

# **Toward a Comprehensive Assurance Argument for the Release of Automated Vehicles**

## **Challenges, Insights, and First Results from the Research Project “VVMMethods”**

Marcus Nolte<sup>1</sup>, Jan Reich<sup>2</sup>, Tino Brade<sup>3</sup>, Roland Galbas<sup>3</sup>, Thomas Goeppel<sup>3</sup>, Frank Junker<sup>3</sup>,  
Thomas Kirschbaum<sup>3</sup>, Thomas Corell<sup>4</sup>, Björn Filzek<sup>4</sup>

<sup>1</sup> TU Braunschweig, Institut f. Regelungstechnik, <sup>2</sup> Fraunhofer IESE, <sup>3</sup> Robert Bosch GmbH, <sup>4</sup> Continental Teves AG & Co. oHG

- Several industry players have recently started offering services implemented by automated vehicles
- Safety remains key question
  - Needs to be **built-in**, not **bolt-on**!
- “How safe is safe enough?”  
is still not fully answered.

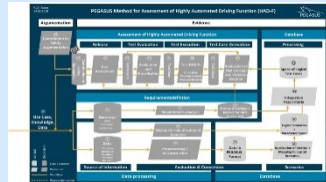


- The **PEGASUS Family** focuses on development / testing methods and tools for AD systems on highways and in urban environments

## 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 4to5



- Scope: **Simulation platform, toolchains, definitions for simulation-based testing**
- Use-Case: L4/5 in 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**

OEM	
Tier-1	
Tech	
Eval	
Science	

## Systematic control of test space

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

$\infty \rightarrow n$



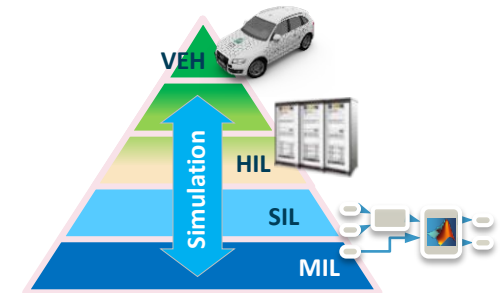
## Consistent interfaces for assurance argumentation, systems and components across the supply chain

- ▶ Definition of incremental tests of subsystems and overall systems



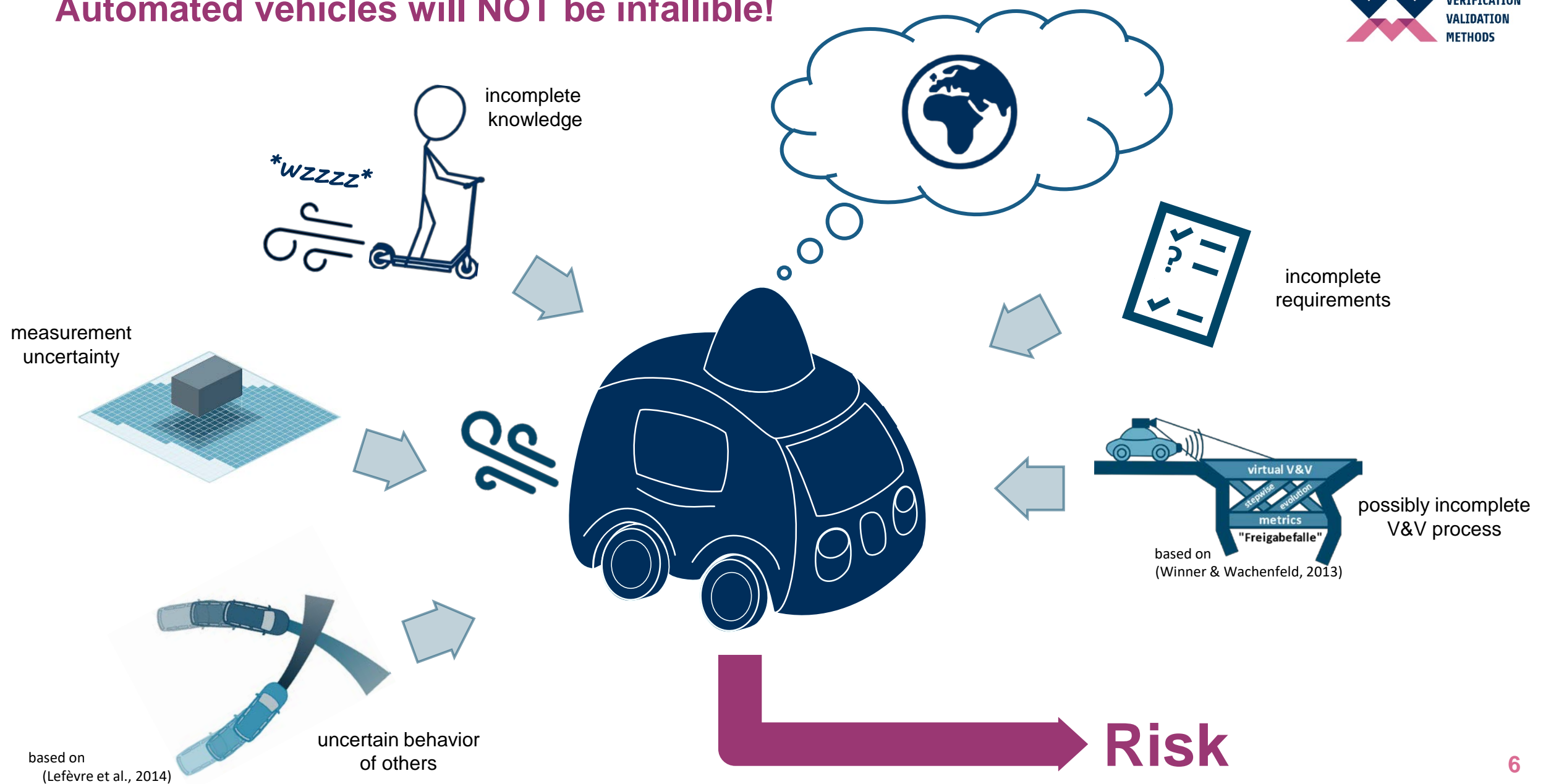
## Significant shift from real-world testing to simulation

