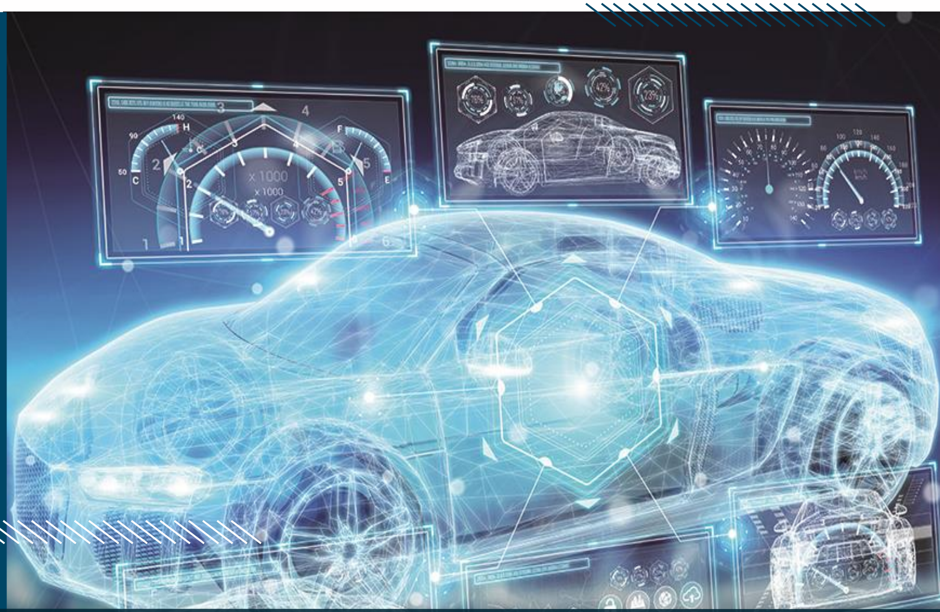
1st NDS Public Conference | June 13, 2019, Munich

HOW SAFE IS SAFE ENOUGH? PEGASUS DELIVERS THE STANDARDS FOR HIGHLY AUTOMATED DRIVING

Udo Steininger, TÜV SÜD



PEGASUS

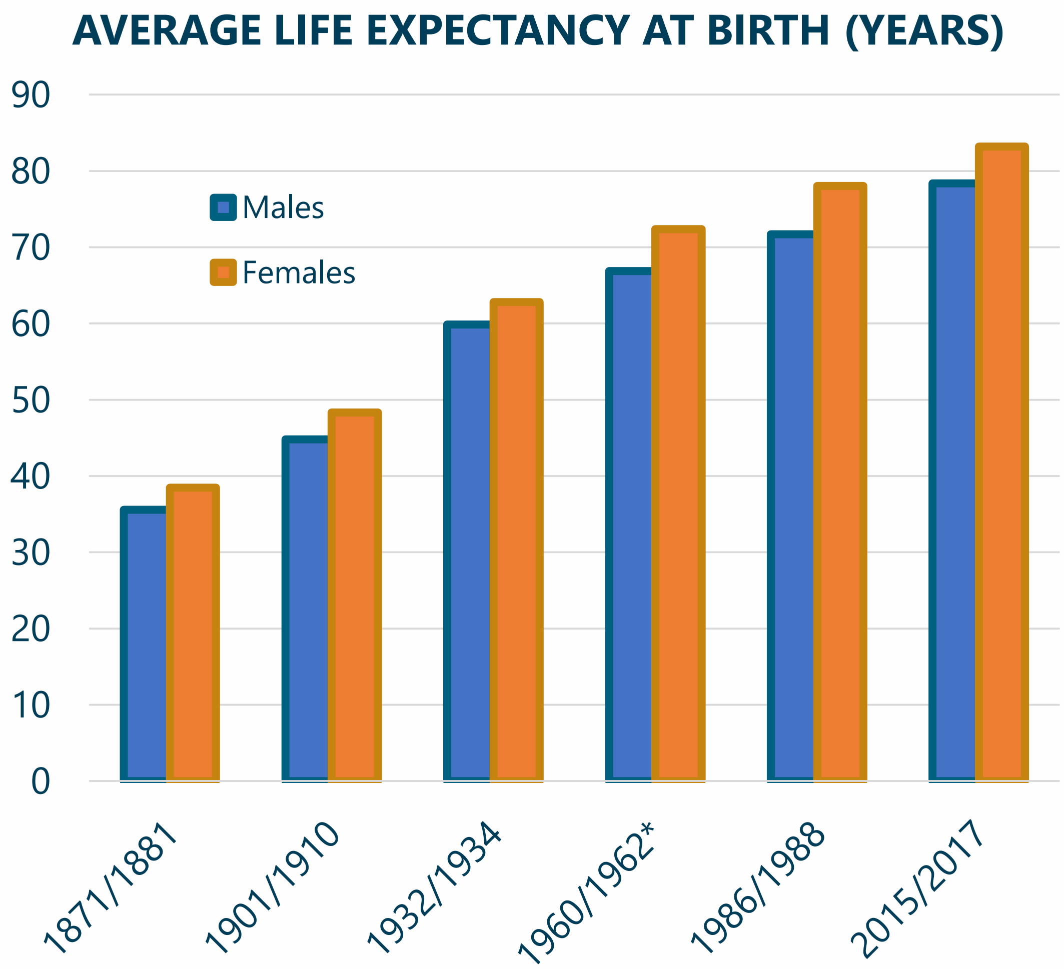
Supported by:

Federal Ministry for Economic Affairs and Energy

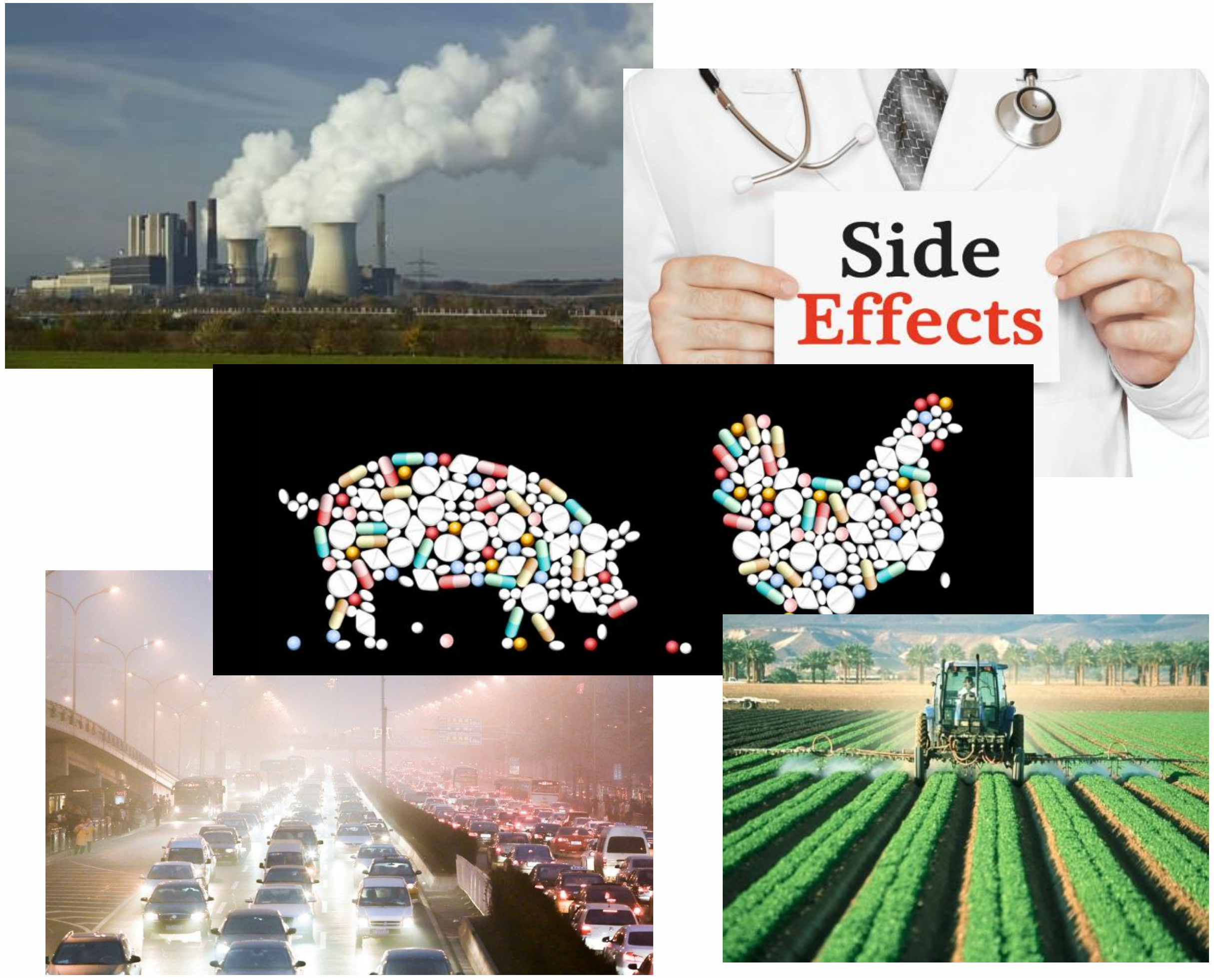
on the basis of a decision by the German Bundestag

