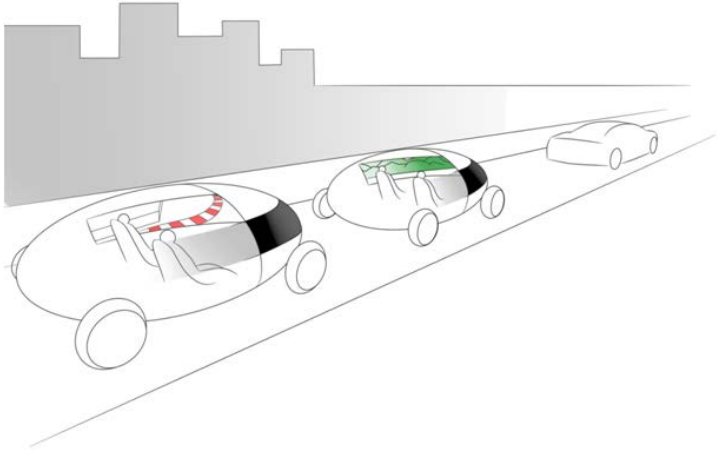
TECHNISCHE UNIVERSITÄT DARMSTADT



Prof. Dr. rer. nat. Hermann Winner

Dipl.-Ing. Walther Wachenfeld

Philipp Junietz, M.Sc.

Safety Assurance for Highly Automated Driving – The PEGASUS Approach

FZD

Considered Levels of Automated Driving

TECHNISCHE UNIVERSITÄT DARMSTADT

Highly Automated Driving:

- **according to definition of BASt level 3 and**
- **VDA level 3: Conditional Automation**
- **NHTSA level 3: Limited Self-Driving Automation**
- **SAE level 3: Conditional Automation**

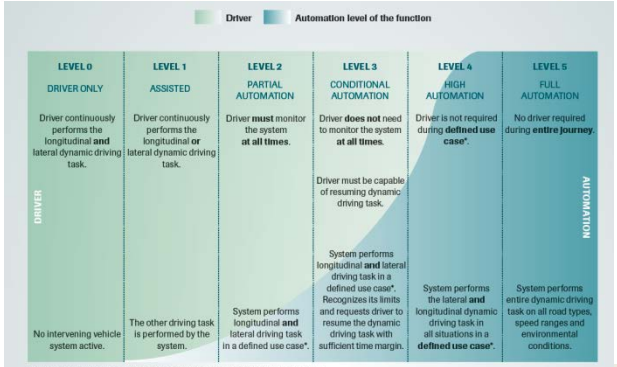
Interpretation:

- **No responsibility of human drivers (operators) during operation of automation, but the automation may shift back the driving task towards human in a reasonable transition time.**

Nomenklatur	Fahraufgaben des Fahrers nach Automatisierungsgrad
Vollautomatisiert	Das System übernimmt Quer- und Längsführung vollständig in einem definierten Anwendungsfall • Der Fahrer muss das System dabei nicht überwachen • Vor dem Verlassen des Anwendungsfalles fordert das System den Fahrer mit ausreichender Zeitreserve zur Übernahme der Fahraufgabe auf • Erfolg dies nicht, wird in den risikominimalen Systemzustand zurückgeführt • Systemgrenzen werden alle vom System erkannt, das System ist in allen Situationen in der Lage, in den risikominimalen Systemzustand zurückzuführen
Hochautomatisiert	Das System übernimmt Quer- und Längsführung für einen gewissen Zeitraum in spezifischen Situationen • Der Fahrer muss das System dabei nicht überwachen • Bei Bedarf wir der Fahrer zur Übernahme des Fahraufgabe mit ausreichender Zeitreserve aufgefordert • Systemgrenzen werden alle vom System erkannt. Das System ist nicht in der Lage, aus jeder Ausgangssituation den risikominimalen Zustand herbeizuführen
Teilautomatisiert	Das System übernimmt Quer- und Längsführung (für einen gewissen Zeitraum oder/und in spezifischen Situationen) • Der Fahrer muss das System dauerhaft überwachen • Der Fahrer muss jederzeit zur vollständigen Übernahme der Fahrzeugführung bereit sein
Assistiert	Fahrer führt dauerhaft entweder die Quer- oder die Längsführung aus. Die jeweils andere Fahraufgabe wird in gewissen Grenzen vom System ausgeführt • Der Fahrer muss das System dauerhaft überwachen • Der Fahrer muss jederzeit zur vollständigen Übernahme der Fahrzeugführung bereit sein
Driver only	Fahrer führt dauerhaft (während der gesamten Fahrt) die Längsführung (Beschleunigen/Verzögern) und die Querführung (Lenken) aus

Automatisierungsgrad ⇒

Quelle: Reichtfolgen zunehmender Fahrzeugautomatisierung, Berichte der Bundesanstalt für Straßenwesen, Heft F 83, 2012.



