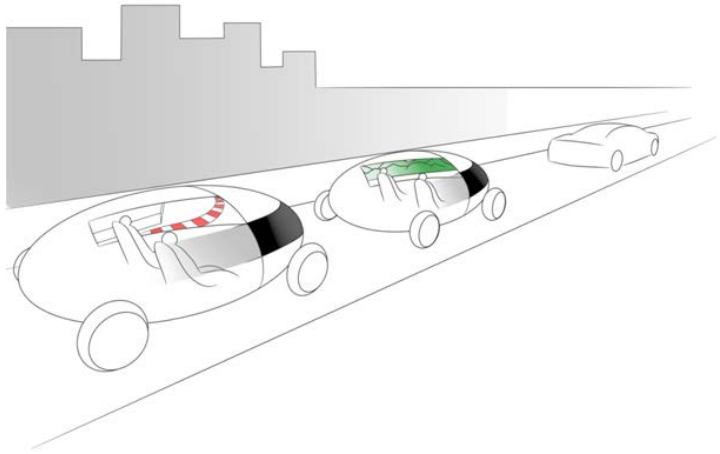
TECHNISCHE UNIVERSITÄT DARMSTADT



Prof. Dr. rer. nat. Hermann Winner

Dipl.-Ing. Walther Wachenfeld

Philipp Junietz, M.Sc.

Safety Assurance for Highly Automated Driving – The PEGASUS Approach

Considered Levels of Automated Driving

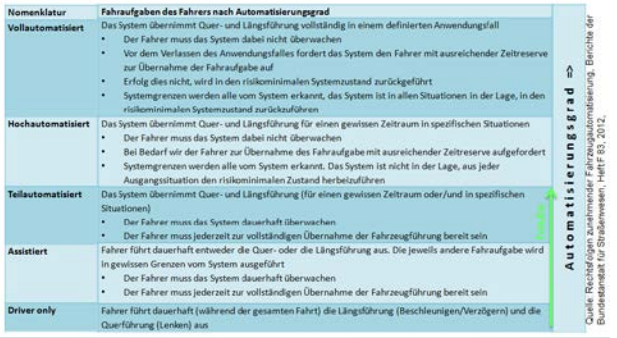
TECHNISCHE UNIVERSITÄT DARMSTADT

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 (ref.)**

Interpretation:

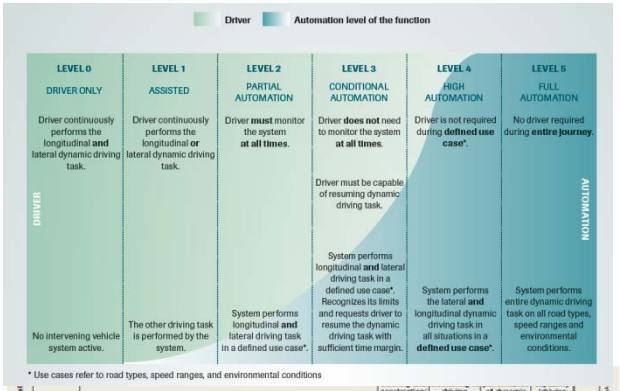
- **No responsibility of human drivers (operators) during operation of automation, but the automation may shift back the driving task towards human in a reasonable transition time.**



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: Rechtsfolgen 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)
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
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* performs all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
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
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
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
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 automated 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

Safety References

TECHNISCHE UNIVERSITÄT DARMSTADT

Reference variants:

- **Possible safety references are within a wide bandwidth (several orders of magnitude), much above today road safety as well as much below.**
- **A progress in safety by automation has to be measured in comparison with today risk as reference.**
- **At least two relevant categories have to be addressed as reference:**
  - **accidents with damage to persons and specifically**
  - **accidents with fatalities**
- **Reference risk figures are far from today testing horizons by real driving tests, e.g. for Autobahn in Germany 2014**

Accident category	Distance between accidents [after 5]	Test-drive distance [6], [7]
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

