PROJECT of the PEGASUS FAMILY

VERIFICATION
VALIDATION
METHODS

SET Level

SIP-adus Workshop, Kyoto
12th of October 2022

From safety argumentation to an assurance framework - The PEGASUS projects SET Level and VV Methods

Henning Mosebach, German Aerospace Center (DLR)

Supported by:
Federal Ministry
for Economic Affairs
and Climate Action

on the basis of a decision
by the German Bundestag

The PEGASUS project, SET Level and VV Methods

VERIFICATION VALIDATION METHODS

SET Level

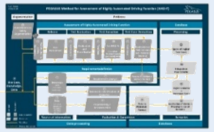
PEGASUS

PEGASUS

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

2016 - 2019

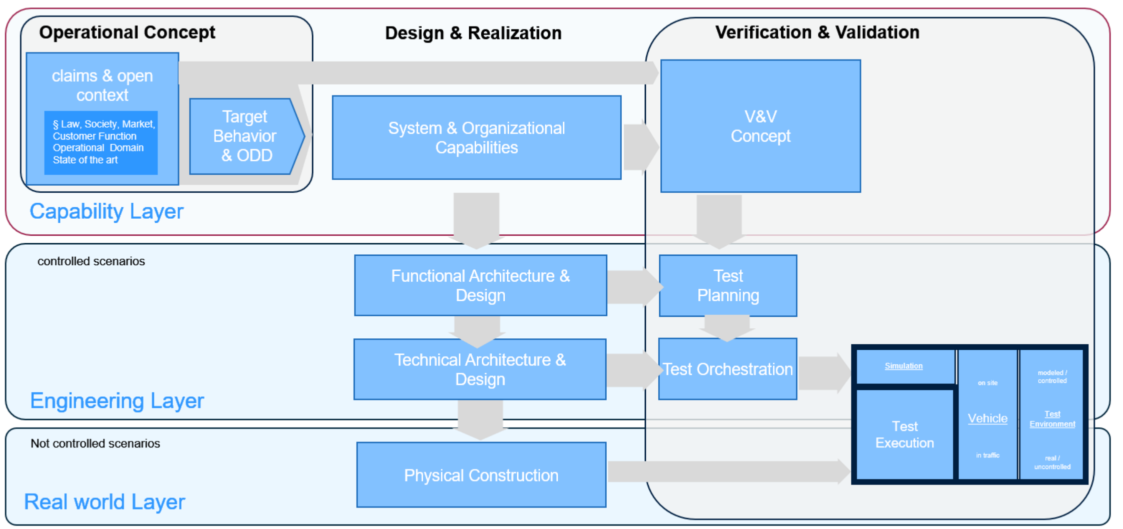
- Scope: **Basic methodological framework**
- Use-Case: L3/4 on highways
- Timeline 2016 - 2019
- Partners: 17



