PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

Final Event 21 / 22 November 2023

Main Approach for Assurance of Automated Driving

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

Assurance Goals for Automated Driving

VERIFICATION
VALIDATION
METHODS

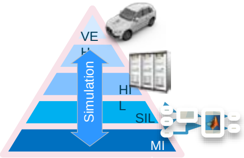
Goal IV – **Explainable Safety**

▶ **Argumentation:** explains safety tracible and consistent.

∞ → n

Feasibility

Efficiency



Goal I **Systematic control of test space**

▶ Systematic decomposition of OD,
Involve traffic-law perspective.

Goal III **Shift to simulation**

▶ Seamless use of virtual and real artefacts.

Goal II **Consistent interfaces**

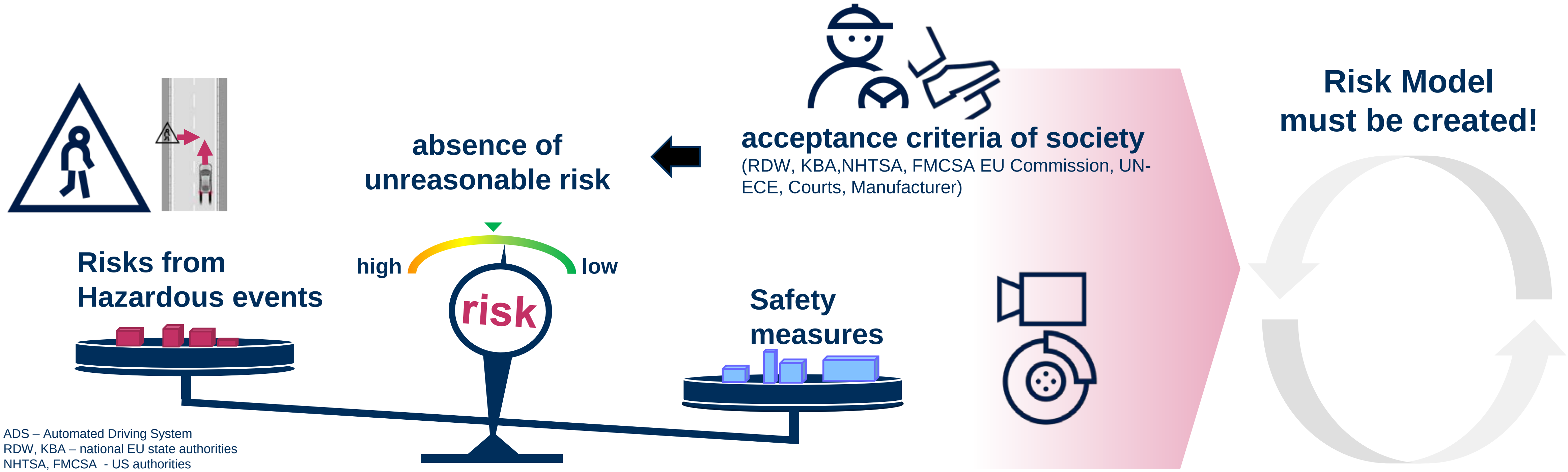
▶ Systematic breakdown of technical contracts,
requirements & tests.

Changeability

Safety expectation and fulfillment

VERIFICATION
VALIDATION
METHODS

- For increasing automation, the focus of safety move to **overall behavior**.
- Safety is defined by **absence of unreasonable risk** (automotive consensus).
- ADS products are safe because they meet **societal safety expectations,** thus societal stakeholders request **risk acceptance criteria**.

