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

A PEGASUS Family Safety Argumentation Approach

23.09.2020

Roland Galbas, coordinator of VV-Methods project

(VV-Methods Co-Coordinated by Mark Schiementz)

Robert Bosch GmbH

VV-METHODS – Project Setup

VERIFICATION VALIDATION METHODS

- **Funded by** Ministry of Economics and Technology (BMWi)
- **Start, Runtime** 07/2019, 4 years
- **Budget total** 47M€
- **Partners**

OEM	BMW, Mercedes-Benz, Volkswagen, Audi, Opel, Ford
Tier-1	Hella, Bosch, Valeo, Continental, ZF
Tech	AVL, PROSTEP integrate the future, dSPACE
Eval	TÜV SÜD, bast
Science	ika RWTH Aachen University, Fraunhofer, Technische Universität Darmstadt, Technische Universität Braunschweig, OFFIS Institut für Informatik, FZI, DLR

VV-METHODS – Main Goals

VERIFICATION
VALIDATION
METHODS

Systematic control of test space

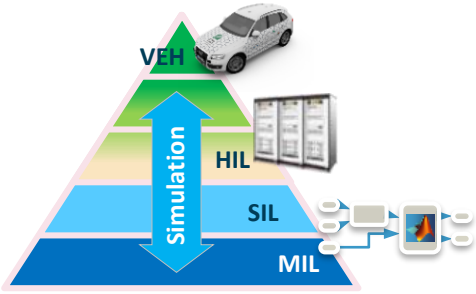
- Methods to optimize (and reduce) the test parameter space to a manageable minimum

Industrial defined interfaces for systems and components

- Definition of incremental tests of subsystems and overall systems

Significant shift from real-world testing to simulation

- Methods for seamless testing across all test instances



VV-METHODS – Structure & Goals

VERIFICATION VALIDATION METHODS

∞ → n

Goal I – Systematic control of test cases

- Understand relevant phenomena & traffic behaviors
- Involve traffic law perspective
- Approach a **nominal behavior**
- Identify **enveloping tests**

Goal II – Industrial interfaces

- Common methods for systematic breakdown of technical contracts, requirements & tests
- Agreed rules for **component exchange** between OEM and supplier
- Efficient **variant-release**, preservation of test-results of unmodified components
- Integration of **systems of different manufacturers**.