Level	Name	Narrative definition	acceleration/ deceleration	driving environment	of dynamic driving task	(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	-	

Sources: bast [1], VDA [2], SAE [3], NHTSA [4]

FZD

Meaning of Highly Automated Driving

TECHNISCHE UNIVERSITÄT DARMSTADT

Highly Automated Driving

- **Expected as introduction path to fully or driverless driving**
- **Typical use case: Autobahn Chauffeur with v_{max} = 130 km/h**
- **Function availability depends on preconditions => if preconditions are not given (foreseen or unforeseen) transition to driver**

Pro (compared to level 4 systems):

- **System can rely on capability of humans for handling of unknown or complex situations**

Con:

- **Transition might lead to new risks**

Validation Challenge of Automated Driving

TECHNISCHE UNIVERSITÄT DARMSTADT

Challenge: Validation of promised safety level above the level of driving by humans

- **Evidence is needed that risk <u>does not exceed</u> today reference.**
- **But what is the safety reference for validation?**

FZD

Safety References

TECHNISCHE UNIVERSITÄT DARMSTADT

Reference variants:

- **Possible safety references vary by several orders of magnitude, both far above and below today's reference safety values.**
- **Progress in safety validation for automated vehicles must be measured in comparison with today's risk values.**
- **At least two relevant metrics must to be measured:**
  - **accidents with personal injuries**
  - **accidents with fatalities**
  - **Present day driving tests are far from collecting enough data to cover the reference risk figures**

Numbers for Autobahn in Germany 2014

Accident category	Distance between accidents [after 1]	Test-drive distance [2], [3]
with injuries	$12 \cdot 10^6$ km	$240 \cdot 10^6$ km
with fatalities	$660 \cdot 10^6$ km	$13.2 \cdot 10^9$ km

FZD

STOP!!!!!

TECHNISCHE UNIVERSITÄT DARMSTADT

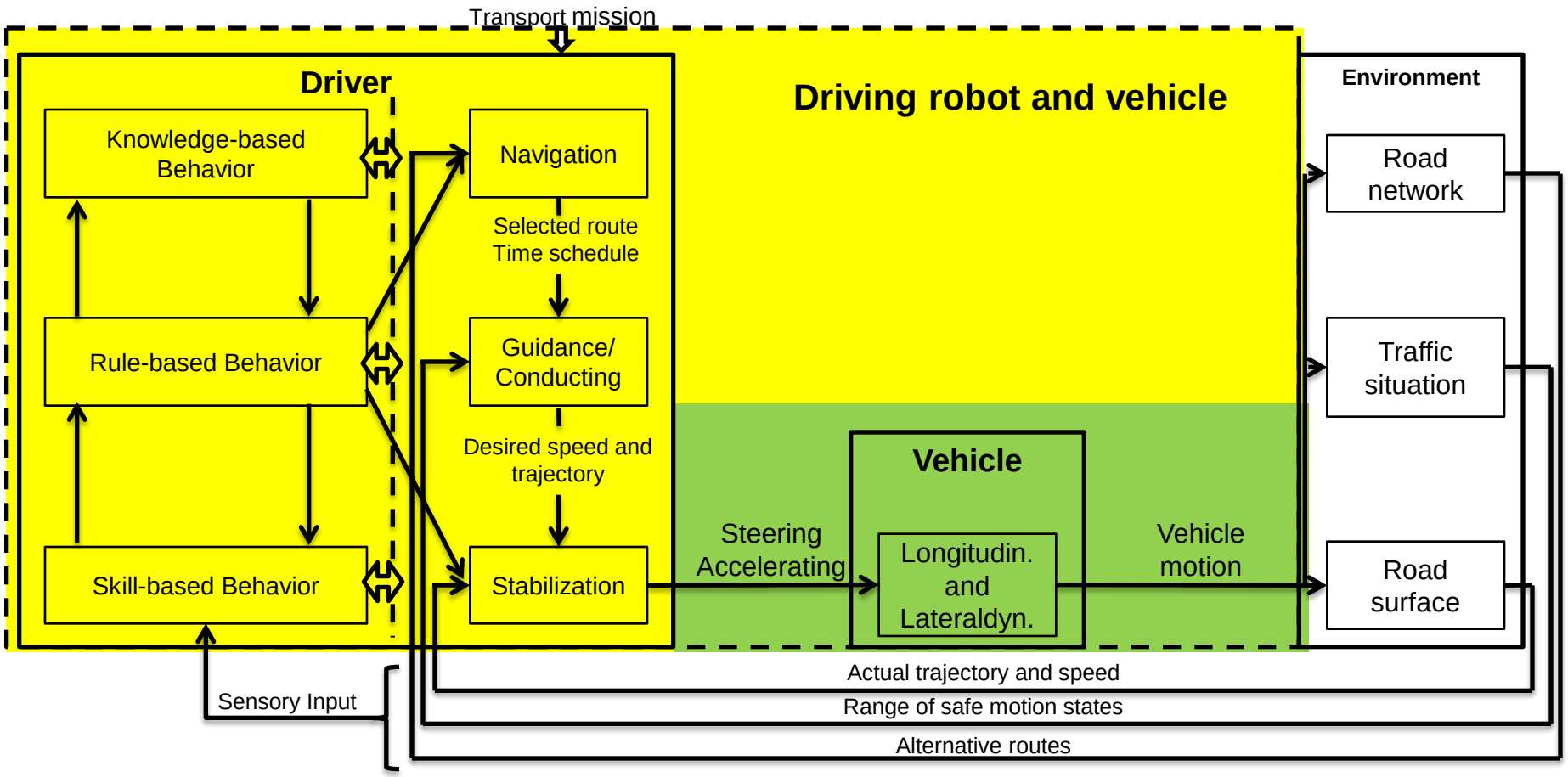
For today's vehicles (as in aviation) there is no need for such high testing distance, why here?