- ▶ Methods for seamless testing across all test instances



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

# Automated vehicles will NOT be infallible!



based on  
(Lefèvre et al., 2014)



# “Safe enough” = “Safer than”?

- Our current traffic system is an **open** system
- Largely works, because human drivers

uncertainty

incompleteness

- This **inherent risk** is obviously
- A **principle of trust** (most often)
- Worst-case assumptions lead

moving in traffic

risk

“always expect the unexpected.”

## What does apply to automated agents?

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

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



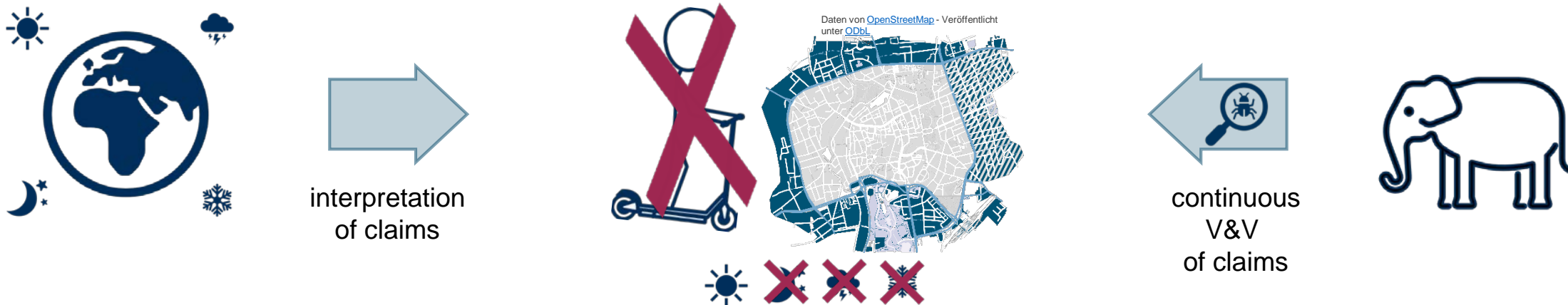
*... to ensure (& enhance) public trust in the technology?*

