VERIFICATION
VALIDATION
METHODS

# OSS.5 Berlin 9/21

## Integrating safety framework development and design
## Facing the challenge of responsibility for a product interacting within the open context


Roland Galbas, Thomas Kirschbaum, Thomas Göppel, Tino Brade,
Frank Junker (Robert Bosch GmbH), Thomas Corell, Björn Filzek
(Continental Teves AG & Co. oHG), Jan Reich (Fraunhofer-IESE),
Marcus Nolte (TUB - IfR)

Federal Ministry
for Economic Affairs
and Energy

PEGASUS
FAMILY

# Agenda

VERIFICATION
VALIDATION
METHODS

- V&V Methods Project
- Industrial Challenges of AD and VVM Approach
- Examples
- Take Away and Outlook

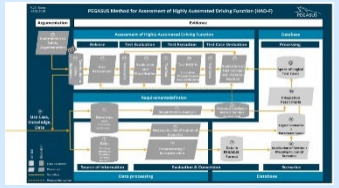
# VV-METHODS PEGASUS family – Publicly-funded projects in Germany

- 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



## *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*

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

\+ future projects of the PEGASUS Family

2016 2019 **Time**

# 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**


Federal Ministry for Economic Affairs and Energy

Thanks to Federal Ministry for Economic Affairs and Energy of Germany.

# VV-METHODS – Main goals

VERIFICATION
VALIDATION
METHODS

**Systematic control of test space**

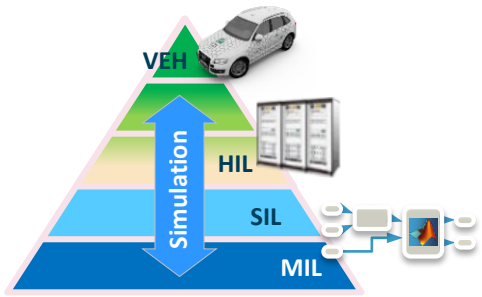
- Methods to optimize (and reduce) the test parameter space to a manageable minimum


**Consistent interfaces for assurance argumentation, systems and components across the supply chain**

- 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




**…and a coherent assurance argument linking the developed methods.**

# Agenda

VERIFICATION
VALIDATION
METHODS

- V&V Methods Project
- Industrial Challenges of AD and VVM Approach
- Examples
- Take Away and Outlook

# Challenges for a coherent assurance argument

How can we argue for the **absence of unreasonable risk** in an open context?

*…in a comprehensible manner for a variety of stakeholders?*

*… to further public trust in the technology?*

*…while not knowing what „reasonable“ really means?*

# Objective & Strategy

VERIFICATION VALIDATION METHODS

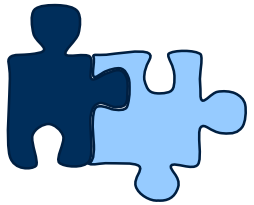
- **Objective**
  - Consider all relevant **societal claims** as laws/standards & **market proposition** in a **common process**.
  - Focus on **resilience** in **open context** over the complete **life cycle** (development & operation).

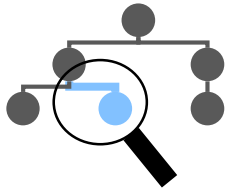
- **Strategy**

  - Use **different viewpoints** and **appropriate levels of abstraction**.

  - Combine **development & operation** with Design, Verification&Validation via an **assurance argumentation.**

