PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

German Japanese Symposium for Safety Assurance

01.- 03. June 2022

# VV Methods
# from assurance framework to data flow

Roland Galbas, Robert Bosch GmbH

Supported by:

Federal Ministry for Economic Affairs and Climate Action

on the basis of a decision by the German Bundestag

# Topics

VERIFICATION
VALIDATION
METHODS

- **VVM History**
- **VVM Goals & Approach**
- **Benefit of VVM towards data flow and tools**
  - **SETLevel** – Engineering Simulation Process
  - **KIA** – Data Driven Engineering – DDE
  - Connection between Scenarios, ODD, Target Behaviour and ADS-design

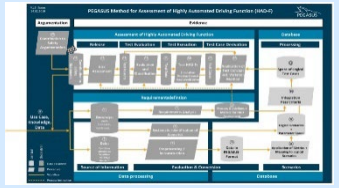
# History - PEGASUS Family

- 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: L3/4/5 in urban environments
- Partners: 23 partners
- Timeline: 07/2019 – 06/2023

## *SET Level 4to5*

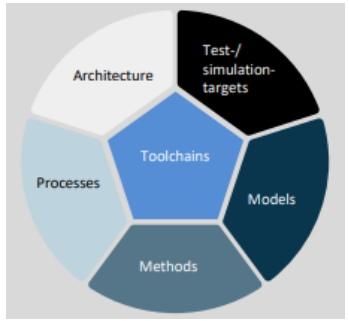
- Scope: **Simulation platform, toolchains, definitions for simulation-based testing**
- Use-Case: L3/4/5 in urban environments
- Partners: 20 partners
- Timeline: 03/2019 – 10/2022

+ future projects of the PEGASUS Family

2016 2019 **Time**

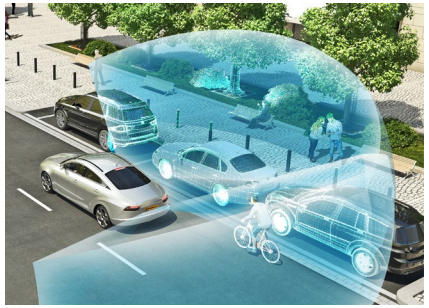
# VVM - Main goals

I. Systematic control of test space




II. Industrial interfaces

How to benefit from tools and data?
How to support them?



III. Shift to simulation

IV Argumentation

# Goals - more close

Goal IV – **Argumentation**

- Explainable Compliance

Goal I **Systematic control of test space**

- Understand relevant hazardous phenomena
- Involve traffic-law perspective
- Identify a target behavior & ODD

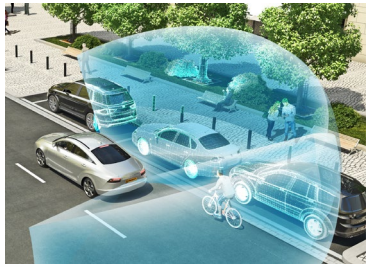
Feasibility

Efficiency

Control of ODD

System Decomposition

V&V Distribution & Generation

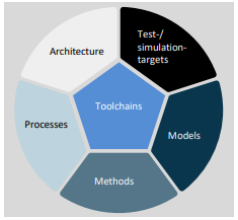


Goal III Shift to simulation

- Seamless use of virtual and real artefacts
- Efficient integration of simulation into the test-infrastructure

Goal II **Consistent interfaces**

- Systematic breakdown of technical contracts, requirements & tests
- Common interfaces for component exchange