2019 - 2023

VERIFICATION VALIDATION METHODS

A comprehensive safety argumentation and V&V methodology



PEGASUS FAMILY

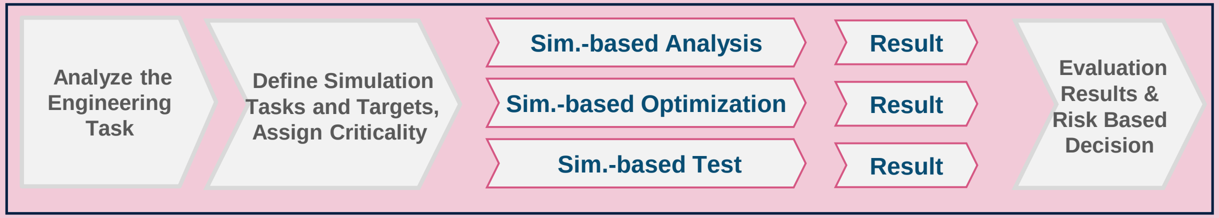
https://pegasus-family.de/

Dissemination, Cooperation, Collaboration

2019 - 2022

SET Level

A generic open simulation and testing architecture

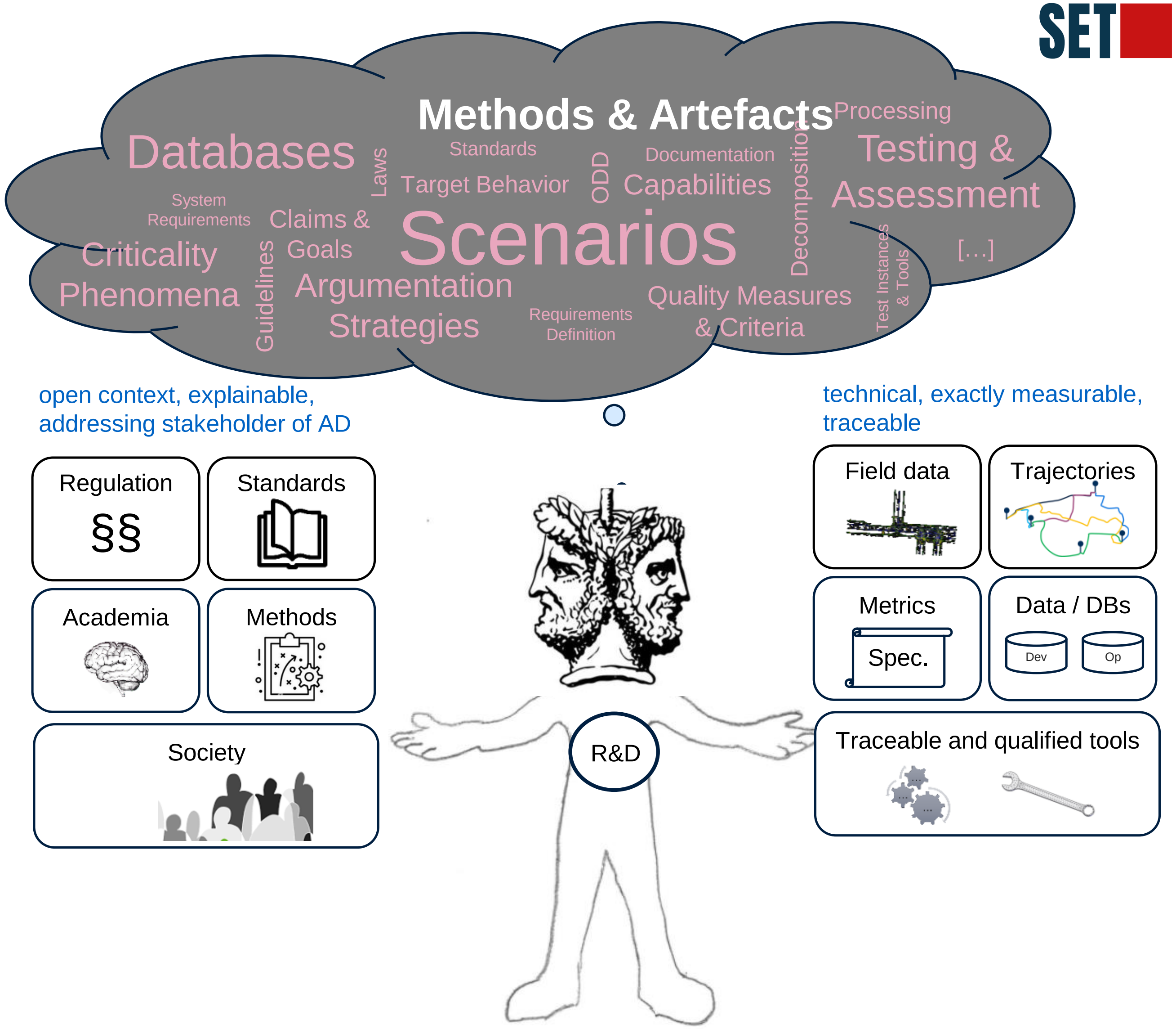


Analyze the Engineering Task
Define Simulation Tasks and Targets, Assign Criticality
Sim.-based Analysis
Sim.-based Optimization
Sim.-based Test
Result
Result
Result
Evaluation Results & Risk Based Decision

Safety argumentation and safety assurance – the challenge

Development and validation of automated driving functions requires a complete evidence based **formalized safety architecture and framework**

- Consistent safety argumentation with open and **non-formal context (law, rules, market, society)**
- Consistent and traceable **technical safety assurance framework**



Methods & Artefacts

Databases

Laws

Standards

Target Behavior

ODD

Documentation

Capabilities

Decomposition

Processing

Testing & Assessment

System Requirements

Claims & Goals

Scenarios

Criticality Phenomena

Guidelines

Argumentation Strategies

Requirements Definition

Quality Measures & Criteria

Test Instances & Tools

[…]

open context, explainable, addressing stakeholder of AD

Regulation §§

Standards

Academia

Methods

Society

R&D

technical, exactly measurable, traceable

Field data

Trajectories

Metrics

Spec.

Data / DBs

Dev

Op

Traceable and qualified tools

Many initiatives already defining content for V&V methods

Some additional questions….

- How can we **harmonize** abstract safety cases and quality metrics of technical systems and sub-systems?
- How do we integrate standards, established formats and **open tools**?
- How can we achieve common approaches for the **decomposition of scenarios** into toolchains for scenario-based testing?
- How can we achieve a **harmonized** handling of risk acceptance criteria and laws over different stakeholder and different countries?

