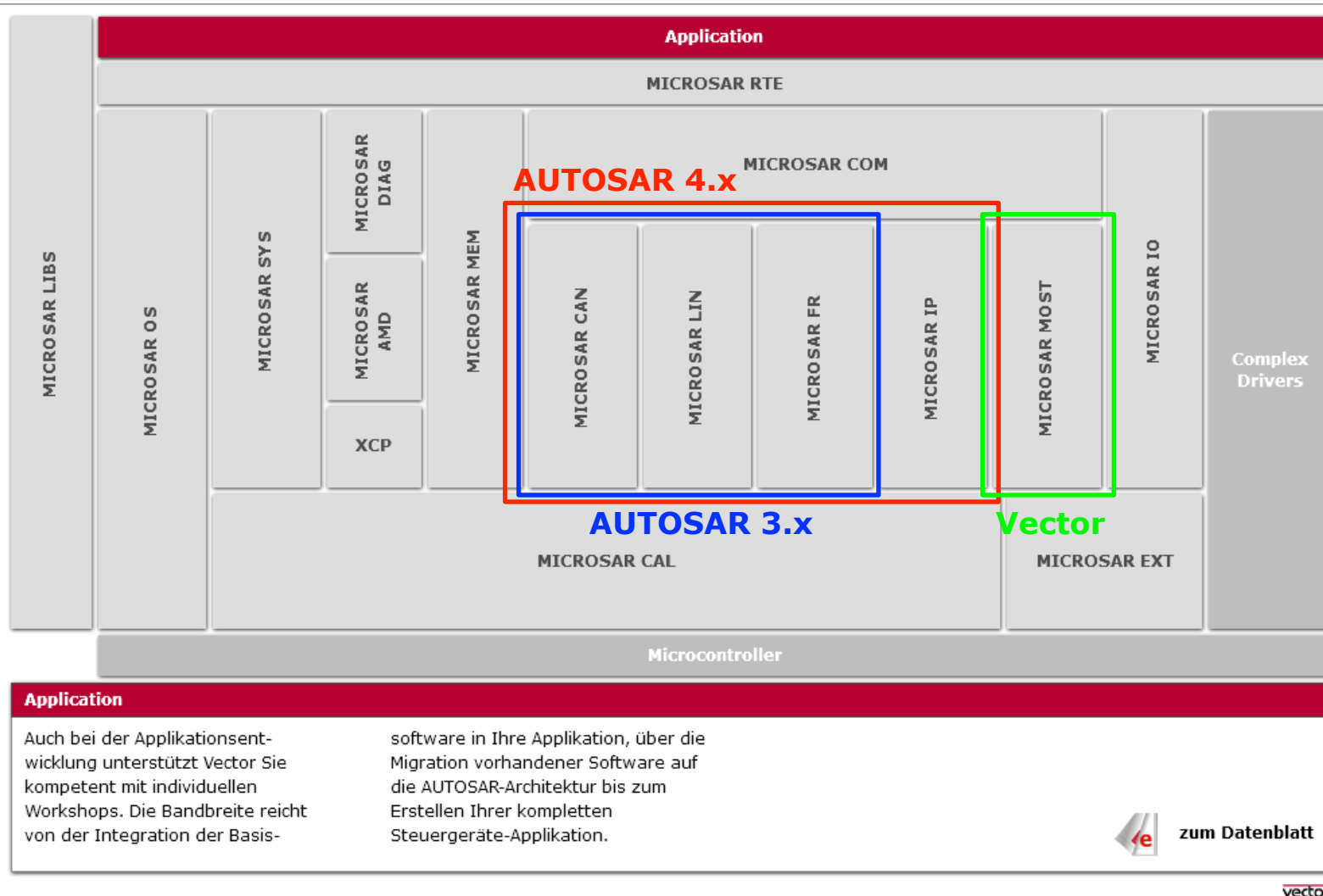
ISO 26262
Road vehicles -
Functional safety



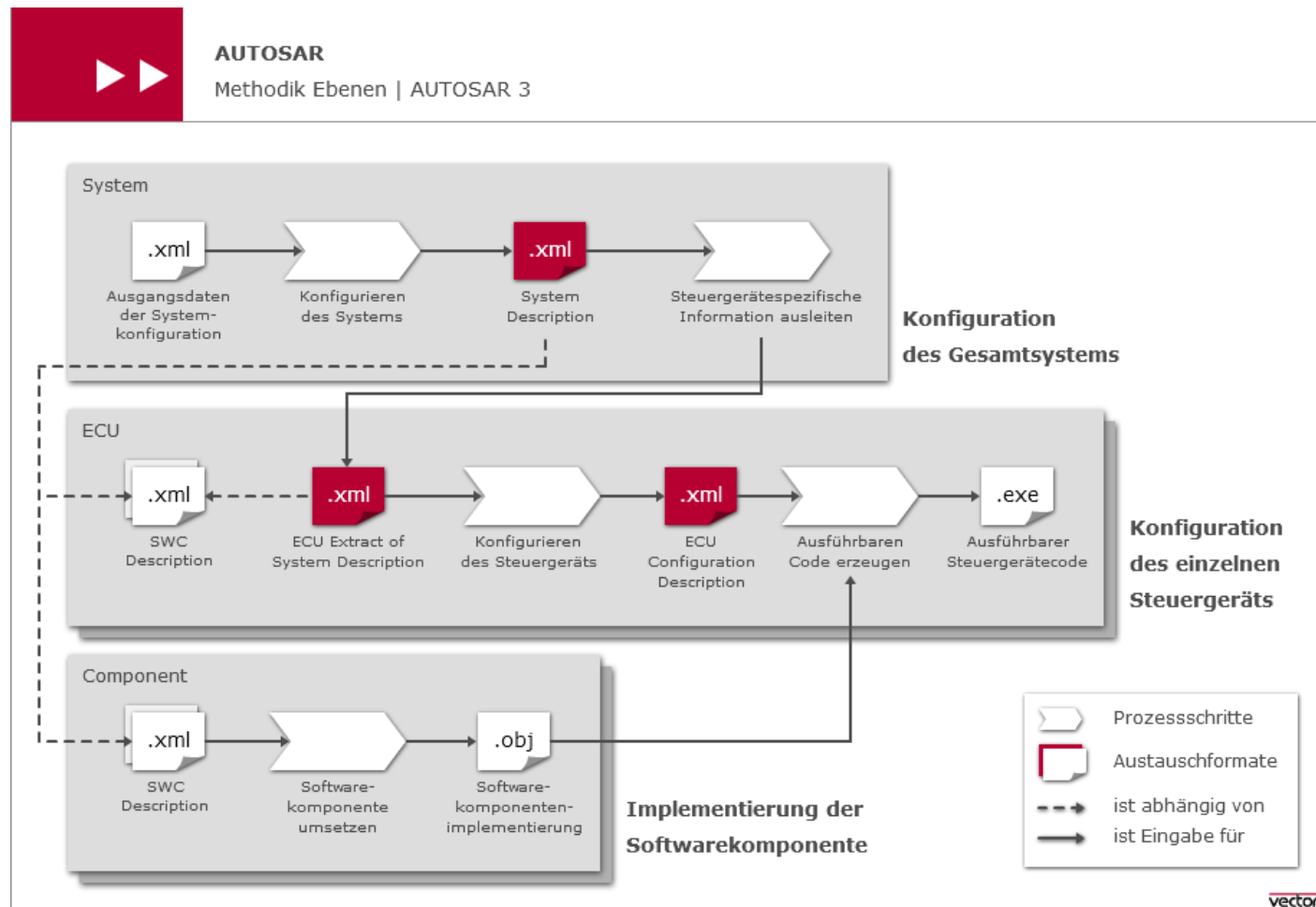
1.1 Was verbirgt sich hinter AUTOSAR?

