VERIFICATION
VALIDATION
METHODS

VVM - Towards a comprehensive framework for AD safety assurance

Roland Galbas - Robert Bosch GmbH

Safetronic 2021

Bild: Continental

Federal Ministry
for Economic Affairs
and Energy

PEGASUS
FAMILY

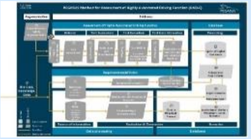
VV-METHODS PEGASUS family – Publicly-funded projects in Germany

- 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: L>=3 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

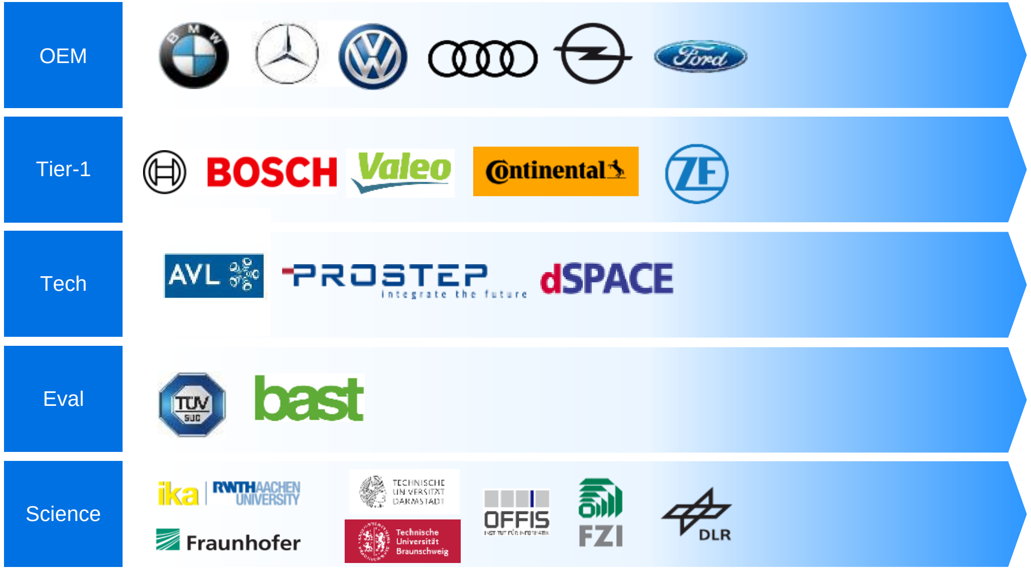
2016

2019

Time

VV-METHODS – Project setup

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



PEGASUS FAMILY

Federal Ministry
for Economic Affairs
and Energy

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

VV-METHODS – Main goals

Systematic control of test space

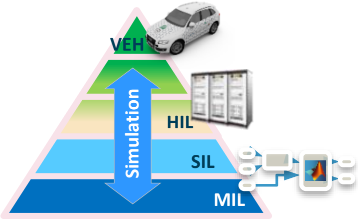
- Methods to map the infinitely-complex open context onto a finite & manageable set of artifacts

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.

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 foster public trust in the technology?

…while not knowing an exact interpretation of „reasonable“?

Approach

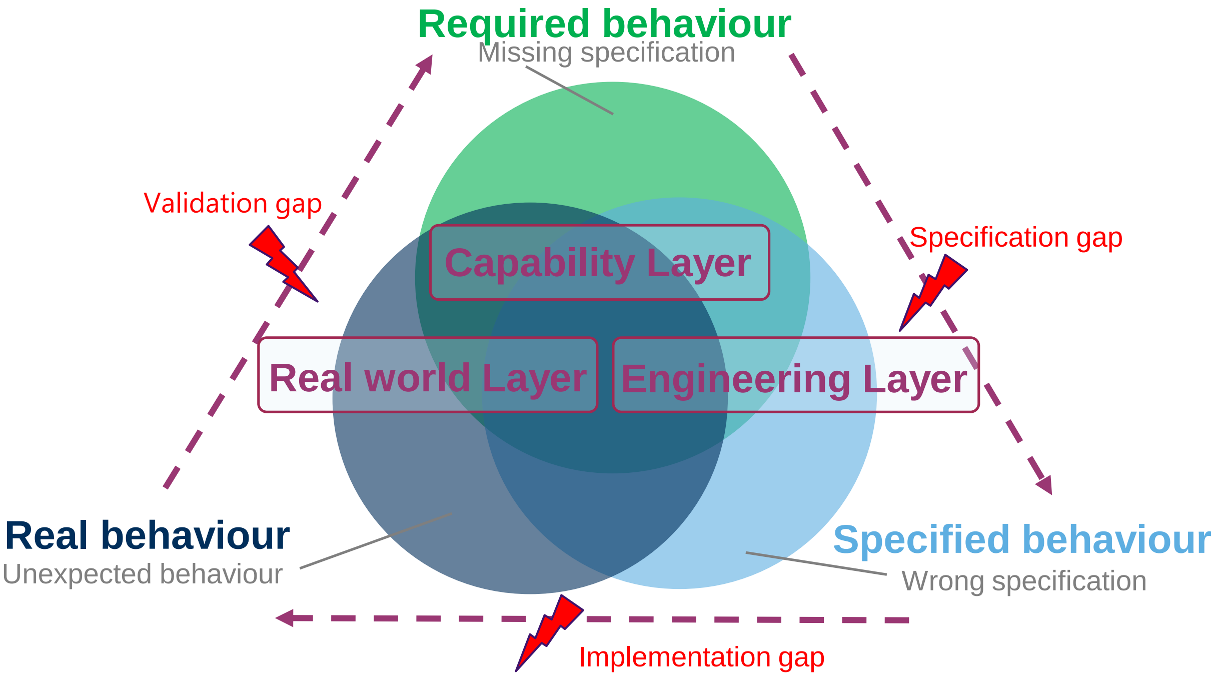
- **Objective – methodological framework – release**
  - Consider all relevant **societal claims** as laws/standards & **market proposition** in a **common process**.
  - Focus on **resilience** in **open context** over the complete **life cycle** (development & operation).

