PROJECT of the PEGASUS FAMILY

VERIFICATION VALIDATION METHODS

Mid-Term Presentation 15 / 16 March 2022

Contributions to a traceable behavior specification for automated driving systems using formal methods

Nayel Fabian Salem[1], Hans Nikolaus Beck[3],

Veronica Haber[2], Matthias Rauschenbach[4], Marcus Nolte[1], Jan Reich[5]

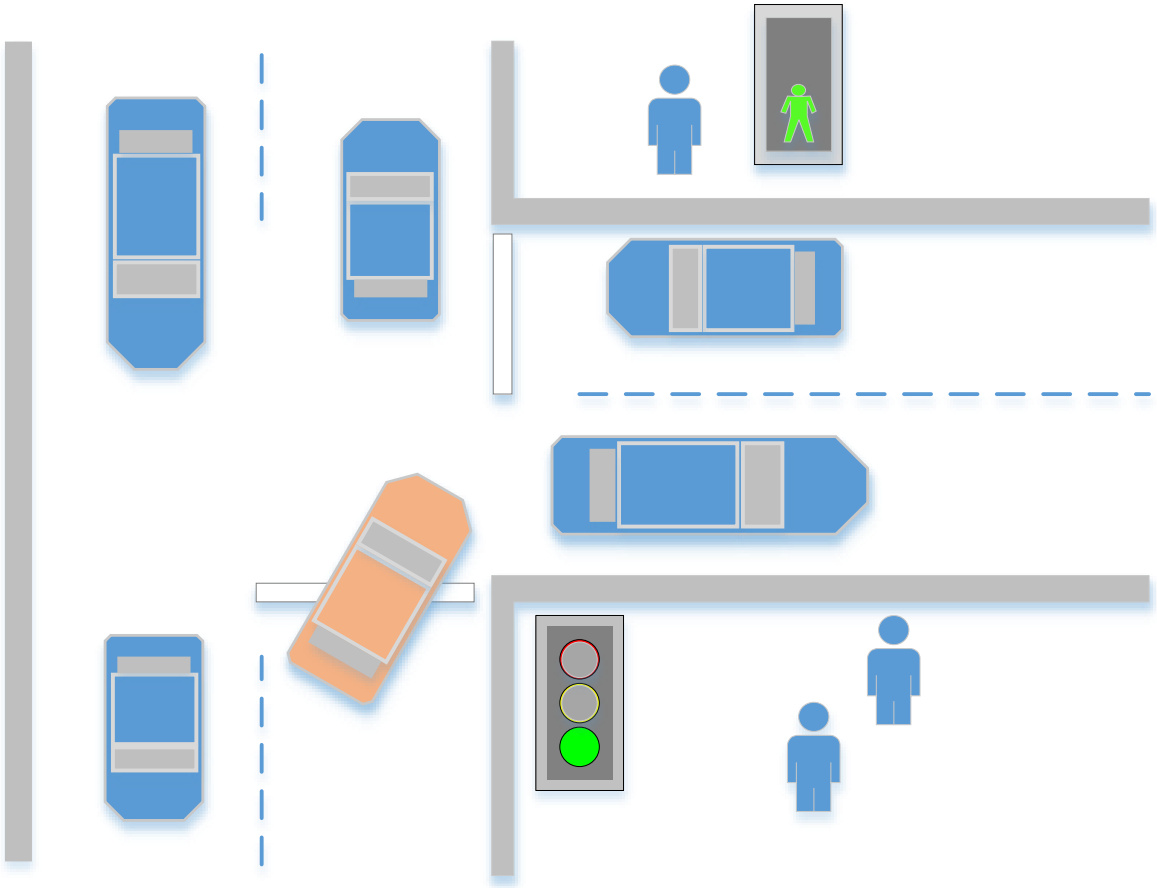
[1] TU Braunschweig
[2] PROSTEP AG
[3] Robert Bosch GmbH
[4] Fraunhofer LBF
[5] Fraunhofer IESE

Supported by:

Federal Ministry for Economic Affairs and Climate Action

on the basis of a decision by the German Bundestag

How should a robot behave in traffic ?



Where could concerns come from?

- societal expectations
- legal regulations

- traffic signs

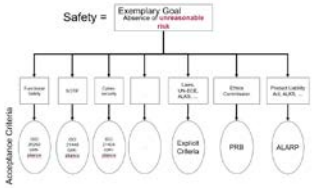
- other traffic participants

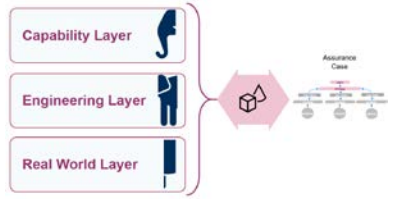
Challenges

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

We need to do more in order to assure safety!

Goals





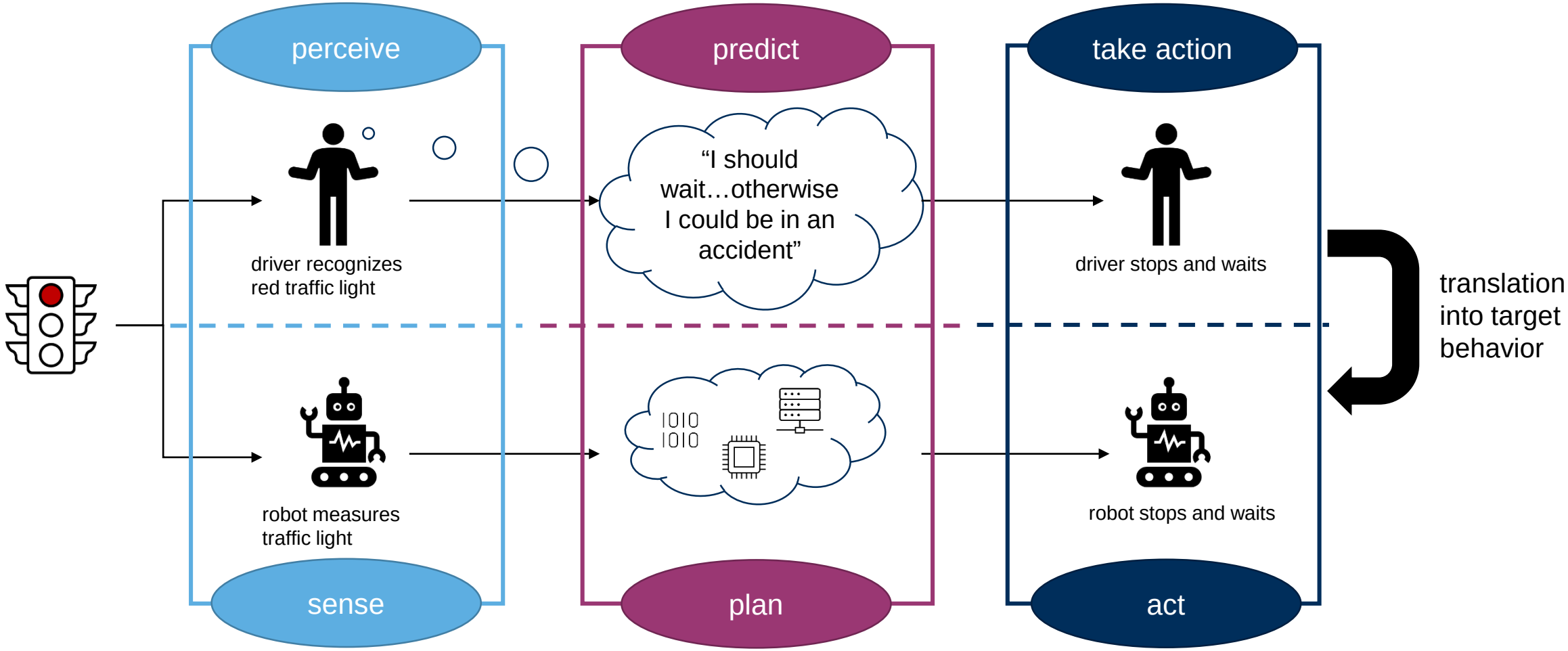
identify and assess hazards and their associated risks

specify behavior with respect to open context criticality phenomena

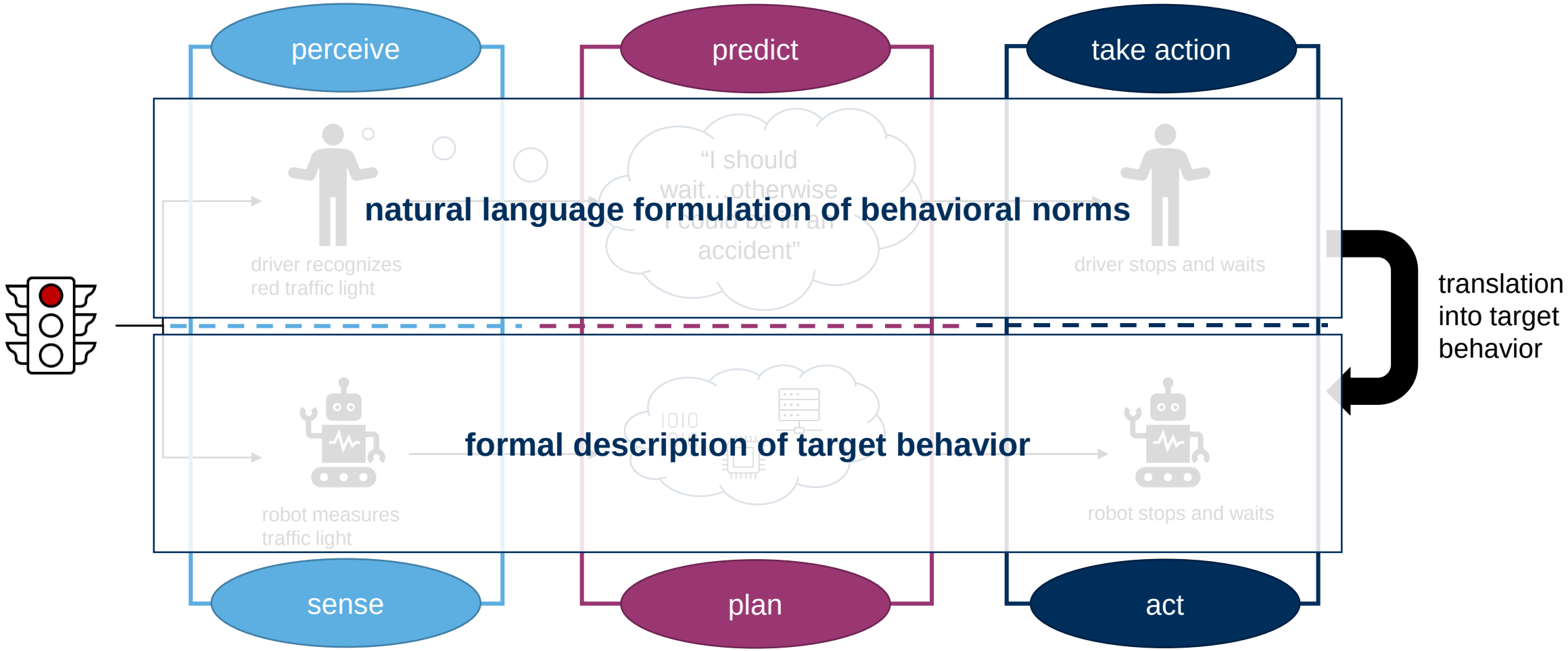
link behavior specification with system architecture traceably by using the concept of capabilities