- AUTomotive Open System ARchitecture
- www.autosar.org
- Eine erste Antwort ist auf der AUTOSAR-Website veröffentlicht; in der dort frei zugänglichen Spezifikation. Sie umfasste Anfang 2009 im AUTOSAR-Release 3.1 einen Umfang von 132 PDF-Dokumenten. In den dazugehörigen Präsentationen beschreibt sich AUTOSAR selbst so [FBH06]:
 - Architektur:
Eine komplette Basissoftware für Steuergeräte als Integrationsplattform für hardwareunabhängige Softwareanwendungen.
 - Methodik:
Austauschformate oder Beschreibungsvorlagen für einen nahtlosen Konfigurationsprozess der Basissoftware und die Integration der Anwendungssoftware auf einem Steuergerät. Hierzu zählt auch die Methodik, wie dieses Gerüst verwendet wird.
 - Application Interfaces:
Die Spezifikation von Schnittstellen typischer Automobilanwendungen aus allen Gebieten in Bezug auf Syntax und Semantik, die als ein Standard für die Anwendungssoftware dienen sollte.

Architektur - MICROSAR 4



Methodik - AUTOSAR 3.x



Application Interfaces

AUTOSAR Application Interfaces Compositions under Consideration

■ **Body Domain**

- Central Locking
- Interior Light
- Mirror Adjustment
- Mirror Tinting
- Seat Adjustment
- Wiper/Washer
- Anti Theft Warning System
- Horn Control

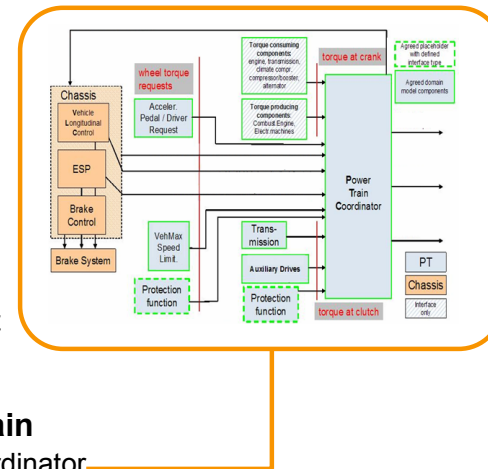
- Exterior Lights
- Defrost Control
- Seat climatization
- Cabin climatization
- Steering wheel climatization
- Window Control
- Sunroof/Convertible control
- Steering column adjustment
- Roller blind control

■ **Chassis Control Domain**

- Vehicle Longitudinal Control
- Electronic Stability Program
- Electronic Parking Brake
- Adaptive Cruise Control
- Roll Stability Control
- Steering System
- Suspension System
- Stand Still Manager
- High Level Steering
 - Vehicle Stability Steering
 - Driver Assistance Steering
- All Wheel Drive/ Differential Lock

■ **Powertrain Domain**

- Powertrain Coordinator
- Transmission System
- Combustion Engine
 - Engine torque and mode management
 - Engine Speed And Position
 - Combustion Engine Misc.
- Electric Machine
- Vehicle Motion Powertrain
 - Driver Request
 - Accelerator Pedal Position
 - Safety Vehicle Speed Limitation



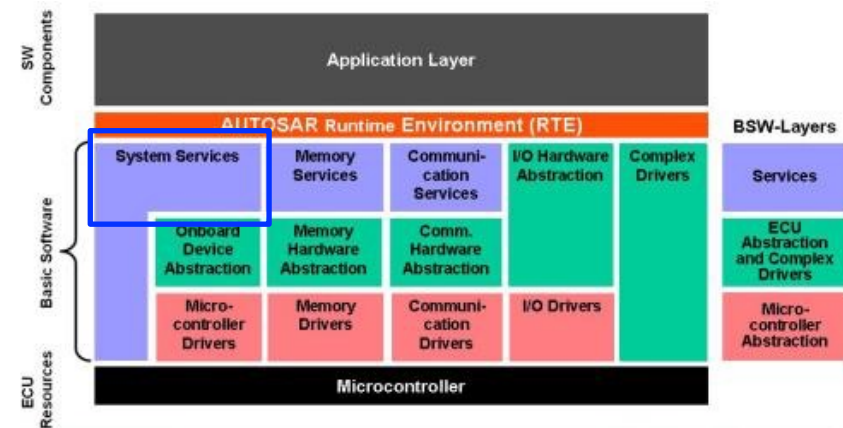
OSEK

- www.osek-vdx.org
- OSEK
 - Offene Systeme und deren Schnittstellen für die Elektronik im Kraftfahrzeug
 - Mai 1993, deutsches Projekt
 - BMW, Bosch, Daimler, Opel, Siemens (jetzt Continental), VW, Universität Karlsruhe (jetzt KIT)
- VDX
 - Vehicle Distributed eXecutive
 - Französisches Projekt
 - PSA, Renault
- 1994 gemeinsames Projekt OSEK/VDX



OSEK und AUTOSAR

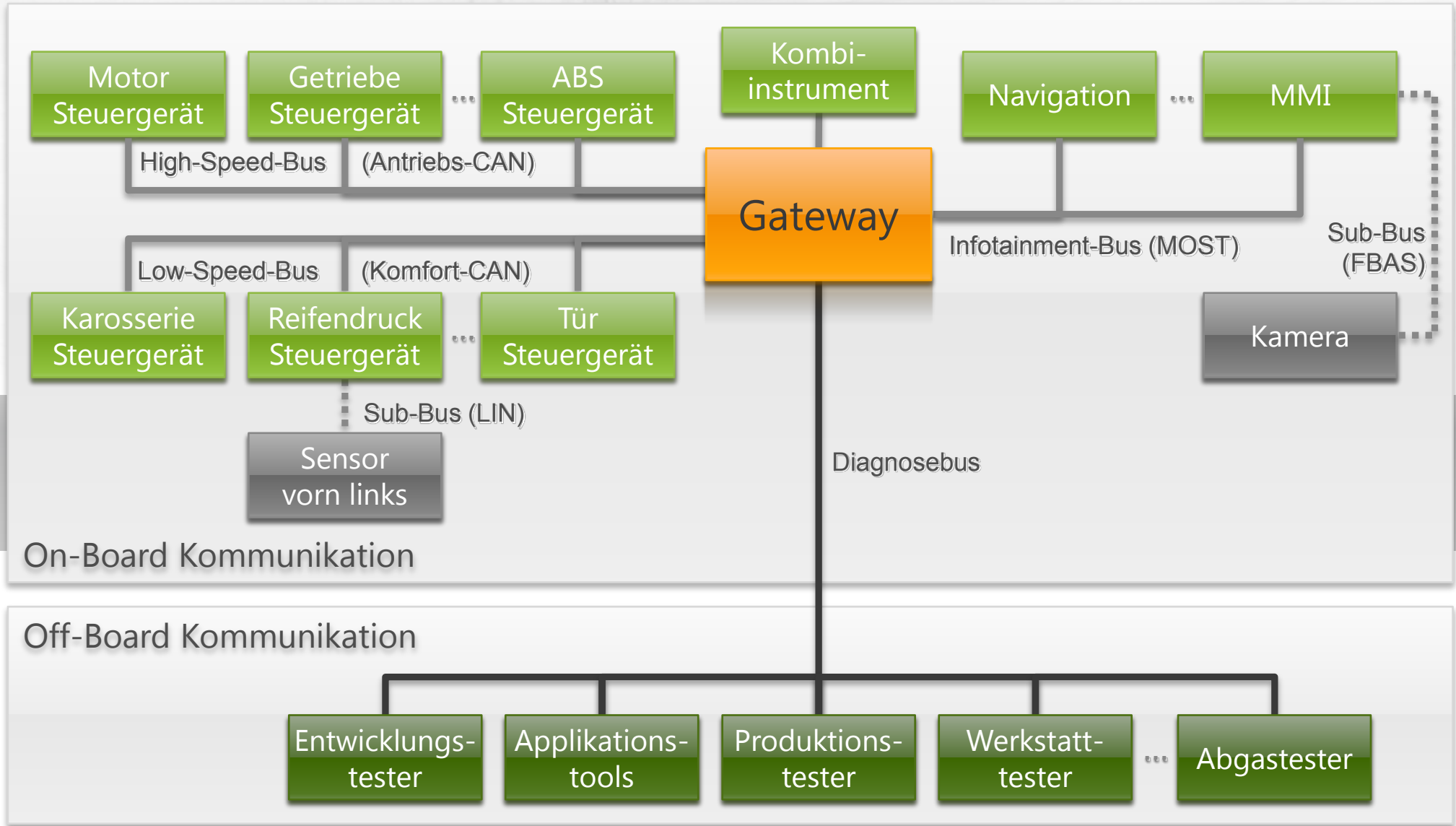
- Das AUTOSAR OS (OS) basiert auf einem OSEK-Betriebssystem mit zusätzlichen Funktionen
 - Speicherschutz
 - Deadline-Überwachung
 - Erweiterte Zähler
- Teil der Systemdienste (8 BSW-Module)