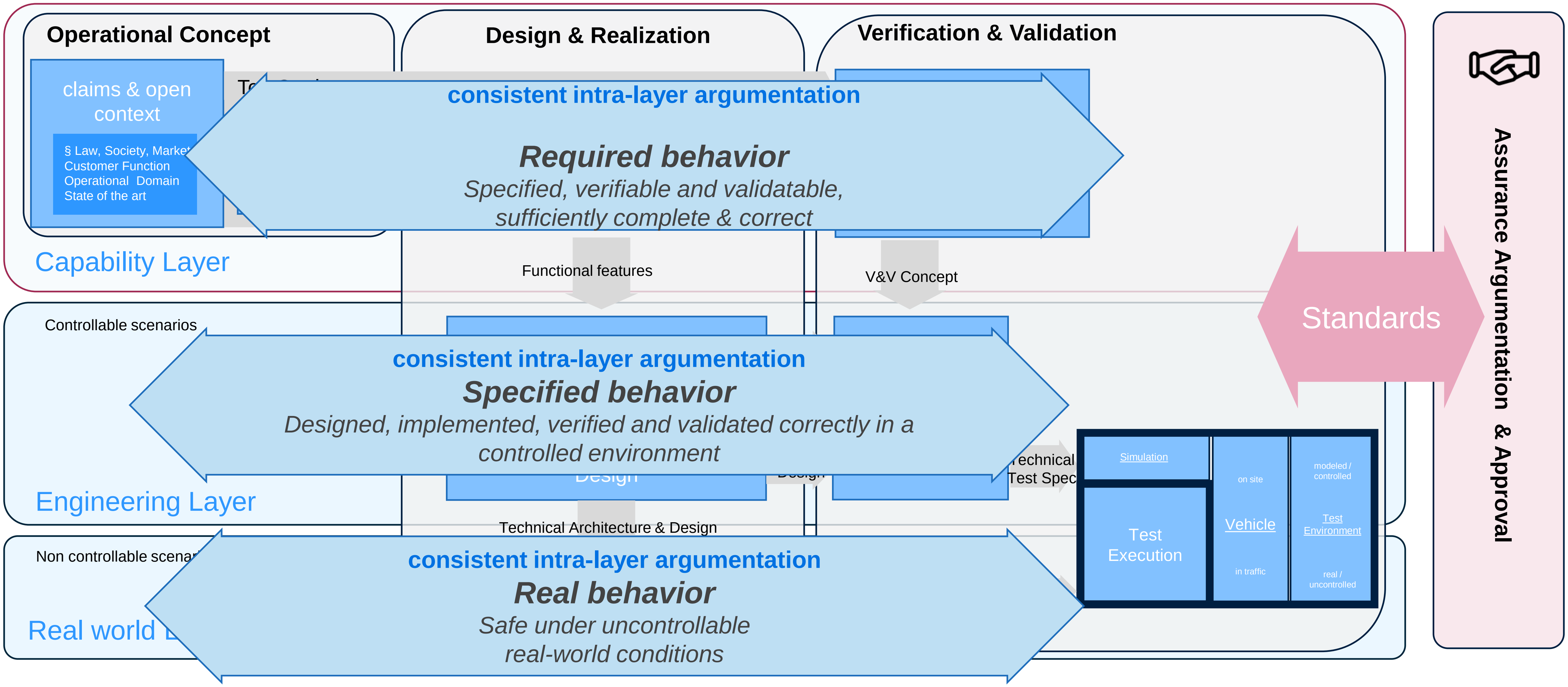
UNECE
IEEE
SAFETY FIRST FOR AUTOMATED DRIVING
White Paper
European Commission
ISO
ECLIPSE FOUNDATION
VERIFICATION VALIDATION METHODS
SET Level
bsi.
CertiCAV
Brought to you by:
CATAPULT
WMG
CCAM
CONNECTED, COOPERATIVE & AUTOMATED MOBILITY
HEADSTART
SUNRISE
ASAM
Safety Pool
Powered by: deepen & WMG
R&D
An Intel Company
SAKURA
Safety Assurance KUdos for Reliable Autonomous Vehicles
DIVP
§
NHTSA
MUSICC
Multi User Scenario Catalogue for Connected Autonomous Vehicles
NIST
U.S. Department of Transportation
National Highway Traffic Safety Administration
SAE INTERNATIONAL
EDGE CASE RESEARCH
ADScene
iamts
foretellix
M city
UNIVERSITY OF MICHIGAN

VV Methods argumentation and assurance framework

VERIFICATION
VALIDATION
METHODS

SET Level

- Synchronisation between Assurance Argumentation Development/Operation, Design and V&V



Operational Concept

Design & Realization

Verification & Validation

claims & open context

§ Law, Society, Market
Customer Function
Operational Domain
State of the art

To

consistent intra-layer argumentation

Required behavior

Specified, verifiable and validatable, sufficiently complete & correct

Capability Layer

Functional features

V&V Concept

Controllable scenarios

consistent intra-layer argumentation

Specified behavior

Designed, implemented, verified and validated correctly in a controlled environment