behavior specification is an iterative refinement process

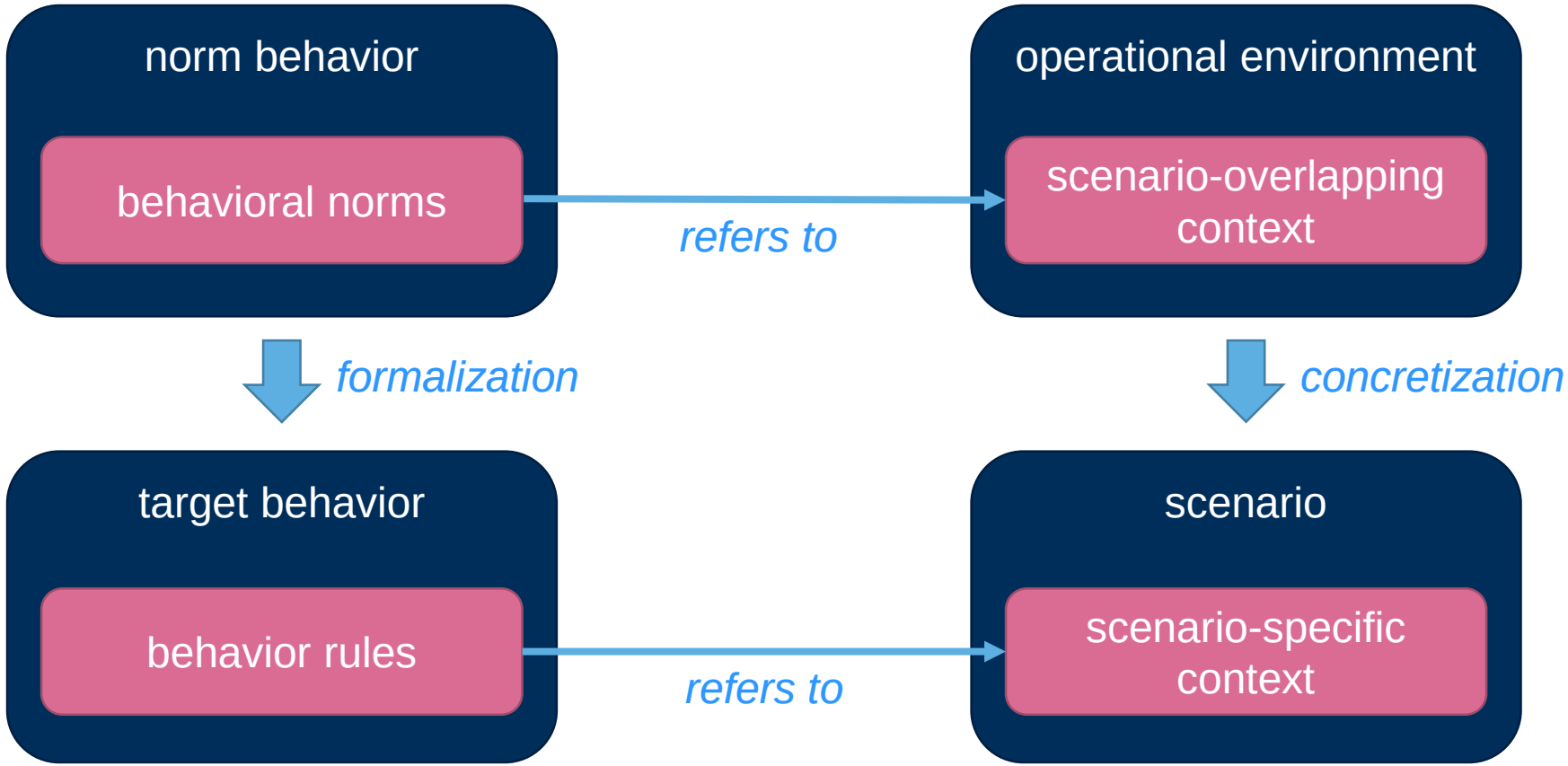
Where do we start with specifying a robots behavior in traffic?



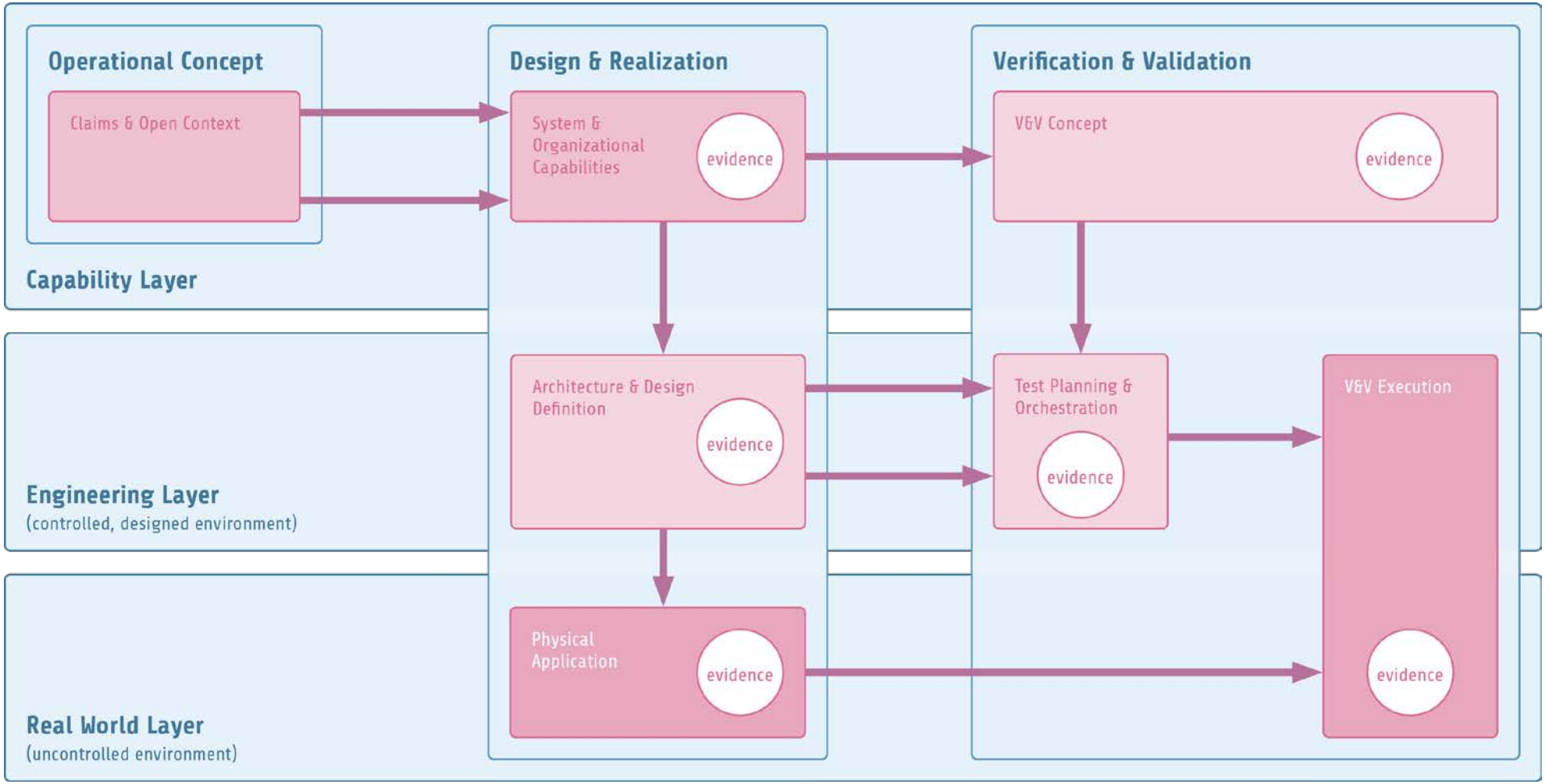
Where do we start with specifying a robots behavior in traffic?



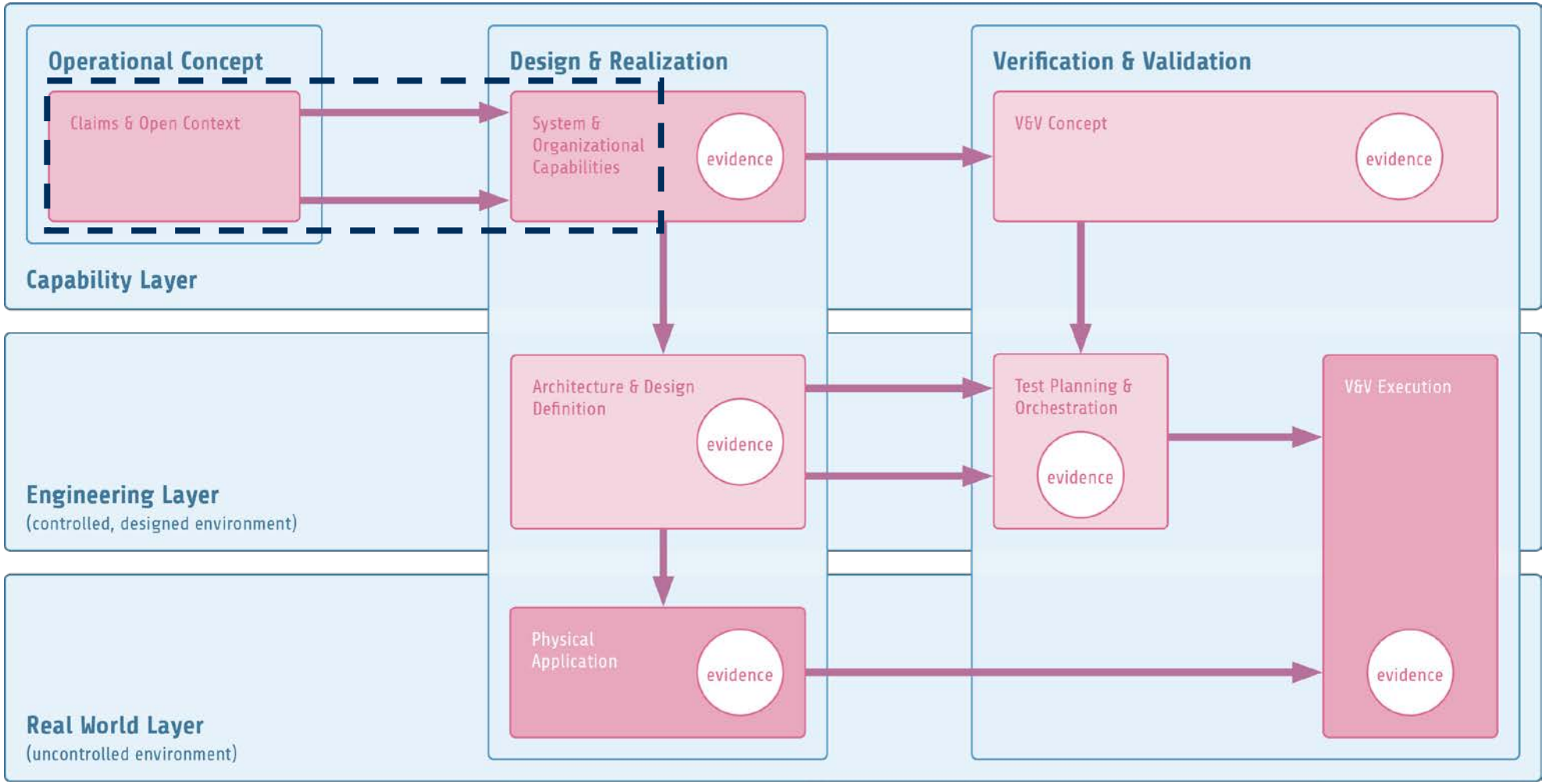
Specifying behavior on different levels of abstraction