Changeability

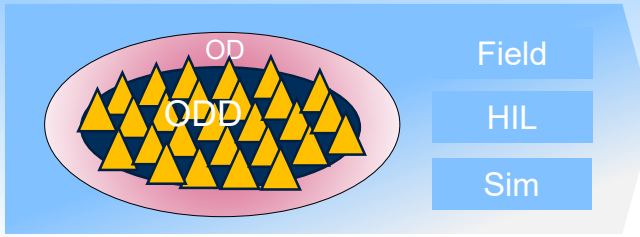
# Main Approach

VERIFICATION VALIDATION METHODS

## Classic

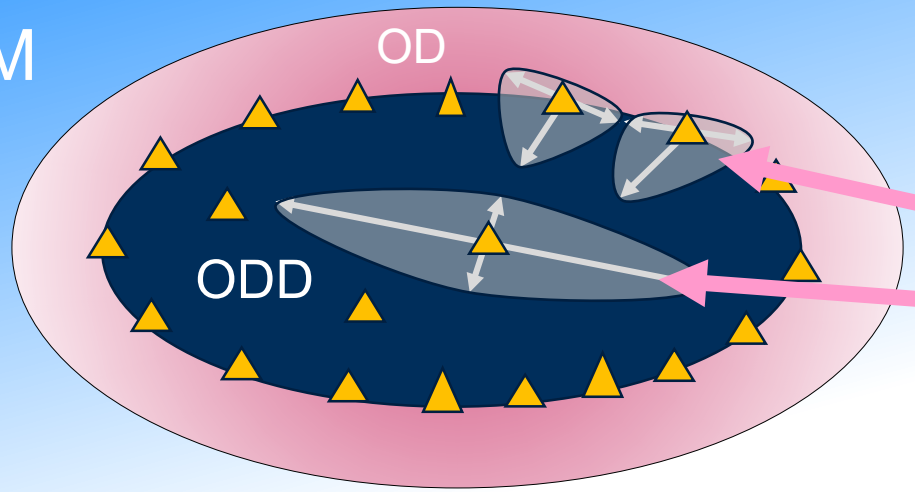
► Brute force: x million miles

## Pegasus



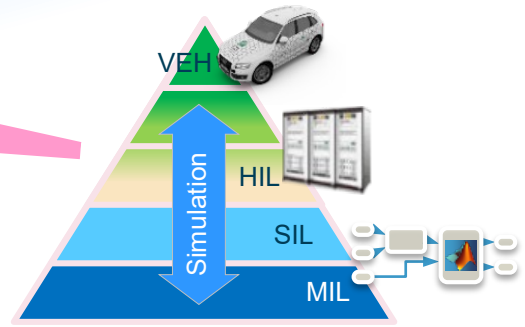

► ODD decomposition & initial argumentation

## VVM



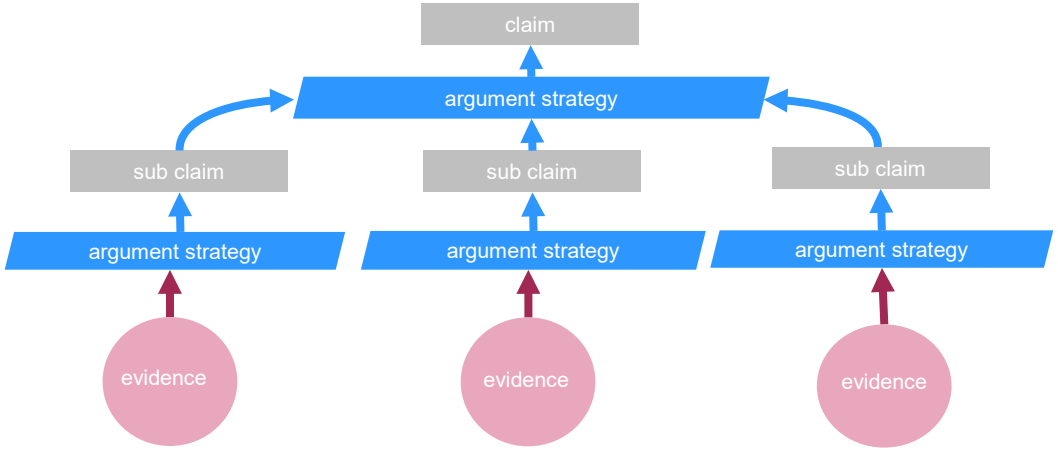

► ODD more complex
► Systematic argumentation of coverage

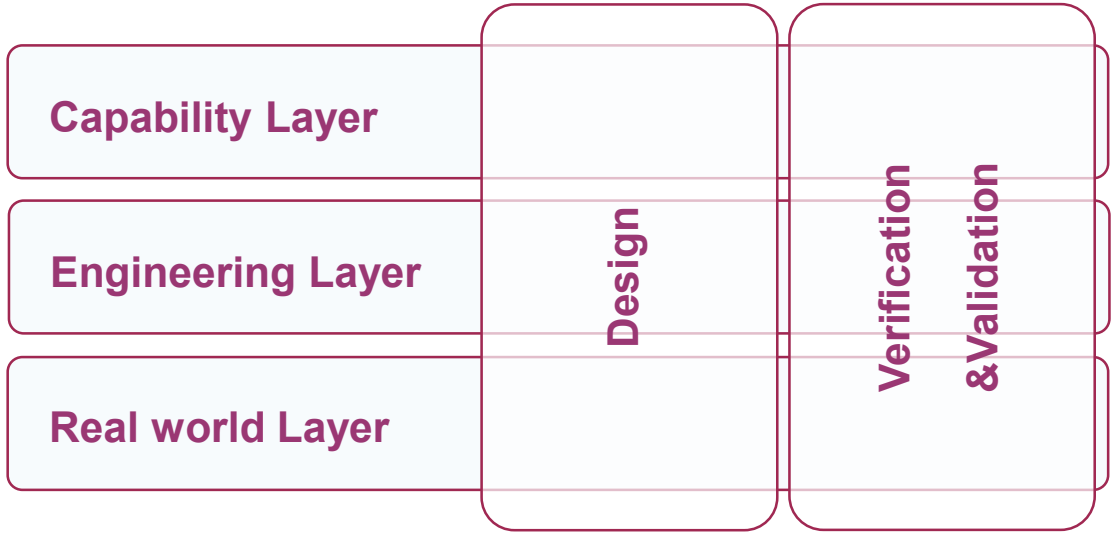
Argumentation




△ full system test

# Assurance Argumentation & Framework



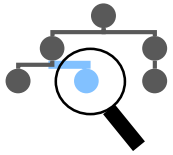




## Assurance Argumentation

- Enabler for traceable decomposition of claims and thus for explainable compliance.

## Argumentation Framework

- Structure the elements of Development & Operation with Design and V&V so that a consistent assurance argumentation is possible.