Design

Design

Technical Test Spec

Engineering Layer

Technical Architecture & Design

Non controllable scenar

consistent intra-layer argumentation

Real behavior

Safe under uncontrollable real-world conditions

Real world L

Simulation

Test Execution

on site

Vehicle

in traffic

modeled / controlled

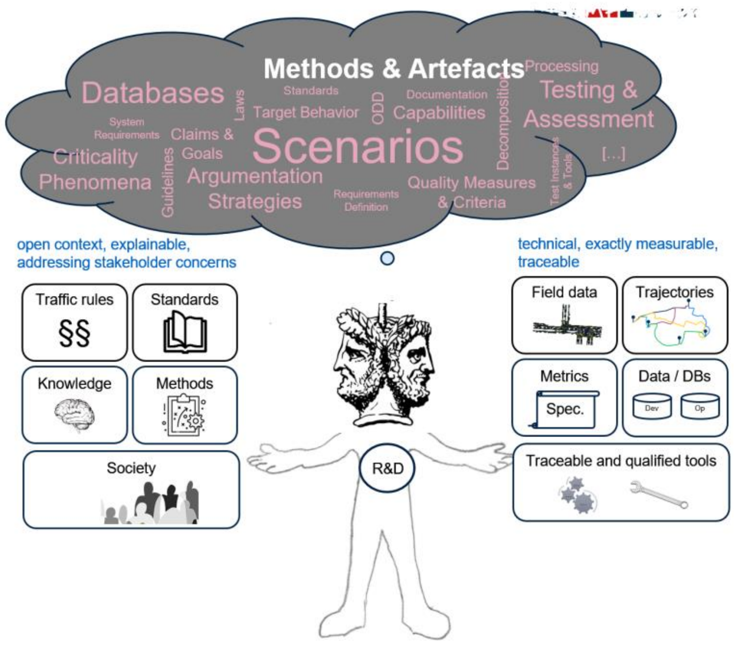
Test Environment

real / uncontrolled

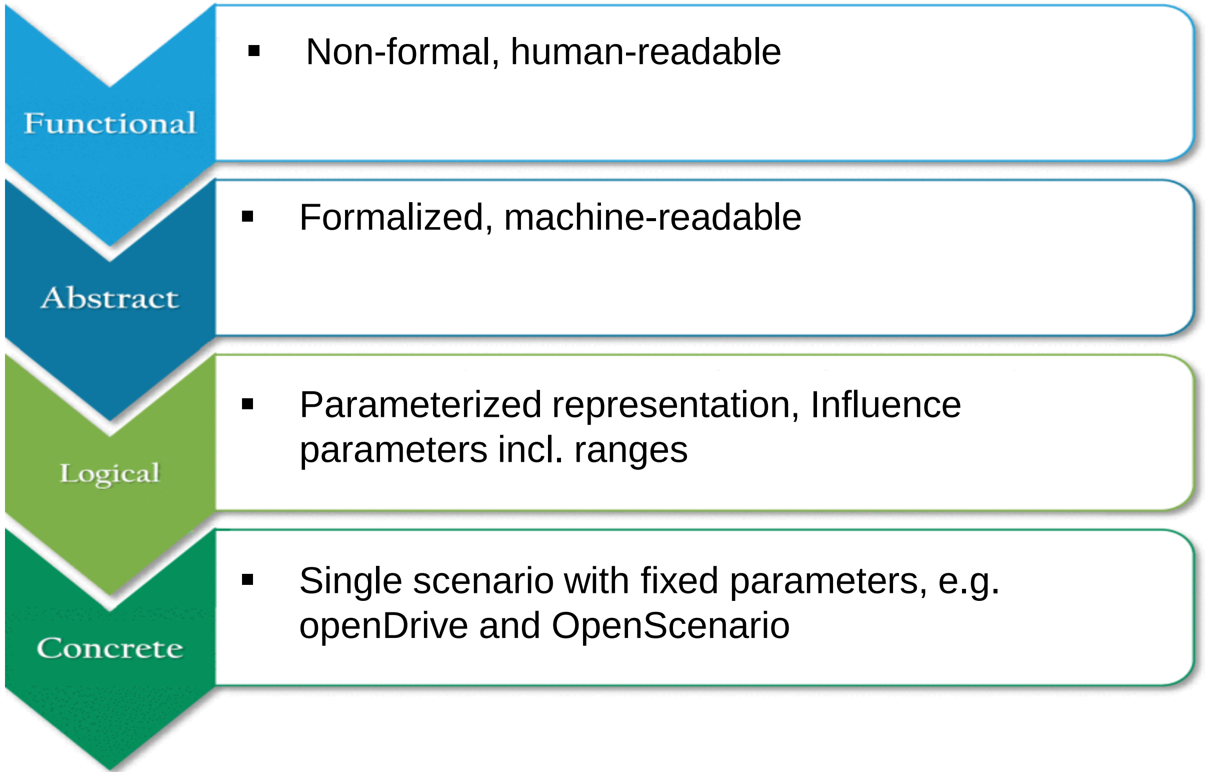
Standards

Assurance Argumentation & Approval

The glue: Scenario driven approach



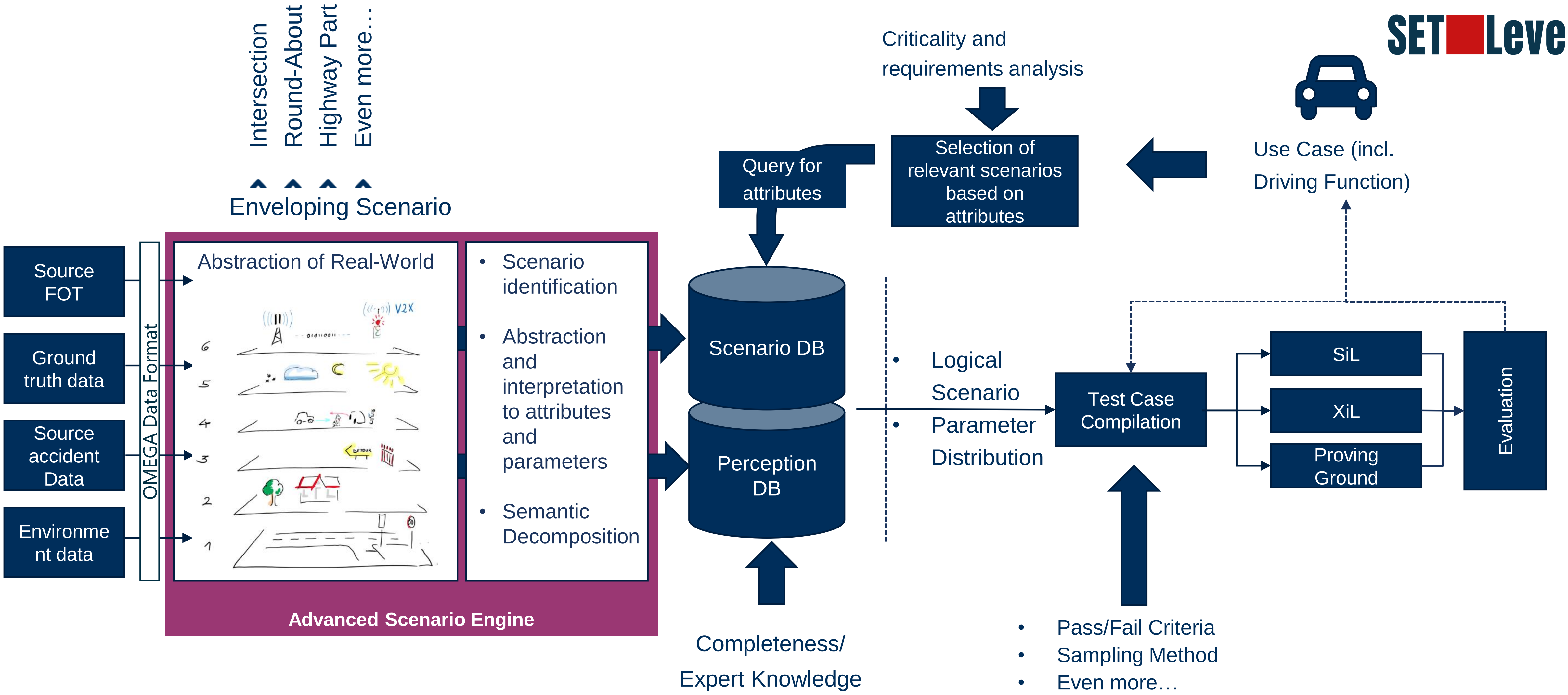
Test scenario categories



- Functional: Non-formal, human-readable
- Abstract: Formalized, machine-readable
- Logical: Parameterized representation, Influence parameters incl. ranges
- Concrete: Single scenario with fixed parameters, e.g. openDrive and OpenScenario

- Scenarios are used to proof system performance e.g. to derive dependencies of sub-system characteristics towards the overall (safety) performance
- Scenarios /data-categories have to be consistent within their abstraction layers

Selected example of VV Methods: Dataflow and scenario engine



Intersection

Round-About

Highway Part

Even more…

Enveloping Scenario

Source FOT

Ground truth data

Source accident Data

Environment data

OMEGA Data Format

Abstraction of Real-World

- Scenario identification
- Abstraction and interpretation to attributes and parameters
- Semantic Decomposition

Advanced Scenario Engine

Query for attributes

Criticality and requirements analysis

Selection of relevant scenarios based on attributes

Use Case (incl. Driving Function)