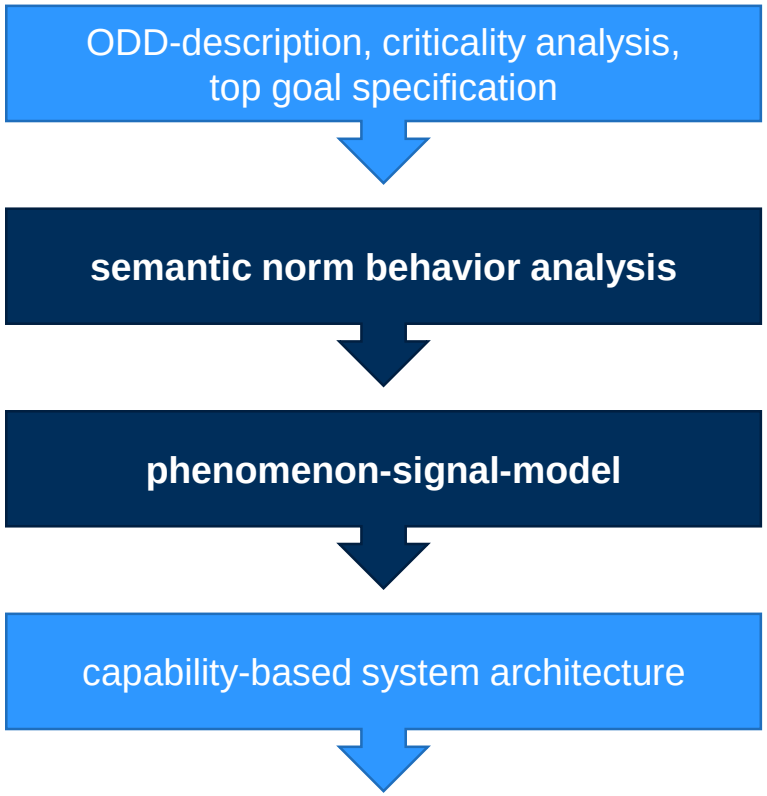
Allocation in the VVM Assurance Framework



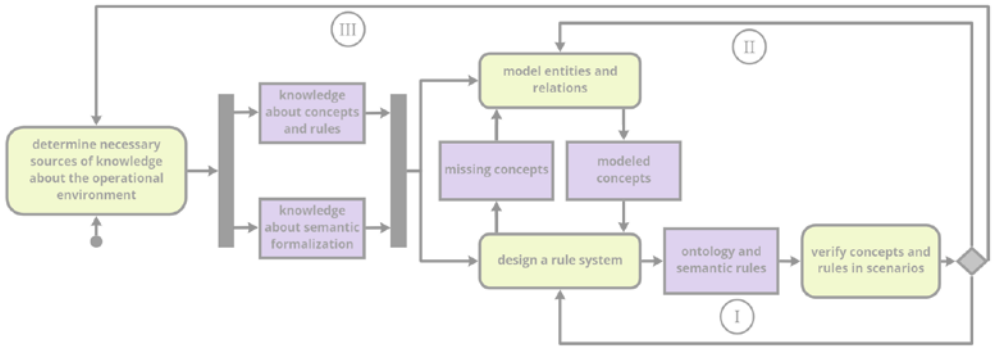
Allocation in the VVM Assurance Framework



Outline



- How could rules of the road and further concerns be integrated into a behavior specification?
- How could a behavior specification be represented?

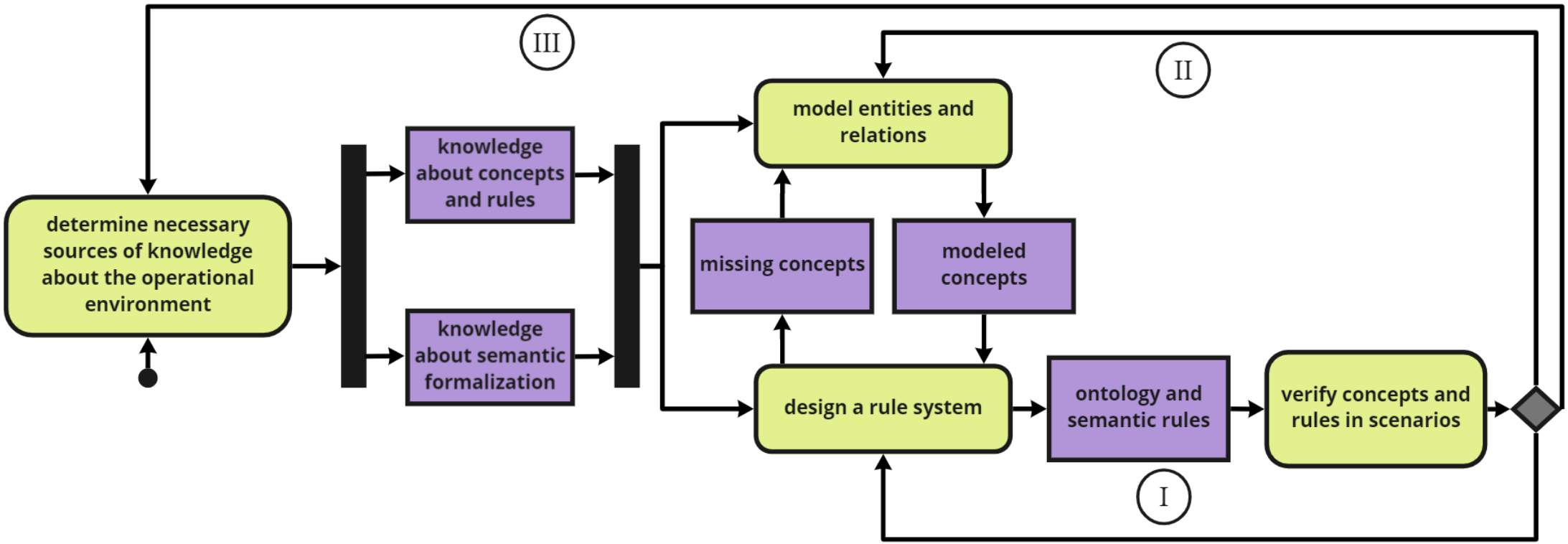


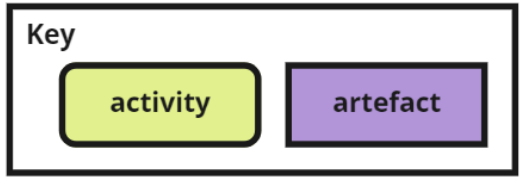
Natural language rule	SWRL rule
If sign and marking **then** valid pedestrian crossing	`Pedestrian_crossing(?cross) ∧ sign_350(?sign) ∧ sign_293(?marking) ∧ is_fact(?sign, true) ∧ is_fact(?marking, true) ∧ consists_of(?cross, ?sign) ∧ consists_of(?cross, ?marking) →` `is_fact(?cross, true)`