- **Strategy**
  - Use **different perspectives** and **appropriate levels of abstraction.**
  - Combine **development & operation** with Design, Verification&Validation via an **assurance argumentation.**
  - **An assurance argumentation** enable **consistency and traceability, prepared for changes** over life cycle.

Approach - Argumentation Framework - perspectives

- Use **<u>different perspectives</u>** and appropriate levels of abstraction.

perspectives

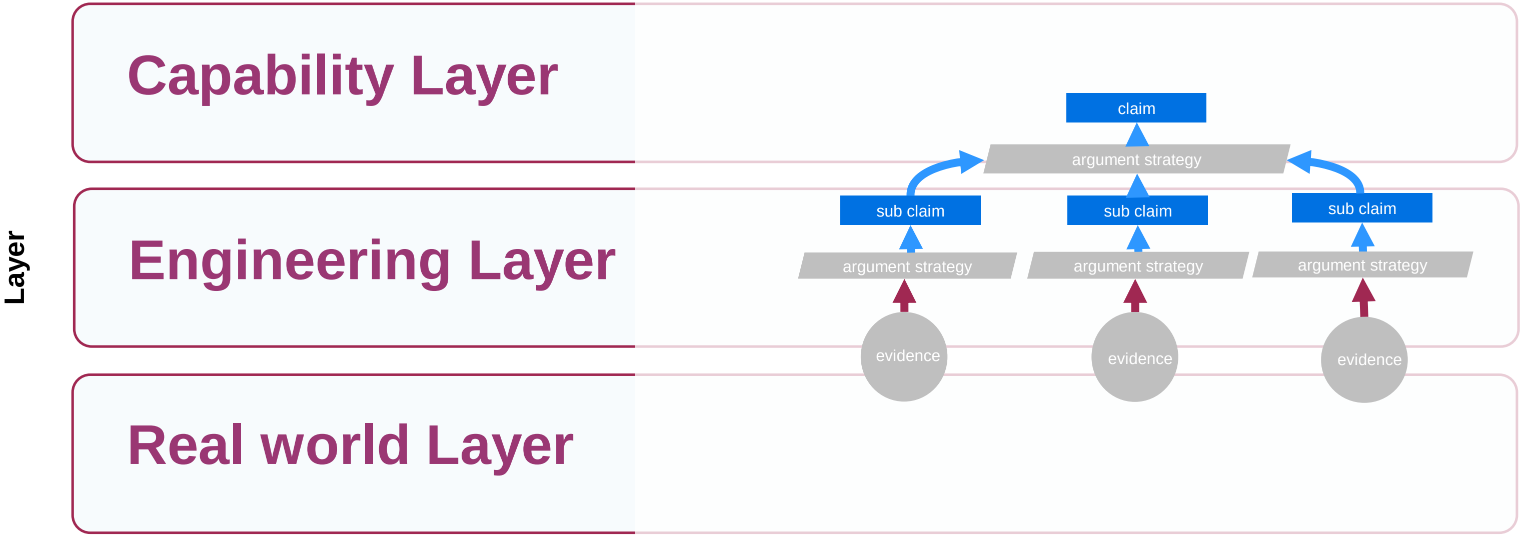


(J. E. Stellet, T. Brade, A. Poddey, S. Jesenski and W. Branz, "Formalisation and algorithmic approach to the automated driving validation problem," *2019 IEEE Intelligent* - with minor changes)

Approach - Argumentation Framework

- Use different perspectives and **appropriate levels (layers) of abstraction** in order to support the **safety argumentation**