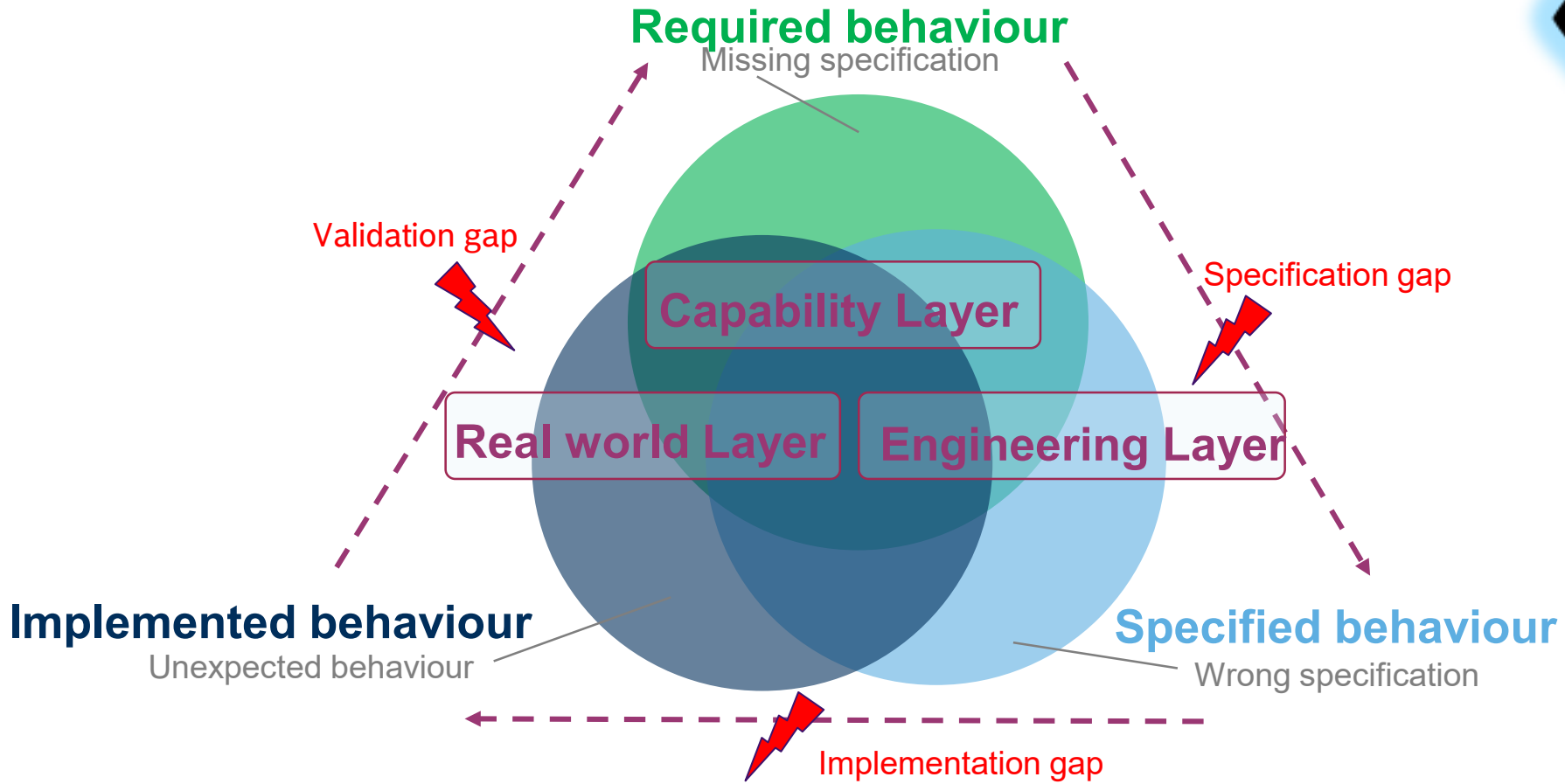
  - **An assurance argumentation** enable **consistency and traceability** over life cycle.





# Layer structure - viewpoint approach

- Use **different viewpoints** and appropriate levels of abstraction.