What is the fundamental difference?

FZD

Differences between conventional and automated vehicles

TECHNISCHE UNIVERSITÄT DARMSTADT



Current validation methods do not cover the yellow area

according to Rasmussen [8] and Donges [9]

FZD

What do we know about driving safety performance?

TECHNISCHE UNIVERSITÄT DARMSTADT

Statistics and Accident Research

- **Reports on accident frequencies and their causes**
- **Figures about time gaps and (exceeding) speeds on some roads**

Driver modeling

- **Qualitative models for information processing and driving tasks (Rasmussen, Donges, …) are able to explain the observed behavior.**
- **Quantitative models for simple scenarios (car following, lane change, intersection crossing) are able to explain and predict traffic flow figures, but not accident frequencies and severity.**
- **Human reliability models (Reichart, …) interpret the observed accident frequencies.**

Swiss Cheese Model (adapted to human drivers)

TECHNISCHE UNIVERSITÄT DARMSTADT

Simple Probabilistic Accident Model

$$n_{accidents,hd} = n_{crit,hd} \cdot \rho_{transition,hd}; \qquad n_{crit,hd} = f(driver_{ego}, E_{traffic/road})$$

$$\rho_{transition,hd} = f(driver_{ego,hd}, driver_{traffic})$$

n = frequency
ρ = transition probability
E = exposure of circumstances for potential hazards

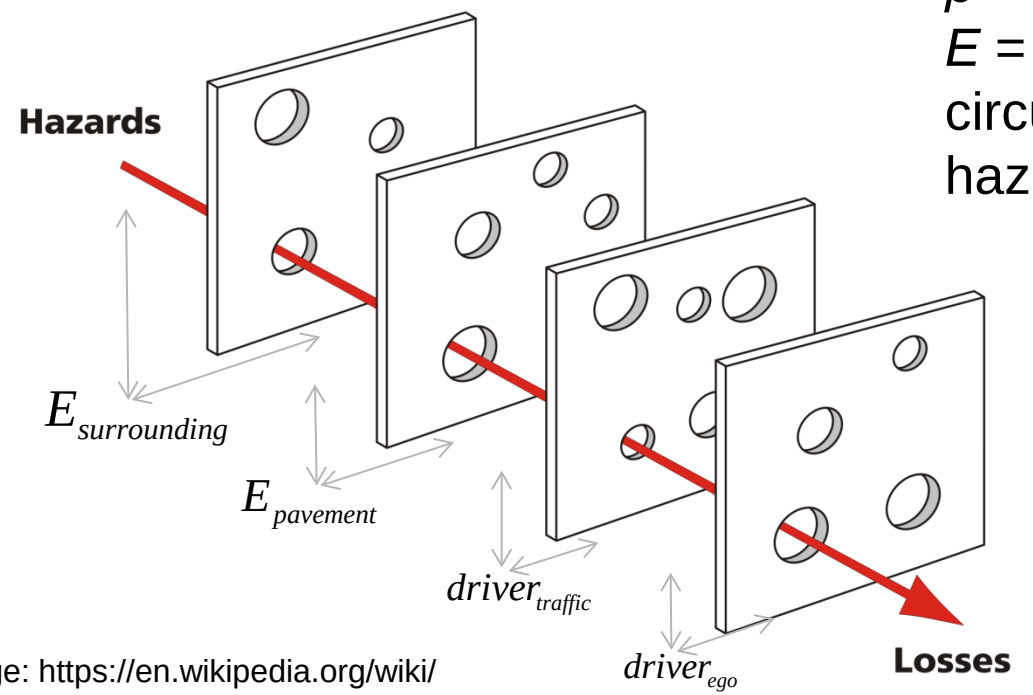


Image: https://en.wikipedia.org/wiki/Swiss_cheese_model#CITEREFReason1990

Cheese model idea from [10]

