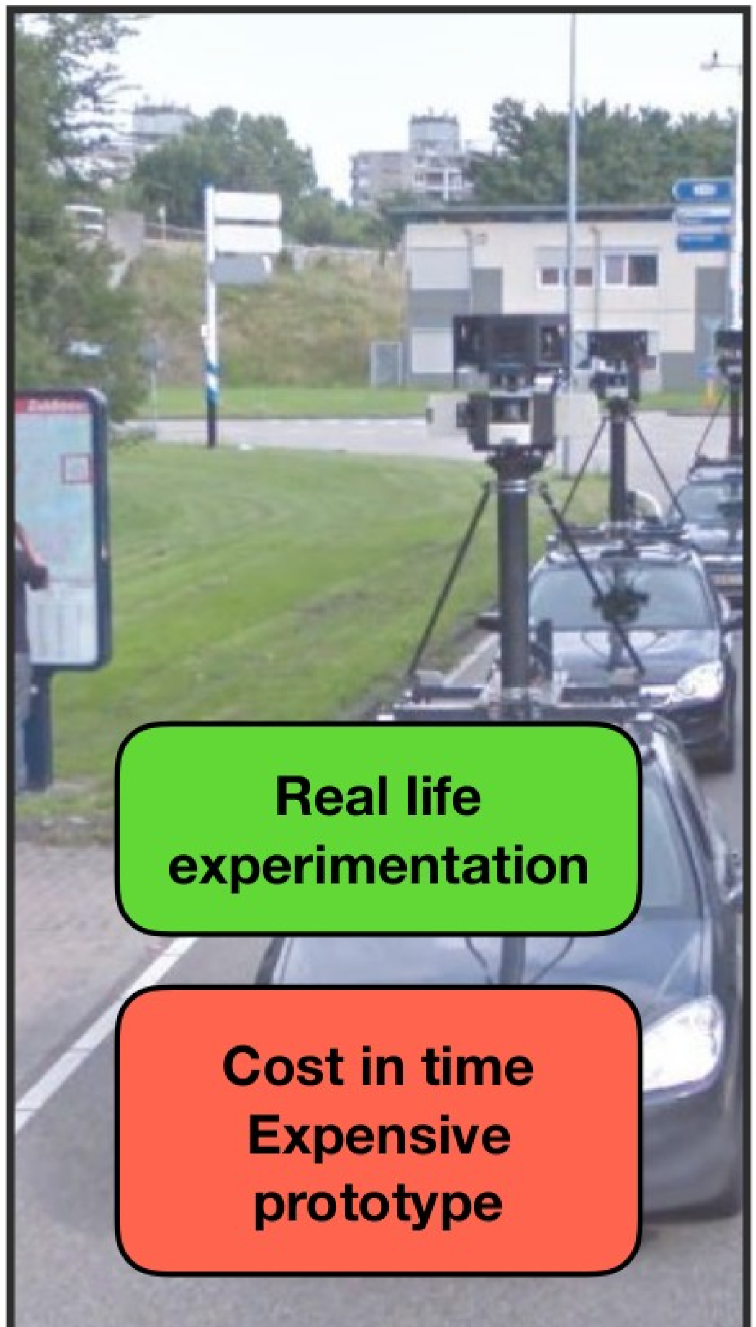
Modeling and checking robustness of autonomous vehicles

Johan ARCILE

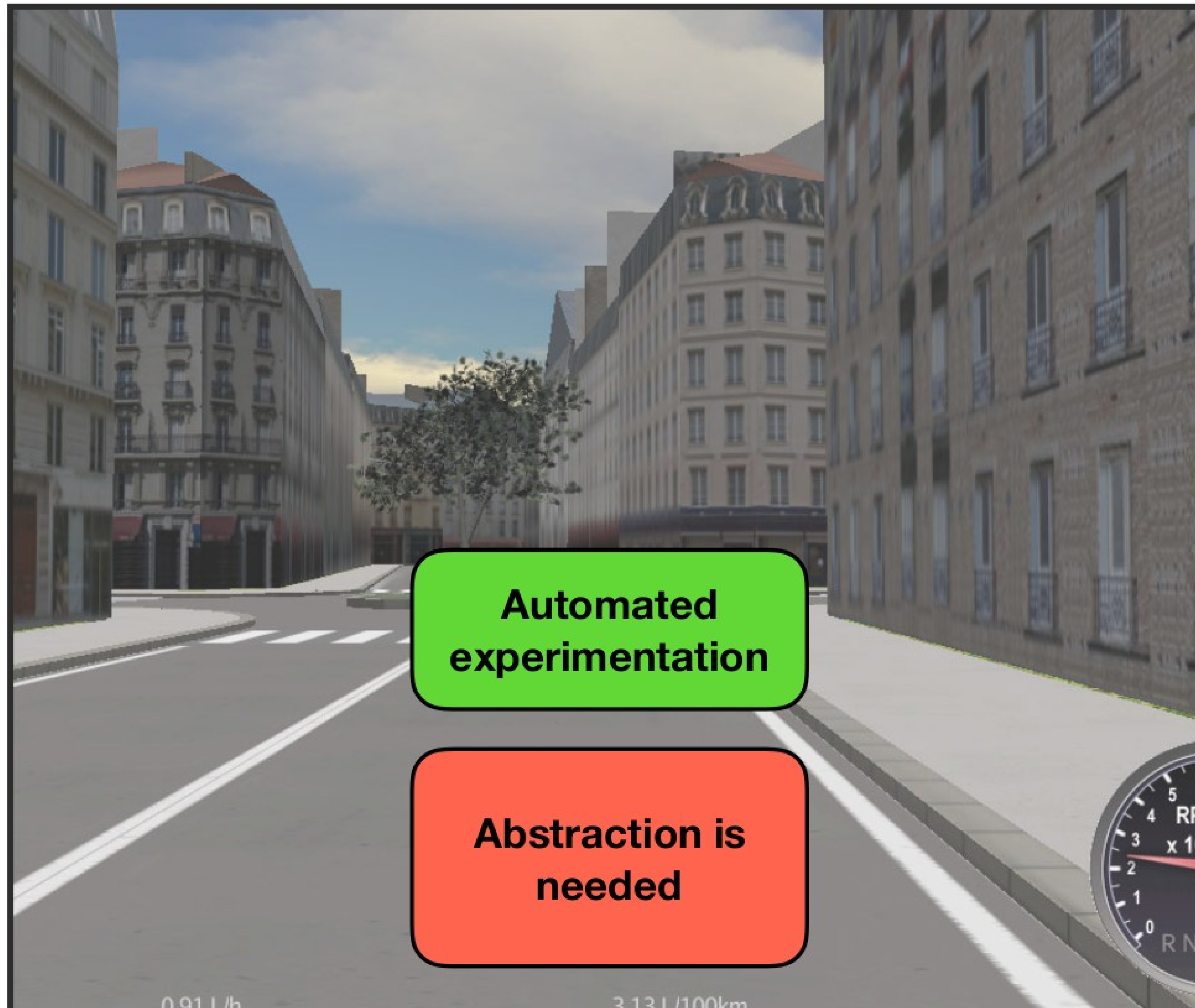
IBISC Laboratory
University of Evry Val d'Essonne, University of Paris-Saclay