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



# Traceable decomposition & continuous validation of claims

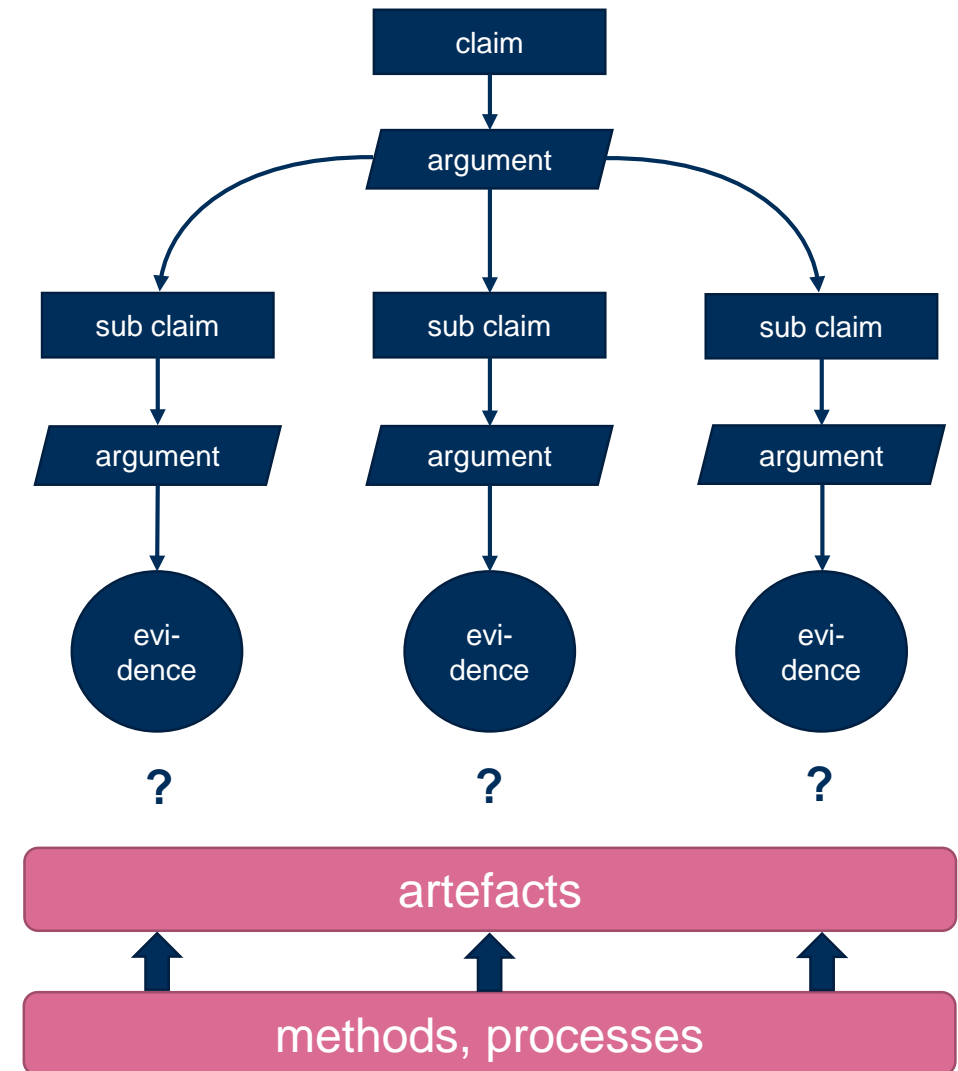
- ▶ Enable argumentation that safety case will remain valid, even if **system context changes**.
- ▶ **Traceable** decomposition / interpretation of claims (assumptions)
- ▶ Continuous **post-release** verification & validation w.r.t **new findings**: Do assumptions still hold?



# There is more to an assurance argument than an ISO 21448- / UL4600-compliant notation

- Not necessarily self-explaining, i.e. accessible for every stakeholder
- **No direct connection** between the argument's structure & processes for evidence generation
- VVM addresses:
  - Methods for a **structured decomposition** of claims
  - Methods for **generating evidence** to support arguments

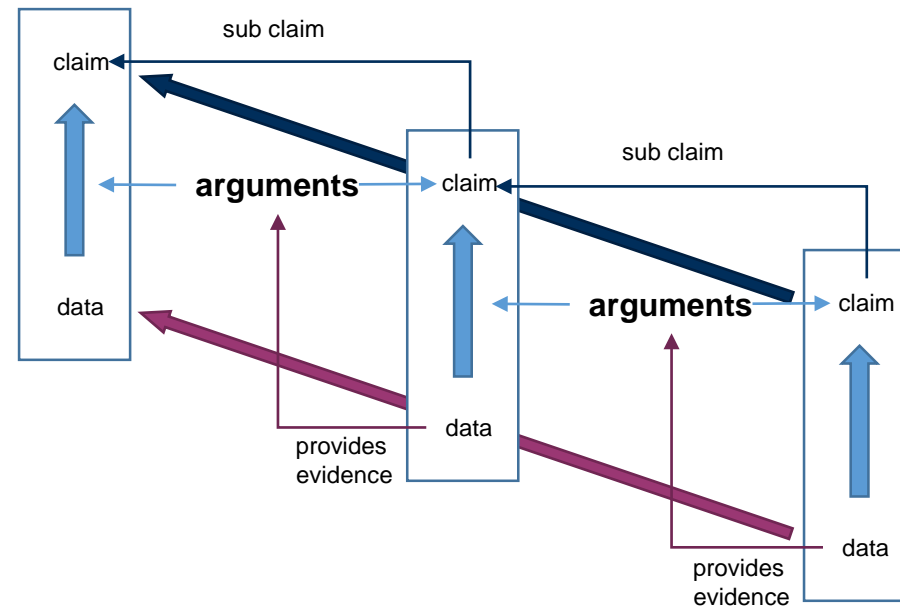
**How do we link methods, artefacts, evidence & argumentation structure?**