Scenario DB

Perception DB

Completeness/ Expert Knowledge

- Logical Scenario
- Parameter Distribution

Test Case Compilation

SiL

XiL

Proving Ground

Evaluation

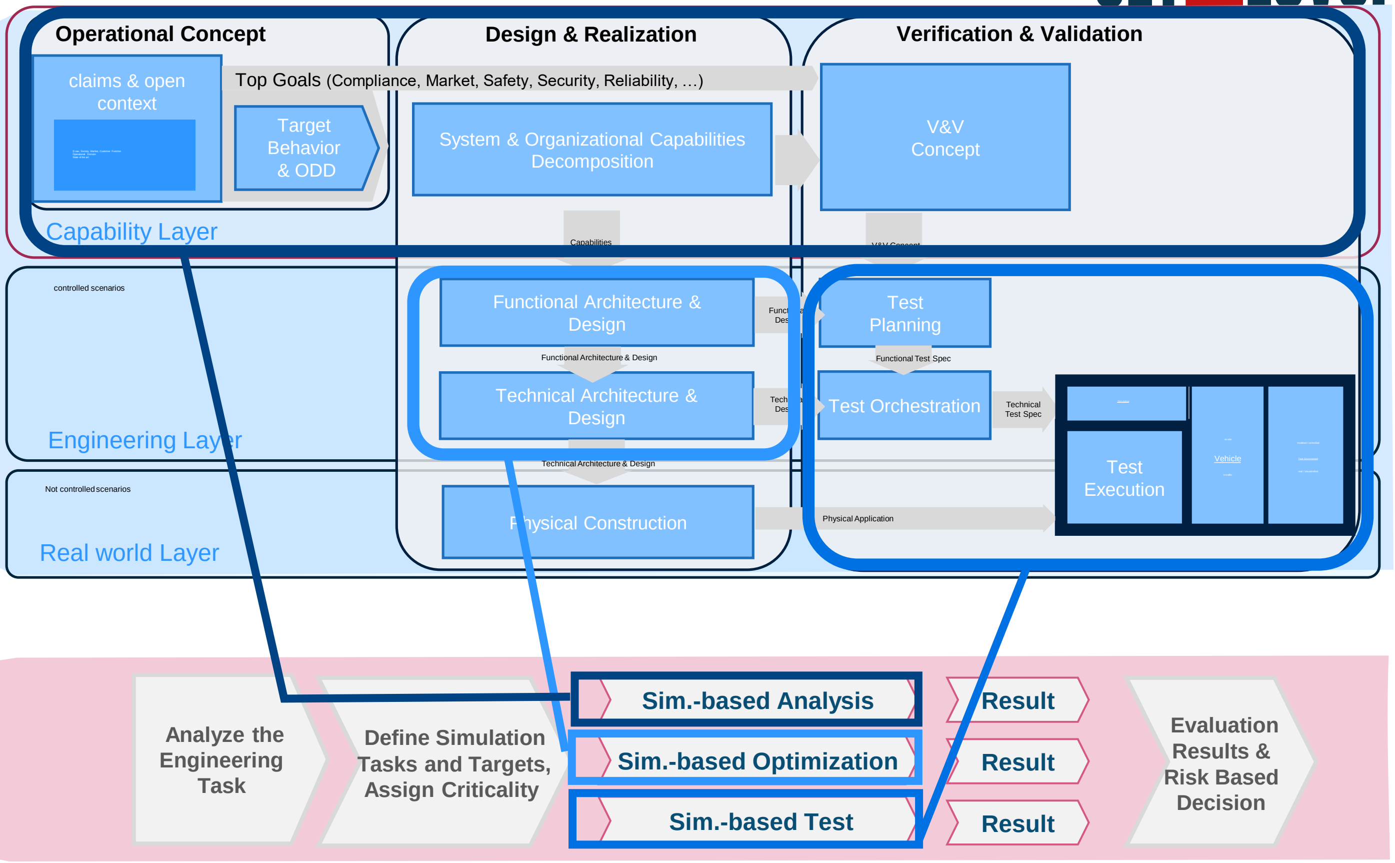
- Pass/Fail Criteria
- Sampling Method
- Even more…

Functional scenarios -> logical scenario classes -> parameters/attributes -> instances of logical scenarios -> concrete scenarios

Link between VV Methods / SET Level

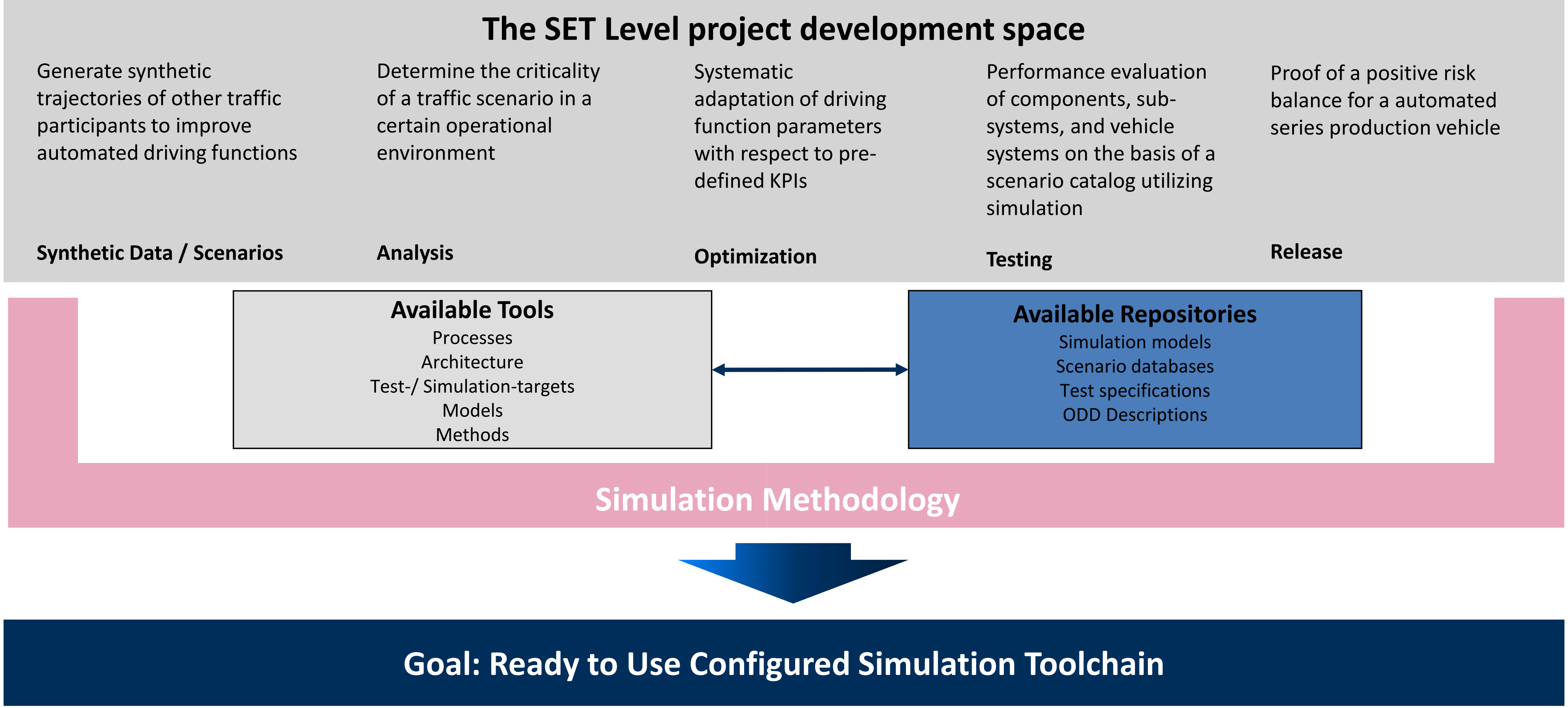
Safety argumentation layer structure.