Behavioural analysis of autonomous vehicles

Road test approaches

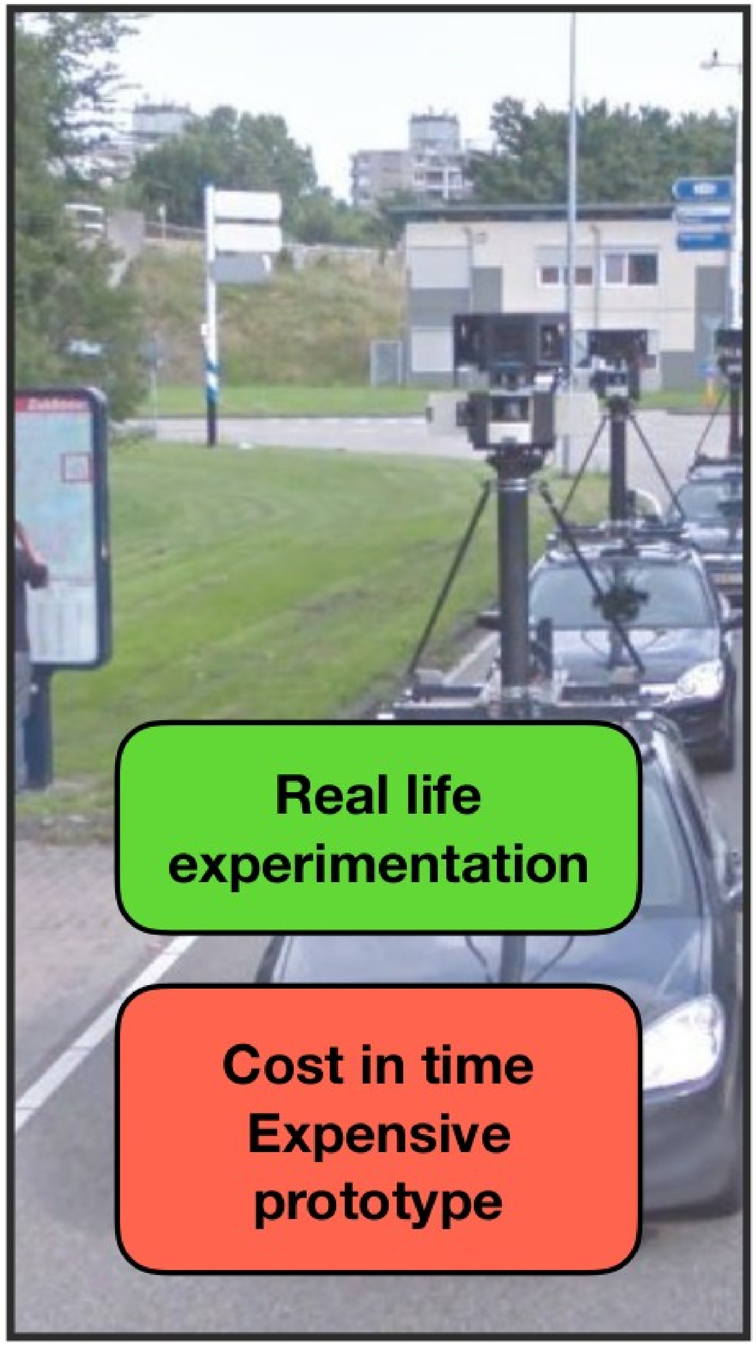


Computer based approaches

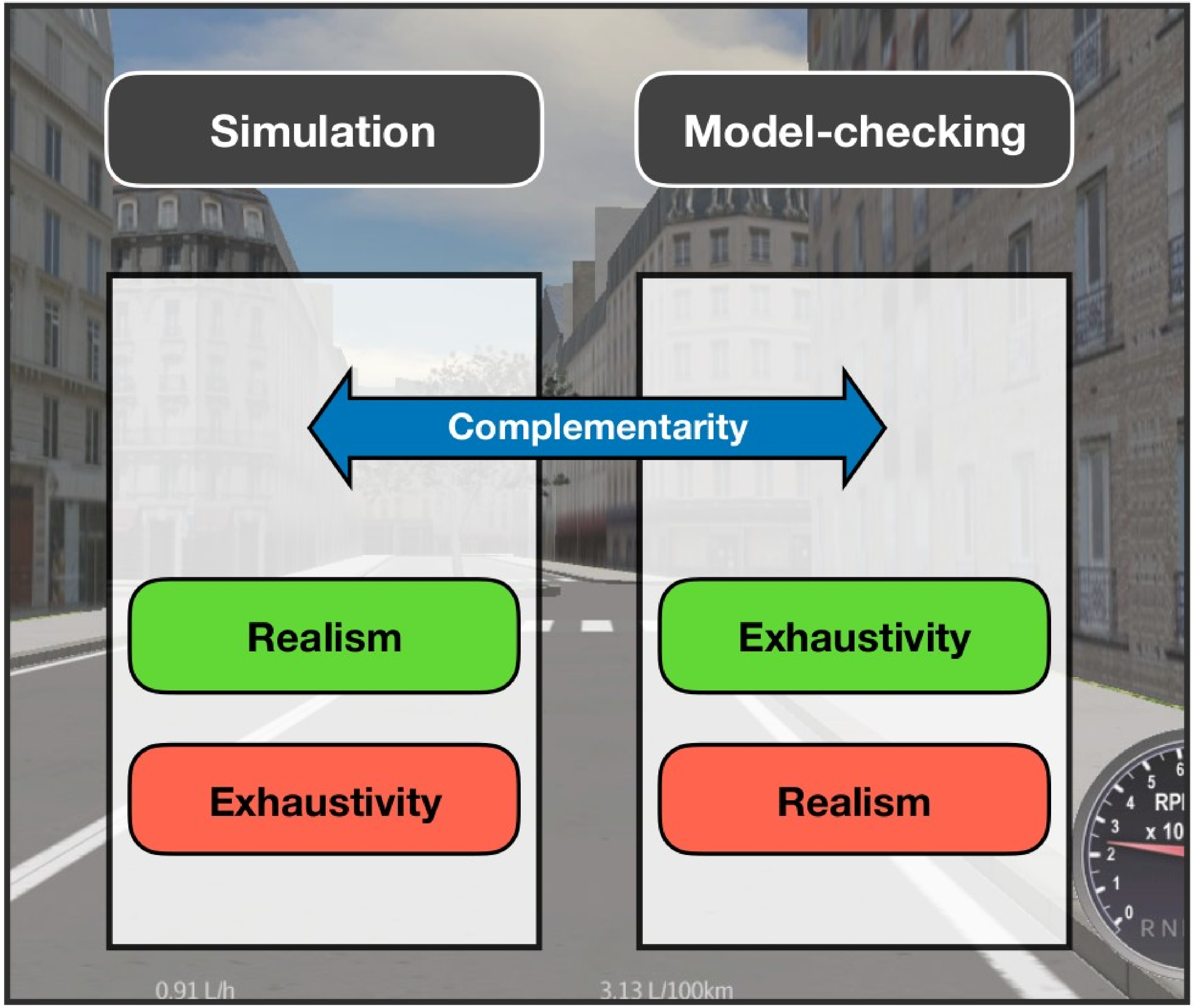


Behavioural analysis of autonomous vehicles

Road test approaches



Computer based approaches



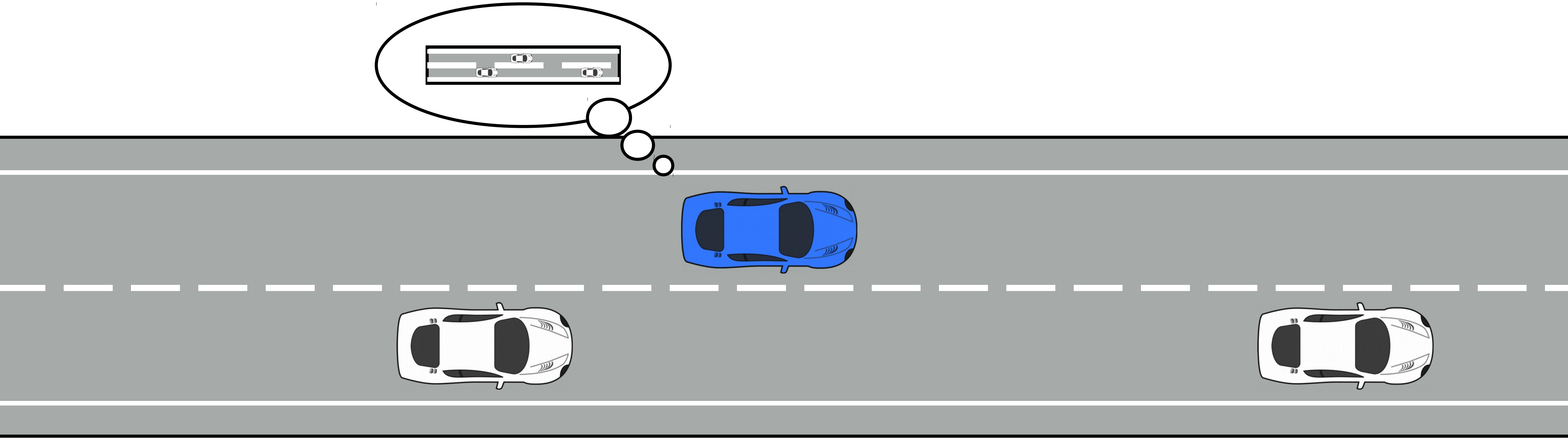
Motivation

- Real time decision
- Distributed interactions
- Various initial environments

How to exhaustively evaluate decision of agents in such system ?