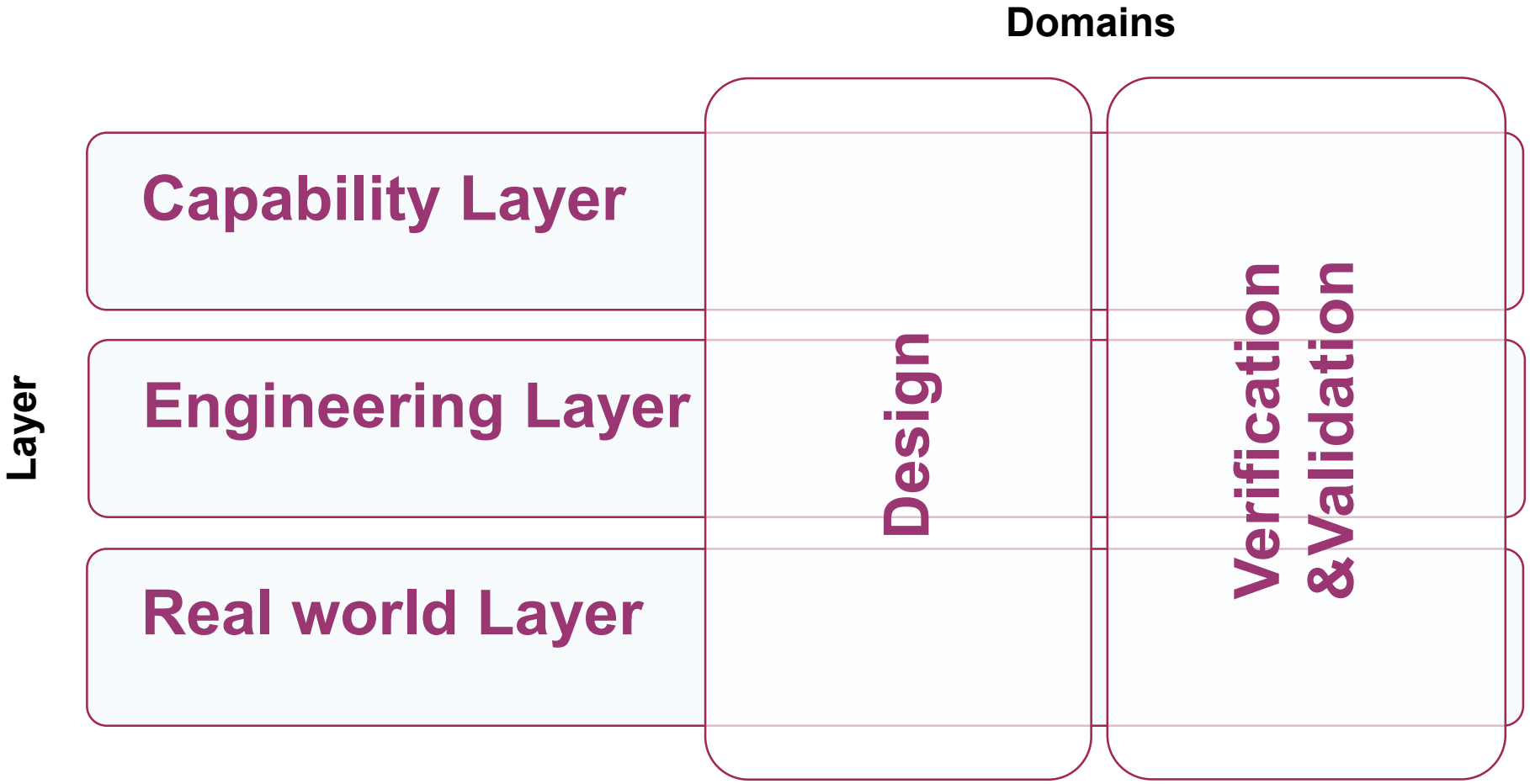



(Reich, 2021)

# Layer structure

VERIFICATION VALIDATION METHODS

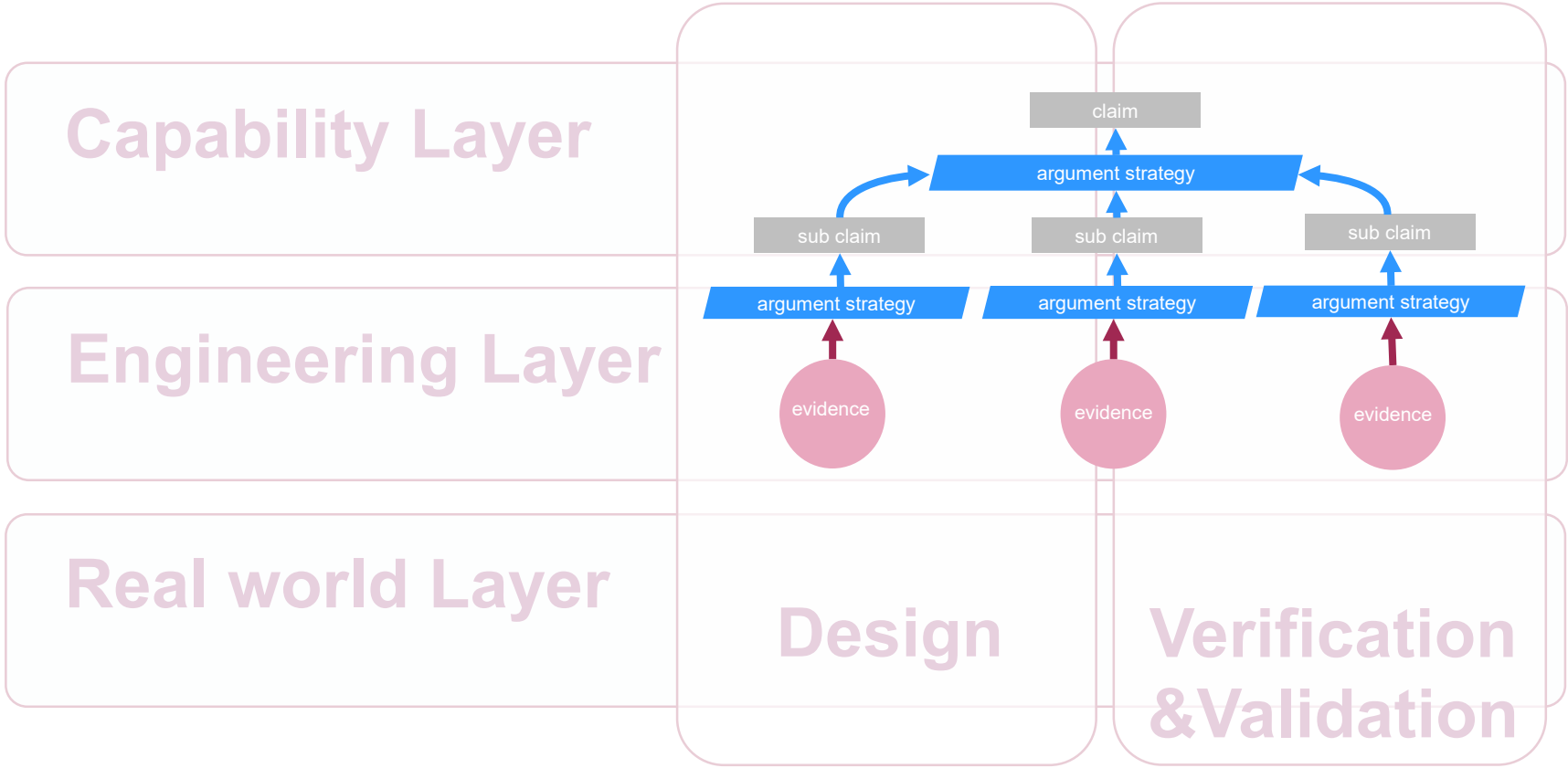
- Use different viewpoints and **appropriate levels of abstraction**.