To get in the mood:

What goes wrong with our perception of safety and risk?



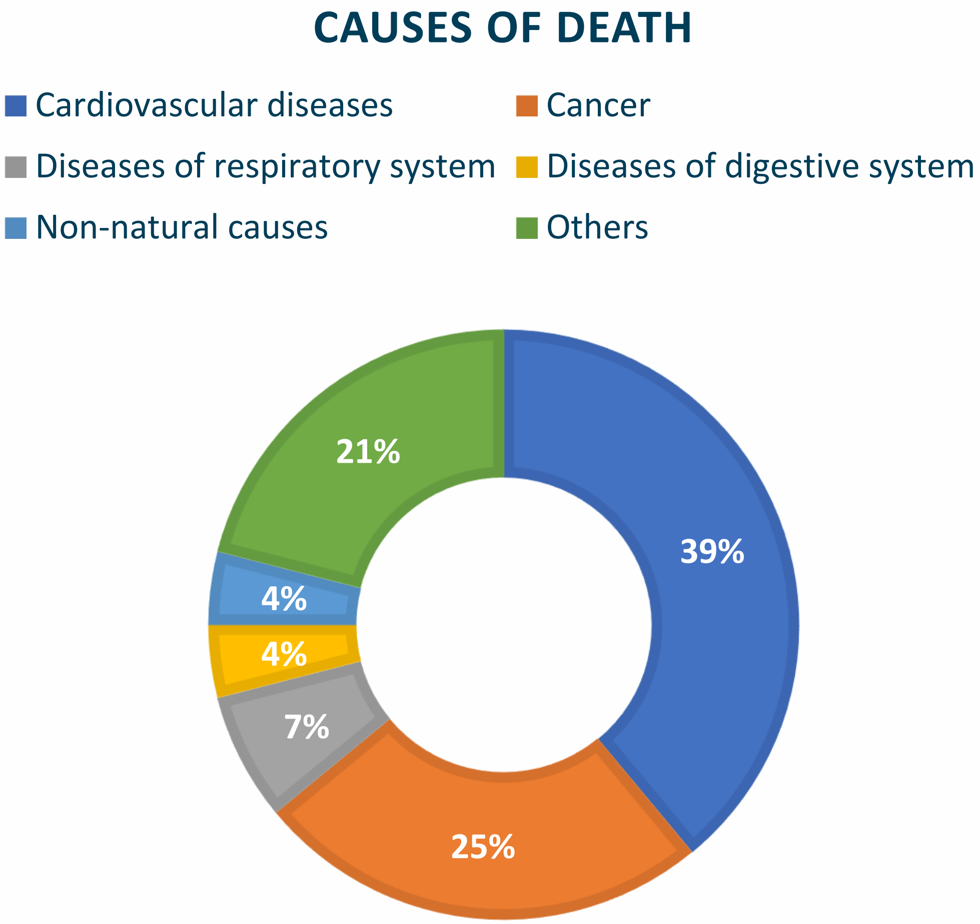
* Former Federal Republic
http://www.demografie-portal.de/SharedDocs/Informieren/DE/ZahlenFakten/Lebenserwartung.html



Images: Spiegel online; ihealth; meat free monday; tasting page

To get in the mood:

What goes wrong with our perception of safety and risk?



Statistisches Bundesamt (Destatis) Pressemitteilung Nr. 022, 19.01.2017

Images: Spiegel online; Shutterstock; Fotolia; dpa

Content

PEGASUS contribute to answer the question …

How safe is safe enough and

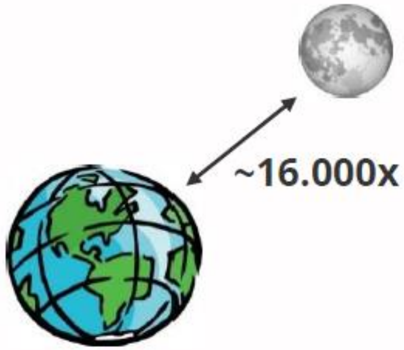
how can we verify that Highly Automated Driving (HAD) achieves the expected performance consistently?

…by introducing a

Scenario Based Approach

… considering that it is not possible to cover the test space for HAD systems with conventional duration tests

- Actual state: 614 million kilometres between two fatal accidents on highways
- Target: Halve the risk of human drivers with 95% confidence
- Result: 6.14 billions kilometres test distance = 16.000 times distance earth to moon



PEGASUS project

January 2016:

Project start with 17 partners

OEM: Audi, BMW, Daimler, Opel, Volkswagen
Tier 1: ADC, Bosch, Continental
Test Lab: TÜV SÜD
SMB: fka, iMAR, IPG, QTronic, TraceTronic, VIRES
Scientific institutes: DLR, TU Darmstadt

Subcontracts: IFR, ika, OFFIS

Key-facts:

42	Months term
149	Man-years
34,5	Mio. EUR budget
4	Sub projects
13	Workpackages
38	Sub workpackages

Mid 2016:

Convention of an Advisory Board

- Federal Ministry for Economic Affairs and Energy
- Federal Ministry of Transport and Digital Infrastructure
- Federal Ministry of Justice and Consumer Protection
- German Association of the Automotive Industry (VDA)
- German Road Safety Council (DVR)
- ADAC

Associated partner:

Federal Highway Research Institute (BASt)

dSPACE

PEGASUS structure

November 2017:
PEGASUS-Half-Time-Event in Aachen

Presentation of Intermediate Results

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 complete-ness 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 proving grounds, what must be tested on the road?

Reflection of Results & Embedding
- Is the concept sustainable?
- How can the PEGASUS-Partners embed the results?