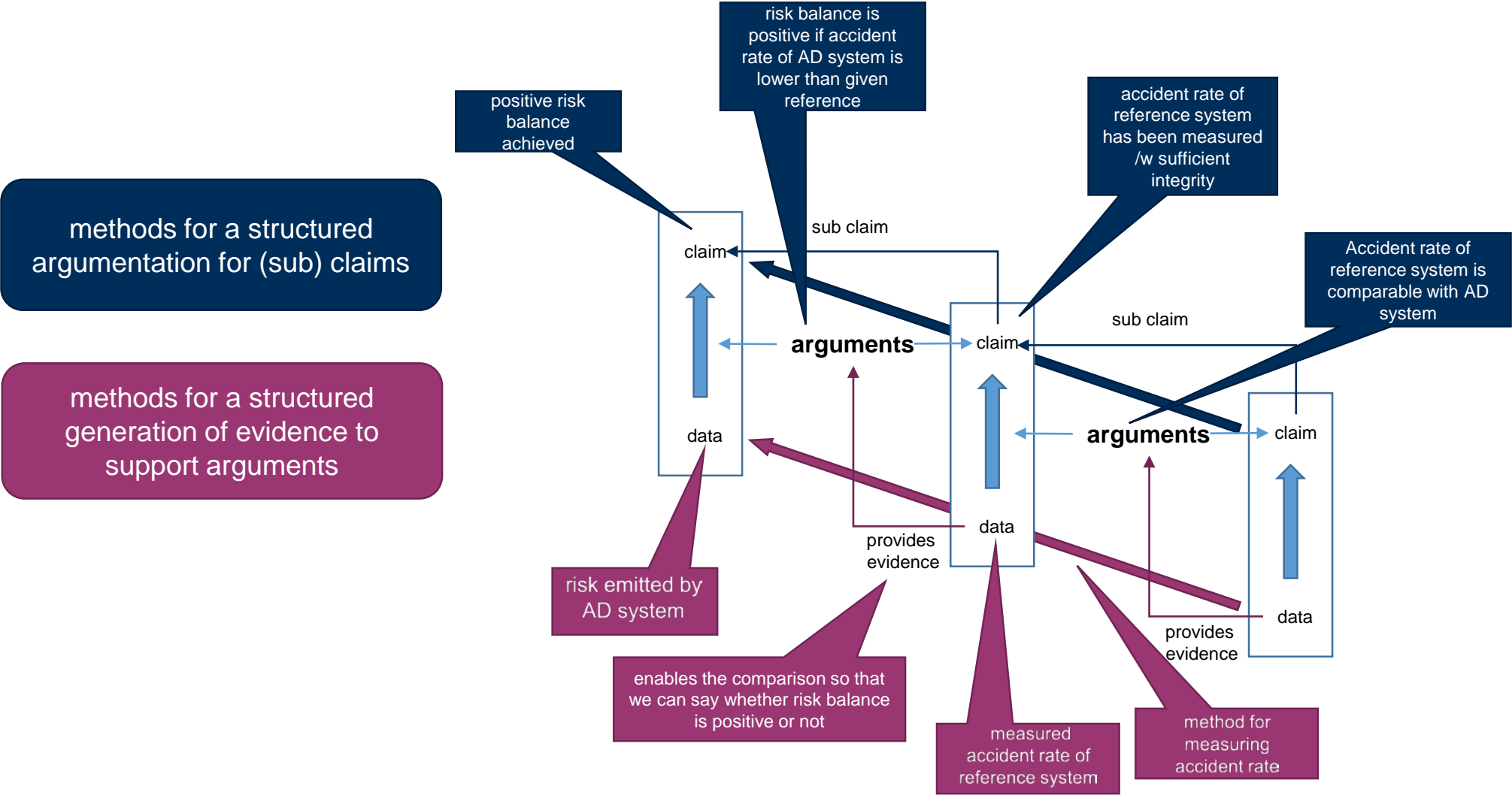
# What does VVM do?