# Layer structure & Assurance Argumentation

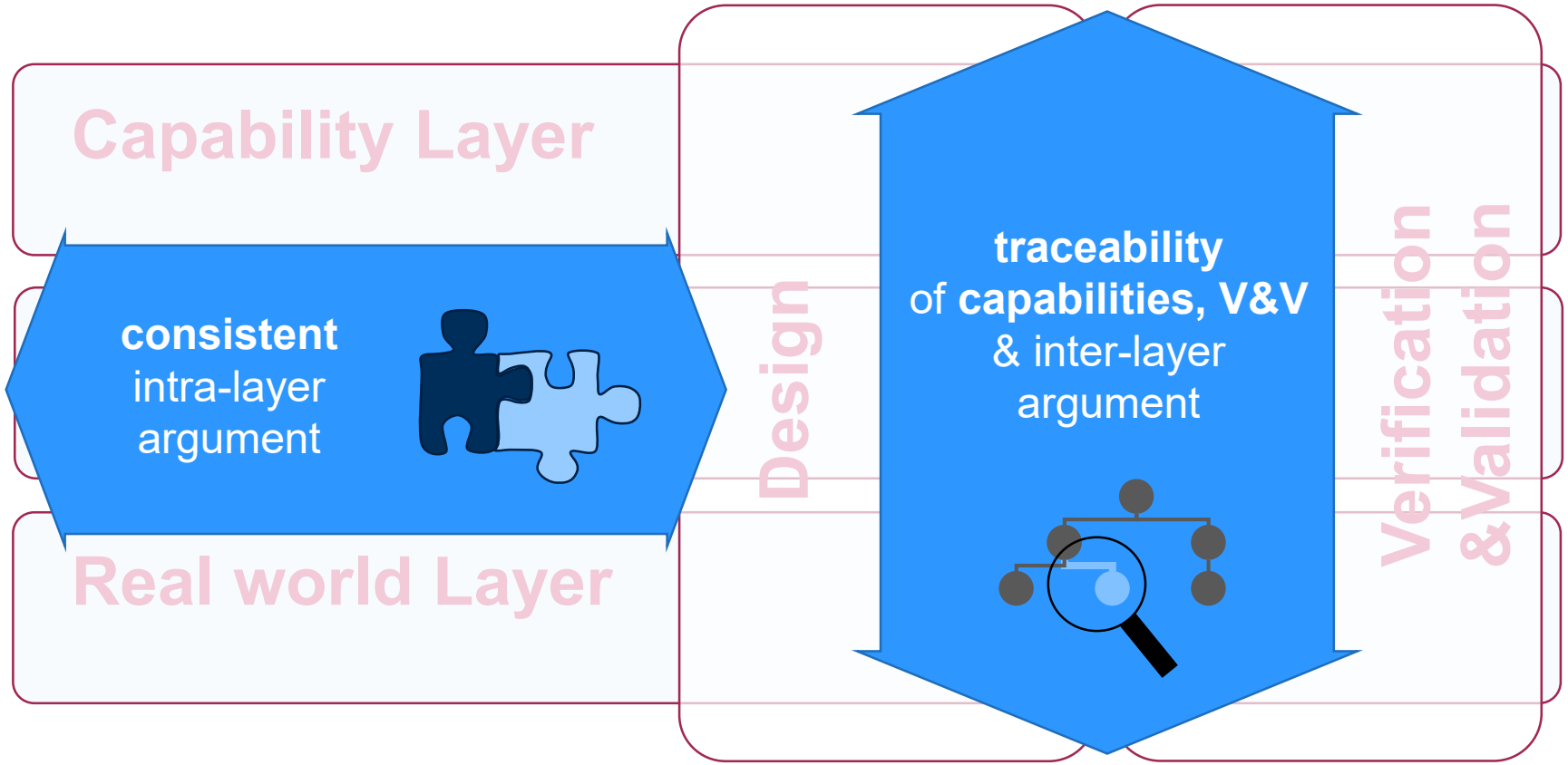
VERIFICATION VALIDATION METHODS

- Combine **development & operation** with Design, Verification&Validation via an **assurance argumentation.**




# Layer structure - principles

- **An assurance argumentation** enable **consistency and traceability** over life cycle.