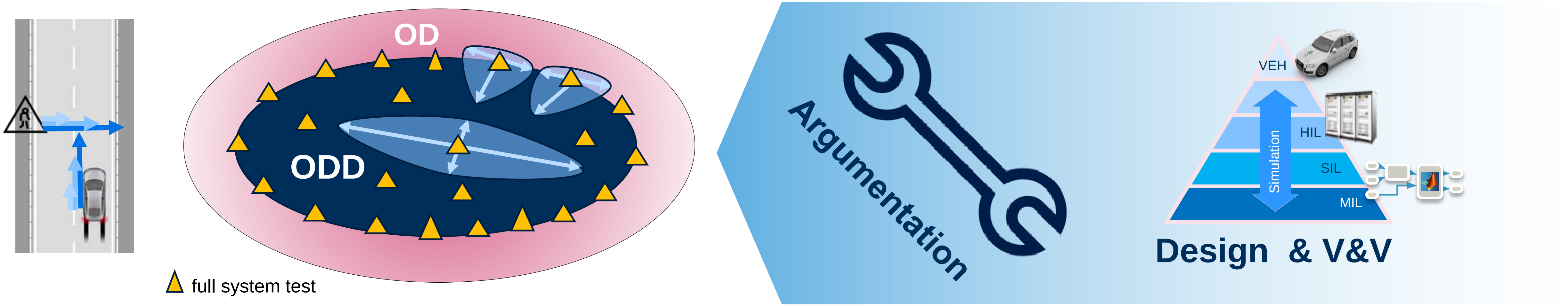


ADS – Automated Driving System
RDW, KBA – national EU state authorities
NHTSA, FMCSA - US authorities

Main Approach

Concept for Assurance of Safety

► Coverage of safe behavior over ODD through systematically argued extrapolation of safe behavior areas, based on evidences given by V&V & Design.

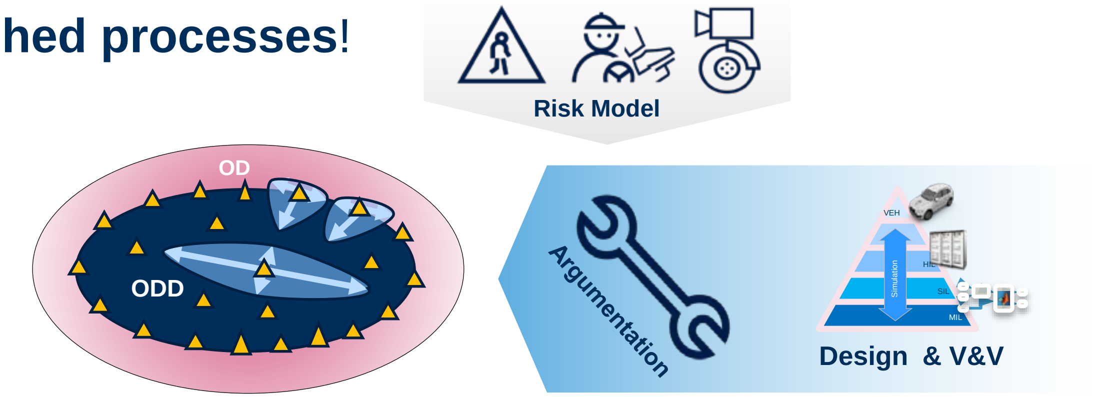


How to explain safety by fulfilling risk acceptance criteria?

► **Use Argumentation:** The Method "Argumentation" is considered as a main enabler for a traceable decomposition of societal claims, the strict format suits to reliably explain risk reduction.

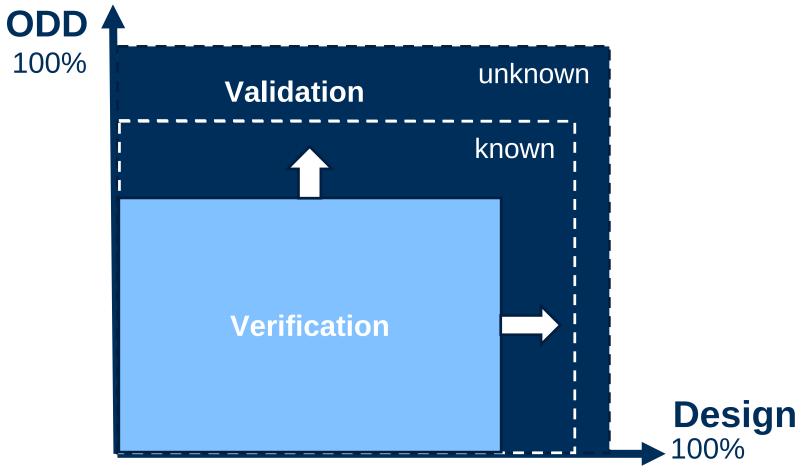
Main Approach

How to extrapolate **safe behavior areas?**
While keeping it **feasible** and maximize the use of **established processes**!



- Select the risk-sensitive areas of behavior by decomposition of ODD and design along risk model.
- Build extrapolation models for safe behavior and define risk and performance thresholds along risk model.

- Verification until performance thresholds are proven (otherwise iterate development).
- Validation to prove that risk is below risk thresholds (otherwise iterate development.).