Model and data structure

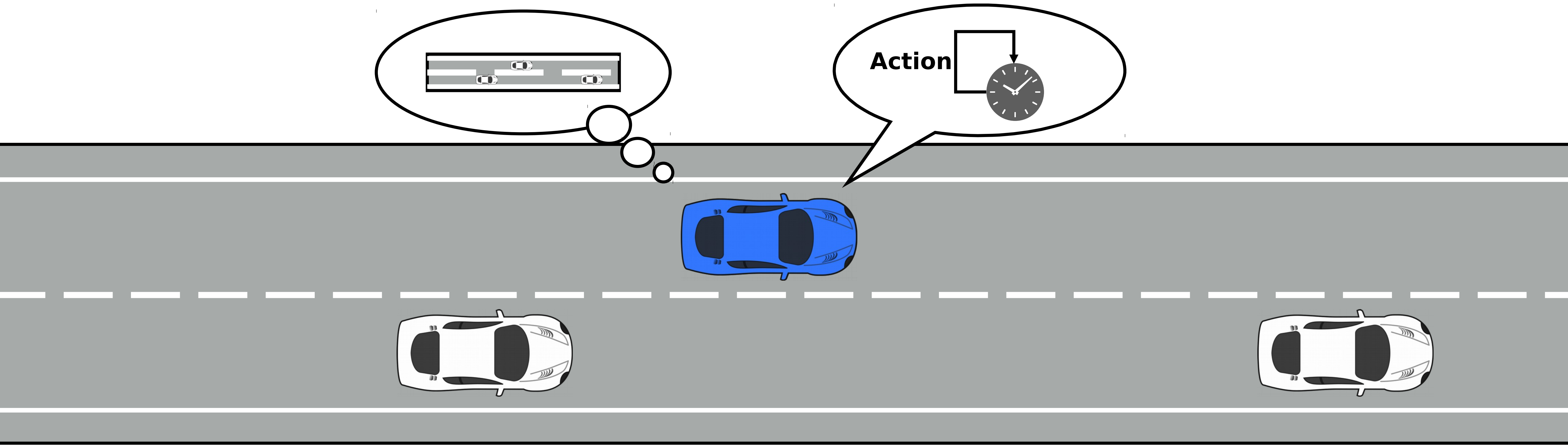
A data structure containing information on agents



Model and data structure

A data structure containing information on agents

Actions performed at a given frequency

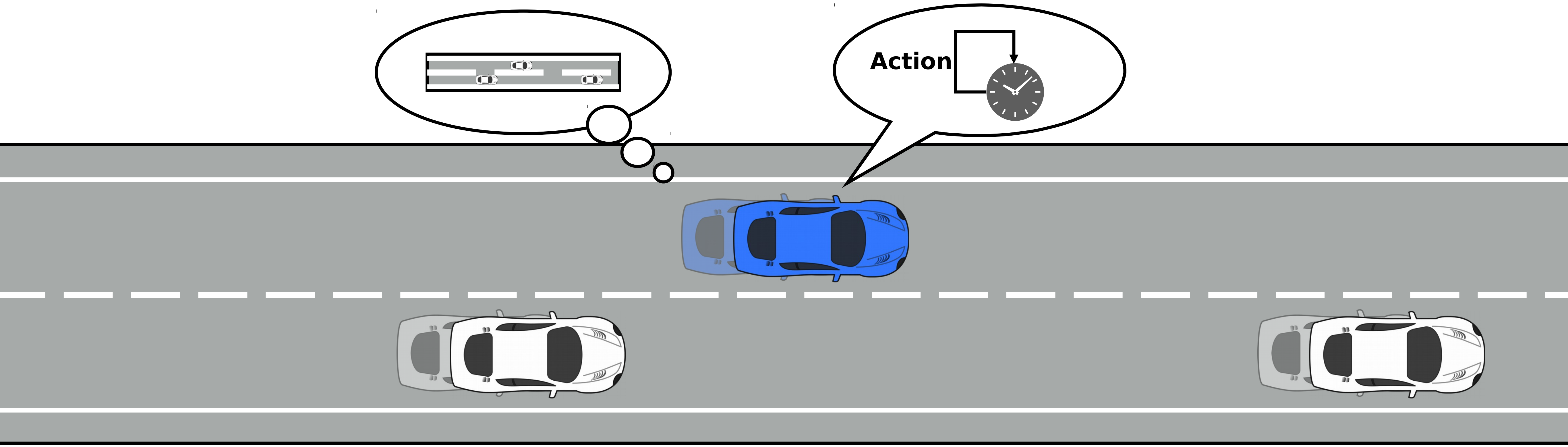


Model and data structure

A data structure containing information on agents

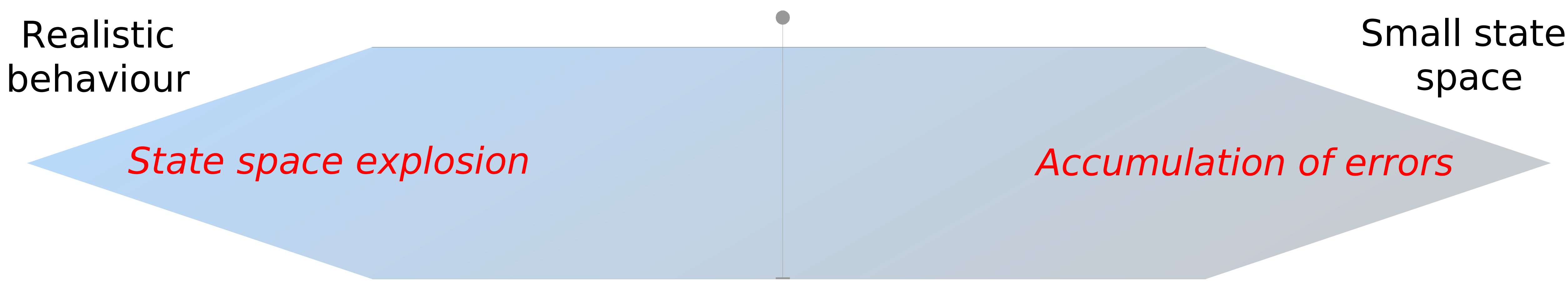
Actions performed at a given frequency

Each agent's state updated simultaneously



Discretization for model-checking

Which compromise between realism and size of the state space ?



Interdependence of variables

Parameters of the system such as update frequency, size of the road, bounds for speed and acceleration, ...

Impacts

Granularity and range of speed, acceleration and both lateral and longitudinal position.

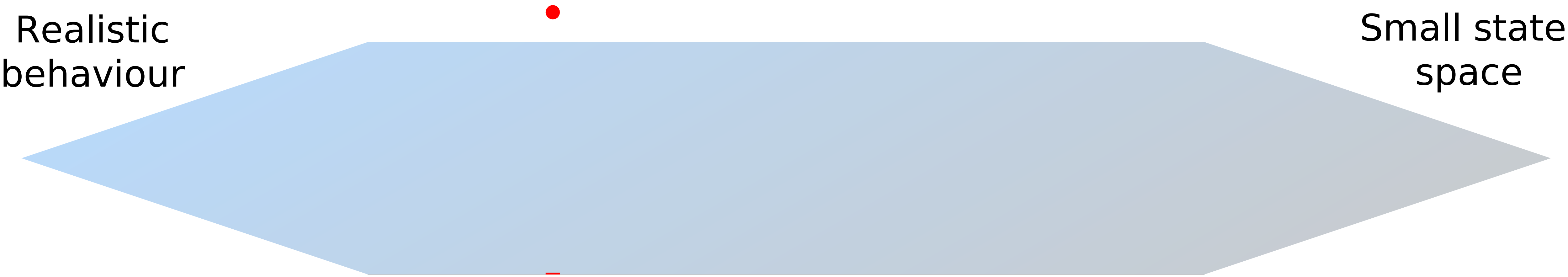
Interdependence of variables

Parameters of the system such as update frequency, size of the road, bounds for speed and acceleration, ...

Granularity and range of speed, acceleration and both lateral and longitudinal position.

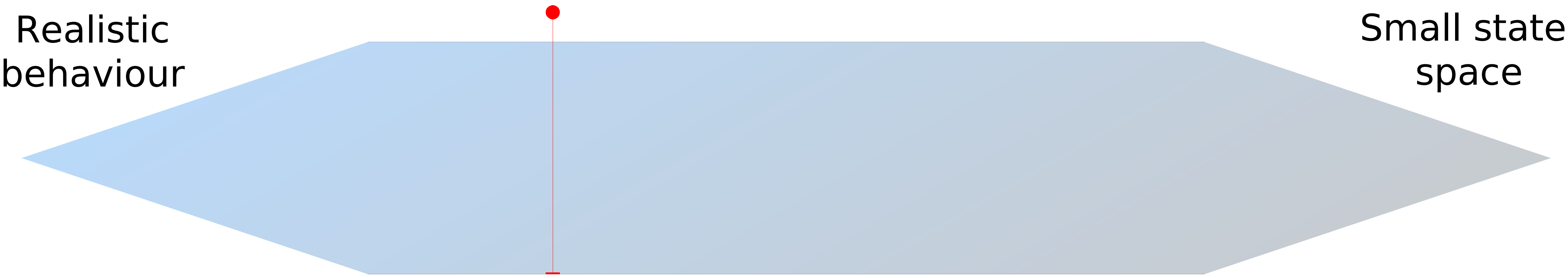
Controlling the size of the state space

Granularities and ranges for optimal precision is defined automatically according to parameters.



Controlling the size of the state space

Granularities and ranges for optimal precision is defined automatically according to parameters.

