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

PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

V&V Methods - PEGASUS Family first Results

SIP-Adus Workshop 10.-12. Nov. 2020 - Session Safety Assurance

Roland Galbas, coordinator of VV-Methods project

(VV-Methods Co-Coordinated by Mark Schiementz)

Robert Bosch GmbH

VV-METHODS PEGASUS Family – Overview

VERIFICATION
VALIDATION
METHODS

- **Agenda**
  - Overview: VV-Methods and PEGASUS Family
  - First Result: Safety Argumentation and related Project Goals

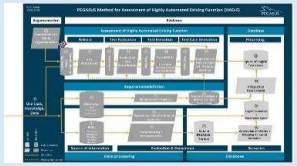
VV-METHODS PEGASUS Family – Publicly-funded Projects in Germany

- The **PEGASUS Family** focuses on development / testing methods and tools for AD systems on highways and in urban environments

PEGASUS

https://www.pegasusprojekt.de/en/home

- Scope: **Basic methodological framework**
- Use-Case: L3/4 on highways
- Partners: 17



PEGASUS FAMILY

VV-Methods

- Scope: **Methods, toolchains, specifications for technical assurance**
- Use-Case: L4/5 in urban environments
- Partners: 23 partners
- Timeline: 07/2019 – 06/2023

SET Level 4to5

- Scope: **Simulation platform, toolchains, definitions for simulation-based testing**
- Use-Case: L4/5 in urban environments
- Partners: 20 partners
- Timeline: 03/2019 – 08/2022

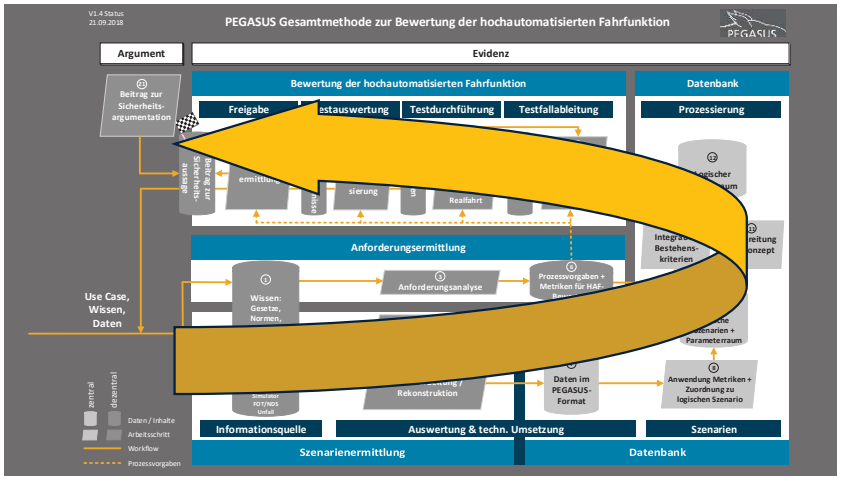
\+ future projects of the PEGASUS Family

2016 2019 Time

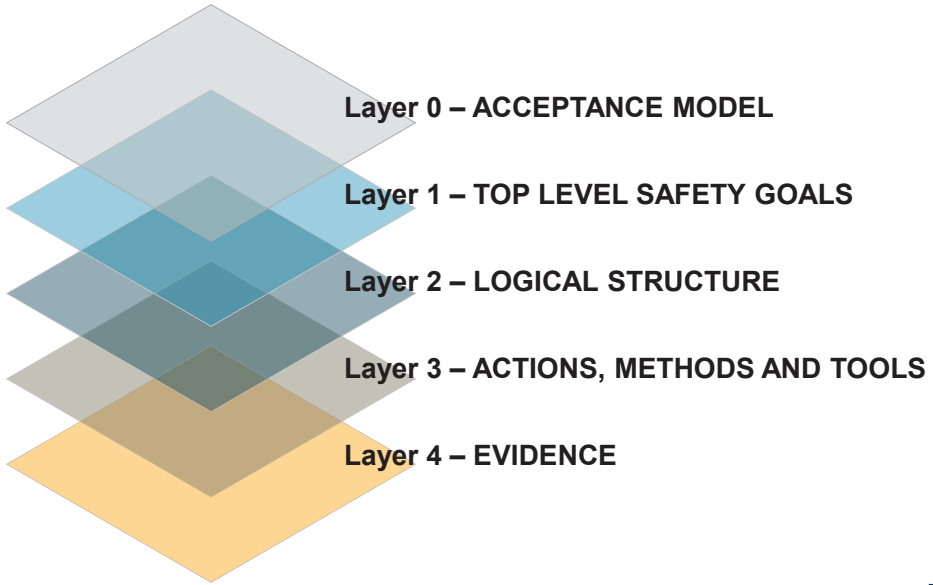
First Result: Safety Argumentation and related Project Goals

