PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

Final Event 21 / 22 November 2023

Contributions to a Traceable Behavior Specification and Capability Analyses

Nayel Fabian Salem, TU Braunschweig (Institute of Control Engineering)

Supported by:

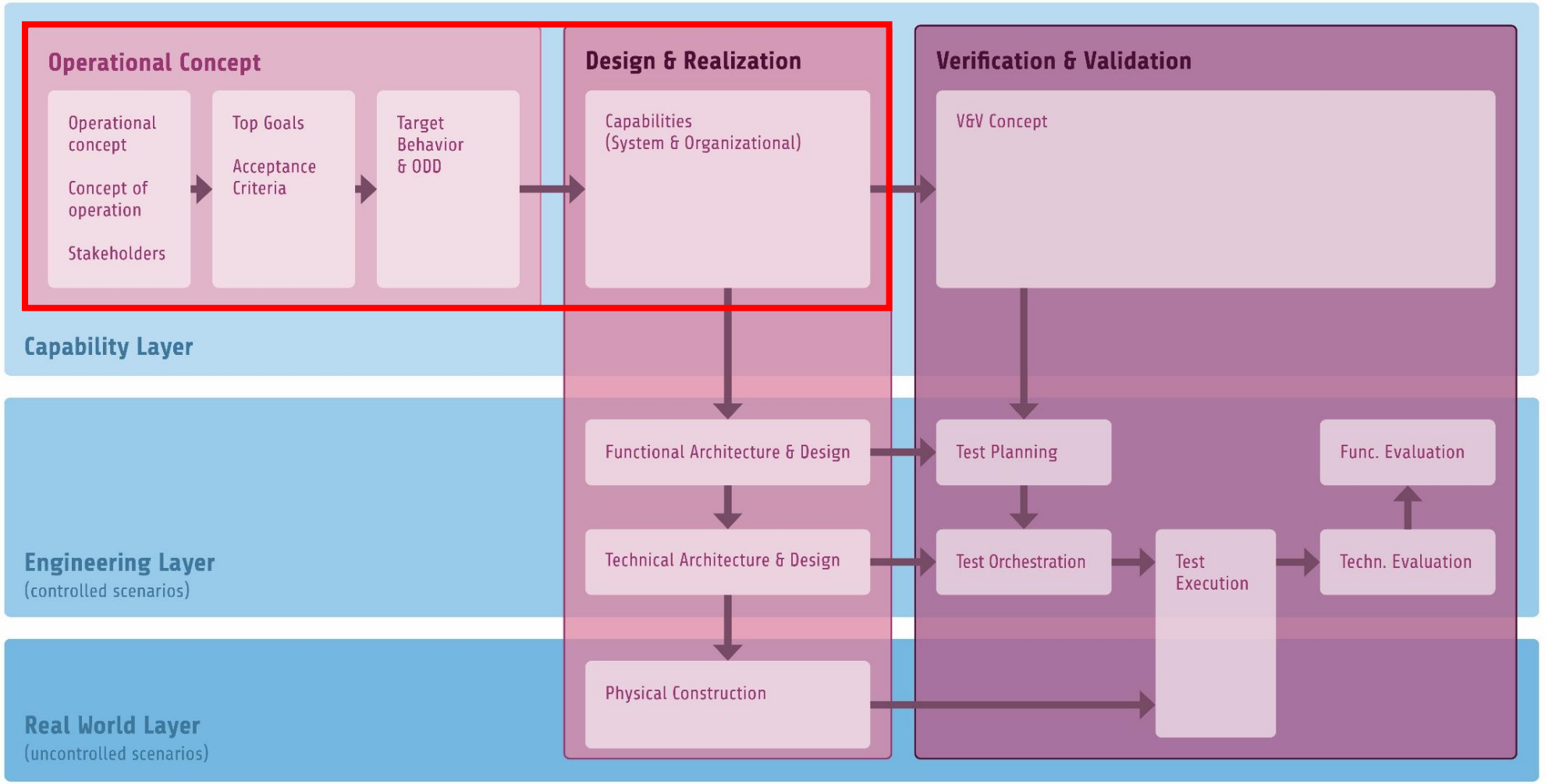
Federal Ministry for Economic Affairs and Climate Action