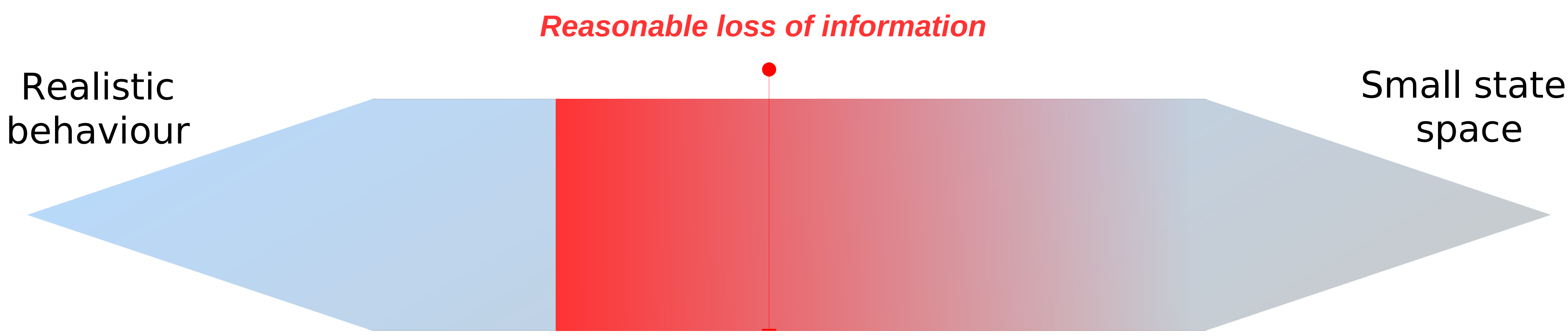


Example

Update = 10 Hz (0.1 s)
Acceleration Gran. = 1 m/s² → **Position Gran. = 5 mm**

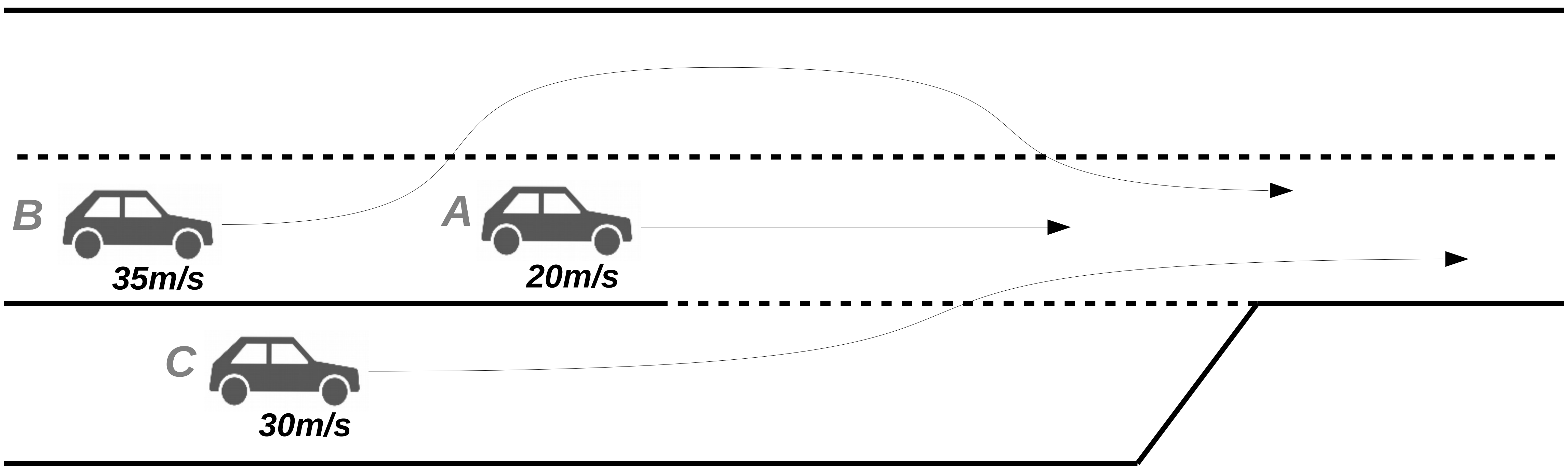
Controlling the size of the state space

Granularities and ranges for optimal precision is defined automatically according to parameters.



To reduce the size of the model, we introduce the loss of precision as a parameter in m/s that define a greater Position Gran.

Experiments



CTL queries

Exists *B* overtakes *A*	T
Always *B* overtakes *A*	F
Exists *C* overtakes *A*	T
Always *C* overtakes *A*	T
Exists *B* overtakes *C*	F
Always *B* overtakes *C*	F

Non-determinism comes from the timed intervals in which actions occur, leading to concurrency between actions of different agents.

Combination with simulation

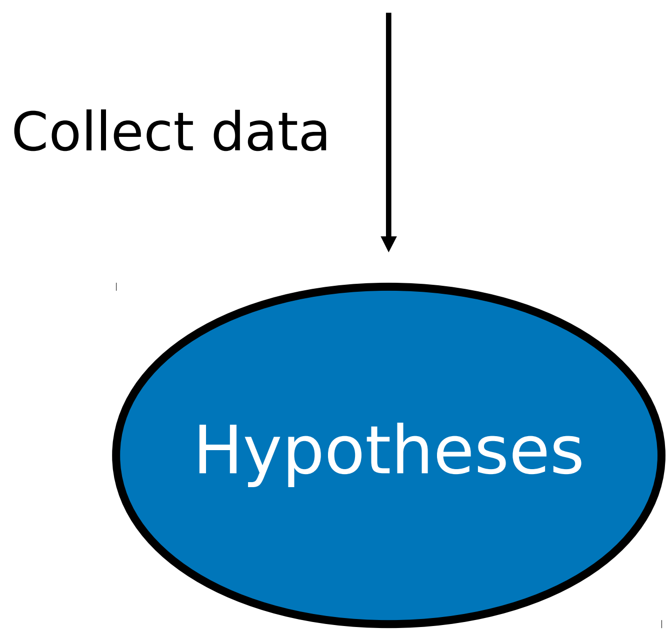
Simulation's realism + Model checking's exhaustivity

How to combine approaches with different levels of abstraction ?

Combination with simulation

Simulation's realism + Model checking's exhaustivity

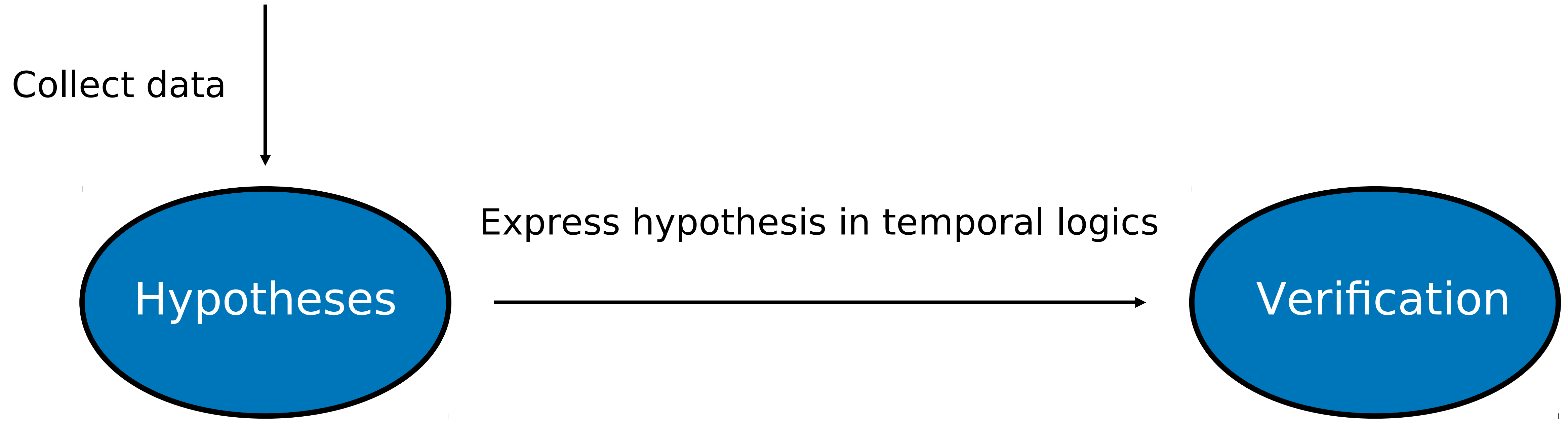
How to combine approaches with different levels of abstraction ?



