PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

Mid-Term Presentation 15 / 16 March 2022

VVM safeguarding automation – how to ensure a safe operation of an automated driving system by a methodological approach? - an interims report

Helmut Schittenhelm, Mercedes-Benz AG

Supported by:

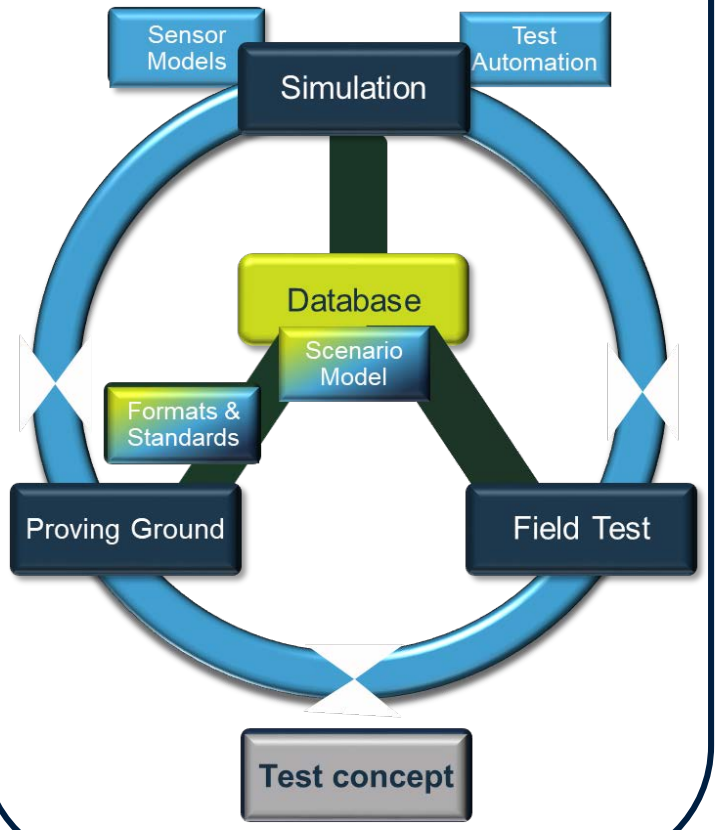
Federal Ministry for Economic Affairs and Climate Action

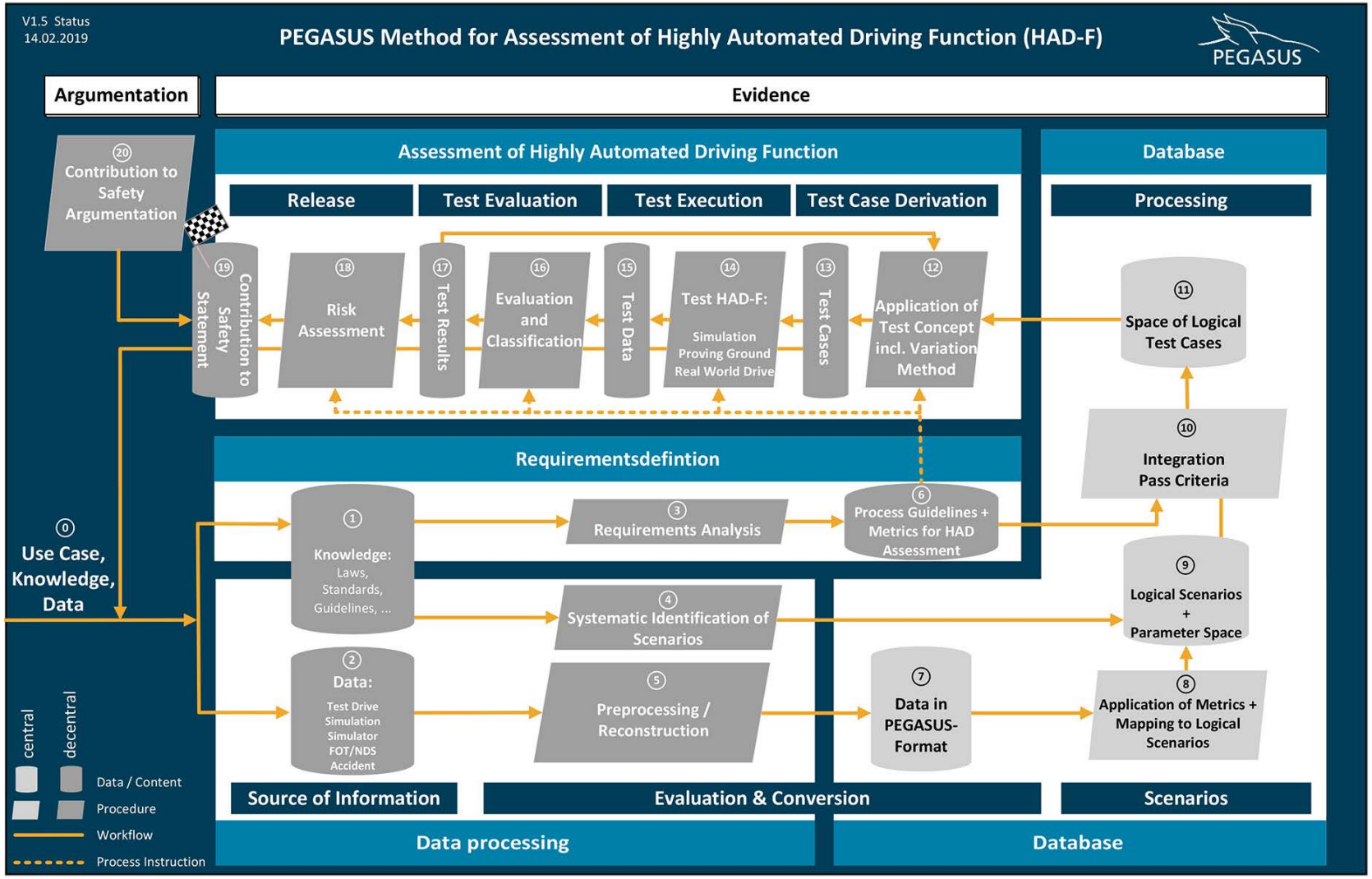
on the basis of a decision by the German Bundestag