For the first time: Presentation of the PEGASUS-Approach

→ PEGASUS becomes international

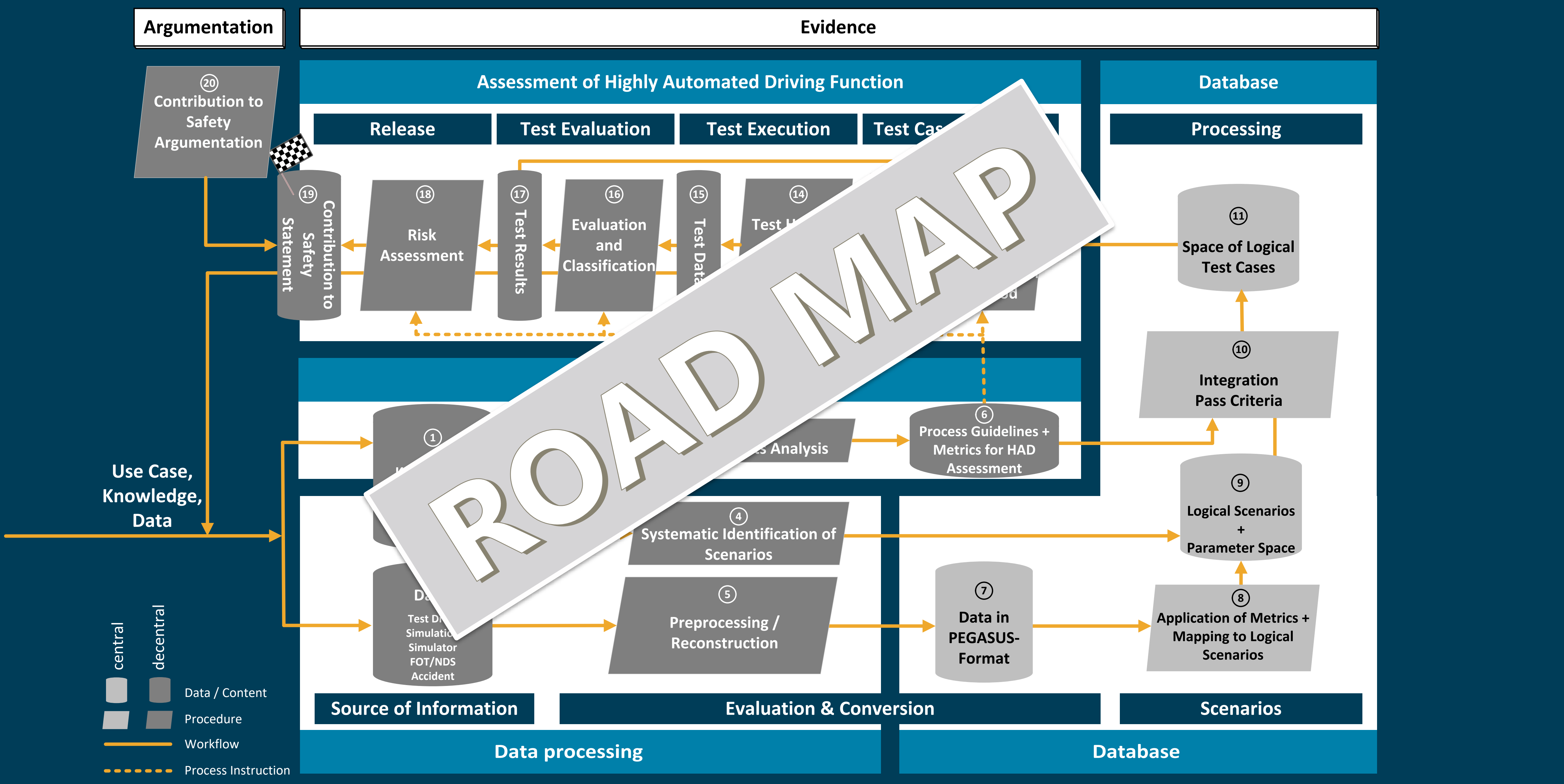
PEGASUS international

World wide:
ISO: ISO/TC 22/SC 33/WG 9 and WG16 as well as ISO TR21959 Part 2 und SOTIF
DIN SAE: Spec Project Terms and definitions

Addtl. Cooperation Requests & bilateral Exchange:
→ FP Nouvelle France Industrielle, AutoAlliance, Jaguar LandRover, Hyundai, Volvo, RDW, etc.