Semantic norm behavior analysis

Contributions to a traceable specification of target behavior rules

Semantic norm behavior analysis

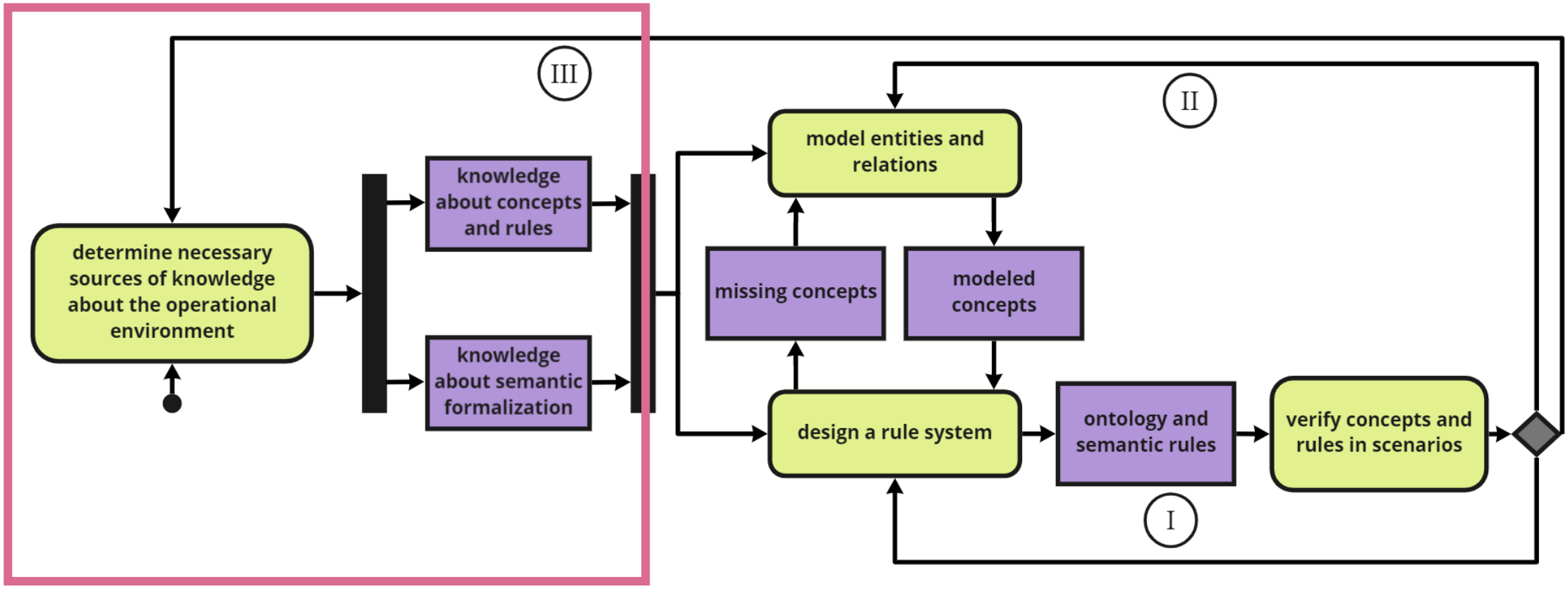


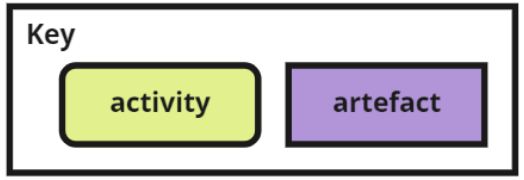


Iterations

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

Semantic norm behavior analysis



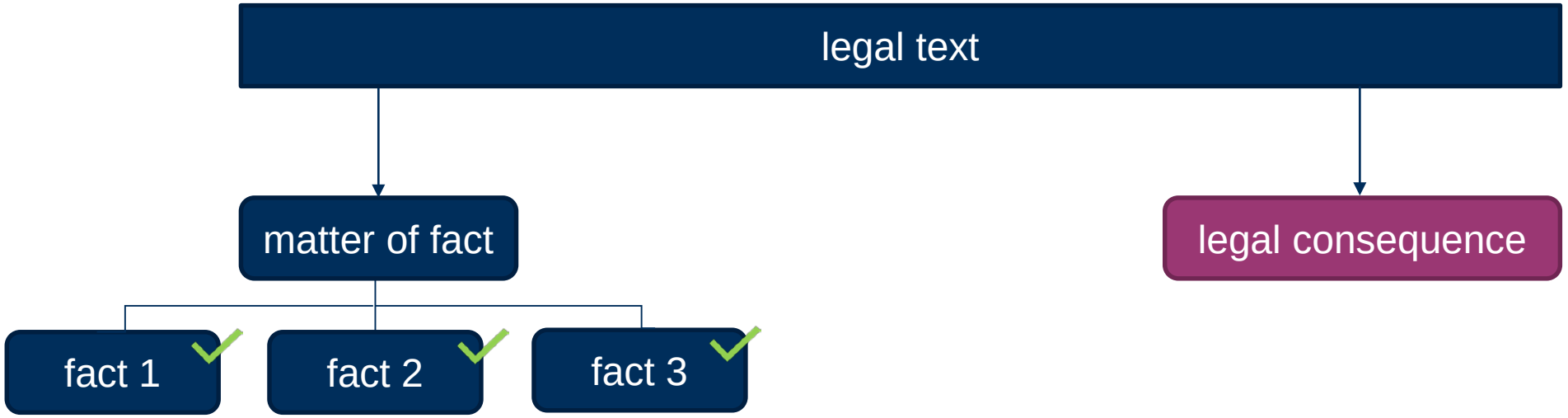


Iterations

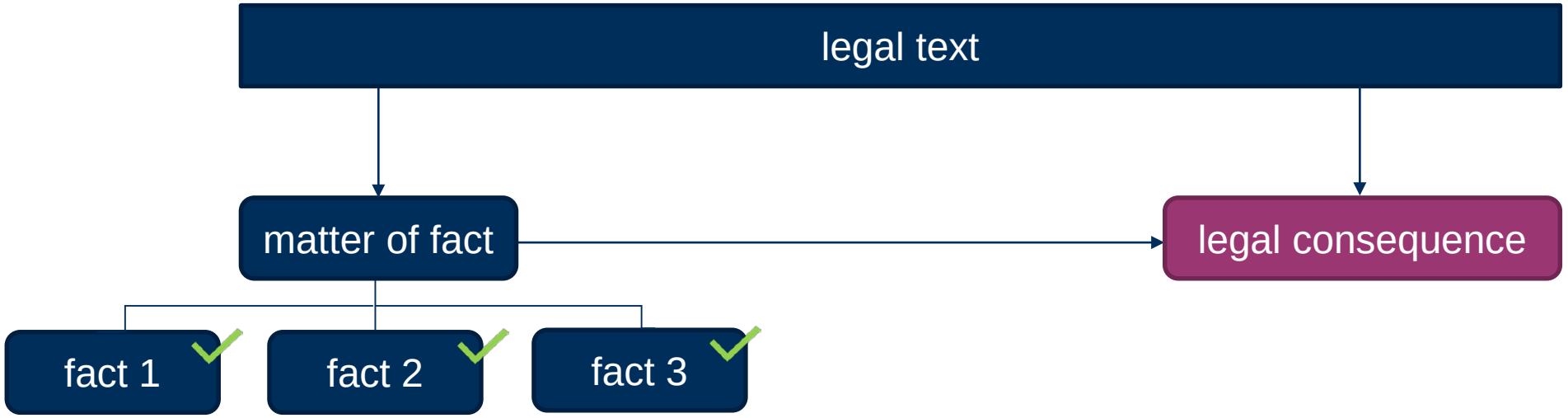
- I adapt false rules
- II adapt false concepts
- III adapt false knowledge sources

Semantic formalization of legal texts (in Germany)

Semantic formalization of legal texts (in Germany)



Semantic formalization of legal texts (in Germany)



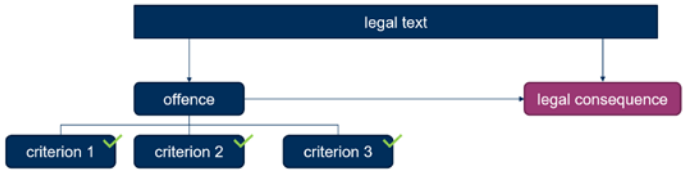
Semantic formalization of legal texts (in Germany)

§ 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. — matter of fact

In that case vehicles may only drive with moderate speed. If necessary vehicles have to wait. — legal consequence

Semantic formalization of legal texts (in Germany)



§ 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

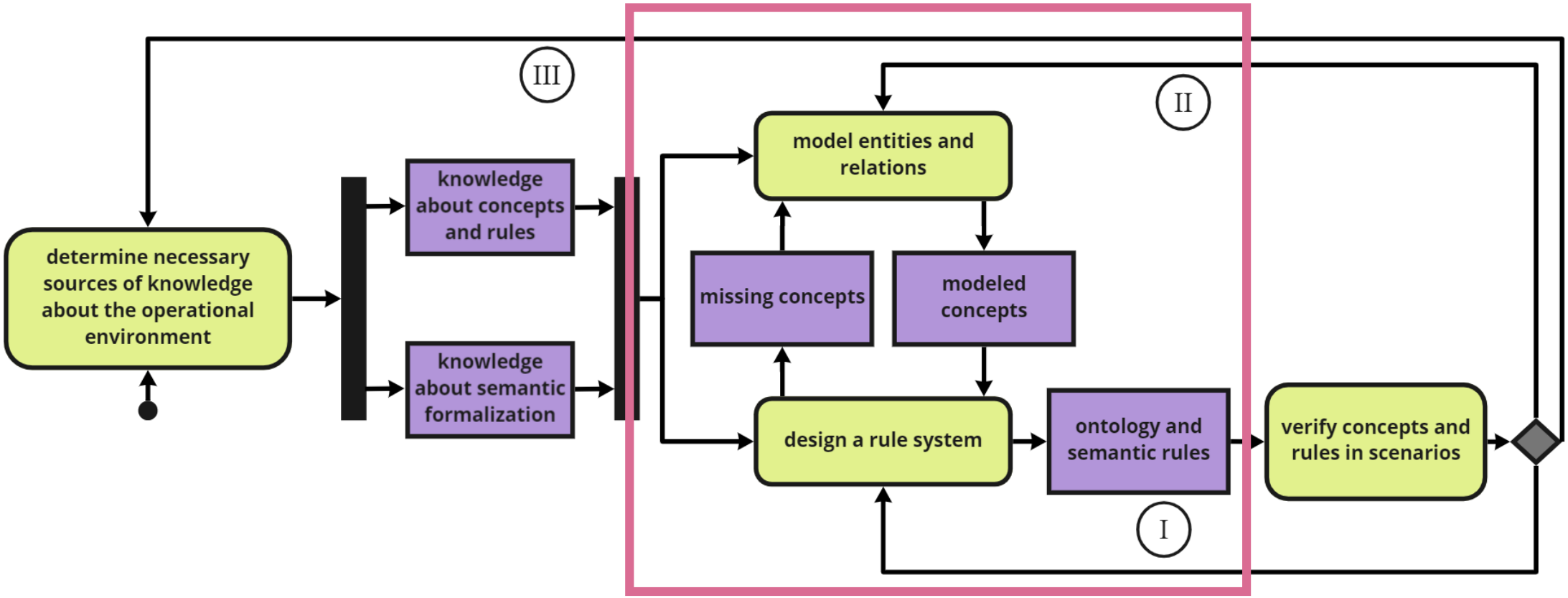
fact 2

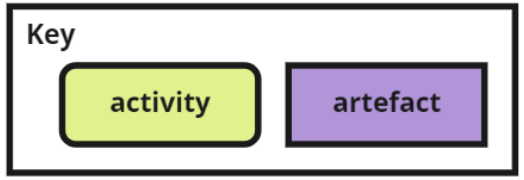
legal consequence

What counts as “noticeable”?

How to decide between slowing down and stopping?