Starting point PEGASUS- Method: Final project presentation 05-2019

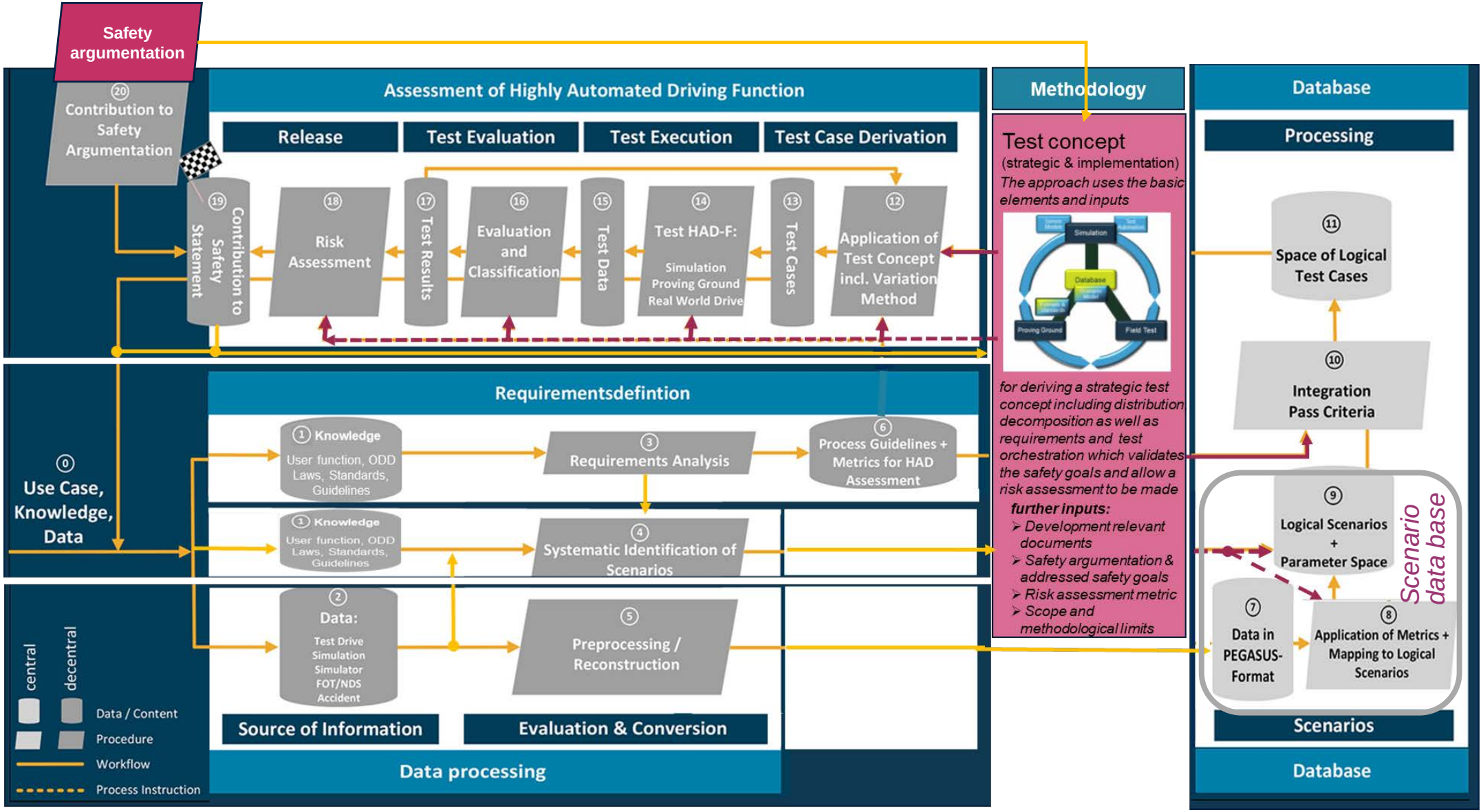
VERIFICATION VALIDATION METHODS

Core elements of PEGASUS Approach





The missing element “test concept” and “safety argumentation”



Different scopes of PEGASUS and VVM

In the scope of VVM:

- **Providing evidence for a safety argumentation of an ADS - on the level of the system and its functional chains - within the ODD.**

  Evidence in

  - behaving safely on behalf of both the driver and all other road users interacting with an ADS equipped vehicle
  - avoidance or mitigation of accidents compared to human driver
  - Compliance with traffic and behavioral law as well as regulation respectively ethical standards and related public expectations

  All components and their decomposition with respect to design and V&V are considered, which have a special influence on the driving automation by integration into a functional chain.

operational area in the scope of VVM:

- Validation phase
- Concept phase, design phase, verification phase

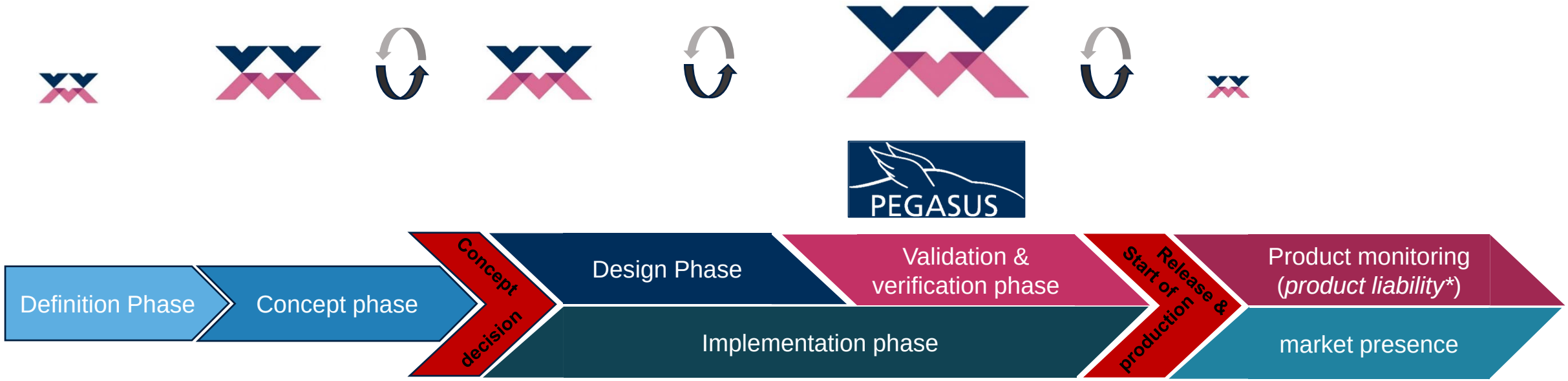
In the scope of PEGASUS:

- **Statistical demonstration of system safety and positive risk balance without driver interaction within the ODD**
- Validation of various system & vehicle configuration / variants / conditions
- Sensor functionality as input for system performance

operational area in the scope of PEGASUS:

- Validation phase, (limited as a measure in design phase)

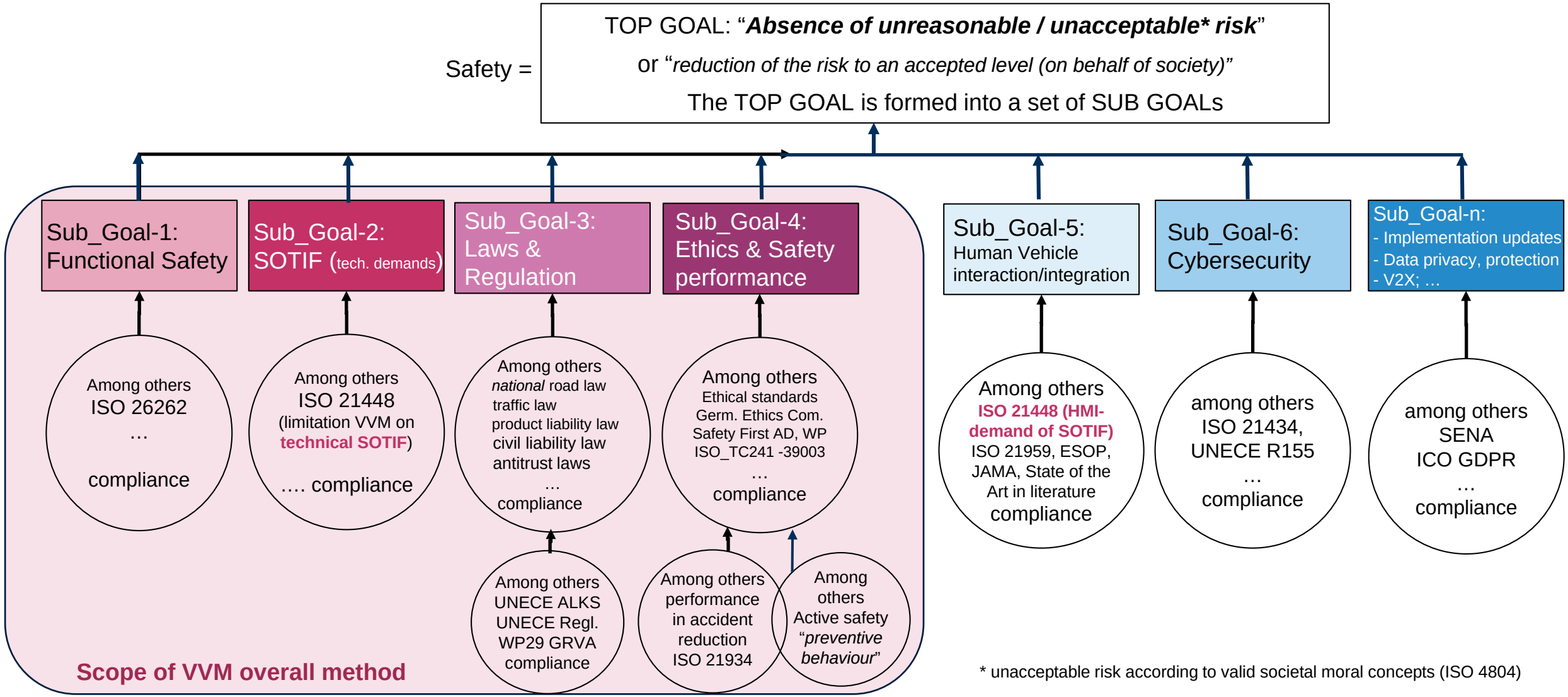
Product Development Phase and presence in market coverage / impact “PEGASUS-method” vs “VVM method” in phases