Content

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



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

PEGASUS

Argumentation

Evidence

Assessment of Highly Automated Driving Function

Database

Requirementsdefintion

Use Case,
Knowledge,
Data

Data processing

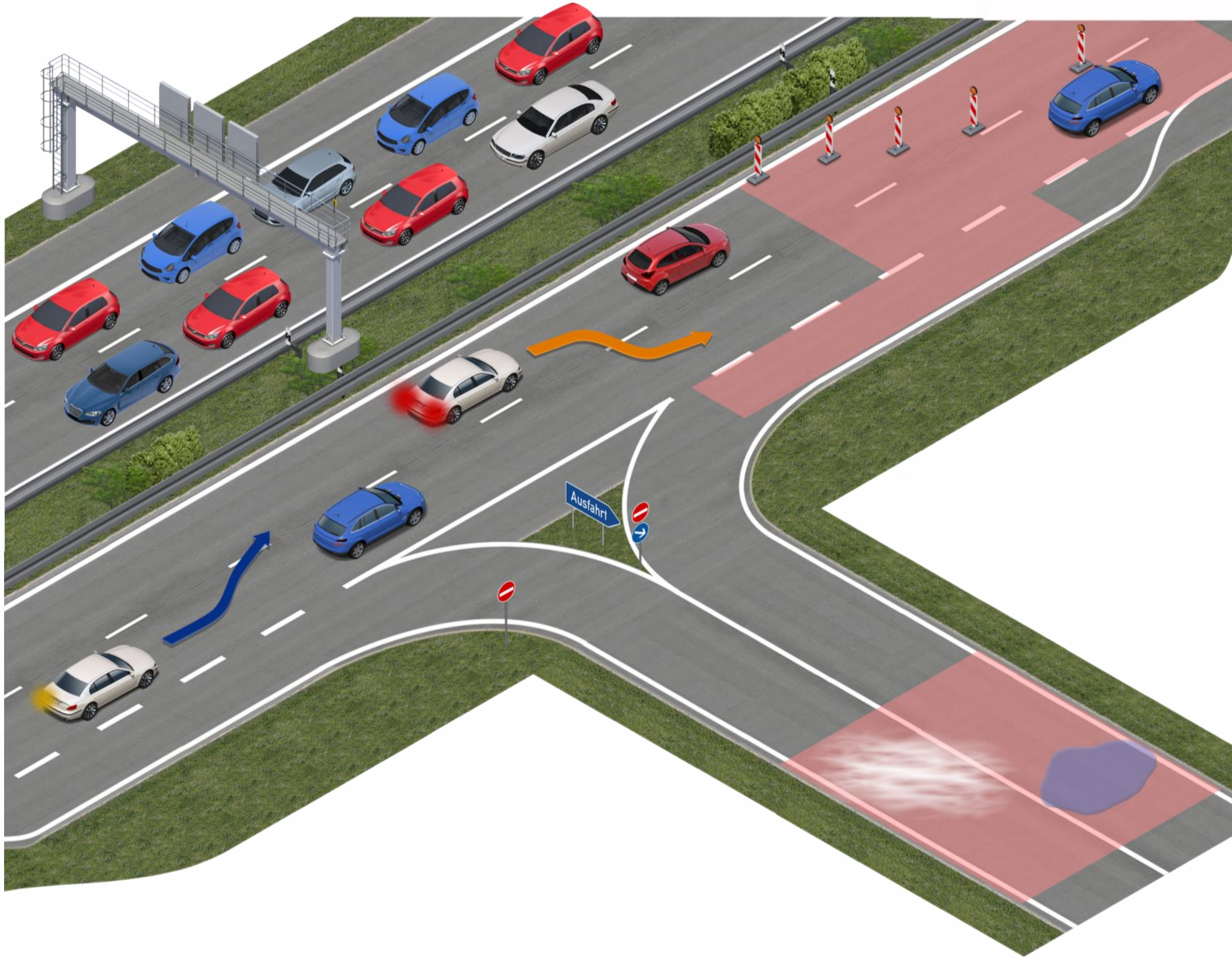
Database

Use case

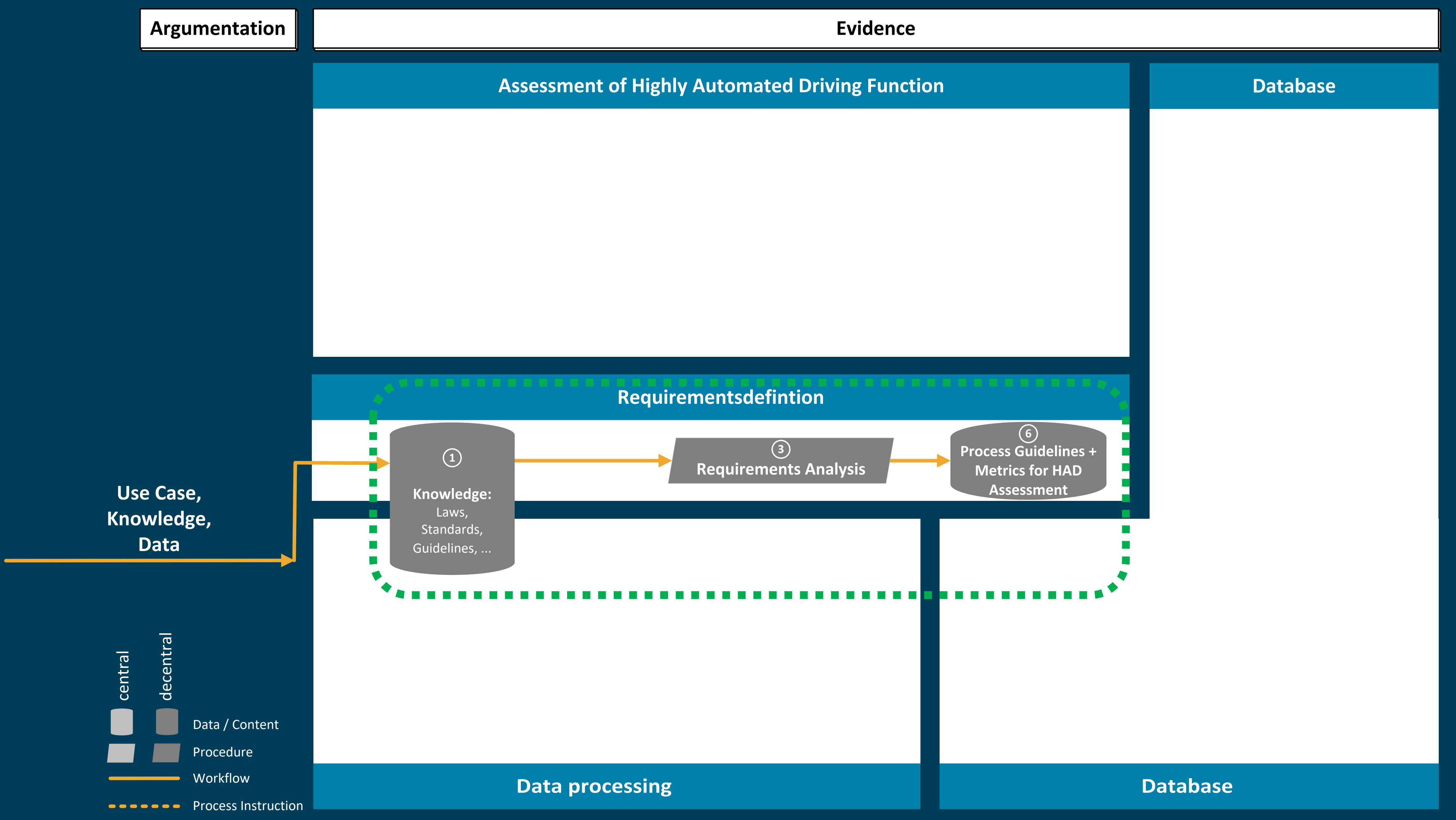
PEGASUS

- SAE Level 3 function (Highly Automated Driving)
- 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
    - × Entering and exiting highway
    - × Extreme weather conditions



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



Proof of sufficient safety

NECESSARY CONDITION

- Social consensus regarding acceptable risk is regulated by liability laws [e.g. German ProdSG §5(2)]: A product that conforms to standards or other relevant technical specifications is presumed to comply with product safety requirements
- Development according to ISO 26262 and ISO/PAS 21448 ensures "absence of unreasonable risk"