Were do we come from: The Pegasus Method

- Based on PEGASUS Requirements Definition



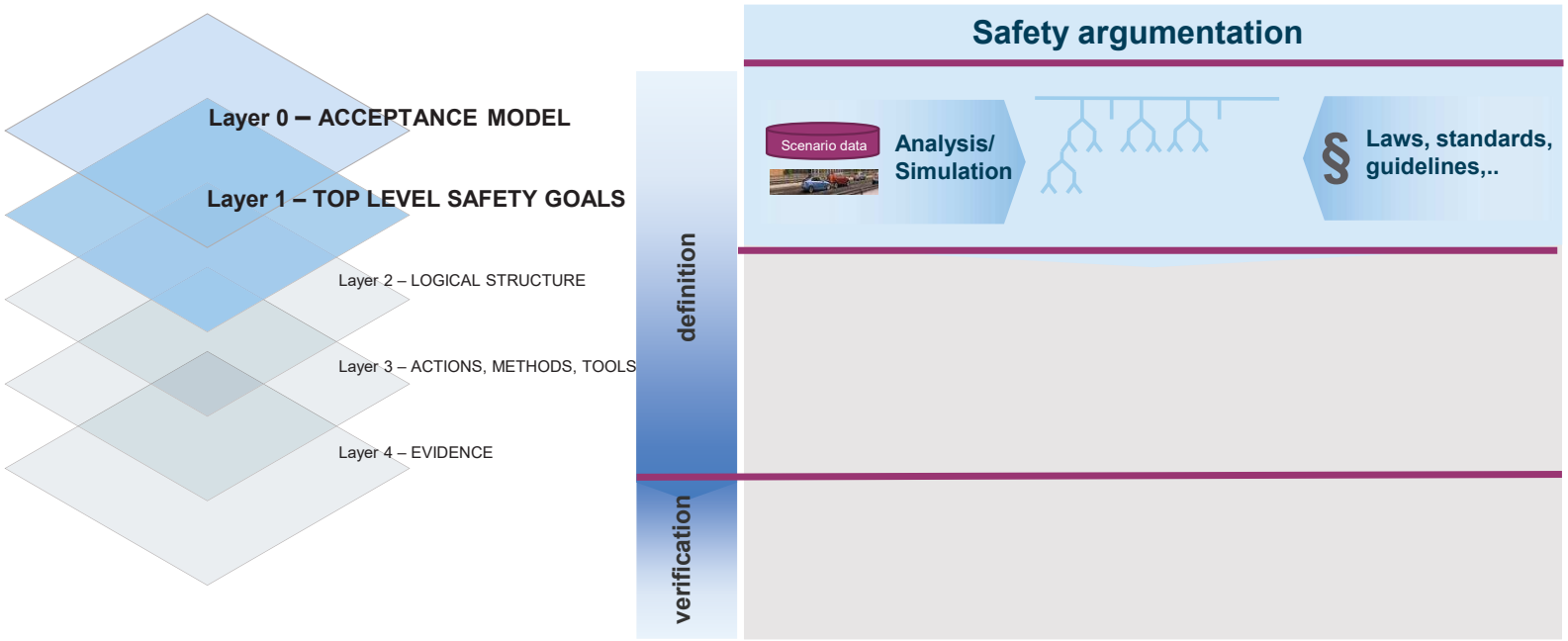
- Consistent with PEGASUS Safety Argumentation