** a manufacturer is liable for damage caused by the use of his product and the underlying cause was present when the product was placed on the market.*

Safeguarding automated driving systems (ADS): ensuring safe operation

Top and Sub_goals concerning Safety



* unacceptable risk according to valid societal moral concepts (ISO 4804)

Sub level goals for ADS in ODD – (exemplary) linguistic formulations

linguistic will be transferred to technical (performance) measures

Sub_Goal-1: Functional Safety

- [1.1]: **All hazards** that may arise by the functionality **in the E/E system** of the ADS to be developed within its ODD **are identified and assigned to the required ASIL**.
  - For hazards that are identified as potential sources of harm, the possible risk that might result under specific situational circumstances is evaluated.
- …

Sub_Goal-2: SOTIF

- [2.1]: The **ADS is sufficient robust** with respect to **sensor input variations**, algorithms used for **sensor data fusion** or diverse **environmental conditions**.
  - The functional und system specifications provide an adequate understanding of the ADS and its functionalities.
- [2.2]: The ADS has the capability to properly comprehend the scenario and respond safely.
  - …

Sub_Goal-3: Laws & Regulation

- [3.1]: The **ADS complies** with the applicable **traffic regulations** (Road Traffic Code) resp. behavioral laws (Code of Conduct) while driving in its ODD and only temporarily deviates from specific rules/laws in defined, approved exceptions.
- [3.2]: The ADS fulfills the standards, laws or approval regulations valid on the day of ADS approval.
  - …

Sub_Goal-4: Ethics & Safety performance

- [4.1]: The **ADS behaves ethically appropriate within its ODD**.
  - [4.1.1]: The vehicle equipped with an automated driving system (ADS) is designed to perform at least as well as a *conscientious* human driver (to be defined in detail) when executing dynamic driving maneuvers to avoid accidents.
  - [4.1.2]: In the operation of the ADS, the protection of human lives is of paramount importance.
  - [4.1.3]: The **ADS is explicable** and **predictable** for the people impacted by its use.
- …

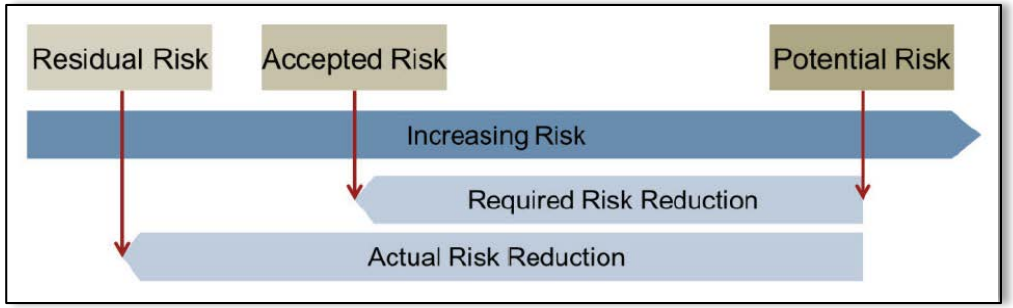
Functional Safety

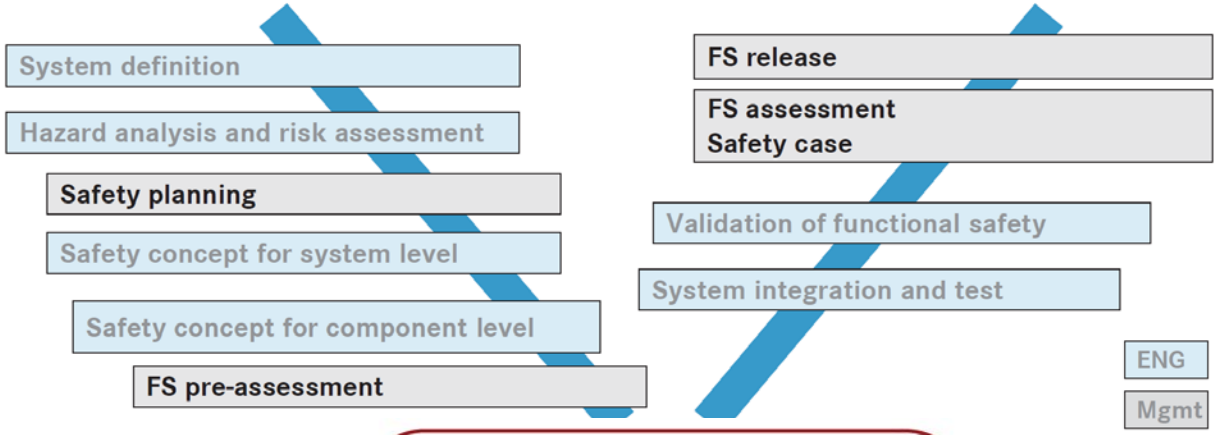
Sub-_Goal-1:
Functional Safety

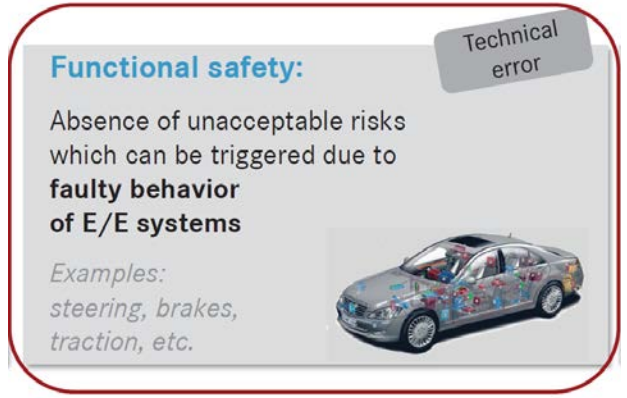
- [1.1]: All hazards that may arise by the functionality in the E/E system of the ADS to be developed within its ODD are identified and assigned to the required ASIL.
  - For hazards that are identified as potential sources of harm, the possible risk that might result under specific situational circumstances is evaluated.
- …

- The objective of FuSa is:

"Reaching of a comparable safety level for all components regardless of the potential risk."