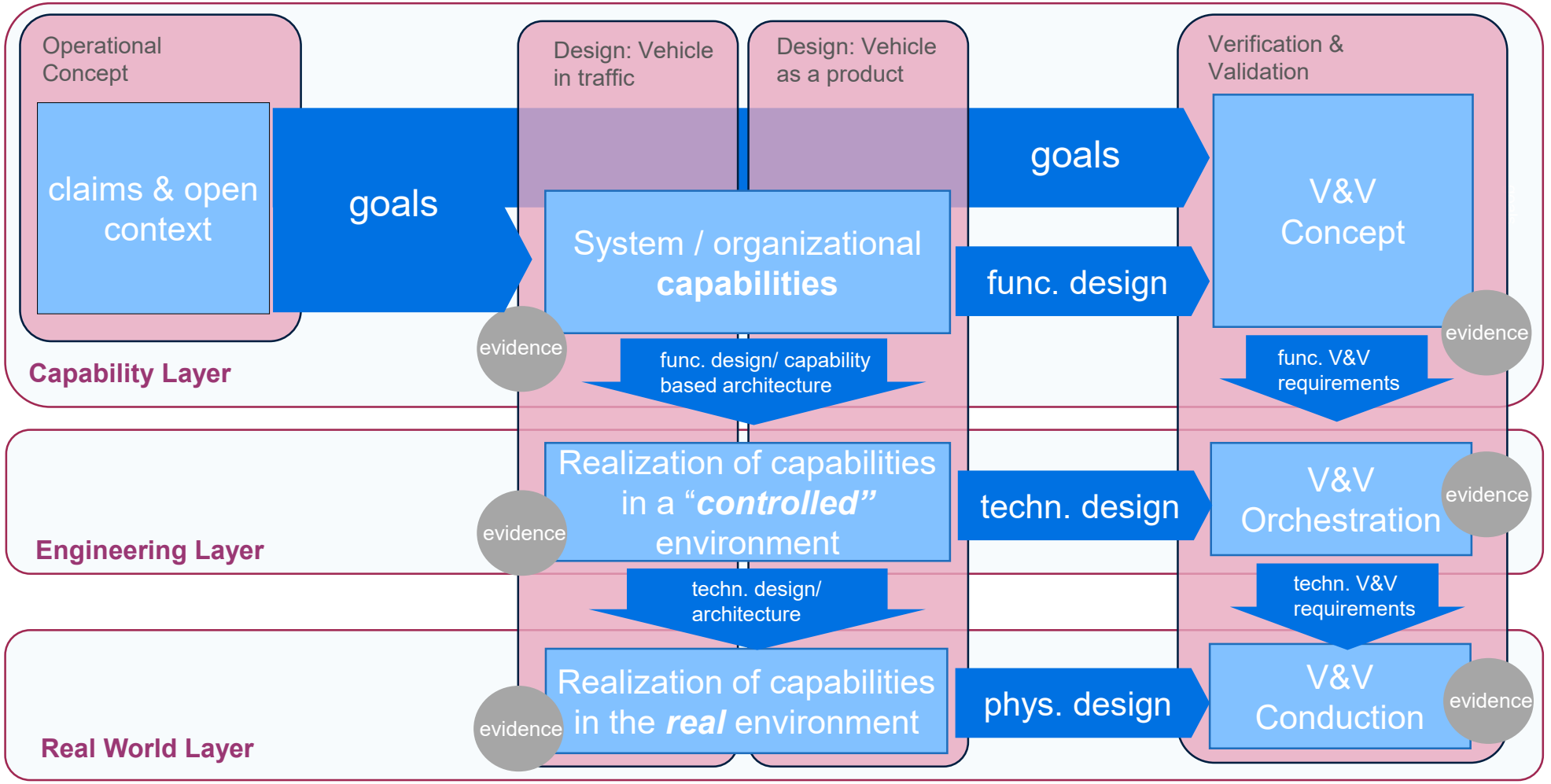

# Agenda

VERIFICATION
VALIDATION
METHODS

- V&V Methods Project
- Industrial Challenges of AD and VVM Approach
- Examples
- Take Away and Outlook

# Layer Structure - Elements

- Layers and domains interact.
- Iterative steps enable convergence of elements.