Combination with simulation

Simulation’s realism + Model checking’s exhaustivity

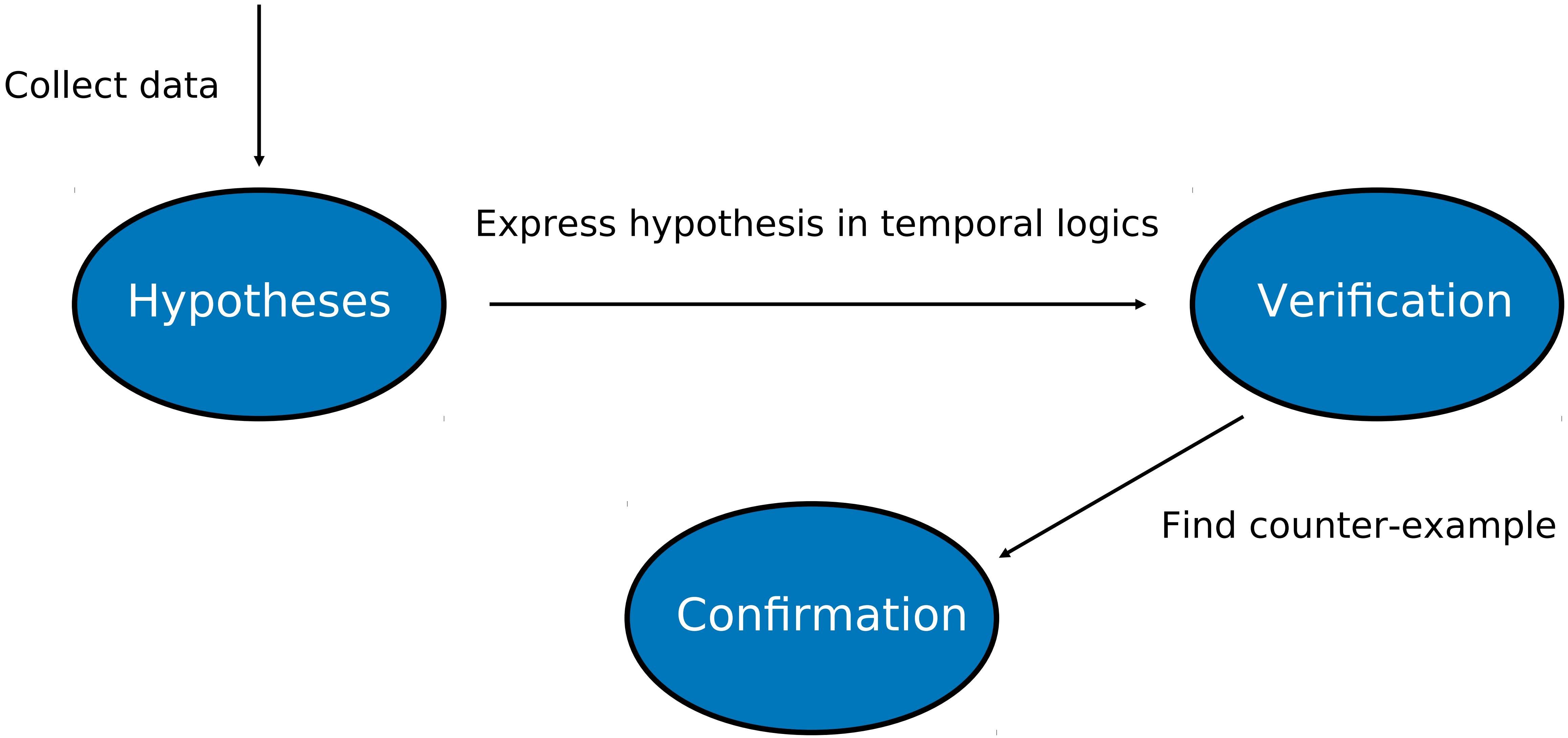
How to combine approaches with different levels of abstraction ?



Combination with simulation

Simulation's realism + Model checking's exhaustivity

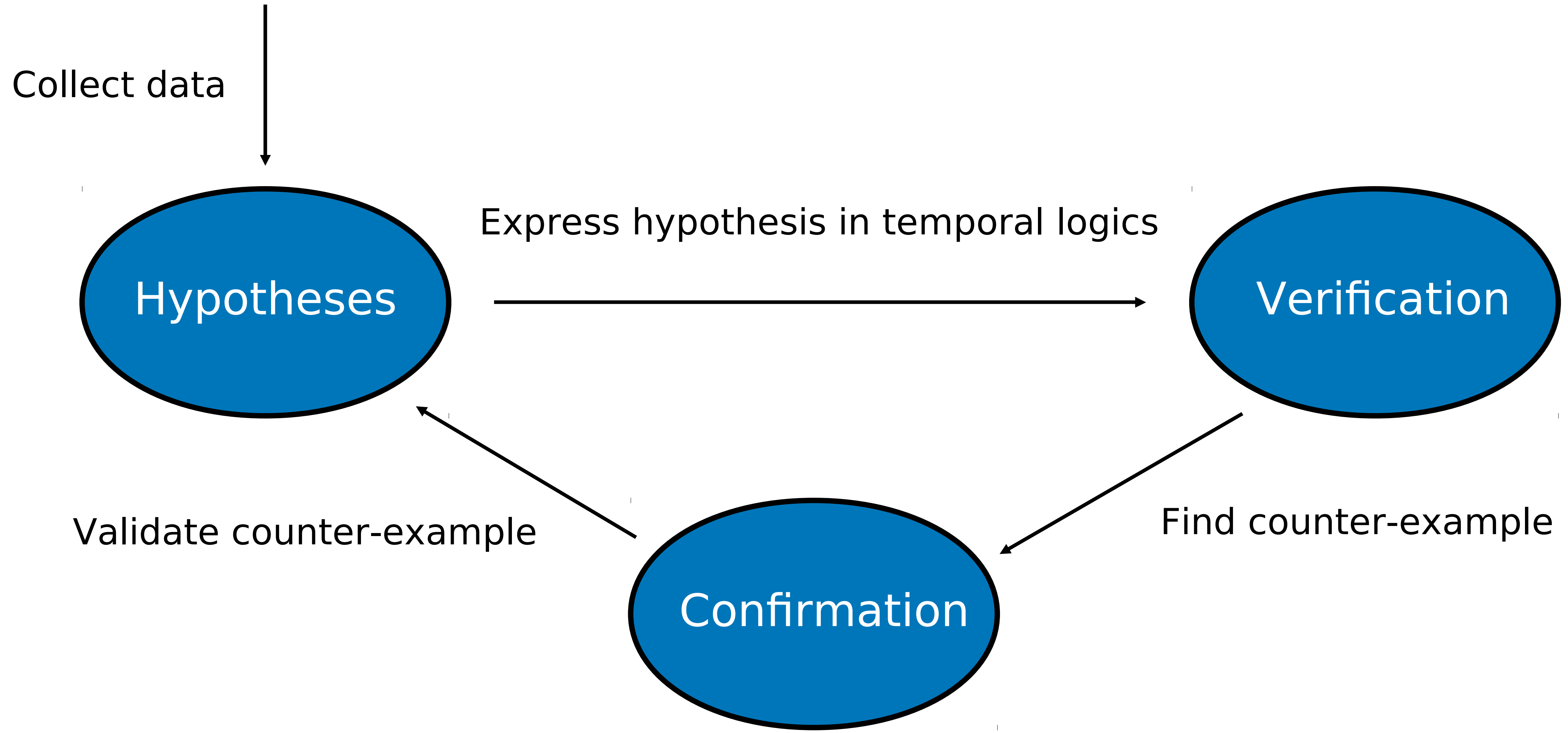
How to combine approaches with different levels of abstraction ?



Combination with simulation

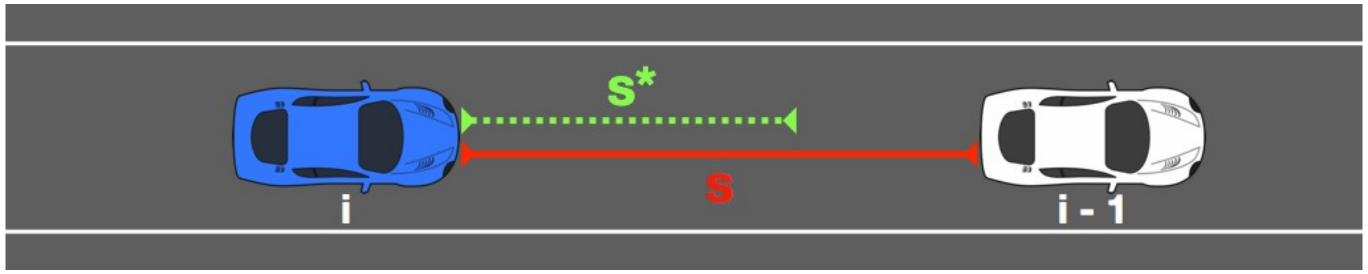
Simulation's realism + Model checking's exhaustivity

How to combine approaches with different levels of abstraction ?