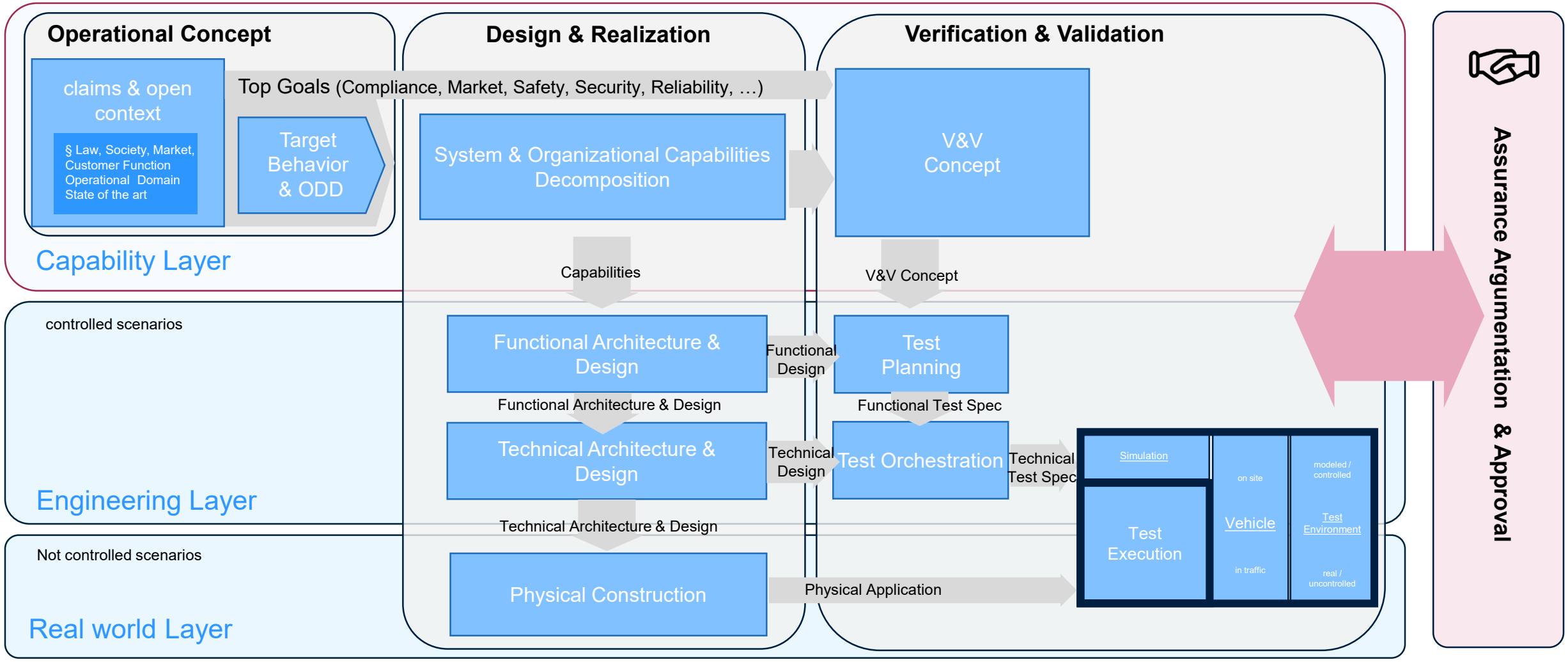
**traceability**

**consistency**

# Assurance Framework

VERIFICATION VALIDATION METHODS

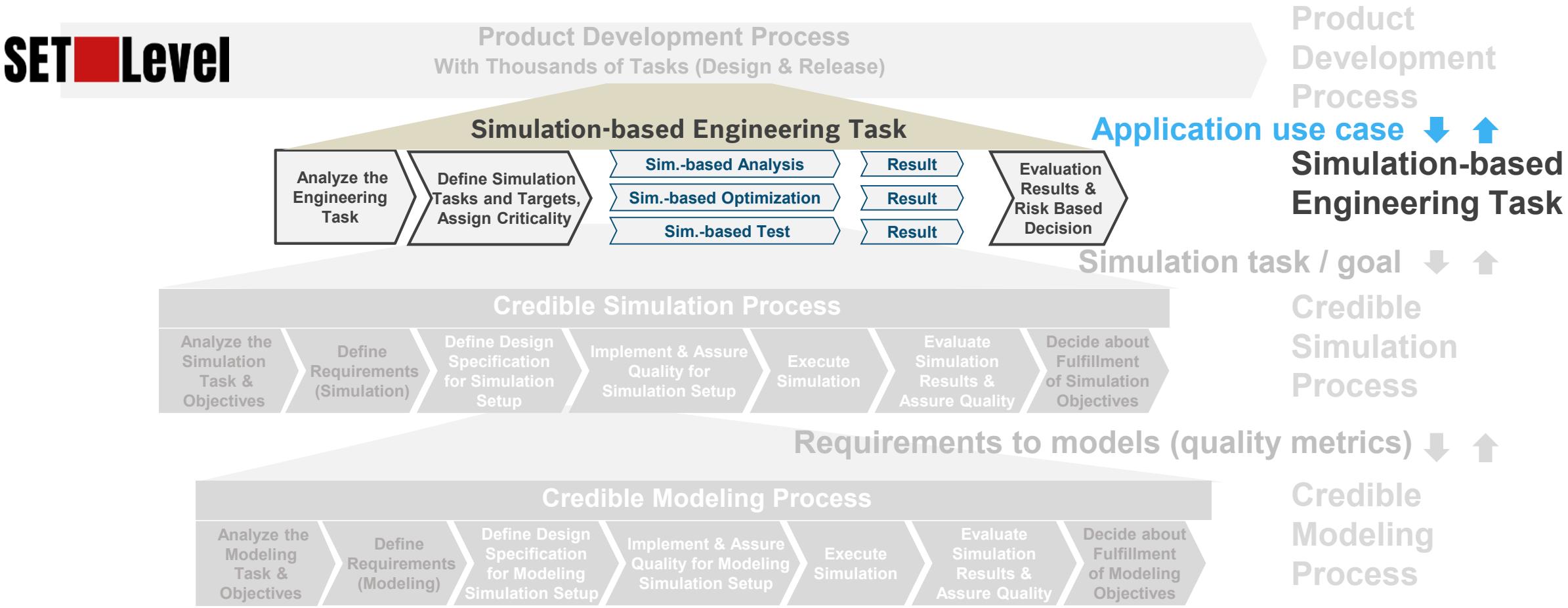
- Defines synchronisation interface between Assurance Argumentation Development/Operation, Design sand V&V.



# SET Level - Processes Link to VVM

## (1) Application use case: Simulation-based Engineering Task

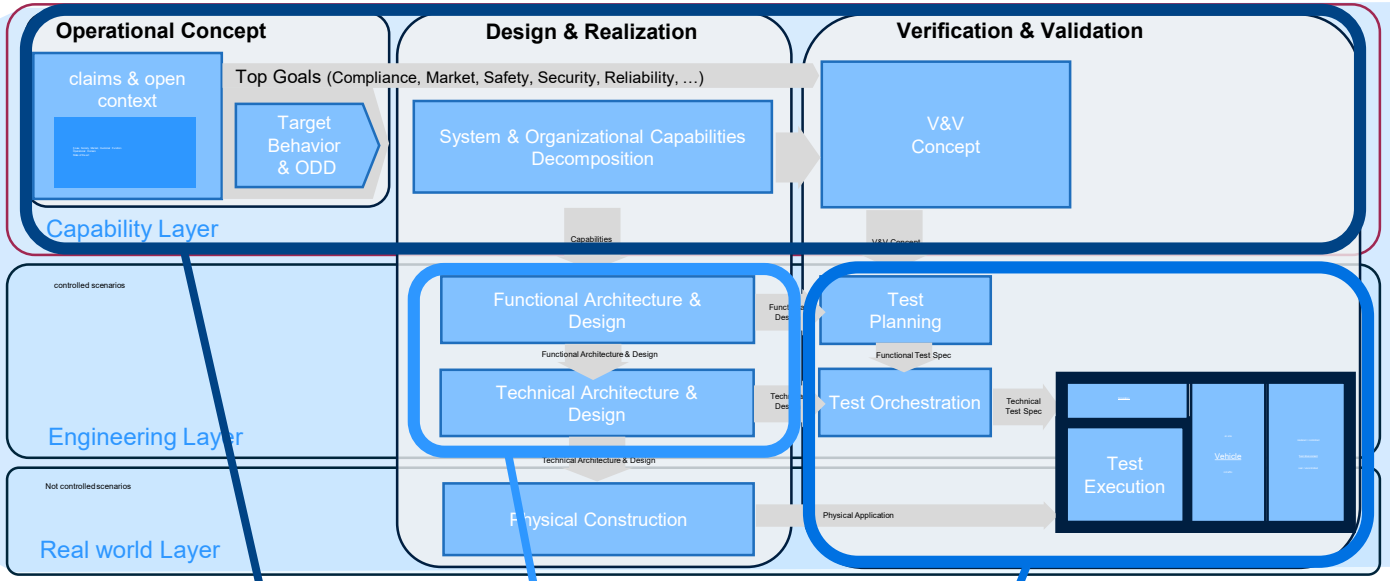
- How to assign the Simulation-based Engineering Task to the VVM Assurance argumentation?