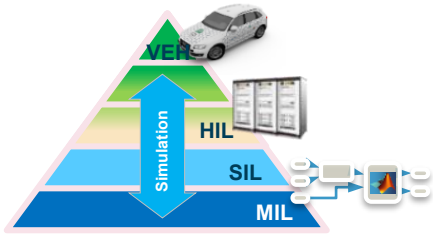
Criticality analysis

Safety assessment & safety concepts

Rules for system and test requirements

Test infrastructure

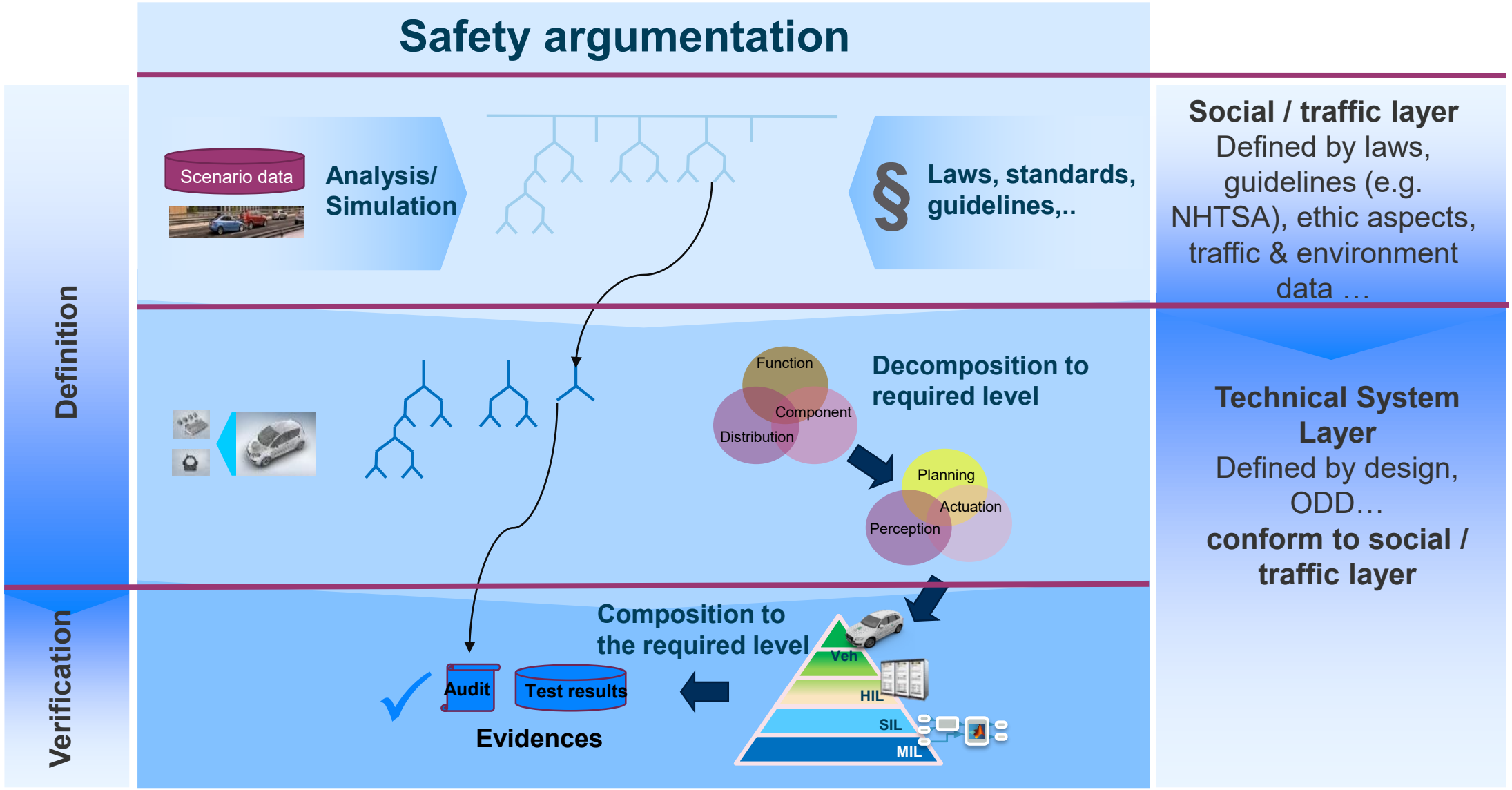
- Simulation (Level 4 to 5)
- HW in the loop
- Proving ground
- Field test