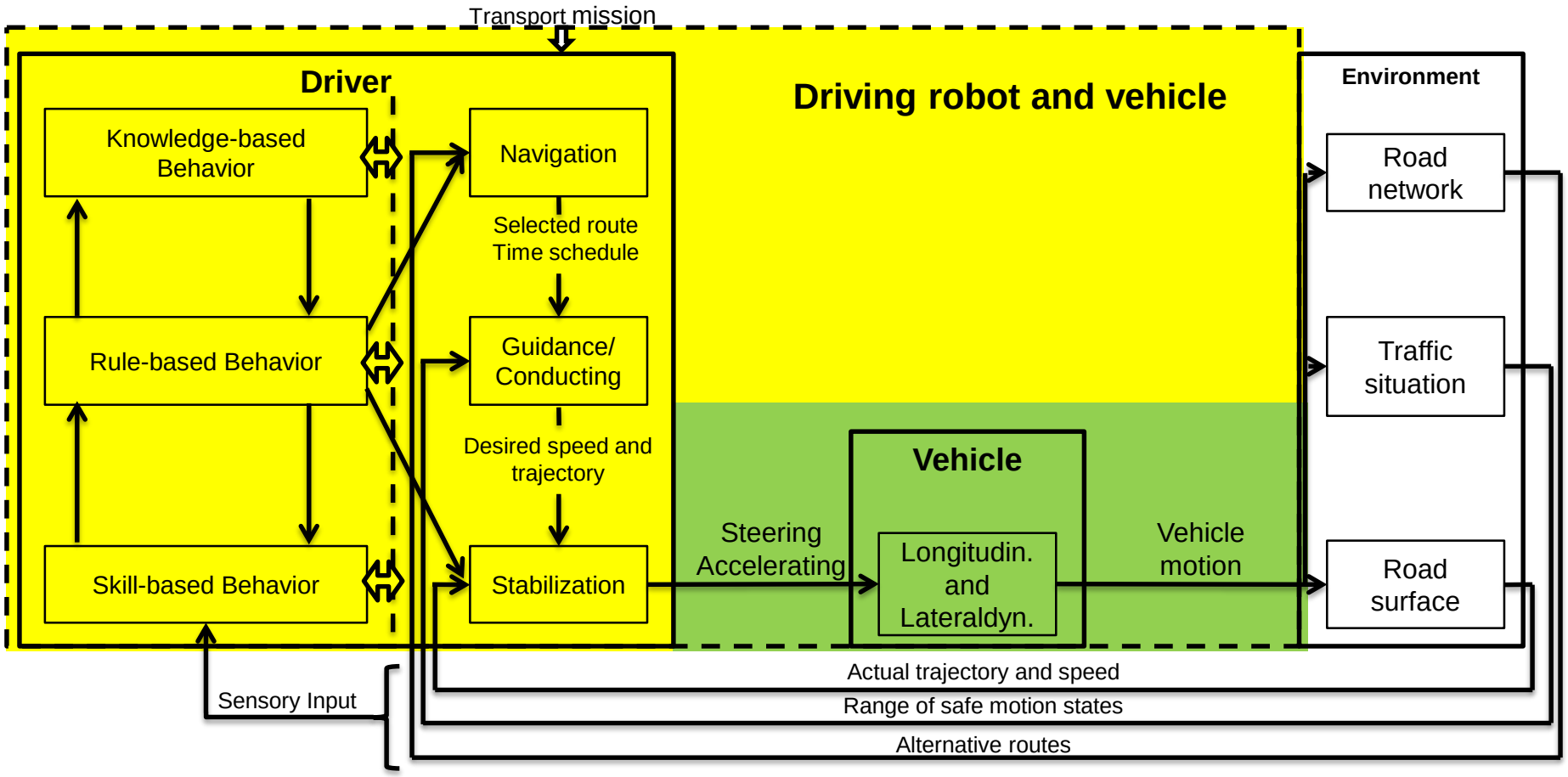
STOP!!!!!

TECHNISCHE UNIVERSITÄT DARMSTADT

For today's vehicles (and more extreme for aviation) there is no requirement for such high testing distance, why here?