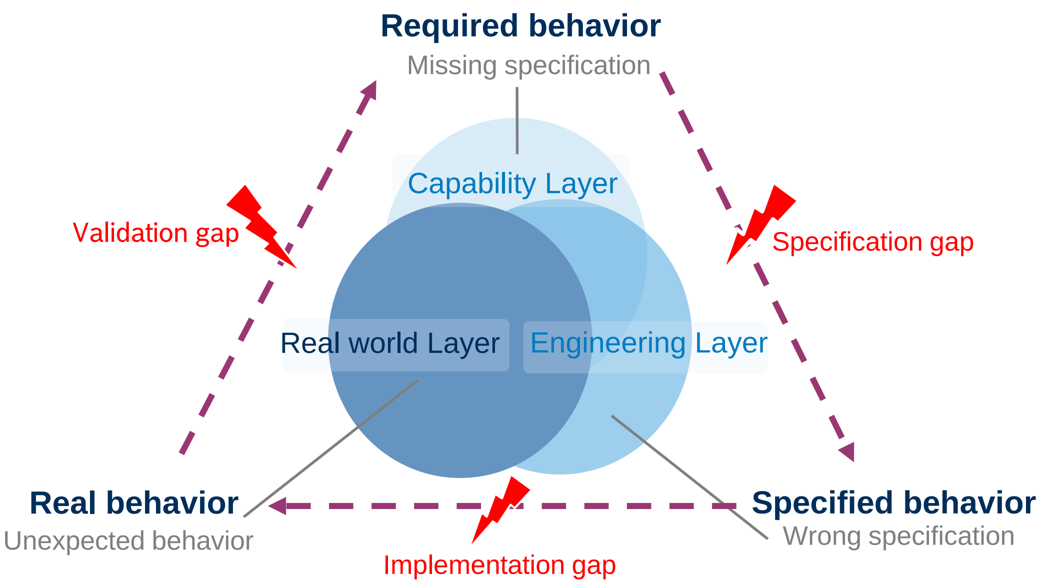


The more verification, the less effort for validation.

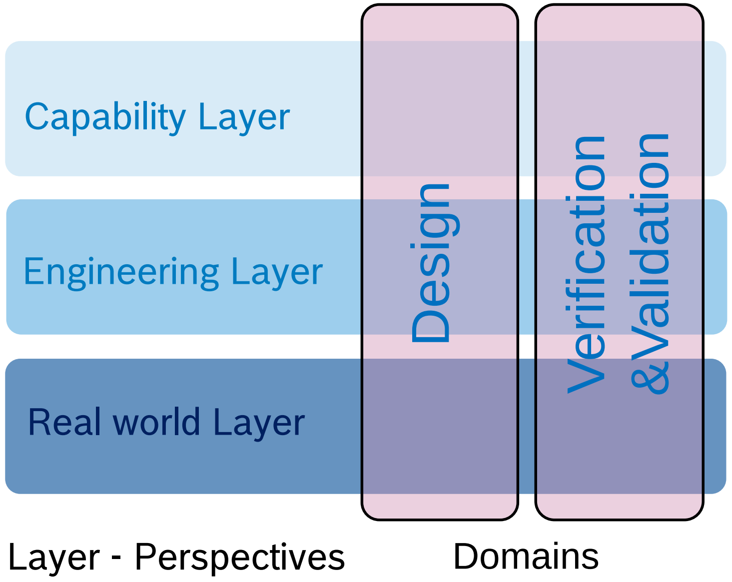
How to argue?