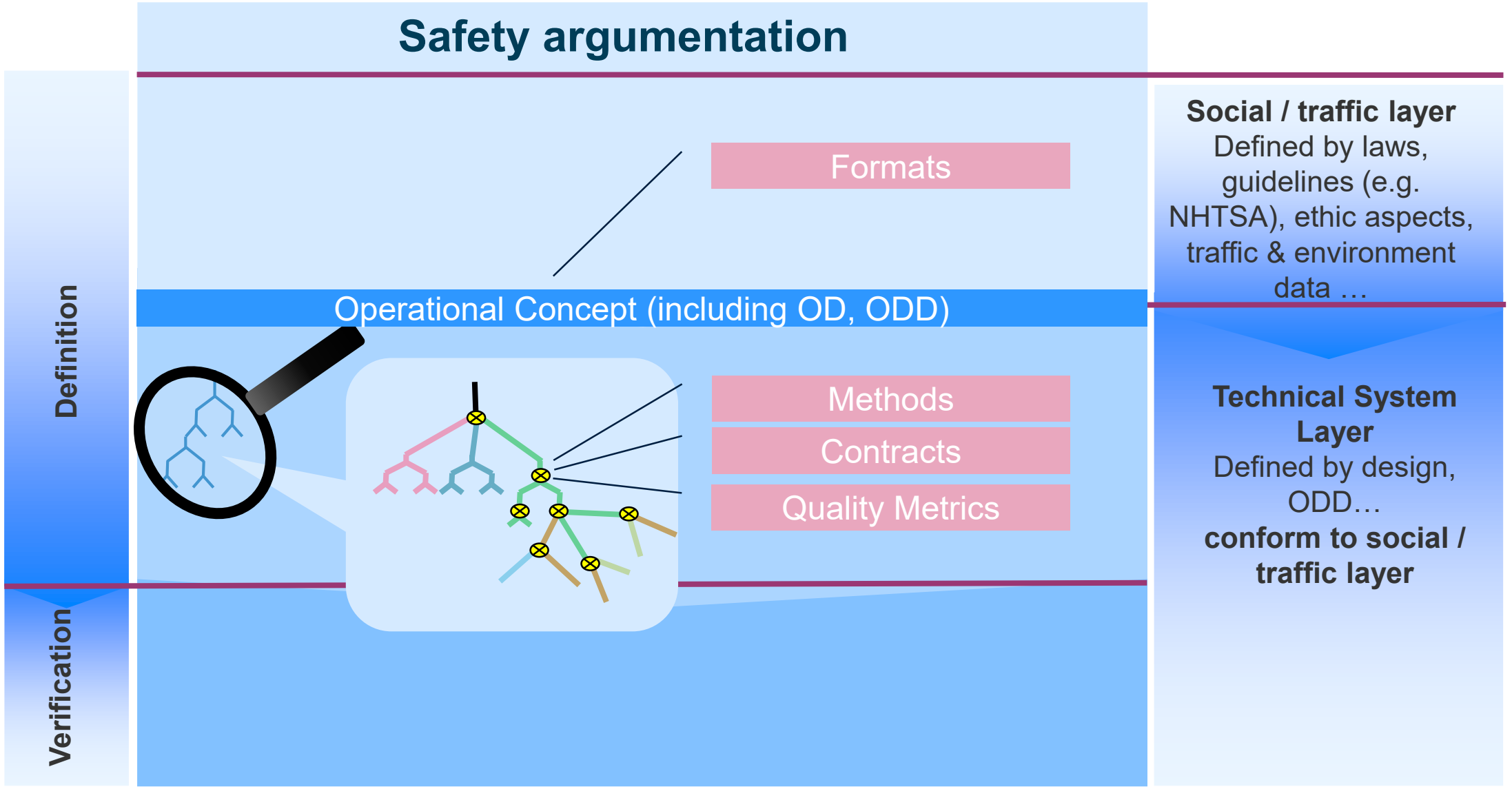
Goal III – shift to simulation

- Seamless use of virtual and real artefacts
- Efficient integration of simulation into the test-infrastructure with focus on
- **Seamless testing** across functional test infrastructures
- Efficient **distribution of test efforts** (Sim-Real).

VV-METHODS – Safety Argumentation



VV-METHODS – Safety Argumentation



VV-METHODS – Safety Argumentation

Safety argumentation

definition

§

Laws, standards, guidelines,..

NHTSA priority safety design elements

- …
- Fallback (minimal risk condition)

ETHICS COMMISSION automated and networked driving – Germany

- …
- **Rule 19** In emergency situations, the vehicle must be able to reach a "safe state" autonomously, i.e. without human assistance….