Case study : IDM (Intelligent Driver Model)

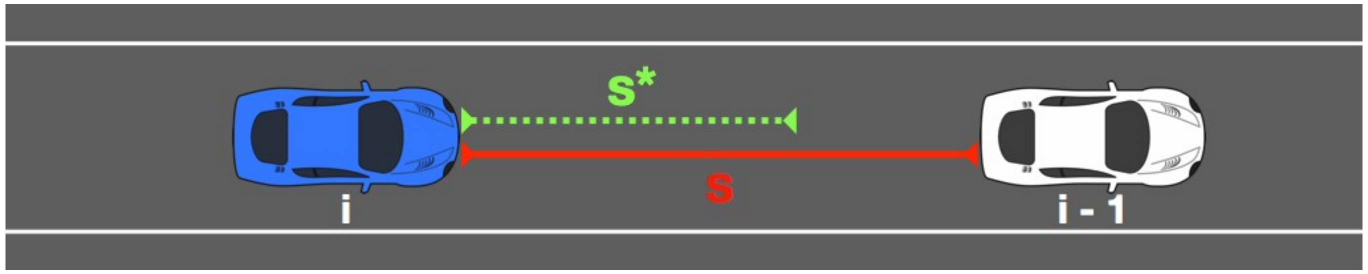
Car following model



$$\frac{dv}{dt} = a\left[1 - \left(\frac{v}{v_0}\right)^{\delta} - \left(\frac{s^*(v,\Delta v)}{s}\right)^{2}\right]$$

Case study : IDM (Intelligent Driver Model)

Car following model



$$\frac{dv}{dt} = a\left[1 - \left(\frac{v}{v_0}\right)^{\delta} - \left(\frac{s^*(v,\Delta v)}{s}\right)^2\right]$$

Discretization for model-checking

↕

Error accumulation

↕

Possibly divergent results between the two approaches

Choice of criteria

Travel time
Time of occurence at a given event

Time-To-Collision
The time before collision between two vehicles if no action is taken

Acceleration
Maximal or minimal acceleration value under certain circumstances

Choice of criteria

Travel time

Time of occurence at a given event

$< 1\ \%$

Time-To-Collision

The time before collision between two vehicles if no action is taken

$\approx 1\ \%$

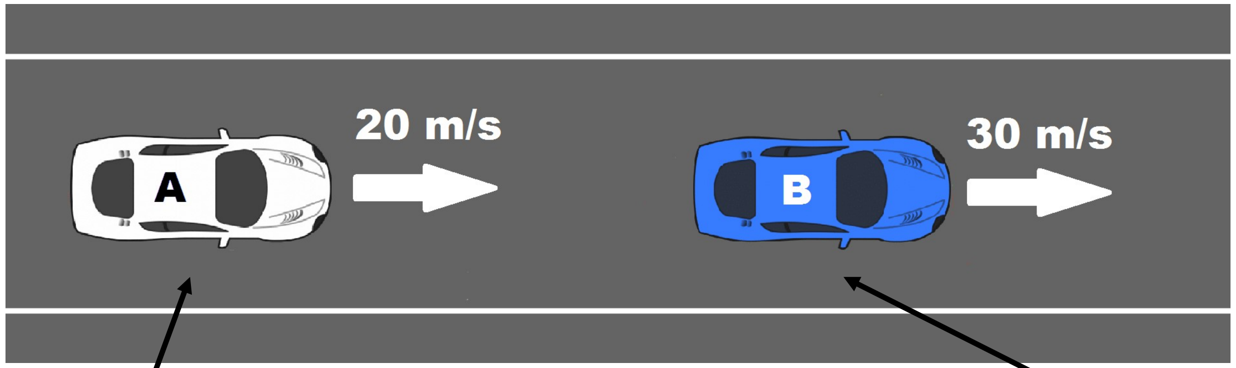
Acceleration

Maximal or minimal acceleration value under certain circumstances

$\approx 25\ \%$

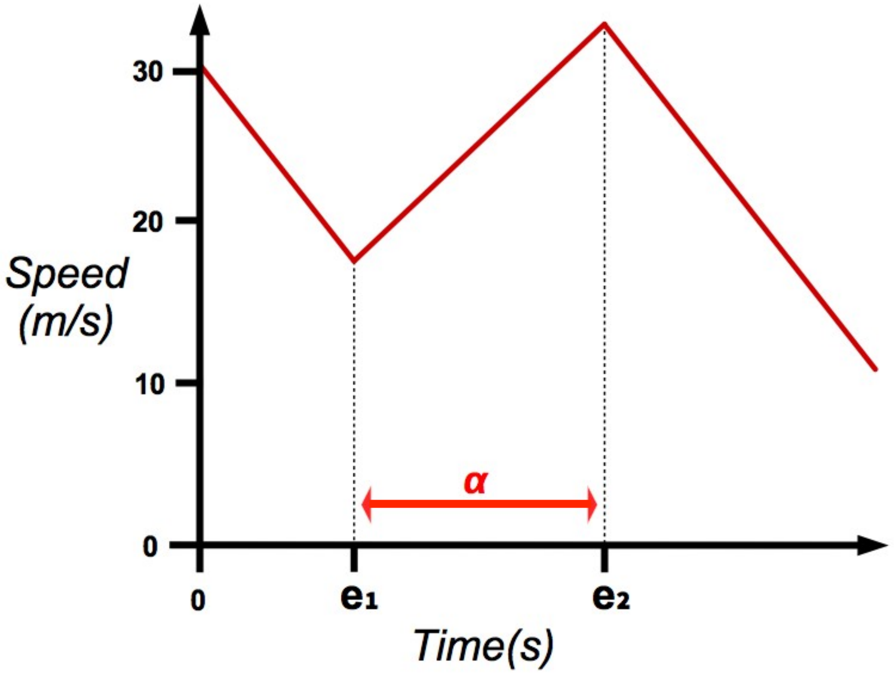
Illustration

A non-deterministic scenario



IDM control

Predefined control



Random activation

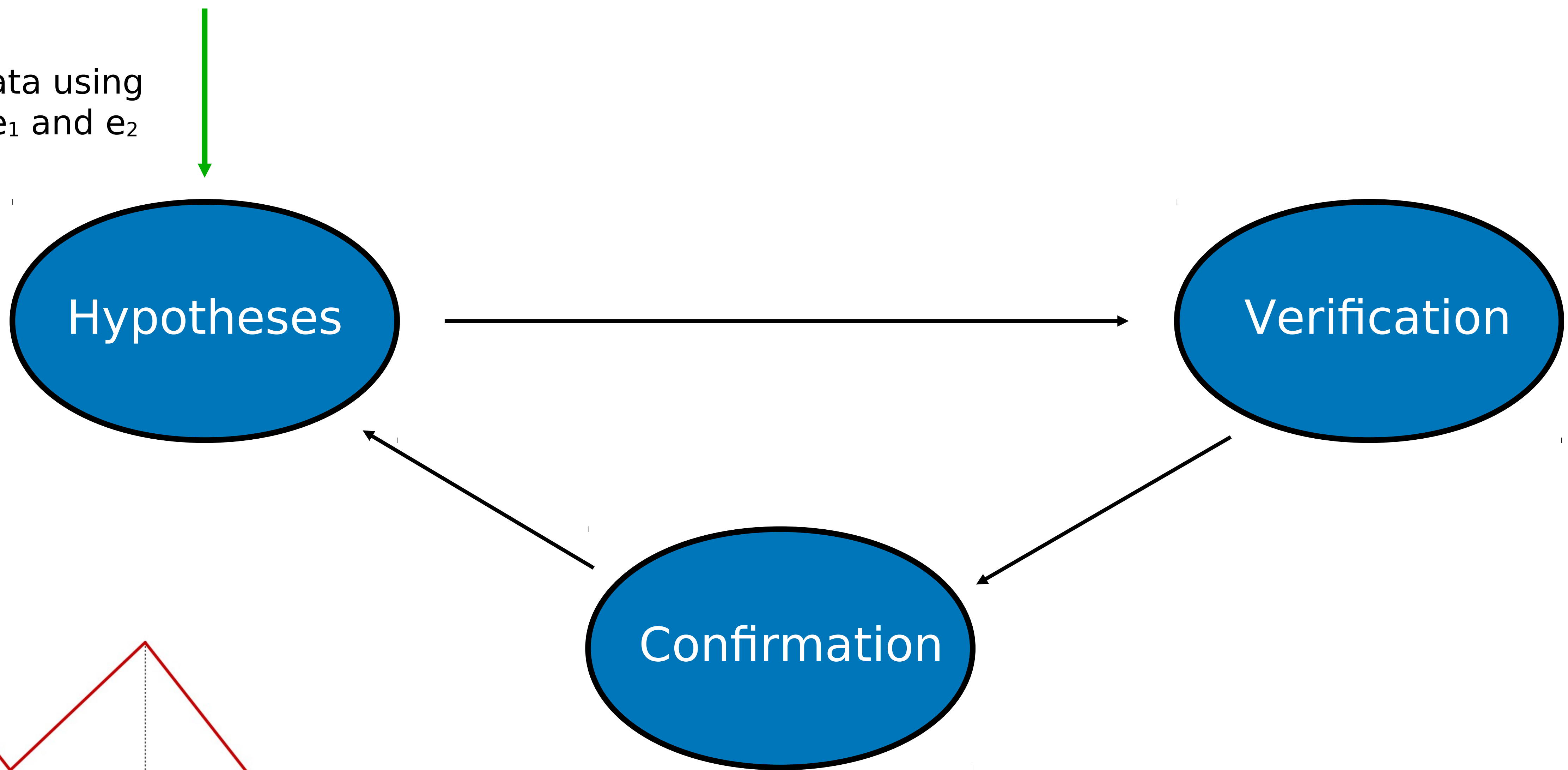
Vehicle A is initially safe

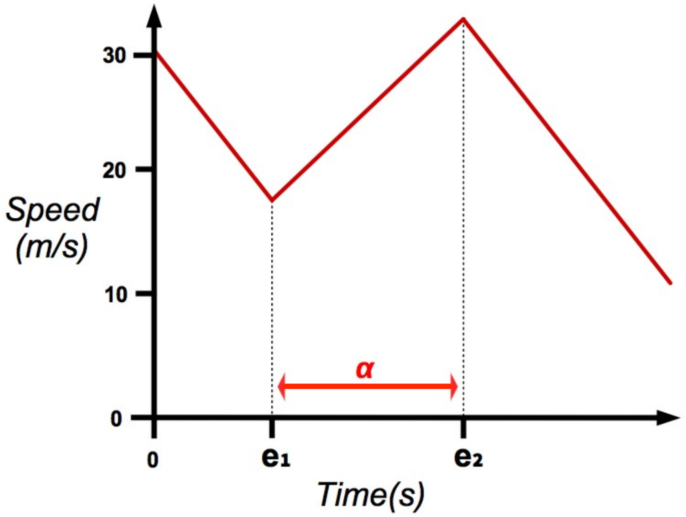
We want to analyse how it reacts to the unexpected behaviour of vehicle B