Consequences of Argumentation

Argumentation Concept



Framework

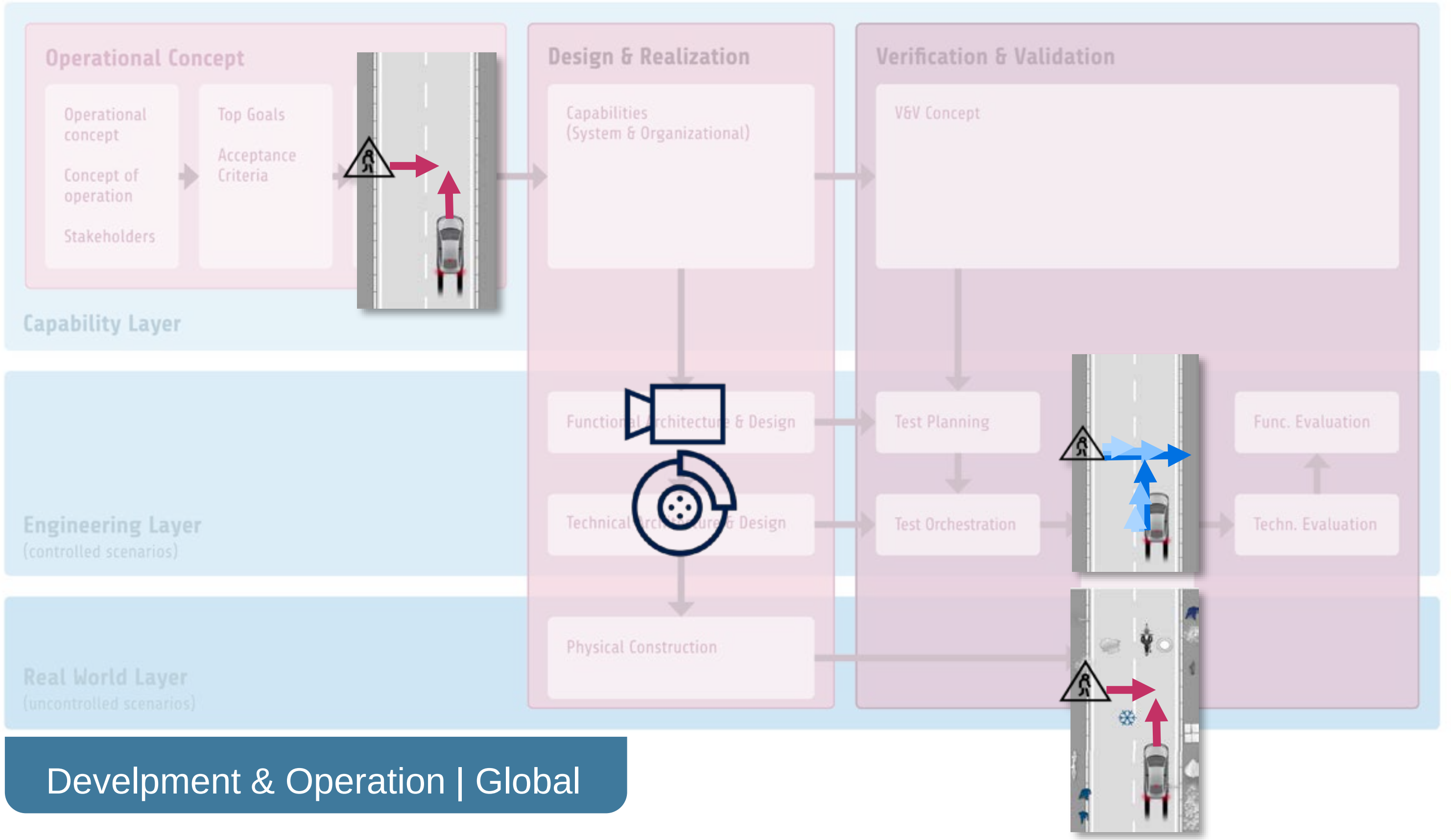


- Argumentation **need different perspectives** - of **behavior.**
- Argumentation **rely on evidences** of the development process.
- The framework of development **must represent is perspectives.**

References: 3 circle model (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)

Solution for Decomposition of Design and V&V Assurance framework

VERIFICATION VALIDATION METHODS



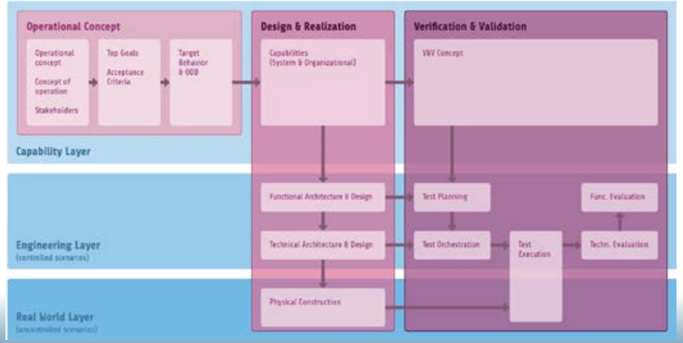
Capability Layer Composition of abstract requirements.
► **"required behavior"**

Engineering Layer System specification by decomposition of the abstract requirements.
► **"specified behavior"**

