PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

Mid-Term Presentation 15 / 16 March 2022

VVM main approach
How to systematically release AD systems?

Roland Galbas, Robert Bosch GmbH

Supported by:

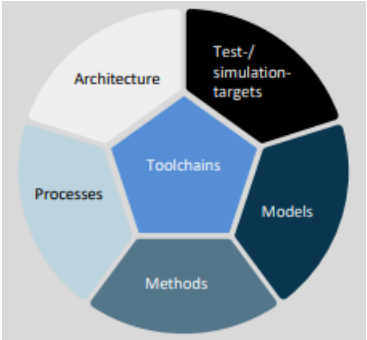
Federal Ministry for Economic Affairs and Climate Action

on the basis of a decision by the German Bundestag

Starting with the goals

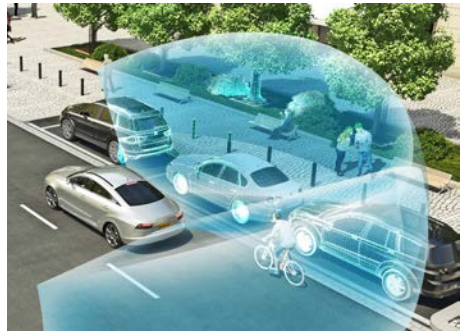
Goal I – Reduction of test cases

Open World Challenge ∞ → n



Goal II – Industrial interfaces

How to realize goals within open context?



Goal III – Shift to simulation

VVM - Main goals more concrete

VERIFICATION VALIDATION METHODS

I. Systematic control of test space

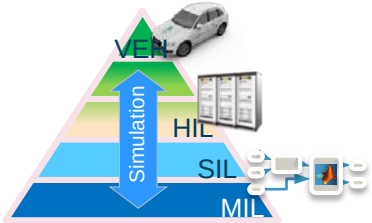
Methods to map the infinitely-complex open context onto a finite & manageable set of artifacts.

II. Consistent interfaces for systems and components

Definition of technical contracts, tests of systems and subsystems.

III. Significant shift from real-world testing to simulation

Methods for seamless testing across all test instances.



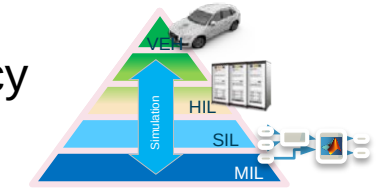
Added: IV Argumentation

- fulfillment of societal claims e.g safety, via law, standards, state of the art.

Analyse goals I-III

Feasibility

Efficiency



Goal I **Systematic control of test space**

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

Goal II **Consistent interfaces**

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

Goal III **Shift to simulation**

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

Changeability

Analyze goal IV

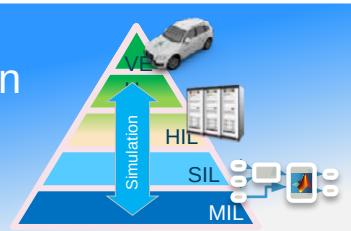
Disruptive Element (selected)	Change of responsibility “Driver decides no more”
Societal Expectation	Argue the fulfillment of e.g. law within open context

