IMoST
Integrated Modelling for Safe Transportation

Modellbasierte Analyse des dynamischen Verhaltens von Mensch-Maschine-Systemen

IMoST-Teilprojekt AN: Analysis

Werner Damm, Martin Fränzle, Hardi Hungar,
Stephanie Kemper, Frank Köster, Michael Langner,
Christoph Läsche, Ernst-Rüdiger Olderog, Jan Patrick Osterloh,
Joachim Peinke, Stefan Puch, Gerald Sauter, Bertram Wortelen

CARL VON OSSIETZKY universität OLDENBURG

OFFIS INSTITUT FÜR INFORMATIK

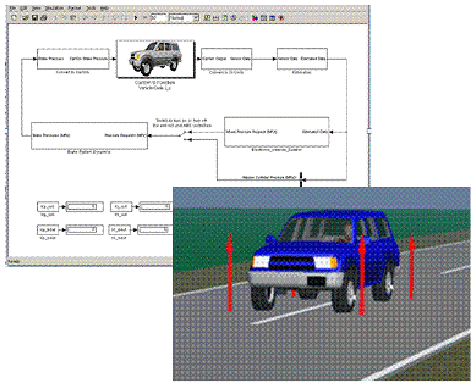
DLR Deutsches Zentrum für Luft- und Raumfahrt e.V. in der Helmholtz-Gemeinschaft

IMoST AN's Mission

To support the prediction of the safety impact of an ADAS in early design phases

- *based on a model-based analysis process,*
- *taking into account human-in-the-loop dynamics,*
- *providing quantitative figures.*

Model-based analysis in the design of advanced driver assistance systems

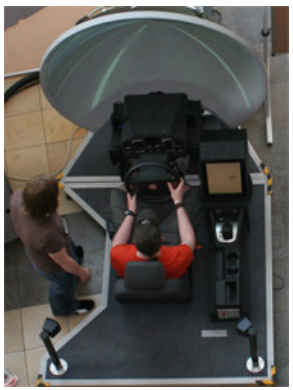
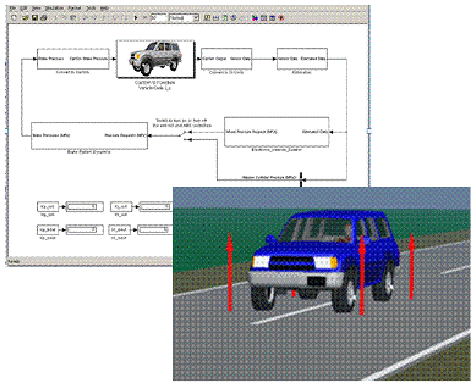


realism
cost & time
risk

availability
speed
coverage

Model-based analysis in the design of advanced driver assistance systems



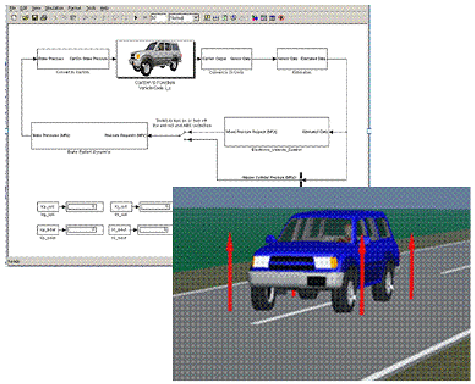



realism
cost & time
risk

availability
speed
coverage

All the usual benefits from model–based design:
A thousand design flaws eliminated before the first expensive prototype is built.

Model-based analysis in the design of advanced driver assistance systems



realism
cost & time
risk

availability
speed
coverage

All the usual benefits from model–based design:
A thousand design flaws eliminated before the first expensive prototype is built.

Enhances safety analysis:
Improved coverage of risky situations, rare situations, hard to provoke situtations...