on the basis of a decision by the German Bundestag

Motivation

- Operating automated driving systems in an **open world** requires **analyses** of their **behavior** in the **operational context** in addition to analyses of the **systems' functionalities**
- **Scenarios** are a means to **structure** the operational context (including residual uncertainties)
- **Traceable** representation of **assumptions** and **decisions** in the life cycle support the **communication of uncertainties**
- This applies to the **behavior specification**
- Therefore we:
  - Elicit **stakeholder needs** towards the behavior of an ADS (e.g., from the traffic code)
  - Specify **behavior** (including behavioral **safety measures**) explicitly
  - Specify required **system capabilities** based on the specification of safe target behavior

What do the approaches presented here contribute to?



Outline

VERIFICATION
VALIDATION
METHODS

Behavior Specification

- How do we address stakeholder needs in the behavior specification in a traceable manner?
- How do we specify behavior in the operational context?
- How do we include safety measures as part of the behavior specification?

Capability Analyses

- How do we specify system capabilities required to exhibit specified behavior?

Outline

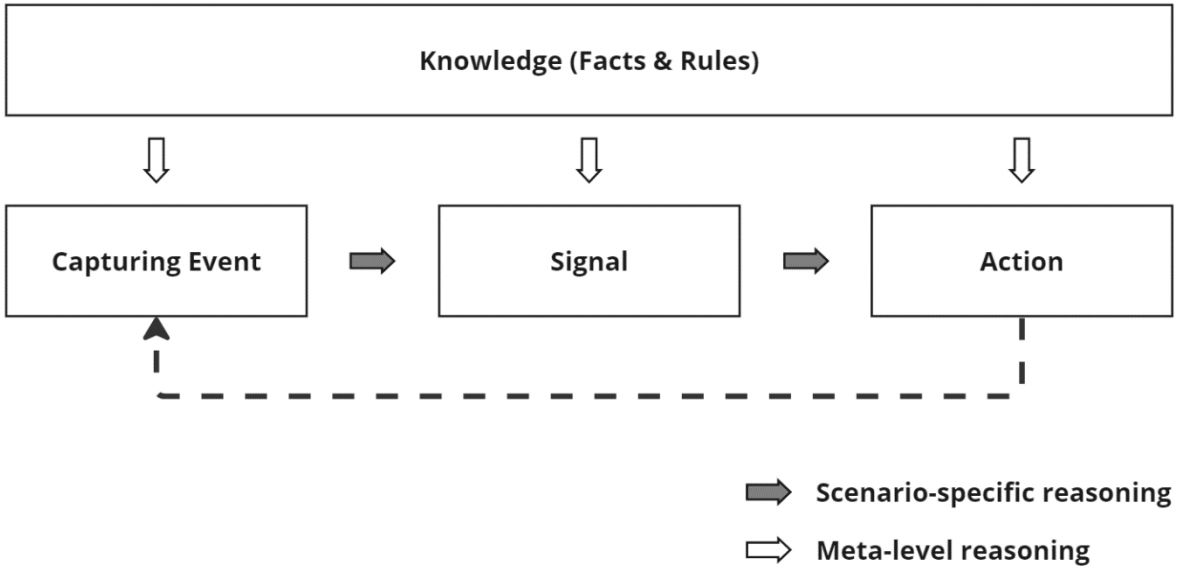
Behavior Specification

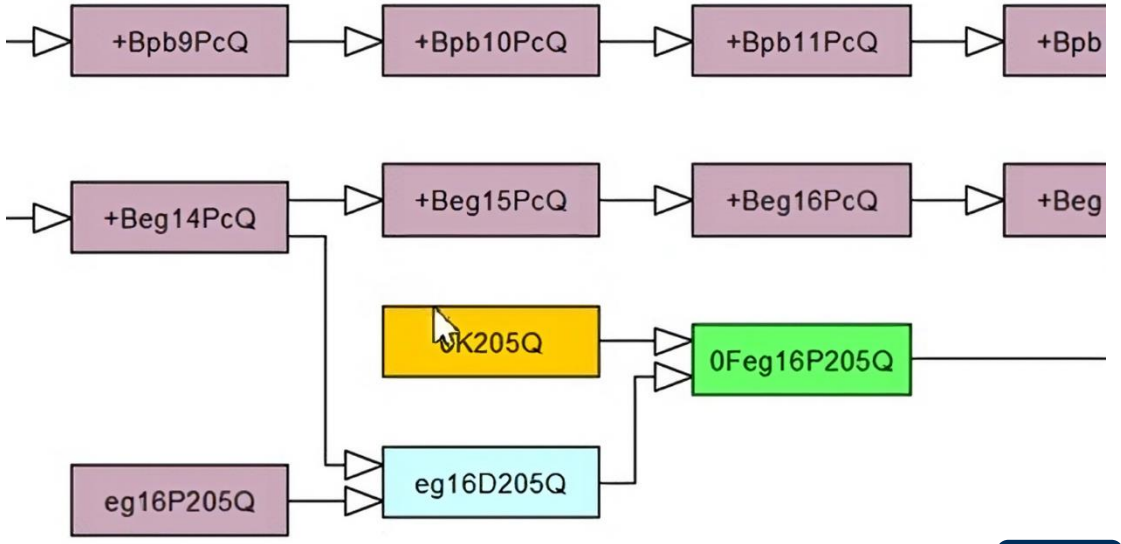
How do we specify behavior in the operational context?

Capability Analyses

How do we specify behavior in the operational context?

- Proposed Method: Phenomenon-Signal Model
  - Supports the explicit consideration of Criticality Phenomena





#10.3
Poster

H. N. Beck, N. F. Salem, V. Haber, M. Rauschenbach, and J. Reich, “Phenomenon-Signal Model: Formalisation, Graph and Application.” arXiv, Jul. 20, 2022. doi: 10.48550/arXiv.2207.09996.