- **Status:** FuSa is **well integrated** in the development process and implemented with a quality management
- **Challenge**: Implementation of **needed adaption for ADS.**
- **Argument: Absence of unacceptable risks of ADS due to faulty behavior trigger in E/E components of ADS. (risks due to technical errors are** below an **acceptable** level)

SOTIF -Safety of the intended Functionality

Sub_Goal-2: SOTIF

- [2.1]: The ADS is sufficient robust with respect to sensor input variations, algorithms used for sensor data fusion or diverse environmental conditions.
  - The functional und system specifications provide an adequate understanding of the ADS and its functionalities.
- [2.2]: The ADS has the capability to properly comprehend the scenario and respond safely.
  - …

V&V activities of the intended functionalities with regard to the risk of safety violations without system faults addresses:

- The ability of sensors and the sensor processing algorithms to **model the encountered driving environment**;
- The ability of the decision algorithm to **recognize** both known and unknown **situations** and
  - make the appropriate decision according to the environment model and the system architecture;
- The **robustness** of the system or function;

Status: SOTIF is **well integrated** in development process for Level 2 and lower Level ADAS, need to be adapted for Level 3 and higher ADS

Challenge: Addressing the SOTIF target, measures had to been implemented during the complete development process:

- Measures in **design phase**, in **verification phase**, in **validation phase** and in operation phase
- Detailed Functional and System specification of ADS incl. ODD serve as the starting point of SOTIF process.
- Systematic identification & evaluation of SOTIF risks including possible hazardous events.

Argument: Absence of unacceptable risks due to insufficient performance or robustness and foreseeable misuse of E/E functions

(**risks due to functional inadequacies** of ADS **are** below an **acceptable** level)

Law and regulation requirements
new challenge: Technical compliance and compliant product design

Sub_Goal-3:
laws & regulation

- [3.1]: The ADS complies with the applicable traffic regulations (Road Traffic Code) resp. behavioral laws (Code of Conduct) while driving in its ODD and only temporarily deviates from specific rules/laws in defined, approved exceptions.
- [3.2]: The ADS fulfills the standards, laws or approval regulations valid on the day of ADS approval.
- …

State-of-of-the-Art: the integration of laws and regulations governing the conditions under which a vehicle equipped with an ADS receives its operating approval.

Challenge: implementation of **technical compliance** and **compliant ADS behavior as a result of product design**

- Road traffic rules and legislation require translation into technical specifications.
- These specs must be drivable, free of contradictions and result in a robust and compliant ADS behavior in the ODD.
- Lifecycle aspect: Define measure that monitor future modifications in traffic law/regulation, implements necessary updates.

Target for methods in V&V:

- Design a target behavior for the Basic Use Cases in the ODD
  - make ensure that is robust in the Use Case / ODD and does not contain dead locks
- Verify the implementation and assess the acceptance of deviations
- Include a test to validate target behavior

Argument: ADS is developed technical compliant, risks of ADS due to implementation of road traffic **laws are** below an **acceptable** level of risk

Balancing requirements from different sub-goals to a target behavior

Defining TARGET BEHAVIOUR is more than complying with laws.

System capabilities

- ✓ The ADS detects crosswalks.
- ✓ The ADS detects vulnerable road user (VRU).
- ✓ The ADS treats cyclists like pedestrians, although it is not allowed for cyclists, in principle, to drive across crosswalks.
- ✓ The ADS detects the motion, at least the moving direction, of vulnerable road user.
- ✓ The ADS gives way pedestrians who want to cross the road.
- ✓ …

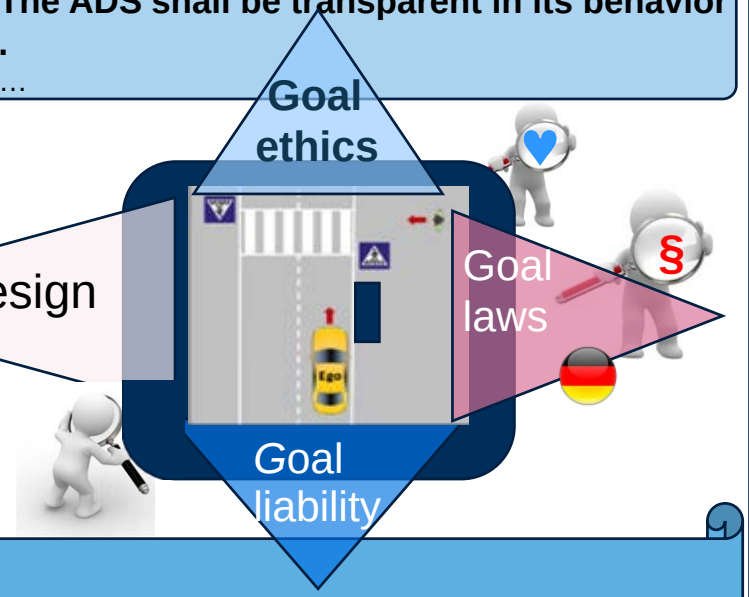
System requirements

- ✓ The ADS shall adjust a #moderate velocity.
- ✓ The ADS shall pass parking vehicles with a minimum of #normal_passing_distance.
- ✓ In case of detecting that pedestrian in the safe area of the crosswalk don‘t want to cross the road, the ADS shall pass the crosswalk with #walking_speed.
- ✓ …

System_Parameter_Definitions

- ✓ #walking_speed = 2m/s
- ✓ #normal_passing_distance = 1.0m
- ✓ #moderate_velocity =[6m/s … 8m/s]
- ✓ …

- ✓ **The ADS shall not discriminate VRU by age, size, gender, color, clothes, handicap, …**
- ✓ **The ADS shall be beneficial to people impacted by its use.**
- ✓ **The ADS shall be transparent in its behavior**
- ✓ **.**
- ✓ …



- ✓ **The ADS shall not operate so slowly that it obstruct the flow of traffic without good reason**
- ✓ …

- ✓ The vehicle must yield to any pedestrian crossing at a marked intersection.
- ✓ Vehicles only have to slow down on pedestrian crossings if pedestrians or wheelchair users clearly want to use the crossing. Otherwise, vehicle drivers may also accelerate in front of the pedestrian crossing to cross it quickly.
- ✓ …
- ✓ According to section 26 paragraph 5 StVO, a vehicle has to approach a pedestrian crossing with moderate speed only if it becomes apparent that a pedestrian wants to cross the street..
- ✓ …

…

Analyze Robustness of target behavior in ODD in the definition phase

System capabilities

- ✓ The ADS detects crosswalks.
- ✓ The ADS detects vulnerable road user (VRU).
- ✓ The ADS treats cyclists like pedestrians, although **it is not allowed for cyclists, in principle, to drive across crosswalks.**
- ✓ The ADS detects the motion, at least the moving direction, of vulnerable road user.
- ✓ The ADS gives way pedestrians who want to cross the road.
- ✓ **… in given context “crosswalk”**

System requierements

- ✓ The ADS shall adjust a #moderate velocity.
- ✓ The ADS shall pass parking vehicles with a minimum of #normal_passing_distance.
- ✓ In case of detecting that pedestrian in the safe area of the crosswalk don‘t want to cross the road, the ADS shall pass the crosswalk with #walking_speed.
- ✓ …