Klassifikation von Bussystemen mit Ergänzungen

Klasse	Übertragungsraten	Anwendung	Vertreter
Klasse A	Geringe Datenraten (bis 10 kBit/s)	Vernetzung von Aktoren und Sensoren	LIN, PSI5
Klasse B	Mittlere Datenraten (bis 125 kBit/s)	Komplexe Mechanismen zur Fehlerbehandlung, Vernetzung von Steuergeräten im Komfortbereich	Lowspeed-CAN
Klasse C	Hohe Datenraten (bis 1 MBit/s)	Echtzeitanforderungen, Vernetzung von Steuergeräten im Antriebs- und Fahrwerksbereich	Highspeed-CAN
	bis zu 15 MBit/s	Wie Klasse C, zusätzlich - Mehr ECUs / CAN - Schnellere Kommunikation über lange CAN	CAN FD (Flexible Data Rate)
Klasse C+	Sehr hohe Datenraten (bis 10 MBit/s)	Echtzeitanforderungen, (Sicherheitsanforderungen,) Vernetzung von Steuergeräten im Antriebs- und Fahrwerksbereich	FlexRay
Klasse D	Sehr hohe Datenraten (ab 10 MBit/s)	Vernetzung von Steuergeräten im Telematik- und Multimediabereich, MOST verliert an Bedeutung	MOST, Ethernet

Quelle: BOSCH: Kraftfahrtechnisches Taschenbuch, Vieweg+Teubner, 28. Auflage, 2014.



*vereinfacht

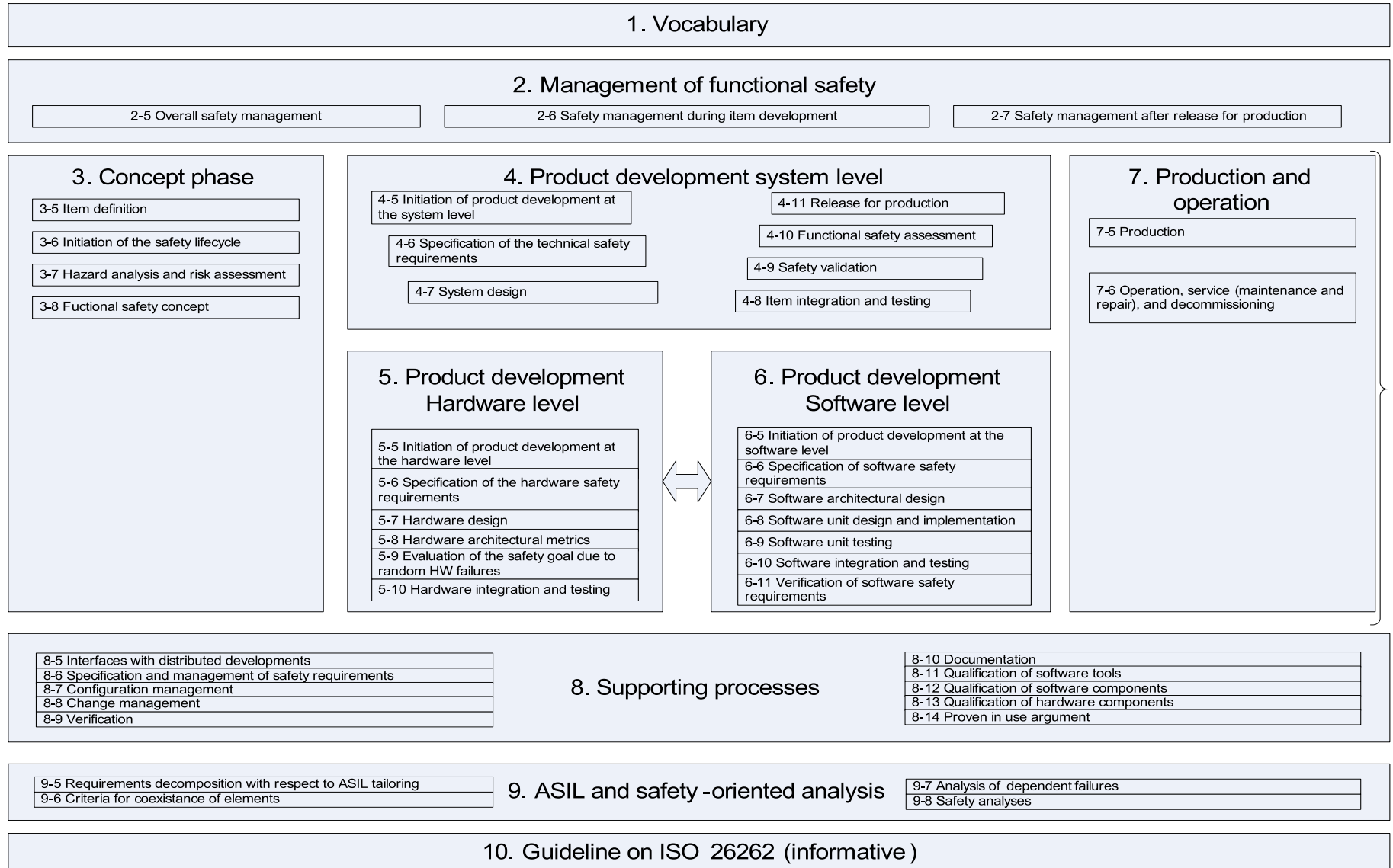
ISO 26262 Road vehicles - Functional safety