Safety Argumentation Building up a systematic Requirement Flow structured by Layer-Interfaces

VV-METHODS – A Systematic Safety Argumentation

Building on PEGASUS and filling the layers

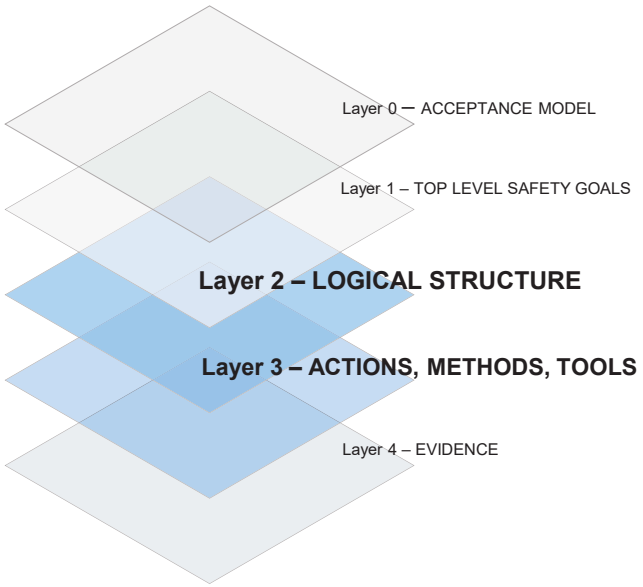


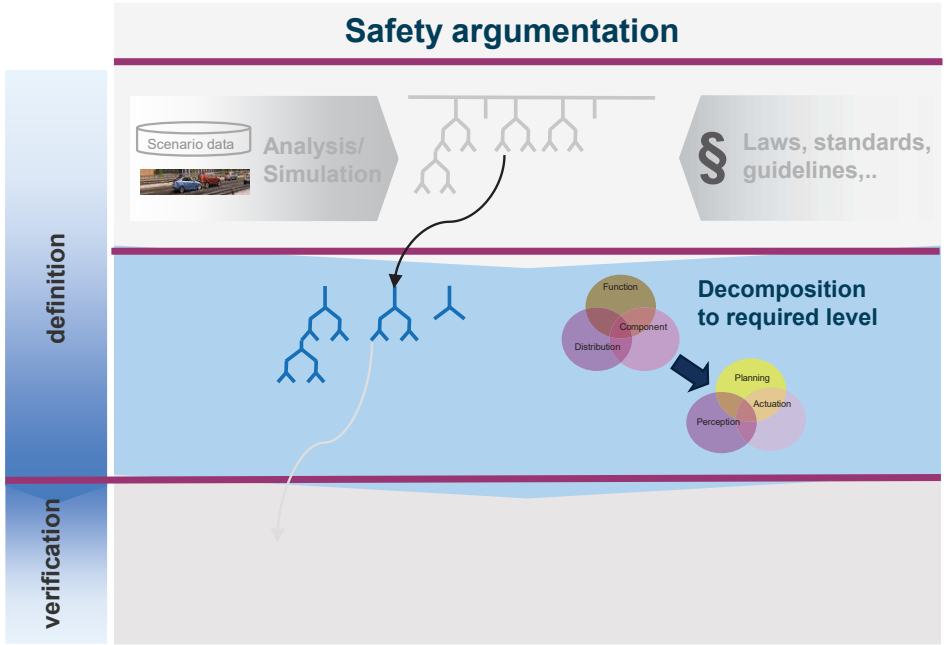
What is a safe / target behavior?