perspectives



Layer

Capability Layer

Engineering Layer

Real world Layer

claim

argument strategy

sub claim

sub claim

sub claim

argument strategy

argument strategy

argument strategy

evidence

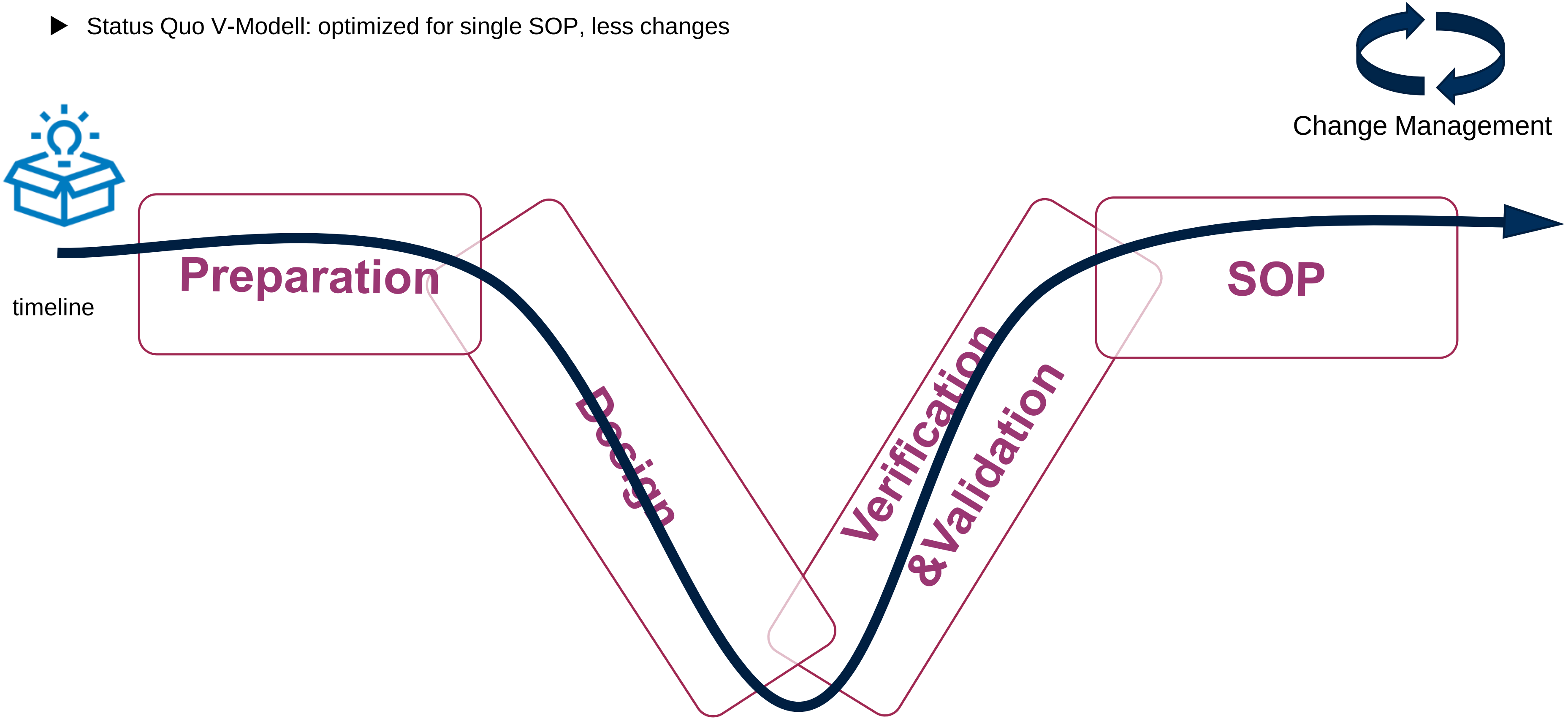
evidence

evidence

Safety argumentation

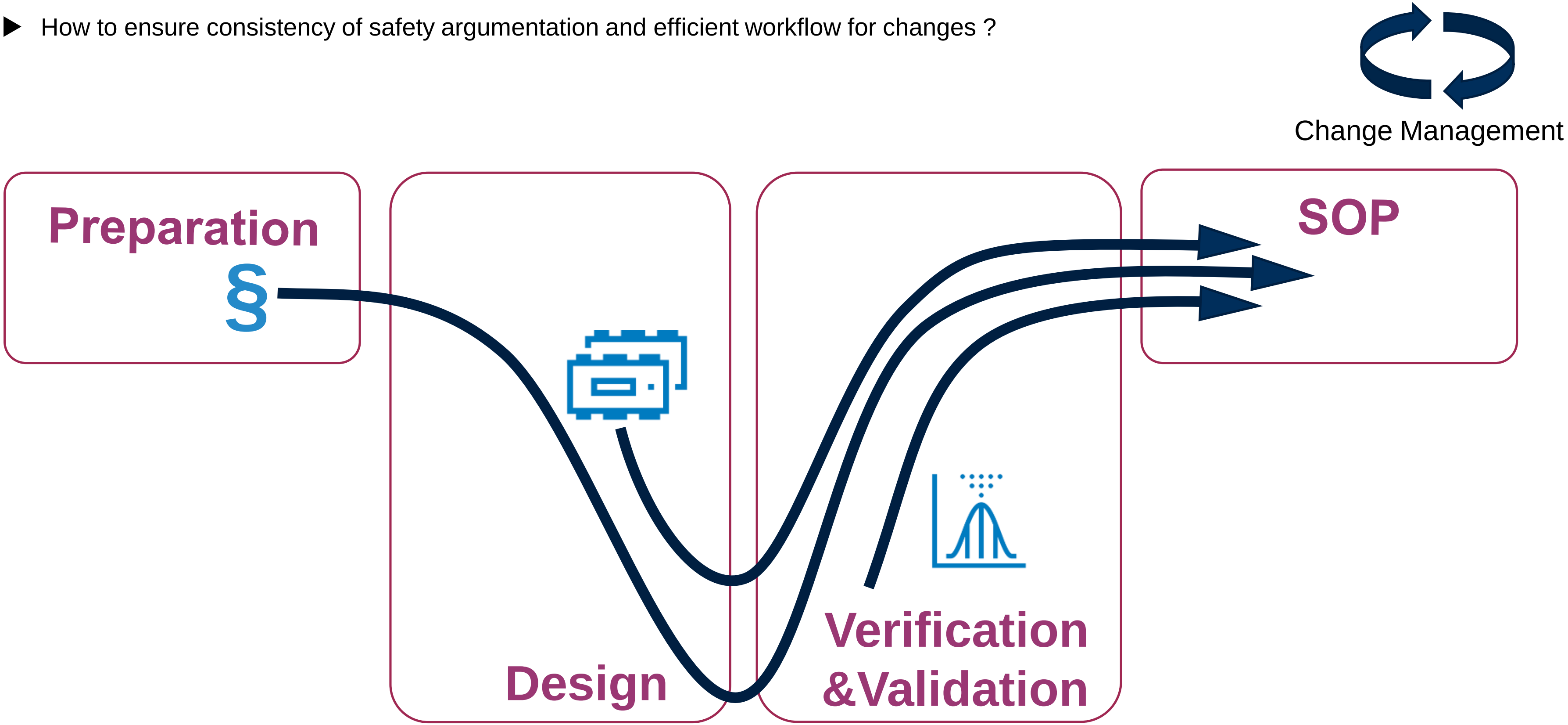
Derive of Approach – V-Model and Open Context