# SET Level - Processes Link to VVM

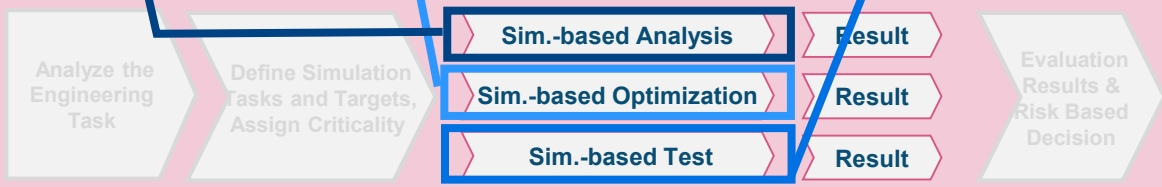
## (1) Application use case: Simulation-based Engineering Task

Safety argumentation layer structure.




SET Level

Simulation-based Engineering Task

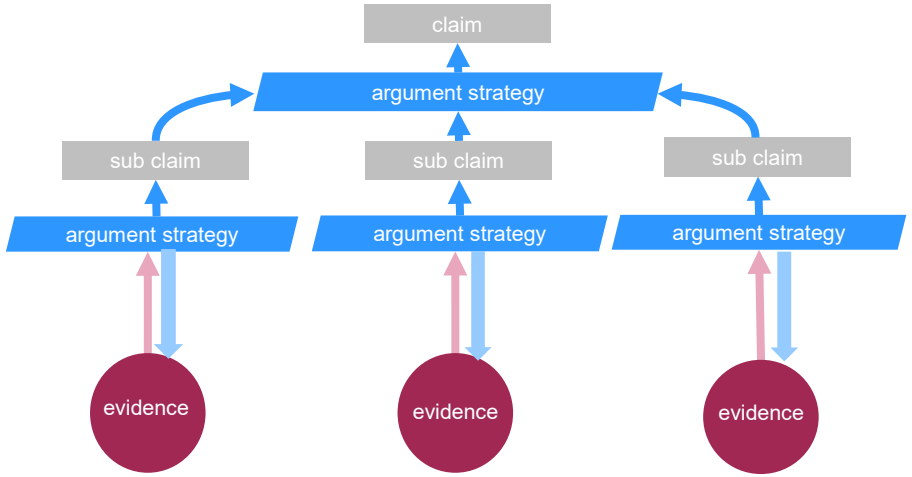


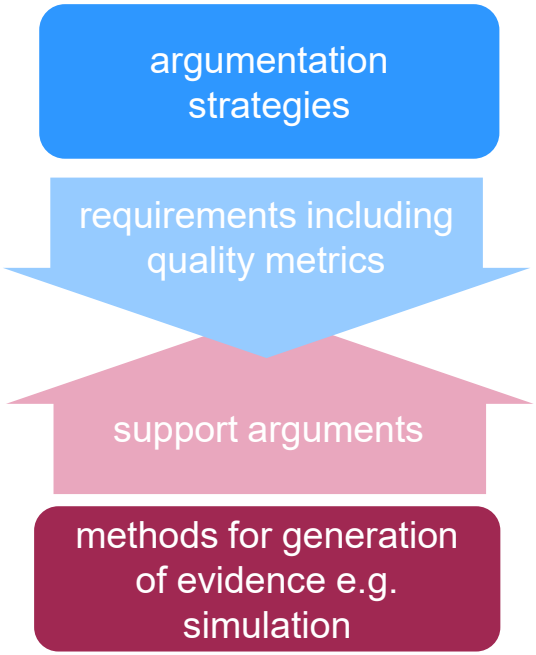

- Simulation Engineering Task can be directly assigned to the VVM safety argumentation layer structure.

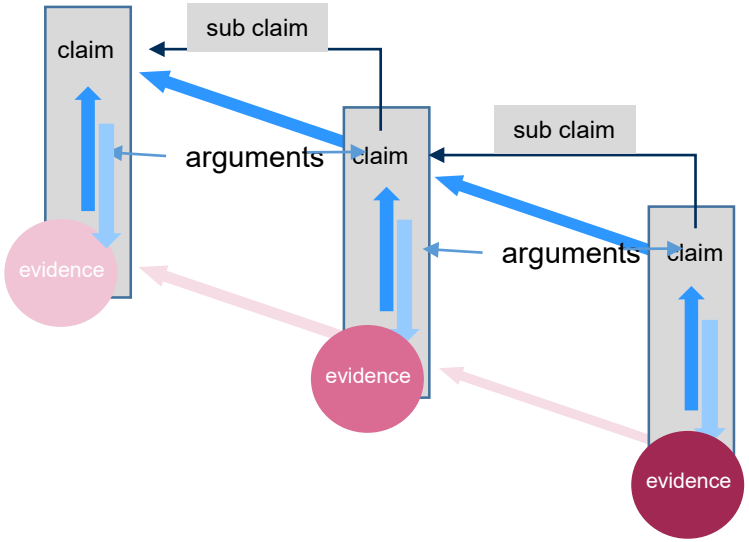
# SET Level - Processes Link to VVM

## (2) Credible Simulation / Modeling Process - Argumentation

- Assurance Argumentation consists of claims, strategies, argumentation and evidences.
- Evidences must be generated systematically according to the argumentation strategy.
- Simulation is a core-method for generation of evidences.
  - In return, the argumentation strategies provide the definition of the simulation output in terms of requirements including quality metrics.