Explainable Compliance

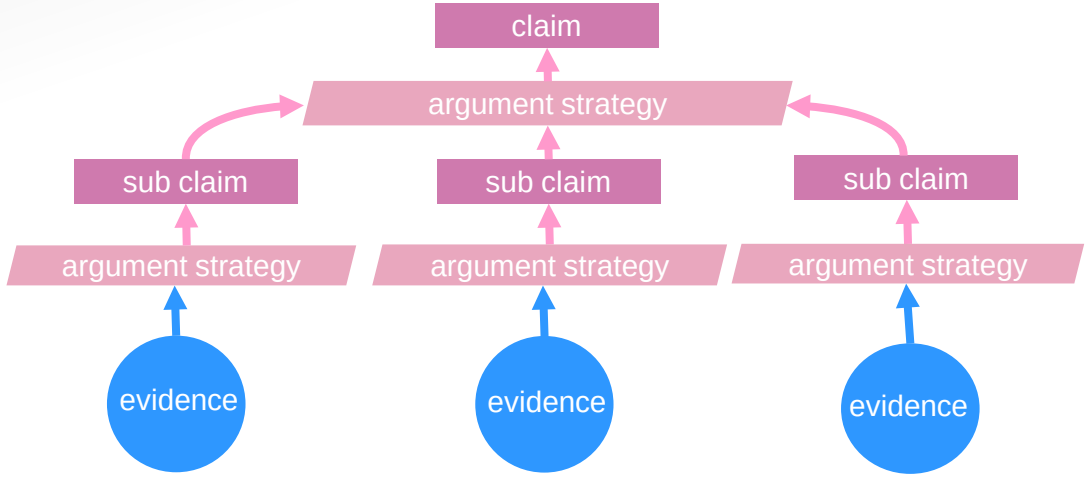
Requirements & Challenges

- ▶ Understand responsibilities within open context
- ▶ Risk acceptance criteria - societal references (e.g. positive risk balance)

- ▶ V&V delivers evidence for argumentation
- ▶ V&V copes with increased complexity