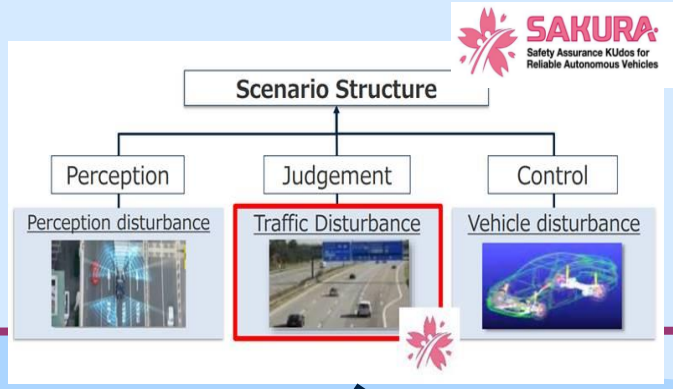
Social / traffic layer
Defined by laws, guidelines (e.g. NHTSA), ethic aspects, traffic & environment data …

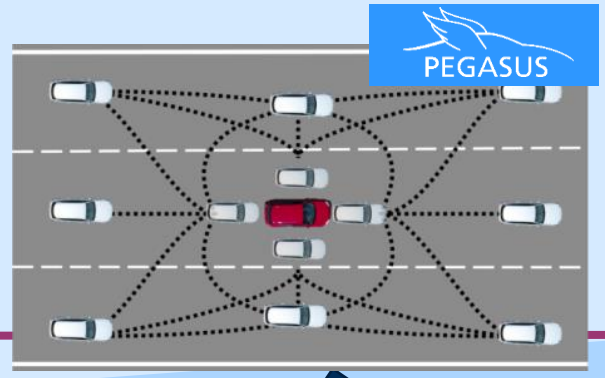
- Consolidation of different claims have to be done on the according layer.