Simulation-based Engineering Task



- Simulation engineering task are assigned to the VVM safety argumentation layer structure

The SET Level functional approach and big picture



The SET Level project development space

Synthetic Data / Scenarios	Analysis	Optimization	Testing	Release
Generate synthetic trajectories of other traffic participants to improve automated driving functions	Determine the criticality of a traffic scenario in a certain operational environment	Systematic adaptation of driving function parameters with respect to pre-defined KPIs	Performance evaluation of components, sub-systems, and vehicle systems on the basis of a scenario catalog utilizing simulation	Proof of a positive risk balance for a automated series production vehicle

Available Tools

Processes
Architecture
Test-/ Simulation-targets
Models
Methods

Available Repositories

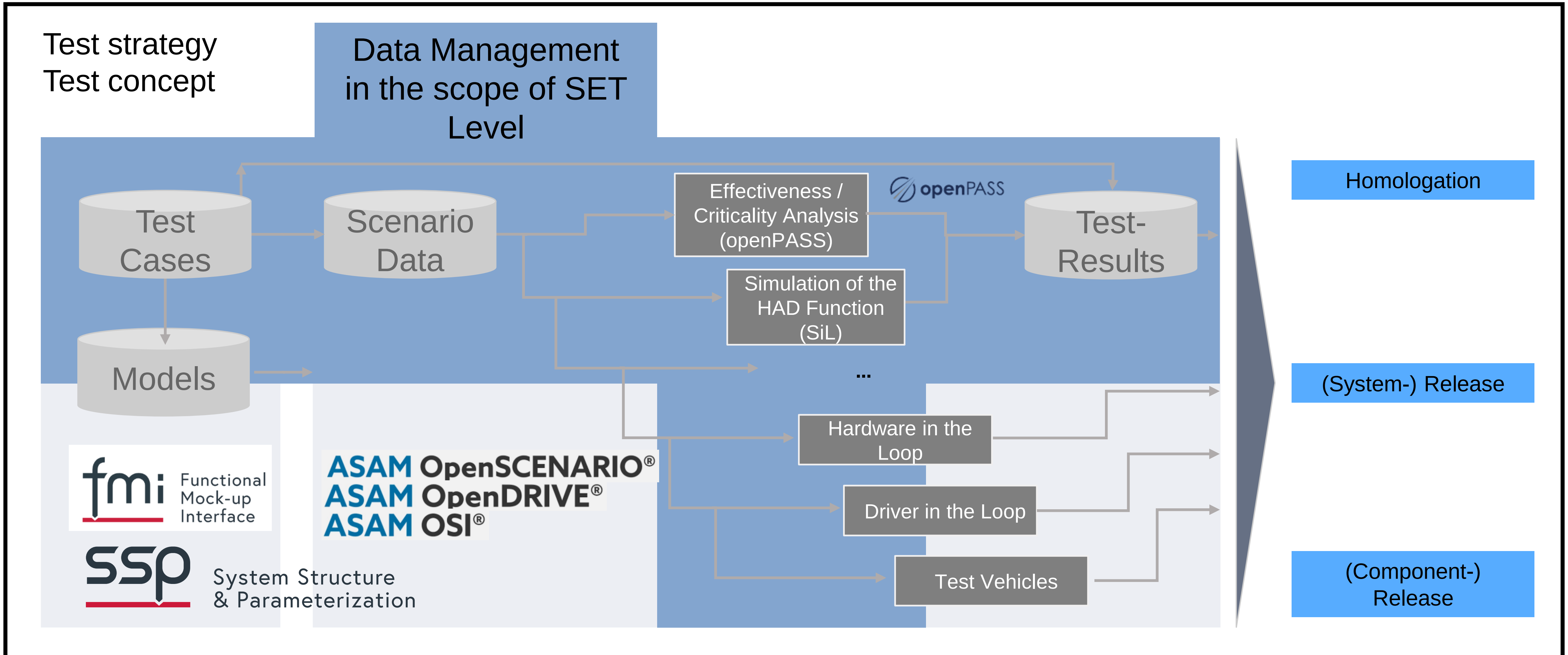
Simulation models
Scenario databases
Test specifications
ODD Descriptions

Simulation Methodology

Goal: Ready to Use Configured Simulation Toolchain

SET Level - Basic approach

Use of standards and traceability



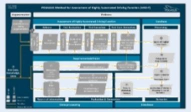
Legend: HAD Function – Highly Automated Driving Function, SiL – Software in the Loop