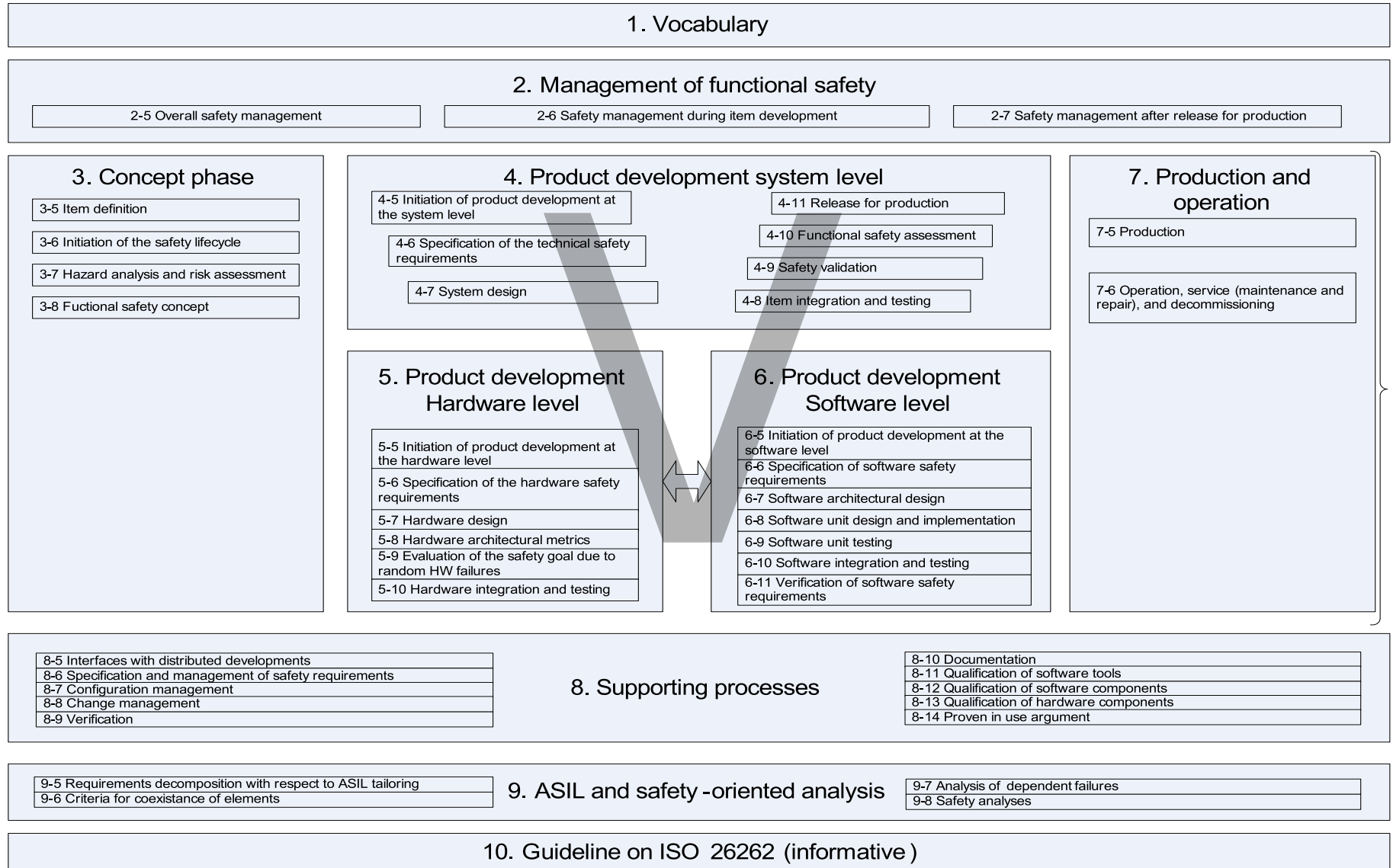
1. Vocabulary			
2. Management of functional safety			
3. Concept phase	4. Product development at the system level		7. Production and operation
	5. Product development at the hardware level	6. Product development at the software level	
8. Supporting processes			
9. ASIL-oriented and safety-oriented analyses			
10. Guideline on ISO 26262			

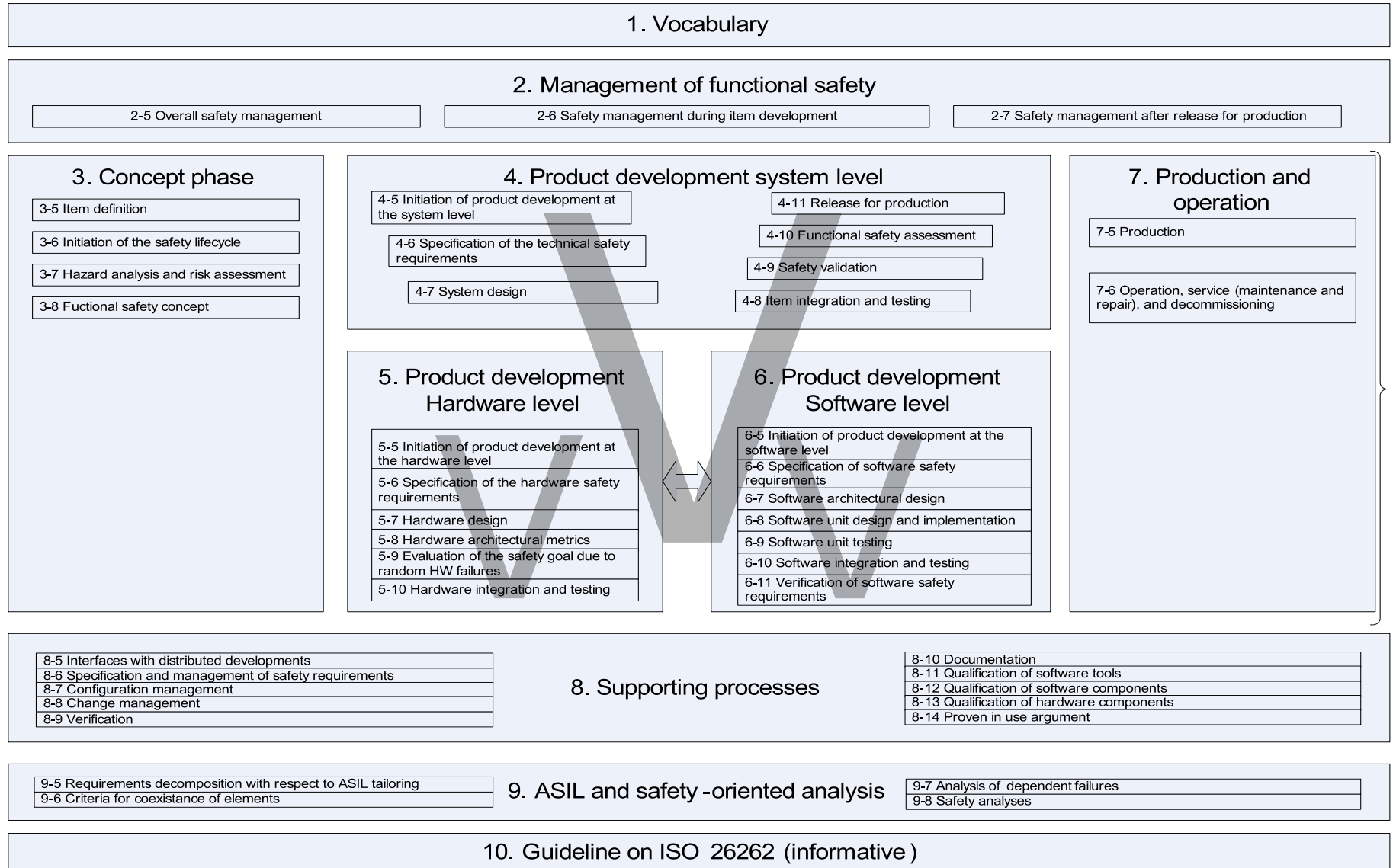
ISO 26262 Road vehicles - Functional safety

1. Vocabulary			
2. Management of functional safety			
3. Concept phase	4. Product development at the system level		7. Production and operation
	5. Product development at the hardware level	6. Product development at the software level	
8. Supporting processes			
9. ASIL-oriented and safety-oriented analyses			
10. Guideline on ISO 26262			