System_Parameter_Definitions

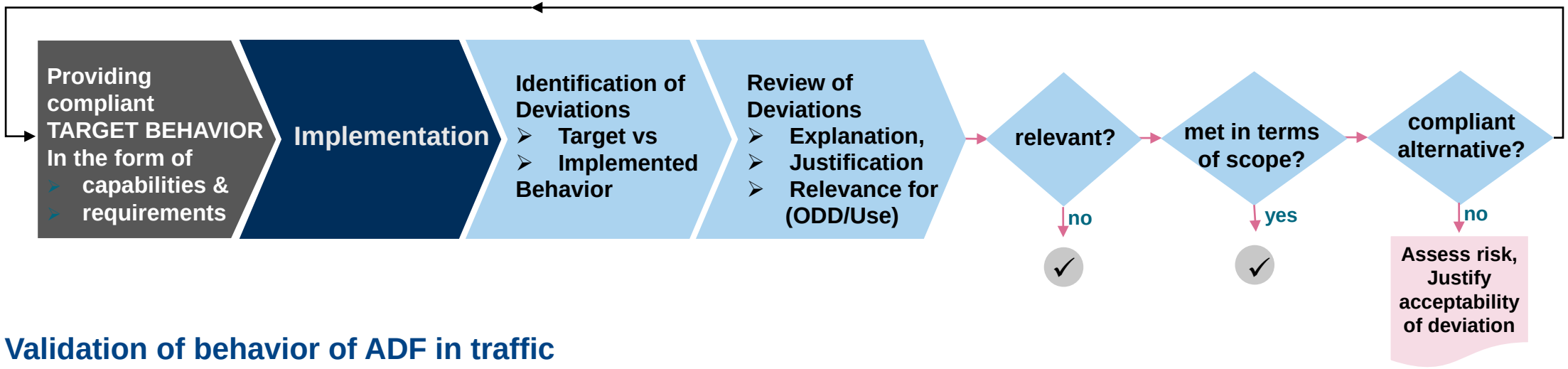
- ✓ #walking_speed = 2m/s
- ✓ #normal_passing_distance = 1.0m
- ✓ #moderate_velocity =[6m/s … 8m/s]
- ✓ …… in given context “crosswalk”

Structure for holistic V&V for TARGET BAHAVIOR of an ADS in traffic

1 Design of behavior of ADF in traffic

Design compliant TAGRET BEHAVIOR, that met Safety Sub Goals in ODD.
Analyze robustness in ODD and the absence of deadlocks.

2 Verification of behavior of ADF in traffic



3 Validation of behavior of ADF in traffic

Validation test (***among others might be included*** – in the V&V Concept):

- Driving [*school*] test preformed in an unknown but ODD compliant environment with given pass criteria which were able to measure the degree of compliance with the related [Safety] Sub Goals (e.g. traffic laws, ethics, …).

Ethics and safety performance

VERIFICATION VALIDATION METHODS

Sub_Goal-4: ethics & safety performance

- [4.1]: The ADS behaves ethically appropriate within its ODD.
  - [4.1.1]: The vehicle equipped with an automated driving system (ADS) is designed to perform at least as well as a *conscientious* human driver (to be defined in detail) when executing dynamic driving maneuvers to avoid accidents.
  - [4.1.2]: In the operation of the ADS, the protection of human lives is of paramount importance.
  - [4.1.3]: The ADS is explicable and predictable for the people impacted by its use.
- …

ISO 39003 defines design principles with purpose of improving the quality of how ADS and humans act individually and interact in traffic. They are: **Non-maleficence, Beneficence, Autonomy, Justice, Explicability**. Ethic commissions specify them with details.

Challenge for the method that integrates this into a V&V process is: design of **target behavior** and assessment of **ADS safety performance**

- **Interpretation of traffic rules** while defining a target behavior.
- Requirements **for considering relevant objects** in the basis use cases in terms of their protection, their **hypothetical behavior and relevant limits in the analyzed basic use case** , in the design of the target behavior in traffic and without it.
- Evaluation of the residual risk left by the defined target behavior in terms of its acceptability,

The benchmark for the assessment of the system performance must be defined in comparison to the performance of a human driver

- Using the **POSITIVE RISK BALANCE** as a measure of ***beneficial***
- Using the concept like the **conscientious human driver** for a performance reference indicator.

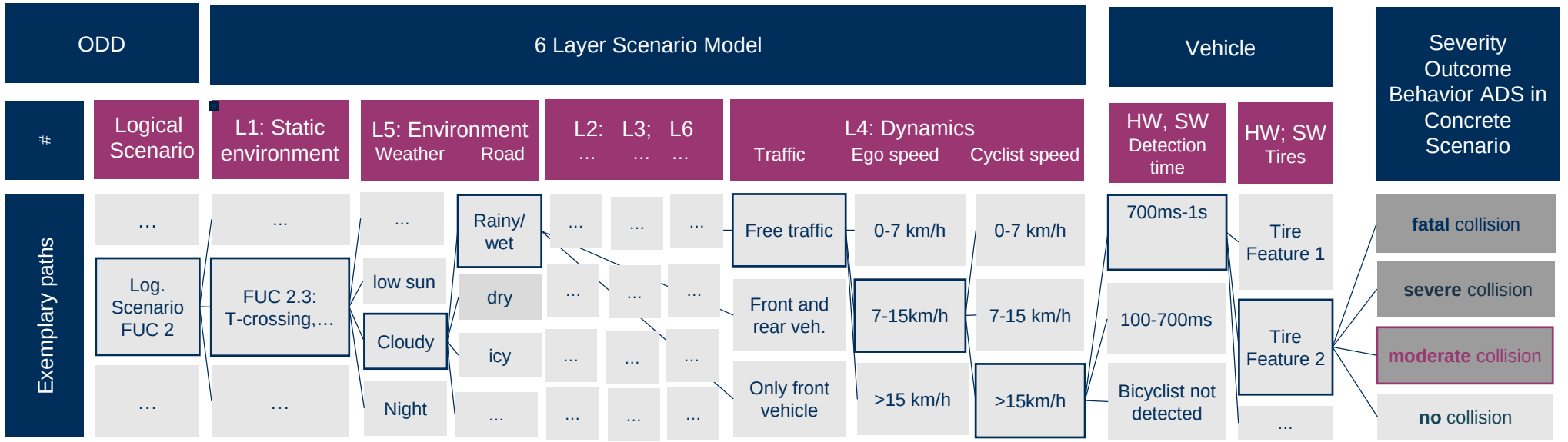
Argument: Design (and implemented) of target behavior is compliant with ethical expectation.

The risk of ADS due to its safety performance **is** below an **acceptable** level (of the society).

Measuring safety: Performance target for traffic system related function design: Positive Risk Balance

By request of Sub_Goal 4 “ethics” the ADS should be beneficial:

(*) Frequency of the occurrence of harm (collision of severity S_n) < threshold value* (collision with S_n in reference years)



**Thresholds for GER, 2014*
Inner city, caused by pc
*S3: 379,048*10^{-6} km*
*S2: 8,902*10^{-6} km*
*S1: 6,740*10^{-6} km*

Highway, caused by pc
*S3: 986,628*10^{-6} km*
*S2: 58,539*10^{-6} km*
*S1: 14,804*10^{-6} km*

Highway, pc involved
*S3: 698,354*10^{-6} km*
*S2: 49,971*10^{-6} km*
*S1: 12,652*10^{-6} km*

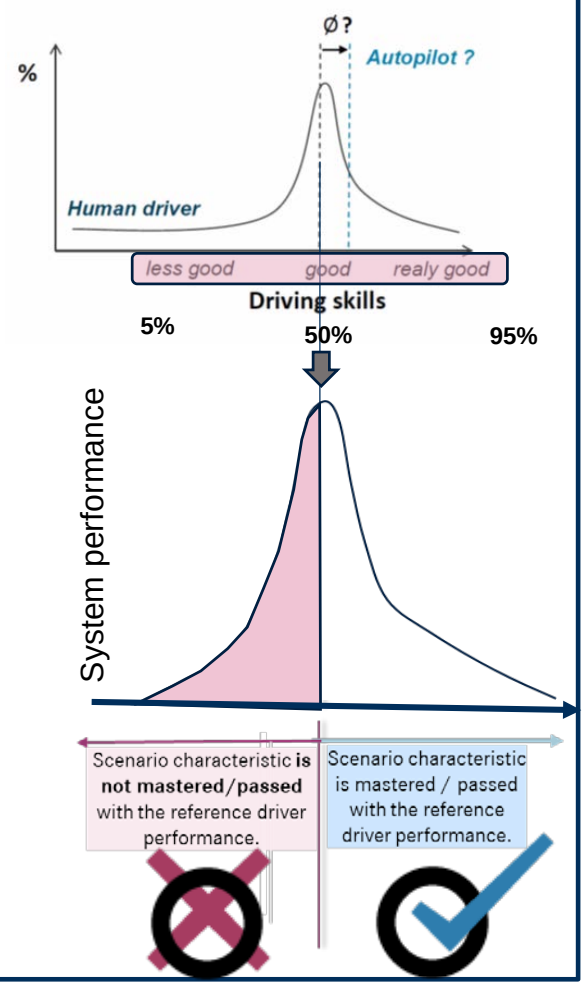
Positive Risk Balance (PRB) for logical FUC / ODD of ADS:

- Measure: The collision probability of an ADS is the sum of all possible paths leading to a collision.
- Algorithm: By definition of PRB the performance of ADS is adjusted in such a way that a positive risk balance is satisfied.

