DAIMLER

BMW

TÜV SÜD Auto Service

Mehr Sicherheit.
Mehr Wert.

© http://www.paleofuture.com/blog/2010/12/9/driverless-car-of-the-future-1957.html

Requirements on tools for assessment and validation of assisted and automated driving systems

7. Tagung Fahrerassistenz
25. – 26. November 2015, München

Udo Steininger, TÜV SÜD Auto Service
Dr. Hans-Peter Schöner, Daimler
Dr. Mark Schiementz, BMW

Agenda

Levels of driving automation according to SAE / BASt / NHTSA

(SAE report J3016)

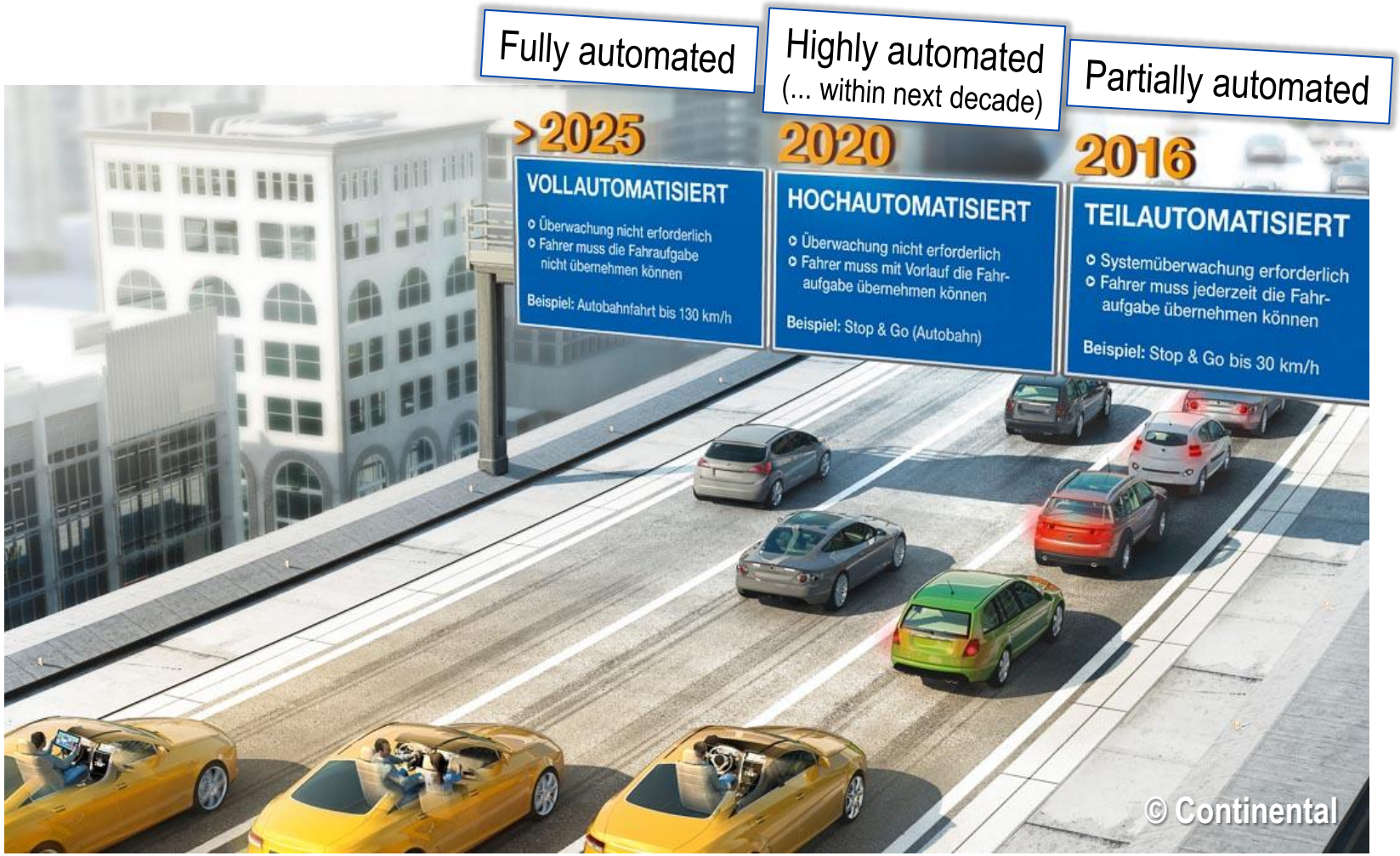
Level	Name	Narrative definition	Execution of steering and acceleration/ deceleration	Monitoring of driving environment	Fallback performance of *dynamic driving task*	System capability (*driving modes*)	BASt level	NHTSA level
***Human driver* monitors the driving environment**								
0	**No Automation**	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a	Driver only	0
1	**Driver Assistance**	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes	Assisted	1
2	**Partial Automation**	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes	Partially automated	2
***Automated driving system* ("system") monitors the driving environment**								
3	**Conditional Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task* with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes	Highly automated	3
4	**High Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes	Fully automated	3/4
5	**Full Automation**	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**	-	