methods for a structured  
argumentation for (sub) claims

methods for a structured  
generation of evidence to  
support arguments

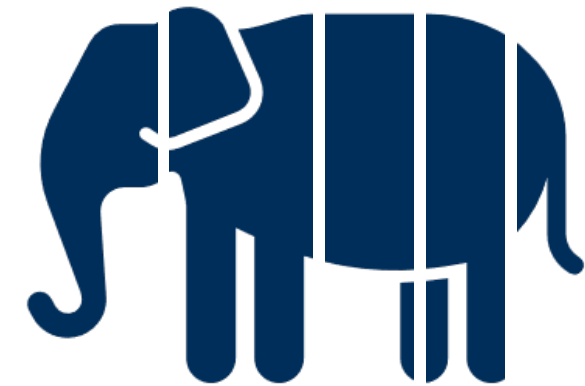


# What does VVM do?



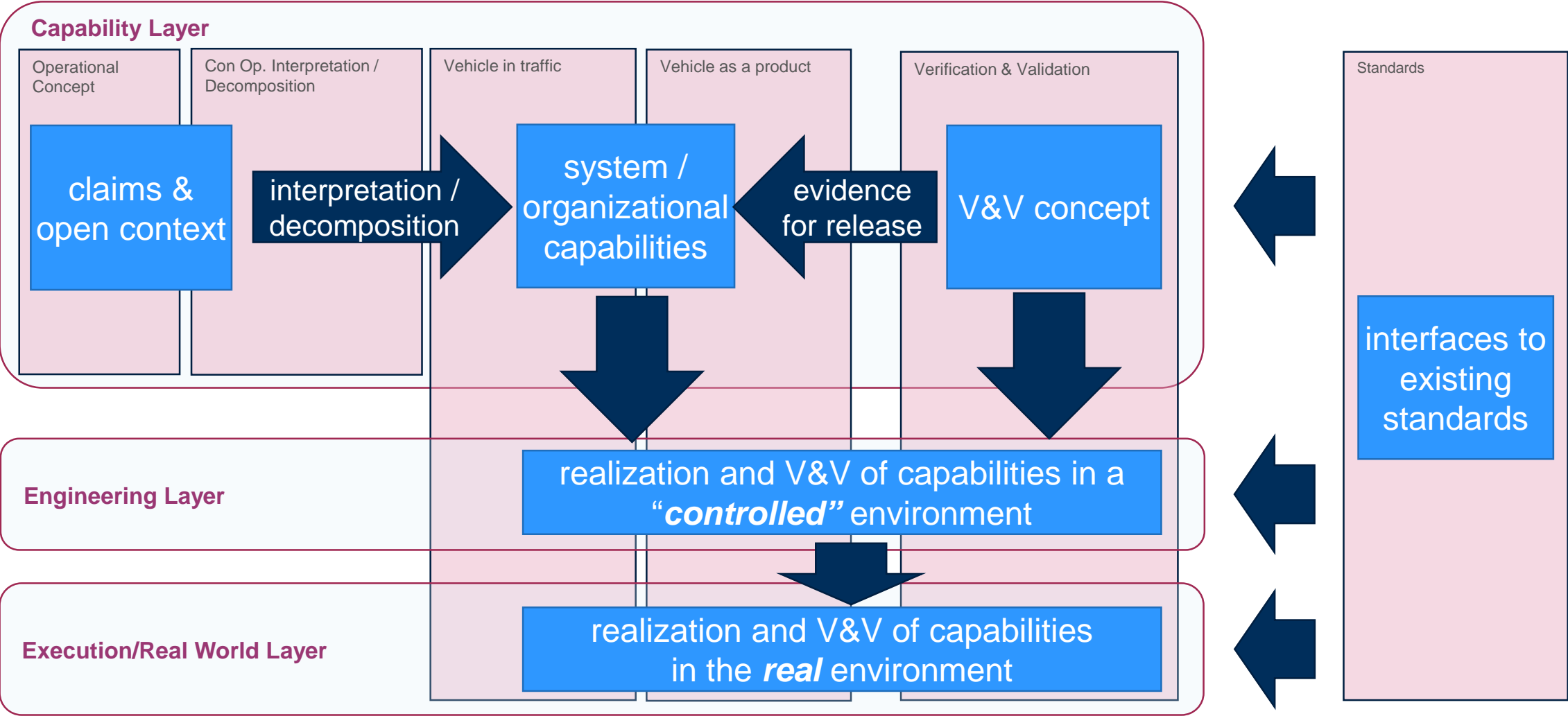
# Requirements for a coherent, comprehensible and traceable safety argument

- ▶ What we found, we need to connect methods, artefacts, evidence & argumentation structure:
  - ▶ A **suitable level of abstraction** to argue the decomposition of the open context
  - ▶ Possibility to argue for available evidence from a **positive & negative** perspective
  - ▶ **Separation of concerns** to provide overview & allow deep dives where necessary
  - ▶ (System- / Enterprise-) **architecture** as integral part of the safety argument
  - ▶ Compliance to **relevant industry standards**



