SAFETYUPDATE

PROJECT of the PEGASUS FAMILY

VERIFICATION
VALIDATION
METHODS

Veronica Haber

Systems Engineering Consultant

PROSTEP AG

Nayel Fabian Salem

Research Associate

TU Braunschweig, Institute of Control Engineering

May 18 – 19, 2022|Würzburg

SAFETYUPDATE

Contributions of VVM to the safety assurance of ADS – insights on specifying behavior and capabilities

Nayel Fabian Salem, Veronica Haber

PROJECT of the PEGASUS FAMILY

VERIFICATION
VALIDATION
METHODS

May 18 – 19, 2022 | Würzburg

carhs Empowering Engineers

Motivation

[1] U. Eberle, “From PEGASUS to VVM - Where do we come from and why the PEGASUS Journey has not yet reached its Final Destination,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.

- SAE Level 2 System
  - Partial Driving Automation

- SAE Level 3/4/5 Automated Driving System
  - ADS-equipped vehicle

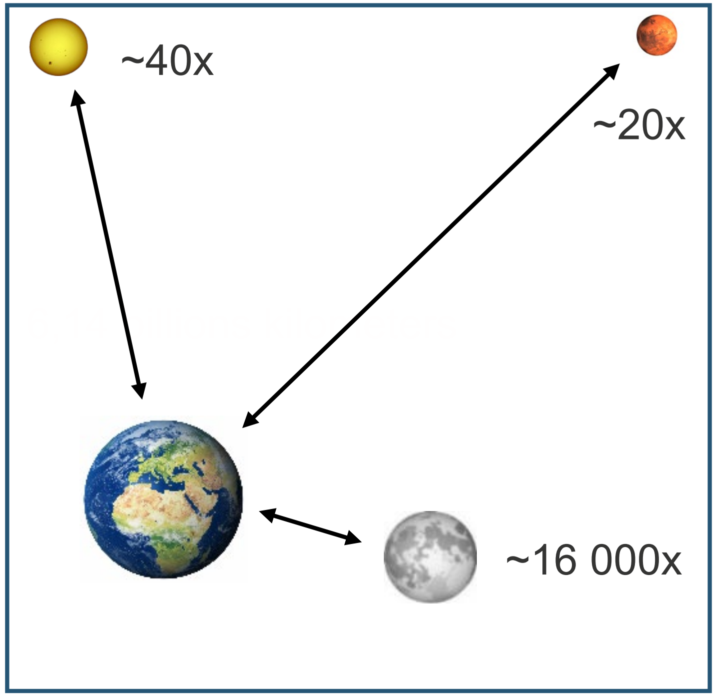
ADS engaged

Object and Event Detection and
Response **OEDR** transferred

Need of validation and safety proof of the vehicle **+ intended functionality of automated driving system within predefined operational design domain**

[1] U. Eberle, “From PEGASUS to VVM - Where do we come from and why the PEGASUS Journey has not yet reached its Final Destination,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.

Hypothesis	Less accidents with fatalities than the average human driver
	614 million kilometers between two fatal accidents by humans
Result	Required test distance → > 6.1 billions kilometers
Challenge	Each system modification requires a re-run of all tests



Distance-based test approach is **NOT FEASIBLE** for automated driving functions
A systematic **SCENARIO-BASED TEST APPROACH** is needed

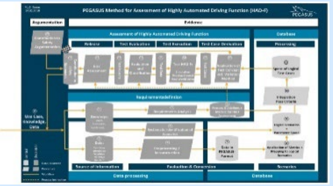
- The **PEGASUS Family** focuses on development / testing methods and tools for AD systems on highways and in urban environments

PEGASUS

https://www.pegasusprojekt.de/en/home

PEGASUS

- Scope: **Basic methodological framework**
- Use-Case: L3/4 on highways
- Partners: 17



+

PEGASUS FAMILY

VV-Methods

VERIFICATION
VALIDATION
METHODS

- Scope: **Methods, toolchains, specifications for technical assurance**
- Use-Case: L3/4/5 in urban environments
- Partners: 23 partners
- Timeline: 07/2019 – 06/2023

SET Level 4to5

SET Level 4to5

- Scope: **Simulation platform, toolchains, definitions for simulation-based testing**
- Use-Case: L3/4/5 in urban environments
- Partners: 20 partners
- Timeline: 03/2019 – 10/2022

+ future projects of the PEGASUS Family

2016

2019

Time

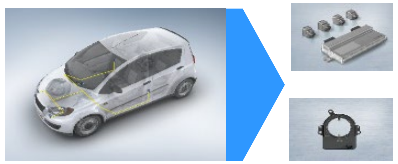
[2] R. Galbas, “VVM Main Approach - How to Systematically Release AD Systems,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.

I. Systematic control of test space

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

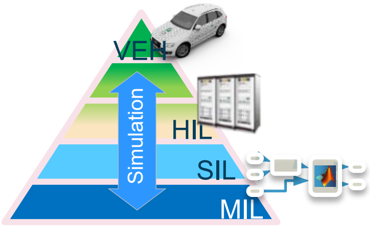
II. Consistent interfaces for systems and components

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.



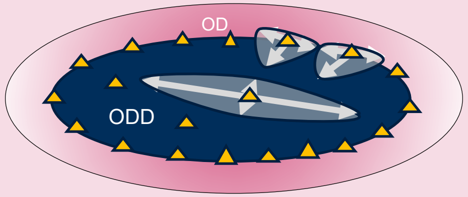
Added: IV Argumentation

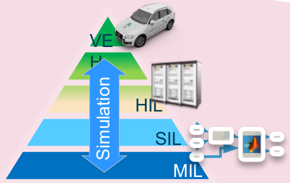
- fulfillment of societal claims e.g. safety, via law, standards, state of the art.

[2] R. Galbas, “VVM Main Approach - How to Systematically Release AD Systems,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.