Outline

VERIFICATION
VALIDATION
METHODS

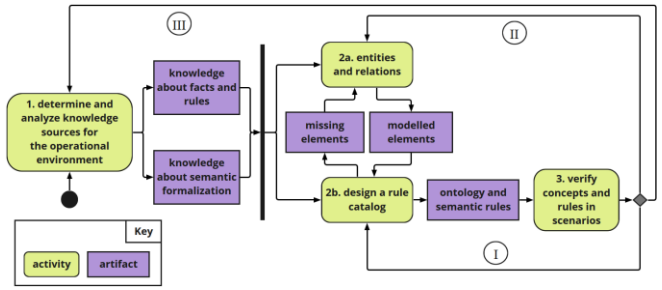
Behavior Specification

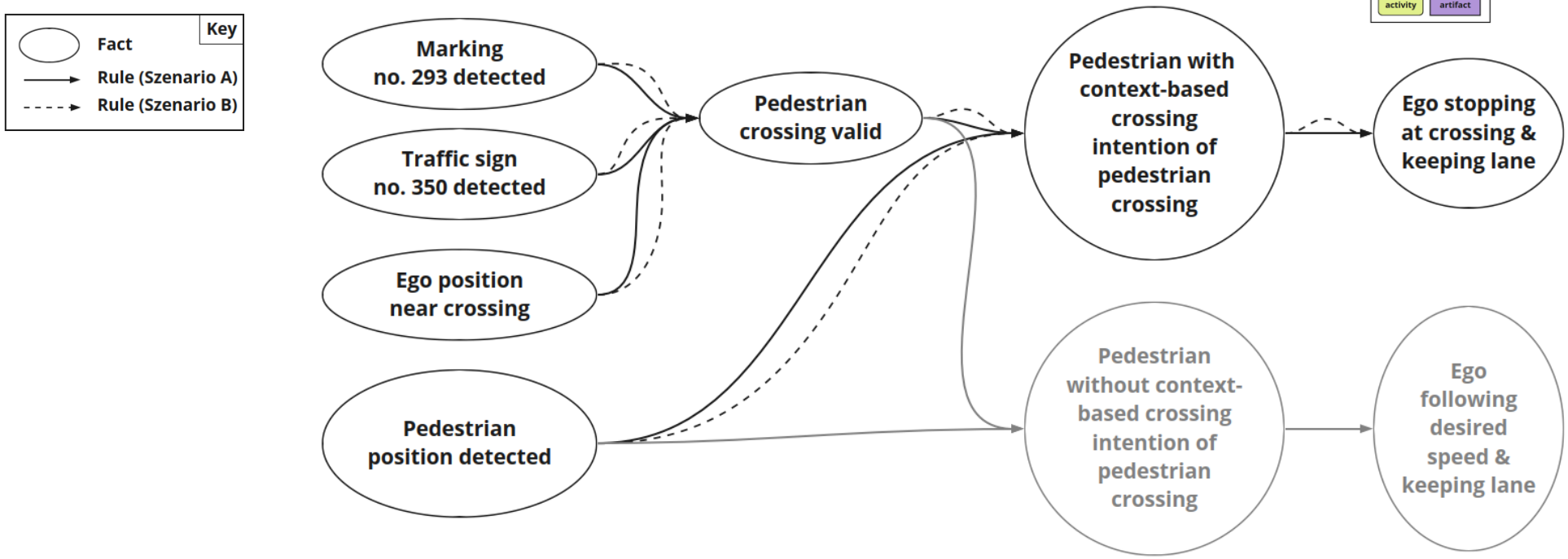
How do we address stakeholder needs in the behavior specification in a traceable manner?

Capability Analyses

How do we include stakeholder needs in the behavior specification in a traceable manner?

- Proposed Method: Semantic Norm Behavior Analysis
  - Terminology: Norm Behavior, Target Behavior
  - Semi-formal representation using ontologies





#10.2
Poster

German paper: N. F. Salem *et al.*, “Ein Beitrag zur durchgängigen, formalen Verhaltensspezifikation automatisierter Straßenfahrzeuge.” arXiv, Sep. 15, 2022. doi: 10.48550/arXiv.2209.07204.