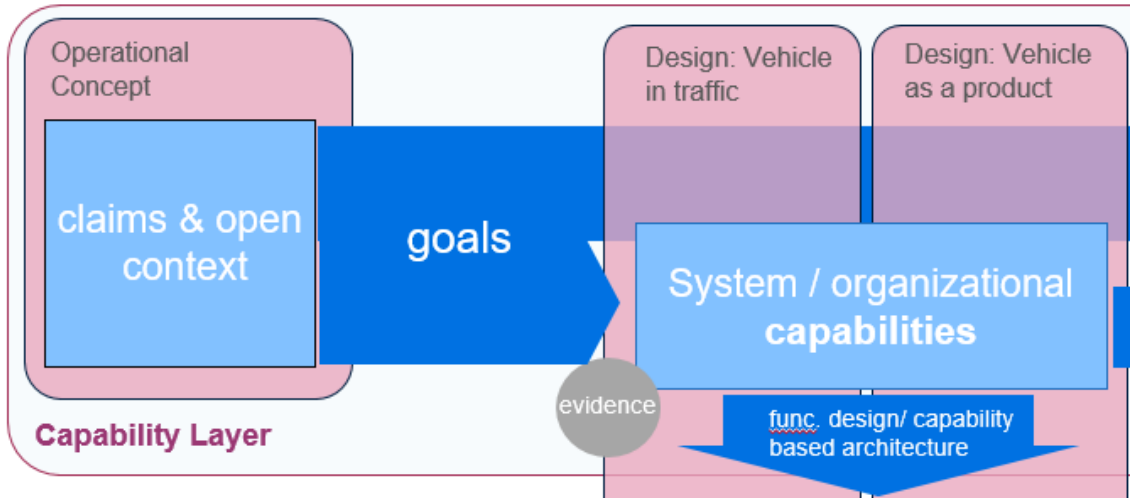


# Linking enterprise & vehicle capabilities

VERIFICATION VALIDATION METHODS

**bridging enterprise architecture & systems engineering**
by leveraging a duality between system & enterprise‘s capabilities

*Which capabilities does the vehicle need to safely operate in traffic?*
*Which capabilities does the enterprise need to monitor safe operation?*