VDA roadmap for introduction of assistance and automation

	Driver is always in the loop and monitors environment.			System monitors environment, driver is (temporarily) out of the loop.		
n.a.						Robot taxi
Automation 2nd gen.				Highway pilot	Parking garage pilot	
Automation 1st gen.				Highway congestion pilot		
New DAS		Eco ACC, Work site assistant	Congestion assistant, Park assist.			
Established DAS	LCA, PDC, LDW, FCW	ACC, S&G, PSA, LKA				
	Driver only (0)	Assisted (1)	Partially automated (2)	Highly automated (3)	Fully automated (4)	Driverless (5)

LCA: Lane Change Assistant
LDW: Lane Departure Warning
ACC: Adaptive Cruise Control
PSA: Park Steering Assistant
PDC: Park Distance Control
FCW: Forward Collision Warning
S&G: ACC incl. Stop & Go
LKA: Lane Keeping Assistant

Time table


Fully automated
Highly automated
(... within next decade)
Partially automated
>2025
VOLLAUTOMATISIERT
Überwachung nicht erforderlich
Fahrer muss die Fahraufgabe nicht übernehmen können
Beispiel: Autobahnfahrt bis 130 km/h
2020
HOCHAUTOMATISIERT
Überwachung nicht erforderlich
Fahrer muss mit Vorlauf die Fahraufgabe übernehmen können
Beispiel: Stop & Go (Autobahn)
2016
TEILAUTOMATISIERT
Systemüberwachung erforderlich
Fahrer muss jederzeit die Fahraufgabe übernehmen können
Beispiel: Stop & Go bis 30 km/h
© Continental

Agenda

Passive vs. active safety

- Assessment and validation of *passive safety* based on a practicable number of crash tests under well defined worst case conditions is well established and widely accepted

- In contrast testing of *active safety* systems is limited by
  - huge number of relevant scenarios and environmental conditions
  - complexity of systems and variability of driver behaviour
  - methodological aspects (functional deficiencies)

Customer's protection

- EuroNCAP, e.g., has a road map for assessment of active safety systems

- Tests are useful for comparison of systems from customer protection's point of view (no driver intervention considered)

- They are only limited applicable for system development and validation because they do not represent real scenarios, environments and driver behaviour

Functional safety

- Systems for highly automated driving have to fulfil very high functional safety requirements, e.g. random hardware failure rates < 10^{-8} / h for ASIL D

- Besides before mentioned methodo-logical limitations it is not possible
  - to prove those failure rates by conventional road tests with reasonable effort and
  - to prove completeness of tests considering very rare events in general

ISO 26262 ASIL Determination		Exposure	Controllability		
			C1	C2	C3
Severity	S1	E1	QM	QM	QM
		E2	QM	QM	QM
		E3	QM	QM	A
		E4	QM	A	B
	S2	E1	QM	QM	QM
		E2	QM	QM	A
		E3	QM	QM	B
		E4	A	B	C
	S3	E1	QM	QM	A
		E2	QM	A	B
		E3	A	B	C
		E4	B	C	D

Regulation

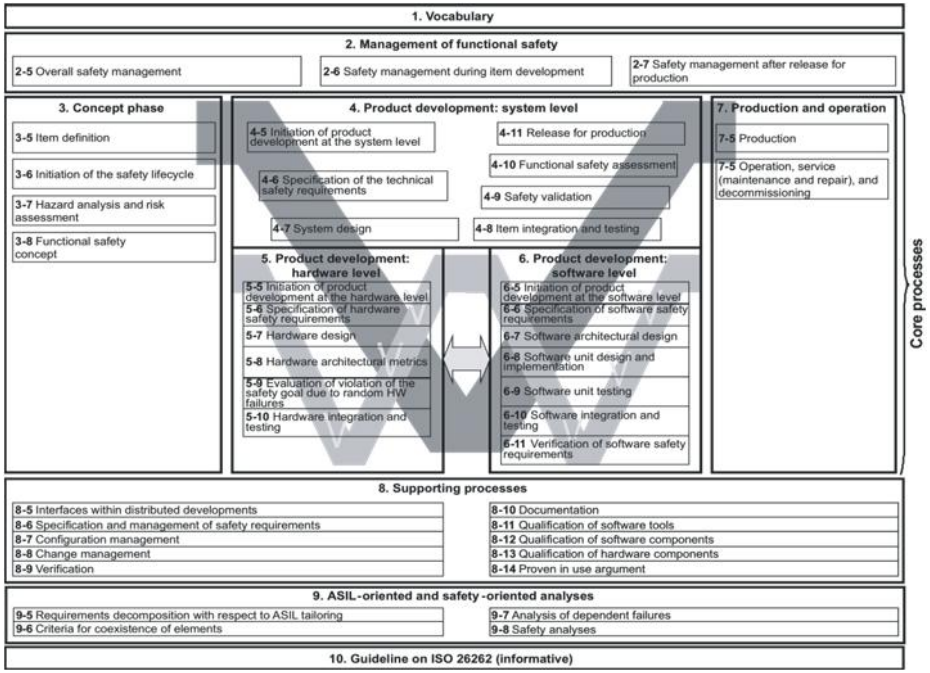
- European type approval for passenger cars, e.g., based on 2007/46/EC and ECE-Regulations 13 & 79 with so called electronic annexes