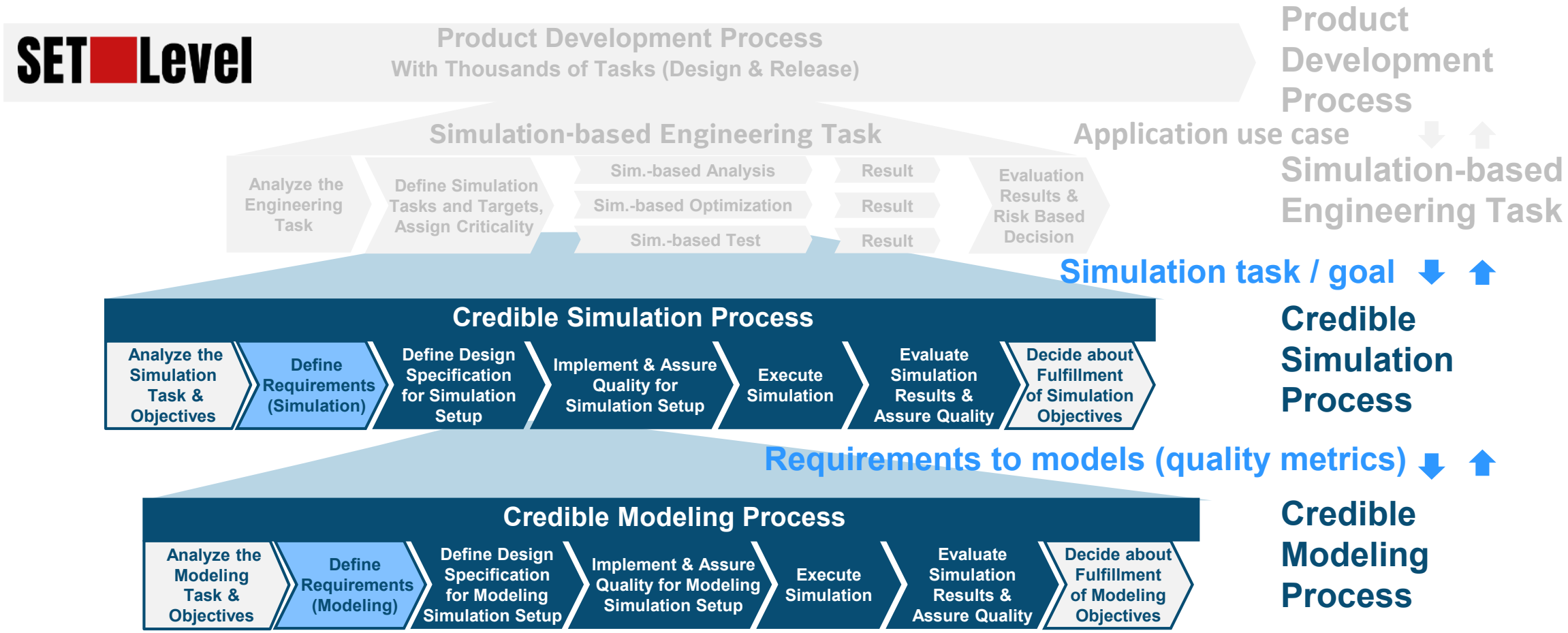




(Brade, 2021 with minor canges)

# SET Level - Processes Link to VVM

## (2) Credible Simulation / Modeling Process - Argumentation

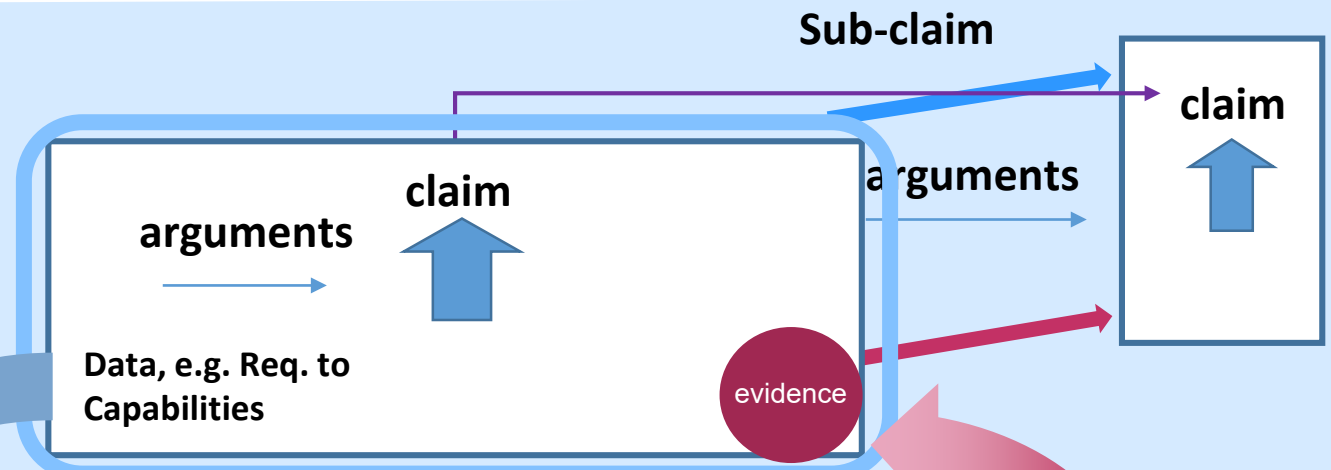
- How to assign the Credible Simulation / Modeling Process to the VVM safety argumentation?



# SET Level - Processes Link to VVM

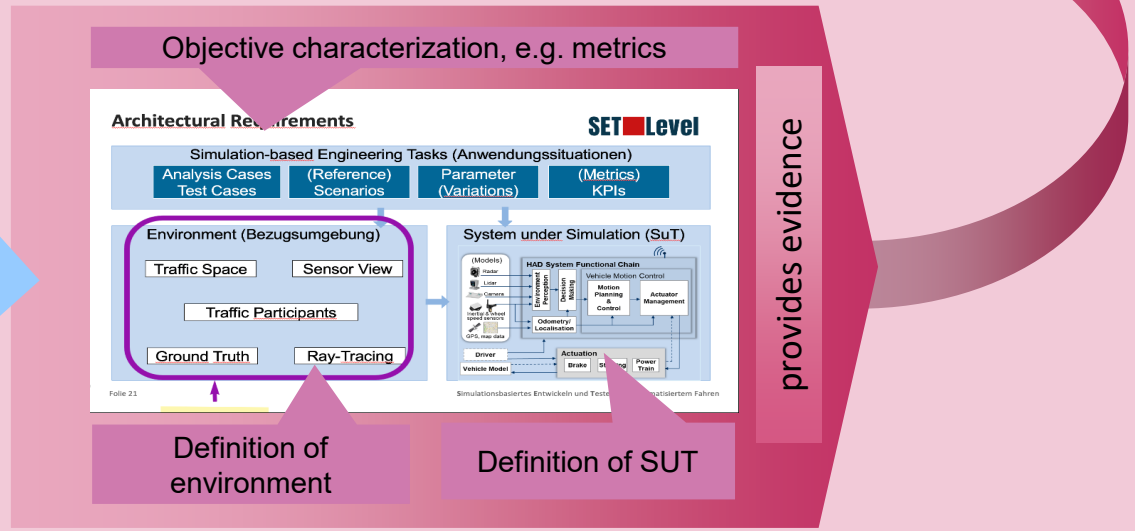
## (2) Process Link: Credible Simulation / Modeling Process

→ Based on VVM **argumentation structure**, the **simulation task / goal** of the Credible Simulation Process can be defined.



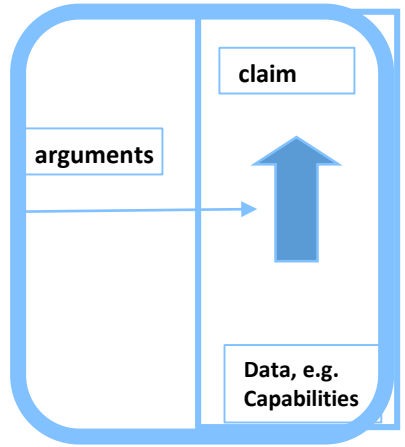

SET Level

→ Simulation objectives, environment and system under test can be derived by **claims**, **arguments** and **system data** as, thus requirements to models can also be derived.