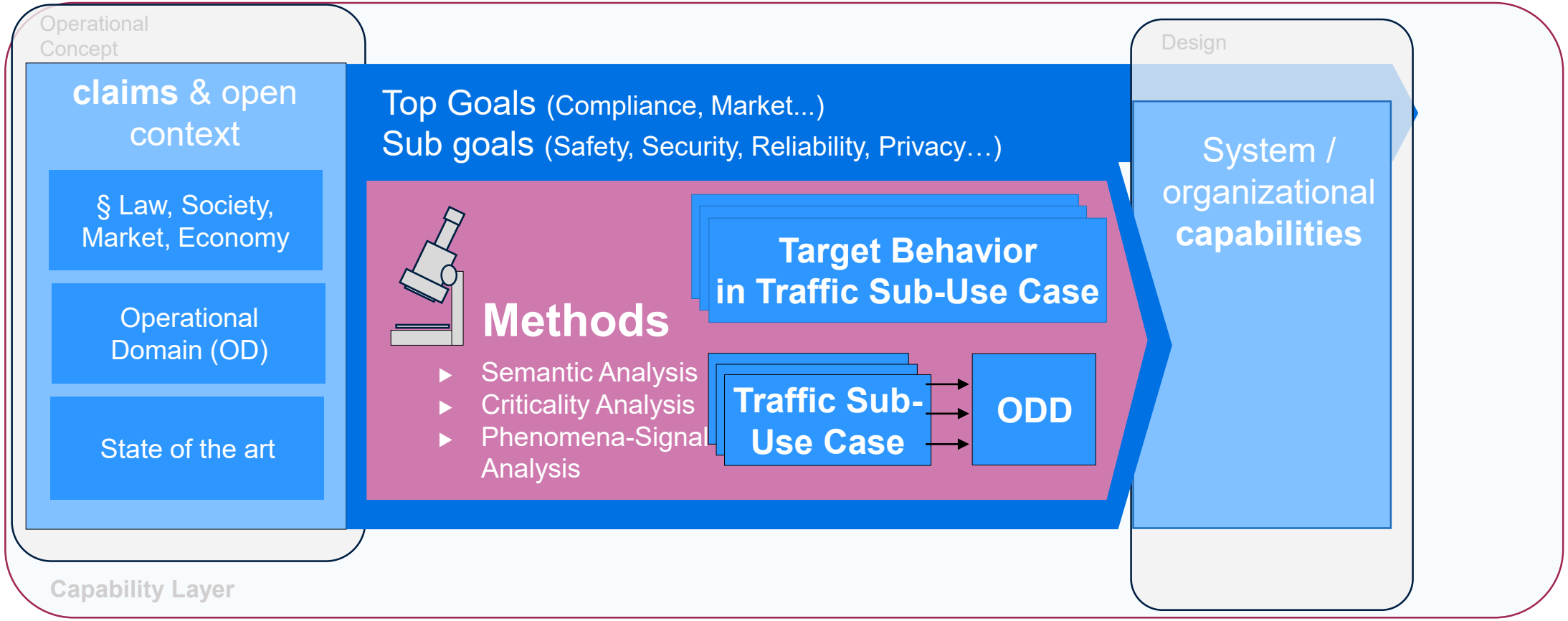

**„capability architecture“** is an established concept in many Enterprise Architecture Frameworks (DoDAF, MODAF, NAF, UAF,…)

*How can an OEM / mobility service provider safely design & operate a(n) (fleet of) automated vehicle(s)?*

# From claims to capabilities

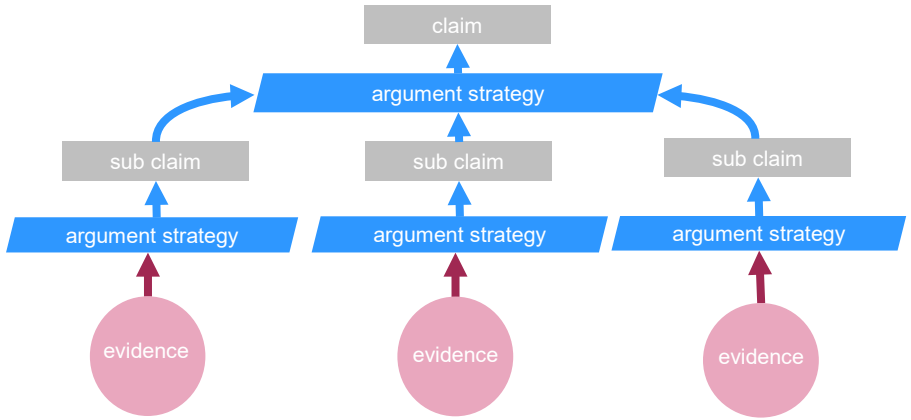
VERIFICATION VALIDATION METHODS

- Target Behavior / Sub use cases / ODD are steps to define capabilities.
- New methods for analysis have been developed.

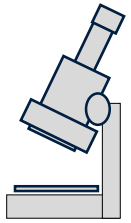


# Example: Assurance Argumentation - principles

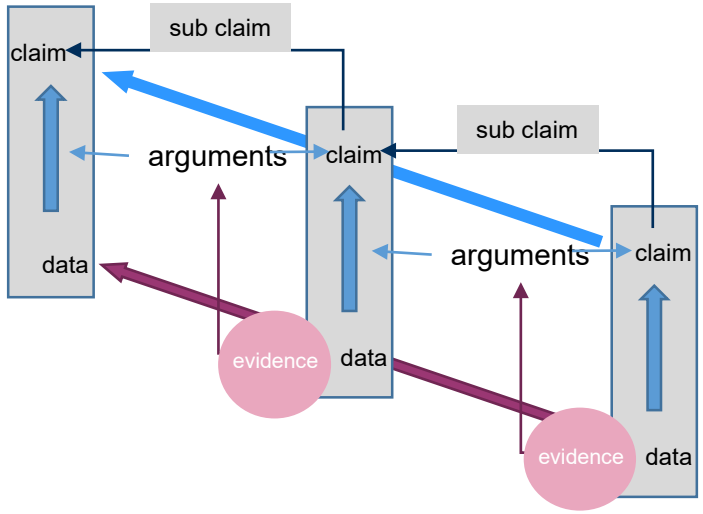
- Beside **methods for evidences** it is necessary to develop **methods for argumentation** strategies.




