Wie gut ist genug?

How good is good enough?

PEGASUS

Daniel Lipinski | 13. Mai 2019

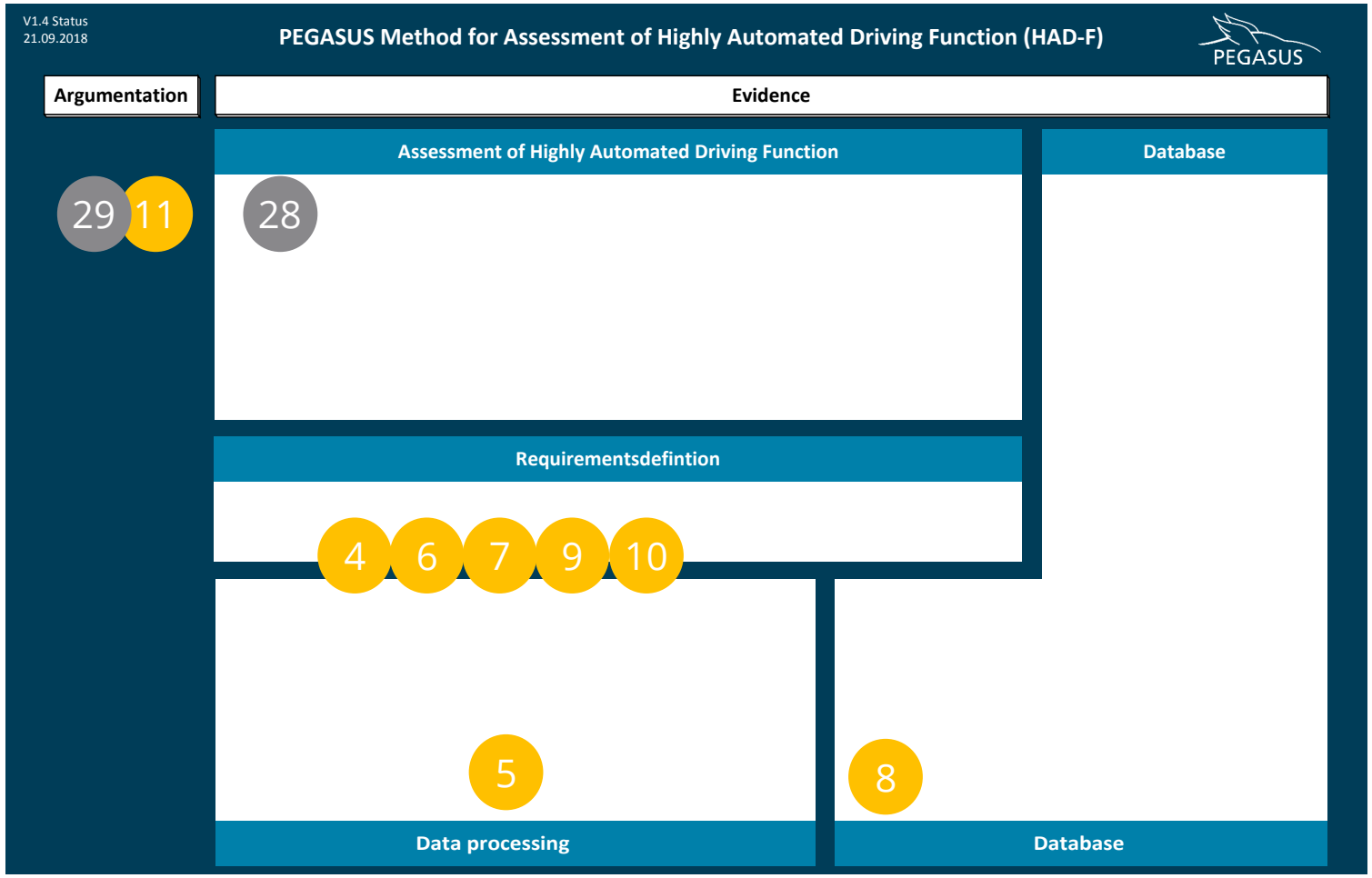
Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

PEGASUS Method for Assessment of Highly Automated Driving Function (HAD-F)

Exhibit Overview



4	The Highway-Chauffeur	TP 1
5	Scenario Description and knowledge-based scenario generation	TP 1
6	L3-Transitions: Driver Takeover Capability in Real Traffic	TP 1
7	Critical Scenarios for Human Drivers - Simulator Studies	TP 1
8	Critical Scenarios for Human Drivers - Criticality	TP 1
9	Critical Scenarios for Human Drivers - Impact Analysis	TP 1
10	Potentially Critical Scenarios for and by the HAD-F (Automationrisiks)	TP 1
11	Social Acceptance for HAD	TP 1
28	Safety Statement	TP 1
29	Safety Argument	TP 1

Part 1:
How Good is good enough?