FZD

Knowledge of the driving task and respective safety

TECHNISCHE UNIVERSITÄT DARMSTADT

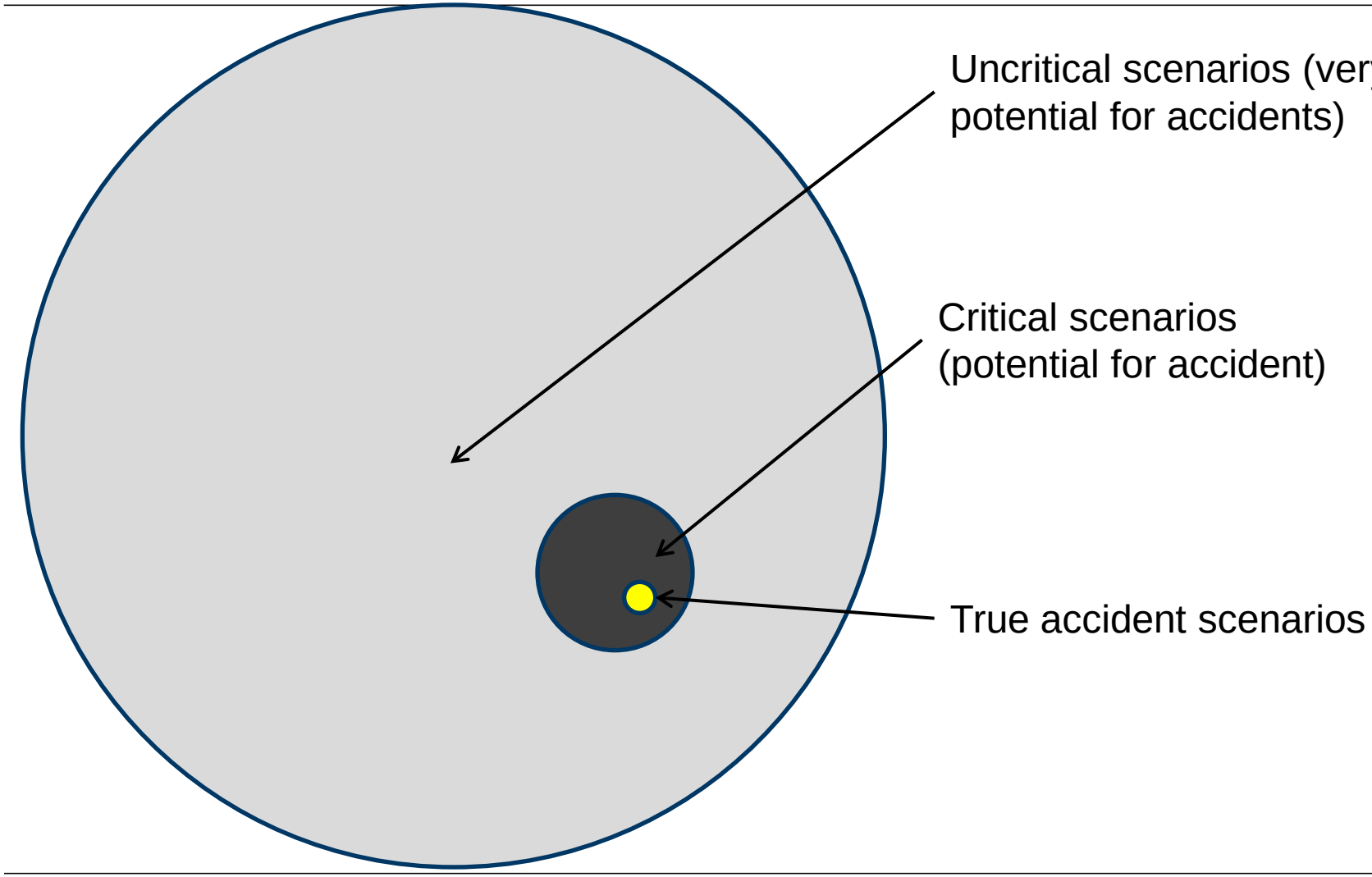
Lacks:

- **Serious figure of the accident avoidance capability of human drivers**
  - **Frequency and type of non-standard situations (both self-caused or innocently exposed)**
  - **Performance of human drivers in non-standard situations**

Dark matter problem:

- **We only know standard scenarios and reported failure scenarios (recorded accidents).**
- **Almost nothing is known about the transition probability from accident-free driving to accident occurrence and the frequency and type of critical scenarios.**
- **Avoiding the accidents that human drivers cause is not necessarily sufficient to reduce accident frequencies.**

Dark Matter Problem (today)