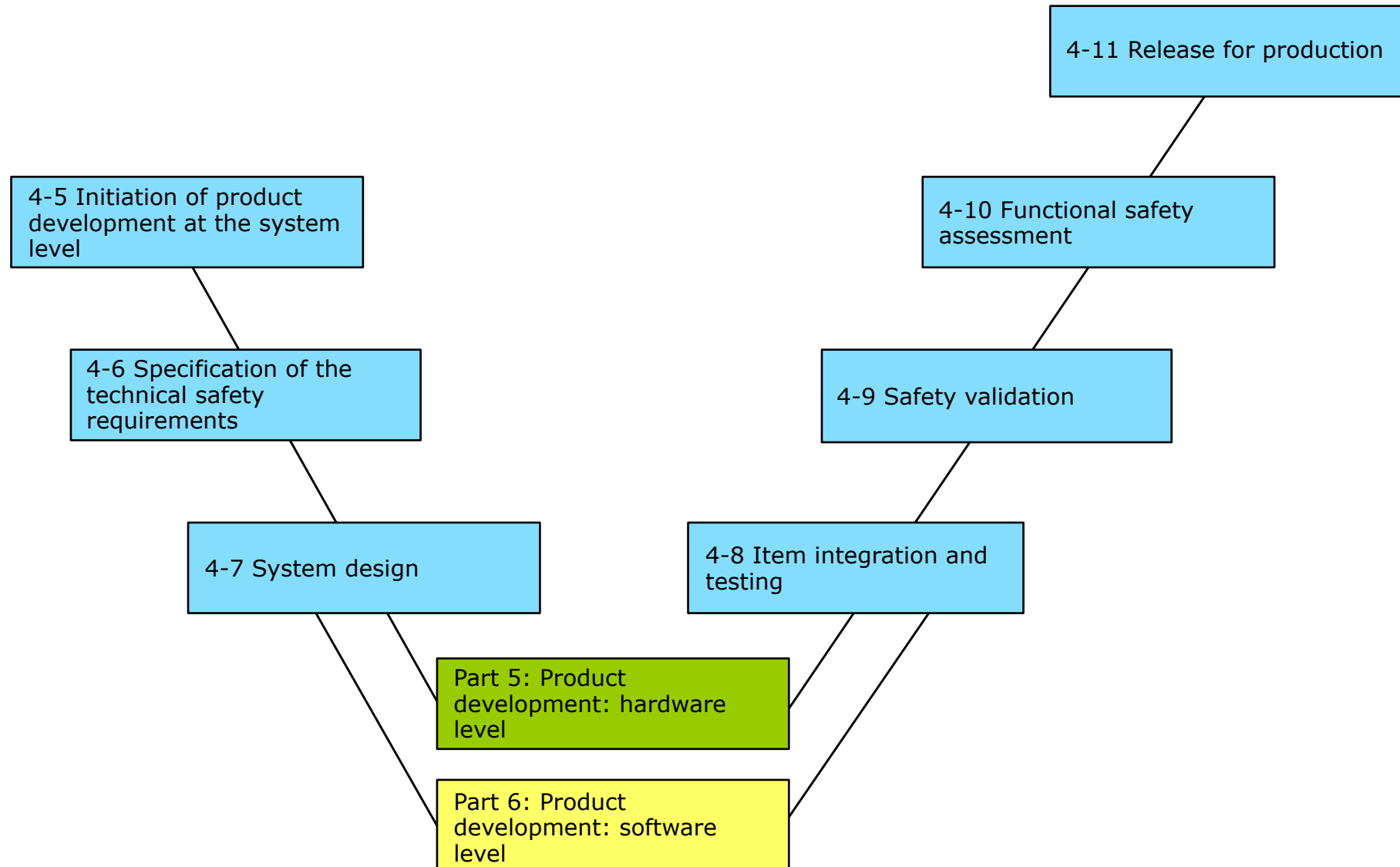
Normen sollten nicht nur vorhanden sein, sondern auch Gebrauchsspuren aufweisen