Measuring safety: Performance target for safety related function design: Human reference performance

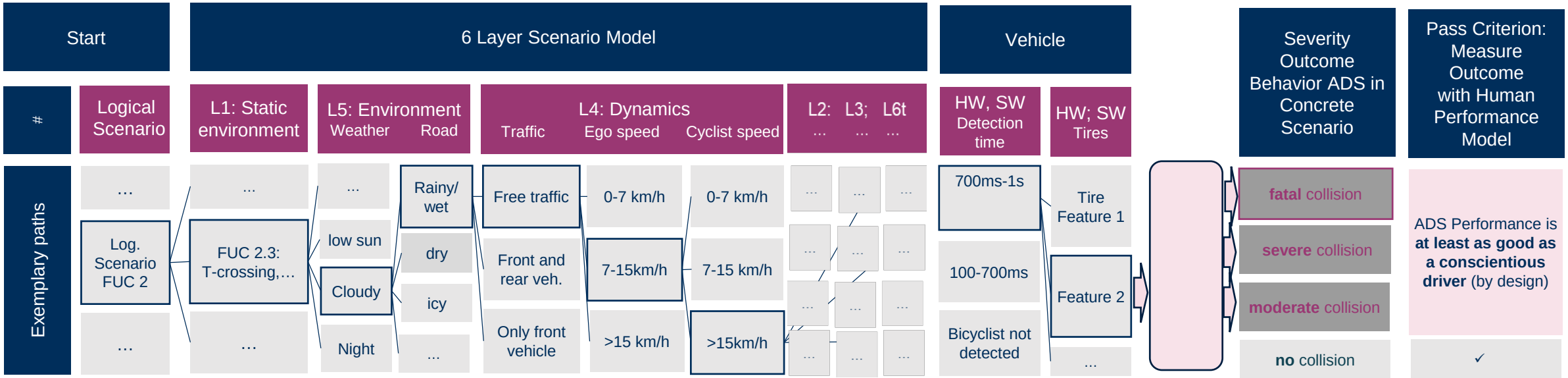
Performance Target for ADS

Controllability of the driving situation with regard to safety	Performance target for system design	Cumulated Performance target
driver equivalent can control the situation in general (~100 %).	The system must be able to handle the relevant scenario generally.	At least reaching the safety level of current road traffic (in the reference years) of all conscientious driver (performance reference driver equivalent).
driver equivalent can control the situation with restrictions.	System must control the scenario statistically at least comparable to driver equivalent.	
driver equivalent basically cannot control the situation (~ 0 %).	System does not have to be designed for the scenario but a mitigation measure has to be implemented.	



- The performance reference is defined by **the conscientious driver who** is willing to **comply with all traffic regulations**, is **fit to drive**, **attentive** and do not act grossly negligent.
- **The performance reference of human controllability** is based on the currently available information (if necessary expert judgments).
- The comparison with the performance reference could be applied in the context of a given driving scenario to **all relevant variants of the driving situation**.

Adding *driver reference performance* in Positive Risk Balance



Advantage of this approach: minimum performance of ADS

1. BY definition of Positive Risk Balance
   - residual **probability of a collision** of severity (S1; S2; S3) **for ADS** is less than
     - **probability of a collision** of severity (S1; S2; S3) **for human driver** in reference years in ODD / logical FUC
2. In Functional Logical Use Case the performance of ADS is at least as good as a conscientious human reference driver.