Application of the method

Hypothesis : $TTC < 1.7s \Rightarrow \alpha \in [\frac{1}{2}e_1, e_1]$

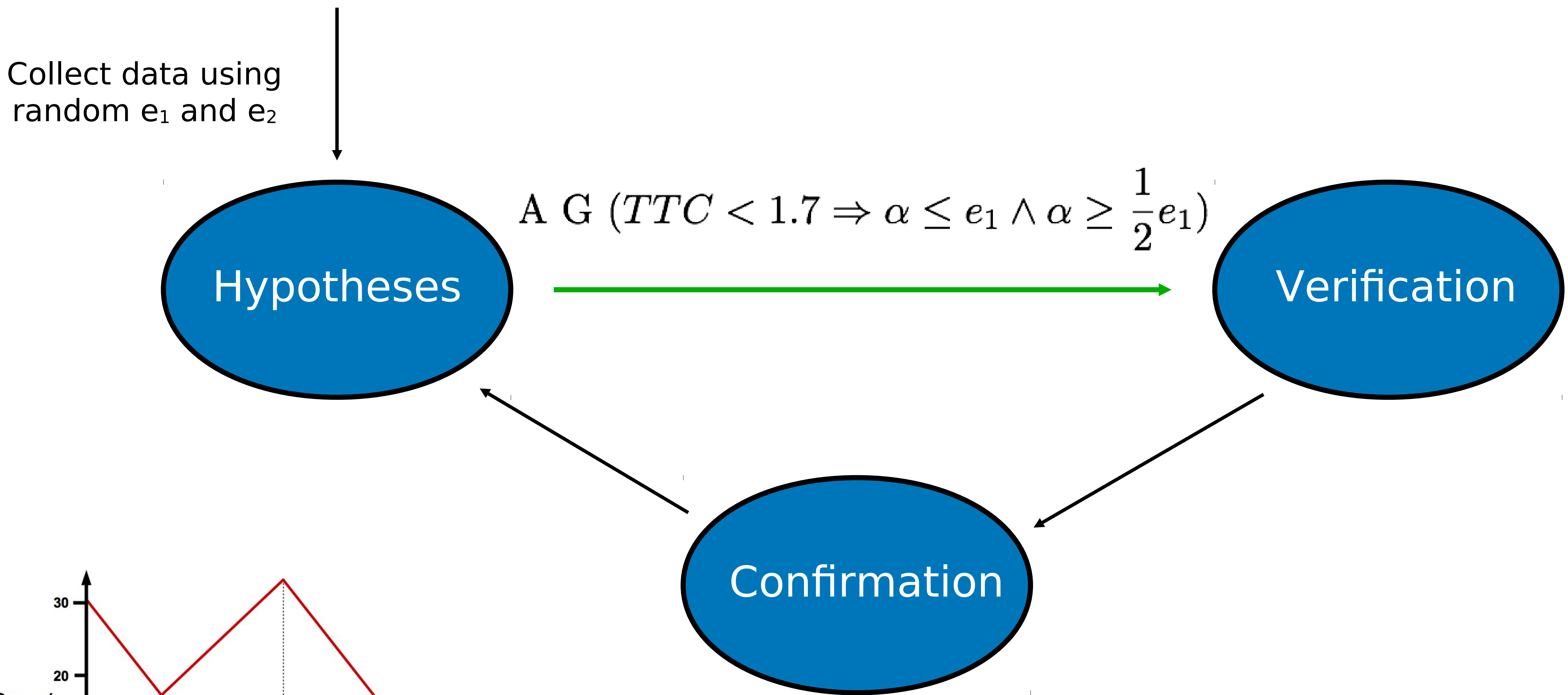
Collect data using random e_1 and e_2

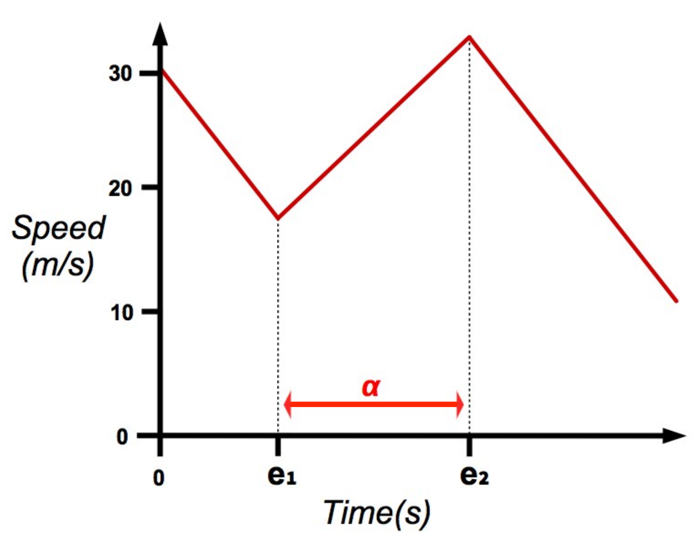




Application of the method

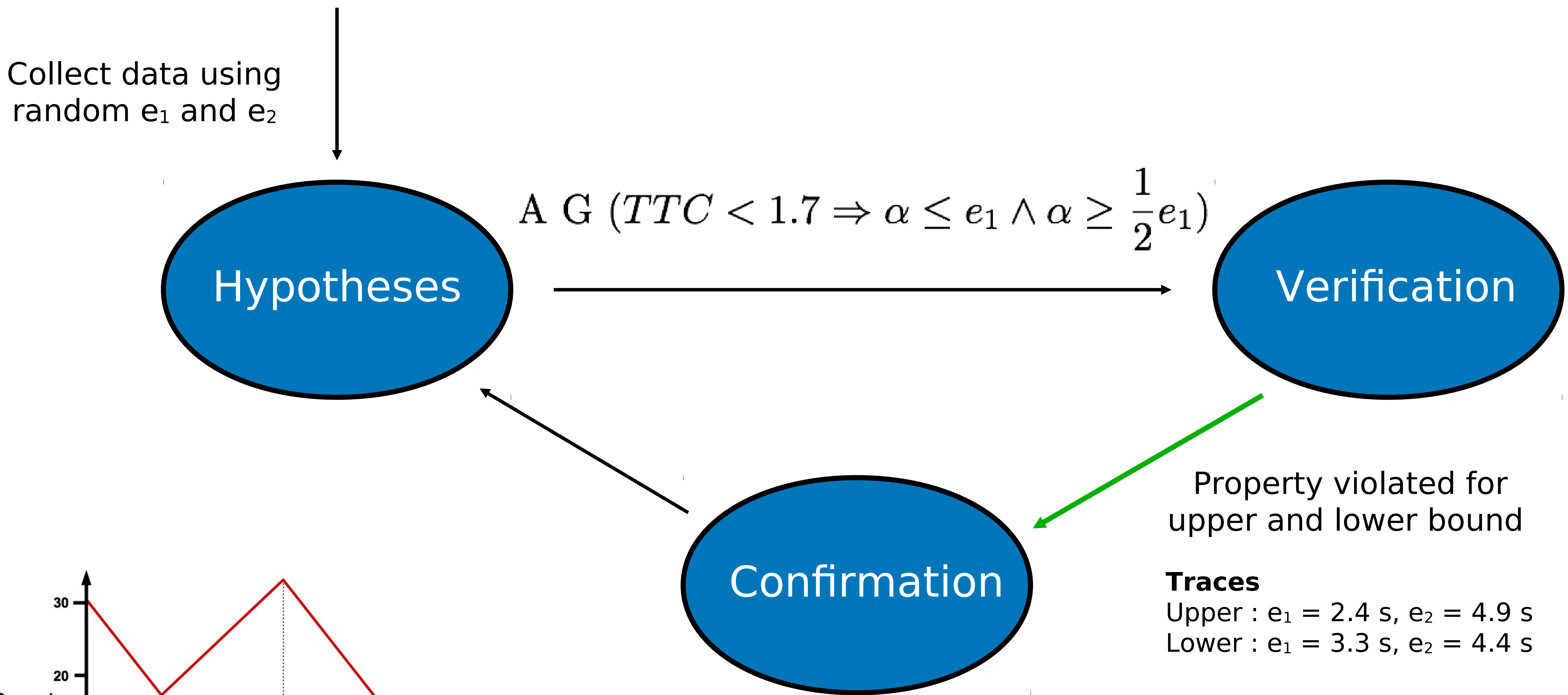
Hypothesis : $TTC < 1.7s \Rightarrow \alpha \in [\frac{1}{2}e_1, e_1]$