- Requirement: No influence of E/E systems on mechanical braking and steering functions

- Not focused on DAS, but sufficient as long as systems are fully controlled by driver in every situation according to 1968 Vienna Convention on Road Traffic (VC 68)

With increasing level of automation, we will reach a point, where those regulations are not longer sufficient → ECE-R13 & 79 are under revision

Standardisation



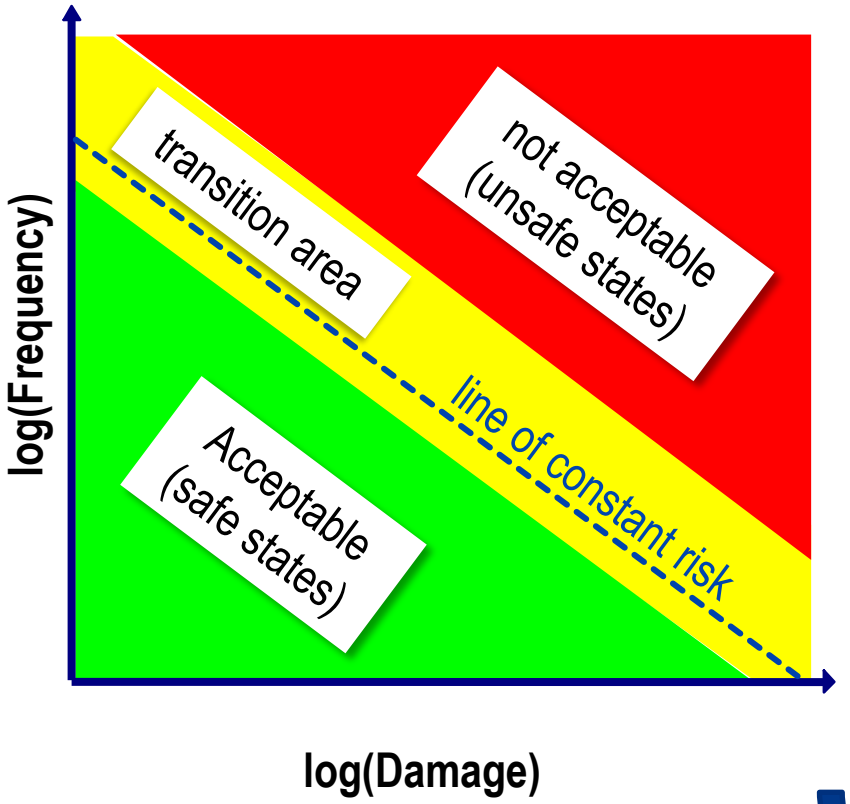
- Product safety confirmation based on ISO 26262 for functional safety of E/E systems in road vehicles
- Applicable for DAS in general and sufficient for established systems
- Limitations: ISO 26262 doesn't cover functional disabilities, for example misinterpretation of objects / traffic situations and resulting false positive system interventions

With increasing level of automation, upgrade of functional safety standard seems to be necessary → also ISO 26262 is under revision