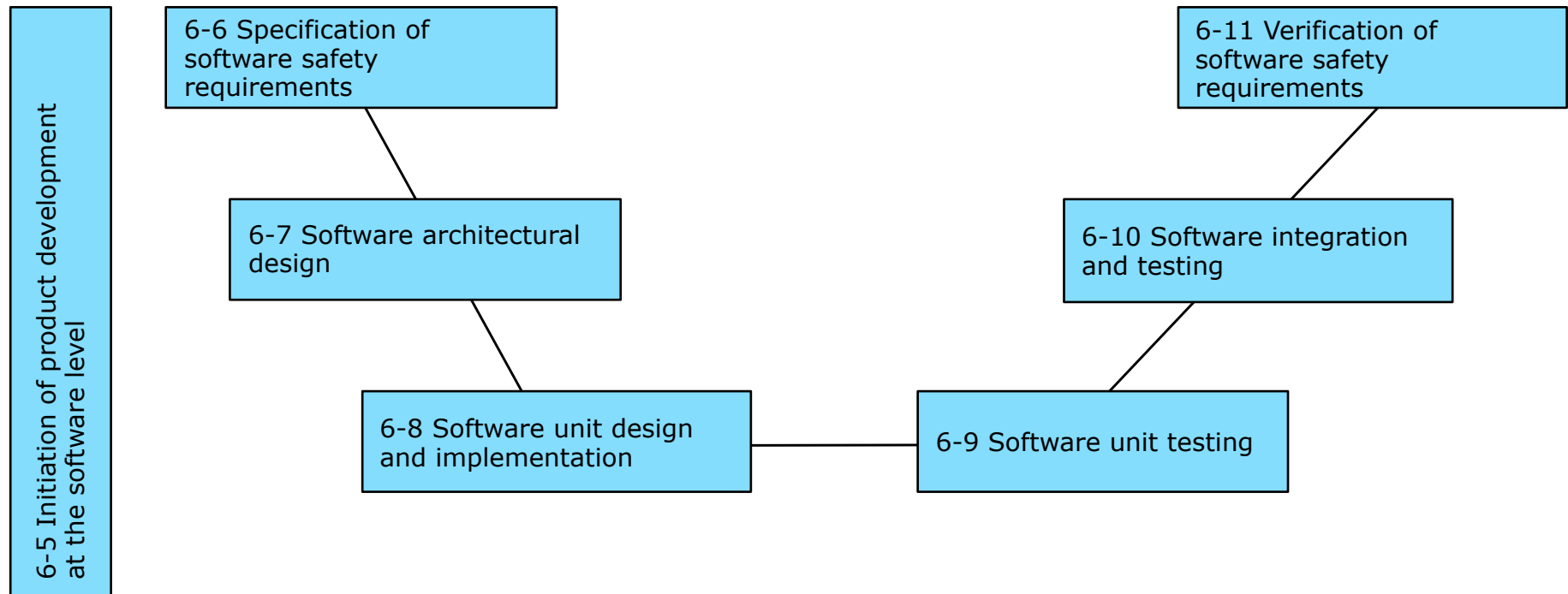




Part 4: Product development at the system level

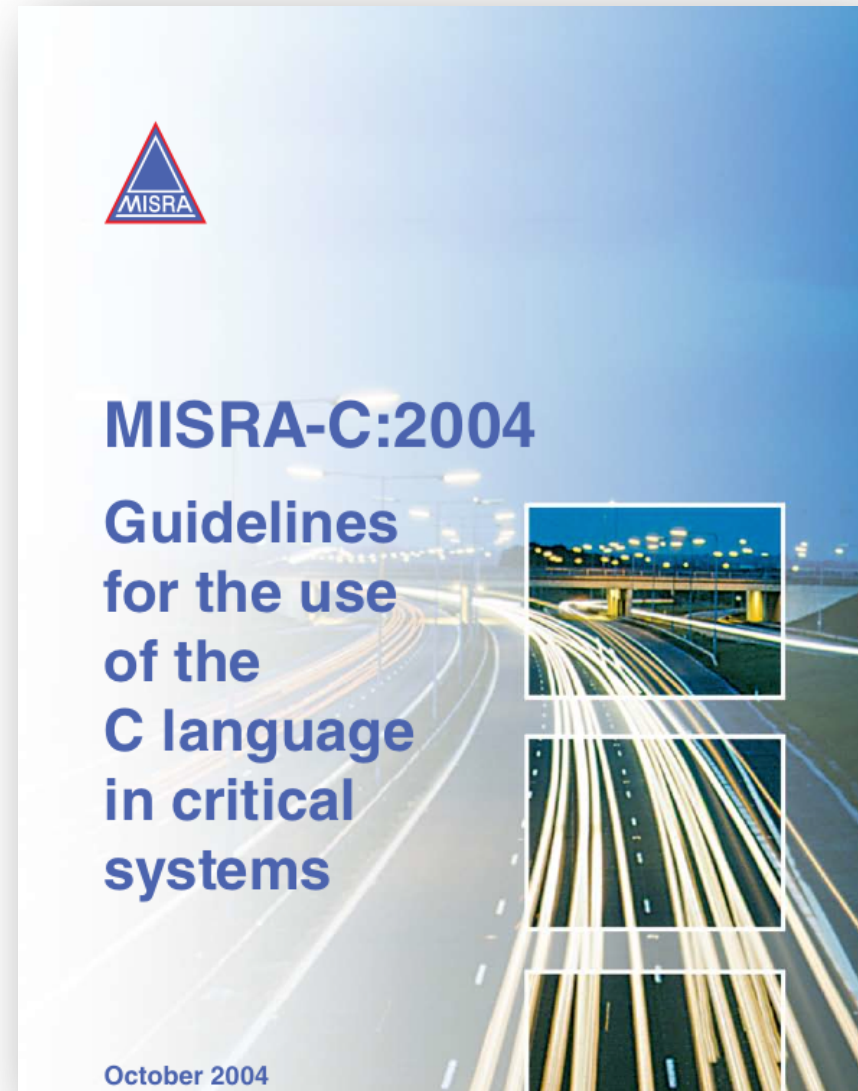


Part 6: Product development: software level



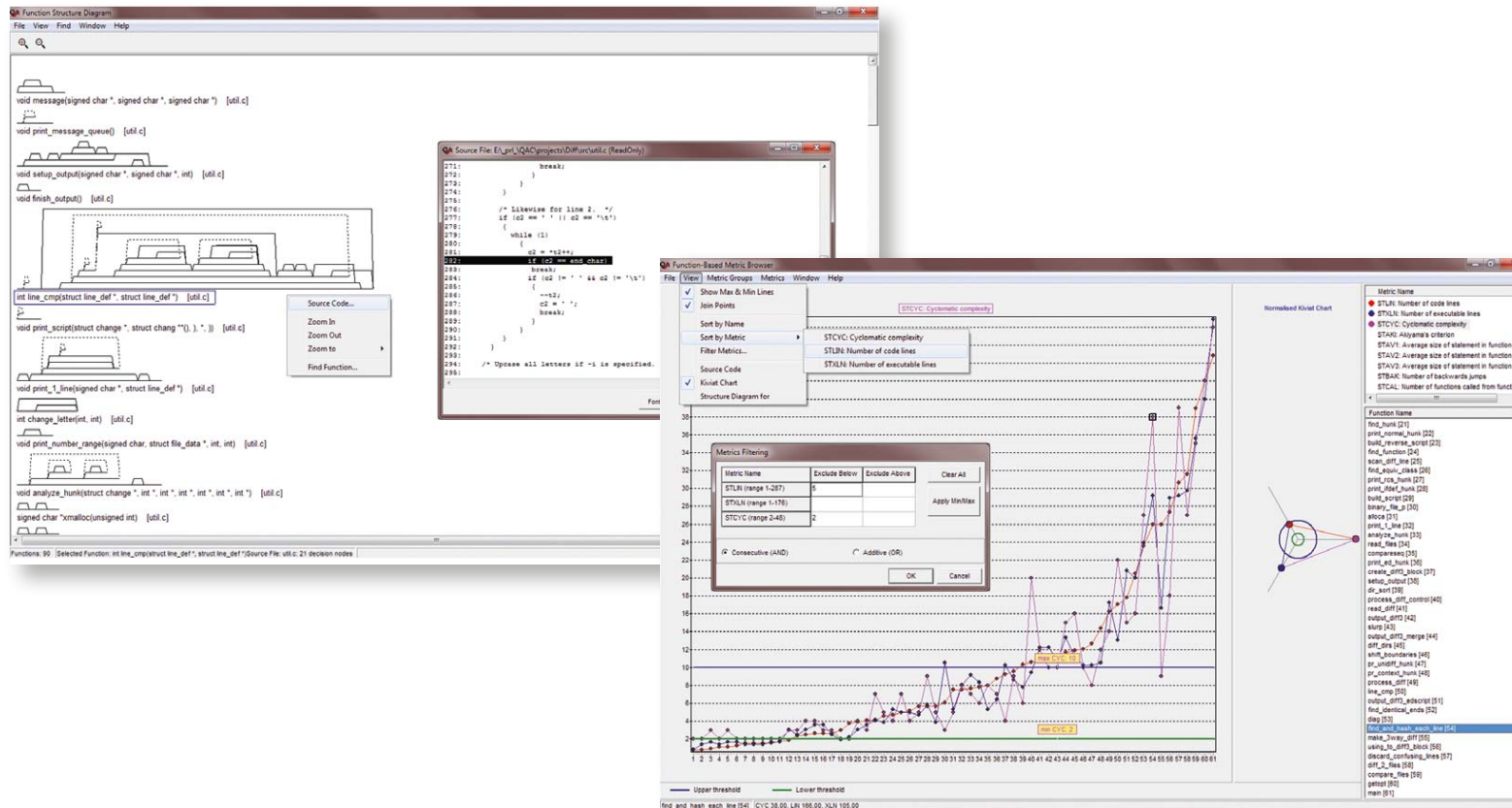
MISRA-C

- Viele firmeninterne und öffentliche Normen und Standards fordern die Anwendung von Entwurfs- und Codier-Richtlinien
- Für die Programmiersprache C ist MISRA-C de facto Standard
- MISRA
 - Motor Industry Software Reliability Association
 - Mission Statement: To provide assistance to the automotive industry in the application and creation within vehicle systems of safe and reliable software.
- Internet MISRA: www.misra.org.uk
- Internet MISRA-C: www.misra-c.com



MISRA-C: Werkzeugunterstützung

- Beispiel: QA-C: Statisches Sourcecode Analyse-Tool für C
 - QA Systems GmbH: www.qa-systems.de



The screenshot displays the QA-C tool interface with three main windows:

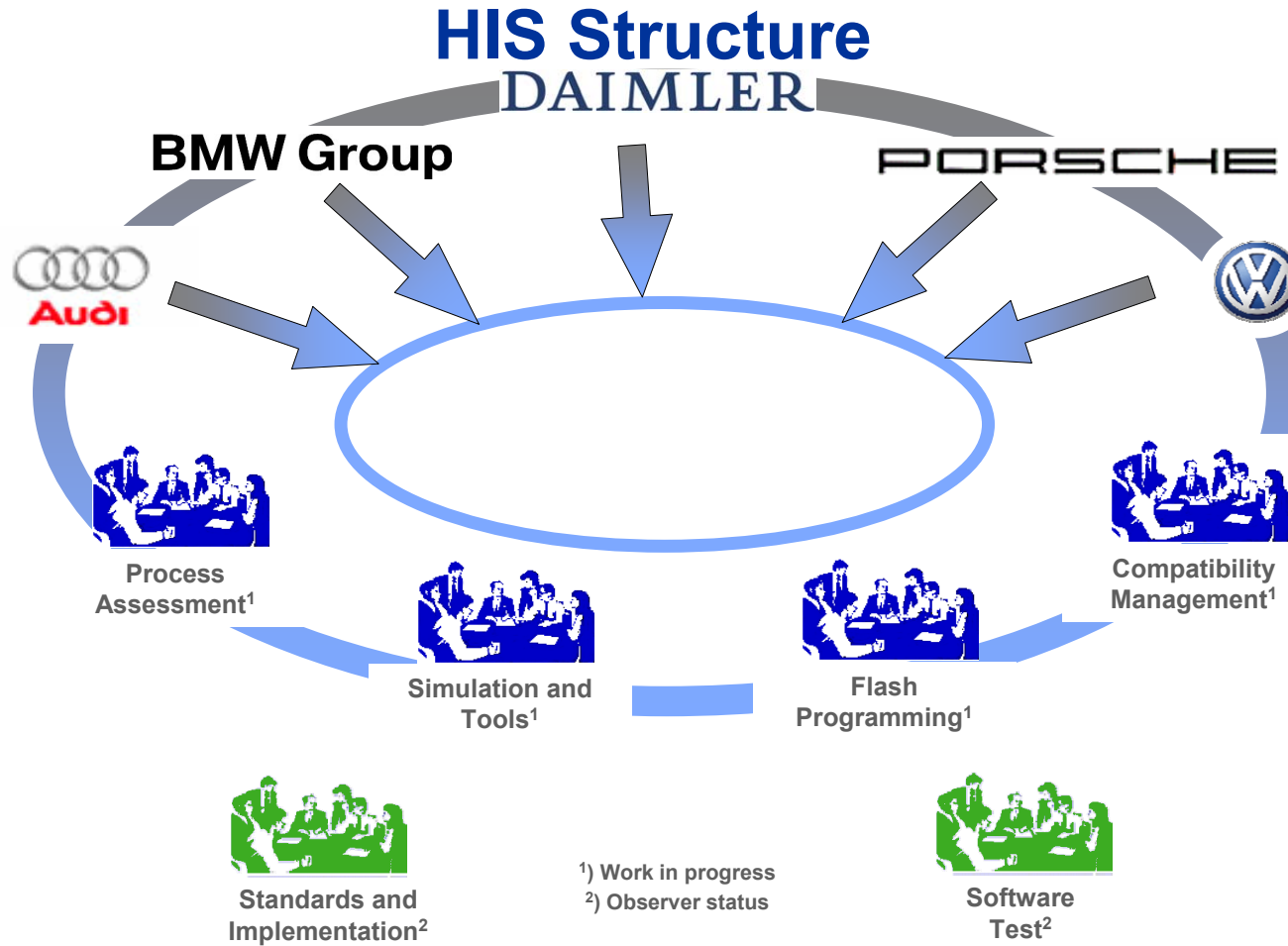
- Function Structure Diagram:** Shows a hierarchical tree of functions and their relationships. Functions listed include `void message`, `void print_message_queue`, `void setup_output`, `void finish_output`, `int line_cmp(struct line_def *, struct line_def *)`, `void print_script(struct change *, struct change **, *, *)`, `void print_line`, `int change_letter`, `void print_number_range`, `void analyze_hunk`, and `signed char xmalloc`.
- Source File:** Displays C source code for `DiffFunc.c`. Visible code includes:


```

                271:         break;
                272:     }
                273:     }
                274:     }
                275:     }
                276:     /* likewise for line 2. */
                277:     if (c2 == ' ' || c2 == '\n')
                278:     {
                279:         while (i)
                280:         {
                281:             c2 = next_char();
                282:             break;
                283:         }
                284:         if (c2 == ' ' || c2 == '\n')
                285:         {
                286:             ++i;
                287:             c2 = ' ';
                288:         }
                289:     }
                290:     }
                291:     }
                292:     }
                293:     }
                294:     /* Update all letters if -i is specified.
                295:     */
            
```
- Function-Based Metric Browser:** Shows a graph of metrics across code lines. A 'Metrics Filtering' dialog is open, showing:

Metric Name	Exclude Below	Exclude Above	Clear All
STLN (range 1-287)	5		Apply Metrics
STLN (range 1-176)			
STCYC (range 2-48)	2		

 The graph shows a sharp increase in metrics around line 30. A 'Normalized Kiviat Chart' on the right provides a circular comparison of metrics for various functions.

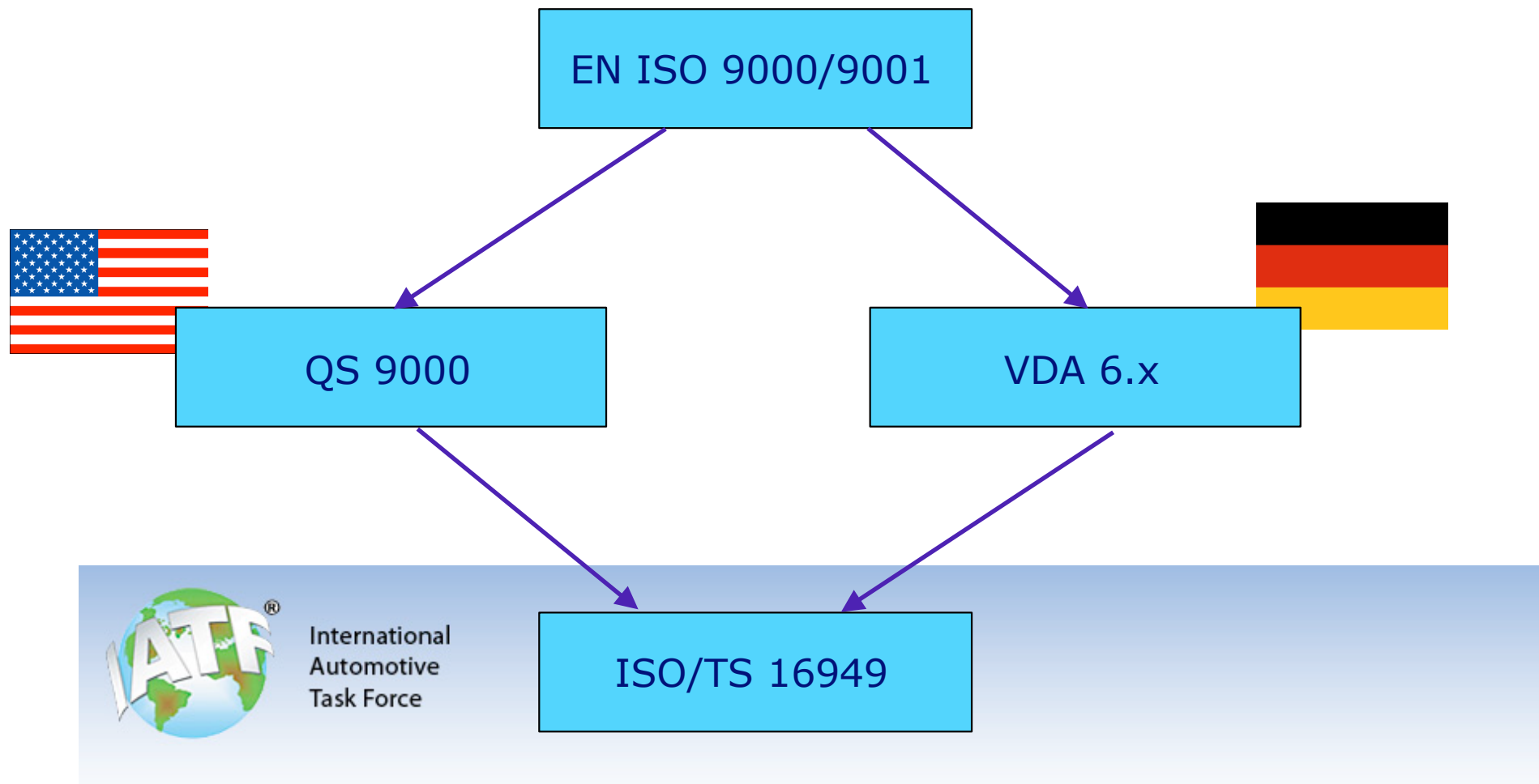


HIS - Herstellerinitiative Software

- <http://www.automotive-his.de>
- Aktivitäten
 - Standardsoftwaremodule für Netzwerke
 - Prozessreifegradermittlung
 - Softwaretest
 - Softwaretools
 - Programmieren von Steuergeräten
- Beteiligung an der Entwicklung von Standards
 - Automotive SPICE (Prozessreifegrad)
 - ASAM-Standardisierung (u.a. Diagnose, Kalibrierung)
 - The open Requirements Interchange Format (RIF)
 - EXERPT (RIF-Austauschwerkzeug für DOORS)
- Aussage HIS [HIS_PR07]:

The results of the standard software group are intermediate solutions. They are in use, but they are being extended by AUTOSAR; The standard software group is therefore currently inactive, the group members contribute actively to AUTOSAR.