- Status Quo V-Modell: optimized for single SOP, less changes



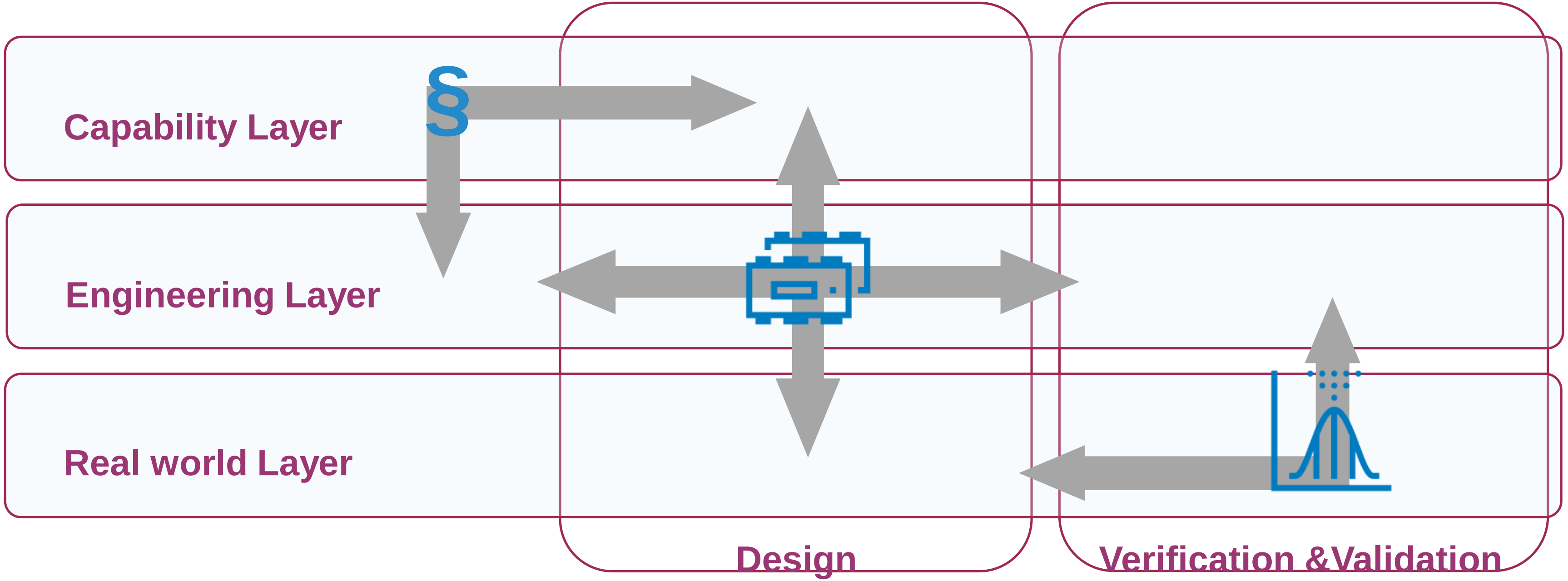
Derive of Approach – Changes from open context

- How to ensure consistency of safety argumentation and efficient workflow for changes ?



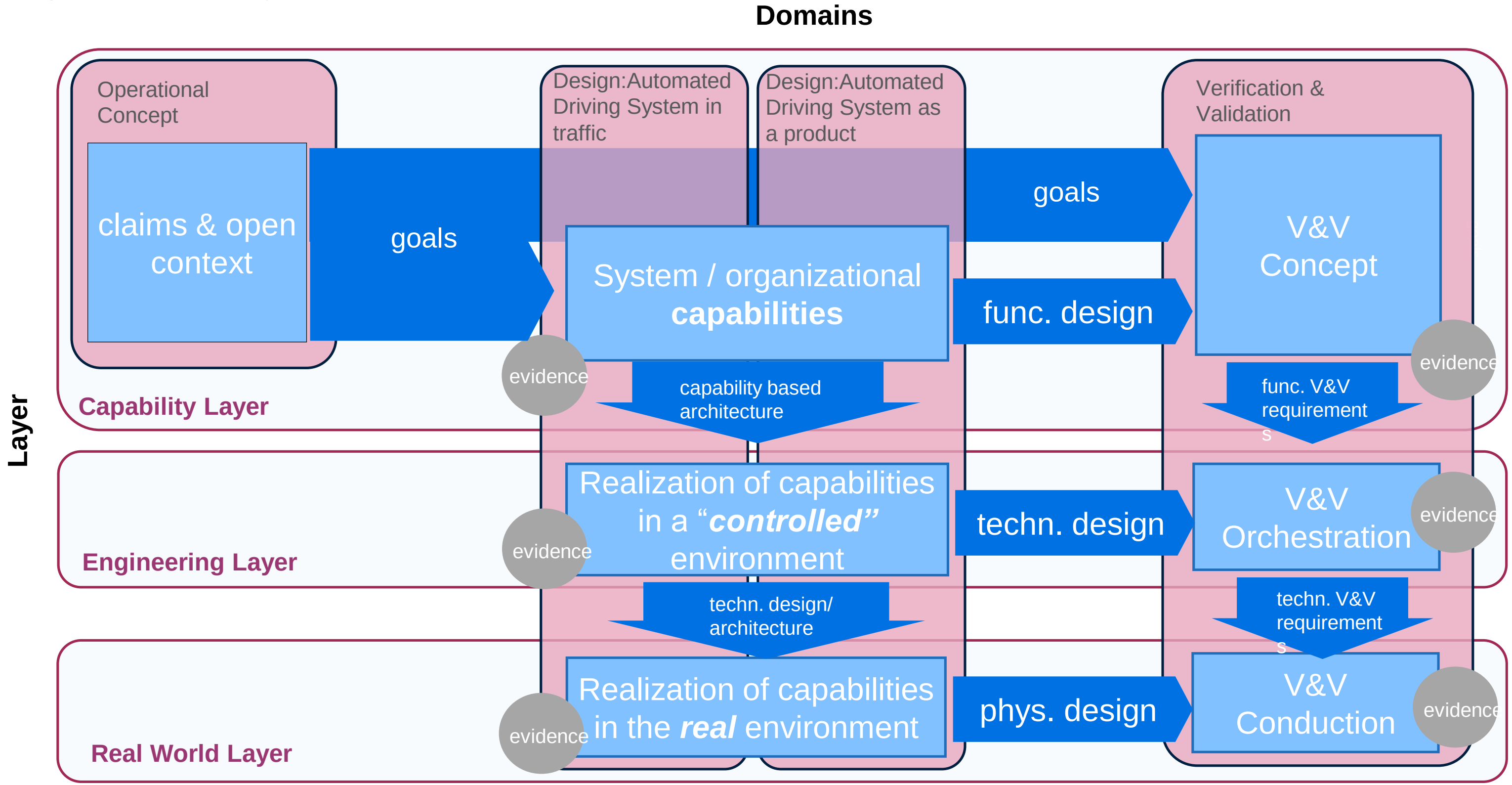
Derive of Approach – Changes from open context