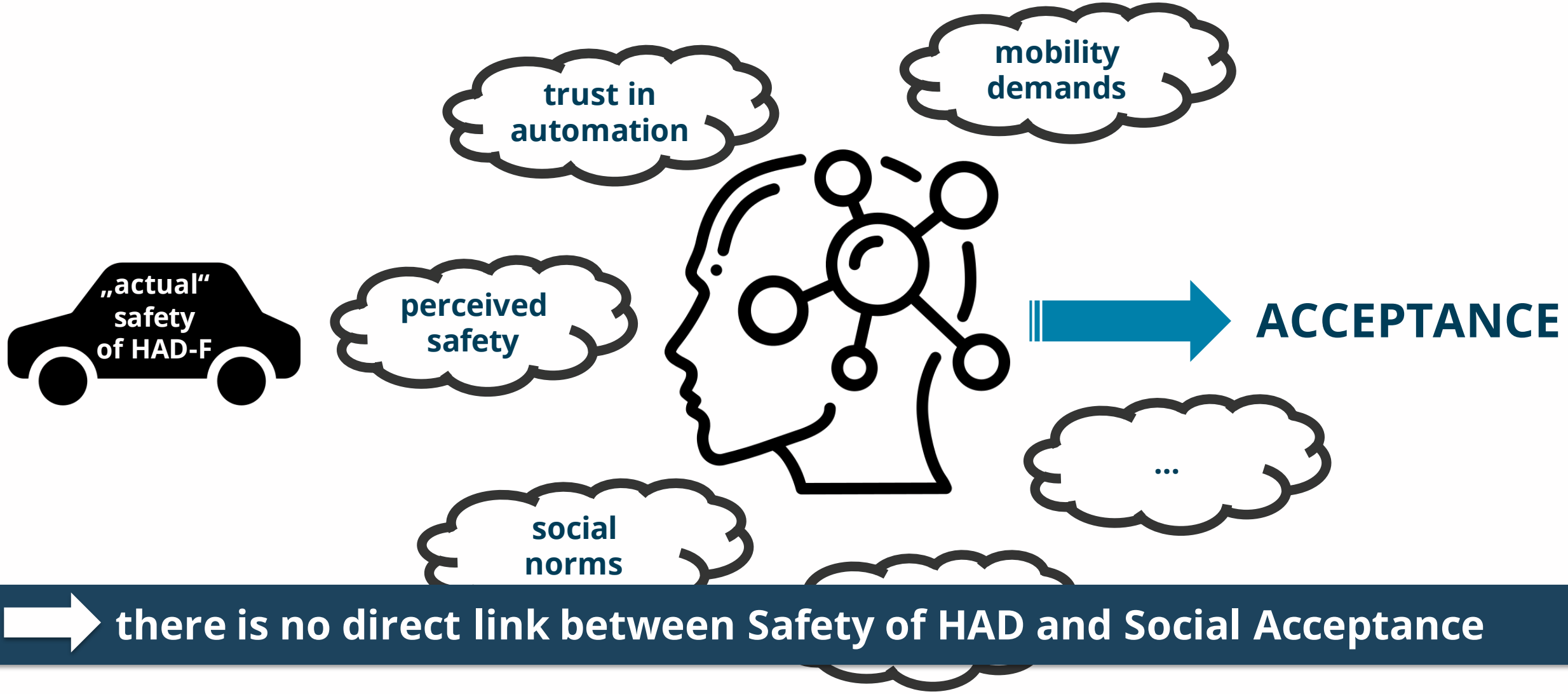
Part 2:
Methods/Tools/Arguments

PEGASUS

Motivation

source: daijiworld.com

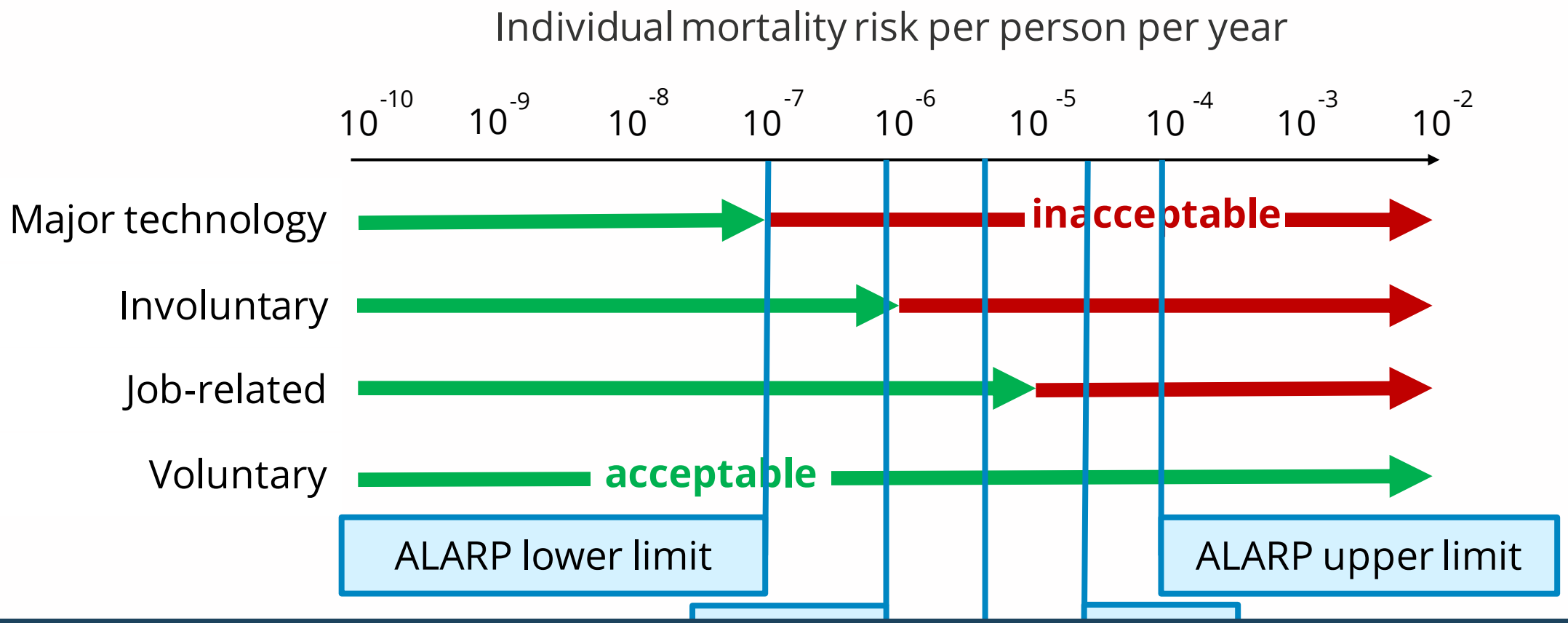
Social Acceptance



there is no direct link between Safety of HAD and Social Acceptance

Icon made by Smashicons from www.flaticon.com
Icon made by kiranshastry from www.flaticon.com

Individual risk acceptance



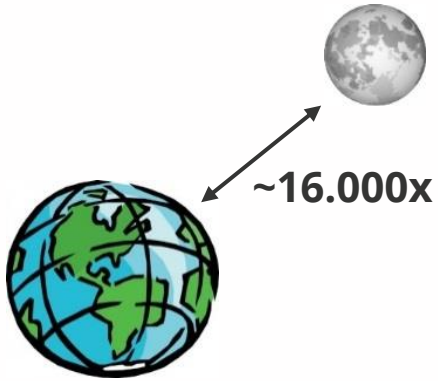
The individual accepted risk depends on the type of technology use!

Application of different risk acceptance principles

Distance Based Approach

How long does an automated driving vehicle need to drive on highways without fatal accidents, in order to be confident (95% prob.) that it is better than a human equivalent?