Outline

VERIFICATION
VALIDATION
METHODS

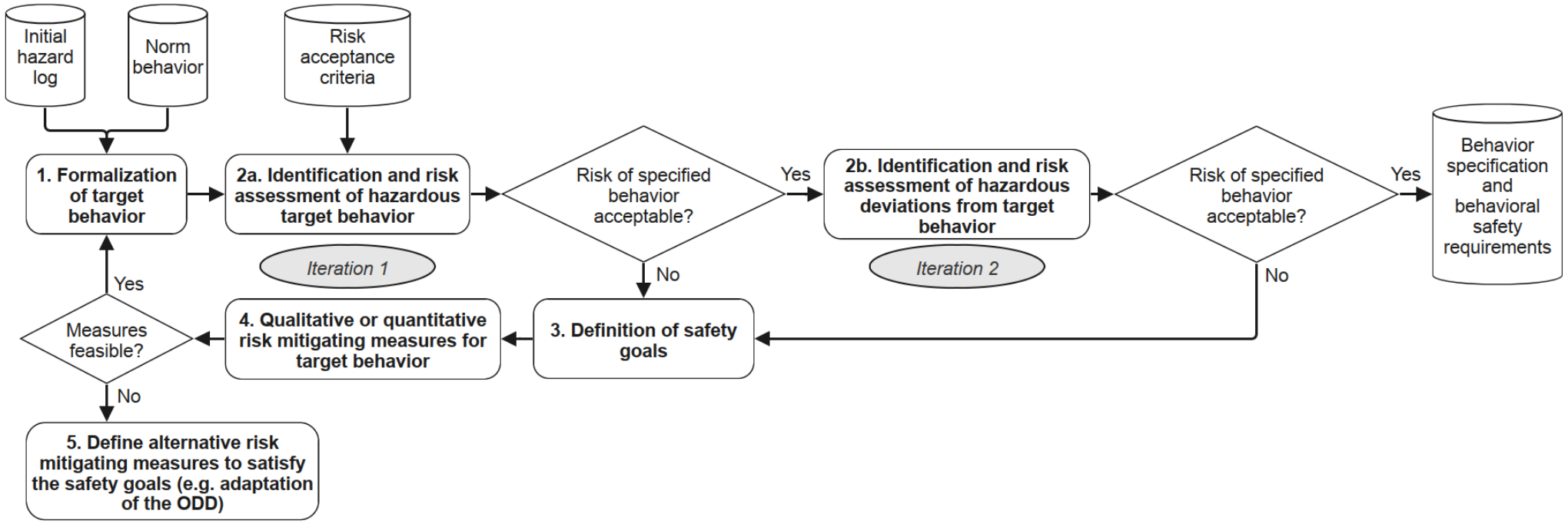
Behavior Specification

How do we include safety measures as part of the behavior specification?

Capability Analyses

How do we include safety measures as part of the behavior specification?

- Proposed Method: Risk-based Refinement of the Functional Specification
  - Based on the Risk Management Core → next talk
  - Supports the creation of a Behavioral Safety Concept



N. F. Salem *et al.*, "Risk Management Core -- Towards an Explicit Representation of Risk in Automated Driving." arXiv, Feb. 15, 2023. doi: 10.48550/arXiv.2302.07715.