# Example: Link SETLevel/VVM – Criticality Analysis

**Claim:** (contribution of the VVM Criticality Analysis to the Safety Argumentation)
We **identified** and **analyzed** the relevant factors influencing criticality in the operational domain (OD).



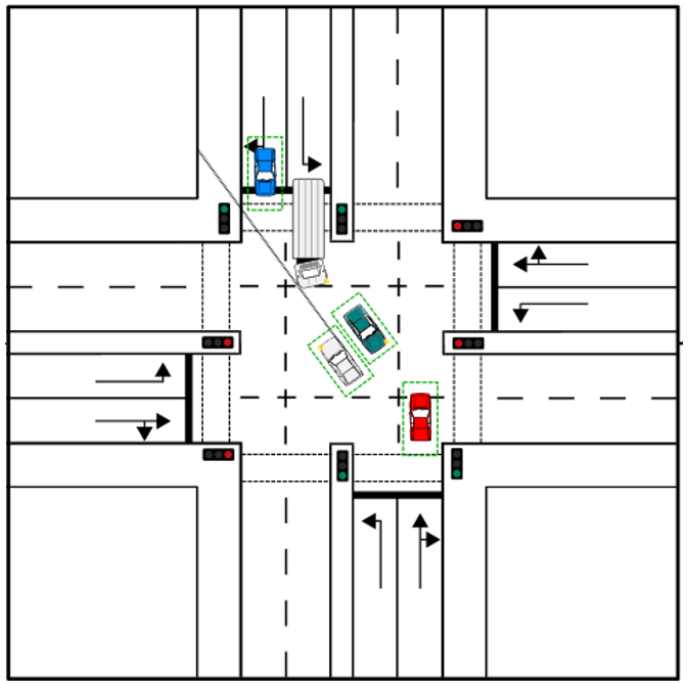

**Arguments:** (to substantiate the claim)
The „Criticality Analysis“ is methodically **sound** and the resulting **artifacts** are sufficiently **complete** and substantiated by **evidences**.

**Artifacts:** (resulting from the Criticality Analysis)

- criticality phenomena (associations with criticality)
- causal relations (plausible relations causing criticality)
- abstract scenarios (featuring phenomena and causal relations)

**Tools:** (employed for the Criticality Analysis)

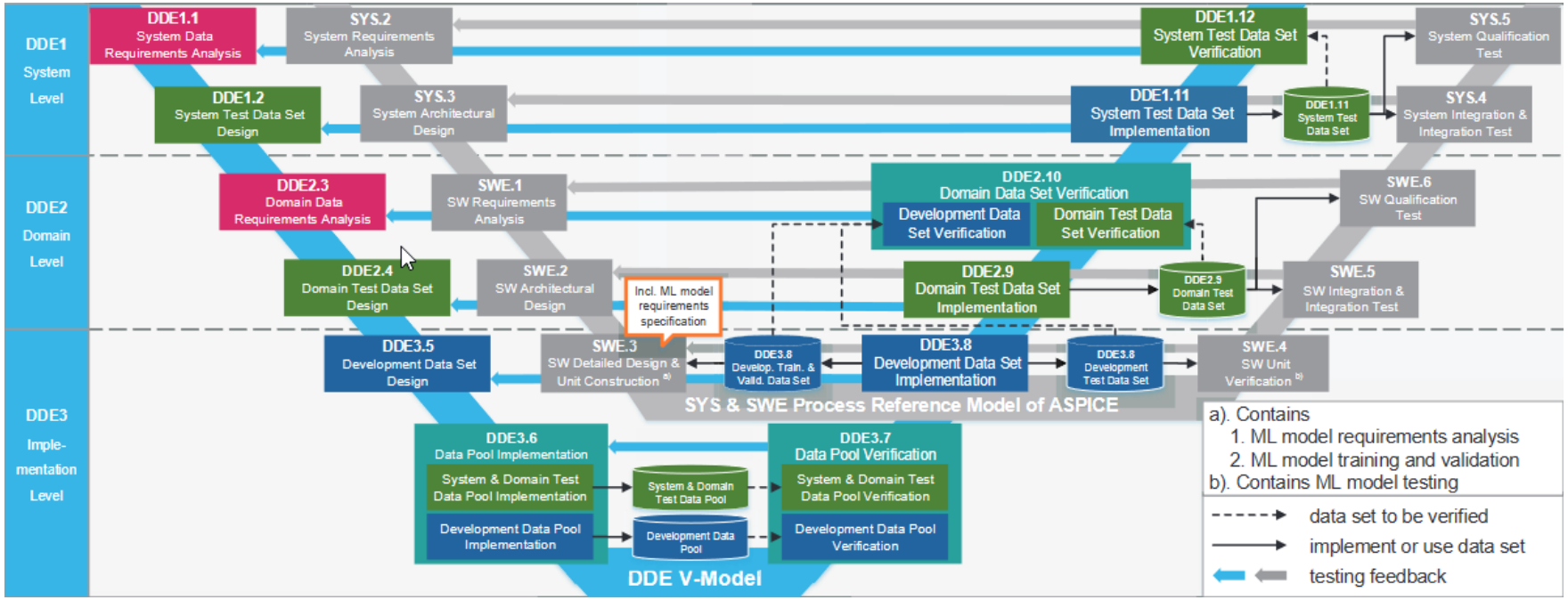
- metrics, ontologies, **simulation**
- acquisition & management of knowledge and data
- data analysis (real-world & synthetic)