Swiss Cheese Model (adapted to automated driving)

TECHNISCHE UNIVERSITÄT DARMSTADT

Accident Model for Automated Vehicles

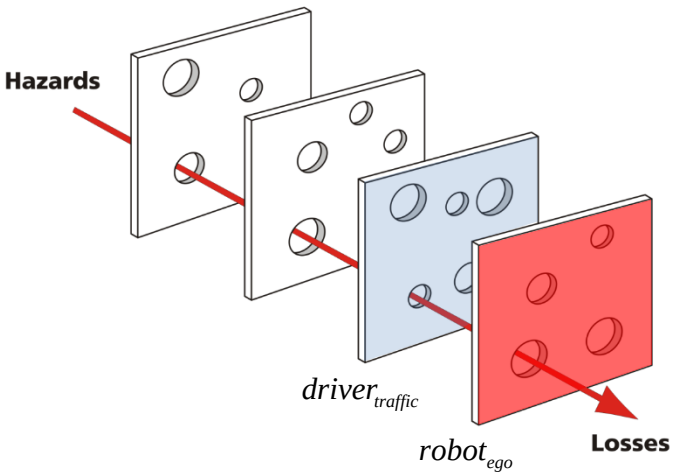
$$n_{accidents,ad} = n_{accidents,ad,old} + n_{accidents,ad,new}$$

$$n_{accidents,ad,old} = n_{crit,ad,old} \cdot \rho_{transition,ad,old}$$

Automation Risks

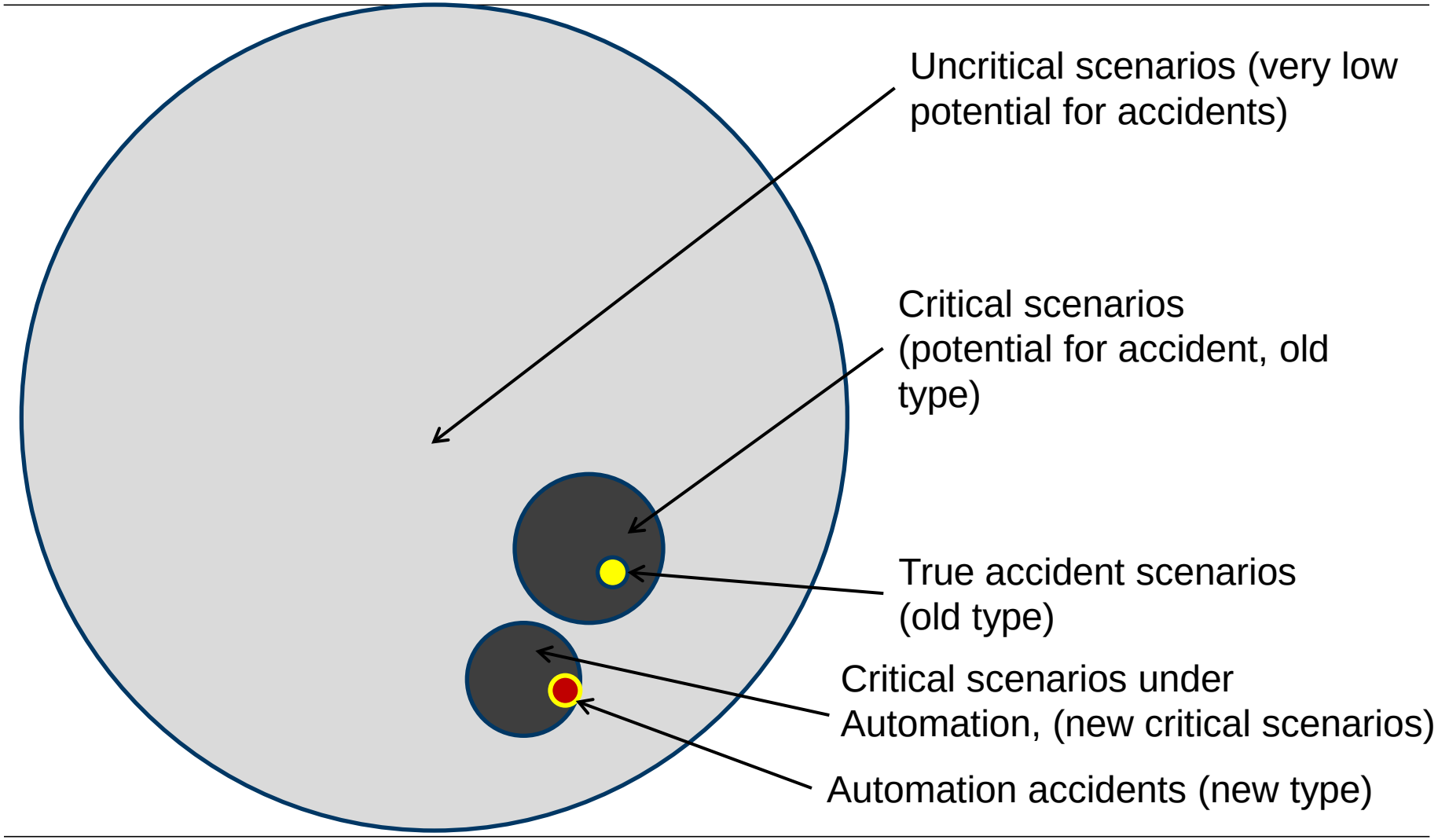
$$n_{accidents,new} = n_{crit,ad,new} \cdot \rho_{transition,ad,new}; n_{crit,ad,old/new} = f(robot_{ego}, E_{traffic/road})$$