Goal IV – **Argumentation**

⚖ Explainable Compliance

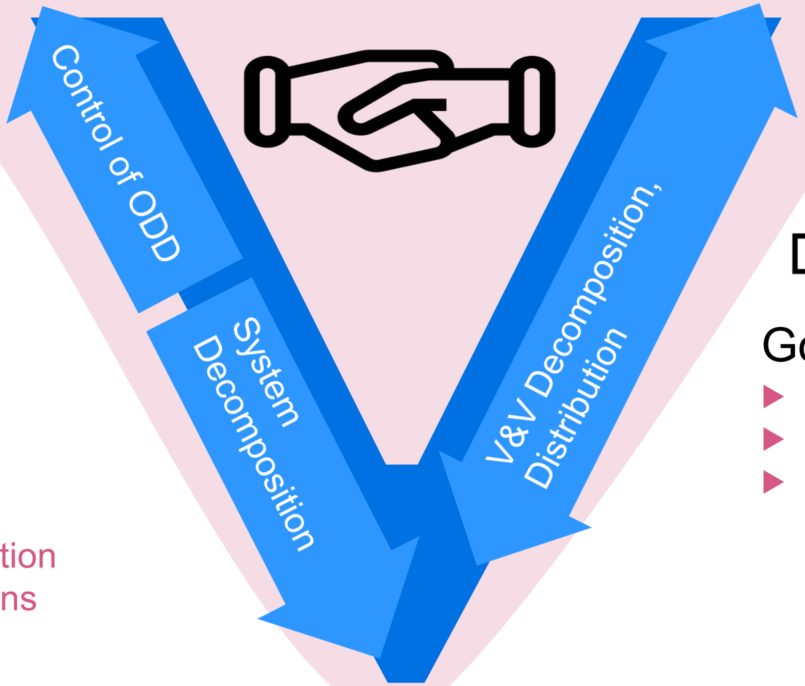




✓ Feasibility

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

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



Efficiency

Goal III – **shift to simulation**

- System Monitoring and Assessment
- Structured Data Handling
- …

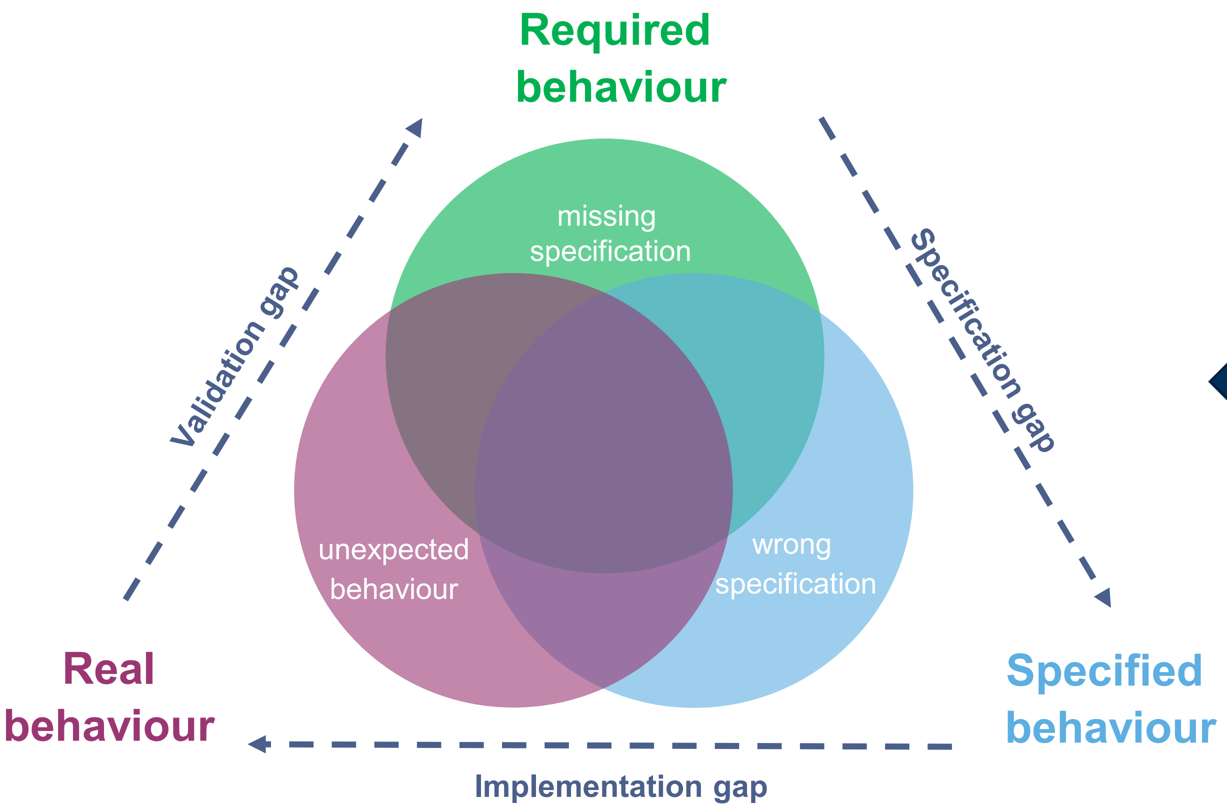
Changeability

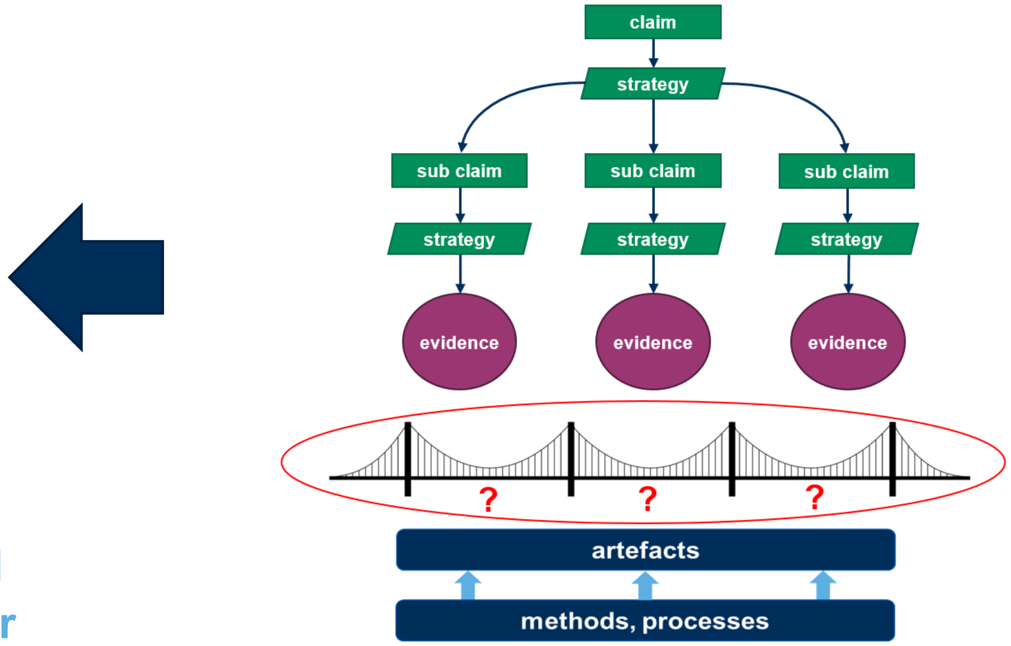
Goal II – **Consistent interfaces**

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

[3] J. E. Stellet, T. Brade, A. Poddey, S. Jesenski, and W. Branz, “Formalisation and algorithmic approach to the automated driving validation problem,” in 2019 IEEE Intelligent Vehicles Symposium (IV), Jun. 2019, pp. 45–51. doi: 10.1109/IVS.2019.8813894.

[4] J. Reich and M. Nolte, “VVM Assurance Argumentation - How to Systematically Organize the Approval Concerns for Safe AD Systems in a Structured Framework,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.

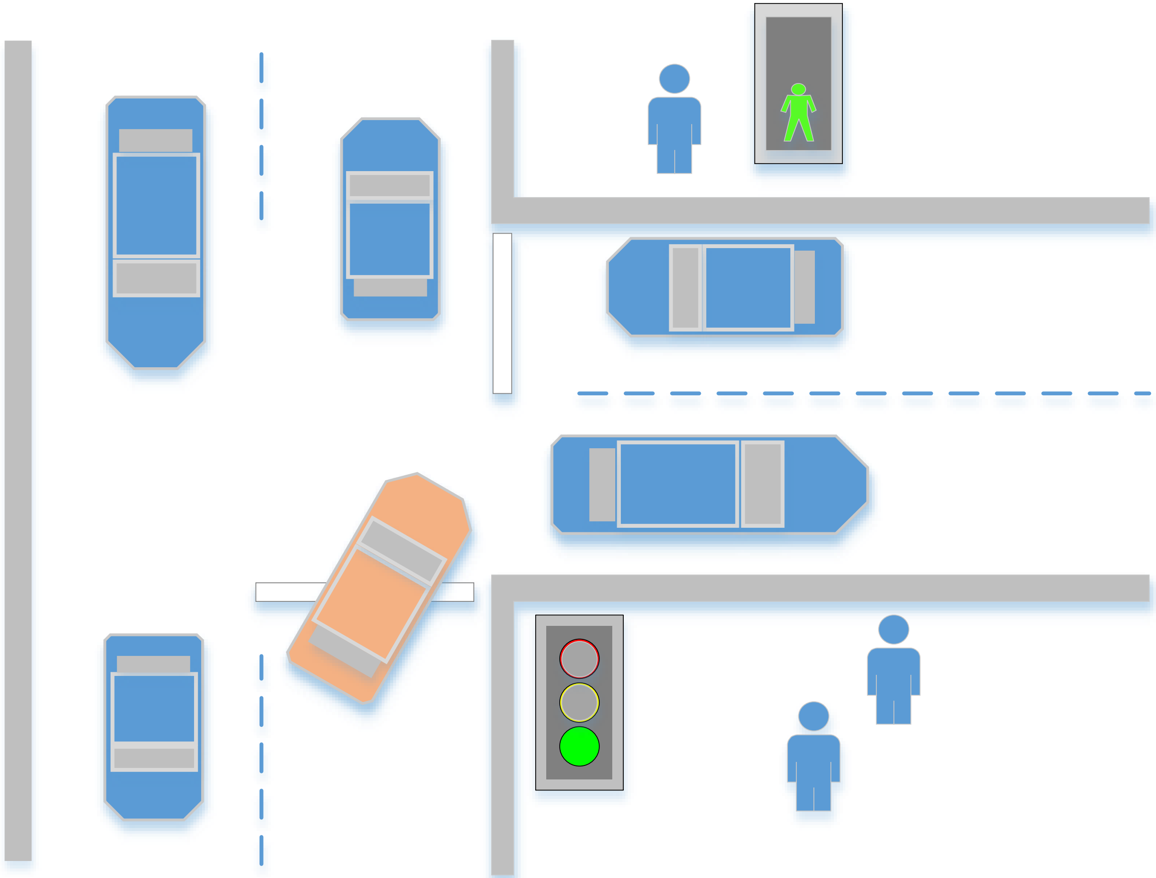




How does VVM approach these gaps?