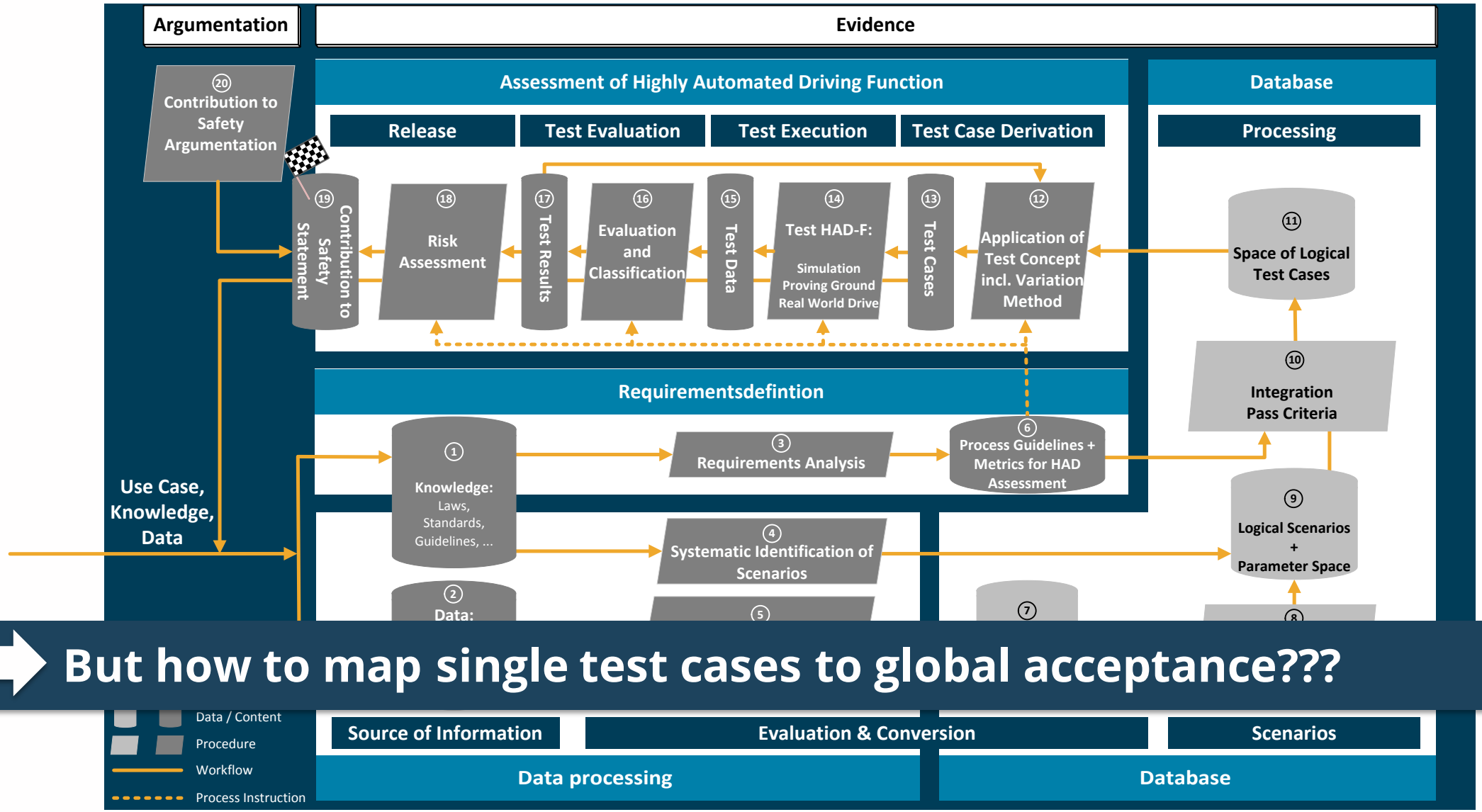
Thesis	A verification of this question needs to proof that the automated vehicle has less accidents with fatalities than the human peer group
Currently	614 million kilometers between two fatal accidents by humans
Target	Halve the risk of accidents with fatalities
Result	The required test distance is 6.14 billions kilometers
Challenge	Every system modification requires a repetition of all tests



6.14 billions kilometers is the 16.000 times distance between the earth and the moon

Distance-based test approach is unfeasible for automated driving functions
A systematic scenario-based test approach is needed

Scenario Based Approach - PEGASUS



But how to map single test cases to global acceptance???

Safety Argument

What do people expect from highly automated mobility in the larger context? — *e.g. convenience, mobility benefits, data privacy*

How to monitor a HAD-F over its entire life cycle? — *e.g. field monitoring*

How to support a Safety Argumentation with evidence? — *e.g. safety case (Goal Structuring Notation, Assurance Case)*

Which elements should a Safety Argumentation contain sufficiently? — *e.g. NHTSA design principles, German ethics commission*

How to ensure necessarily compliance with all relevant standards and directives needed for homologation? — *e.g. ISO 26262, ISO/PAS 21448:2019(E)*

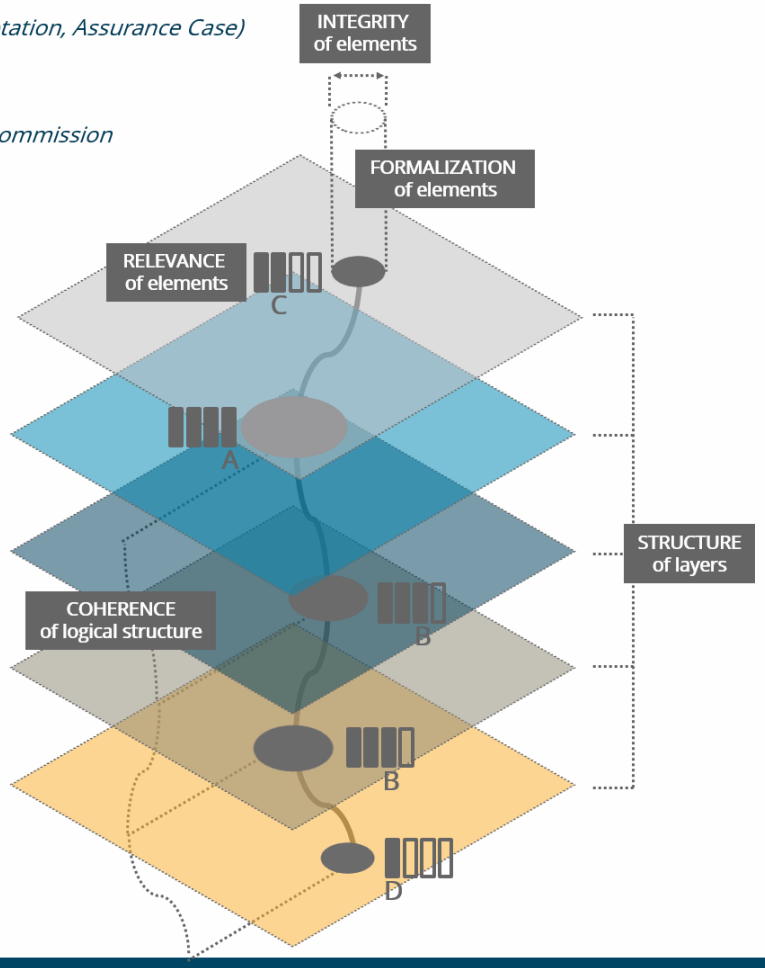
LAYER 0 – ACCEPTANCE MODEL
Embed a Safety Argumentation in a broader context of technology acceptance.

LAYER 1 – TOP LEVEL SAFETY GOALS
Derive safety goals from agreed upon design principles in order to meet expectations such as positive risk balance.

LAYER 2 – LOGICAL STRUCTURE
Build a logical link between safety goals to meet and evidence to support the Safety Argumentation.