$$\rho_{transition,ad,old/new} = f_{old/new}(robot_{ego}, driver_{partner})$$



FZD

Dark Matter Problem



Missing Knowledge

TECHNISCHE UNIVERSITÄT DARMSTADT

In order to predict the safety of automated vehicles we need:

- **Valid critical scenarios (remaining and new critical scenarios) and their specific characteristics, in sufficient quantity**
- **Valid models of the AV capability to control critical situations in a safe manner.**
- **All figures must be compared with the reference risks for each relevant class.**

With respect to the Swiss Cheese Model:

- **We must model each slice in order to predict the risk of AVs with high accuracy.**

With respect to the Dark-Matter-Problem:

- **The occurrence of critical scenarios and the capability to control them have made „bright“.**

First conclusion

TECHNISCHE UNIVERSITÄT DARMSTADT

The obvious safety gain:

- **The functional design of automated driving promises higher safety by reduction of frequency of known critical situations.**

But we do not know:

- **Capability of AD to avoid accidents in the remaining critical situations**
- **Frequency of new critical situations generated by automated driving and the capability to control them safely.**

Validation of automated driving has to cover both and has to gain all necessary knowledge prerequisites.

Research project PEGASUS

EFFECTIVELY ENSURING AUTOMATED DRIVING.

PEGASUS

Supported by:

Federal Ministry
for Economic Affairs
and Energy

on the basis of a decision
by the German Bundestag

What is PEGASUS?

- **P**roject for **e**stablishing **g**enerally **a**ccepted quality criteria, tools and methods, as well as **s**cenarios and (in German: **u**nd) **s**ituations for the release of highly automated driving functions

- Founded by the Federal Ministry for Economic Affairs and Energy (BMWi)

- PEGASUS will close gaps in the area of testing and approving automated vehicles with the aim to transfer existing highly automated vehicle-prototypes into products

- PEGASUS provides corresponding results and standards for product development and release

Key Figures

42 months term	January 1, 2016 – June 30, 2019
17 Partners	▪ OEM: Audi, BMW, Daimler, Opel, Volkswagen ▪ Tier 1: Automotive Distance Control, Bosch, Continental Teves ▪ Test Lab: TÜV SÜD ▪ SMB: fka, iMAR, IPG, QTronic, TraceTronic, VIRES ▪ Scientific institutes: DLR, TU Darmstadt
12 Subcontracts	▪ i.a. IFR, ika, OFFIS
Project Volume	▪ approx. 34,5 Mio. EUR ▪ Subsidies: 16,3 Mio. EUR
Personnel deployment	▪ approx. 1.791 man-month or 149 man-years

Current State of Development of HAD

Prototypes

Lab / Testing Ground

Products

current status

Current State of Development of HAD

Prototypes

- Multitude of prototypes built by OEM with HAD-functionality
- Evidence, that HAD is technologically possible
- Partially tested in real traffic situations
- Test drives involve backup safety driver at all times

Lab / Testing Ground

- Individual analyses to optimize prototypes
- Current test stands/ testing grounds do not provide enough test coverage for all HAD features currently in focus
- There is no procedure for adequate testing (particularly performance) of HAD-systems

Products

- No release or introduction of variety of HAD features without sufficient assurance

current status

Resulting Starting Position – Automated Driving

Together with electric driving, automated driving is tomorrow's subject matter.

Basic functionality is technologically given

Has been demonstrated in various projects

High standards regarding quality and performance of the automated vehicle

➔ Measures that product needs to meet

Existing measures for testing and release are insufficient, too cost-intensive and too complex

➔ Consequently, the introduction of highly automated driving features today can only be achieved with great expenditure.

Central Issues of the Project

What level of performance is expected of an automated vehicle?
How can we verify that it achieves the desired performance consistently?

Scenario Analysis & Quality Measures

- What human capacity does the application require?
- What about technical capacity?
- Is it sufficiently accepted?
- Which criteria and measures can be deducted from it?

Implementation Process

- Which tools, methods and processes are necessary?