- Harmonized interfaces will support both:
  - Efficient workflow for changes in development and operation
  - Consistency of Safety argumentation



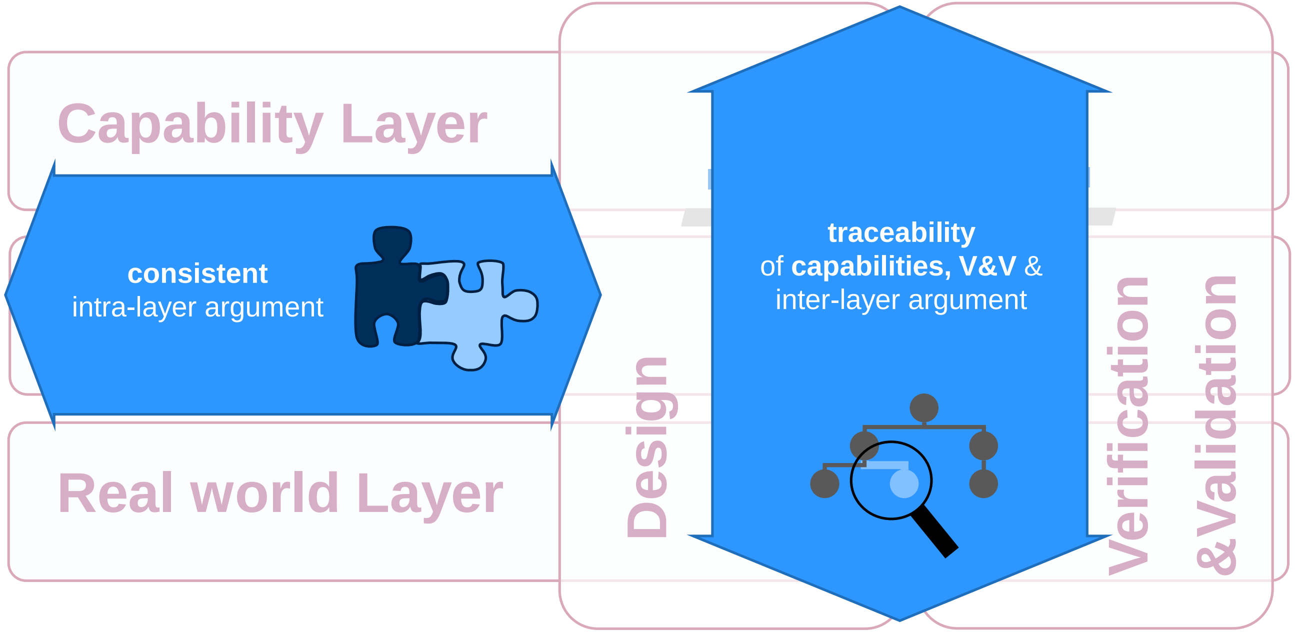
Argumentation Framework - Elements

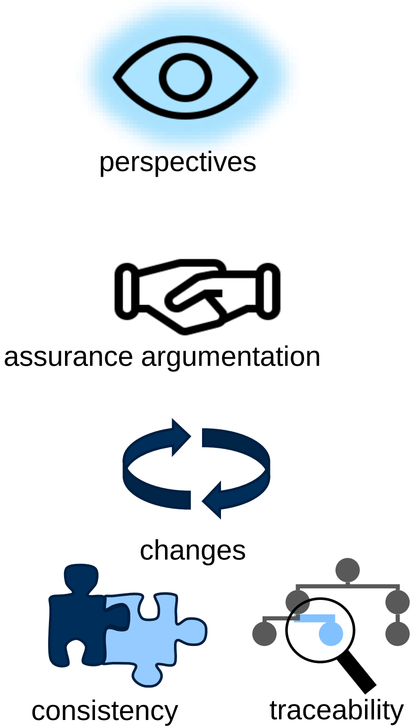
- Layers and domains interact over harmonized interfaces.
- Iterative steps enable convergence of elements.