Argumentation



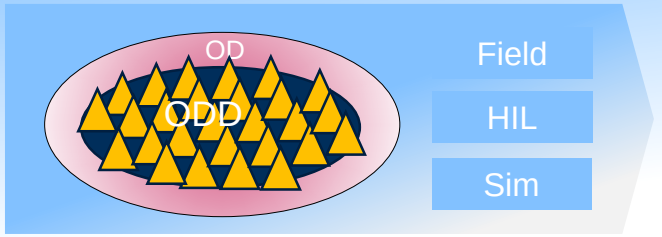
Way towards assurance

VERIFICATION VALIDATION METHODS

Classic

► Brute force: x million miles

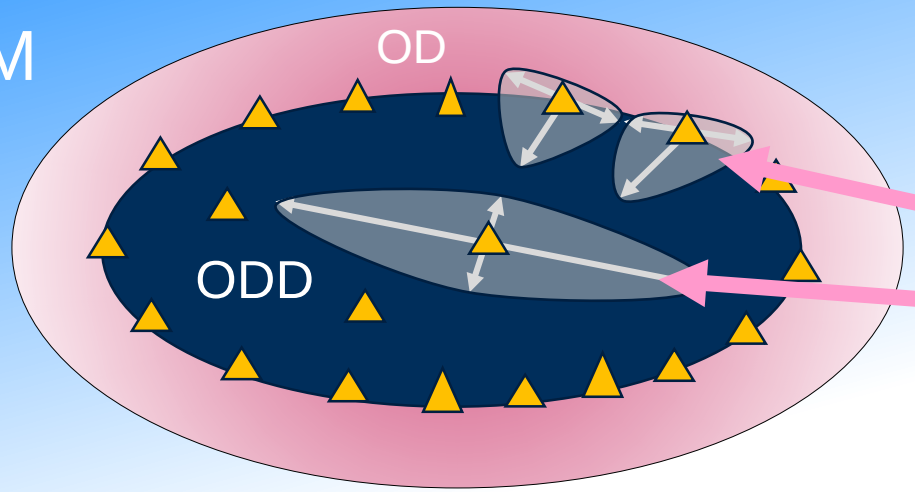
Pegasus



► ODD decomposition & initial argumentation

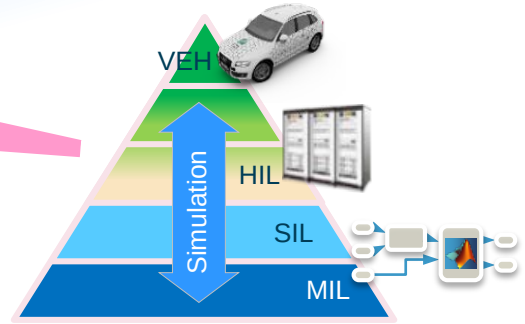
VVM

► ODD more complex
► Systematic argumentation of coverage



full system test

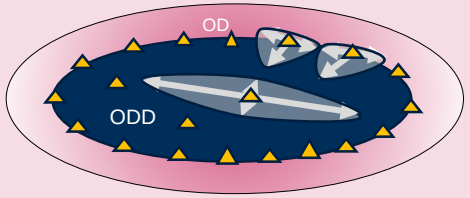
Argumentation

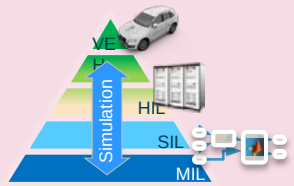


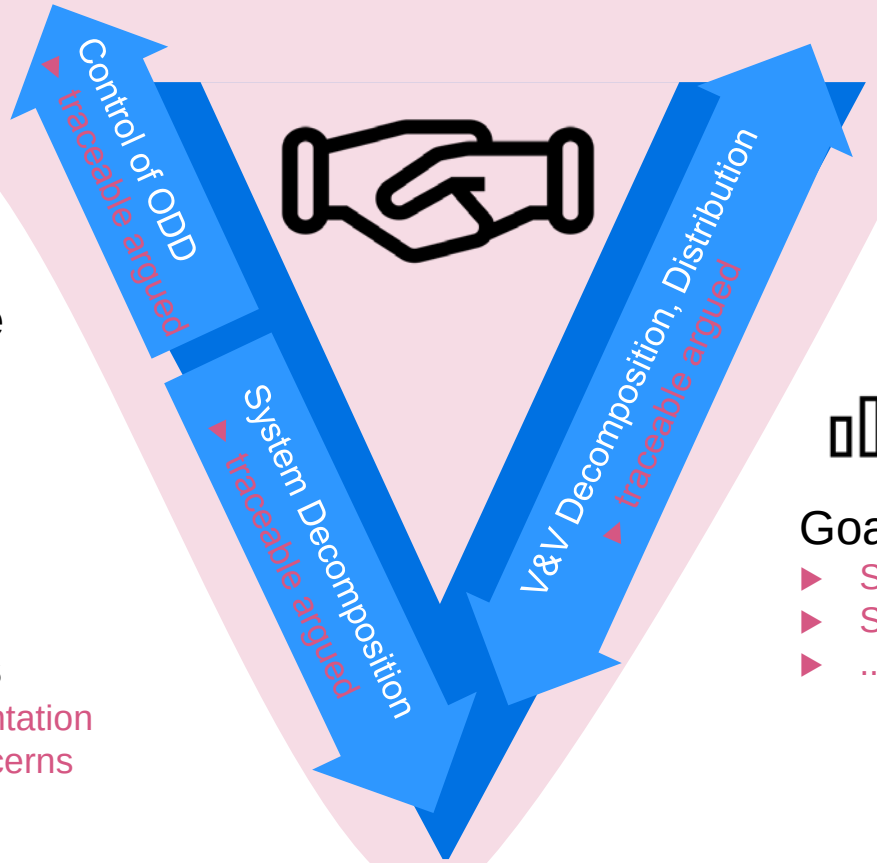
Combining goals

Goal IV – **Argumentation**

Explainable Compliance







Feasibility

Goal I – **Systematic control of test space**

- Design of System Monitoring
- Integration of V&V into Design
- …

Changeability

Goal II – **Consistent interfaces**

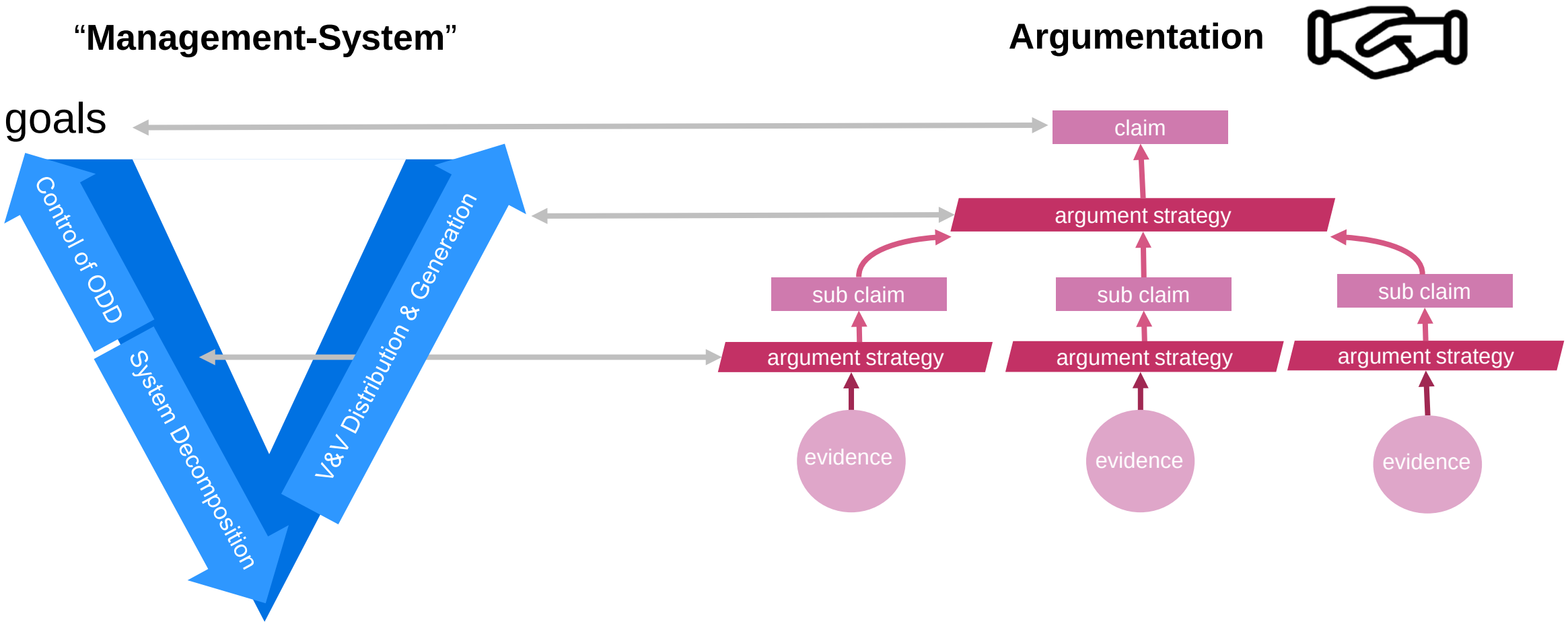