Testing

- How can completeness of relevant test runs be ensured?
- What do the criteria and measures for these test runs look like?
- What can be tested in labs or in simulation? What must be tested on test grounds, what must be tested on the road?

Reflection of Results & Embedding

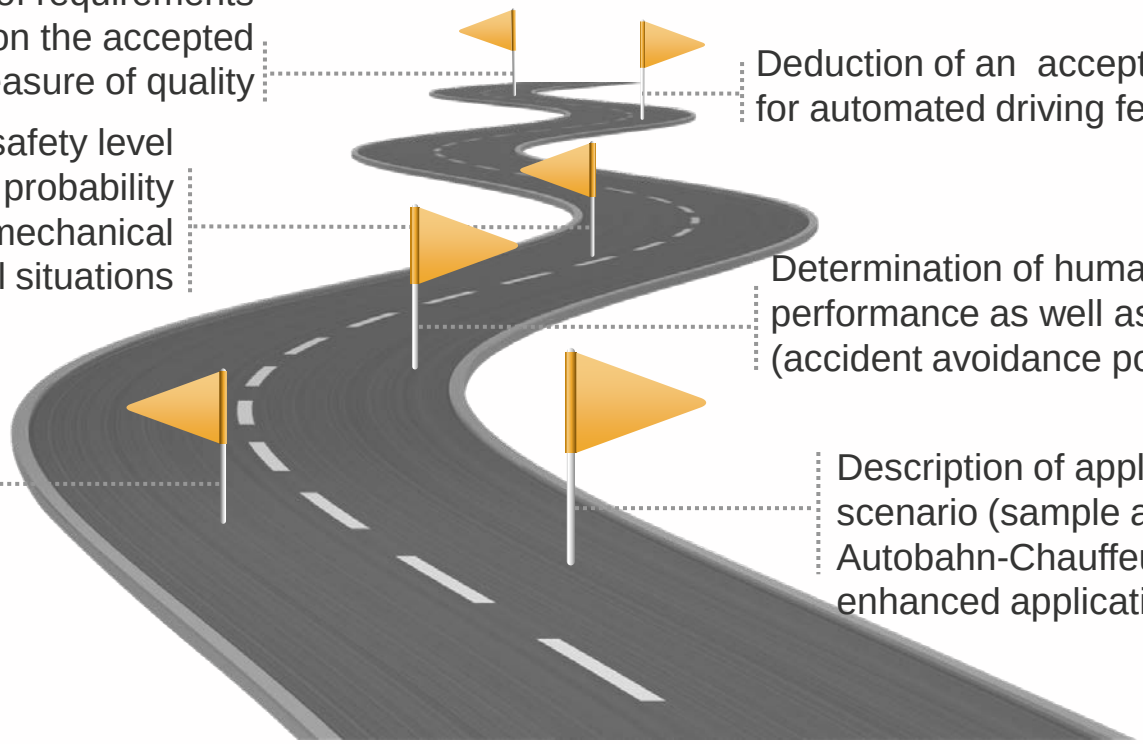
- Is the concept sustainable?
- How does the process of embedding work?

SP 1 Scenario Analysis and Quality Measures

Deduction of requirements based on the accepted measure of quality

Deduction of an accepted quality measure for automated driving features

Determination of safety level through assessment of probability of occurrence and mechanical manageability in critical situations



Determination of human and mechanical performance as well as effectiveness (accident avoidance potential)

Determination of critical traffic situations

Description of application scenario (sample application: Autobahn-Chauffeur + enhanced application scenario)

SP 2 Implementation Process

1

Analysis
of modification needs of existing metrics and automobile series development processes

2

Transfer
of systematic scenario guidelines into process steps in consideration of system classifications and levels of vehicle utilization

3

Transfer
of target value parameters into process steps

4

Preparation
of requirements definition for simulation, lab tests, testing ground and field coverage

5

Refinement
of the guidelines for required documentation of process steps

6

Guidelines and Protocols
for the documentation of technological state-of-the-art compliance during the development process

SP 3 Testing

- Detailing and completion of test scenarios of subproject 1, including technical quality measures as well as approval criteria
- Construction and filling of test specification database
- Establishment and verification of testing methods, interfaces, tools in the lab, on testing grounds and in real traffic
- Development and coordination of industrywide established models, tools and interfaces for the simulation
- Compilation of a test catalog and requirements for lab, testing ground and field coverage
- Construction of reference elements for practical testing and demonstration of functions
- Testing in the lab, on testing grounds and on the street