Domains
Layer
Operational Concept
claims & open context
goals
Design:Automated Driving System in traffic
Design:Automated Driving System as a product
goals
Verification & Validation
V&V Concept
System / organizational **capabilities**
func. design
evidence
evidence
capability based architecture
func. V&V requirements
Capability Layer
Realization of capabilities in a "***controlled***" environment
techn. design
V&V Orchestration
evidence
evidence
Engineering Layer
techn. design/ architecture
techn. V&V requirements
Realization of capabilities in the ***real*** environment
phys. design
V&V Conduction
evidence
evidence
Real World Layer

Argumentation Framework

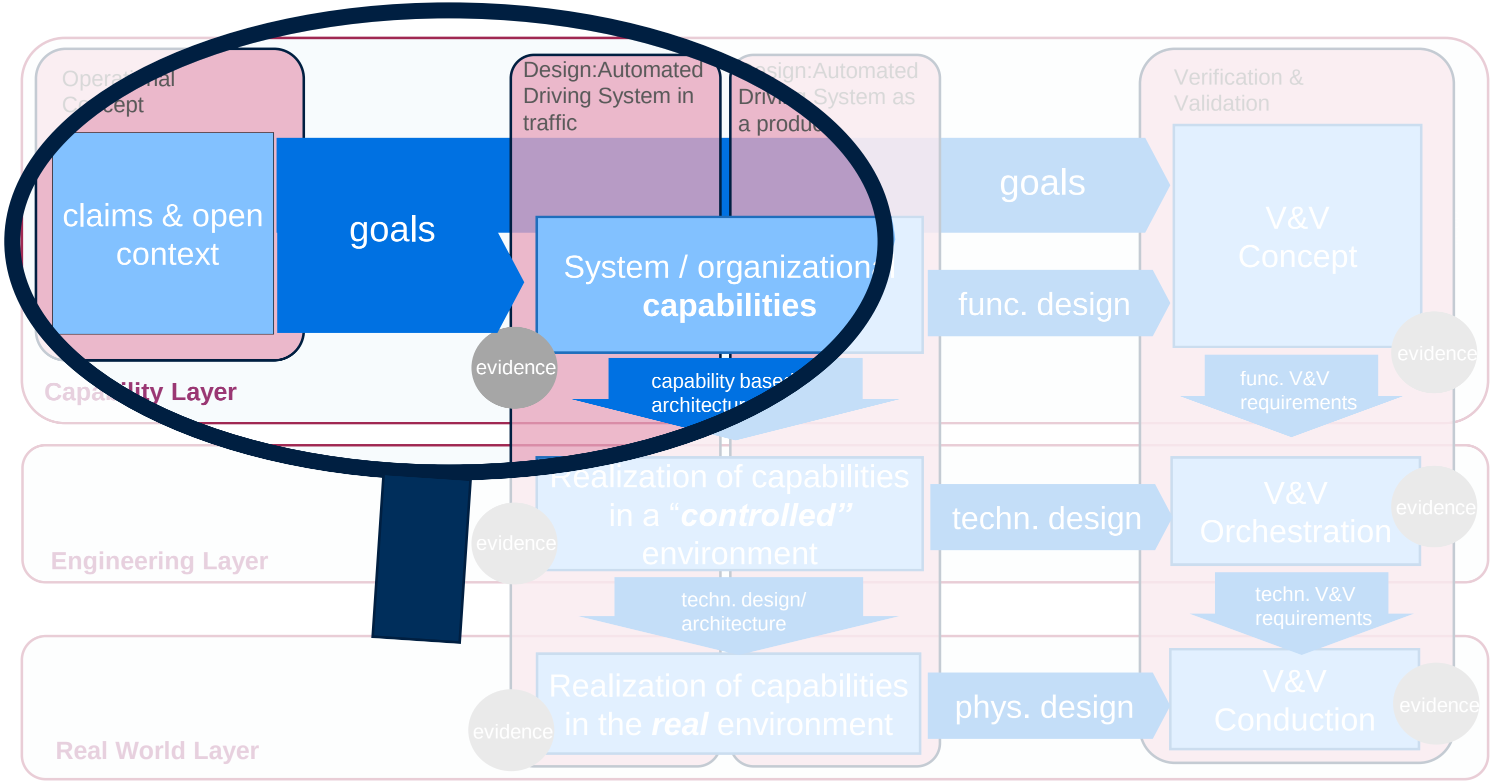
- Use different perspectives and **appropriate levels (layers) of abstraction.**
- Combine **development & operation** with Design, Verification & Validation via an **assurance argumentation.**
- Assign process interfaces **prepared for changes**





Argumentation Framework - Elements

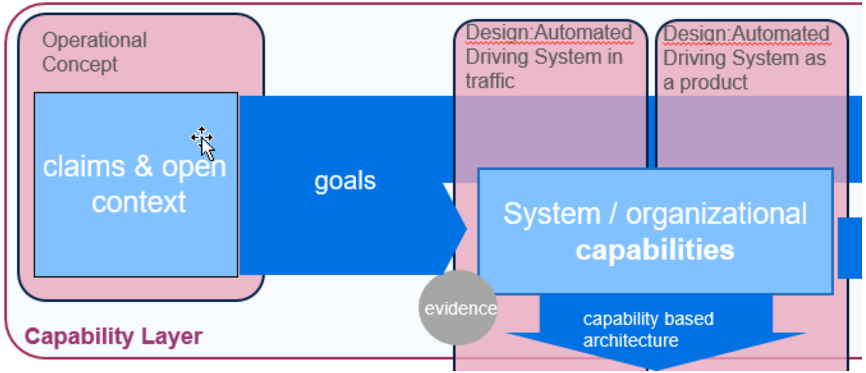
- Layers and domains interact.
- Iterative steps enable convergence of elements.


Operational Concept
claims & open context
goals
Design:Automated Driving System in traffic
Design:Automated Driving System as a product
System / organizational capabilities
evidence
capability based architecture
Capability Layer
goals
func. design
Verification & Validation
V&V Concept
evidence
func. V&V requirements
Realization of capabilities in a "controlled" environment
evidence
Engineering Layer
techn. design
V&V Orchestration
evidence
techn. design/ architecture
techn. V&V requirements
Realization of capabilities in the real environment
evidence
Real World Layer
phys. design
V&V Conduction
evidence

Linking enterprise & vehicle capabilities

bridging enterprise architecture & systems engineering
by leveraging the interaction 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?