Today’s focus: the specification gap

[5] H. N. Beck and N. F. Salem, “Contributions to a Traceable Behavior Specification for Automated Driving Systems Using Formal Methods,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.



Where could concerns come from?

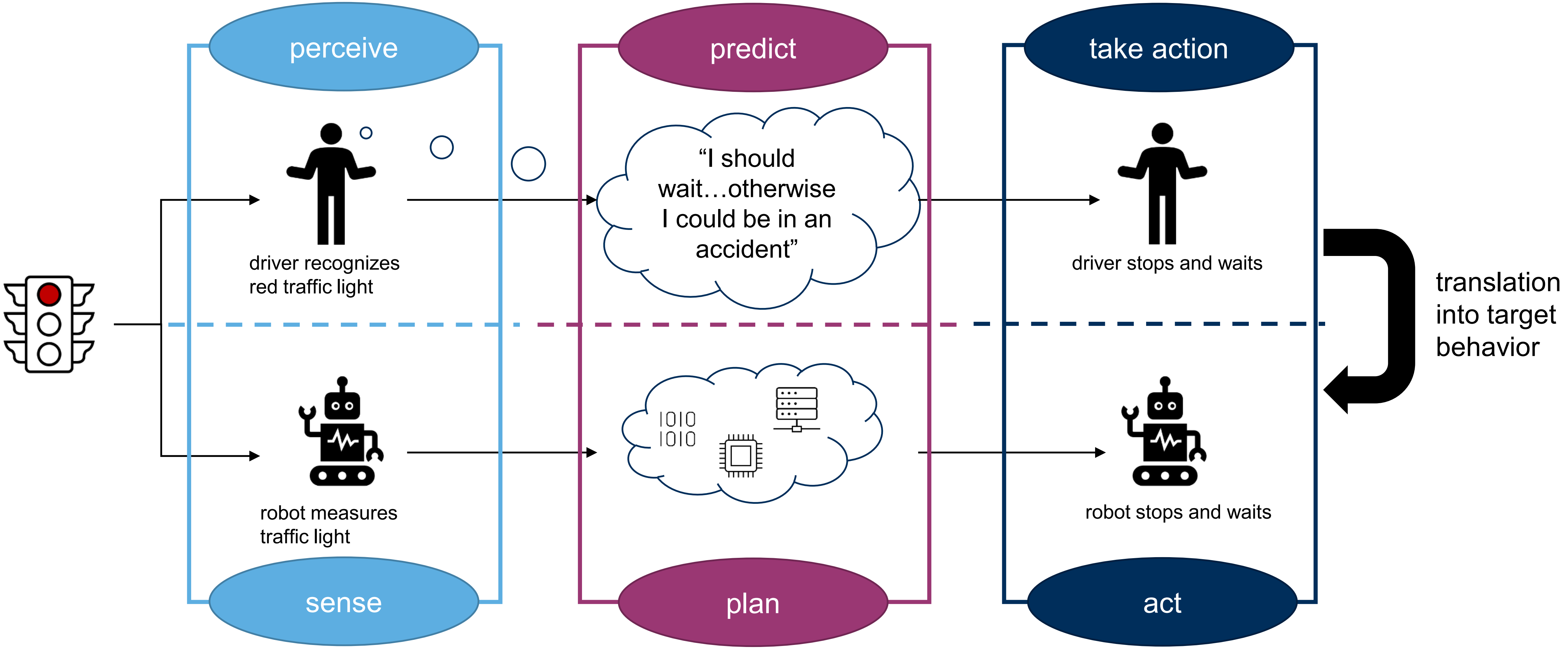
- ⚖ societal expectations
- legal regulations
- traffic signs
- other traffic participants

[5] H. N. Beck and N. F. Salem, “Contributions to a Traceable Behavior Specification for Automated Driving Systems Using Formal Methods,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.

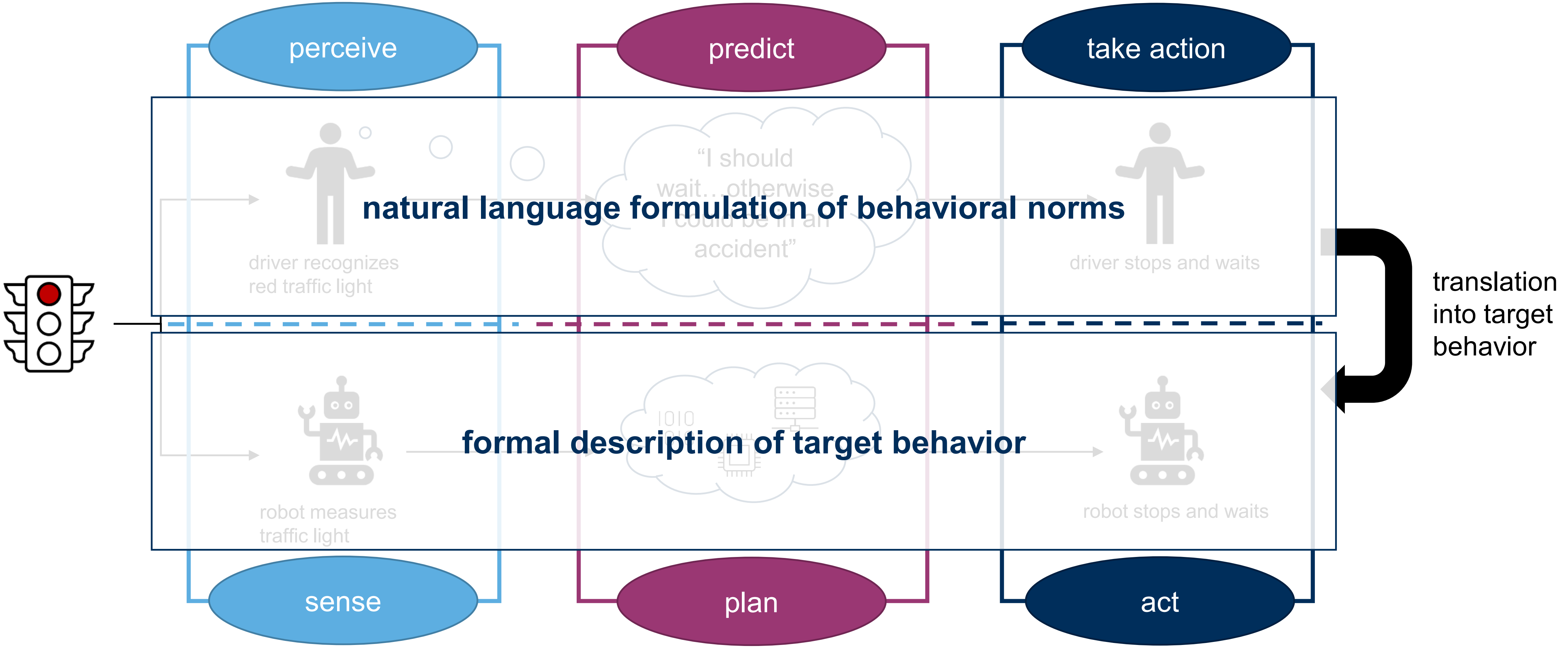
Conformity with rules of the road is one of our key concerns.

We need to do more in order to assure safety!