- Laws, Requirements, Standards
- Understand relevant traffic phenomena
- Identify rules for behavior

VV-METHODS – A Systematic Safety Argumentation

Building on PEGASUS and filling the layers





What is a safe / target behavior**?**

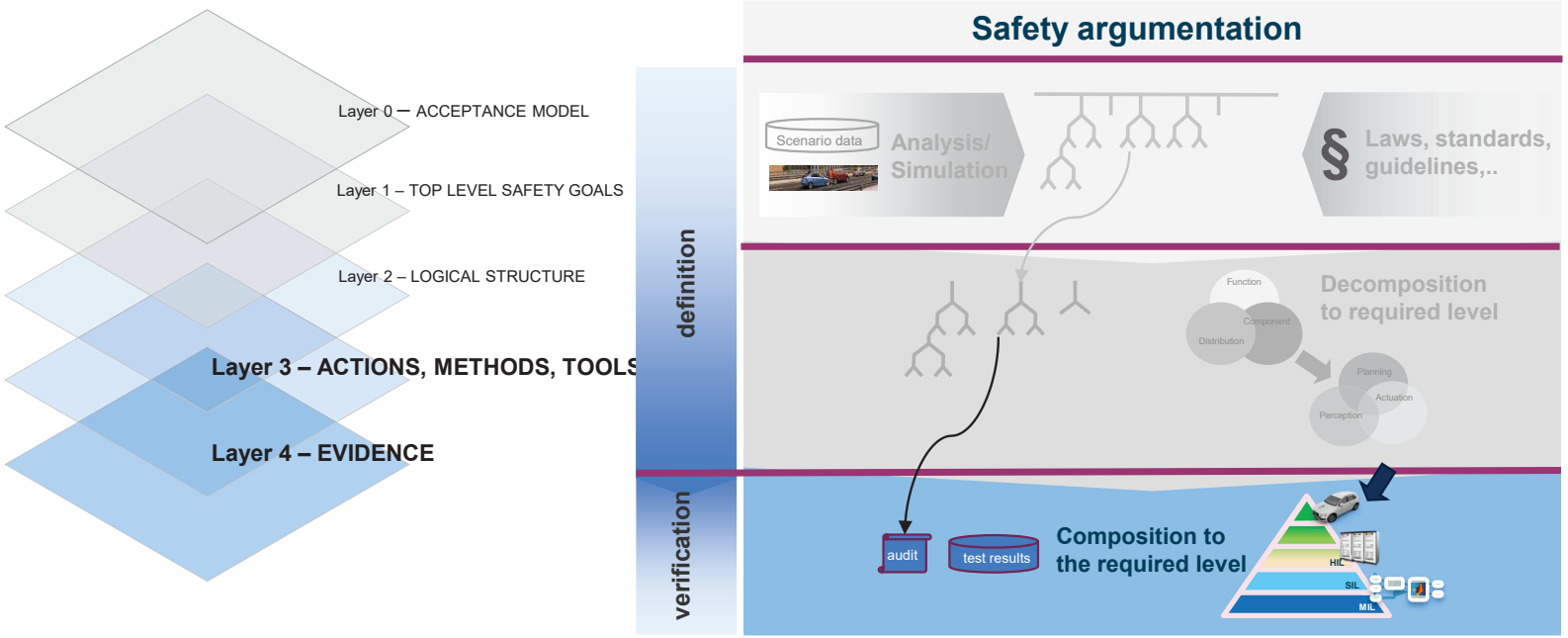
- Laws, Requirements, Standards
- Understand relevant traffic phenomena
- Identify rules for behavior

Transform in technical requirements

- Decomposition to required level
- Rules for argumentation
- Systematic analysis of cross cutting dependencies

VV-METHODS – A Systematic Safety Argumentation

Building on PEGASUS and filling the layers



What is a safe / target behavior?

- Laws, Requirements, Standards
- Understand relevant traffic phenomena
- Identify rules for behavior

Transform in technical requirements

- Decomposition to required level
- Rules for argumentation
- Systematic analysis of cross cutting dependencies

Verify and audit

- Choose best verification methods
- Derive tests from test catalogue
- Move tests to simulation wherever possible
- **Build up Evidences**

VV-METHODS – Safety Argumentation & Project Goals

VERIFICATION VALIDATION METHODS

Safety argumentation

definition

verification

Goal I – Systematic control of test cases
- Understand relevant phenomena & traffic behaviors
- Involve traffic law perspective
- Approach a **target behavior**
- Identify **enveloping tests**