Methods for a structured decomposition of claims via arguments

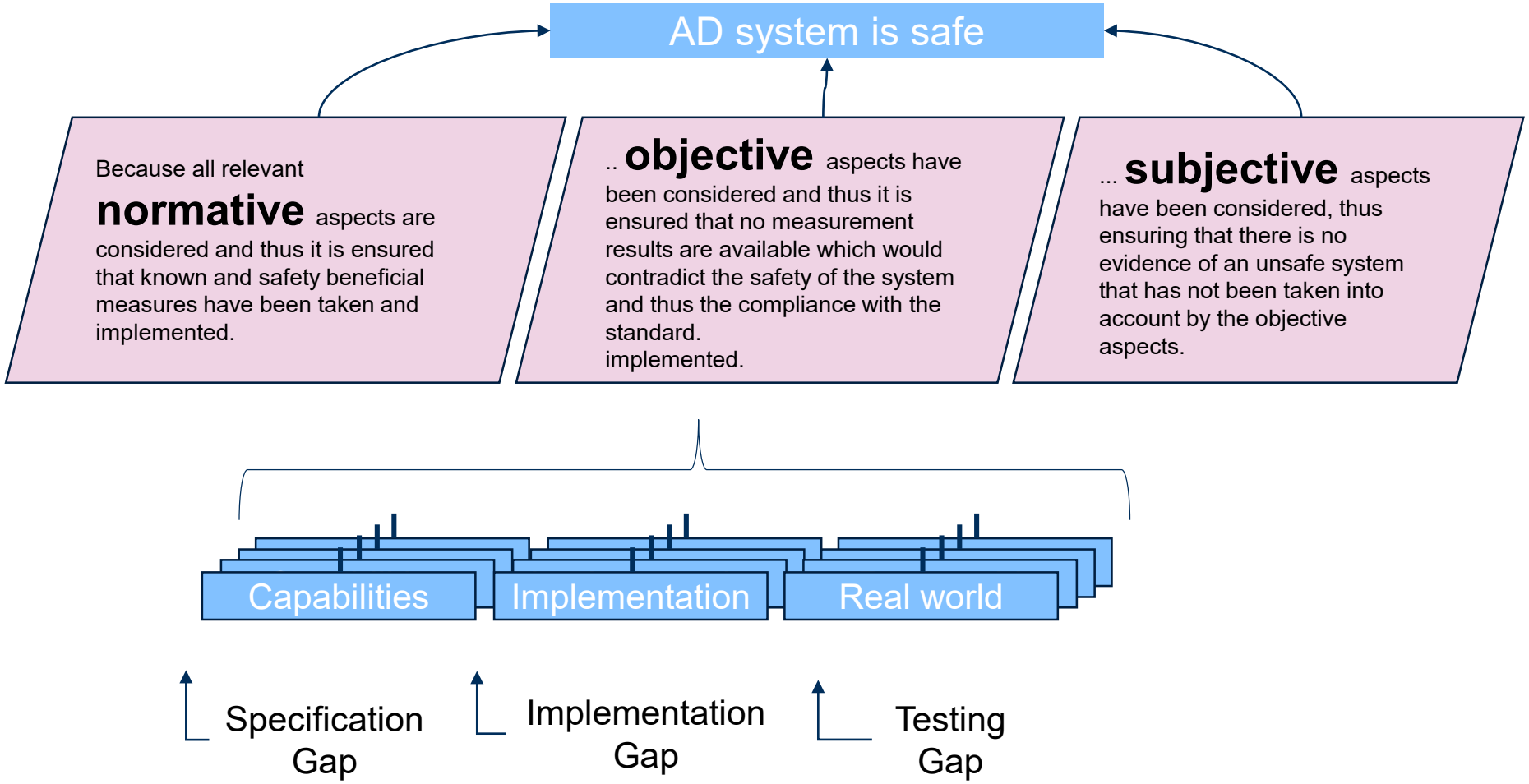


Methods for a structured generation of evidence to support arguments



# Assurance Argumentation - Approach

- Primary argumentation strategy: **normative, objective** and **subjective** .
- Argumentation structure is linked to layer structure and gap structure.



# Agenda

VERIFICATION
VALIDATION
METHODS

- V&V Methods Project
- Industrial Challenges of AD and VVM Approach
- Examples
- Take Away and Outlook

# Take Away / Outlook

VERIFICATION
VALIDATION
METHODS

- **Enabler**
  - **Layer structure** enables **iterative development** and thus convergence of results from different **perspectives**.
  - The **assurance argumentation** builds a backbone for **traceable decomposition** of claims. This enables efficient **post-release** when changes appear in the **open context**.
  - The abstract **capability-based architecture** combines **system and organization** to achieve a **consistent argumentation.**
  - Developed **methods** comply to **relevant industry standards.**

- **Next Steps**
  - Exemplary application of the methodical chain.
  - Further development of new methods and integration of existing methods.
  - Getting feedback and harmonization with existing approaches.

PEGASUS FAMILY

VERIFICATION
VALIDATION
METHODS

# Thank you for your attention!

# Time for questions.

Roland Galbas
Robert Bosch GmbH
roland.galbas@de.bosch.com

Federal Ministry
for Economic Affairs
and Energy