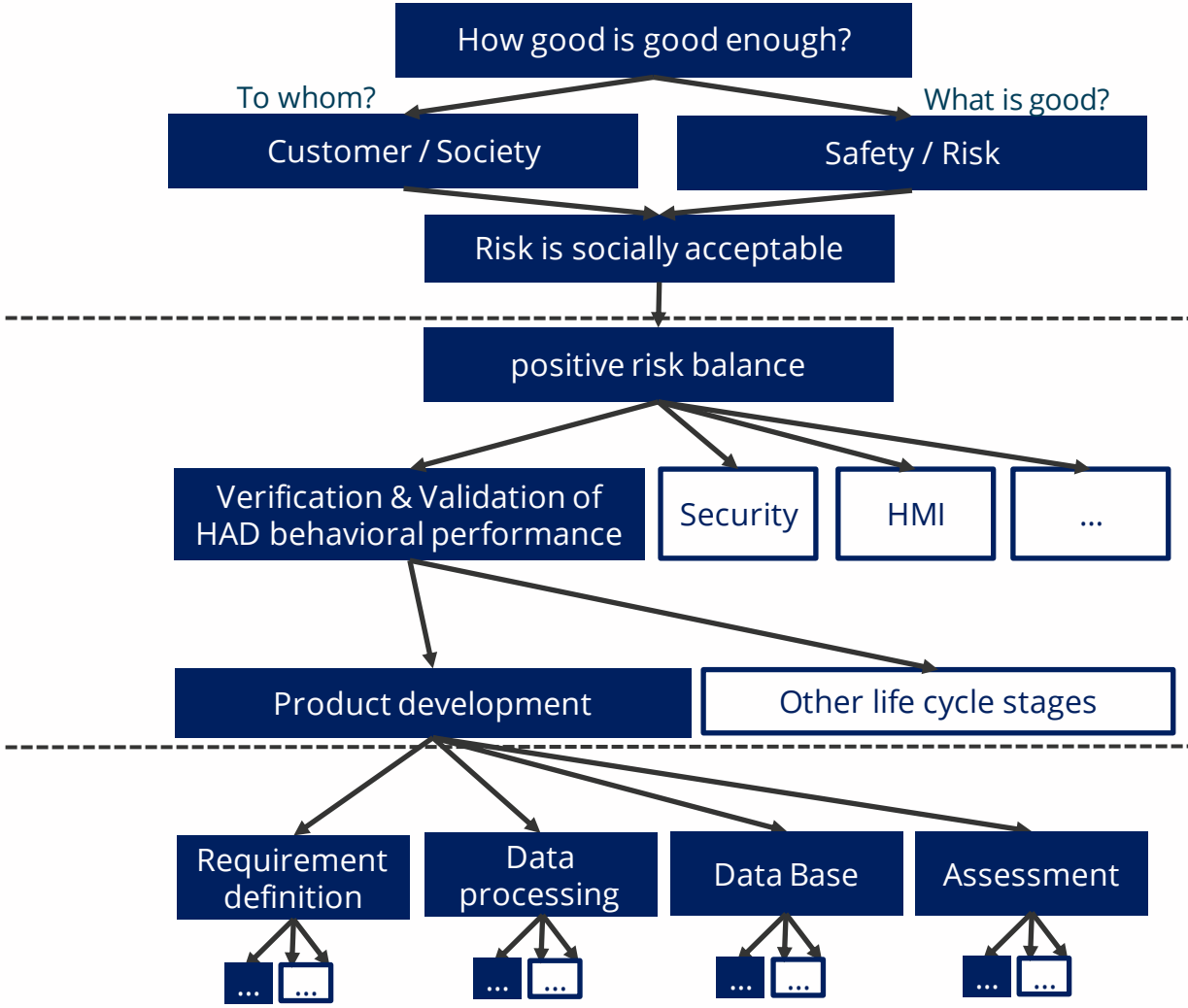
LAYER 3 – ACTIONS, METHODS AND TOOLS
Develop and implement actions, methods and tools to meet the top level safety goals.

LAYER 4 – EVIDENCE
Consider results obtained by applying actions, methods and tools as evident because they are linked to top level goals.



NOT addressed in PEGASUS — EXEMPLARILIY addressed in PEGASUS — Focus of PEGASUS

So what's the answer to the question?



L0 Technology Acceptance

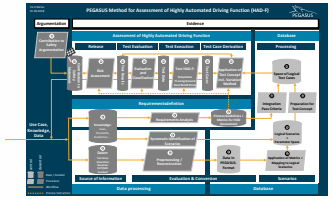
- *„The world in our heads is not a precise replica of reality; our expactations about the frequency of events are distorted by the prevalence and emotional intensity of the messages to which we are exposed."* – Daniel Kahnemann (2011). *Thinking, Fast and Slow* (p.138)

L1 Top Level Safety Goals

- *„... Homologation of automated Systems is acceptable, if they diminute damages in terms of a positive risk balance in comparison to human driving capabilities"* - German Ethics commisstion, June 2017

- *12 NHTSA design principles*

L2



- *PEGASUS and other Methods*

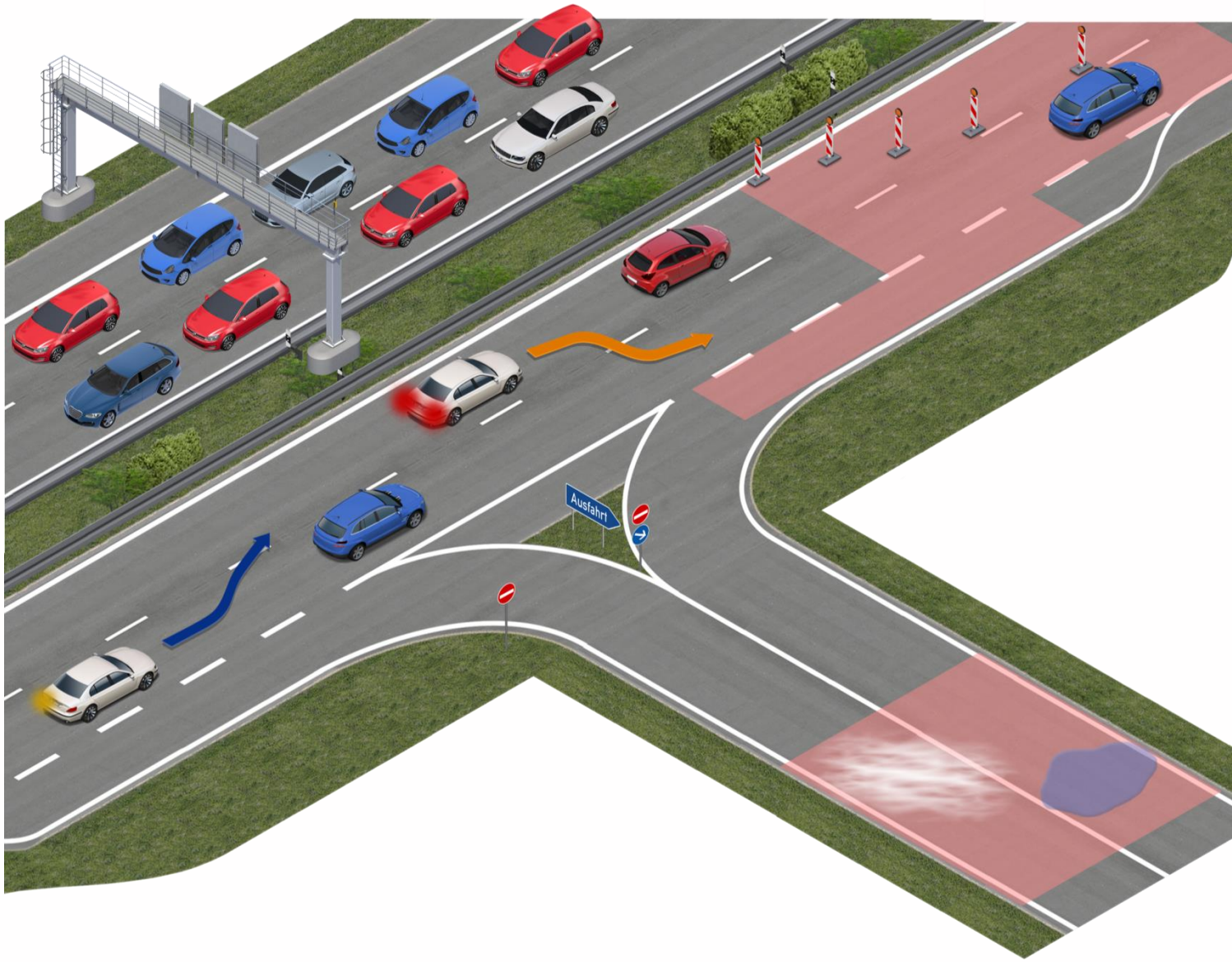
➡ The PEGASUS Method contributes to the Safety Argument