What is the fundamental difference?

Differences between conventional and automated vehicles



Current validation of vehicle doesn‘t cover the yellow area

according to Rasmussen [8] and Donges [9]

What do we know about Driving Safety Performance?

TECHNISCHE UNIVERSITÄT DARMSTADT

Statistics and Accident Research

- Reports on frequency of accidents and their causes
- Figures about time gaps and exceeding speeds of 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 accidents frequency and severity.
- Human reliability models (Reichart, …) interpret the observed accidents frequency.

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

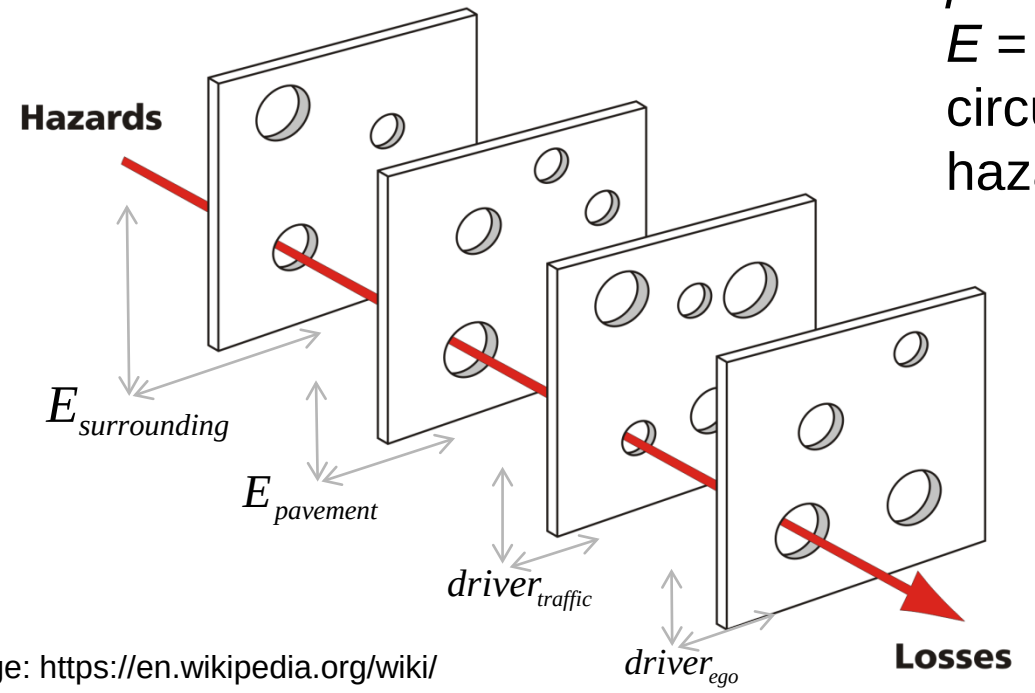


Image: https://en.wikipedia.org/wiki/Swiss_cheese_model#CITEREFReason1990

Cheese model idea from [10]

FZD

Knowledge about Driving Task and respective Safety

TECHNISCHE UNIVERSITÄT DARMSTADT

Lacks:

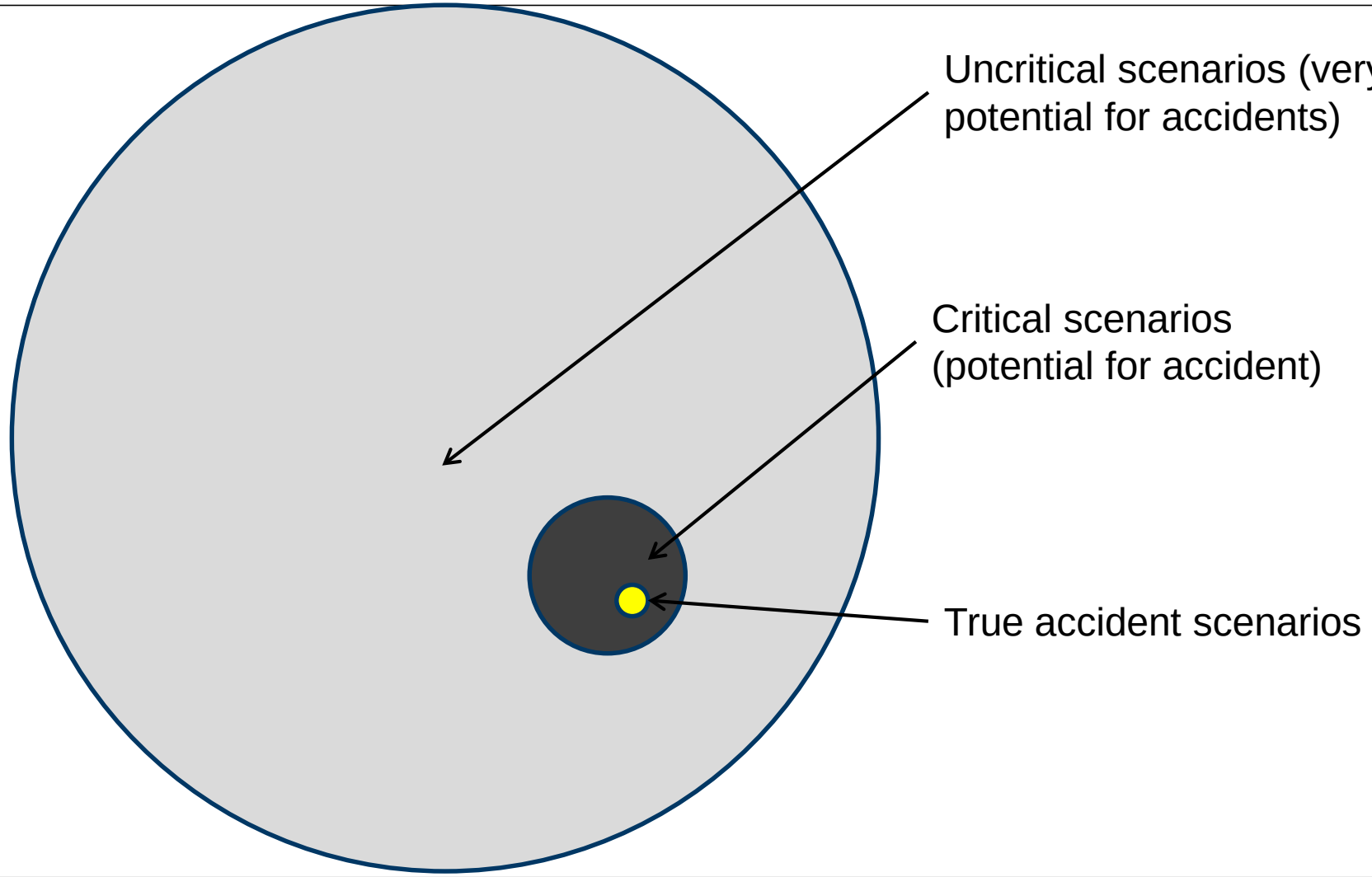
- Serious figure of the accident avoidance capability of human drivers
- Frequency and type of non-standard situations (both self caused or innocently exposed)
- Performance of human drivers in non-standard situations

Dark matter problem:

- We only know standard scenarios and the reported fail scenarios (accidents), but do not know the probability for transition from accident free driving to real accident occurrence.
- Avoiding the known human accident causes are not sufficient:

1. The accidents avoidance capability of humans is not recorded.
2. No quantitative figure about types of critical scenarios and their frequency where humans avoid accidents.