Agenda

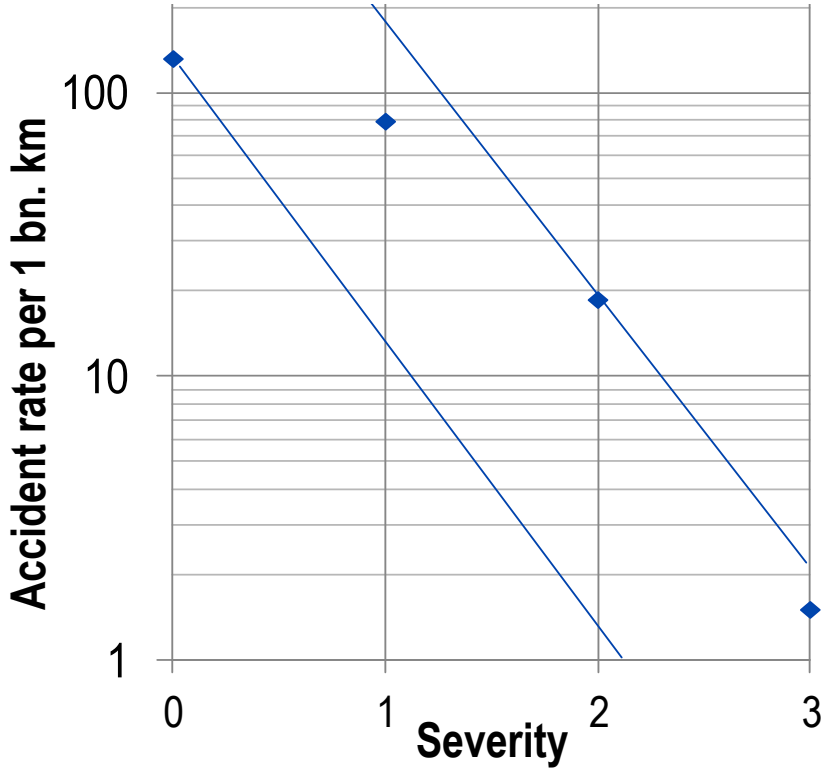
Basis: General accepted safety requirements and risk criteria

General approach: Risk = Frequency x Damage



Accident statistics on German „Autobahn“

With assumption, that there is 1 order of magnitude between severity levels according to ISO 26262:



Sources: H.-P. Schöner, CESA 2014, and DESTATIS (German Federal Statistics Agency) 2013

Approach for assessment and validation

- Systems have to be able to control scenarios → therefore an integral, scenario based approach is necessary

- taking into account different test levels like
  - virtual testing
  - proving ground tests
  - field tests

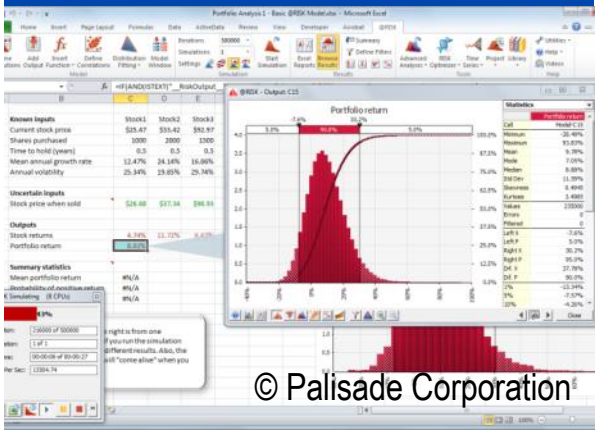
  in an adequate way

- sufficient for partial + high automation

- applicable
  - in the system development process as well as
  - for assessment and validation in frame of type approval and confirmation of product safety

Characteristics of test levels

Virtual tests



☑ Analysis of a huge number of scenarios, environments, system configurations and driver characteristics

Proving ground tests

☑ Reproducibility by use of driving robots, self driving cars and targets; critical manoeuvres are possible