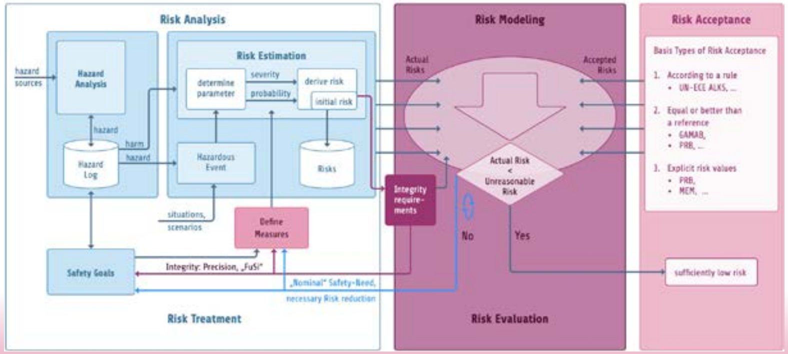
Real World Layer Interaction of the physical system with the uncontrolled environment.
► **"real behavior"**

► **Main Result:** A development framework that aligns seamlessly with the structure of Argumentation while also integrating effectively with established automotive engineering processes.

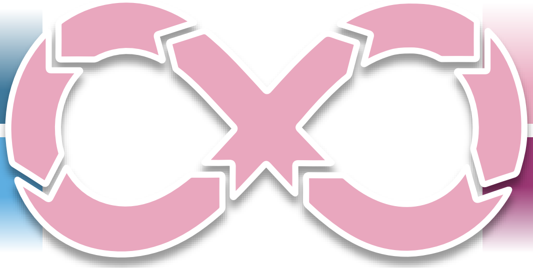
Solution: Assurance Framework



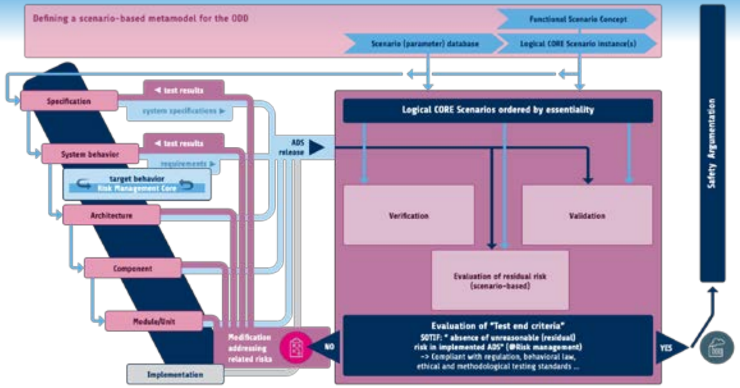
Develpment & Operation | Global



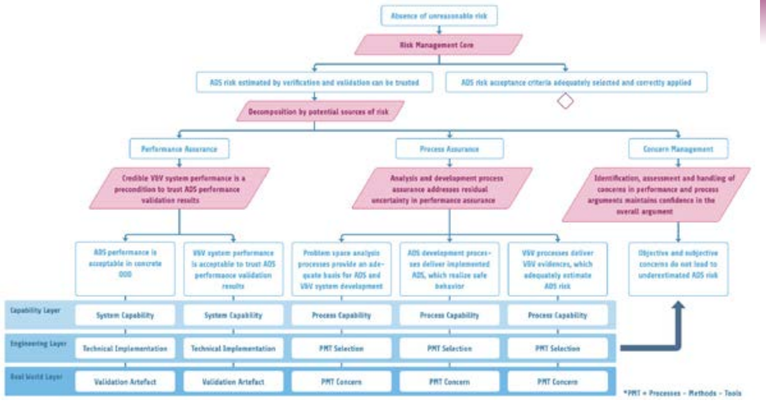
Risk Management



Develpment & Operation | Scenarios



Argumentation

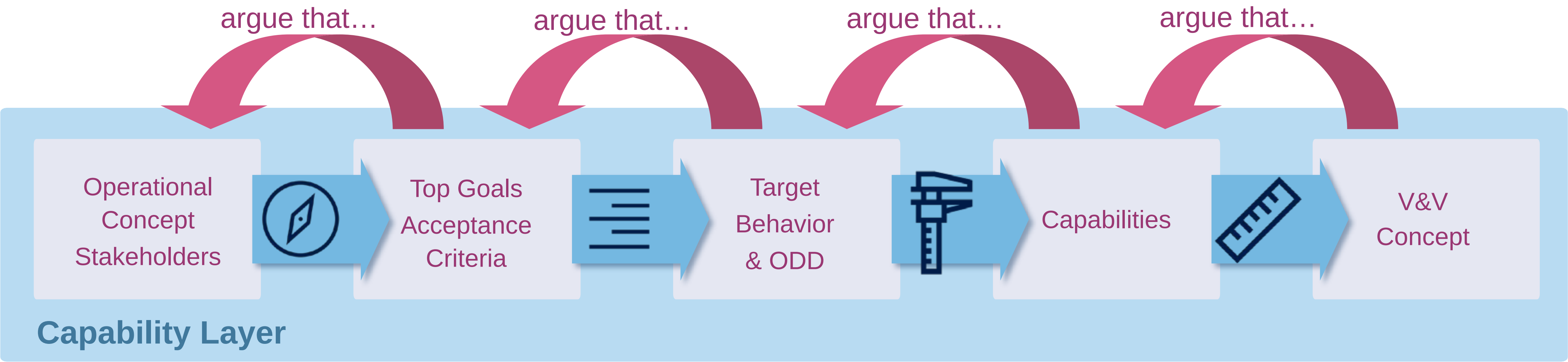


► **Feasibility is enabled by consequent separation of perspectives and their seamless interaction by clearly defined links.**

Feasibility of Argumentation

Principles

- ► **Consistency of metrics ► enable traceability**
  Use of metrics which can transfer between representations.
- ► **Reproducibility ► avoid explosion of “argumentation paths”**