Semantic norm behavior analysis

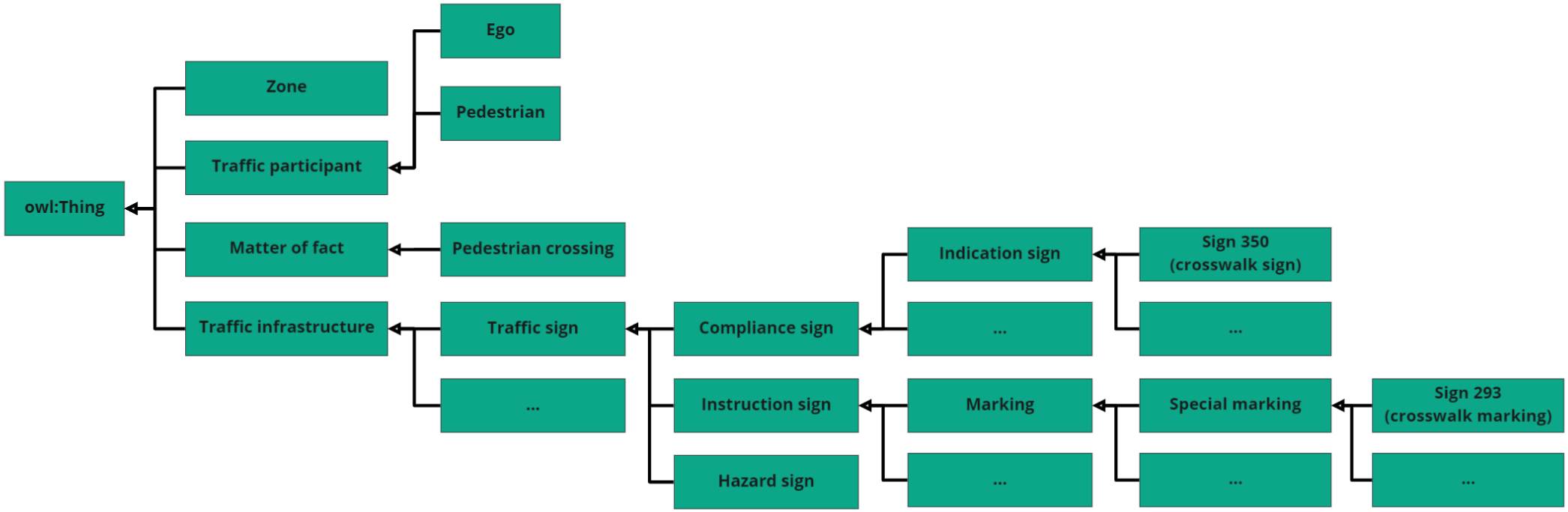




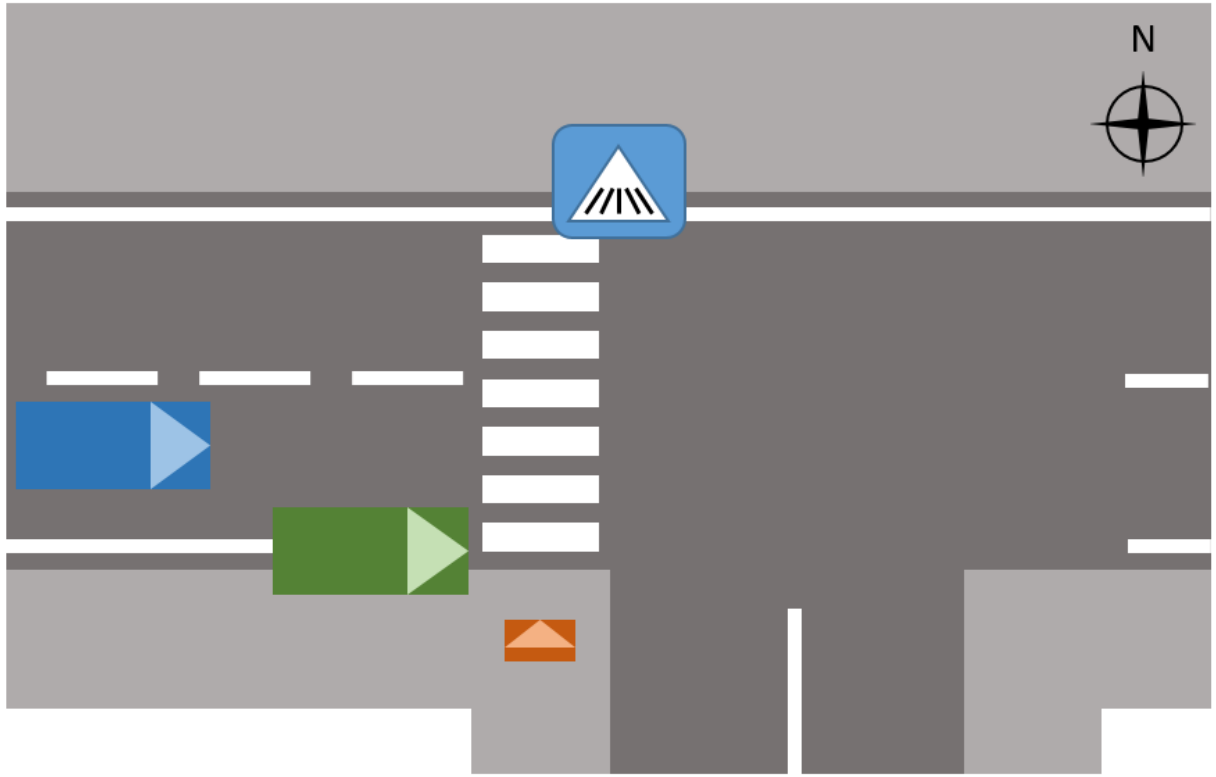
Iterations

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

Top-down conceptualization using ontologies

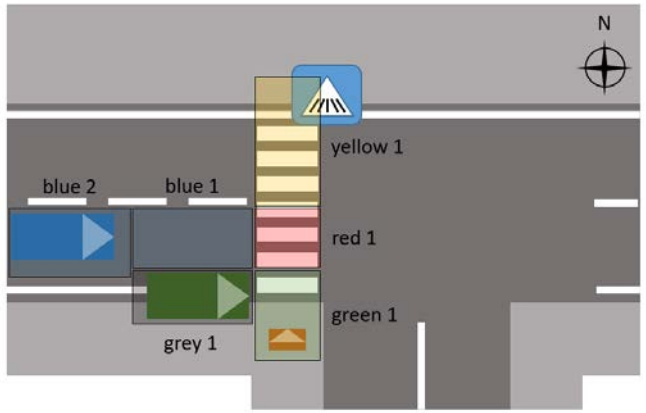


Example scenario

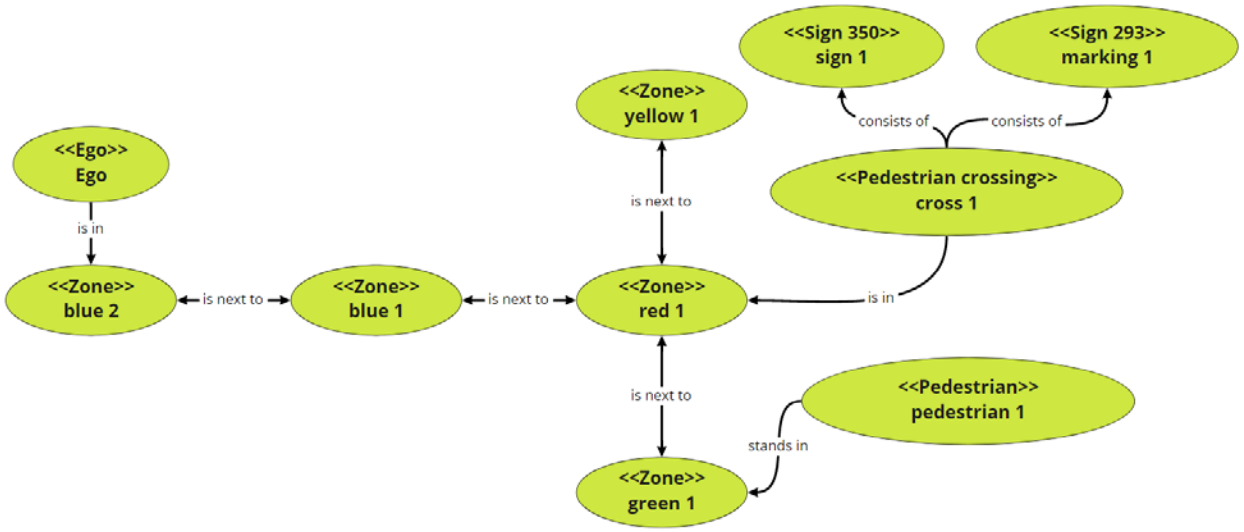


Bottom-up conceptualization

Scene

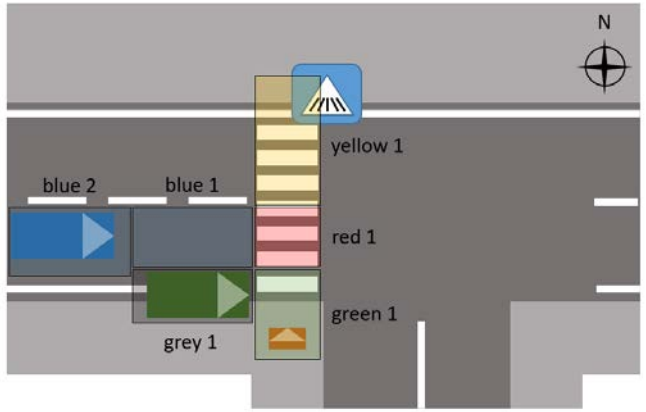


Ontology

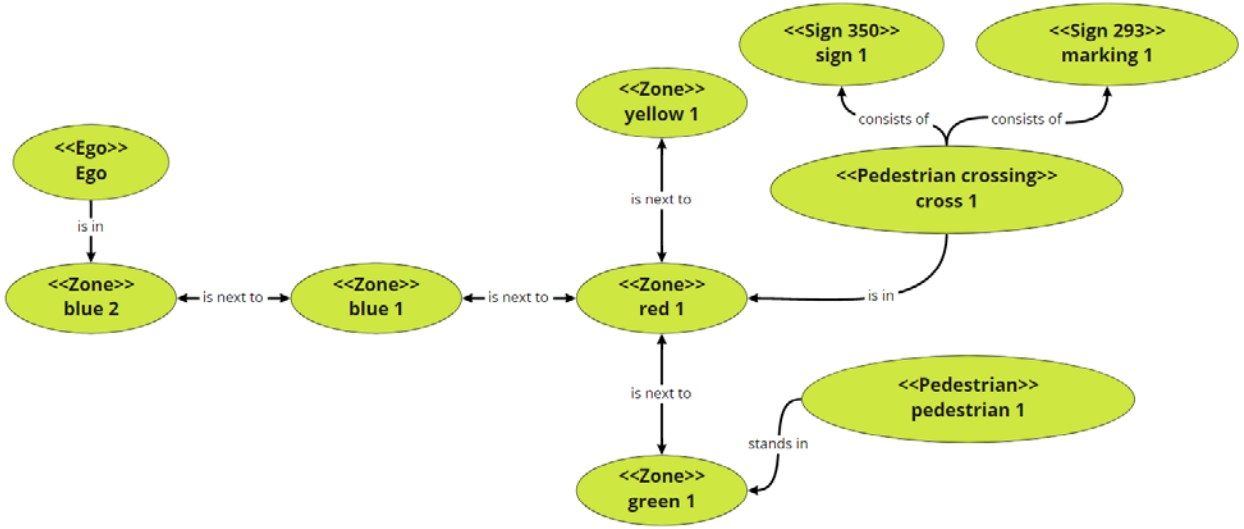


Designing rules for target behavior

Scene



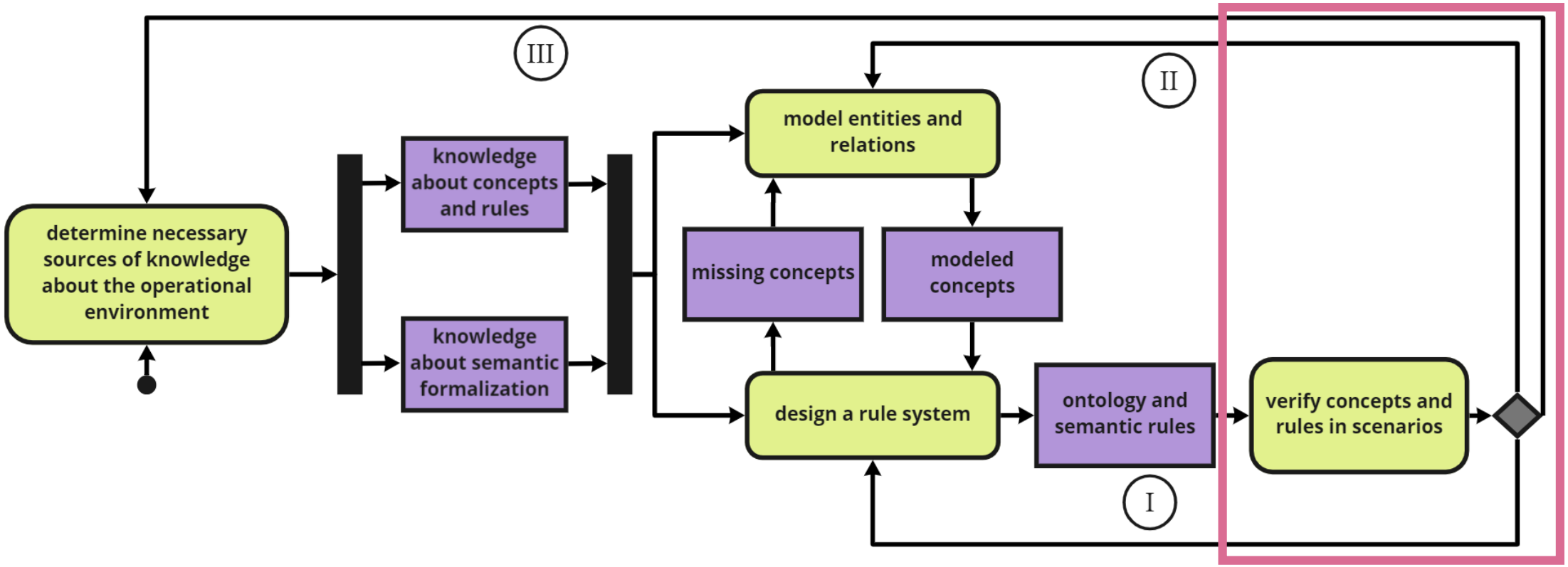
Ontology



Inference rule

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

Semantic norm behavior analysis



Iterations

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

Evaluating the target behavior rules

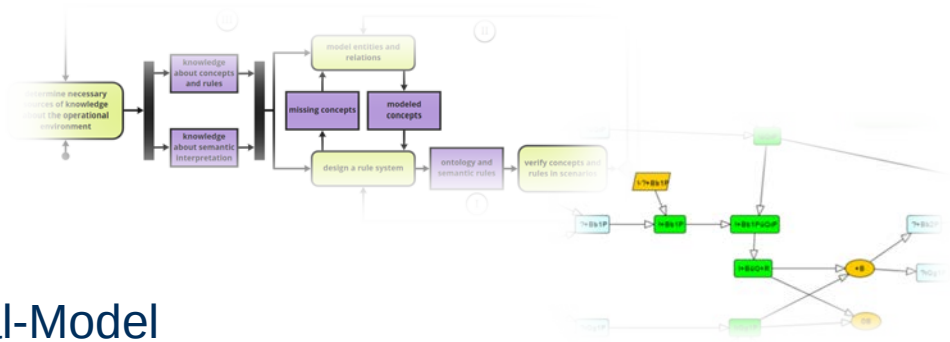
- expert-based
  - analysis of a given scenario
  - comparison of the inferred target behavior with behavioral norms
- automated