# Data-Driven engineering process (DDE process)

VERIFICATION VALIDATION METHODS

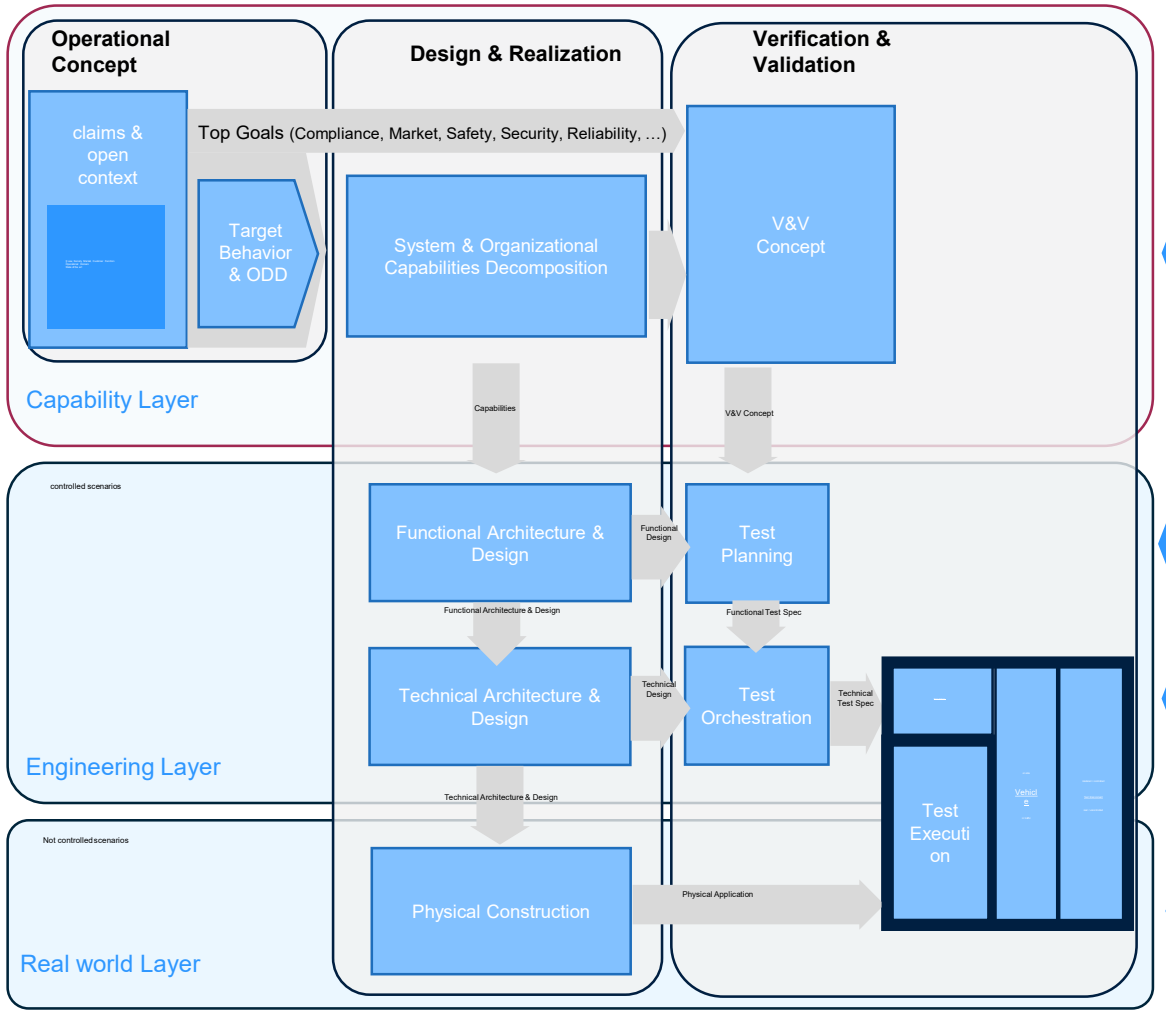
- DDE is a systematic and structured approach for leveraging future application of ML in industry.
- DDE is assigned towards ASPICE process architecture (Incl. hierarchical requirements engineering).




- DDE Approach Each system-level of the V-model has a specific demand for data, thus each system level generate its own requirements towards the characteristic of data.

# Link: ML-DDE Process vs VVM Assurance Framework

- DDE data concept could be transferred to VVM assurance framework via layer-models.
- The assurance argumentation provides the requirements for data at different levels.




**DDE0**

**Vehicle Level:** The vehicle level addresses the AD system functions on an abstract level and its ODD. There is no concrete technical solution or sensor set yet. Just the sensor principles are defined. So the focus is on the AD system's overall,…

**DDE1**

**System Level:** The system level deals with the AD system functions, or with the AD system's technical cause-effect chains or parts of them, respectively,...

**DDE2**

**Domain Level:** The domain level addresses a single element in a technical cause-effect chain regarding data aspects, e.g. a SW (sub-)system or a SW component sets,..