Dark Matter Problem



Swiss Cheese Model (adapted to automated driving)

TECHNISCHE UNIVERSITÄT DARMSTADT

Accident Model for Automated Vehicles

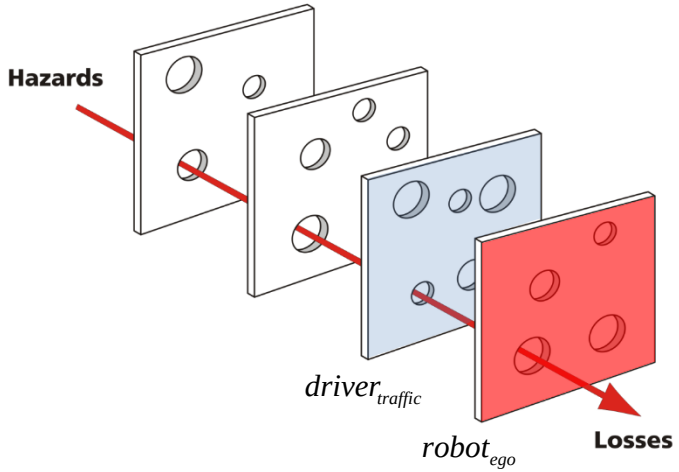
$$n_{accidents,ad} = n_{accidents,ad,old} + n_{accidents,ad,new}$$

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

Automation Risks

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

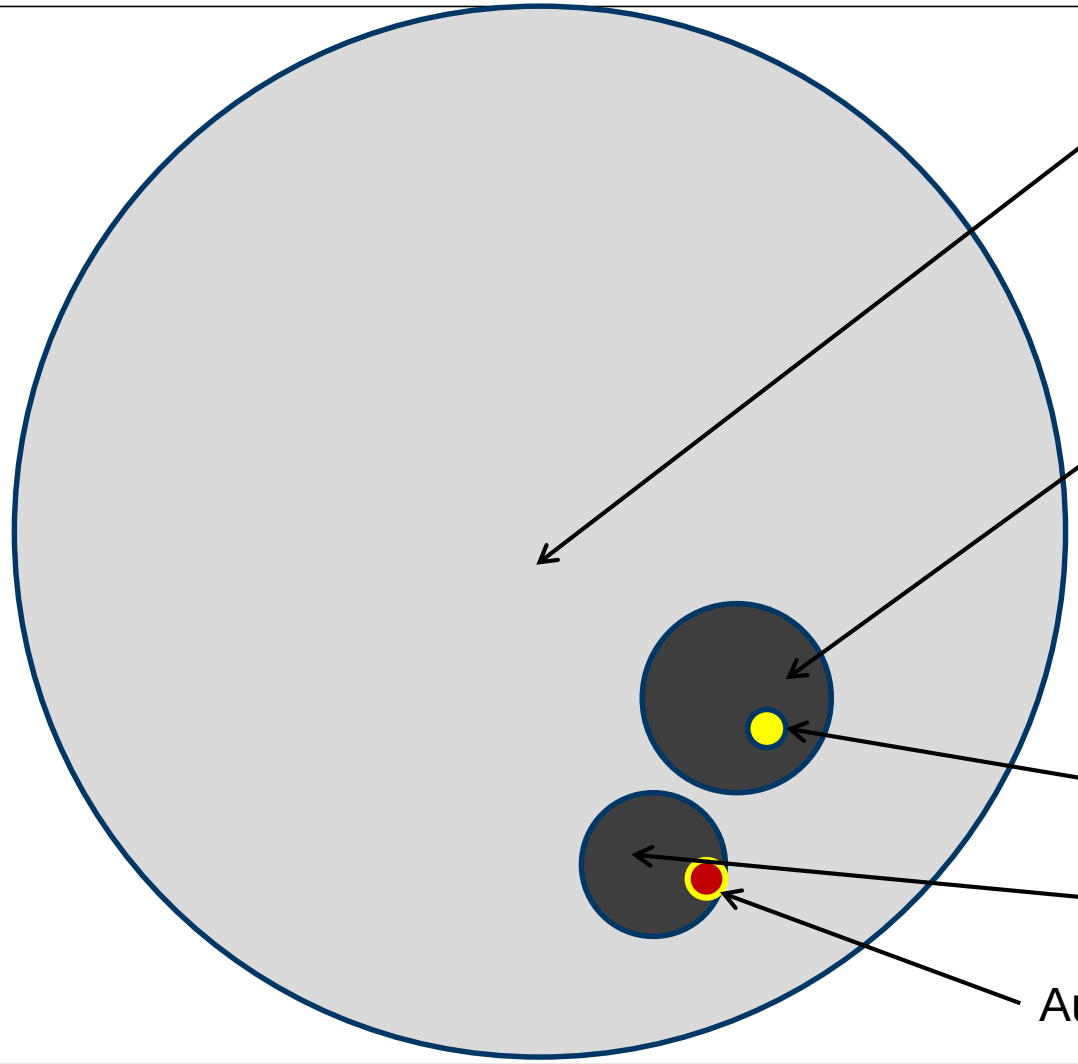
$$\rho_{transition,ad,old/new} = f_{old/new}(robot_{ego}, driver_{partner})$$