- Systematic Decomposition by Argumentation
- Dependability Analysis of System Concerns
- ….

Efficiency

Goal III – **shift to simulation**

- System Monitoring and Assessment
- Structured Data Handling
- …

Prerequisites

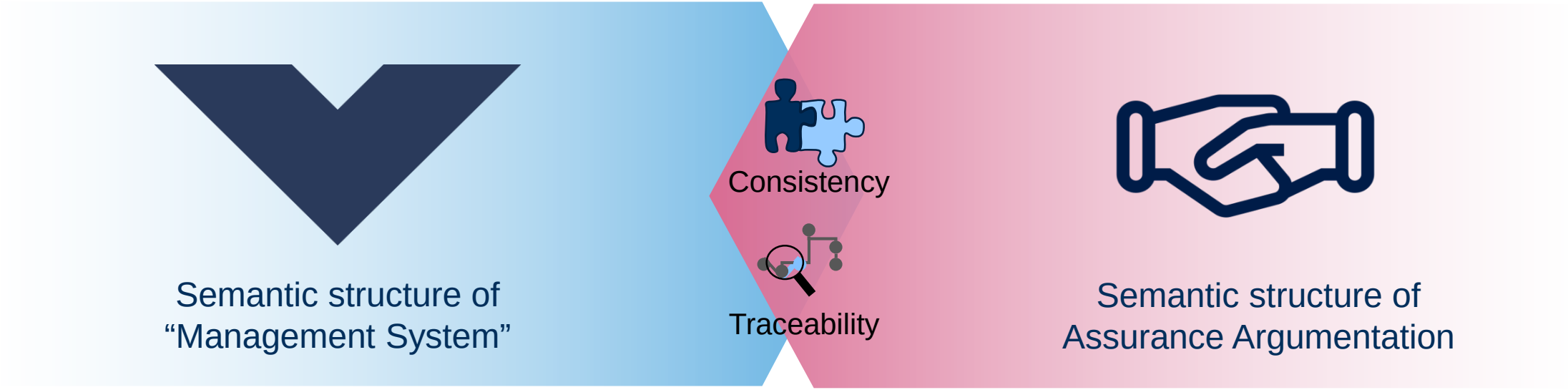


- **Goals** of the "Management- System" correspond to Argumentation **Claims**
- **Processes** of the "Management System" correspond to Argumentation **Strategies**, **traceable argued.**

Strategy

In order to fulfill the goals Feasibility Changeability Efficiency Explainable Compliance

- The semantic structure of the “Management-System” must **correspond** to the semantic structure of the assurance argumentation.
- Thus the assurance argumentation must provide **consistency and traceability** also for the “Management-System”.