#10.4
Poster

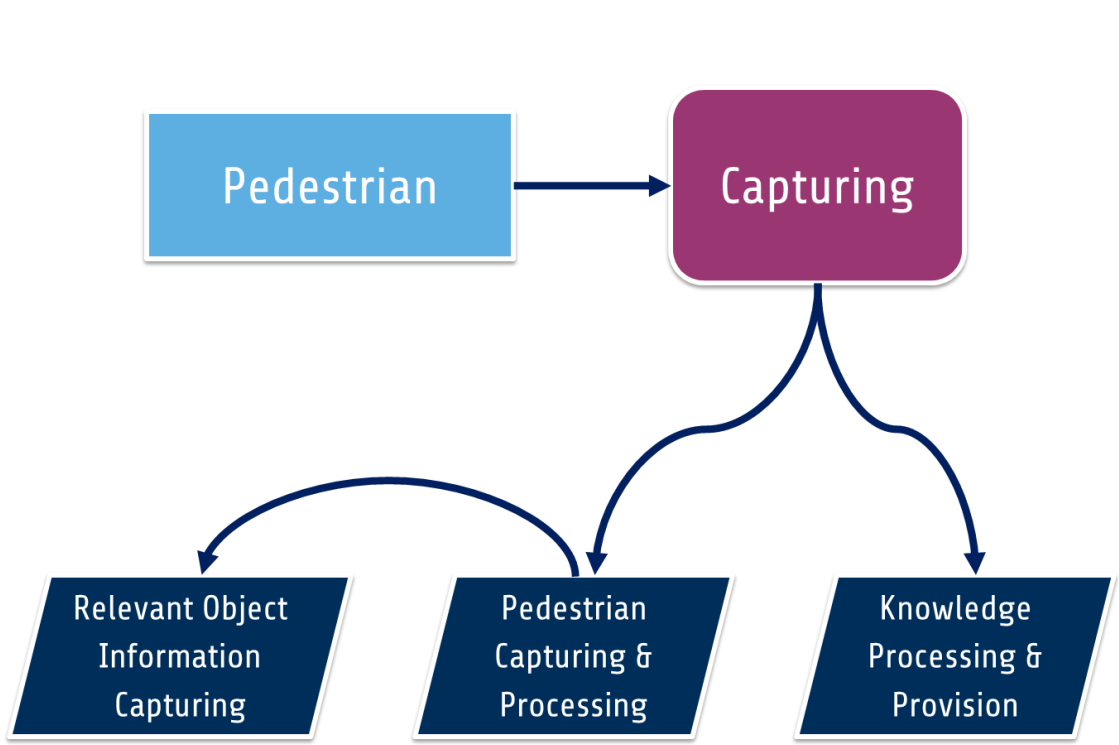
Outline

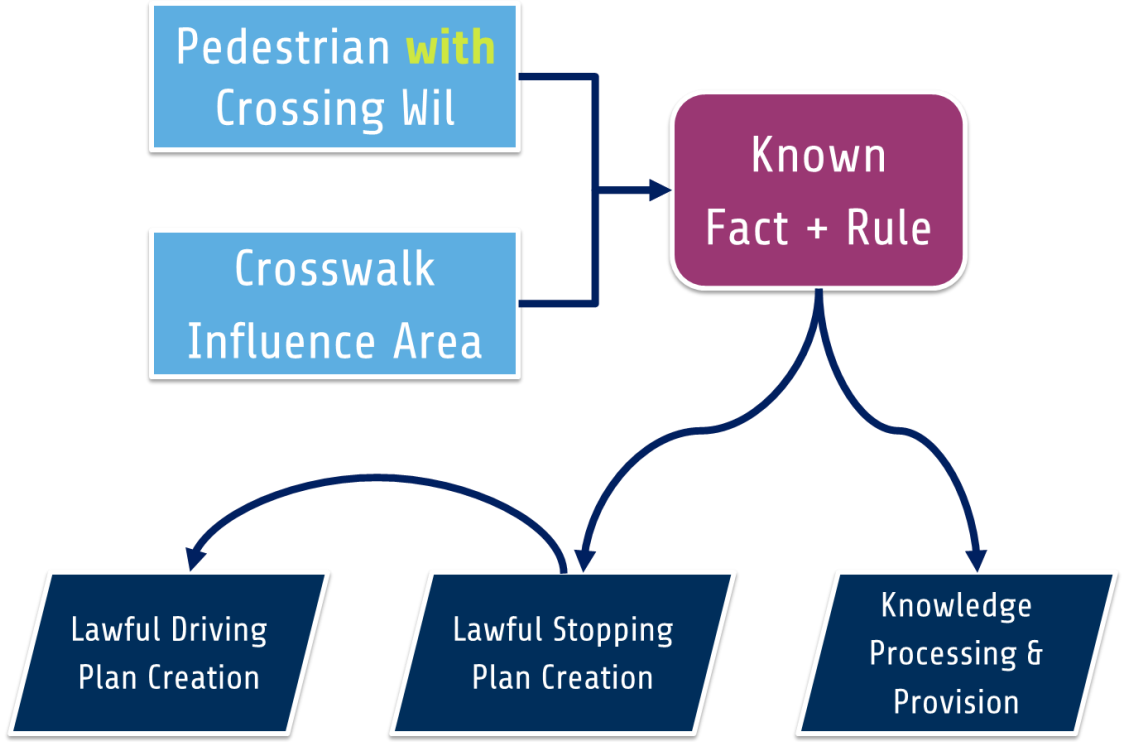
Behavior Specification

Capability Analyses

How do we specify system capabilities required to exhibit specified behavior?