Major challenges: verification & validation *general method* for ADS

VERIFICATION VALIDATION METHODS

Sub-_Goal-1: Functional Safety

Challenge: Adaptation established process

Sub_Goal-3: laws & regulation

Major challenge: Target behavior & tech. compliance

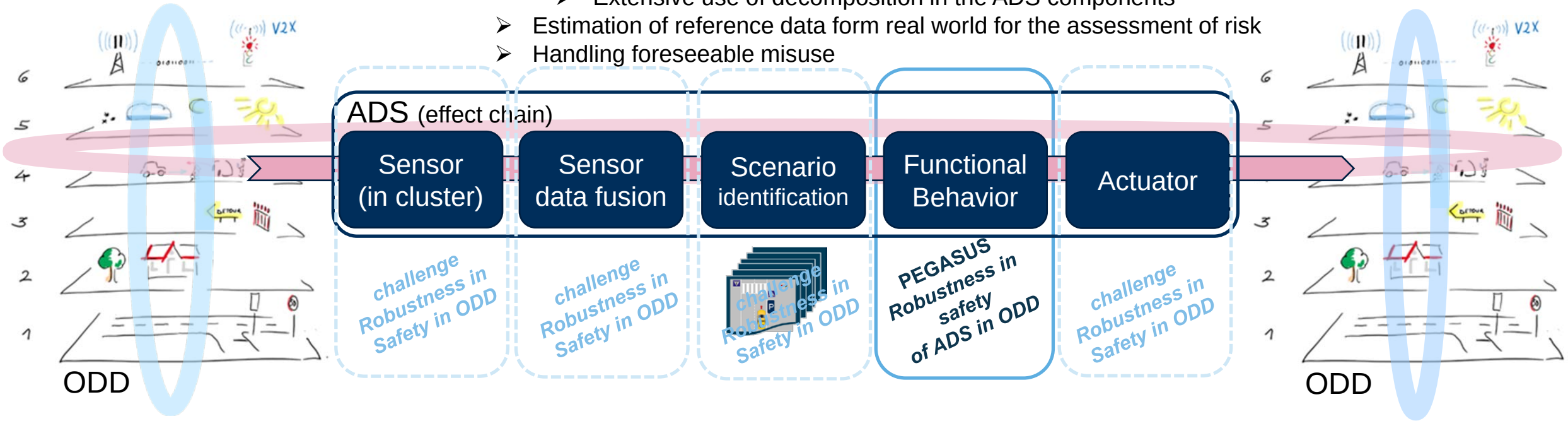
Sub_Goal-4: ethics & safety performance

Major challenge: Performance measure & tech. compliance

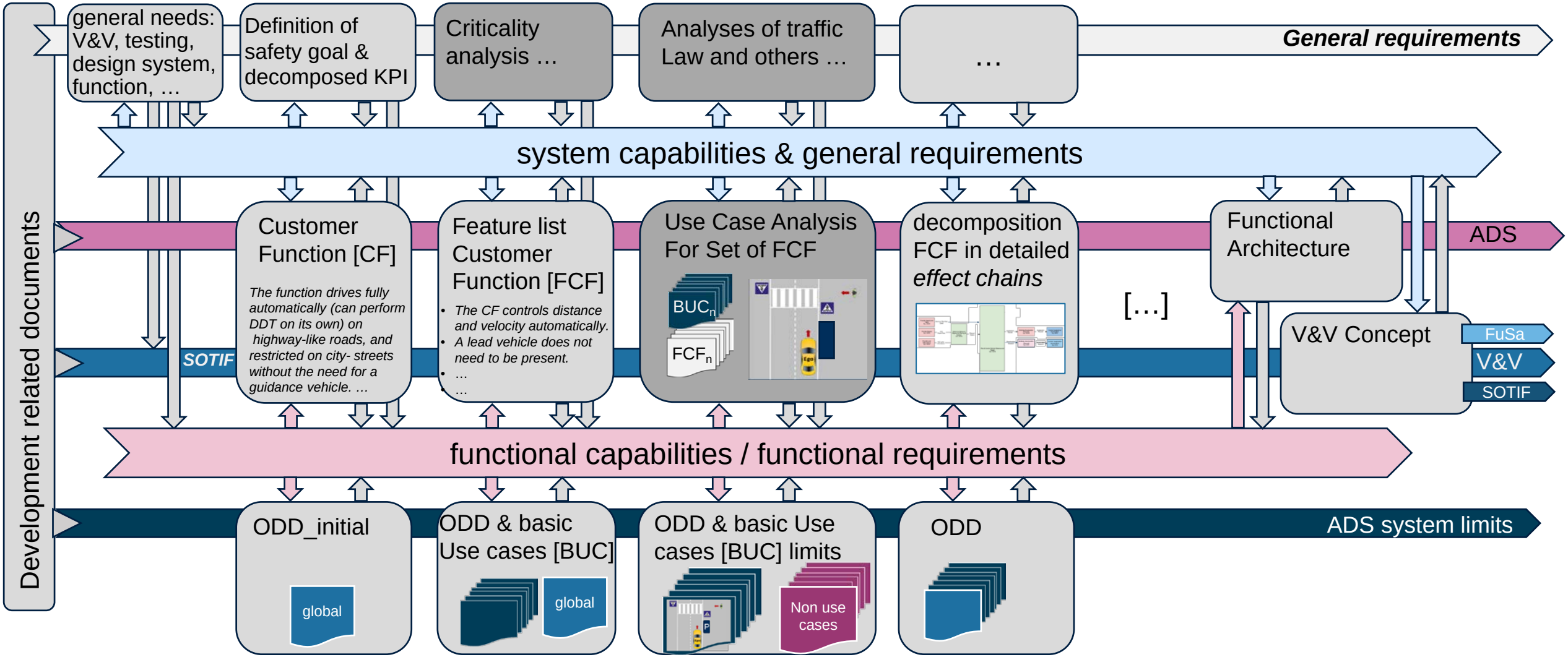
Sub_Goal-2: SOTIF

Major challenge:

- Robustness of the intended ADS functionality
  - distributing the task among the different test instances by an intelligent decomposition, defining the cross checking of the achieved efficiencies on one instance
  - Extensive use of decomposition in the ADS components
- Estimation of reference data form real world for the assessment of risk
- Handling foreseeable misuse



A sketch of the overall method on the capability layer



A sketch of the overall method on the capability layer

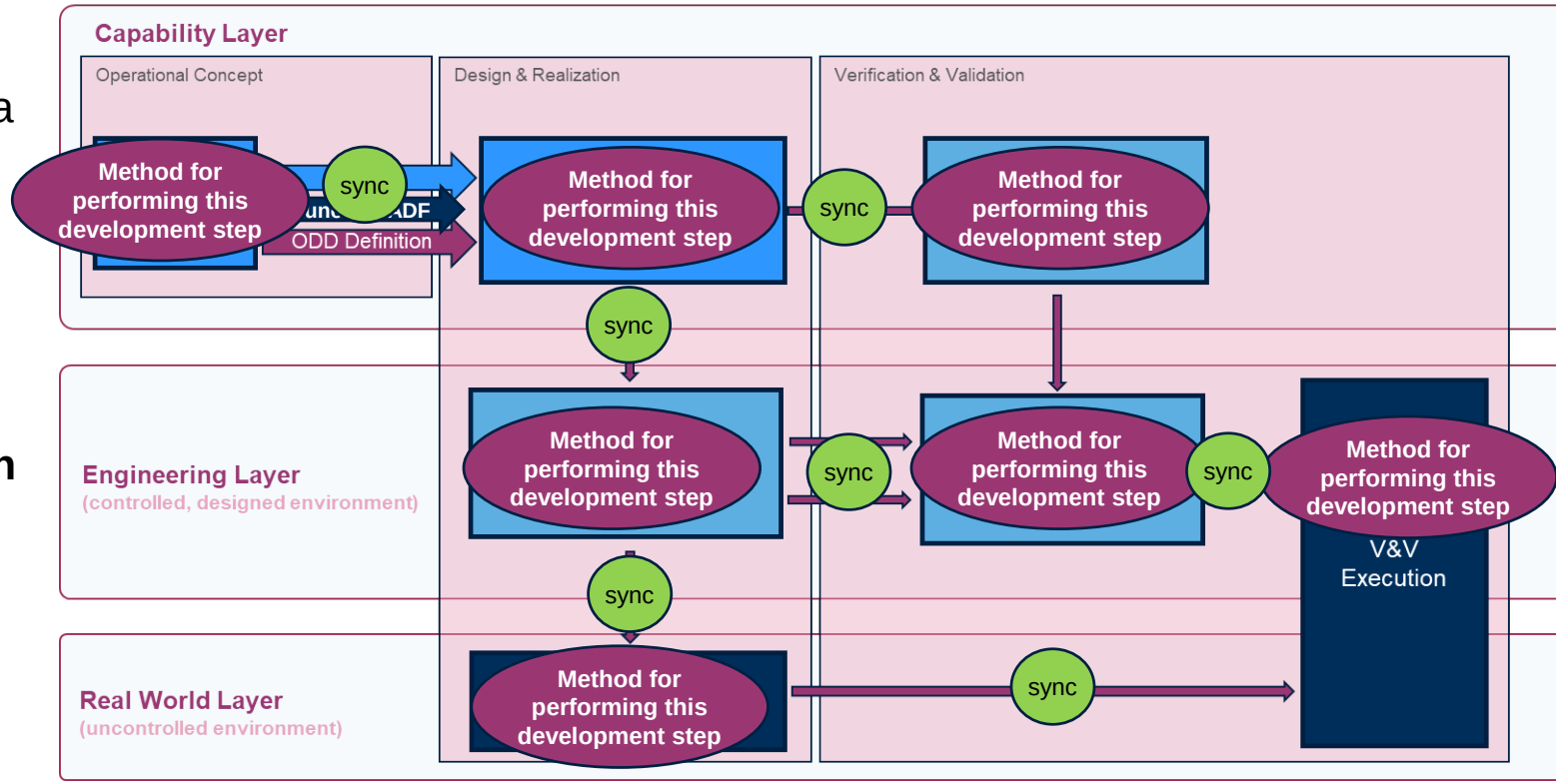
Interaction between *assurance framework* and method

The **interacting** of **methods** and **assurance framework**:

The **assurance framework** is a way for **systematically deriving and structuring** the right **evidences** which are necessary to argue the identified concerns.

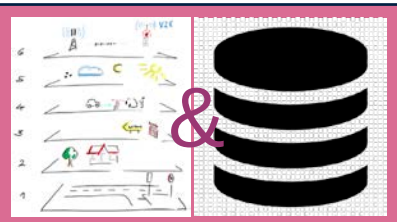
The **methodological approach provides the methods and tools for** a reliably **generating the evidence** for this process that are realistically producible by methods/processes.

The evidences are **the sync-points** of the interaction.