Operational Concept
claims & open context
goals
Design:Automated Driving System in traffic
Design:Automated Driving System as a product
System / organizational capabilities
evidence
capability based architecture
Capability Layer

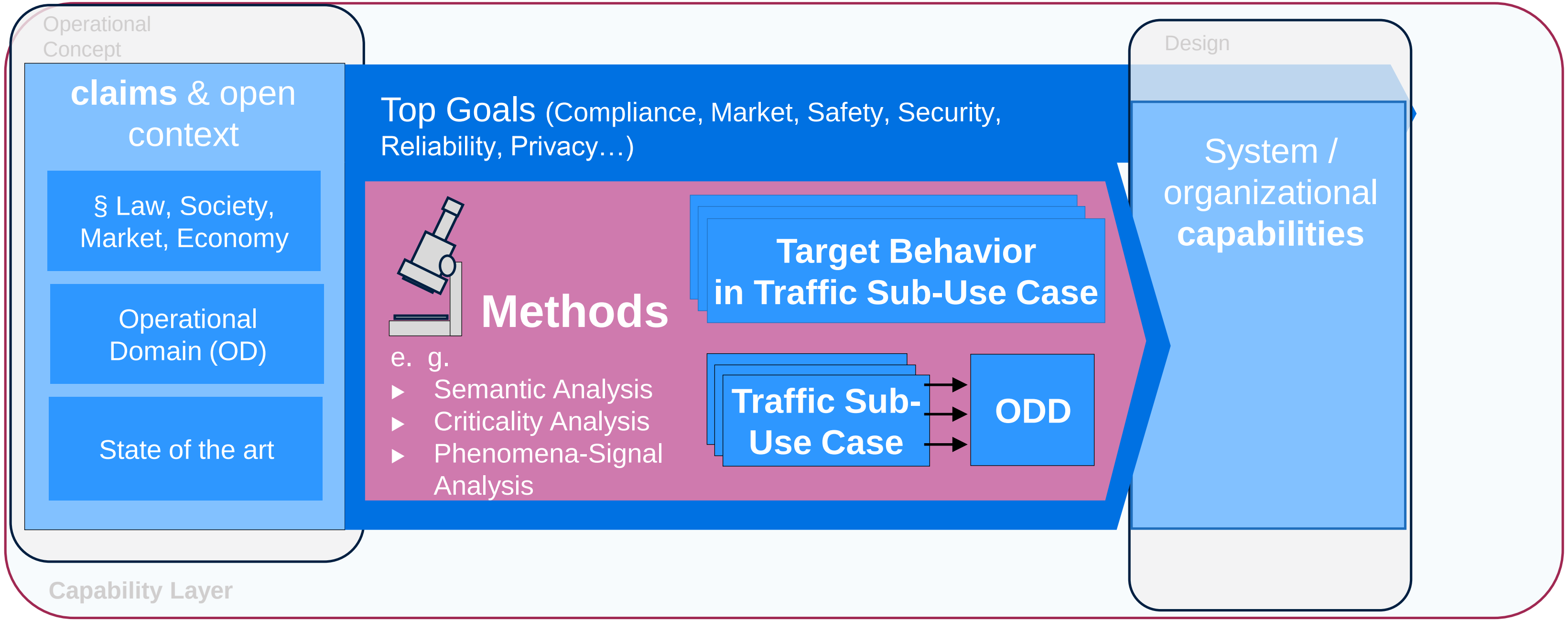
„capability architecture“ is an established concept grown in many Enterprise Architecture Frameworks (DoDAF, MODAF, NAF, UAF,…)

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

From claims to capabilities

VERIFICATION
VALIDATION
METHODS

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

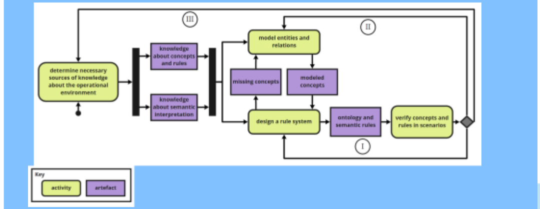


Operational Concept
claims & open context
§ Law, Society, Market, Economy
Operational Domain (OD)
State of the art
Top Goals (Compliance, Market, Safety, Security, Reliability, Privacy…)
Methods
e. g.
▸ Semantic Analysis
▸ Criticality Analysis
▸ Phenomena-Signal Analysis
Target Behavior in Traffic Sub-Use Case
Traffic Sub-Use Case
ODD
Design
System / organizational capabilities
Capability Layer

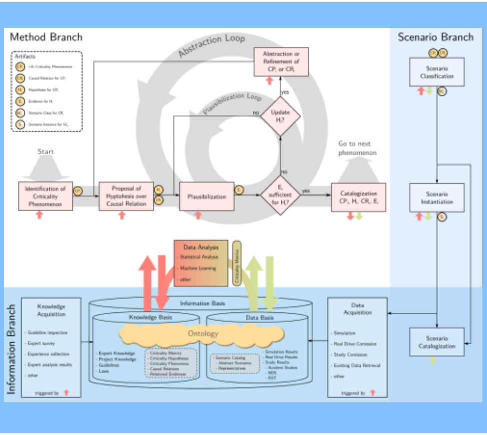
From claims to capabilities

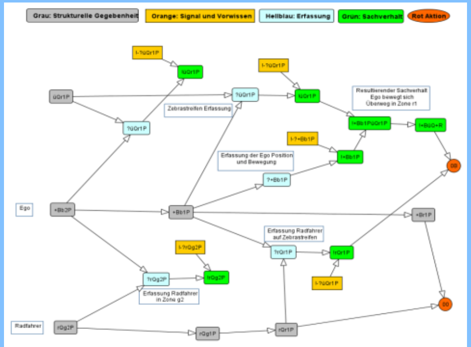
VERIFICATION
VALIDATION
METHODS

- Exemplary Analysis Methods



III
II
I
determine necessary sources of knowledge about the operational environment
knowledge about concepts and rules
knowledge about semantic interpretation
model entities and relations
missing concepts
modeled concepts
design a rule system
ontology and semantic rules
verify concepts and rules in scenarios
Key
activity
artefact