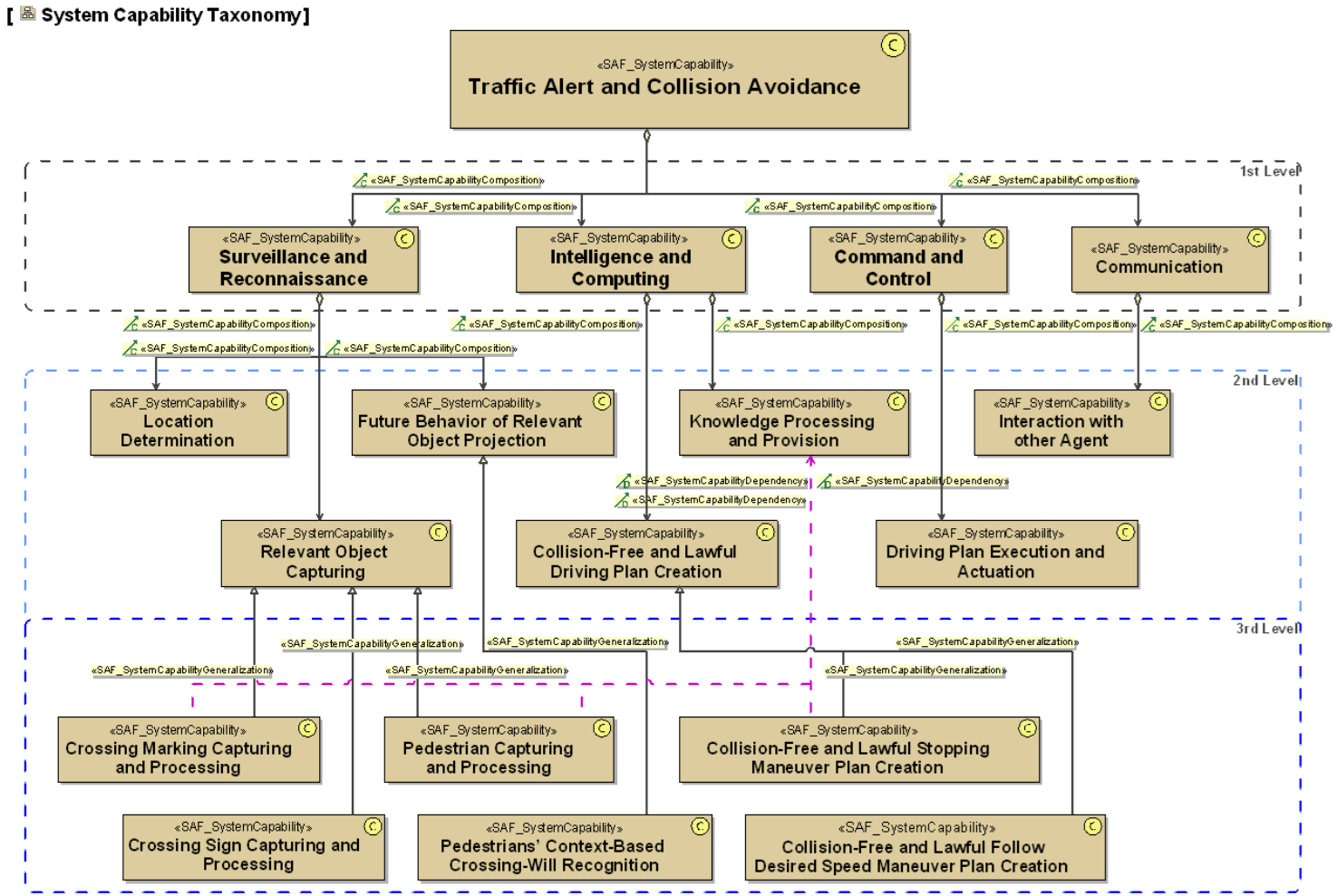
How do we specify system capabilities required to exhibit specified behavior?





Research publications planned

How do we specify system capabilities required to exhibit specified behavior?



Research publications planned

#10.6 Poster

#10.7 Poster

Summary

- VVMethods proposes **methods** to **support traceable specifications** focusing on the **operational context**
  - Traceability from **stakeholder needs to the behavior specification** is supported by the **Semantic Norm Behavior Analysis** and the **Phenomenon-Signal Model**
  - Traceability from the **behavior specification to the system design** is supported by a structured **specification of system capabilities**
- How do these approaches contribute to the absence of unreasonable risk?
  - The **absence of a driver** requires an **argumentation** for why an **ADS is able to behave safely** in its environment. The **proposed methods** provide **evidences** for such an argumentation.

VERIFICATION
VALIDATION
METHODS

Thank you!

Nayel Fabian Salem, Technische Universität Braunschweig (Institute of Control Engineering)
n.salem@tu-bs.de

Marcus Nolte, Technische Universität Braunschweig (Institute of Control Engineering)
Christian Lalitsch-Schneider, ZF Friedrichshafen AG

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