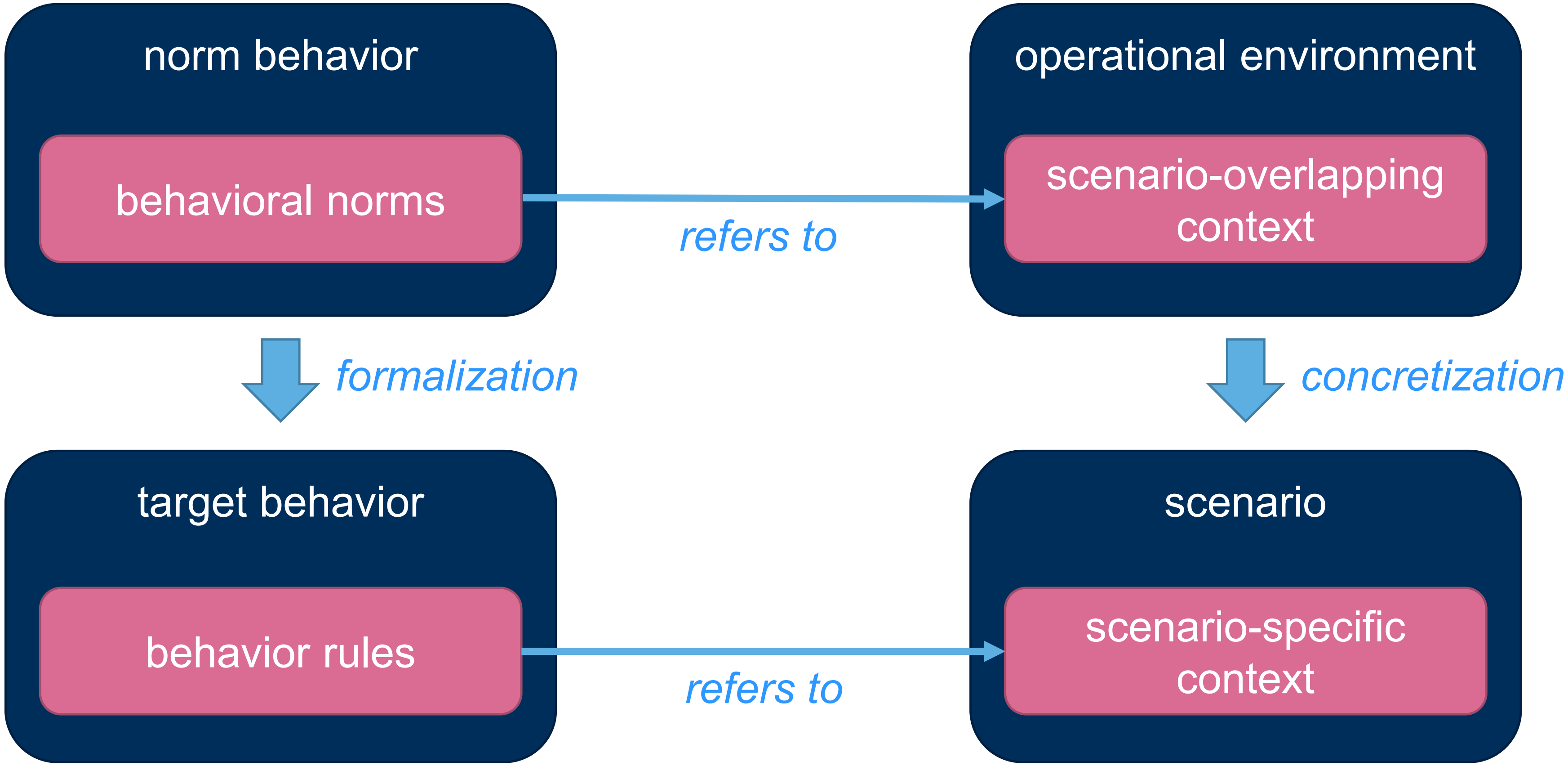
[5] H. N. Beck and N. F. Salem, “Contributions to a Traceable Behavior Specification for Automated Driving Systems Using Formal Methods,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.


perceive
predict
take action
driver recognizes red traffic light
“I should wait…otherwise I could be in an accident”
driver stops and waits
translation into target behavior
robot measures traffic light
IOIO
IOIO
robot stops and waits
sense
plan
act

[5] H. N. Beck and N. F. Salem, “Contributions to a Traceable Behavior Specification for Automated Driving Systems Using Formal Methods,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.

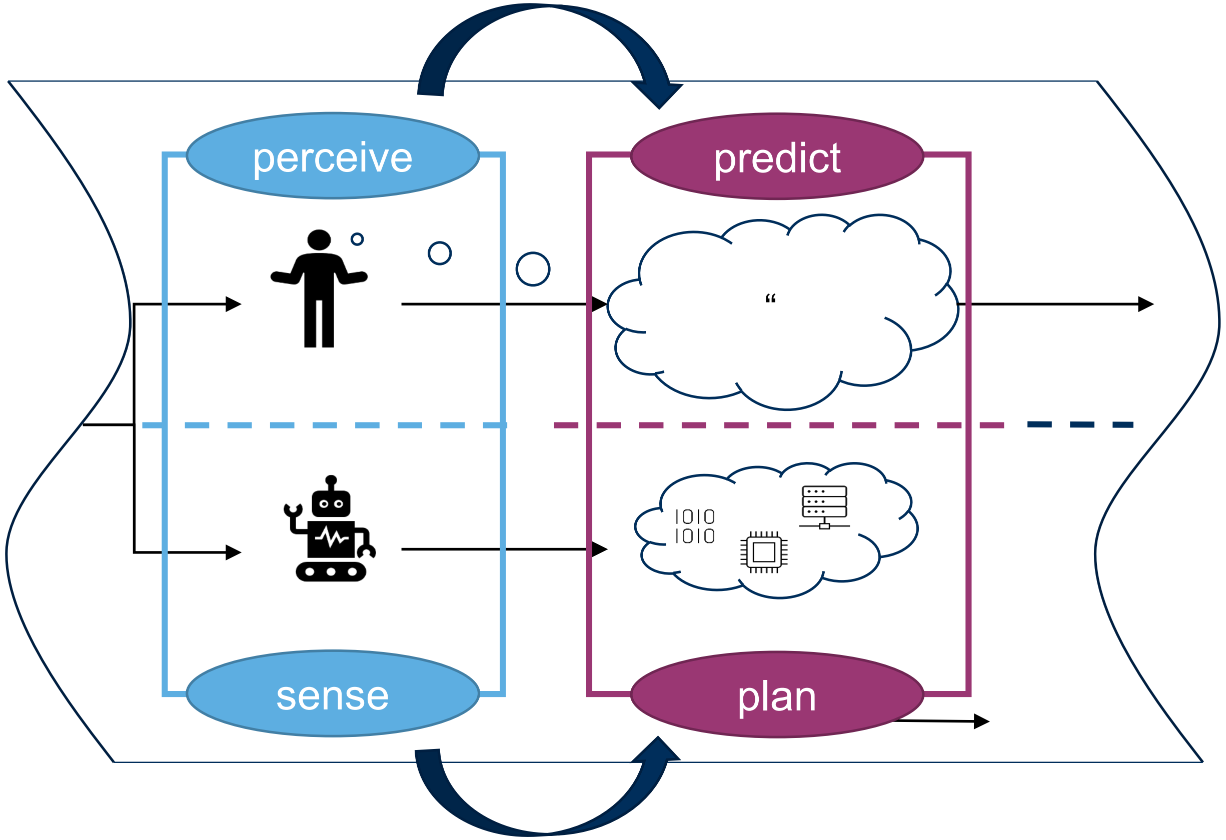

perceive
predict
take action
driver recognizes red traffic light
“I should wait… otherwise I could be in an accident”
driver stops and waits
natural language formulation of behavioral norms
translation into target behavior
IOIO
formal description of target behavior
robot measures traffic light
robot stops and waits
sense
plan
act

[5] H. N. Beck and N. F. Salem, “Contributions to a Traceable Behavior Specification for Automated Driving Systems Using Formal Methods,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.



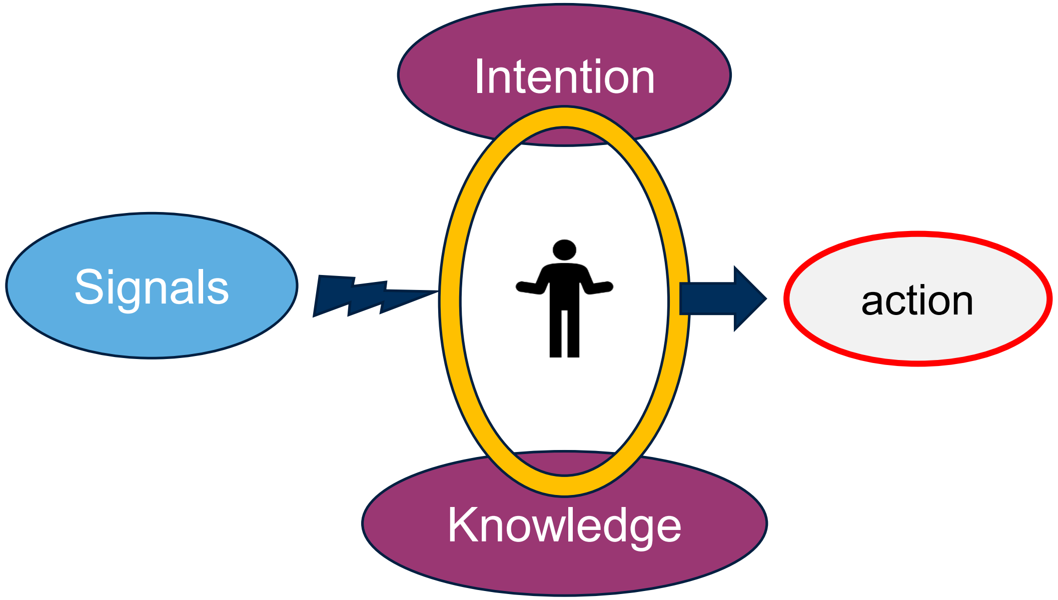
[5] H. N. Beck and N. F. Salem, “Contributions to a Traceable Behavior Specification for Automated Driving Systems Using Formal Methods,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.