*„slicing the elephant“*

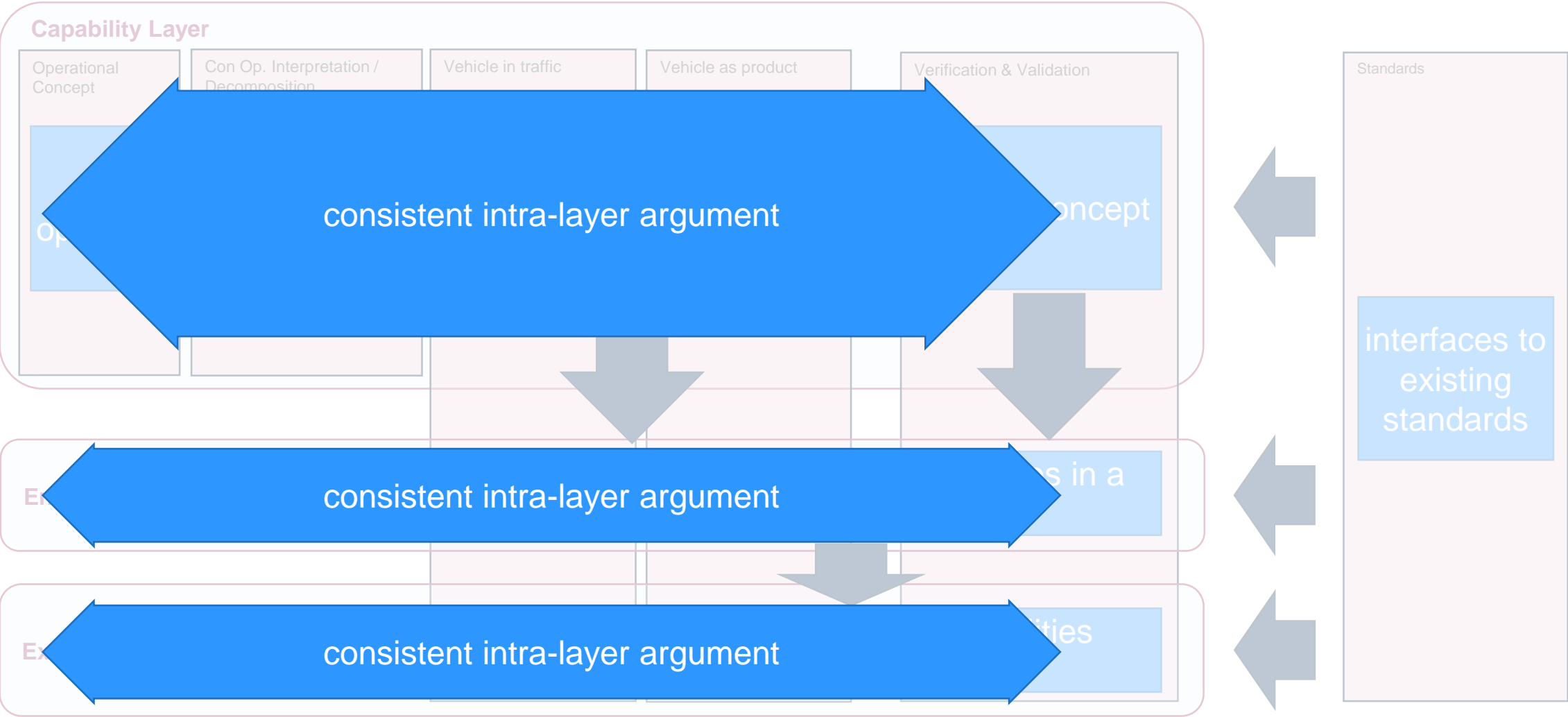
# High level assurance argument structure



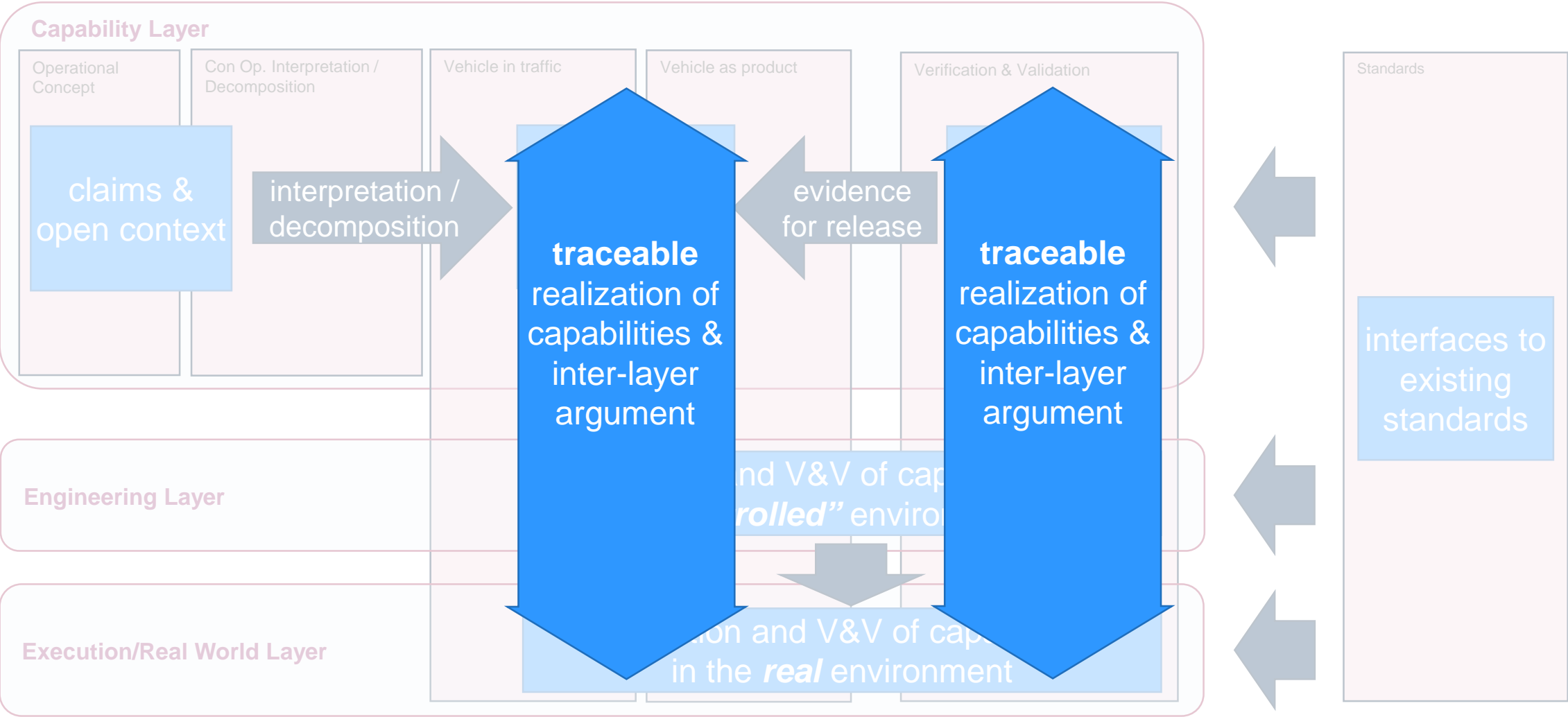
(Reich, 2021)