Part 1:
How Good is good enough?

Part 2:
Methods/Tools/Arguments

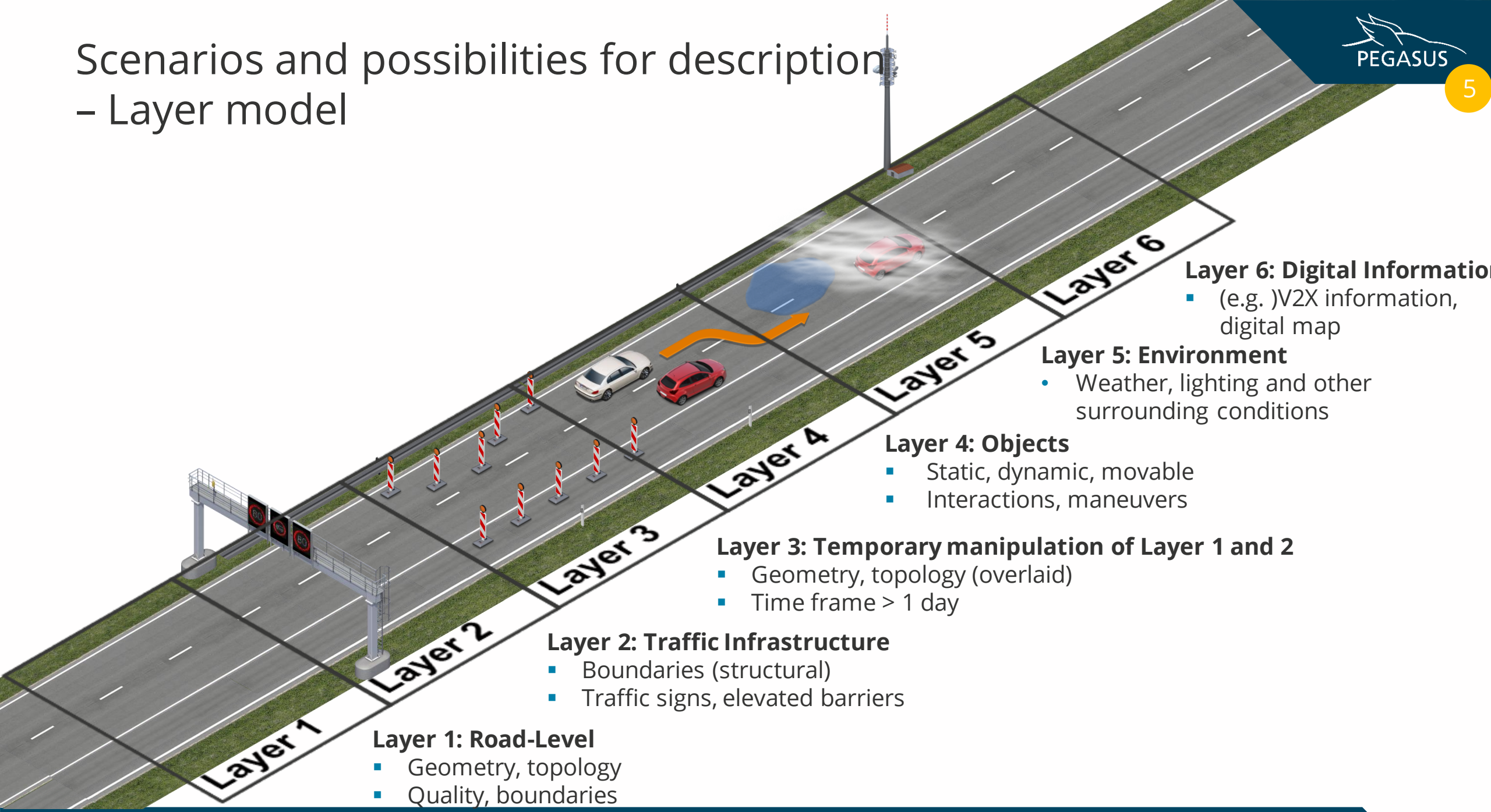
The Highway Chauffeur

- Safeguarding of Level 3 (Highly Automated Driving) function
- Based on an application-oriented example, highway chauffeur
  - Basic function:
    - ✓ Highways or highway-like roads incl. road markings
    - ✓ Speed 0 - 130 km/h
    - ✓ Automated following in stop & go traffic jams
    - ✓ Automated lane changing
    - ✓ Automated emergency braking and collision avoidance
    - ✗ Construction sites
    - ✗ Automated exiting off the highway
    - ✗ Extreme weather conditions



source: VW

Scenarios and possibilities for description – Layer model



Layer 6: Digital Informatio
- (e.g.)V2X information, digital map

Layer 5: Environment
- Weather, lighting and other surrounding conditions

Layer 4: Objects
- Static, dynamic, movable
- Interactions, maneuvers

Layer 3: Temporary manipulation of Layer 1 and 2
- Geometry, topology (overlaid)
- Time frame > 1 day

Layer 2: Traffic Infrastructure
- Boundaries (structural)
- Traffic signs, elevated barriers

Layer 1: Road-Level
- Geometry, topology
- Quality, boundaries (surface)

Scenarios and possibilities for description – Level of abstraction

PEGASUS 5

Functional scenarios

Base road network:

Three-lane motorway in a curve, 100 km/h speed limit indicated by traffic signs

Stationary objects:

-

Moveable objects:

Ego vehicle, Traffic jam;
Interaction: Ego in maneuver „approaching" on the middle lane, traffic jam moves slowly

Environment:

Summer, rain

Logical scenarios

Base road network:

Lane width	[2..4] m
Curve radius	[0,6..0,9] km
Position traffic sign	[0..200] m

Stationary objects:

-

Moveable objects:

End of traffic jam	[10..200] m
Traffic jam speed	[0..30] km/h
Ego distance	[50..300] m
Ego speed	[80..130] km/h

Environment :

Temperature	[10..40] °C
Droplet size	[20..100] µm
rainfall	[0,1..10] mm/h

Concrete scenarios

Base road network:

Lane width	3
Curve radius	0,7 km
Position traffic sign	150 m

Stationary objects:

-

Moveable objects :

End of traffic jam	40 m
Traffic jam speed	30 km/h
Ego distance	200 m
Ego speed	100 km/h

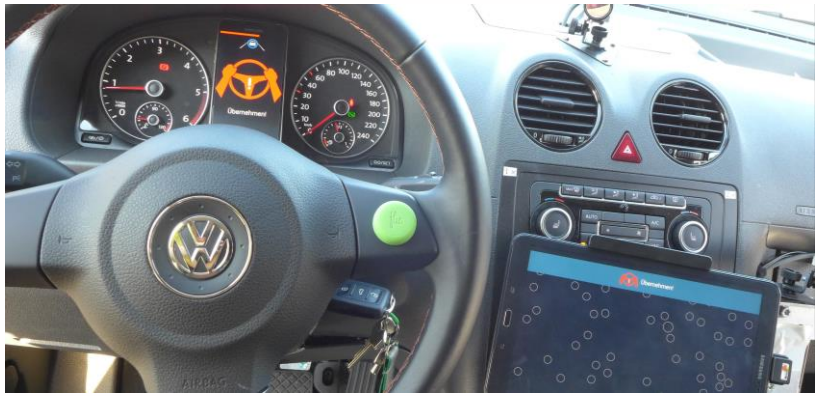
Environment :

Temperature	20 °C
Droplet size	30 µm
rainfall	2 mm/h

Number of scenarios

Level of abstraction

The human driver - driver takeover capability in real traffic



HMI and non-driving related task

- holistic view on safeguarding of HAD requires consideration of the transition to manual
- testing of driver performance with a Level 3 driving function in real traffic on an approx. 120 km long motorway stretch near Cologne
- short takeover times, but partly insufficient or no safeguarding of the surrounding traffic during takeover

takeover time (real traffic)	n	M (SD)	Min	Max	10th percentile	90th percentile
normal traffic	130	3.87 (1.35)	2.02	8.24	2.48	5.87
rush-hour traffic	107	3.21 (0.83)	2.05	6.69	2.46	4.11

- The question arises as to how a previous automated journey affects the handling of an unexpected event immediately after a completed takeover: Do the subjects really have control over the traffic situation after approx. four seconds?
  - A second study on a test track was conducted in order to investigate the subjects' handling of an unexpected event (suddenly braking vehicle in front).
  - A first evaluation of 20 participants shows that all were able to avoid a collision (16 participants by braking, 4 by braking and changing lanes). This could indicate that the human driver is able to handle an unexpected event after a completed takeover. It should be noted that there was no surrounding traffic.
  - The takeover times from the first study were confirmed in the second study.

Modeling Human Performance in Critical Scenarios

- Human Performance in PEGASUS [3]
  - … a minimum requirement for the performance of highly automated vehicles
  - … a benchmark against which highly automated driving functions can be compared [1]
  - … a product of the driver's capabilities and the task demands of the driving scenario [2].

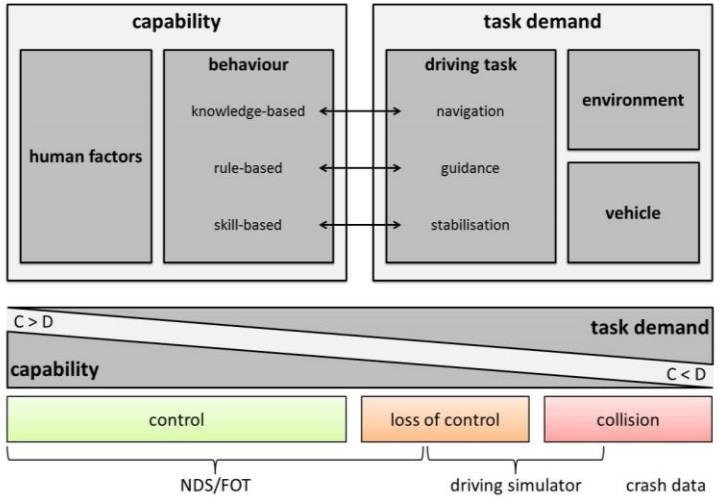


Figure 1. Simplified model of human performance in PEGASUS [3] based on the task-capability-interface model [2], three-level hierarchy of the driving task [4] and levels of human performance [5]. NDS = naturalistic driving study; FOT = field operational test.

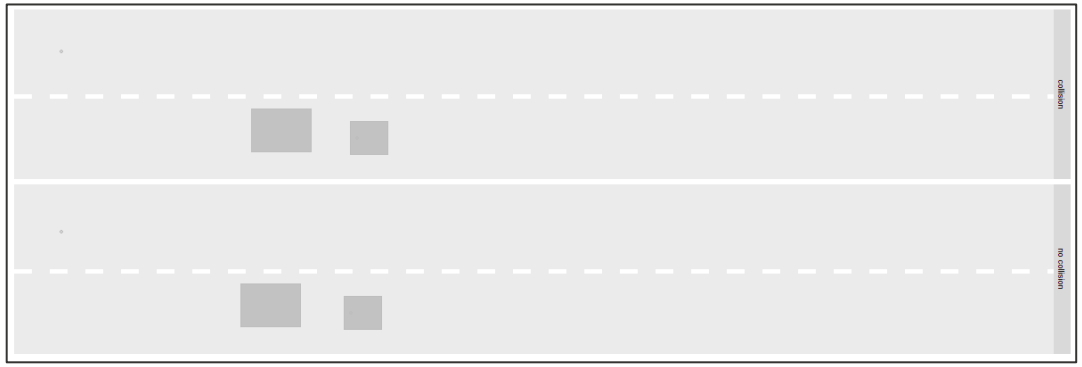


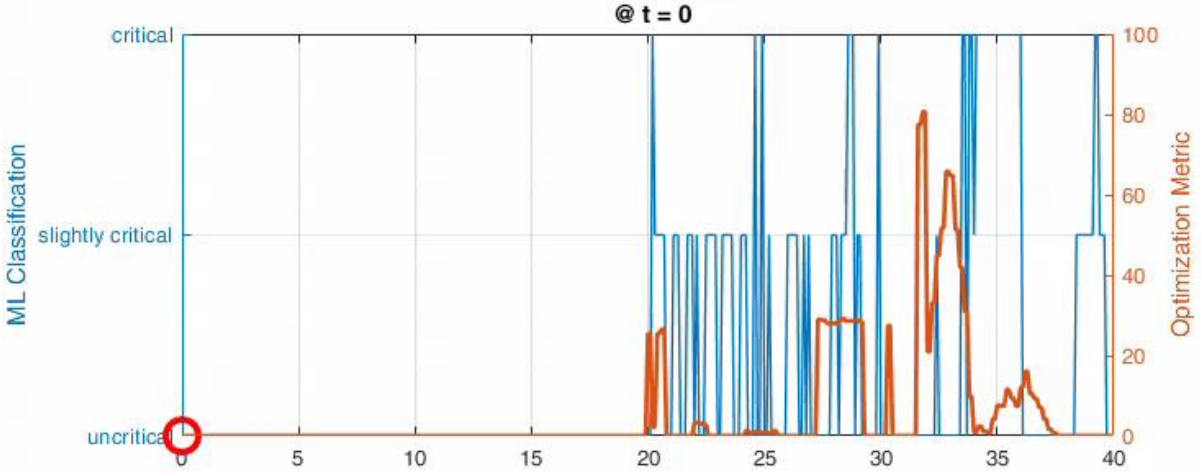
Figure 3. Cut-in scenario: ego speed = 130 km/h; relative speed = 50 km/h. One case with a collision (top) and one case without collision (bottom).