Model this…



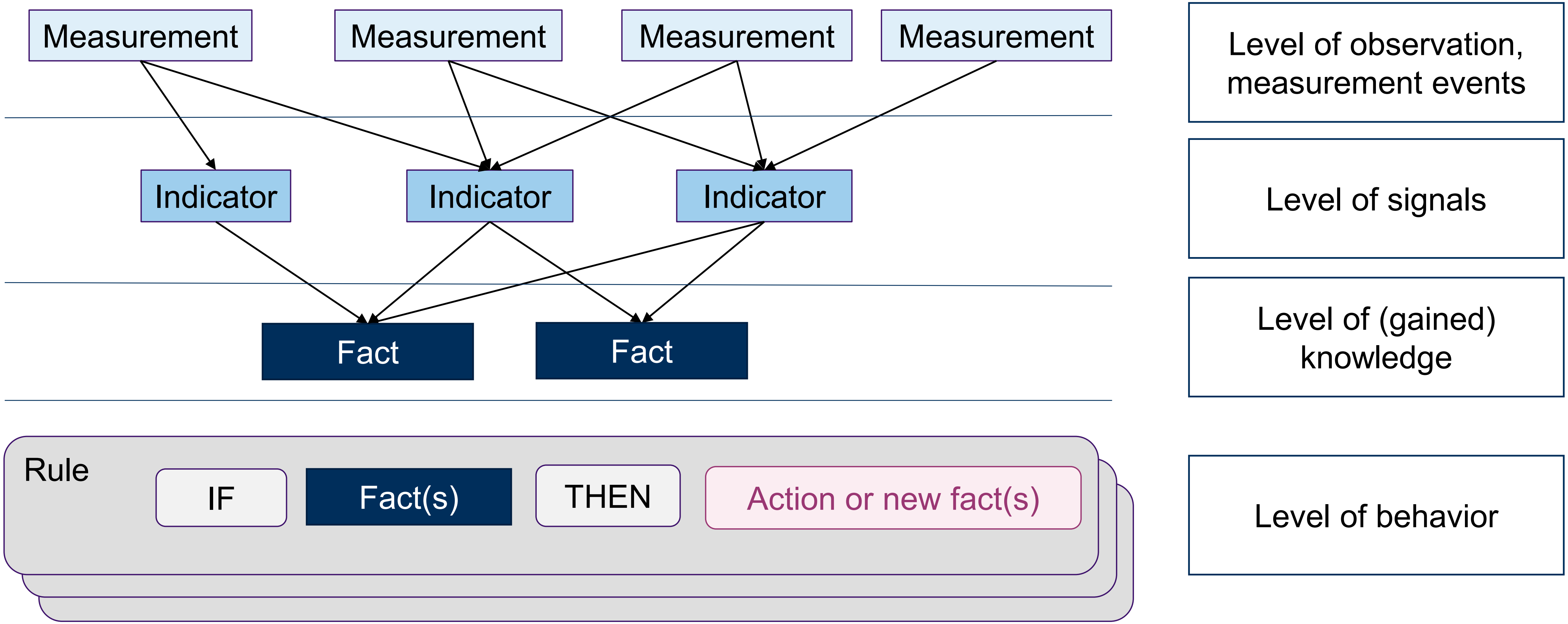
…. to get that

Starting point: Phenomenology by Edmund Husserl



These factors are relevant to derive a model

[5] H. N. Beck and N. F. Salem, “Contributions to a Traceable Behavior Specification for Automated Driving Systems Using Formal Methods,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.



Level of observation, measurement events

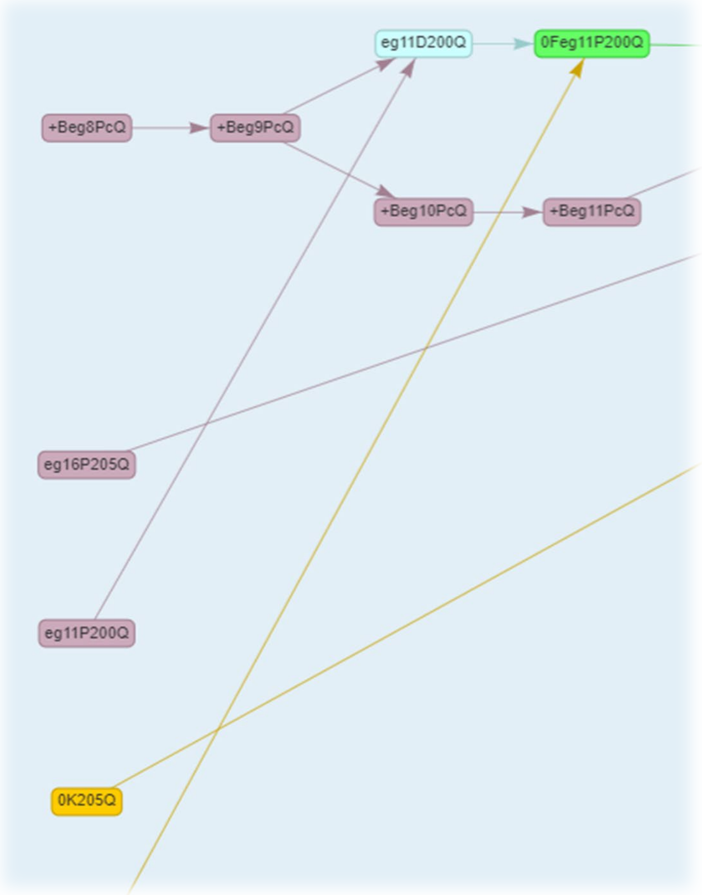
Level of signals

Level of (gained) knowledge

Level of behavior

Phenomenon-Signal-Model

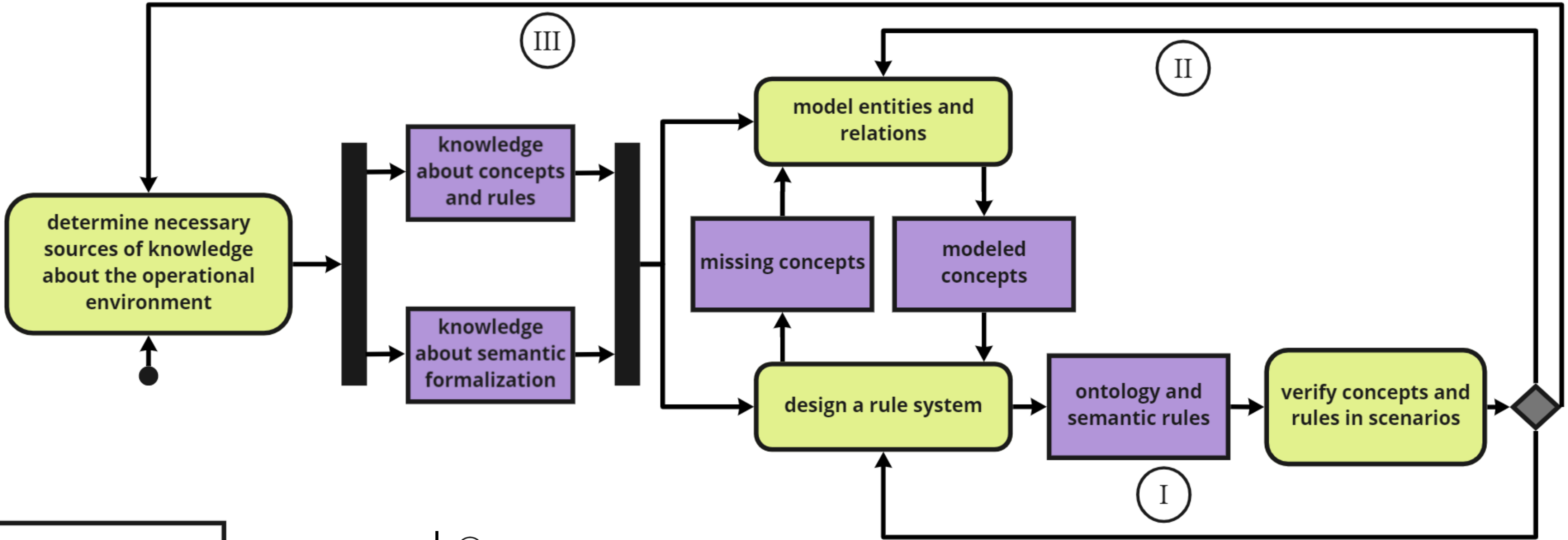
[5] H. N. Beck and N. F. Salem, “Contributions to a Traceable Behavior Specification for Automated Driving Systems Using Formal Methods,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.