§

$\infty \rightarrow n$

Common Requirements

social / traffic layer
defined by traffic laws, NHTSA, Ethic aspects, traffic & environment data …

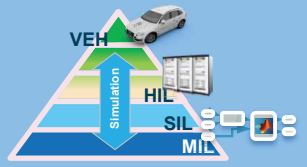
Goal II – Industrial interfaces
- Common methods for systematic breakdown of technical contracts, requirements & tests
- Agreed rules for **component exchange** between OEM and supplier
- Efficient **variant-release**, preservation of test-results of unmodified components
- Integration of **systems of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

Design & Brake-down

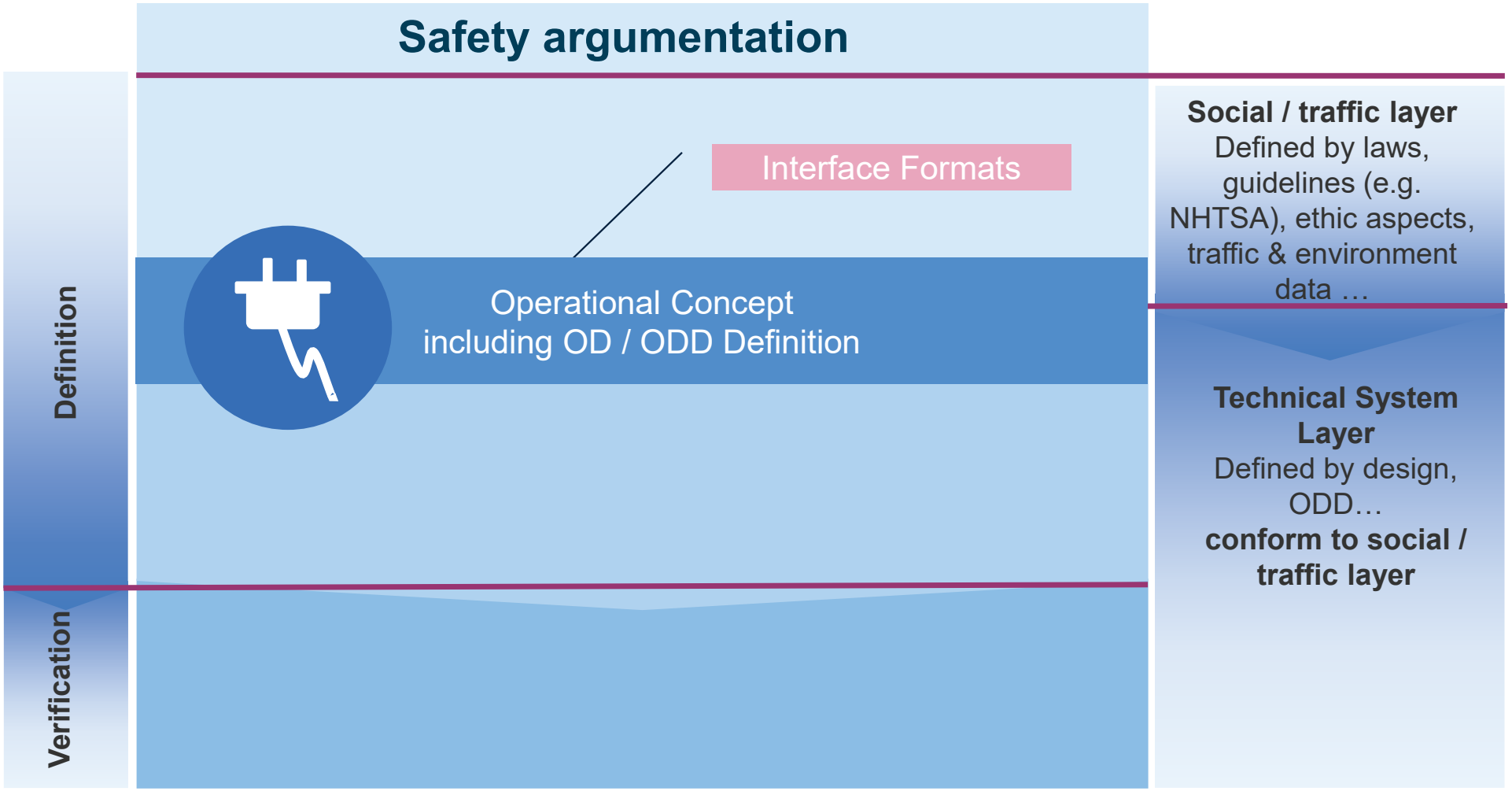
technical system layer
defined by design, ODD…
conform to social / traffic layer