- Driving simulator studies are used to assess the thresholds of human performance in critical situations
  - A stimulus (e.g. a cutting-in vehicle) is presented repeatedly with randomly varying intensity (e.g. criticality of the scenario).
  - Criticality was quantified by time to collision (TTC).
  - The threshold of human performance is represented by the probability to collide at a certain criticality.

Figure 2. Driving simulator used in the two studies. © DLR

Critical Scenarios for Human Drivers – Criticality Metric

- Goal: Definition of a metric to identify critical scenarios
  - Applied on human traffic, but eligible for automation
  - Identification for test case definition based on data recordings
- Two Approaches
  - Machine learned classification based on labelled scenarios
  - Optimization to find the trajectory with minimum criticality



The Human Driver – Impact Analysis

PEGASUS

9

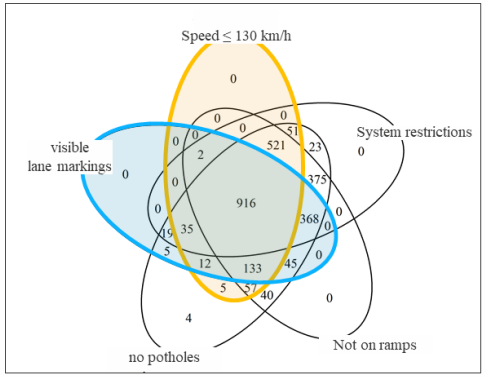
- Computation of the target population and the effectiveness of the highway chauffeur
  - ~27% of all fatalities on highways are adressed by the highway chauffeur
  - ~80% of all crashes of the target population of the highway chauffeur arr caused by human factors

Human Factor		
Alcohol, drugs, fatigue, etc	329	37%
(maybe) Distraction		
Maybe Human Factor		
Lane change interactions		
No Human Factor		
Overtake, standing at the		

	All	Highway Chauffeur		
	GIDAS	Target Population	Ratio to all highways	Ratio to GIDAS All
Cars	33 024	916	35%	2,8%
Injured Persons ISSx ≥ 1	3 671	184	33%	5,0%
Severe injured Persons ISSx ≥ 2,5	1 116	52	28%	4,7%
Fatalities	362	21	27%	5,8%

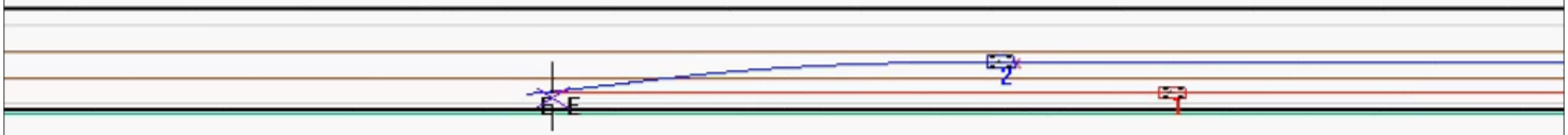
GIDAS
GERMAN IN-DEPTH ACCIDENT STUDY

- Identification of extensions to the highway chauffeur or further actions, which have the highest benefit of increasing the target population
  - e.g. Extend the function that it could drive without lane markings or the lane markings have to be intact and visible



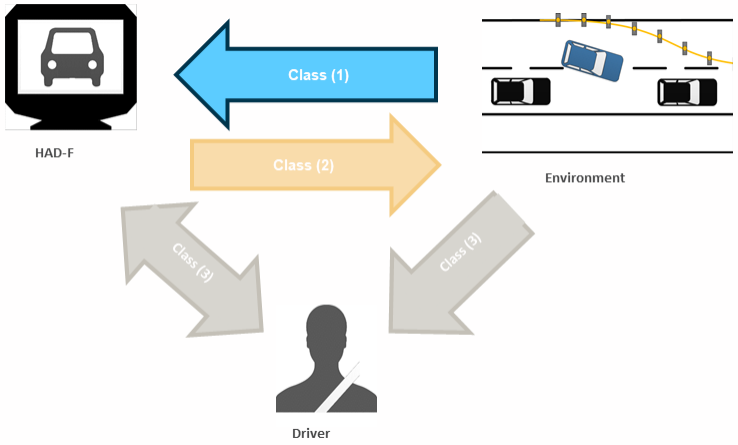
- Simulation of a generic highway chauffeur and comparision with the human

The human driver from GIDAS



Potentially Challenging Scenarios for Highly Automated Driving

- Scenarios that are relatively easy to handle for humans may be challenging for HAD-F (e.g. missing lane markings)
- These scenarios need to be identified early to be tested exhaustively
- In order to do so and to ensure a view at this problem from different perspectives these scenarios were divided into three classes



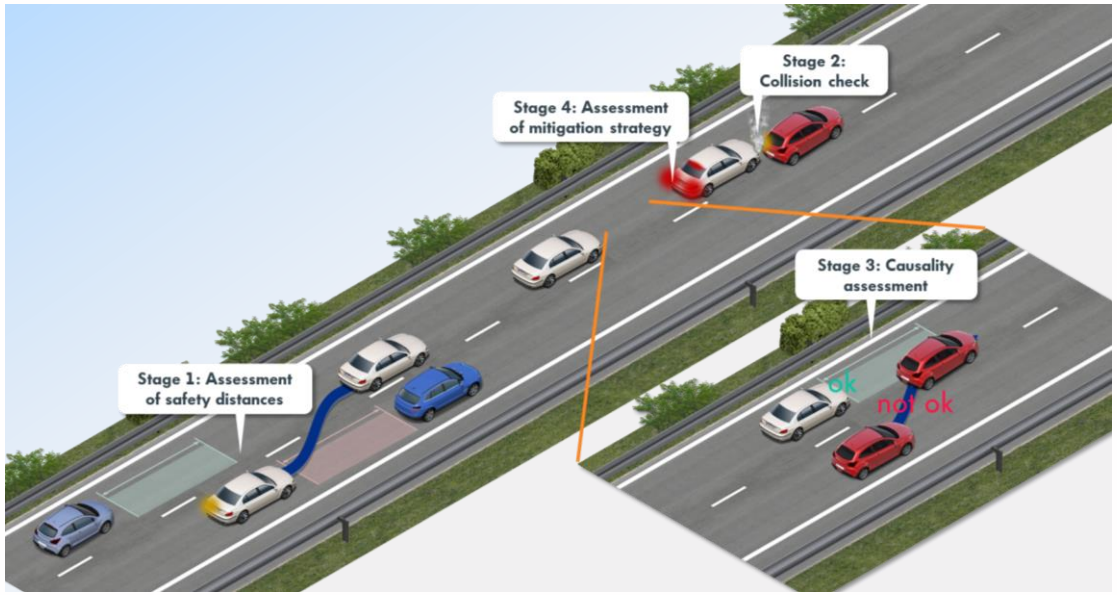
- Challenges that arise from
  - Class (1): Impacts of the environment on the automation (e.g. performance limitations of sensors, misguided interpretation of the environment)
  - Class (2): Impacts of the automation on other traffic participants (e.g. reaction of automation cannot be anticipated by other road users)
  - Class (3): Interaction with the human driver (e.g. mode confusion)