FZD

Dark Matter Problem

TECHNISCHE UNIVERSITÄT DARMSTADT



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.

PEGASUS

OBJECTIVES AND WORK CONTENTS OF PEGASUS

Project for establishing generally accepted quality criteria, tools and methods, as well as scenarios and situations for the release of highly automated driving functions

Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

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

General conditions

Duration	January 2016 – June 2019
Partners	*OEM:* Audi, BMW, Daimler, Opel, Volkswagen *Tier 1:* Automotive Distance Control, Bosch, Continental *Test Lab:* TÜV SÜD *SME:* fka, iMAR, IPG, QTronic, TraceTronic, VIRES *Scientific institutes:* DLR, TU Darmstadt
Subcontractors	IFR, ika, OFFIS, BFFT, Carmeq, EFS, Fortiss, MBTech, Nordsys, Philosys, VSI, WIVW
Volume	total 34.5 Mio. EUR, supported volume 16.3 Mio. EUR
Working capacity	150 person-years

Current stage of development for HAD

PEGASUS

Prototypes

Test lab / test ground

Products

today

Current stage of development for HAD

PEGASUS

Prototypes

- OEM built many prototypes with HAD functionality
- Proof that HAD is technologically feasible
- Partially tested in real traffic, but always with a safety driver

Test lab / test ground

- Single considerations for optimizing prototypes
- Current test benches / test sites do not provide adequate test coverage for HAD functionalities
- There is no procedure for sufficient safety assurance validation of HAD systems

Products

- Without adequate validation, the release or introduction of HAD vehicles is not possible

Main research questions

- **What performance and safety criteria do systems for highly automated driving have to fulfill?**
- **How do we validate their performance?**
- **Starting with Autobahn Chauffeur, later for HAD under more complex conditions.**

- How good is the human perfor-mance within the use case?
- How good is the machine's performance?
- Is it sufficiently socially accepted?
- Which quality criteria can be derived from that?

- Which tools, methods, and processes are required?

- How can the completeness of relevant test cases be guaranteed?
- Pass/fail criteria for these test cases (from quality factors)
- Which part of these test cases can be tested in simulations / labs, which on roads?

- Does the concept work in practise?

Subprojects

PEGASUS

PEGASUS

SP 1	SP 2	SP 3	SP 4
SCENARIO ANALYSIS & QUALITY METRICS	**IMPLEMENTATION PROCESSES**	**TESTING**	**PROFIT REFLECTION & EMBEDDING**
• Application scenario • Quality metrics • Extended application scenario	• Process methodology • Process specification	• Test specification database • Laboratory and simulation tests • Proving ground tests • Field tests	• Proof of concept • Embedding
Lead: Volkswagen	**Lead: Adam Opel**	**Lead: Daimler, BMW, TÜV SÜD**	**Lead: Continental**

Closing the gap by PEGASUS

Prototypes

Test lab / test ground

Products

today

advancements by PEGASUS

PEGASUS goals beyond research

- PEGASUS is a national project implementation for fast progress in automated driving.
- Embedding of knowledge into the industry, as well as dissemination of knowledge and experience across the appropriate committees for standardization.
- Open access to all essential project results.
- Collaboration with other consortia is highly appreciated.
- Exchange with safety assurance experts worldwide (starting with asymposium in spring 2017, presumably in Munich)
- We need a worldwide common understanding about how safety of automated driving has to be assured.