SP 4 Reflection of Results & Embedding

Statement

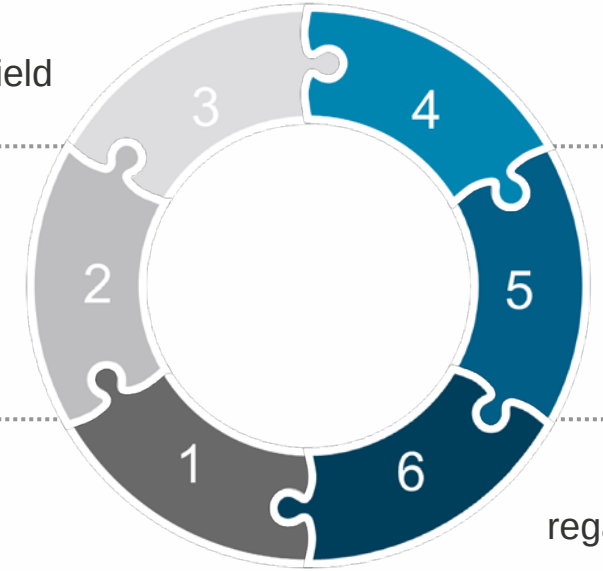
about the distribution ratio between the applied test methods (from simulation to testing ground to field test)

Assessment,

whether the test goal can be achieved with the utilized processes and methods in PEGASUS

Verification

of methods to identify relevant situations, quality and criticality measures for the assurance of HAD features



➔Proof of Concept

Assistance

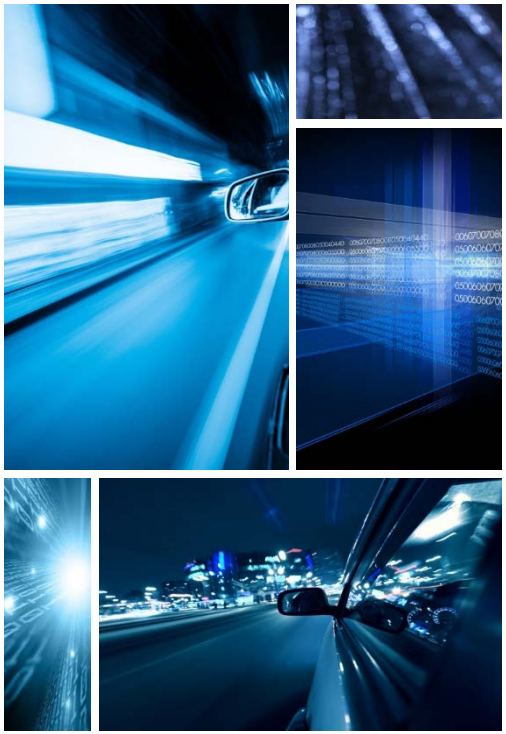
with embedding of acquired results with our project partners

Lessons learned

regarding the implementation of the results in existing corporate structures

Selected Goals of the Project

- Development of a procedure for the determination of design criteria and establishment of quality measures
- Considering the driver in regards to his abilities
- Design of the development process for the release of highly automated vehicle systems
- Conceptual design, assembly and demonstration of building blocks for an efficient toolchain for simulation, testing ground and field test

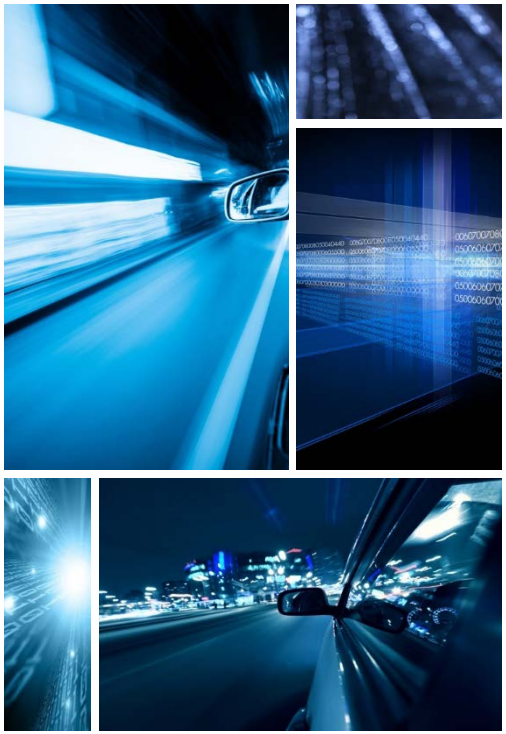


PEGASUS Goals beyond Research

- PEGASUS is a national project implementation for fast progress in automated driving
- Embedding of findings in the industry
- Distribution and pioneering of a standardization

➔All essential project results are freely accessible

- Collaboration with other consortia is highly appreciated
- We need a worldwide common understanding about how safety of automated driving has to be assured
- Exchange with safety assurance experts worldwide at PEGASUS interim presentation
(Mid of October 2017)



Contact:
Technische Universität Darmstadt
Prof. Dr. rer. nat. Hermann Winner
winner@fzd.tu-darmstadt.de
+49 (0) 6151 / 16 24 200

More information:
www.pegasusprojekt.de