- For each of these classes a systematic method was developed to identify potentially challenging scenarios early with the help of expert knowledge

Assessment of a single test-case

Overall Result	Safety distances (Stage 1)	Collision (Stage 2)	Causality (Stage 3)	Mitigation Strategy (Stage 4)
FAIL	fail	fail	-	fail
PASS-	fail	pass	-	-
PASS/FAIL	fail	fail	pass/fail	pass
PASS	pass	-	-	-

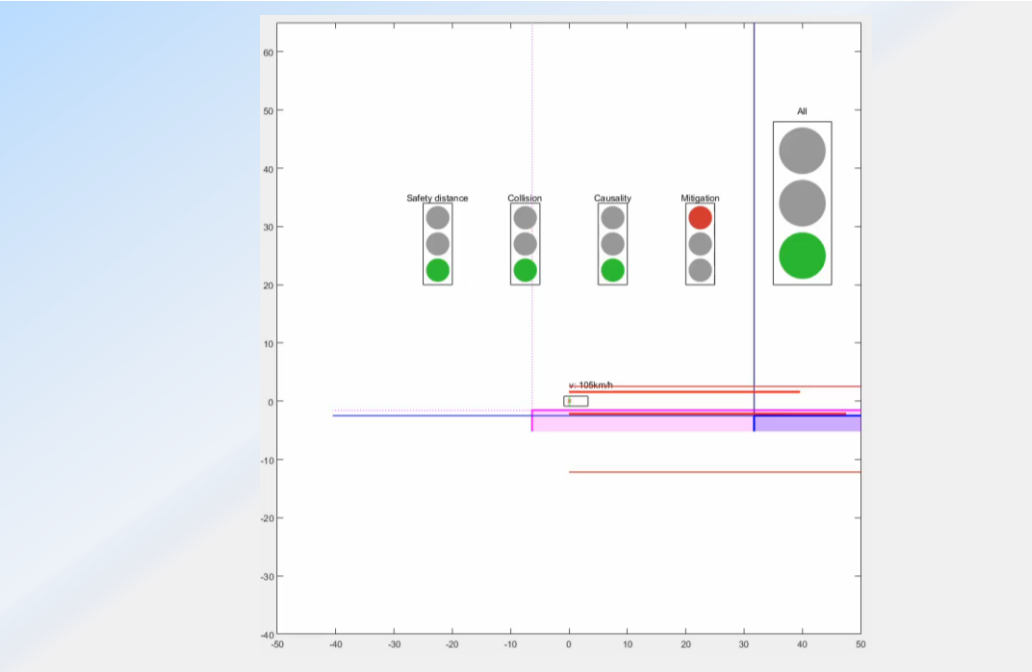
Picture, example of overall test-case rating based on the 4 proposed stages. 0 and 1 are indicating if a stage is failed or passed, respectively.



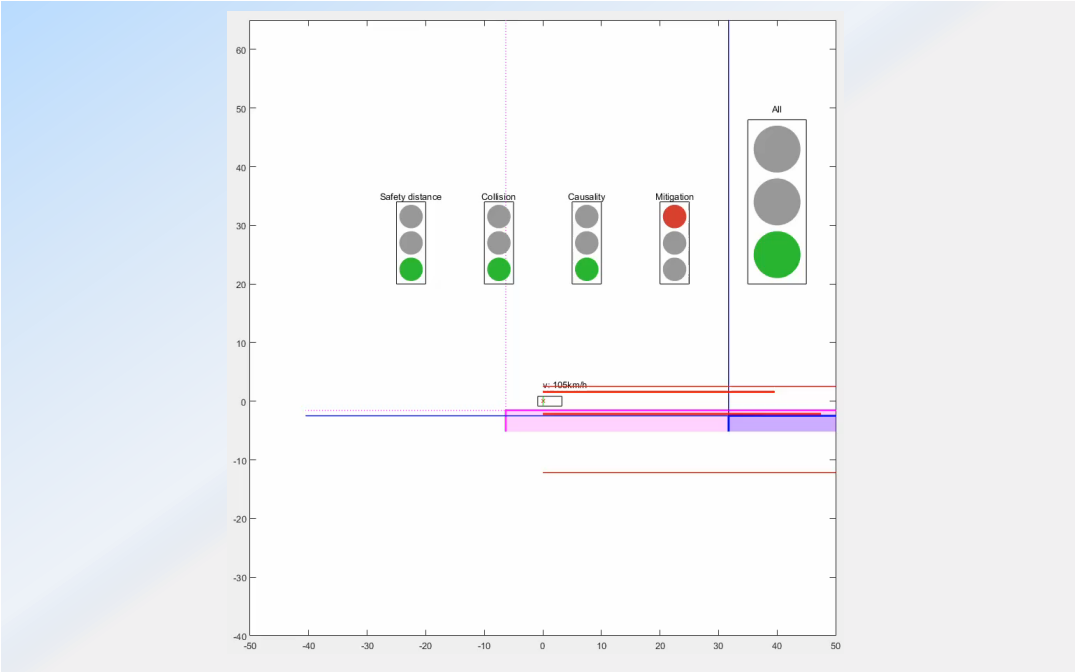
Picture, application the different safety criteria over time. The result is PASS with stage 1 fail, stage 2 fail, stage 3 pass und stage 4 pass.

- The overall rating of a test-case is derived by aggregating the time-discrete results of the multiple stages.
- The contribution of the different stages to the overall test-case result differs depending on their character.

Example for the multi-stage safety assessment



Video, re-simulation of a real world crash, where a merging car violates appropriate safety distances. The ego-vehicle (in this case a human driver) responses with a late braking intervention.



Video, same real world crash, where the ego-vehicle is now an automated car. In this simulation, the automated vehicle brakes earlier and thus avoids the crash.

PEGASUS

Vielen Dank für Ihre Aufmerksamkeit!

Many thanks for your attention!