The Phenomenon-Signal-Model

- describes target behavior as a set of rules and facts
- represents these concepts in a traceable manner
- facilitates a formalized analysis (and optimization) of target behavior in a scenario catalogue

[5] H. N. Beck and N. F. Salem, “Contributions to a Traceable Behavior Specification for Automated Driving Systems Using Formal Methods,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.


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

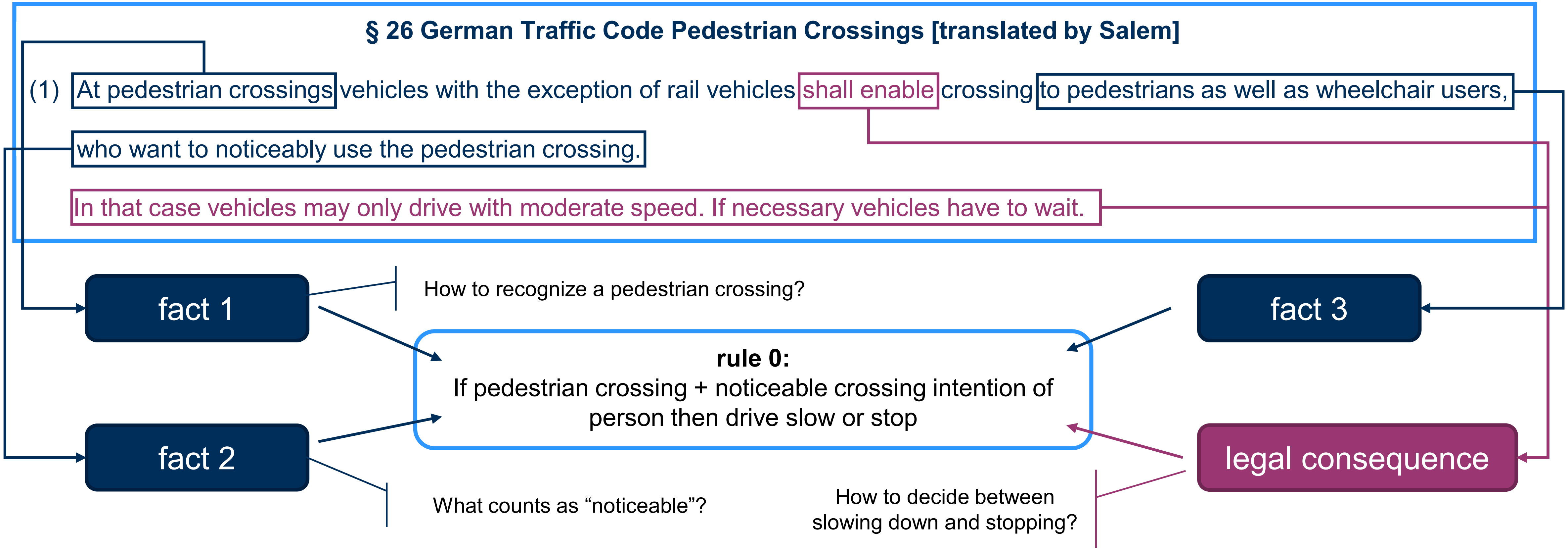
Key

- 🟩 activity
- 🟪 artefact

Iterations

- I adapt false rules
- II adapt false concepts
- III adapt false knowledge sources

[5] H. N. Beck and N. F. Salem, “Contributions to a Traceable Behavior Specification for Automated Driving Systems Using Formal Methods,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.



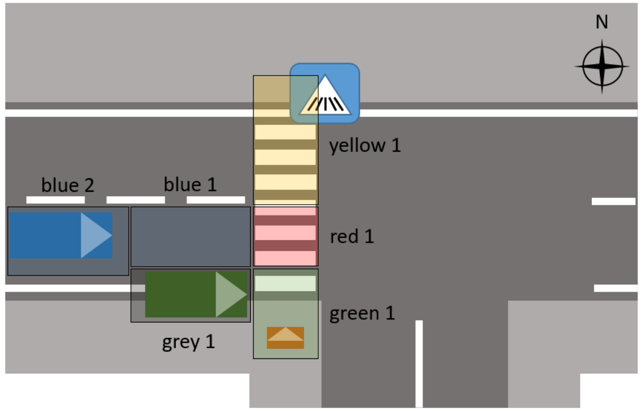
§ 26 German Traffic Code Pedestrian Crossings [translated by Salem]

(1) At pedestrian crossings vehicles with the exception of rail vehicles shall enable crossing to pedestrians as well as wheelchair users, who want to noticeably use the pedestrian crossing. In that case vehicles may only drive with moderate speed. If necessary vehicles have to wait.

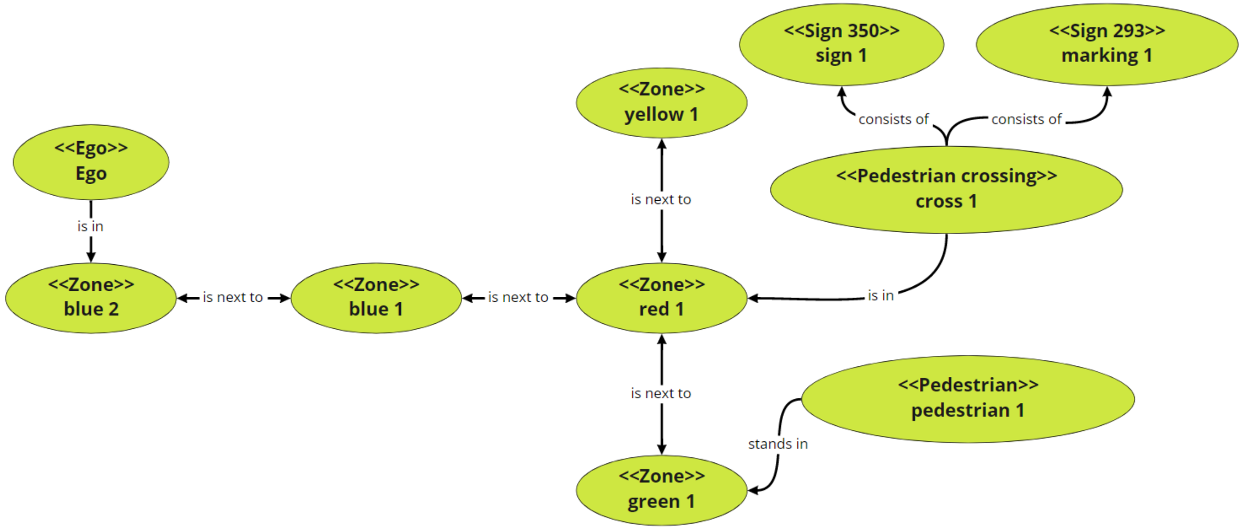
fact 1
How to recognize a pedestrian crossing?
fact 3
rule 0:
If pedestrian crossing + noticeable crossing intention of person then drive slow or stop
fact 2
legal consequence
What counts as “noticeable”?
How to decide between slowing down and stopping?

[5] H. N. Beck and N. F. Salem, “Contributions to a Traceable Behavior Specification for Automated Driving Systems Using Formal Methods,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.