SET Level and VV Methods – latest results

PEGASUS

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

- Scope: **Basic methodological framework**
- Use-Case: L3/4 on highways
- Timeline 2016 - 2019
- Partners: 17



PEGASUS FAMILY

https://pegasus-family.de/

Dissemination, Coorperation, Collaboration

A comprehensive safety argumentation and V&V methodology

Mid-term Event March 15th, 2022

- ➢ Slides and videos: https://www.vvm-projekt.de/en/midterm-docs
- ➢ All VVM publications https://www.vvm-projekt.de/en/project
- ➢ Final methodology scheduled for end of 2023

https://www.vvm-projekt.de/

A generic open simulation and testing architecture

Final Event: ***TODAY! (11th/12th October 2022)***

- ➢ Presentations and slides from 2021 mid-term: https://setlevel.de/en/news/slides-and-video-recordings-mte
- ➢ Presentations and slides soon on https://setlevel.de/en

https://setlevel.de/en

A look ahead: 6 collaboration areas to reach a common ground on

1 - Safe systems on the road

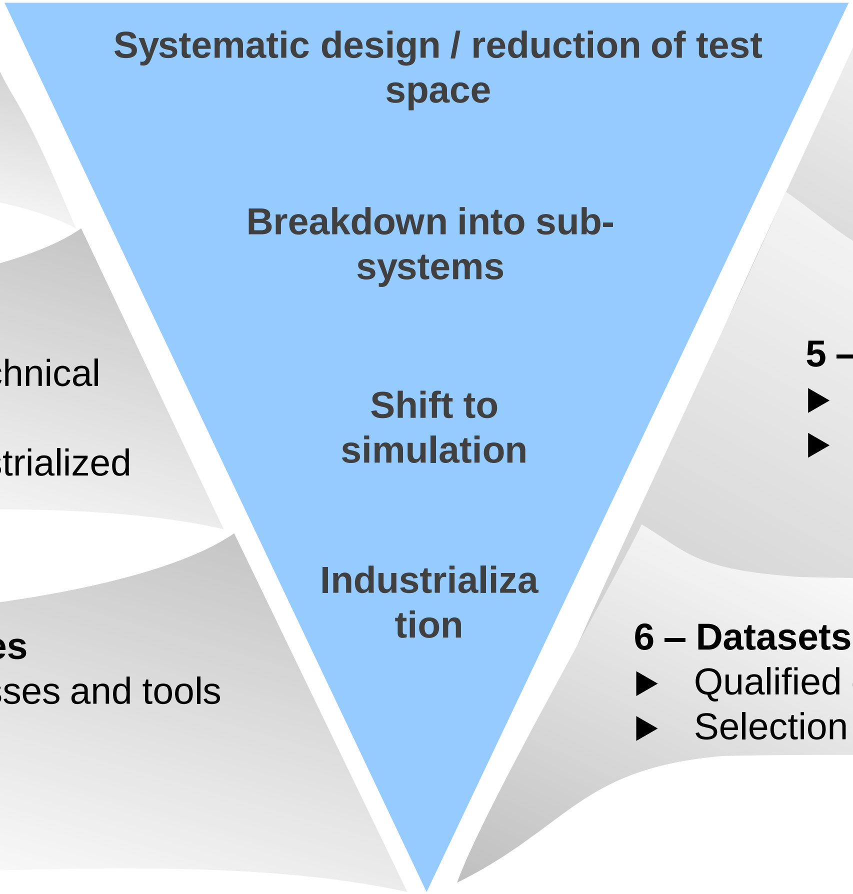
- Definition of “safe” in argumentation
- Relation to society, laws and regulation
- Accepted and defined quantification of risk

2 – ODD decomposition by scenarios

- Systematic breakdown of scenarios into technical contracts, requirements & tests
- Common interfaces and seamless for industrialized component exchange

3 – Argumentation and development processes

- Shift of argumentation to development processes and tools
- Abstraction followed by formal decomposition



Systematic design / reduction of test space

Breakdown into sub-systems

Shift to simulation

Industrializa tion

4 - Virtualization

- Virtualized components (models, data) are mandatory
- Seamless exchangeability of virtual and physical components required

5 – Tools and formats

- Tools and formats have to cover ODD
- Quality metrics and interfaces have to fit into both – argumentation method and standards

6 – Datasets for executing V&V

- Qualified data – field and synthetical
- Selection of exchangeable scenarios

Open for future collaboration

- 1st safeCAD-DJ expert workshop in June 2022

- Collaboration topics
  - Methodologies and toolchains for assurance (simulation and test)
  - Models, data, validation metrics
  - Proof-of-concepts, how to implement standards

- Strategic exchange on
  - Future research topics for safety assurance in automated driving
  - Data driven approaches and data driven ecosystems
  - Combining industrial, governmental and scientific perspectives

German-Japanese Symposium
on Safety Assurance for Connected and Automated Driving, 1.-3. June 2022, Berlin

VVM – SET Level – VIVID – DIVP – JAMA – JARI - ASAM workshop

VERIFICATION
VALIDATION
METHODS

Thank you!

PEGASUS Family international dissemination and collaboration

Henning Mosebach, German Aerospace Center (DLR)

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