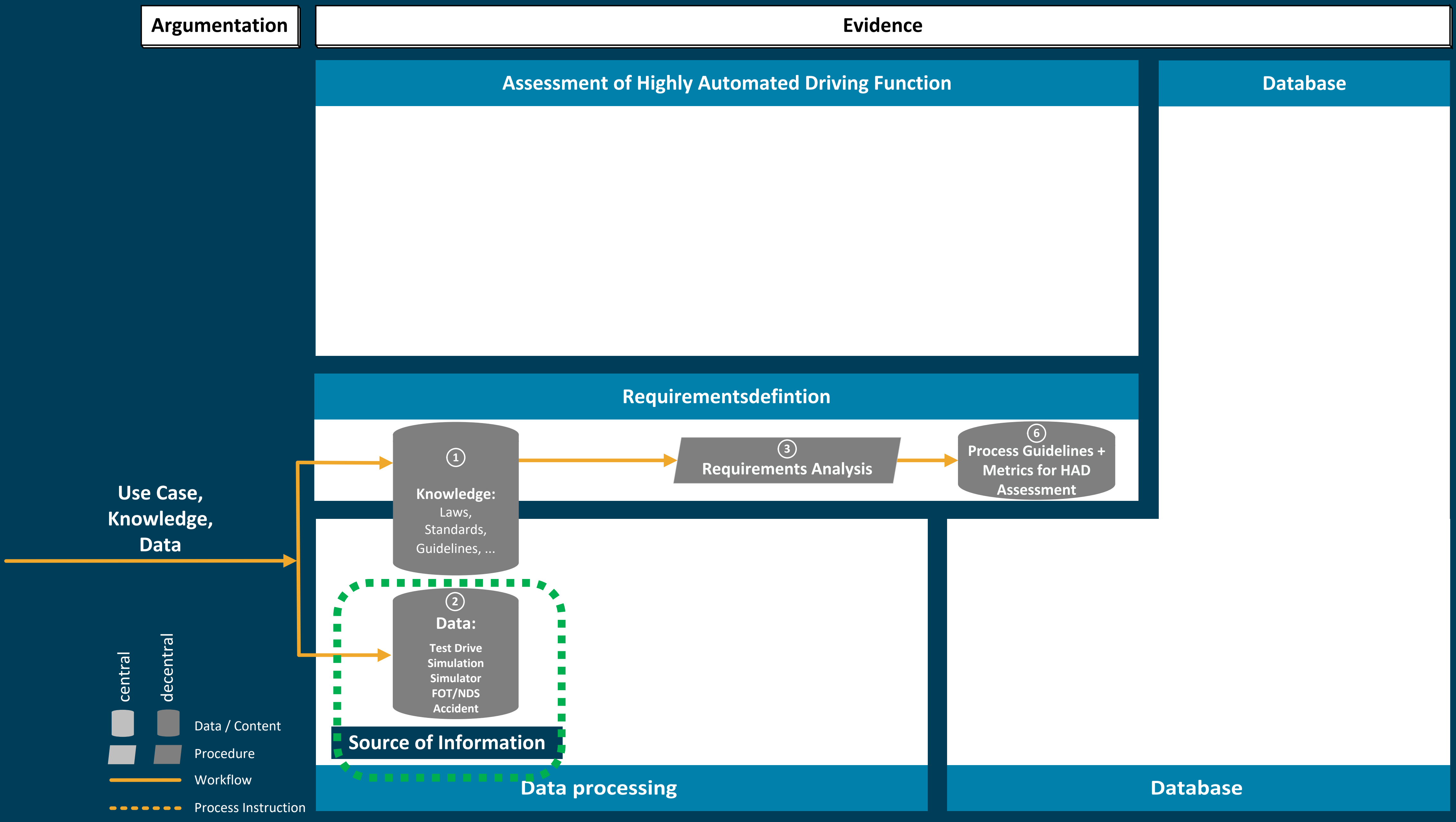
SUFFICIENT CONDITION

- Rules of the Ethics Committee [Ethik-Kommission Automatisiertes und Vernetztes Fahren, BMVI, Juni 2017]:
  - HAD is reasonable if it promises to reduce damage in the sense of a positive balance of risk compared to human performance
  - If there is a fundamentally positive balance of risk, technically unavoidable residual risks do not preclude an introduction
- Experts from several governments, scientific institutes and the business community expect benefit of vehicle automation for traffic safety (e.g. NHTSA, EC, German Federal Government, VDA, VDI)
- The test concept developed in PEGASUS ensures exemplarily, that the systems achieve at least human driving performance