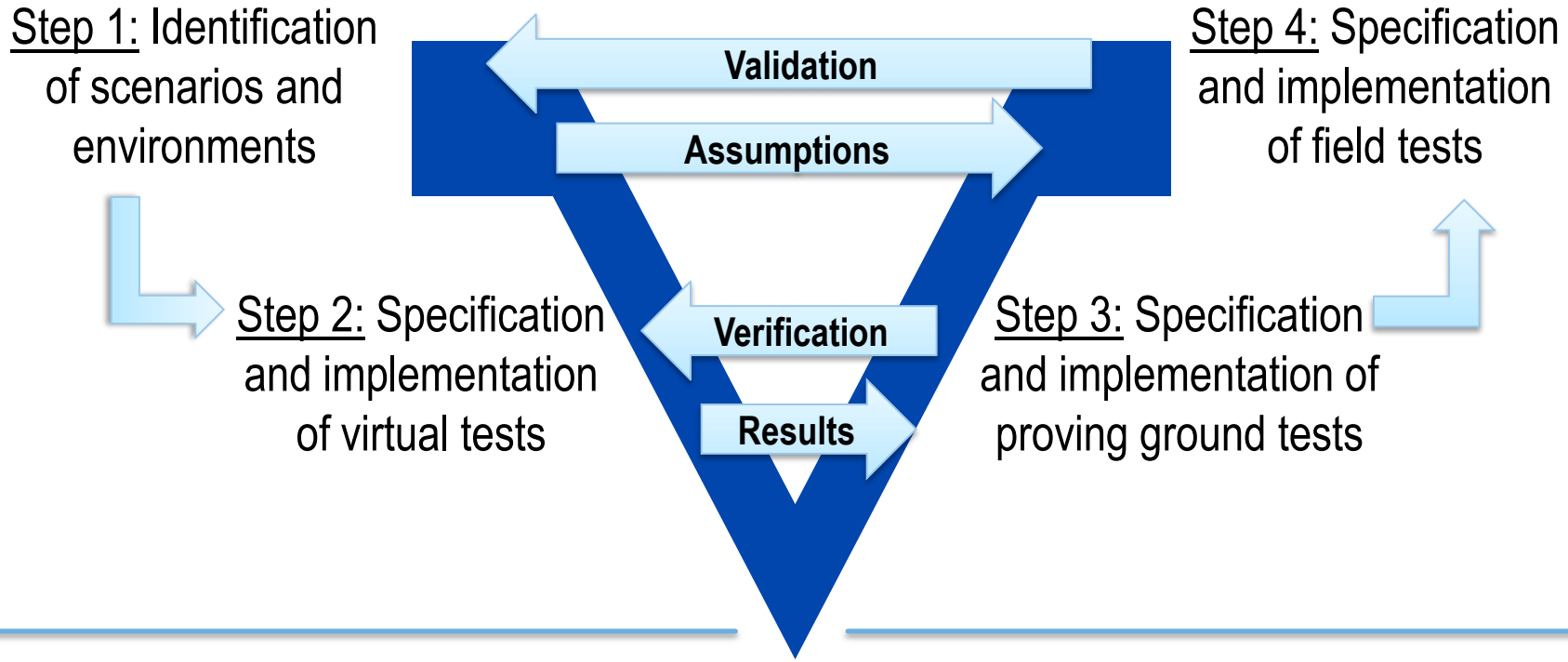
Field tests

☑ Investigation of real driving situations and comparison with system specifications

Effort for coverage of all relevant scenarios & environments

Uncertainties & simplifications

Test process according to V model of HW & SW development



Verification: Have I done things right?

…means to check whether proving ground tests confirm virtual tests

Validation: Have I done the right things?

…means to check whether field tests confirm scenarios and environments

Validation plan

… should include amongst others:

- Requirements
  - derived from scenarios and requirements (step 1)
  - taking into account results from virtual tests (step 2) and proving ground tests (step 3)
  - include confirmation, how system fulfills these requirements

- Acceptance criteria to confirm that system meets defined requirements (confirmation of scenarios and environments ←→ driven km, time)

© Nunforest 2014

Comparison with other approaches

Scenario based approach

- Integral approach with focus on use cases / entire system (instead of km or time ←→ rare events)
- Applicable in system development as well as in type approval and confirmation of product safety
- High effort for adaptation to different systems specifications / degrees of automation and resulting use cases / scenarios

System based approaches

- Decomposition: Confirmation of reliability / safety by system architecture (redundancy, diversity) → high potential because several sensors and sensor types are used in every application
- Probabilistic approaches: e.g. Fault Tree Analysis → very useful for system understanding / limitations
- Stochastic approaches: Road tests versus proven in use → some potential because of incremental increase of automation

Conclusion: Combination of different approaches can be helpful / necessary!

Agenda

Scenarios and requirements

Goals

- find all relevant (even rare) possibly critical incidents
- consider the identification of system limitations
- specify test cases

Tools

- Systematic procedure is necessary, e.g.
  - Hazard Analysis and Risk Assessment
  - Event Tree Analysis
  - Fault Tree Analysis

Challenges

- Generally accepted safety requirements and scenarios
- Reduction of test cases to a significant and sufficiently complete set

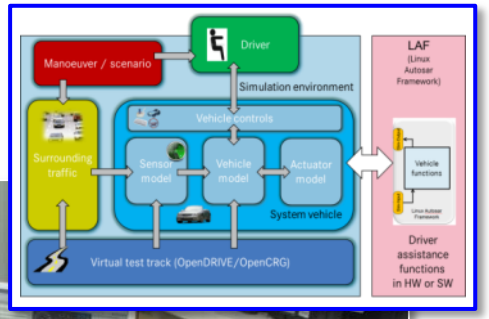
Virtual Tests

Goals

- Cover a large number of different test cases
- Combine base events to establish rare situations