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).

Evidences



VV-METHODS – Safety Argumentation - current focus

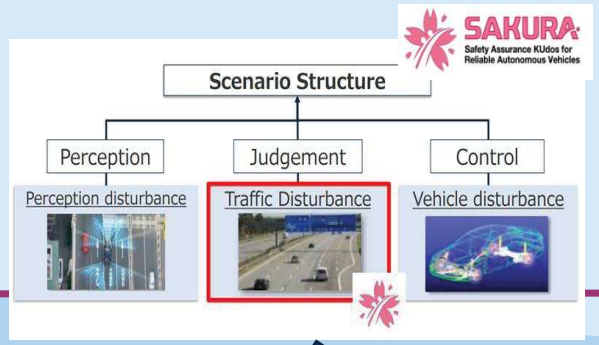


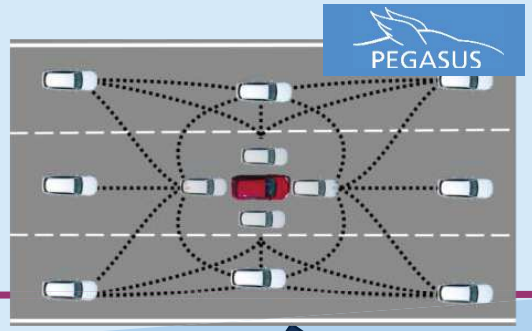
VV-METHODS – Safety Argumentation

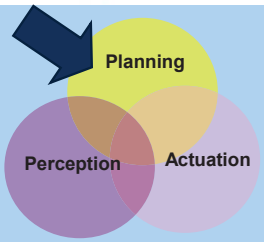
VERIFICATION VALIDATION METHODS

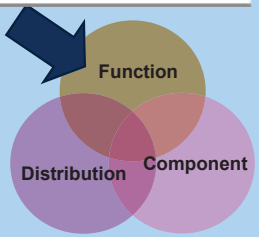
Safety argumentation

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 – 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.

BACKUP SLIDES

VV-METHODS – Project Setup

VERIFICATION VALIDATION METHODS

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

- **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, FZI, DLR

VV-METHODS – Main Goals

VERIFICATION
VALIDATION
METHODS

Systematic control of test space

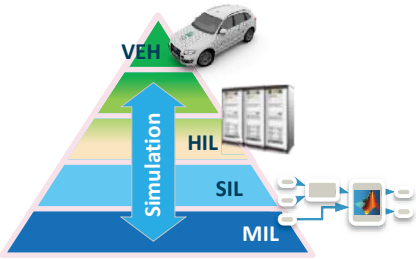
- Methods to optimize (and reduce) the test parameter space to a manageable minimum

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 **target 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**.

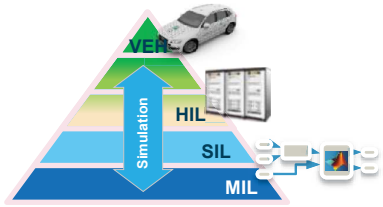
Criticality analysis

Safety assessment & safety concepts

Rules for system and test requirements

Test infrastructure

- Simulation (SET 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

VERIFICATION VALIDATION METHODS

Safety argumentation

definition

§

Laws, standards, guidelines,..