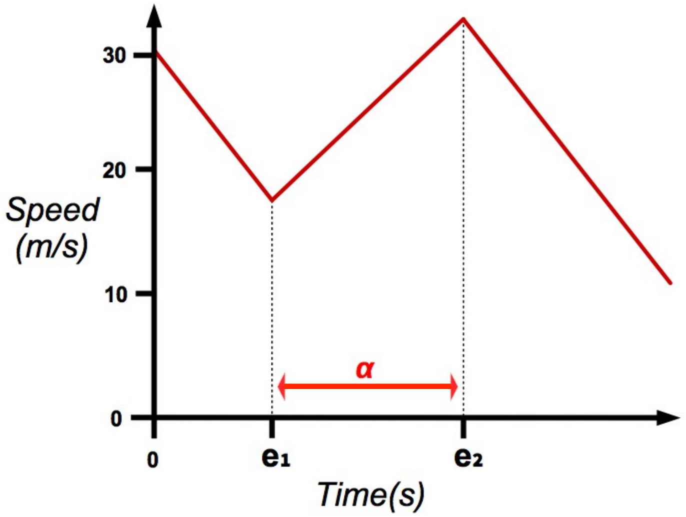




Application of the method

Hypothesis : $TTC < 1.7s \Rightarrow \alpha \in [\frac{1}{2}e_1, e_1]$





Application of the method

Hypothesis : $TTC < 1.7s \Rightarrow \alpha \in [\frac{1}{2}e_1, e_1]$

Collect data using random e_1 and e_2

Hypotheses

$$\text{A G } (TTC < 1.7 \Rightarrow \alpha \leq e_1 \wedge \alpha \geq \frac{1}{2}e_1)$$

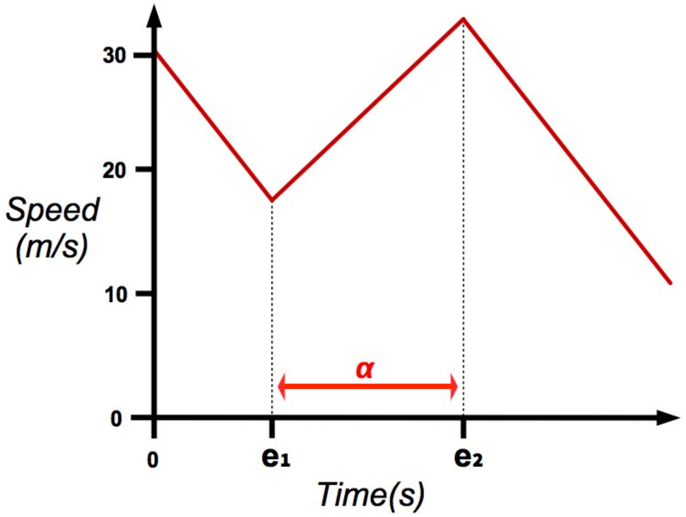
Verification

Property violated for upper and lower bound

Traces
Upper : e_1 = 2.4 s, e_2 = 4.9 s
Lower : e_1 = 3.3 s, e_2 = 4.4 s

Confirmation

Traces confirmed by simulation (no false positive)



Application of the method

New hypothesis : $TTC < 1.7s \Rightarrow \alpha \in [\frac{3}{10}e_1, \frac{11}{10}e_1]$

Collect data using random e_1 and e_2

Hypotheses

$\text{A G } (TTC < 1.7 \Rightarrow \alpha \leq e_1 \wedge \alpha \geq \frac{1}{2}e_1)$

Verification

Property violated for upper and lower bound

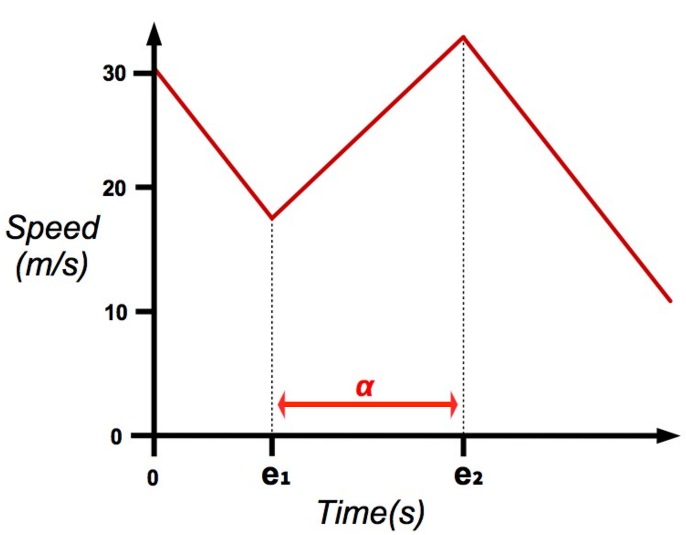
Traces

Upper : e_1 = 2.4 s, e_2 = 4.9 s

Lower : e_1 = 3.3 s, e_2 = 4.4 s

Confirmation

Traces confirmed by simulation (no false positive)



Conclusion and perspectives

- Design and implementation of a parametric model of communicating autonomous cars.
- Controlled size of the state space
- Efficient combination with simulation for validation
- Conclusive experiments featuring fault injection and complex communication was performed with the model

Conclusion and perspectives

- Design and implementation of a parametric model of communicating autonomous cars.
- Controlled size of the state space
- Efficient combination with simulation for validation
- Conclusive experiments featuring fault injection and complex communication was performed with the model

---

Ongoing work : towards more expressivity

- Exploit characteristics of the application
- High level Petri net approach via Zinc
- On-the-fly exploration of the state space
- Heuristics for efficiency

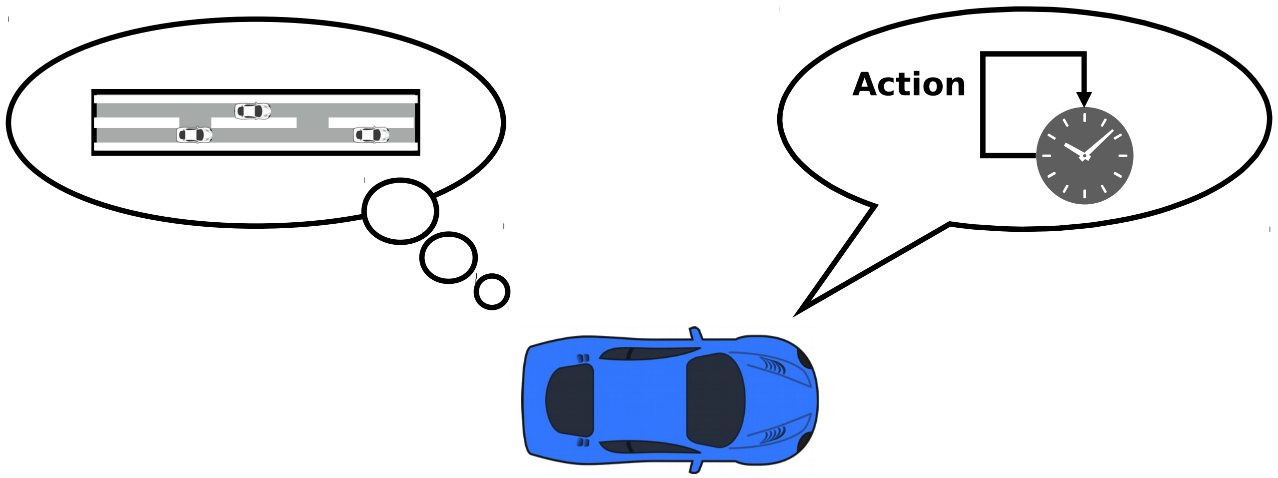
Merci pour votre attention

J. Arcile, R. Devillers, H. Klaudel, W. Klaudel, and B. Wozna-Szczesniak
Modeling and checking robustness of communicating autonomous vehicles.
In Distributed Computing and Artificial Intelligence, Springer, 2018

J. Arcile, J. Sobieraj, H. Klaudel, and G. Hutzler
Combination of simulation and model-checking for the analysis of autonomous vehicles' behaviors: a case study.
In Multi-Agent Systems and Agreement Technologies, Springer, 2018

J. Arcile, R. Devillers and H. Klaudel
VerifCar: A framework for modeling and model checking communicating autonomous vehicles
Accepted for Journal of Autonomous Agents and Multi-Agent Systems, Springer, 2019

Tools



Simulation	Model-checking
Multi-agent system representation of the environment	Network of timed automata associated with data structure
Fast exploration of complex scenarios	Automated scaling of discrete types
Using GAMA	Using UPPAAL