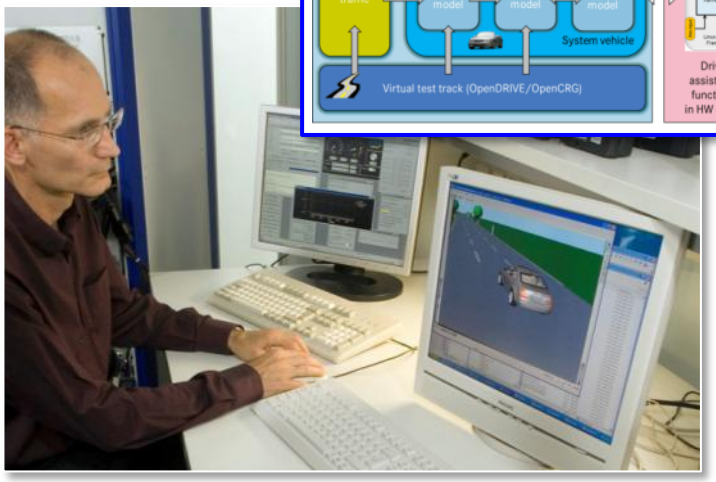
Tools

- Test benches for MIL / SIL / VIL / HIL
- Simulation models for all relevant components



Challenges

- Importance of sensor and driver models (= interfaces to real world complexity)
- Perform a sufficiently dense coverage of the test state space



Proving ground tests

Goals

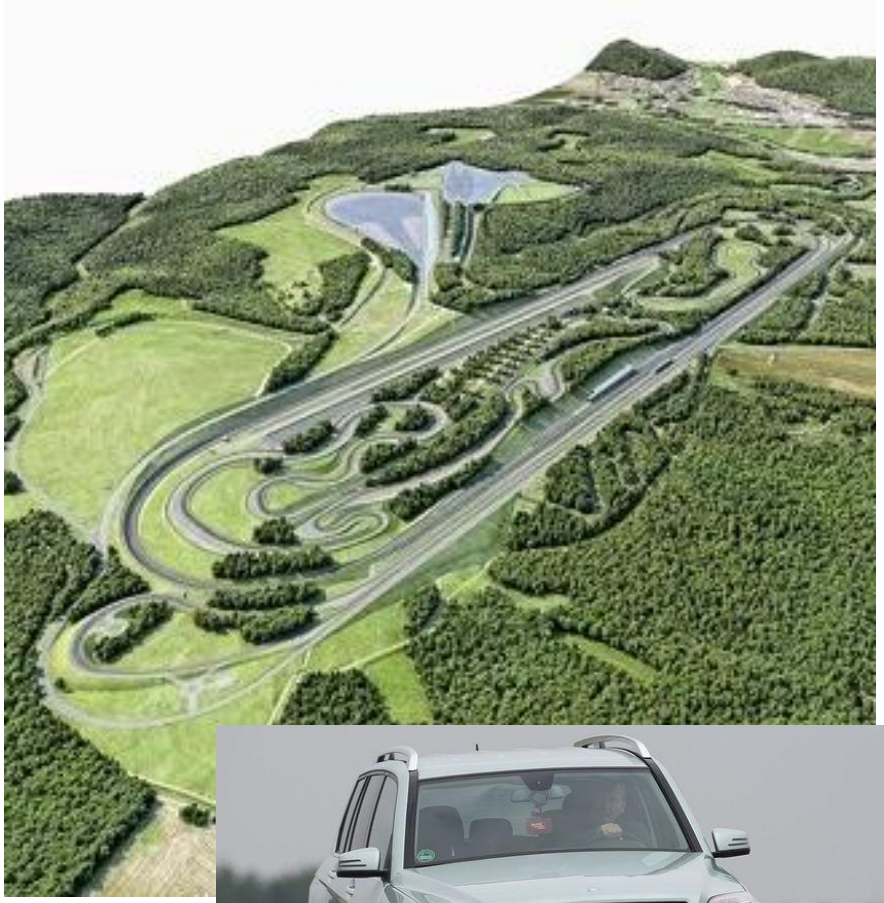
- Verify reference scenarios of the virtual tests
- Test of situations, which are unlikely to meet in field tests and which are hard to simulate
- Test of safety critical manoeuvres along the system limitation

Tools

- Reproducibility and accuracy by use of driving robots, self driving cars and targets for high statistical confidence level

Challenges

- Tool set to perform even critical tests



Field tests

Goals

- Validation of statistical probability of relevant situations or events
- Verification of automatic recognition of system limitations in field operation
- Safe handling of functional deficiencies of system components in random situations
- Interaction of drivers with the system