NHTSA priority safety design elements

- …
- Fallback (minimal risk condition)

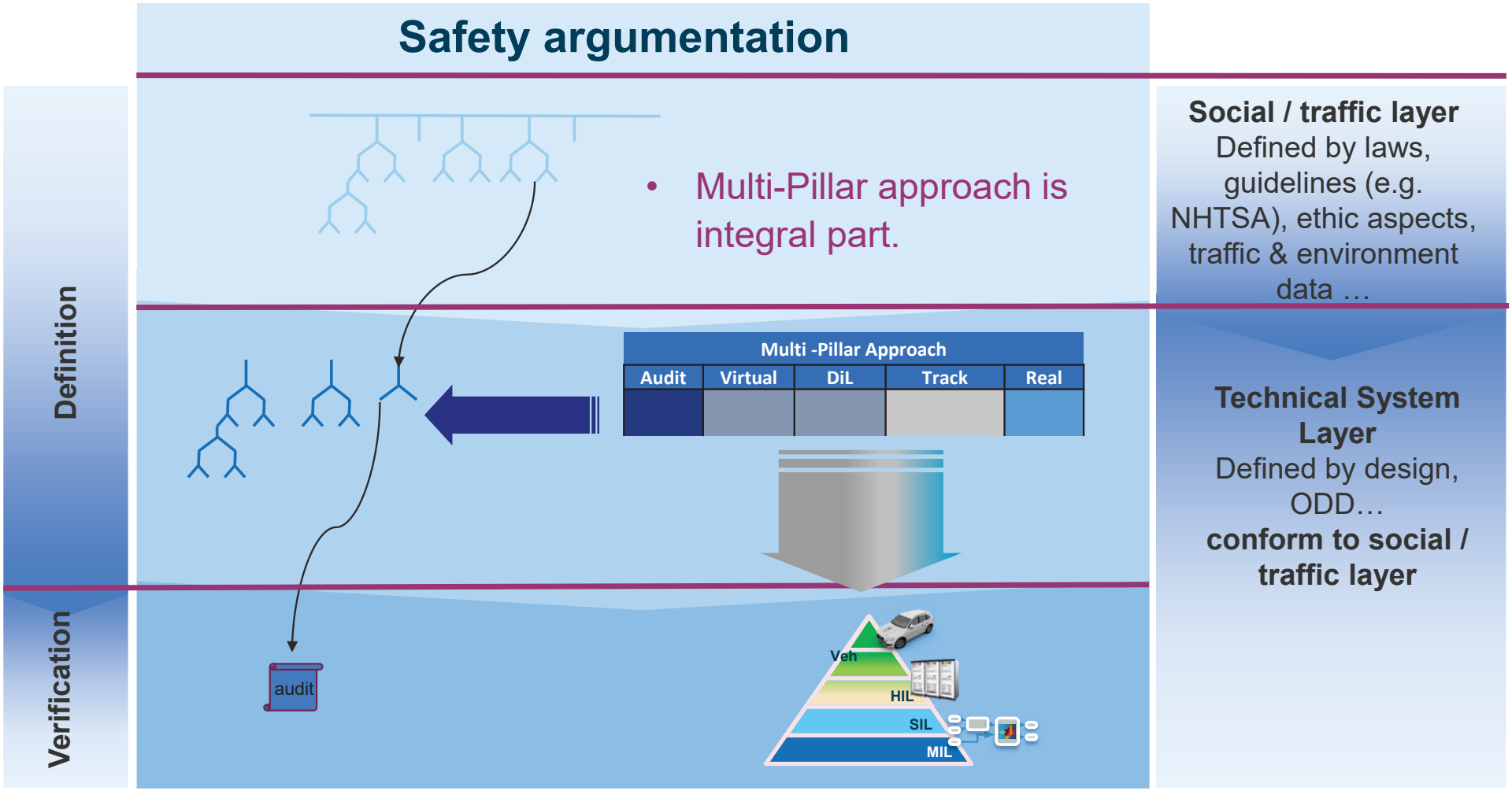
ETHICS COMMISSION automated and networked driving – Germany

- …
- **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



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 guarantees** define shape the safety argumentation – thus supporting **industrial interfaces** (based on open standards)
- **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.