© Wikipedia

Content

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



Input data

NDS / FOT

Simulation

Simulator studies

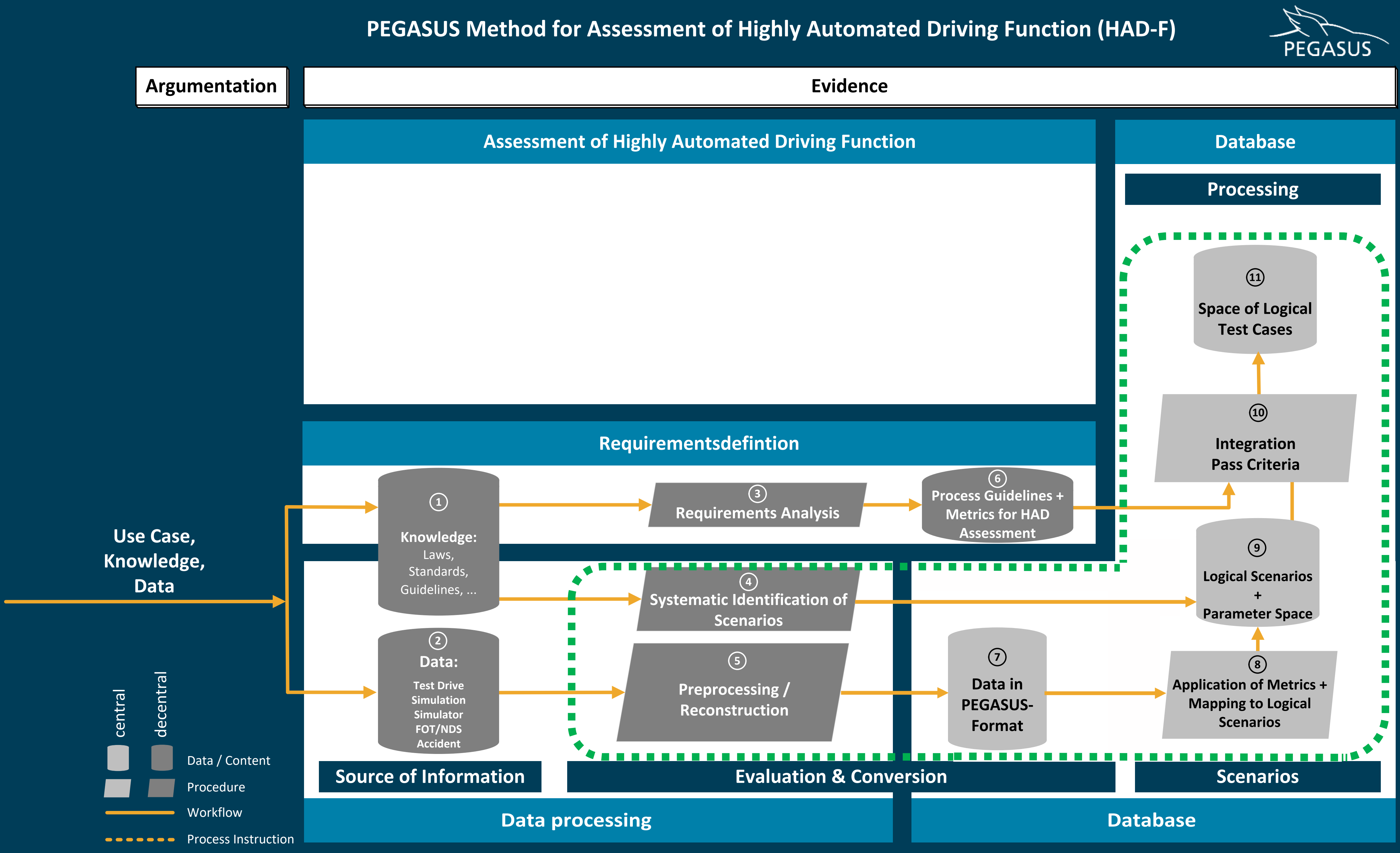
Real world driving

Crash

GIDAS

GERMAN IN-DEPTH ACCIDENT STUDY

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



Scenarios and possibilities for description – Levels of abstraction

PEGASUS

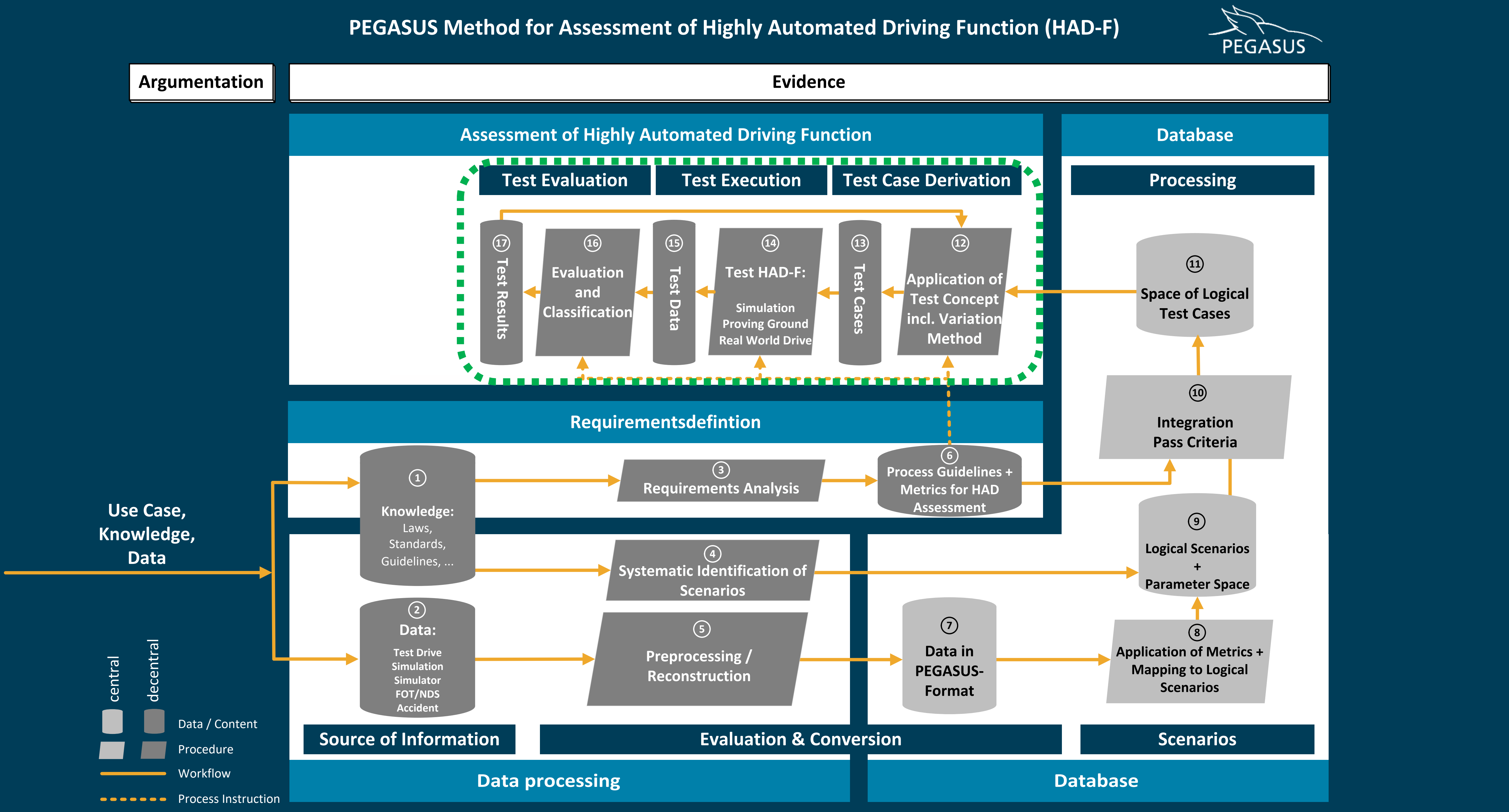
Functional scenarios	Logical scenarios	Concrete scenarios
Base road network: Three-lane motorway in a curve, 100 km/h speed limit indicated by traffic signs	**Base road network:** Lane width [2…4] m Curve radius [0,6…0,9] km Position traffic sign [0…200] m	**Base road network:** Lane width 3 Curve radius 0,7 km Position traffic sign 150 m
Stationary objects: -	**Stationary objects:** -	**Stationary objects:** -
Moveable objects: Ego vehicle, Traffic jam; Interaction: Ego in maneuver „approaching“ on the middle lane, traffic jam moves slowly	**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	**Moveable objects :** End of traffic jam 40 m Traffic jam speed 30 km/h Ego distance 200 m Ego speed 100 km/h
Environment: Summer, rain	**Environment :** Temperature [10…40] °C Droplet size [20…100] µm rainfall [0,1…10] mm/h	**Environment :** Temperature 20 °C Droplet size 30 µm rainfall 2 mm/h