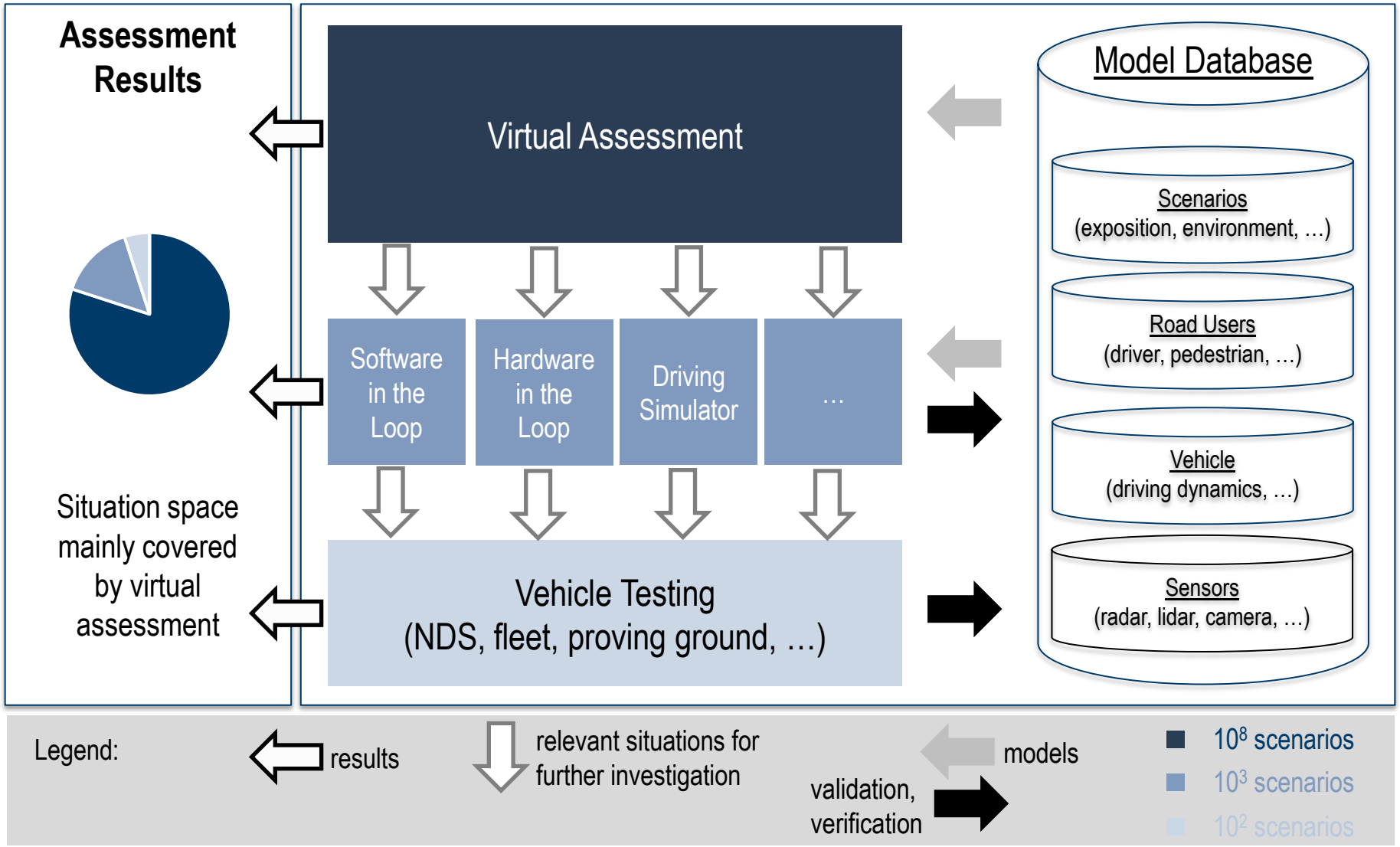
Tools

- Test vehicles with reference measurement equipment

Challenges

- Duration of field tests or indicators for sufficient test coverage
- …

Consolidation of results

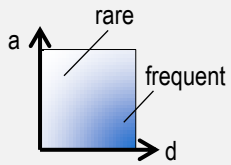


Agenda

System design – general approach

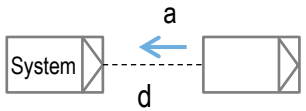
Verification and validation at the end of the process requires careful specification in the early system design phase

Investigation of properties of the system environment:
Basis for system design

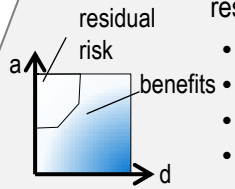


typical behaviour and parameters of
- infrastructure, traffic, environment
- sensors, actuators
- drivers

Illustration for example:

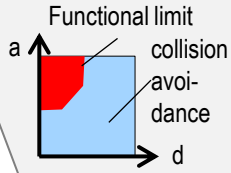


Validation: Assessment of implementation with respect to desired functionality



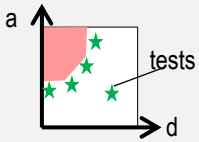
- Confirmation of design assumptions
- Confirmation of risk assessment
- Examination of retroactive effects
- Safety in use, customers' benefits and acceptance

System design: specification of system performance



- Risk assessment & management
- Functional limitations
- Functional requirements including fault management
- Define performance criteria and tests