Challenges for a coherent assurance argument

How can we argue 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“?

… and which Systematic is suitable?

What do we mean by Safety or Acceptance Criteria?

Society, Standards, Regulations …

Safety =

Exemplary GOAL: "***Absence of unreasonable / unacceptable* risk***"

or "*reduction of the risk to an accepted level (on behalf of society)*"

The TOP GOAL is formed into a set of SUB GOALs

Sub_Goal-1: Functional Safety

Among others
ISO 26262
…
compliance

Sub_Goal-2: SOTIF (tech. demands)

Among others
ISO 21448
(limitation VVM on **technical SOTIF**)
…. compliance

Sub_Goal-3: Laws & Regulation

Among others
national road law
traffic law
product liability law
civil liability law
antitrust laws
…
compliance

Among others
UNECE ALKS
UNECE Regl. WP29 GRVA
compliance

Sub_Goal-4: Ethics & Safety performance

Among others
Ethical standards
Germ. Ethics Com.
Safety First AD, WP
ISO_TC241 -39003
…
compliance

Among others
performance
in accident
reduction
ISO 21934

Among others
Active safety
"*preventive behaviour*"

Scope of VVM overall method

Sub_Goal-5: Human Vehicle interaction/integration

Among others
ISO 21448 (HMI-demand of SOTIF)
ISO 21959, ESOP,
JAMA, State of the Art in literature
compliance

Sub_Goal-6: Cybersecurity

among others
ISO 21434,
UNECE R155
…
compliance

Sub_Goal-n:
- Implementation updates
- Data privacy, protection
- V2X; …

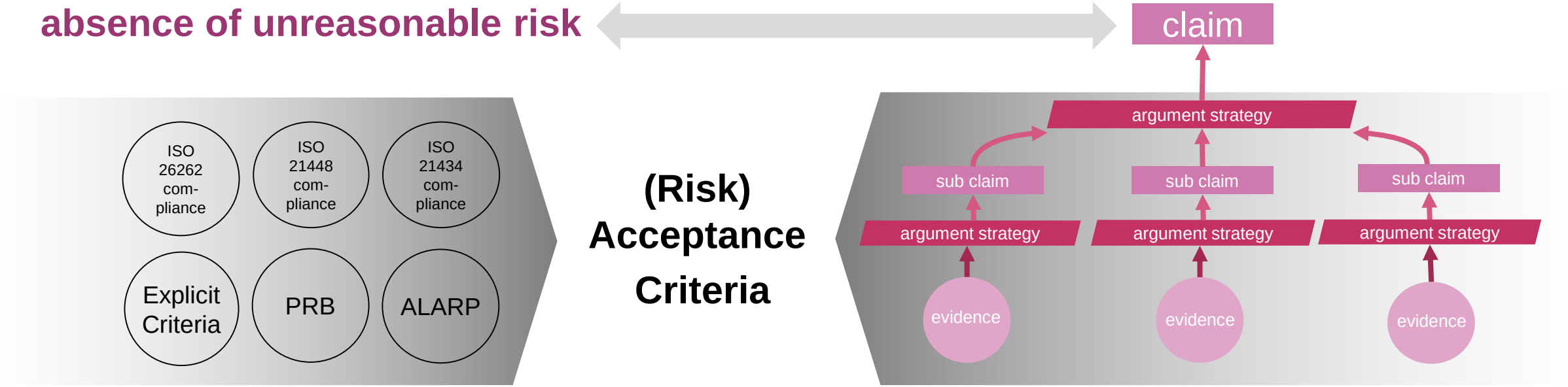
among others
SENA
ICO GDPR
…
compliance

* unacceptable risk according to valid societal moral concepts (ISO 4804)