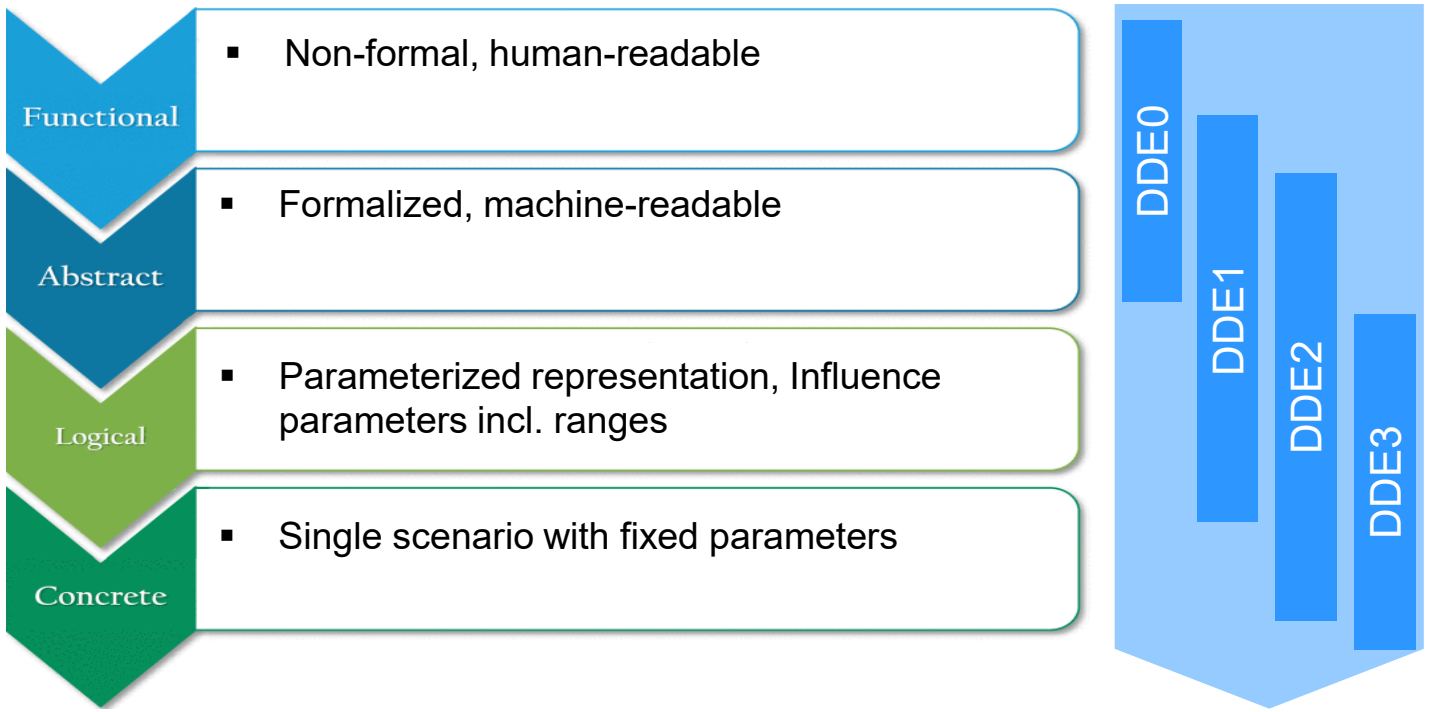
**DDE3**

**Implementation Level:** The implementation level DDE3 addresses the implementation of data sets,..

# Scenarios, DDE

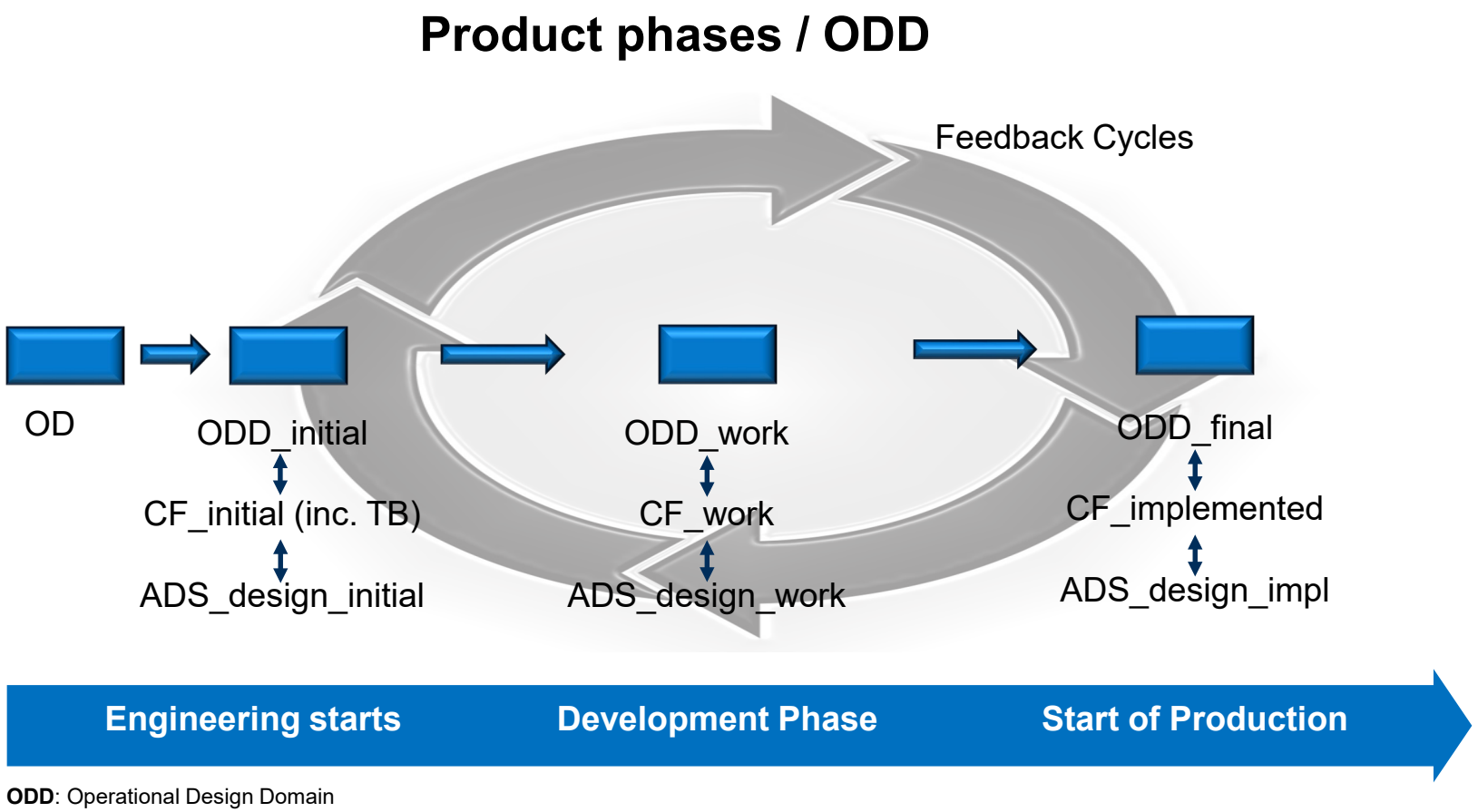
VERIFICATION
VALIDATION
METHODS

## Scenario Categories




- Scenarios are used to proof system performance e.g. to derive dependencies of sub-system characteristics towards the overall (safety) performance.
- Scenarios /data-categories should correspond in terms of abstraction.

# Scenarios, ODD, Target Behaviour and ADS-design



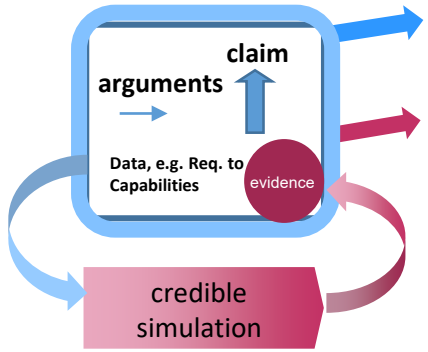

**ODD**: Operational Design Domain

- Scenarios are main element of the representation of a Target Behavior (TB) within an ODD*. Customer Function (CF) include the Target Behavior.
- ODD (incl. scenarios), the CF and the ADS-design iterate over product phases.

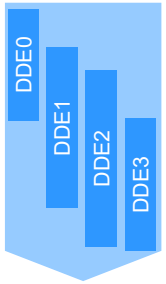
# Summary

VERIFICATION
VALIDATION
METHODS

- **Assurance framework and argumentation build the base for an efficient use of simulation**
  - **SETlevel example (1)** Application use cases correspond to the elements of Assurance Framework.
  - **SETlevel example (2)** Requirements and metrics for Credible Simulation can be derived by claims and its argumentation strategy.




- **Assurance framework build the base for defining the demand for data.**
  - **KIA example** Layer of the Assurance Framework and DDE data-categories correspond in terms of abstraction.




**The assurance framework supports simulation and data processes, so that exact fit evidences for the assurance argumentation can be provided.**

VERIFICATION
VALIDATION
METHODS

# Thank you!

Roland Galbas - Robert Bosch GmbH

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