# High level assurance argument structure



# High level assurance argument structure



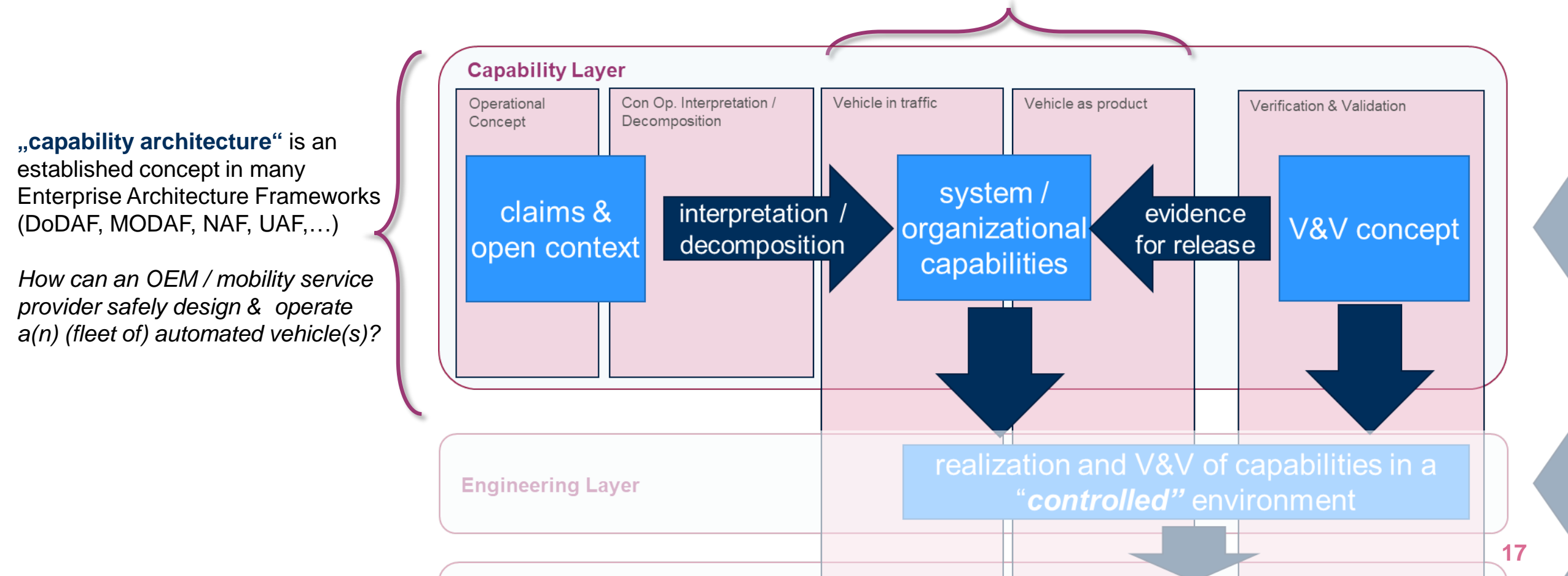
# Capability Layer: Linking enterprise & individual vehicle