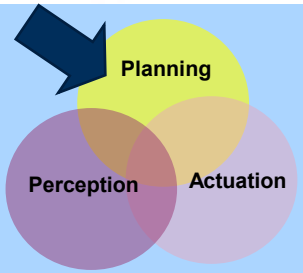
VV-METHODS – Safety Argumentation

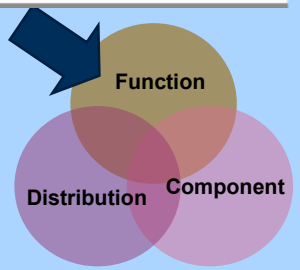
Safety argumentation

Definition







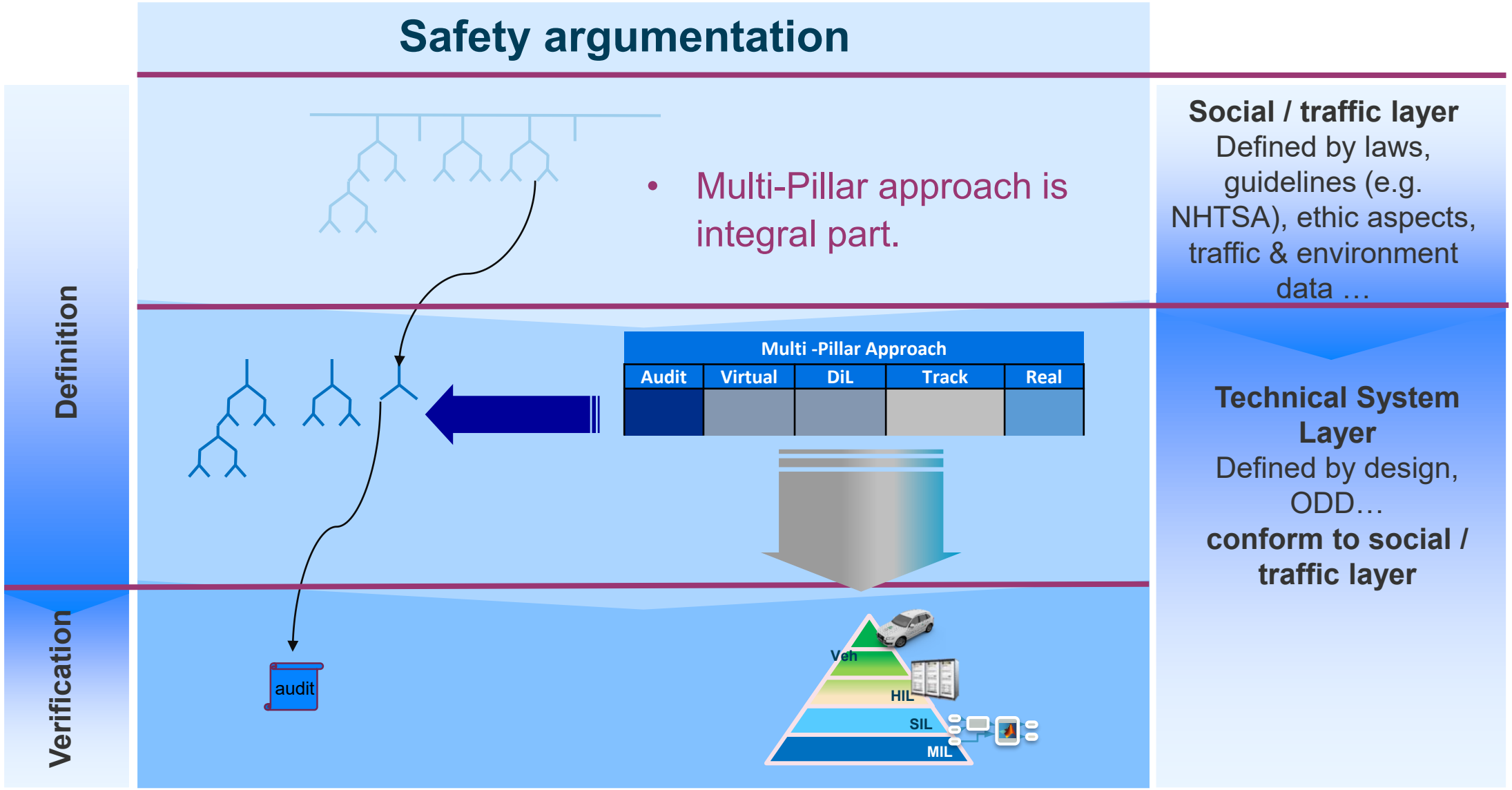


- Scenario based approach remain central element.
- Decomposition is core element of approach.

Social / traffic layer
Defined by laws, guidelines (e.g. NHTSA), ethic aspects, traffic & environment data …

Technical system layer
defined by design, ODD…
conform to social / traffic layer

VV-METHODS – Safety Argumentation



VV-METHODS – Safety Argumentation

VERIFICATION
VALIDATION
METHODS

Why safety argumentation?

It is a systematic approach to the requirements flow. It enables and supports the project goals

- structuring the inputs of open world traffic behaviour and law perspective.
- enable the systematic breakdown of contracts.
- define quality-requirements to simulation.

What is needed?

- **Contracts** based on **assumptions and guaranties** define the safety argumentation – thus building up **industrial interfaces**.
- **Methods** for definition and brake-down of contracts.
- **Quality criteria and metrics** to define social and technical contracts
  e.g. the **Positive Risk Balance** could be considered a quality criteria on a high level of the social layer.
- **Formats** e.g. the functional architecture as a structuring method for knowledge.

VV-METHODS – Summary

- **VV-Methods and SETLevel4to5 are successors of PEGASUS** and build on its results.
  Main goal: Enabling and industrialization of AD system.
- **Safety Argumentation is main element and enabler**
  - Systematical flow of requirements – can be decomposed into 3 main layers.
  - Quality criteria and metrics are building the basis to define contracts within the safety argumentation.
- **Criticality Analysis** – Core element at the social / traffic layer of the safety argumentation
  - **Managing dilemma of completeness and condensation of test space**

- **Next steps**
  - Publification of Criticality Analysis in 2020
  - Further development of Phenomenon Signal Model, Ontology, overall method and safety metrics concept

WELCOME – Starting Page

Henning Mosebach, German Aerospace Center, German Aerospace Center (DLR)

Moderators:

- Lutz Eckstein, ika – RWTH Aachen University
- Hermann Winner, University of Darmstadt
- Steve Shladover, University California Berkeley, PATH

Meeting coordination support by: Jane Lappin, TRB Committee on Vehicle-Highway Automation (US), Adrian Zlocki, fka GmbH (Germany), Steven Shladover, UC Berkeley PATH Program (US)