Scene



Ontology

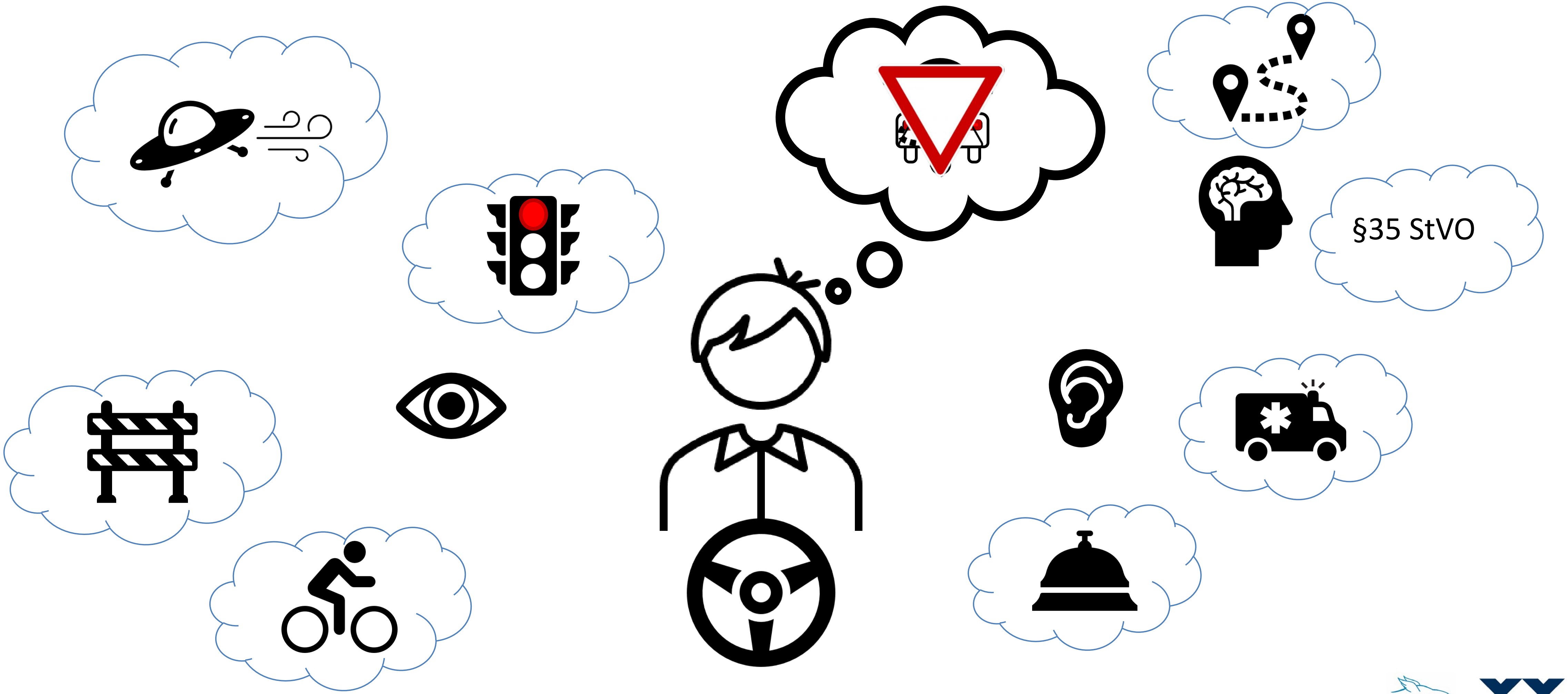


Inference rule

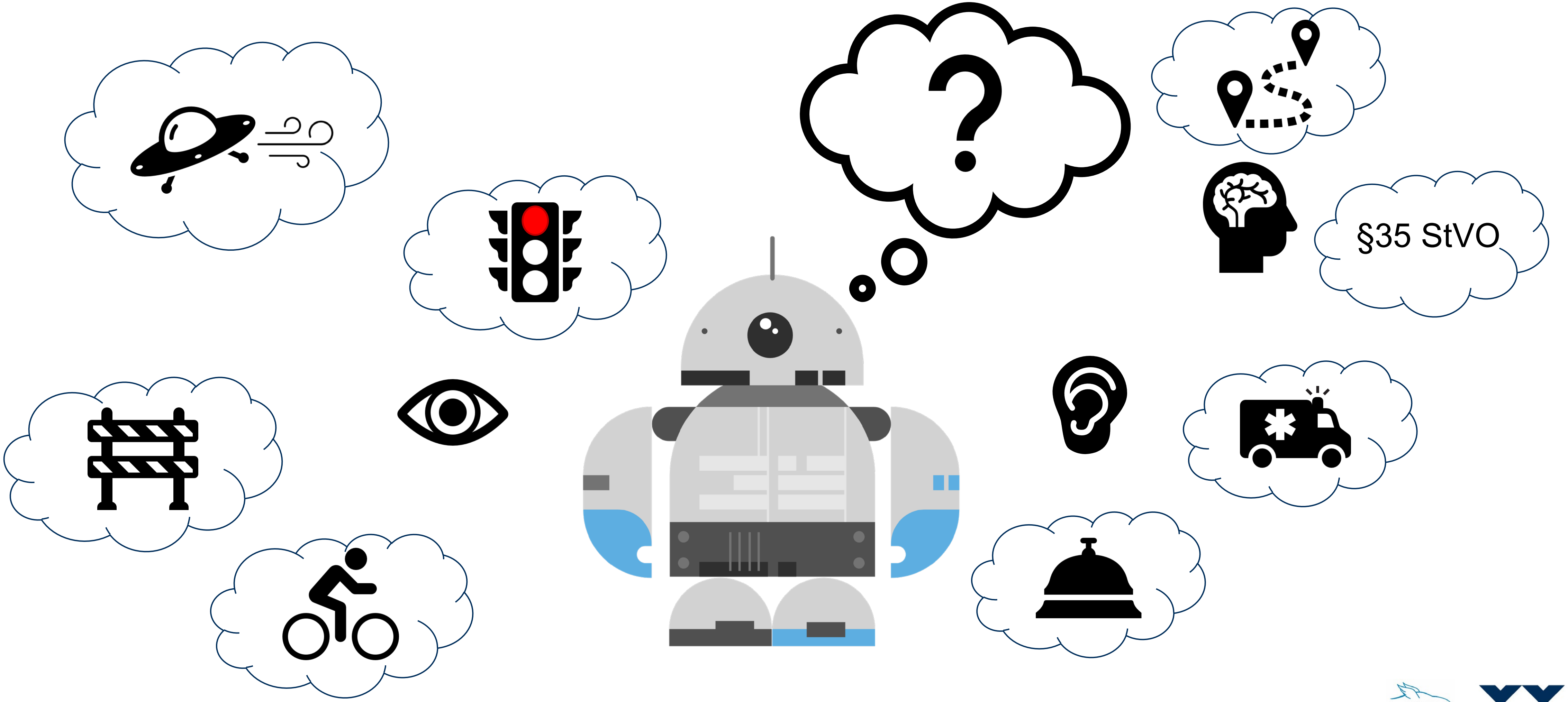
Natural language rule	SWRL rule
If sign and marking **then** valid pedestrian crossing	Pedestrian_crossing(?cross) Λ sign_350(?sign) Λ sign_293(?marking) Λ is_fact(?sign, true) Λ is_fact(?marking, true) Λ consists_of(?cross, ?sign) Λ consists_of(?cross, ?marking) → is_fact(?cross, true)

How could a behavior specification be utilized in further systems engineering activities?

[6] T. Hofmann, “Capability-based Architecture for Automated Vehicles in Urban Environment,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.



[6] T. Hofmann, “Capability-based Architecture for Automated Vehicles in Urban Environment,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.



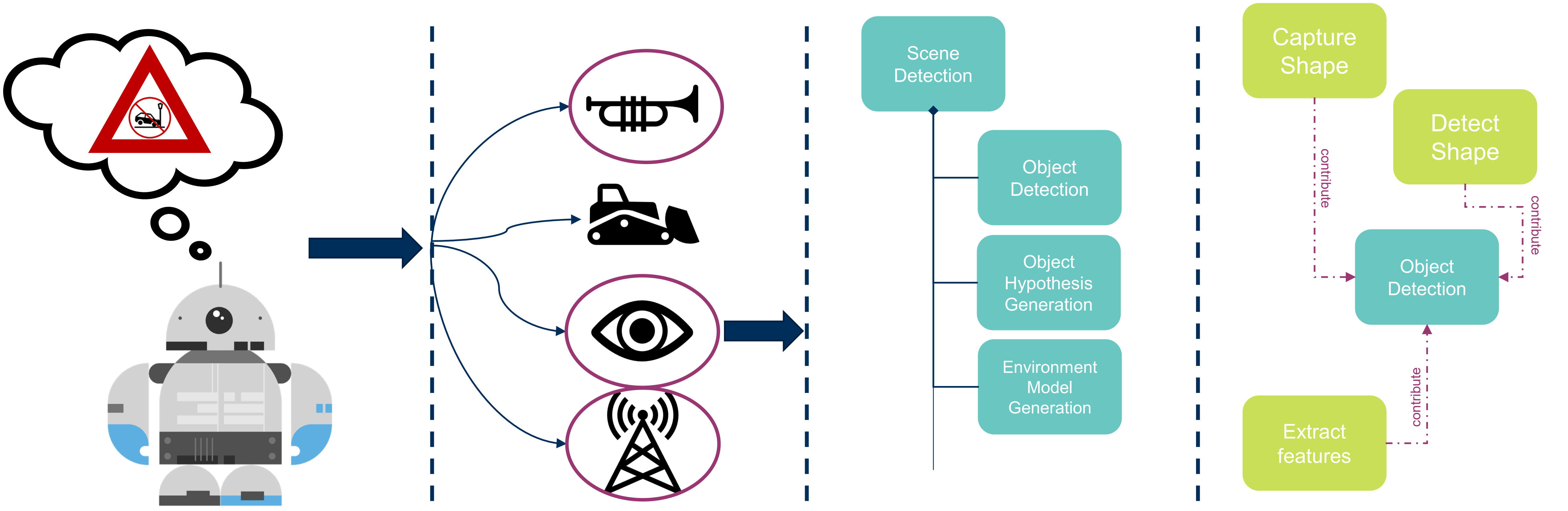
[6] T. Hofmann, “Capability-based Architecture for Automated Vehicles in Urban Environment,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.