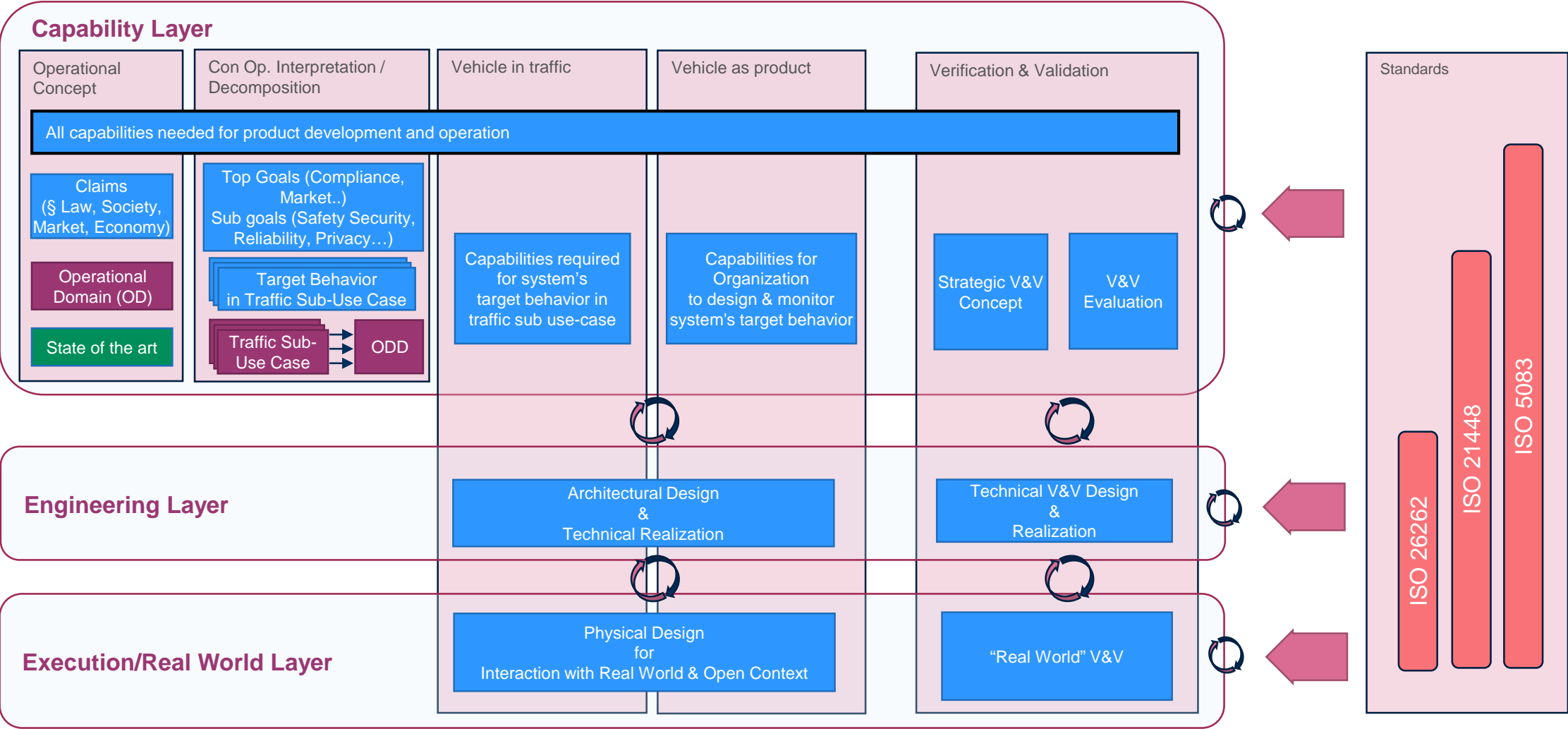
**bridging enterprise architecture & systems engineering**

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?*





- Focus on capability layer
  - finding a **suitable level of abstraction** for the formulation of capabilities
  - connecting **organizational & system** capabilities
  - including capabilities as **integral part** of the safety case
- Integrating developed methods in the project with the 3-layer structure
- Assigning evidence generated by those methods to the 3-layer structure
- Connecting existing standards to the 3-layer structure

**Structure seems to provide a helpful „bridge“ to fulfill the project goals w.r.t coming up with a coherent & traceable safety argument, acknowledging the challenges of the open context!**

- ▶ There is more to a coherent assurance argument than the notation of a safety case
- ▶ VVM contributes by
  - ▶ Tackeling the complexity of the assurance argument by means of **separation of concerns**
  - ▶ Linking methods, artefacts, evidence and argumentation structure in a **structured & traceable manner.**
  - ▶ Implementing a **capability-based concept** that allows for a coherent argument across claims, architecture, evidence in an open context on an organizational & system level





# Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:

**Marcus Nolte**

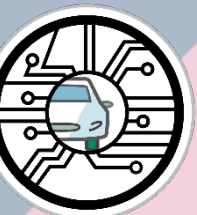
*TU Braunschweig*

*Institut für Regelungstechnik*

 nolte@ifr.ing.tu-bs.de     +49 531 391 3827

 [https://www.researchgate.net/profile/Marcus\\_Nolte](https://www.researchgate.net/profile/Marcus_Nolte)

 <https://www.linkedin.com/in/marcus-nolte-95974a143/>



Gefördert durch:



aufgrund eines Beschlusses  
des Deutschen Bundestages

Lefèvre, S., Vasquez, D. & Laugier, C. (2014) **A survey on motion prediction and risk assessment for intelligent vehicles**. *Robomech J* 1, 1  
<https://doi.org/10.1186/s40648-014-0001-z>

Winner, H., Wachenfeld, W. (2013). **Absicherung automatischen Fahrens**. 6. FAS-Tagung München.

Gasser, T., Frey, A. (2018), *Oberseminar am IfR*, Braunschweig

Reich, J., Galbas, R., Kirschbaum, T., Junker, F., Corell, T., Filzek, B. (2021) **Herausforderungen und Lösungsansätze für die durchgängige Freigabeargumentation von automatisierten Fahrfunktionen – Erste Ergebnisse aus dem BMWi „V&V Methoden“-Projekt**.  
*TÜV SÜD safe.tech Tagung*

Brade, T. (2021) **Insights into the VVM Argumentation Chain** (internal presentation)