  - logical consistency check of the formalized target behavior rules

Summary and outlook

- contributions
  - argumentation of the semantic norm behavior analysis regarding the open traffic context
  - proposal of an approach to systematically formulate target behavior
  - example implementation of target behavior rules in a machine-readable format

Summary and outlook

- contributions
  - argumentation of the semantic norm behavior analysis regarding the open traffic context
  - proposal of an approach to systematically formulate target behavior
  - example implementation of target behavior rules in a machine-readable format
- future work
  - resolve or moderate conflicting rules
  - operational integration with the Phenomenon-Signal-Model

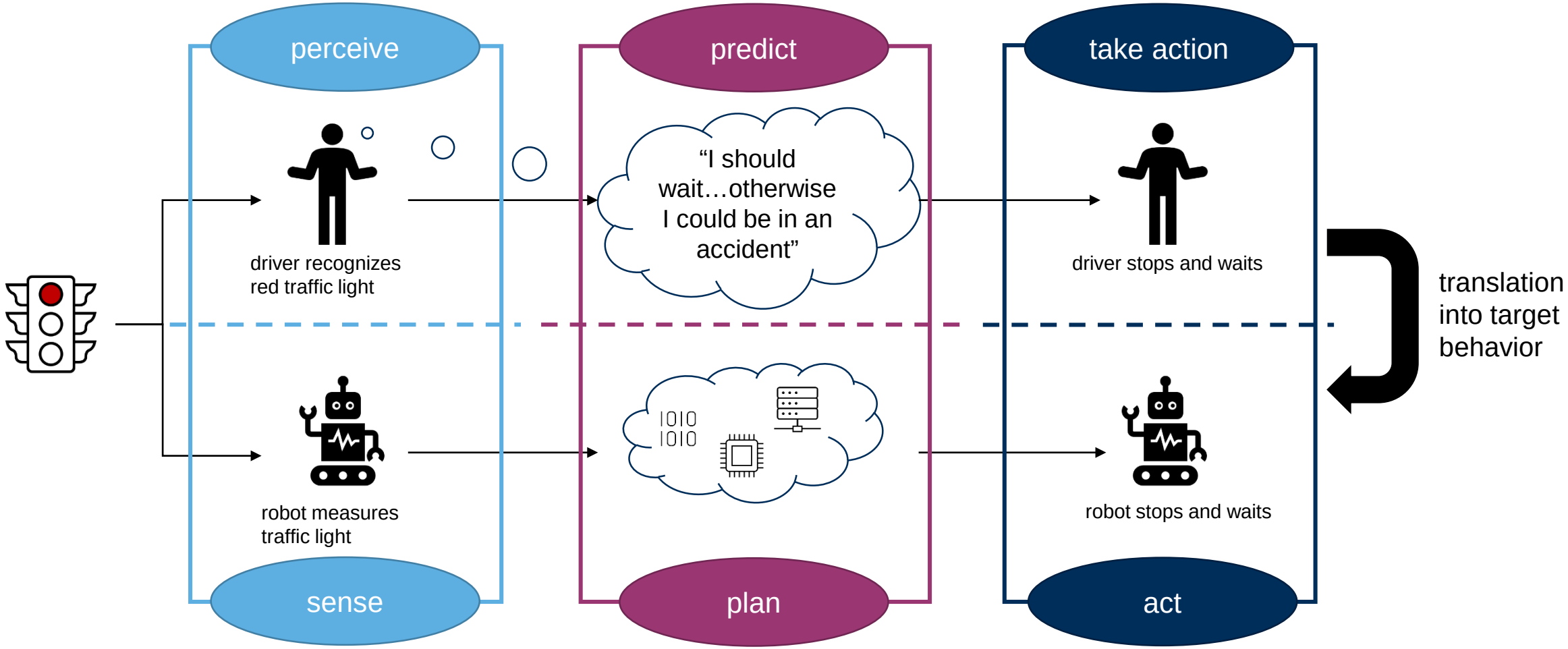


VERIFICATION
VALIDATION
METHODS

Phenomenon-Signal-Model (PSM)

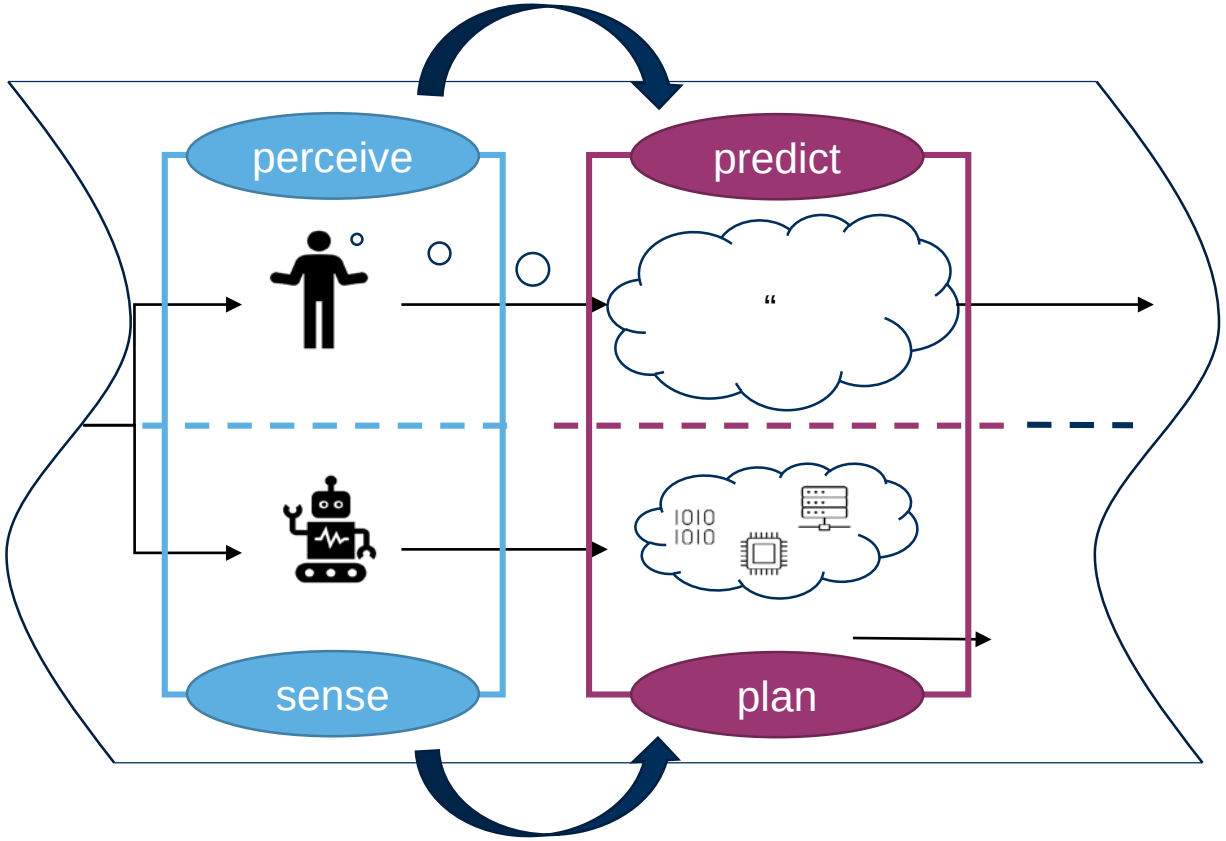
An approach for representing target behavior

Where do we start specifying robots behavior in traffic?