Verification: Comparison of implementation with respect to design specification



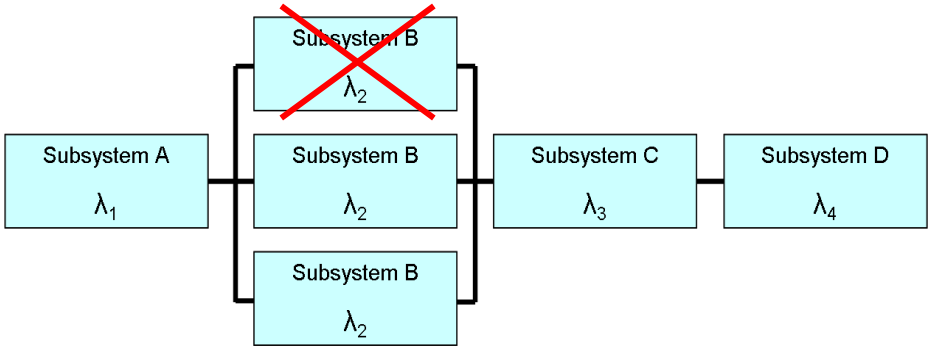
- Perform system tests
- Evaluate test coverage

Implementation

Functional decomposition of complex systems

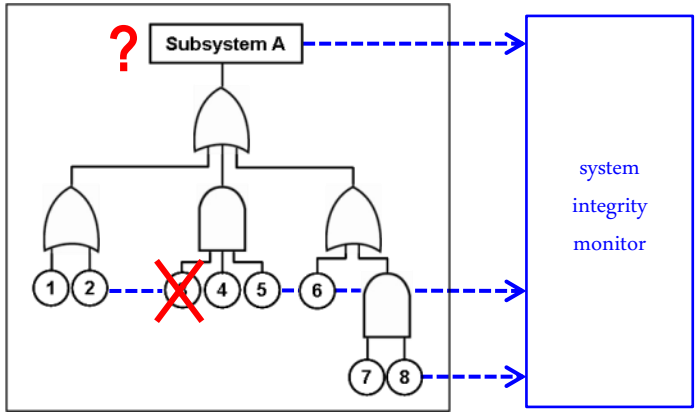
Design for high reliability:

- Redundant, self monitoring components
  - ➢ fault tolerant system design
- Diverse components
  - ➢ avoid common mode (correlated) faults
- Fault tree analysis
  - ➢ avoid systematic errors
- Derive system failure rate by mathematical model



$$\lambda_{total} = \lambda_1 + (\lambda_2)^3 + \lambda_3 + \lambda_4$$

(only if all subsystems are uncorrelated !)



Type approval and product safety confirmation

- Range (i.e. number of relevant scenarios and environments) and level of detail (number of influence parameters, complexity of tests) of approvals and confirmations
  - depend on certain system specification and
  - increase with level of automation

- Next generation of partially automated systems (e.g. congestion and park assistants) are entering the market and will provide further field experience under drivers' supervision

- BMVI has installed "FKT-Sonderausschuss Fahrerassistenzsysteme" to identify necessary changes within ECE-R13 and 79

- Because highly automated systems will be introduced within next decade, there is still some time for type approval and product safety confirmation, but
  - manufacturers and system developers need to know requirements in early development states and
  - public discourse about benefits and risks of highly automated driving is necessary

Next steps

- Achieve common understanding of authorities, test labs, notified bodies, manufacturers, system developers, scientific institutes ...
- Detailed development and test of general approach and all parts of tool chain
- Preparation of national / international legislation and standardisation
- For this purpose some national and international projects have been started or are in preparation, respectively

Contact and acknowledgement

Udo Steininger	Dr. Hans-Peter Schöner	Dr. Mark Schiementz
Assisted and Automated Driving TÜV SÜD Auto Service GmbH Business Unit Automotive 85748 Garching Daimlerstraße 13 Phone: +49 89 32950-631 Mobile: +49 160 360 1992 udo.steininger@tuev-sued.de	Leiter Fahrsimulatoren, Werkstätten & Erprobung Daimler AG - Forschung und Vorentwicklung Fahrerassistenz- und Fahrwerksysteme 71059 Sindelfingen Phone: +49-7031-90-74704 Mobile: +49-160-862 2615 hans-peter.schoener@daimler.com	Fahrdynamik und Fahrerassistenz Applikation und Systemversuch BMW Group 80788 München Phone: +49-89-382-35903 Mobile: +49-151-601-35903 mark.schiementz@bmw.de

The authors thank Horst Mock and Axel Blumenstock, Daimler, and Thomas Ziegler, TÜV SÜD, for contributions to this lecture and helpful suggestions.

Picture credits (if not otherwise denoted): BMW, Daimler, TÜV SÜD