Interaction of Standards and Argumentation

Exemplary Goal:
absence of unreasonable risk

Argumentation



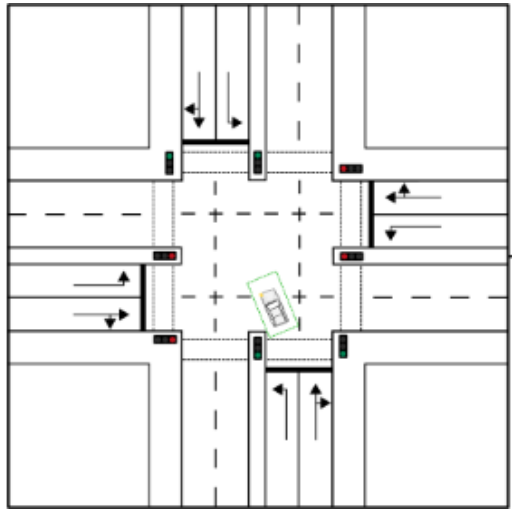
- For safe products automotive industry shows the “absence of unreasonable risk” which is considered to represent sufficiently low risk.
- A set of appropriate Risk Acceptance Criteria (RAC) support evidence.

Scope

- **Customer function**
  - Dual Mode, typical weather conditions, urban (60km/h), highways (100km/h)

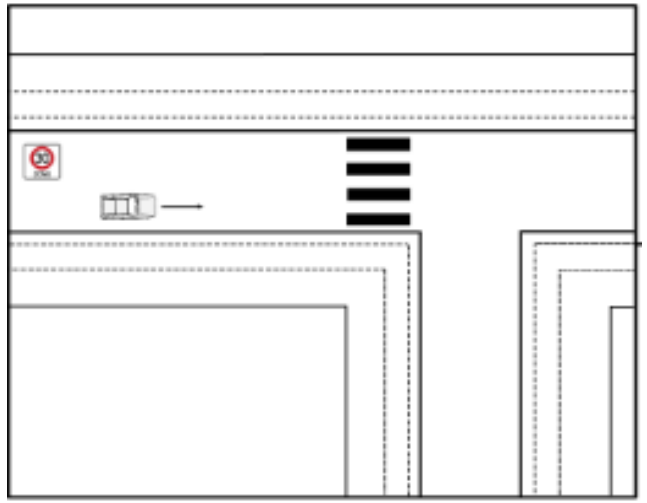
- **Functional Use Cases (FUC)**

FUC1



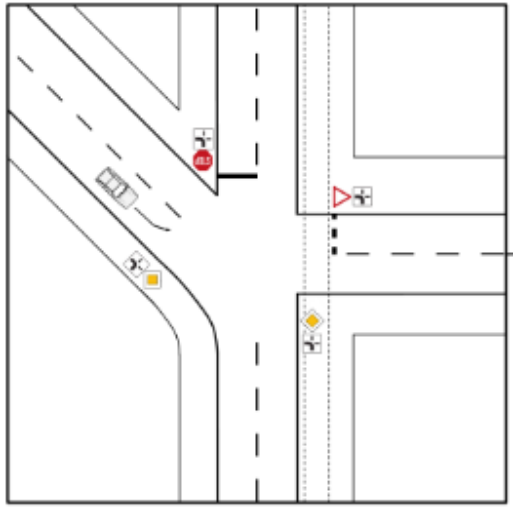
Left Turn on an X-Crossing with Traffic Lights

FUC2



Straight Passing of a T-Crossing with Pedestrian Crossing

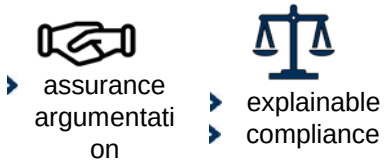
FUC3

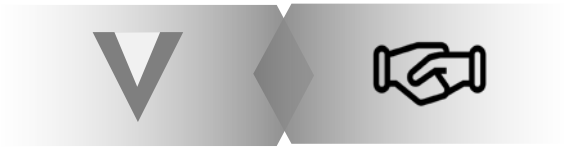


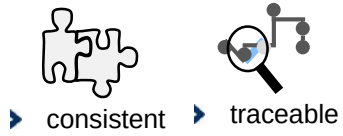
Left Turn on an X-Crossing with Traffic Lights

Take Away

- An **assurance argumentation** enables **explainable compliance**.
- Assurance argumentation and **management system** should base on the **same semantic structure**, thus suitable evidences are delivered by the management system.
- The assurance argumentation enables a **consistent and traceable decomposition** from claims down to **verification & validation, methods** should comply to relevant **industry standards and regulations.**
- Thus, following the concepts, the ***goals can be enabled in common***.







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