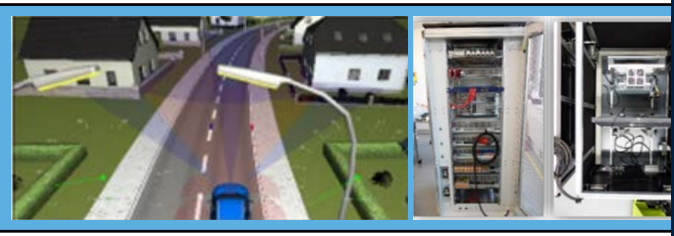


Innovations in the field of test instances

Scenario data base
- Realistic, representative real world data
- An most important tool for robustness analysis



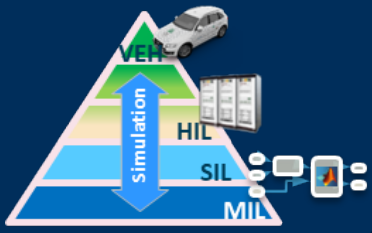
Simulation
- Models, environment, tooling
- Standard-Interfaces



Proving ground testing
- Innovative test technologies

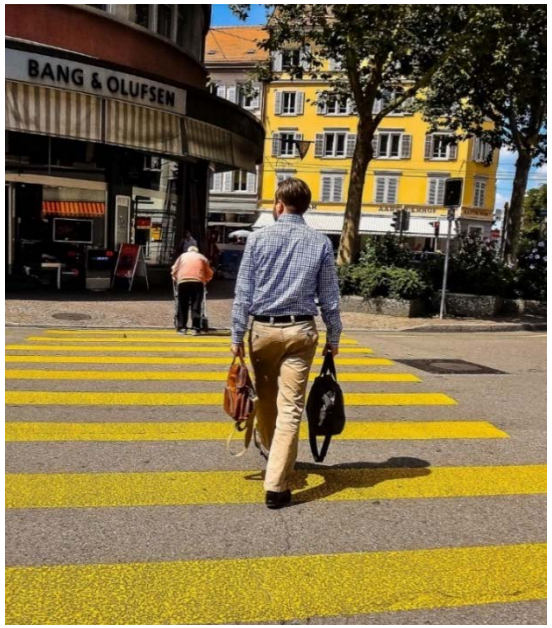
Used in VVM

- model in the loop
- SW in the loop
- HW in the loop
- Vehicle in the loop

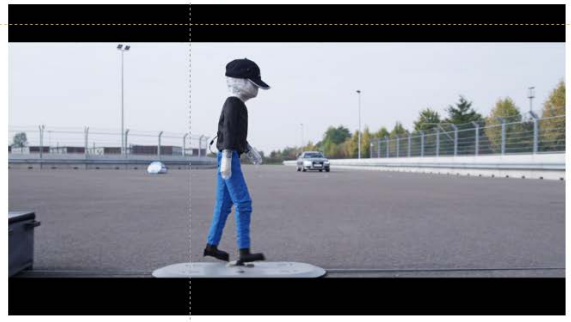


Innovation to increase the degree of realism of test instances: Example proving ground test equipment “road crossing by VRU”

- real-world



- over-simplified



ref: https://www.youtube.com/watch?v=pLOoOIVKAHs

challenge

goal

- over-realistic

ref.: "Fahrerassistenzsysteme - Notbremssystem mit Personenerkennung“, ADAC, Tech. Rep. [Online]. Available: 2016 https://www.adac.de/infotestrat/tests/assistenzsysteme/fussgaengererkennung/default.aspx

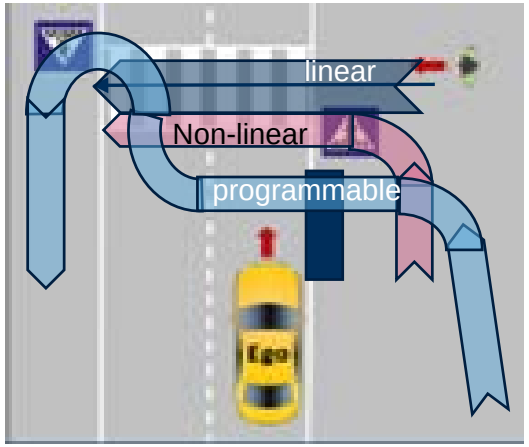
COORDINATED
REAL WORLD
SAFETY TESTS

- realistic
- reasonable
- reproducible
- research-based

REAL WORLD PEDESTRIAN SAFETY

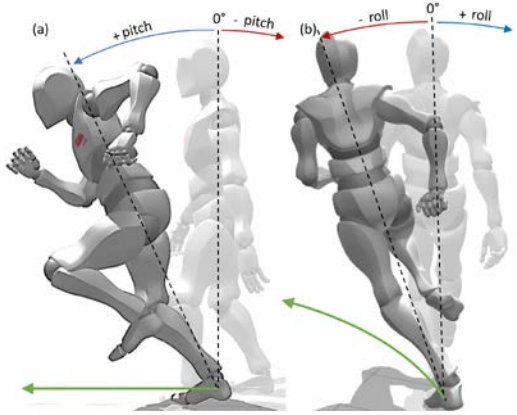
Most relevant pedestrian features

1 Global features



- Trajectory
  - Linear,
  - non-linear,
  - programmable
- Velocity on trajectory
  - Linear,
  - non-linear,
  - programmable
- Head rotation
- Radar reflectivity

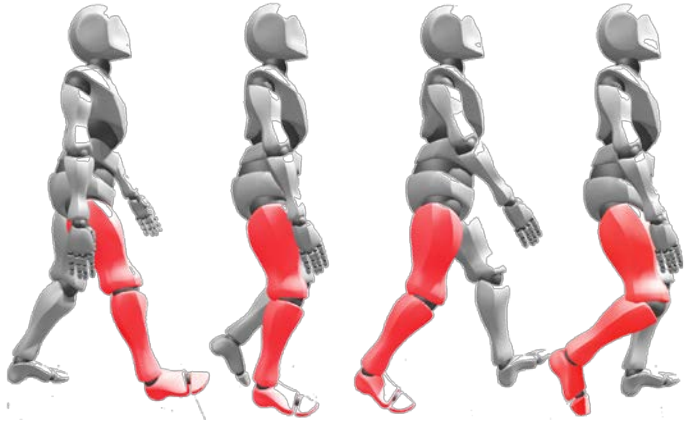
2 Macroscopic features [6 DoF]



	Walking	Jogging	Running
Velocity [m/s]			
Acceleration [m/s²]			
Decelerion [m/s²]			
Pitch Phase 1 [°]			
Pitch Phase 2 [°]			
Roll [°] R = 8m/4m/ 2m/1m			

Current measurements are performed and analyzed

3 Microscopic features

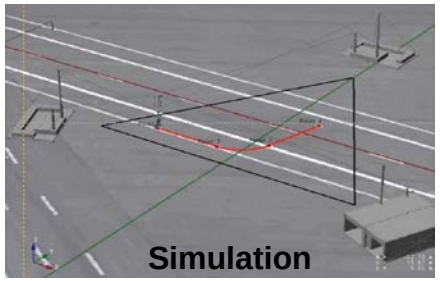


	Walking	Jogging	Running
Step frequency [1/min]			
Hip joint angles range [°]			
Knee joint angles range [°]			

Current measurements are performed and analyzed

COORDINATED REAL WORLD SAFETY TESTS
closer to real world - multidimensional Target Mover & dummy

- Replication of macroscopic pedestrian features [6 degrees of freedom]: initial solution (more in the final event)



Seamless through Simulation and proving ground

- realistic
- reasonable
- reproducible

test tool

VERIFICATION
VALIDATION
METHODS

Thank you!

Dr. Helmut Schittenhelm

Helmut.Schittenhelm@Mercedes-benz.com

PROJECT of the PEGASUS FAMILY

A project developed by the
VDA Leitinitiative
autonomous and connected driving

Supported by:

Federal Ministry
for Economic Affairs
and Climate Action

on the basis of a decision
by the German Bundestag