Number of scenarios

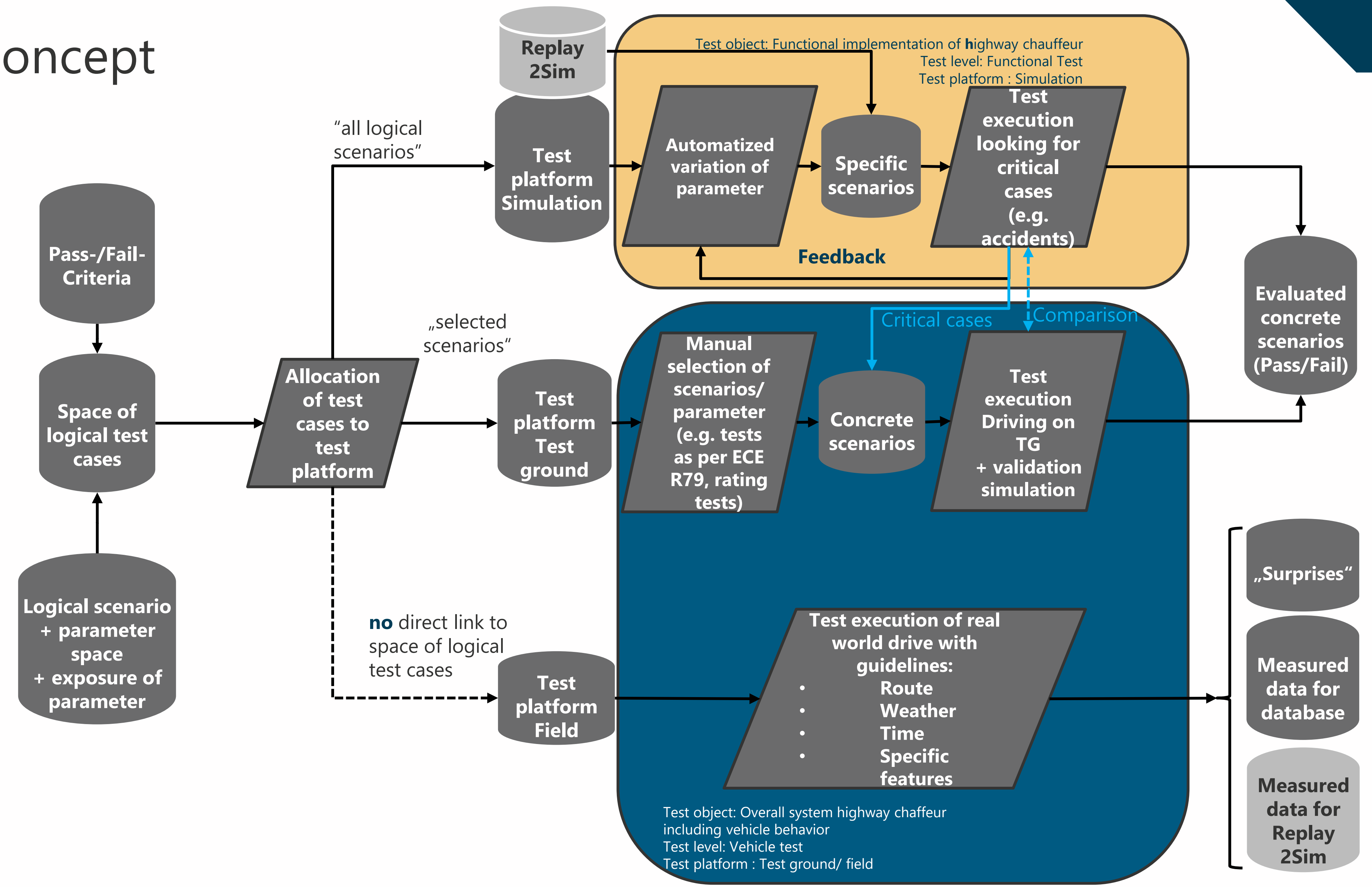
Level of abstraction

Content

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

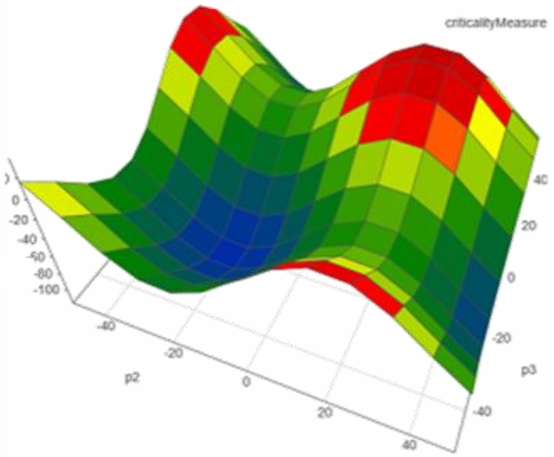


Test concept

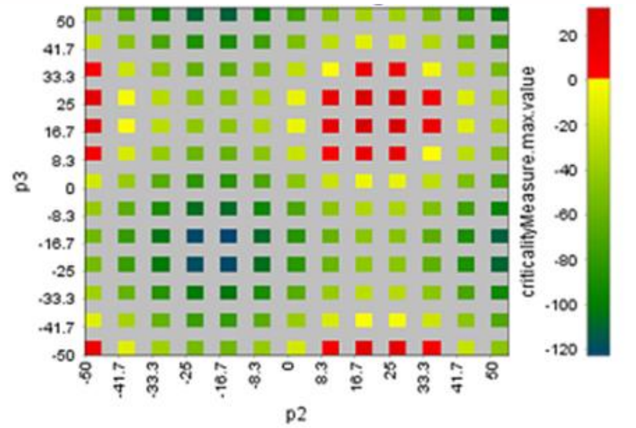


Test objectives for simulation

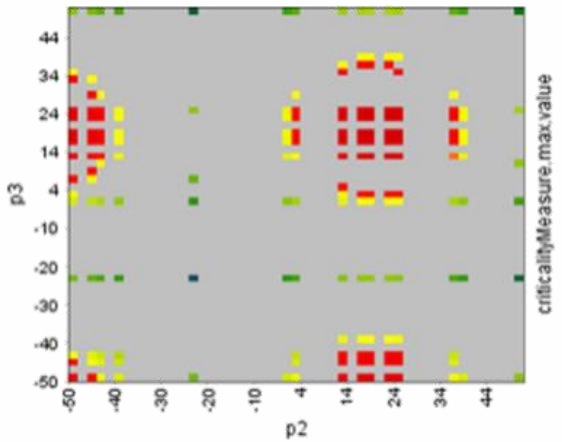
- <u>Search</u> for safety violations / worst case(s)



- <u>Characterize</u> the regions with safety violations, e.g. find their borders



- <u>Deliver</u> coverage reports for one or for a suite of experiments

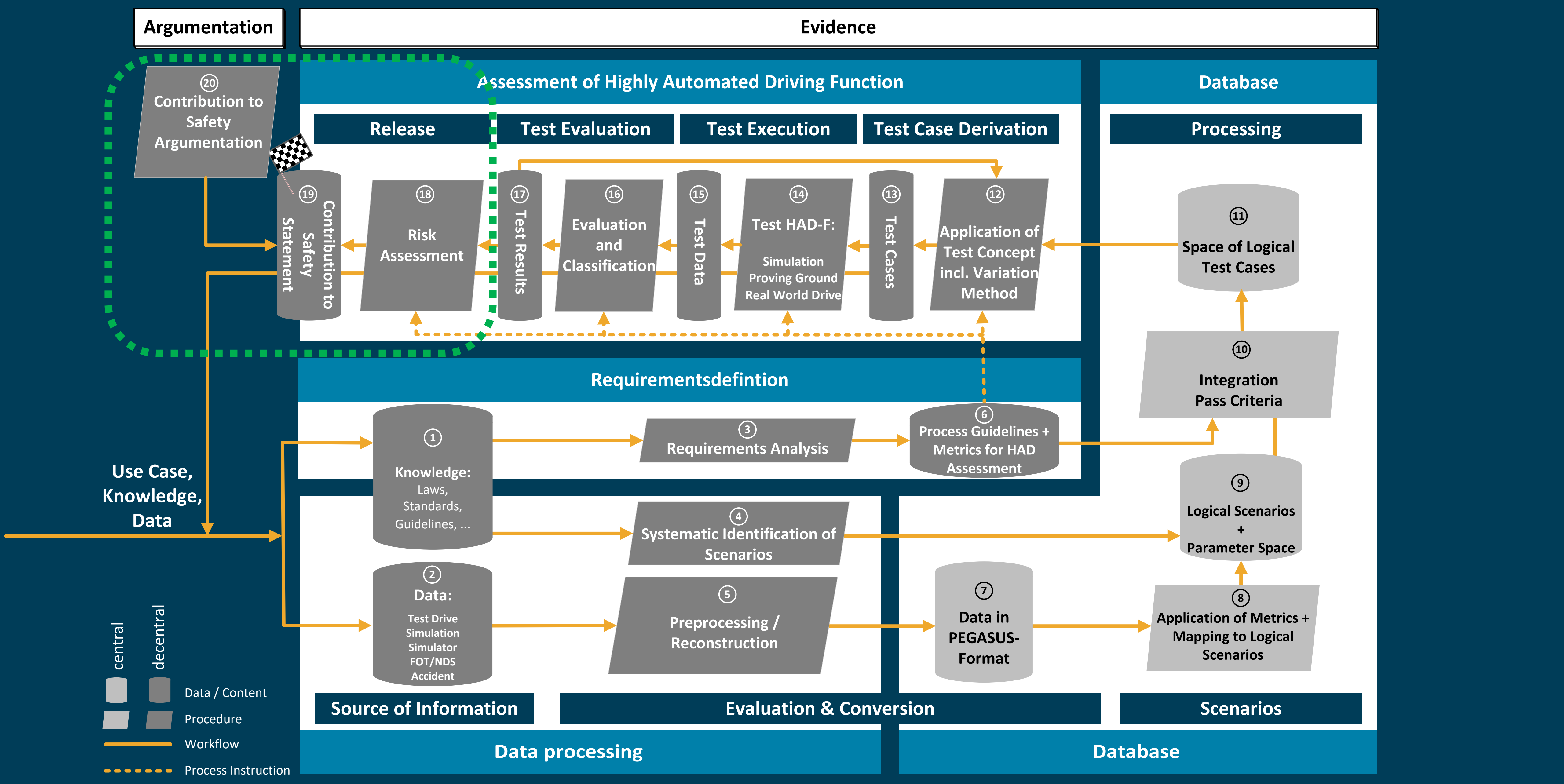


➔ Assessment result for concrete sample scenario depending on multiple parameters. Color range form green (not critical) to red (critical)

Proving ground tests - Automated traffic simulation vehicle (TSV)