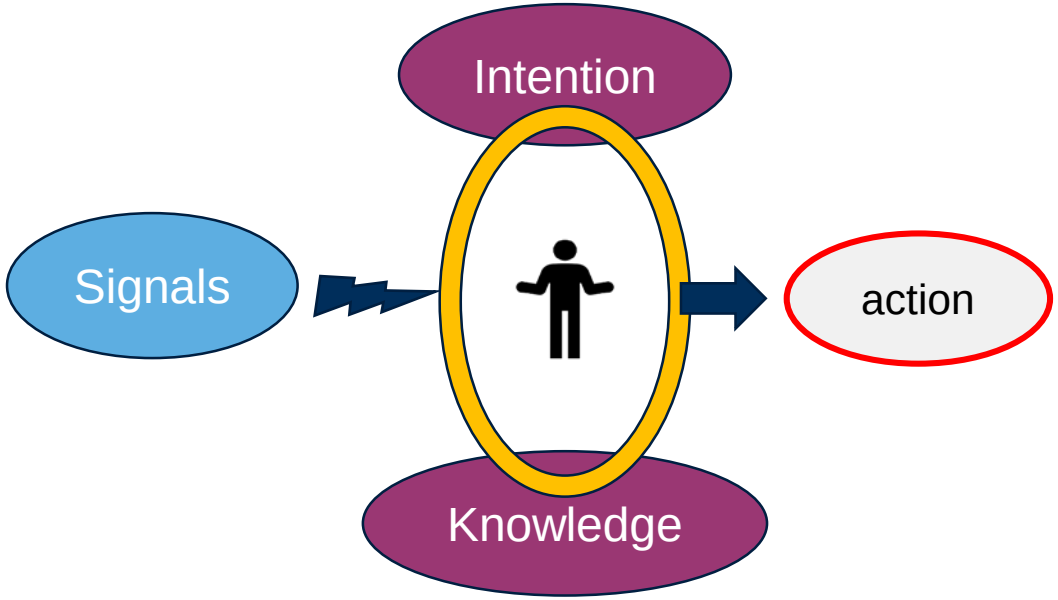
The signal action path

Model this…



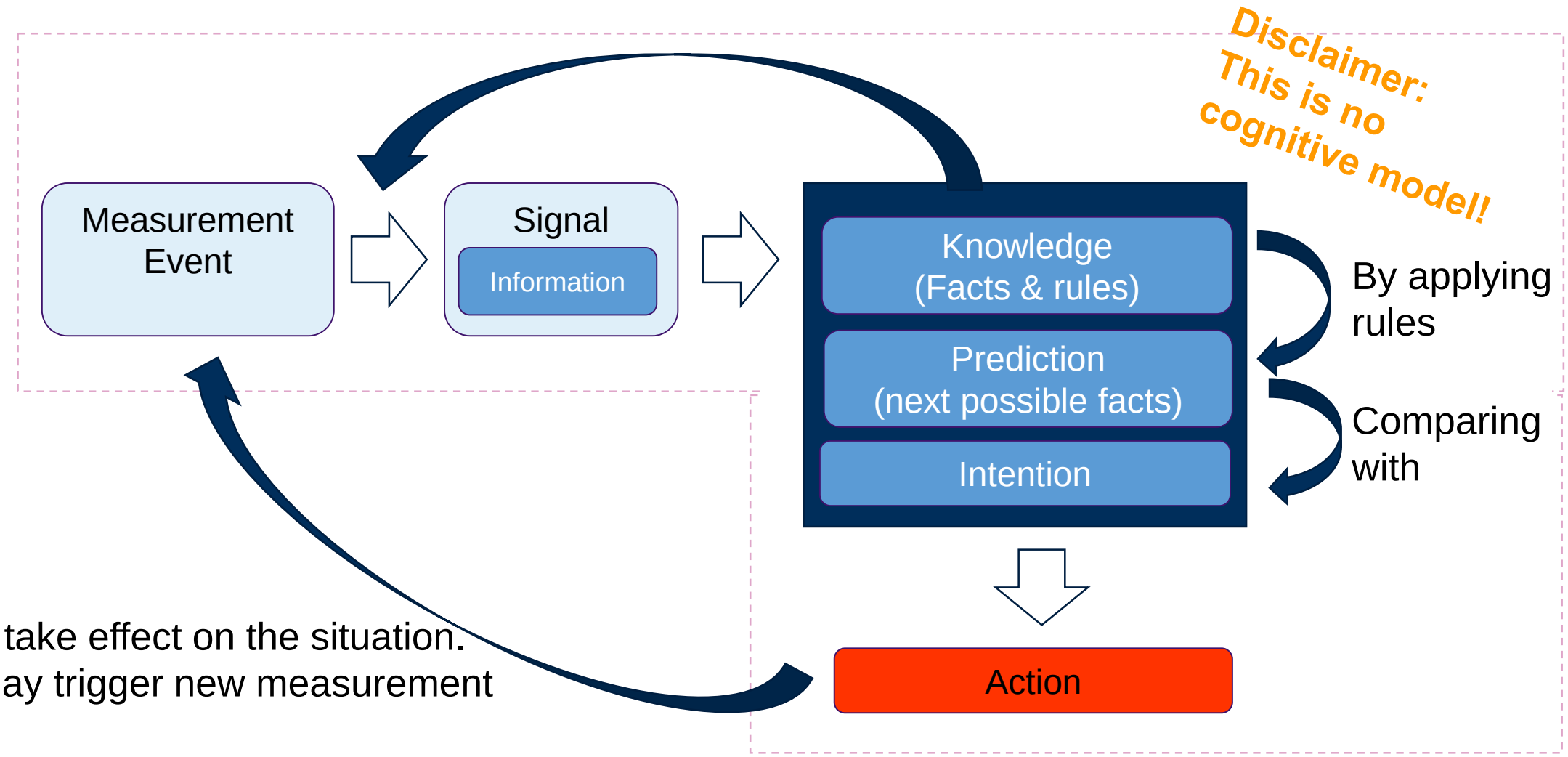
…. to get that

Starting point: Phenomenology by Edmund Husserl

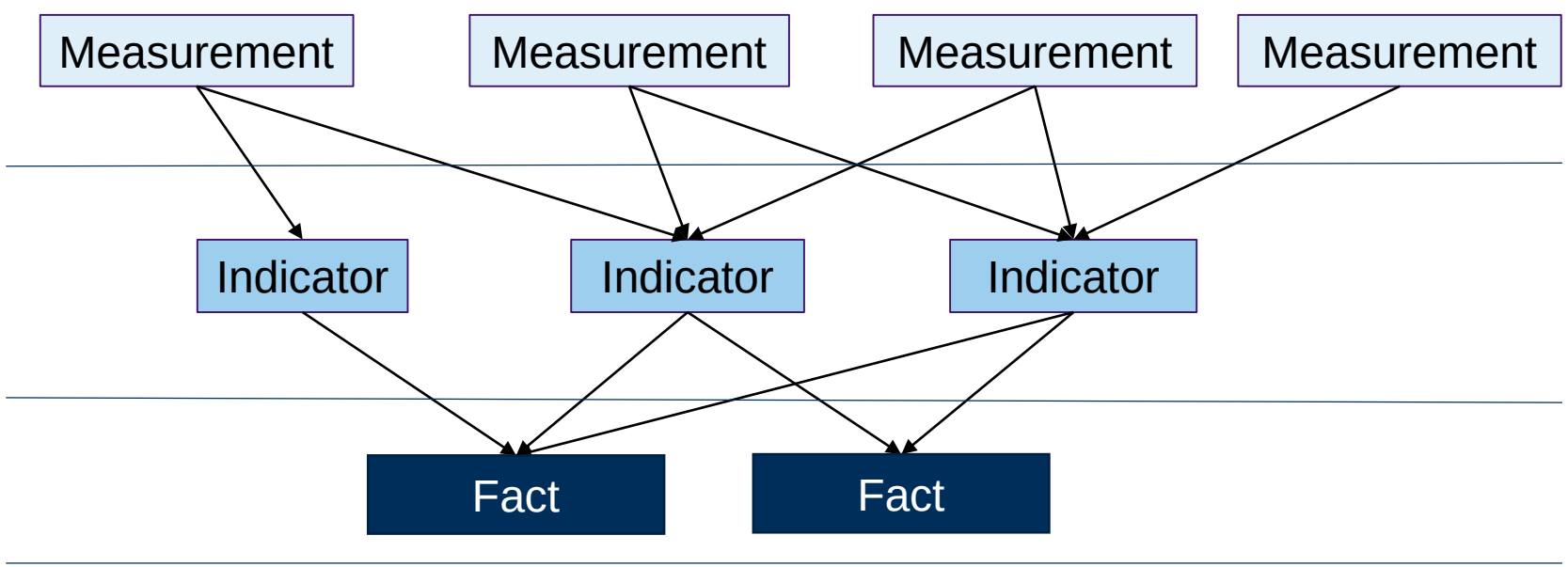


These factors are relevant to derive a model

Formalization of the signal action path



Indicators as means for formalization



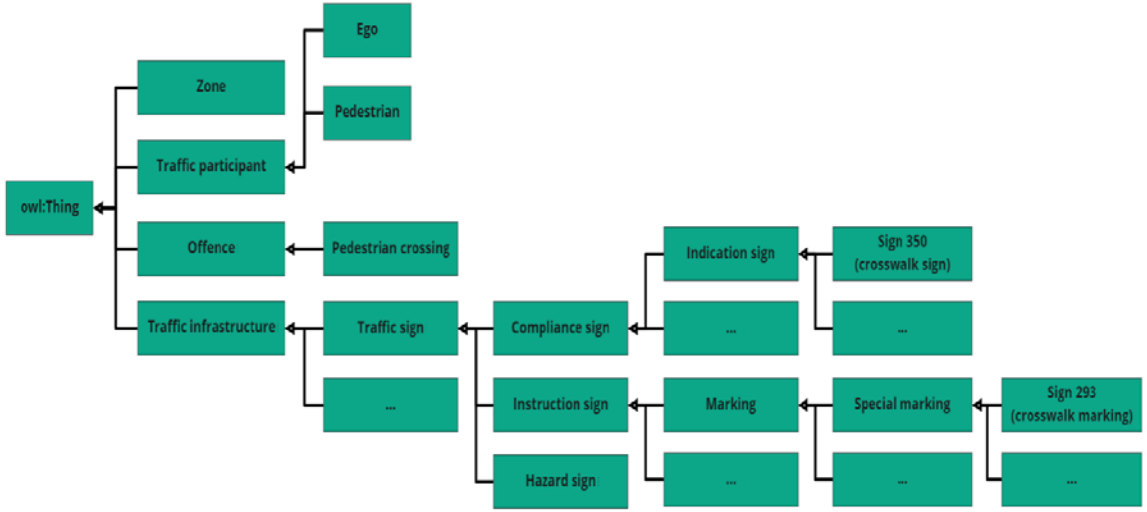
Level of observation, measurement events

Level of signals

Level of (gained) knowledge

Level of behavior

Top-down conceptualization using ontologies



Indicator	Meaning	Values
P	Position	b1, b2, r, g1…
Q	Quality	r, f, ü,
A	Size	p, f, l,
R	Direction	+, -, <, >
B	Movement	0, +, - <, >