Qualitätsstandards



ASAM

- ASAM - Association for Standardisation of Automation and Measuring Systems
- <http://www.asam.net>

6 | 2014

ASAM SOLUTIONS GUIDE

STANDARDS | MEMBERS | PRODUCTS

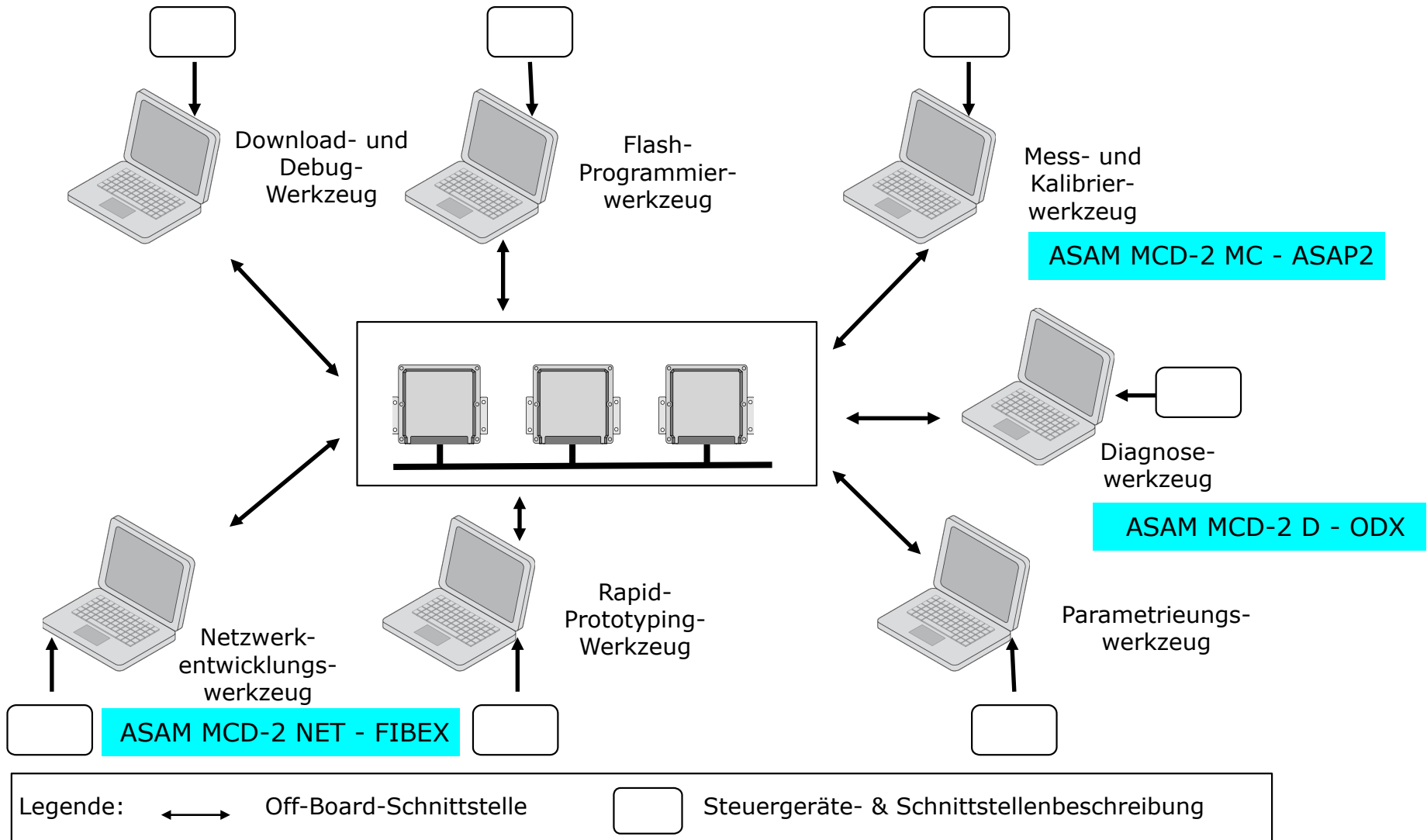
ASAM SOLUTIONS GUIDE



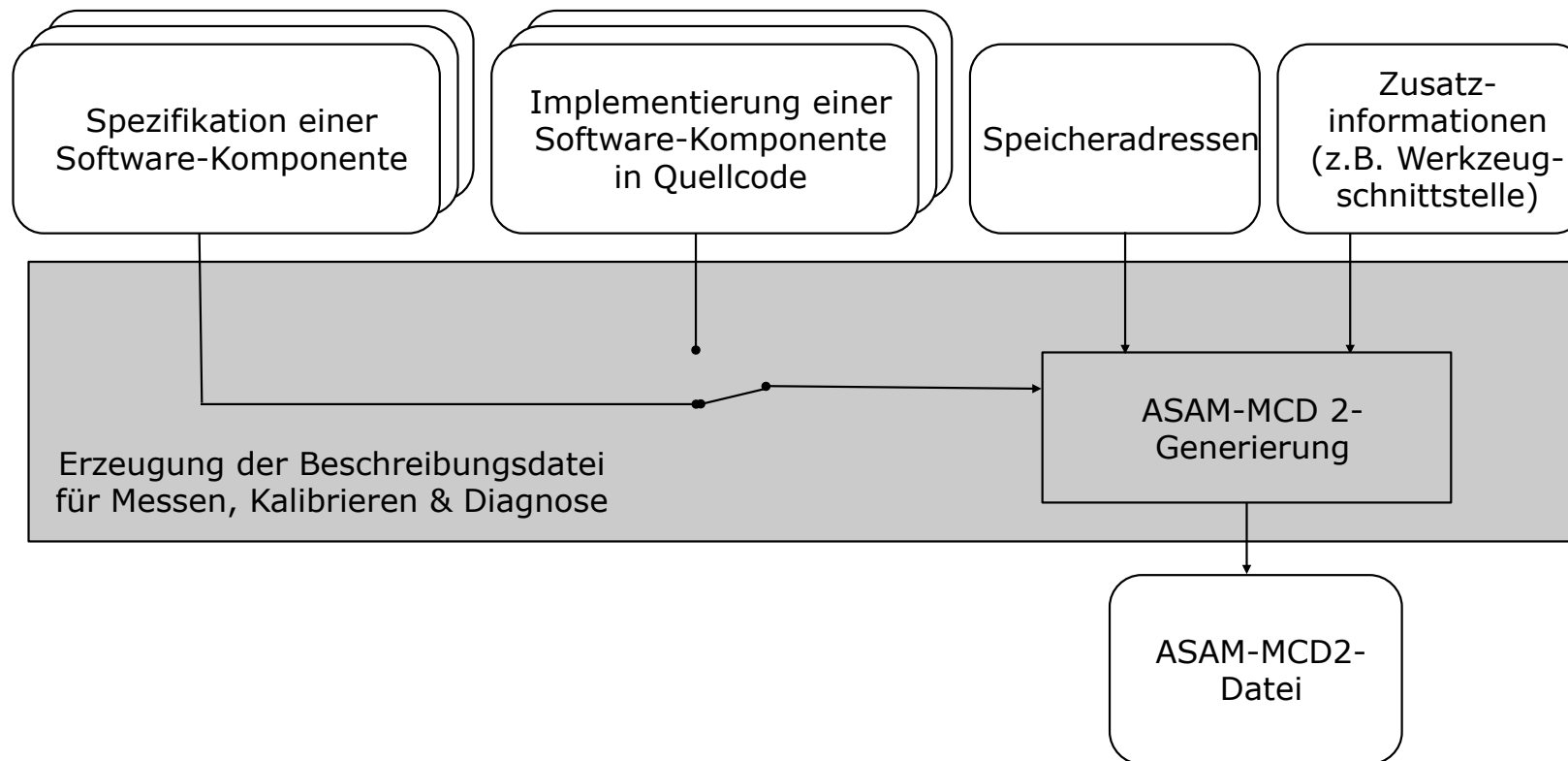
ASAM



Association for Standardisation of
Automation and Measuring Systems



Erzeugung der Beschreibungsdateien



Relevanz für die Automotive Domänen

Domäne	ISO 26262	AUTOSAR
Karosserie	+	++
Antriebsstrang	++	+
Fahrwerk	++	+
Telematik / Infotainment	-	-

Beispiel ESP bei Mercedes

- Entwickelt und geliefert von Bosch
- AUTOSAR
 - BSW von ETAS
 - Grundsätzlich bei Daimler: BSW gem. AUTOSAR 3.1 von Vector (Microsar)
- ISO 26262 - Alternativen
 - Entwickelt nach ISO 26262-4, -5 und -6 (system-, HW- und SW-Entwicklung)
 - Qualifiziert nach ISO 26262-8 (Unterstützungsprozesse, hier HW- und SW-Qualifizierung)
 - Entwickelt vor ISO 26262 (veröffentlicht Ende 2011) und damit nicht betroffen (wahrscheinlich)