- Our current traffic system is an **open system**
- We have to deal with **uncertainty** and **incompleteness**
  - Today the human driver must be capable to deal with these
  - In Future the ADS equipped vehicle must be capable to **operate in this open context**
- How to argue that safety case will remain valid, even if **system context changes**.
- The expected behavior has to be addressed also in systems architecture

→ Modeling capabilities as an approach to enable argumentation on an abstract level

„slicing the elephant“

[6] T. Hofmann, “Capability-based Architecture for Automated Vehicles in Urban Environment,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.



Scene Detection

Object Detection

Object Hypothesis Generation

Environment Model Generation

Capture Shape

Detect Shape

Object Detection

Extract features

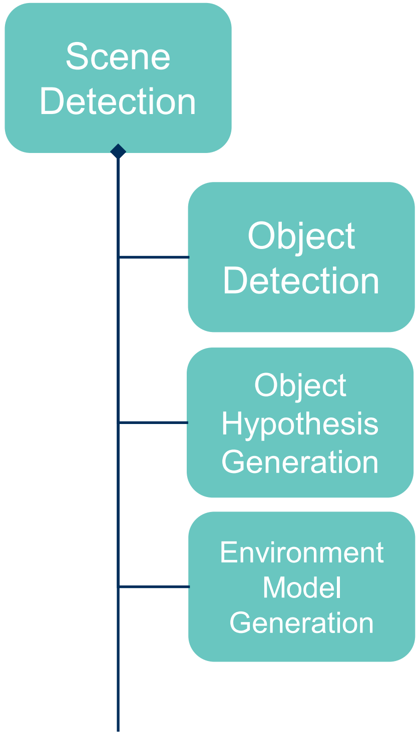
Target Behavior:
Don’t hit objects, drive compliantly

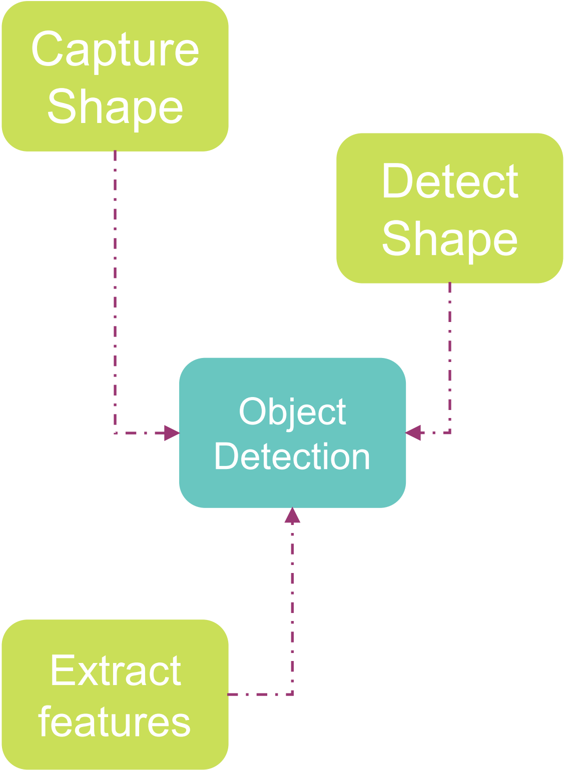
Required System Capability:
Scene Detection

System Capability Decomposition:
Scene Detection

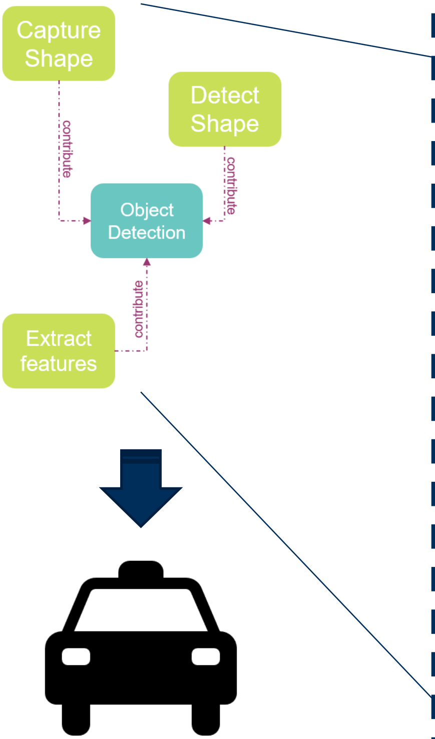
Contributing Functional Element:
Object Detection

[6] T. Hofmann, "Capability-based Architecture for Automated Vehicles in Urban Environment," presented at the VVM Mid-term presentation, Munich, Mar. 2022.





Contributing Functional Blocks: Object Detection



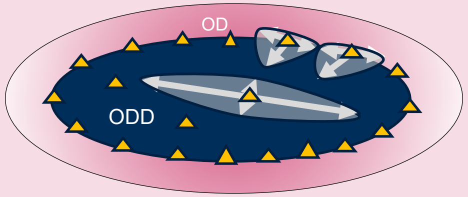
Allocate capabilities and functions to EGO

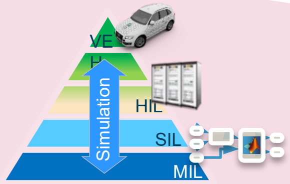
System requirements for the car: The system shall

[2] R. Galbas, “VVM Main Approach - How to Systematically Release AD Systems,” presented at the VVM Mid-term presentation, Munich, Mar. 2022.

Goal IV – **Argumentation**

Explainable Compliance

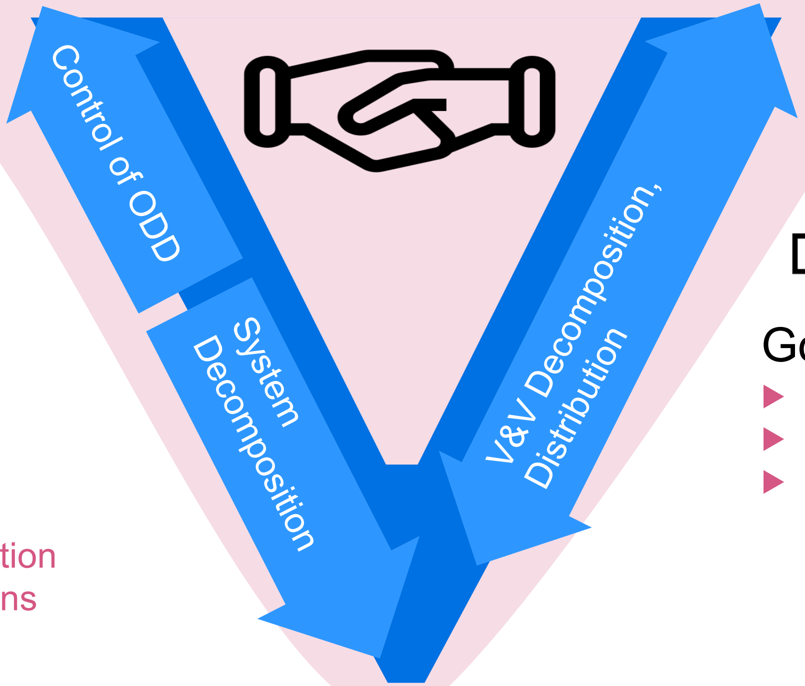




Feasibility

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

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



Efficiency

Goal III – **shift to simulation**

- System Monitoring and Assessment
- Structured Data Handling
- …

Changeability

Goal II – **Consistent interfaces**

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

pproach from PEGASUS by acknowledging
:hin the **safety case**

icit **modeling of target behavior**

ns to bridge the gap between **behavior**
ents

it **representation of risks** within the

Thank you!

Nayel Fabian Salem, Technische Universität Braunschweig, Institute of Control Engineering
salem@ifr.ing.tu-bs.de

Veronica Haber, PROSTEP AG
veronica.haber@prostep.com