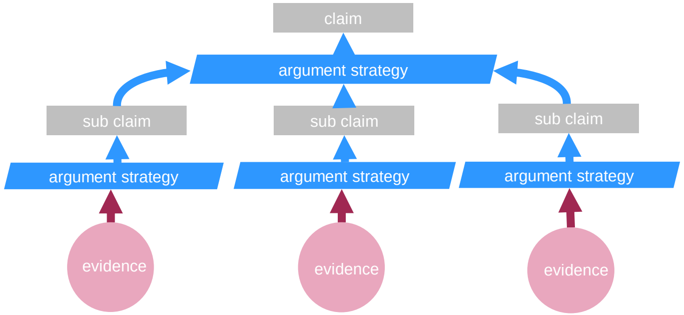
- **Semantic Analysis**
understand the perspective of law concerning scenarios and their ontology.

- **Criticality Analysis**
Identification and causal analysis of traffic phenomena associated with criticality.

- **Phenomena-Signal Analysis**
understand and assess the interexchange of traffic by decisions, sequences, law and traffic-phenomena based on the information flow.

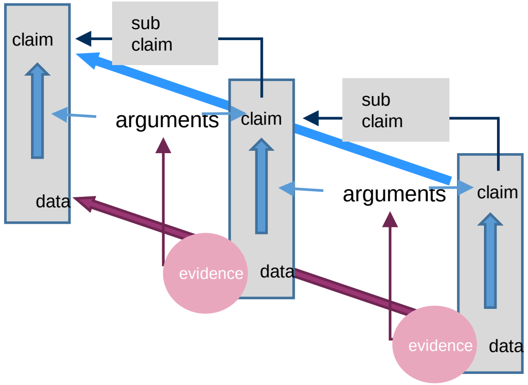
Example: Assurance Argumentation - principles

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



argumentation strategies

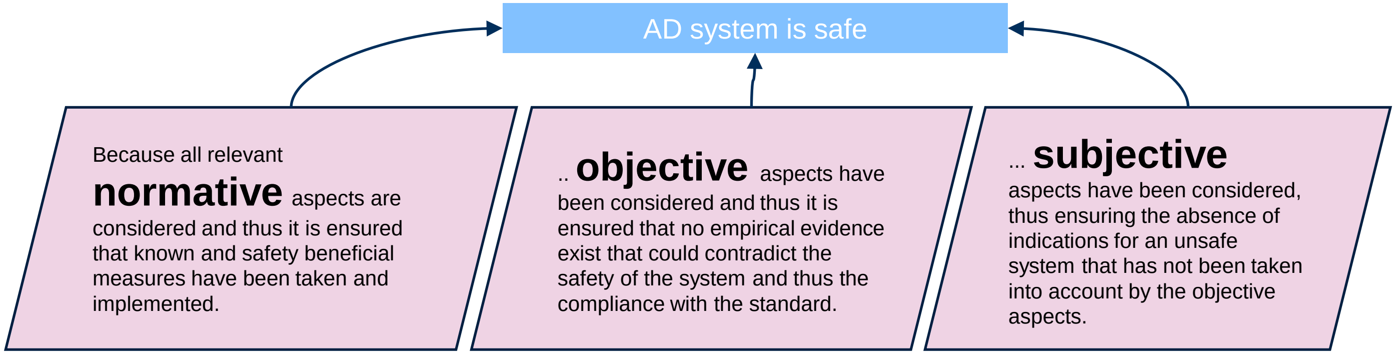
Methods for a structured generation of evidence to support arguments



(Brade, 2021 with minor changes)

Assurance Argumentation - Approach

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

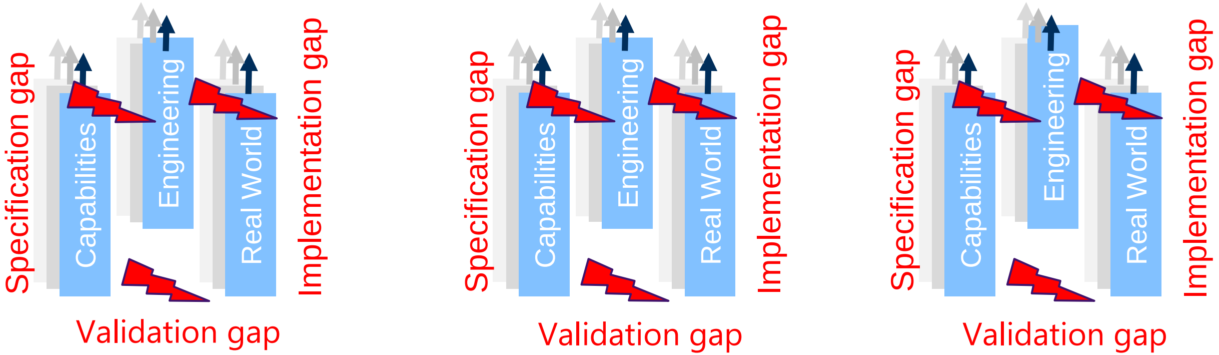


AD system is safe

Because all relevant **normative** aspects are considered and thus it is ensured that known and safety beneficial measures have been taken and implemented.

.. **objective** aspects have been considered and thus it is ensured that no empirical evidence exist that could contradict the safety of the system and thus the compliance with the standard.

... **subjective** aspects have been considered, thus ensuring the absence of indications for an unsafe system that has not been taken into account by the objective aspects.



(Brade, 2021 with minor changes)

Take Away / Outlook

- **Enabler for consideration of societal /market claims and resilience in open context**
  - **Argumentation Framework** enables **iterative development** and thus convergence of results from different **perspectives**.
  - The **Asssurance 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.

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