  Build a chain of representations, whereby each representation unite the requirements of the previous.

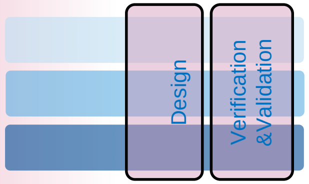


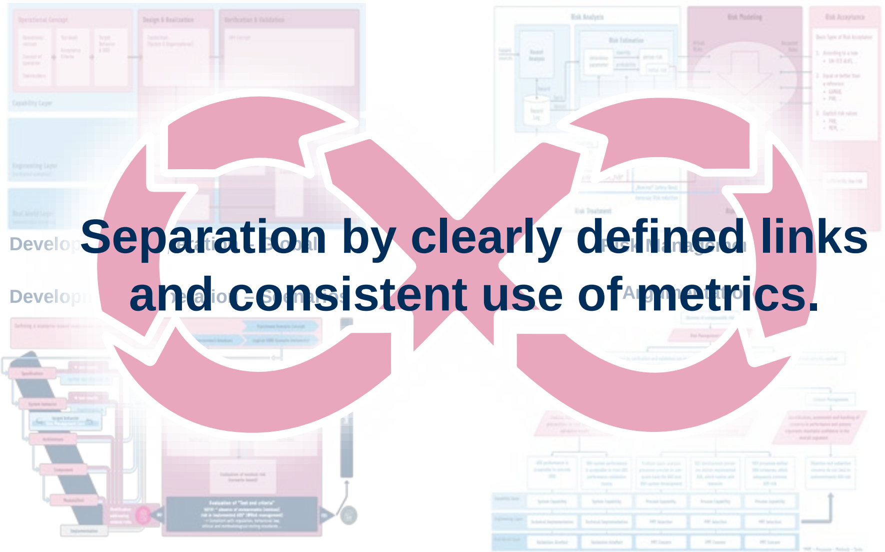
► **Feasibility is enabled by reproducibility of domain-elements and their traceability by consistency of metrics.**

Summary

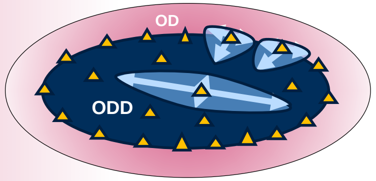
Safe behavior can be argued

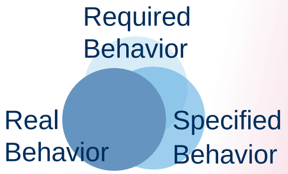
- Decomposition of Design and V&V suits to other perspectives.
- Risk is modeled according to the other perspectives.



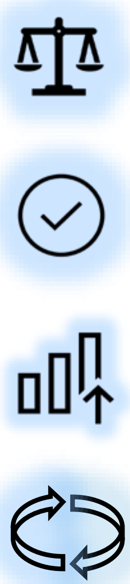


Separation by clearly defined links and consistent use of metrics.





- Decomposition of ODD suits to other perspectives.
- Argumentation is structured according to the other perspectives.



VERIFICATION
VALIDATION
METHODS

Thank you!

Roland Galbas, Robert Bosch GmbH

Roland.Galbas@de.bosch.com

PROJECT of the PEGASUS FAMILY

VDA LEITINITIATIVE

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