Ontology helps to categorise and formalise indicators

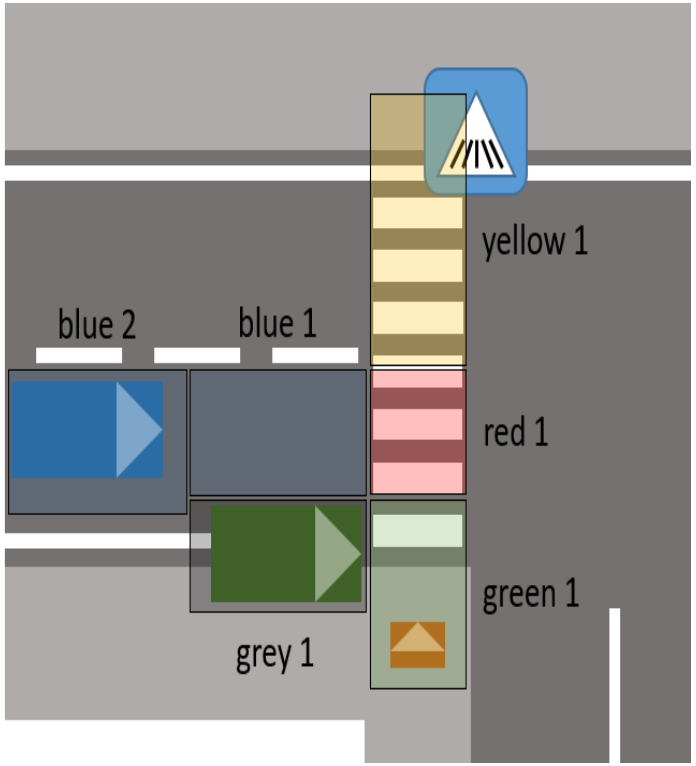
r = cyclist, f = pedestrian
+ = forward
b1, b2…. = name of positions

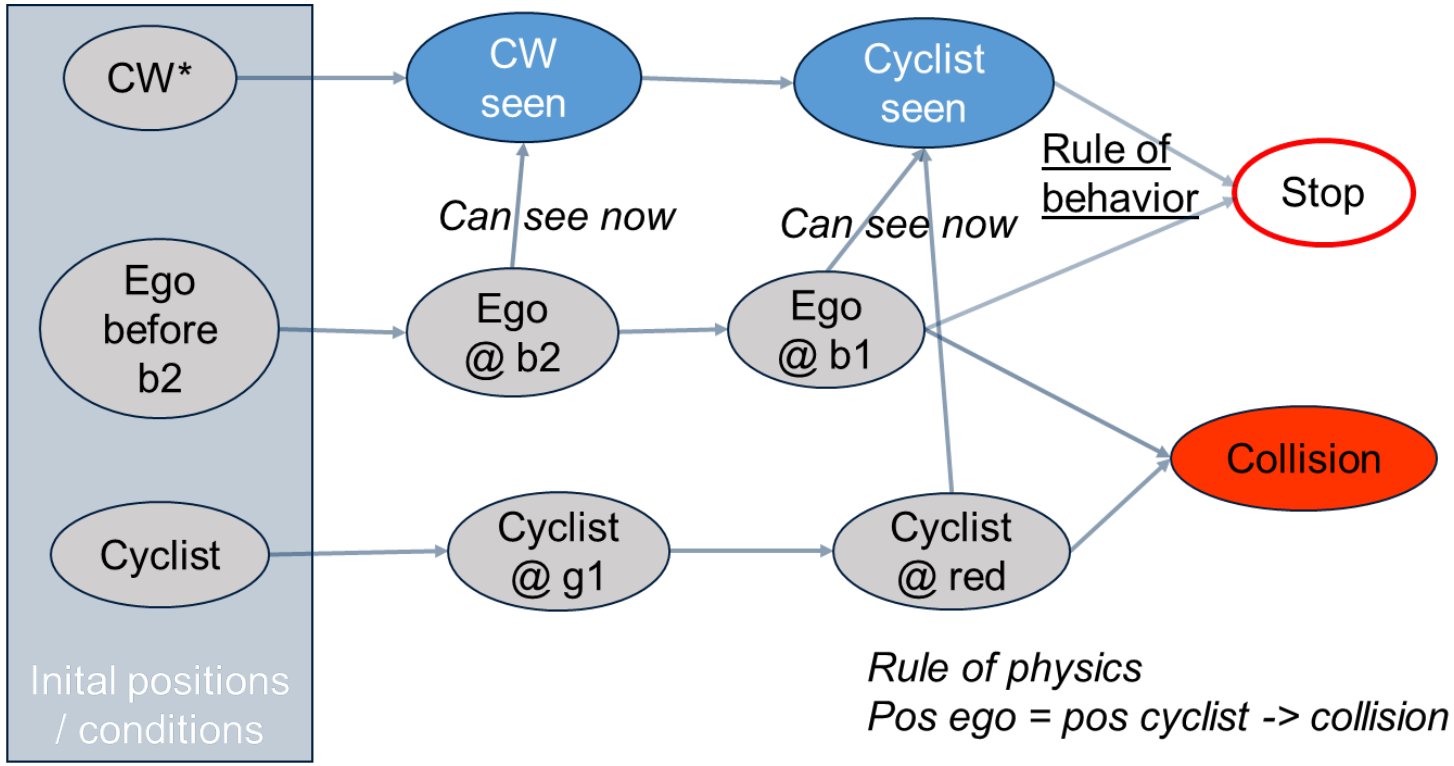
Example:

Fact = rQ ^ b1P ⟵ Q = r + P = b1

Meaning: Fact : there is a cyclist at position b1

Structure of a PSM Graph – simplified example



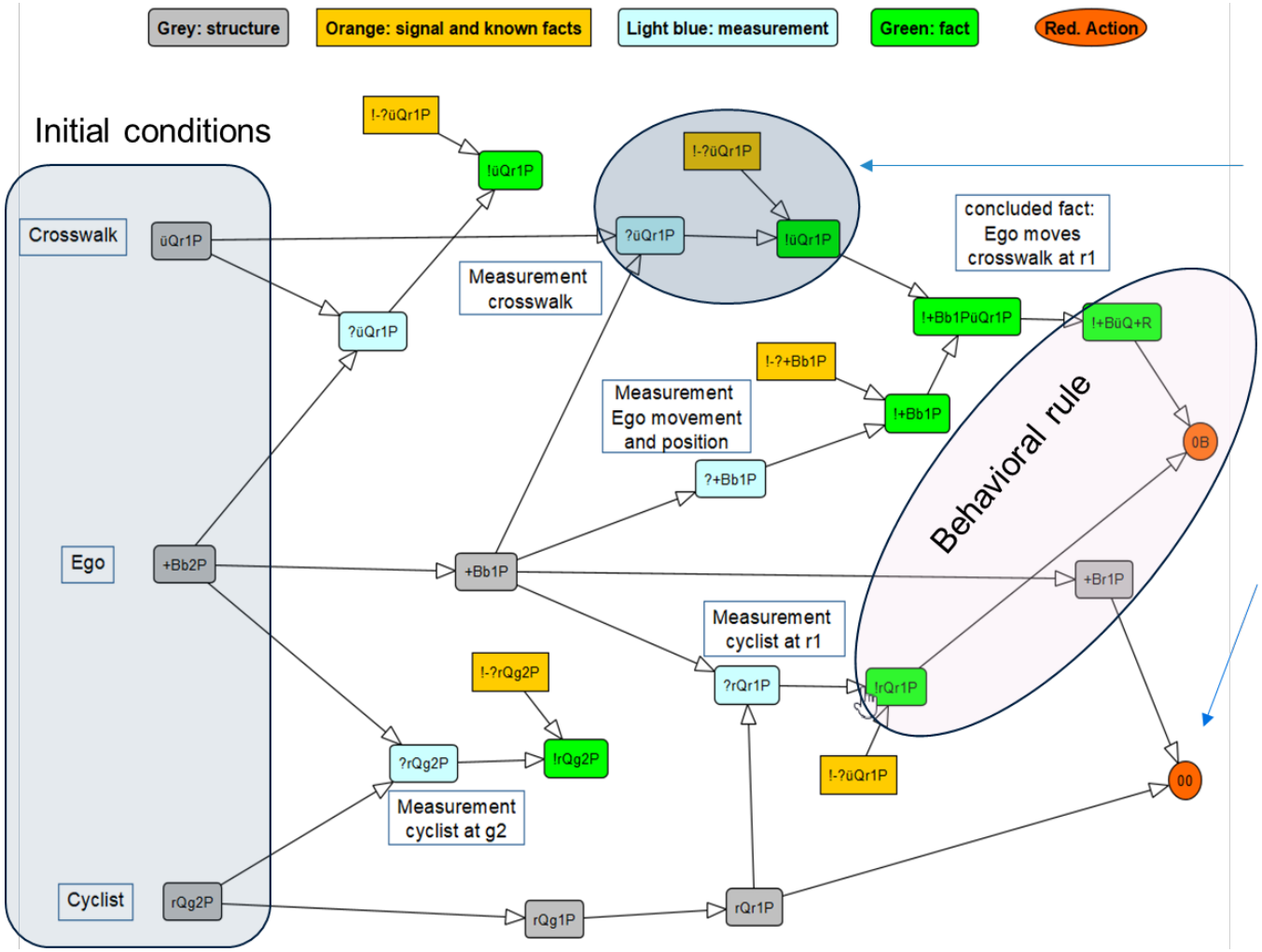


Every → means application of one or more rules

Every ⬭ represents facts in scenario

* CW= Crosswalk

Possible analysis results



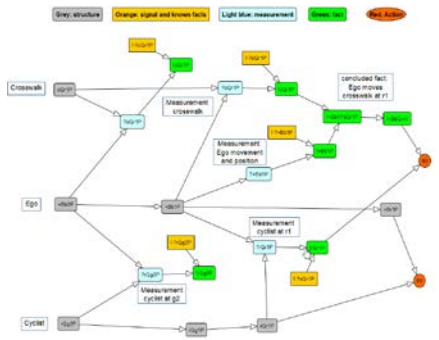
Such a triple indicates which measurement and which knowledge the ADS shall have to realise (or to avoid) a certain path in graph.

This indicates **necessary capabilities**.

The graph may indicate that there exist paths into a collision or other unwanted consequences.

Depending of semantic of rules and rule sets, different analysis goals can be checked -> it‘s a tool!

Summary

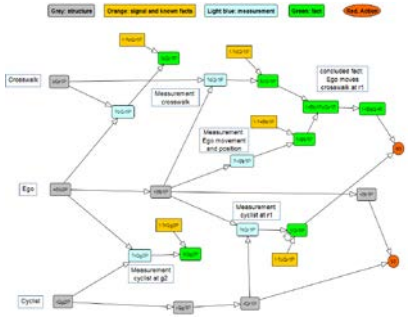


The presented formalization and the PSM graph allows

- to describe target behavior as a set of rules and facts,
- to perfom computer experiments in order to optimize rules and facts,
- to apply various analyses as a toolset,
- to enable the iterative identification and optimization of relevant factors.

Future Work

- Develop more detailed methods for creating zones.
- Create example workflows for analysis and optimization.
- Define evaluation methods for the PSM graph.
- Implement more complex rules and rule selection strategies.
- Connect this method with safety relevant process steps.



VERIFICATION
VALIDATION
METHODS

Thank you!

Hans Nikolaus Beck Robert Bosch GmbH HansNikolaus.Beck@de.bosch.com

Nayel Fabian Salem Technische Universität Braunschweig salem@ifr.ing.tu-bs.de

Veronica Haber, Prostep AG; Matthias Rauschenbauch, Fraunhofer LBF; Marcus Nolte, TU Braunscheig;
Jan Reich Fraunhofer IESE

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