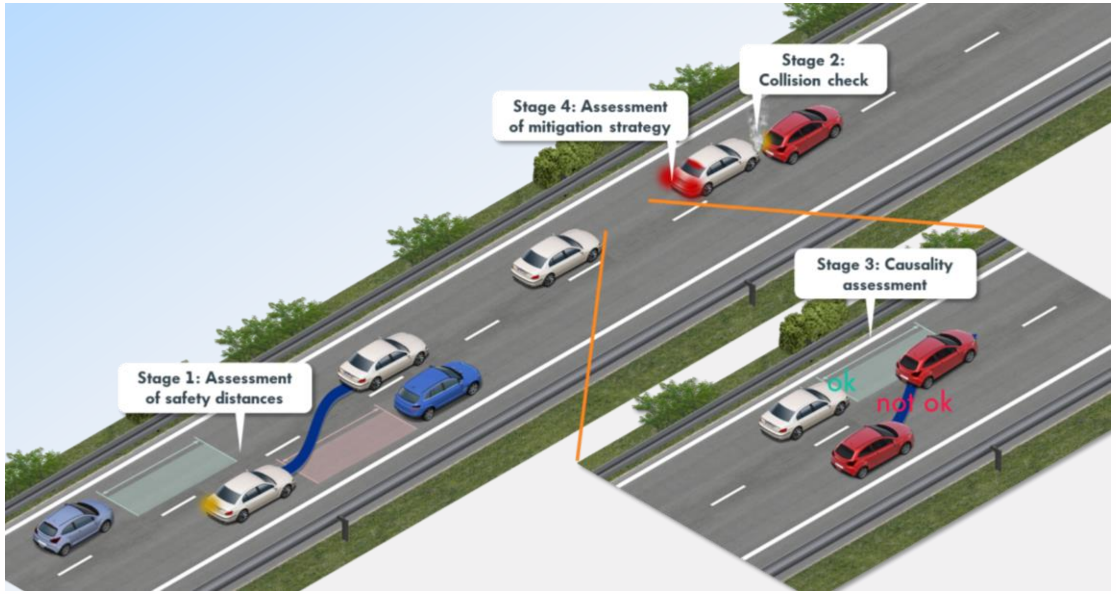
Proving ground tests - Right cut in scenario with vehicle under test (VUT), guided soft target (GST) and 2 TSV

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



PEGASUS

Safety Statement - Assessment of a single test-case



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.

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.

- The overall rating of a test-case is currently 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.
- Further knowledge about exposure and significance will improve strength of argument

Layers of the Safety Argumentation

Automated Driving Systems (ADS) are widely ***accepted*** *in the public.*

Motivation

There is an understanding of what **factors** foster acceptance of ADS.

0

Context

1 **Top level goals** are set to be met in order to achieve acceptance of ADS.

2 **Logical structure** of the Safety Argumentation links top level goals with methods & tools and their results.

3 The Safety Argumentation is implemented using **methods & tools**.

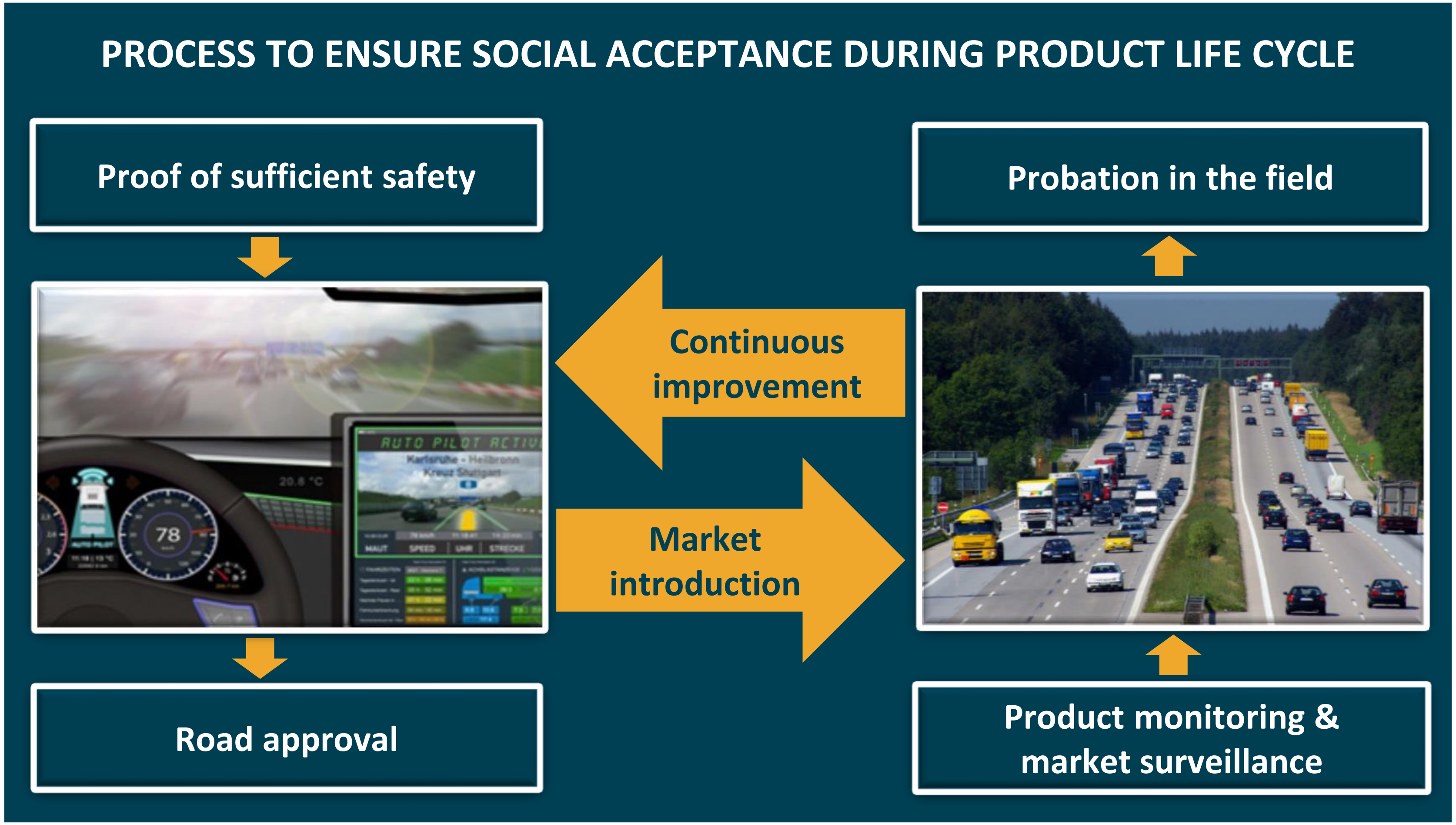
4 **Results** become evident when they can be traced back to the achievement of a goal.

Argumentation / Approval Recommondation

Content

PEGASUS results and product life cycle

- PEGASUS delivers a method for the assessment of level 3 HAD functions and an exemplary tool chain
- Valid statistical proof, that HAD actually meets the aforementioned safety expectations, can not be provided before it is launched on the market
- Not only proof of sufficient safety is necessary but also probation in the field and continuous improvement of systems



Outlook

- Legal: Transfer of results to national and international legislation, regulation and standardization

- Technological:
  - Extension of autonomous driving domain to urban areas and outside cities
  - Higher levels of automation, Car2X (security and privacy), AI (proof of safety)…

- For higher levels of automation, completely new system architectures - and corresponding new safety requirements - will arise, driven by
- change from fail safe to fail operational systems (homogenous redundancy)
- increasing complexity of the processing (diversity, i.e. processing channel with low or without safety integrity level and safety monitoring channel(s) with high safety integrity level)

- Not only AD systems themselves will be affected but also braking, steering and power train as well as – for example – navigation, (high-precision) positioning and other map-based functions in the vehicle or at a backend server

Udo Steininger

Team Leader Automotive
TÜV SÜD Rail GmbH

Barthstr. 16
80339 München, Germany

Phone +49 89 5791-3163
Mobile +49 160 3601992

udo.steininger@tuev-sued.de