The challenge

To achieve reliable predictions of

- behavior and
- safety impact

of assistance systems from extremely heterogeneous models incorporating

- diverse types of agent models
  - operator models, covering cognition, perception, and motor behavior
  - vehicle and environment dynamics
  - assistance and control systems (functional and non-funct. aspects)
- with various forms of probabilistic and non-deterministic behavior
  - unmodelled entities, open inputs, parameter variations, noise, etc.
  - mental states & decisions
- and a plethora of temporal interaction patterns
  - hybrid time featuring durational and instantaneous actions
  - event-driven, time-driven, and rate-driven dynamics

The challenge

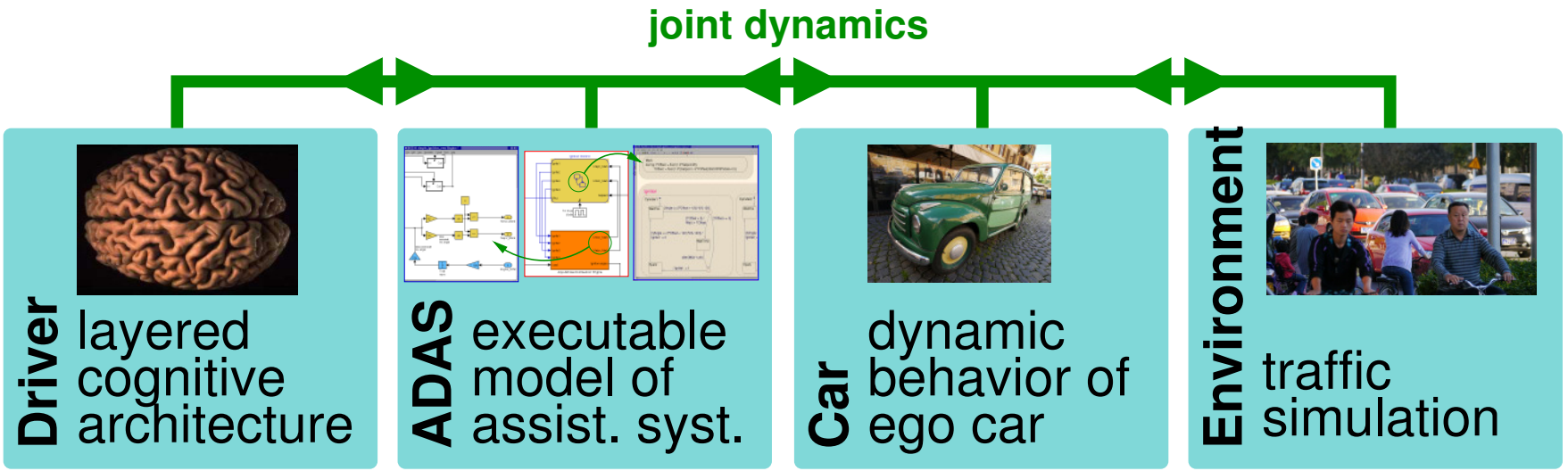
To achieve reliable predictions of

- behavior and
- safety impact

of assistance systems from extremely heterogeneous models incorporating

- diverse types of agent models
  - operator models, covering cognition, perception, and motor behavior
  - vehicle and environment dynamics
  - assistance and control systems (functional and non-funct. aspects)
- with various forms of probabilistic and non-deterministic behavior
  - unmodelled entities, open inputs, parameter variations, noise, etc.
  - mental states & decisions
- and a plethora of temporal interaction patterns
  - hybrid time featuring durational and instantaneous actions
  - event-driven, time-driven, and rate-driven dynamics

> *"Prediction is very difficult, especially about the future."*
> [Niels Bohr]

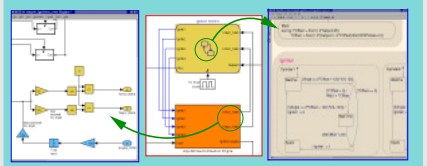

joint dynamics
Driver
layered cognitive architecture
ADAS
executable model of assist. syst.
Car
dynamic behavior of ego car
Environment
traffic simulation

joint dynamics

Driver

layered cognitive architecture

ADAS



executable model of assist. syst.

Car

dynamic behavior of ego car

Environment

traffic simulation

differential equations
+ (state–dependent) mode shifts
+ triggered events
= hybrid discrete–continuous systems

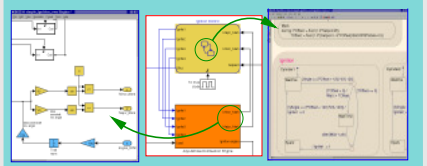
joint dynamics

Driver

layered cognitive architecture

?

ADAS



executable model of assist. syst.

Car

dynamic behavior of ego car

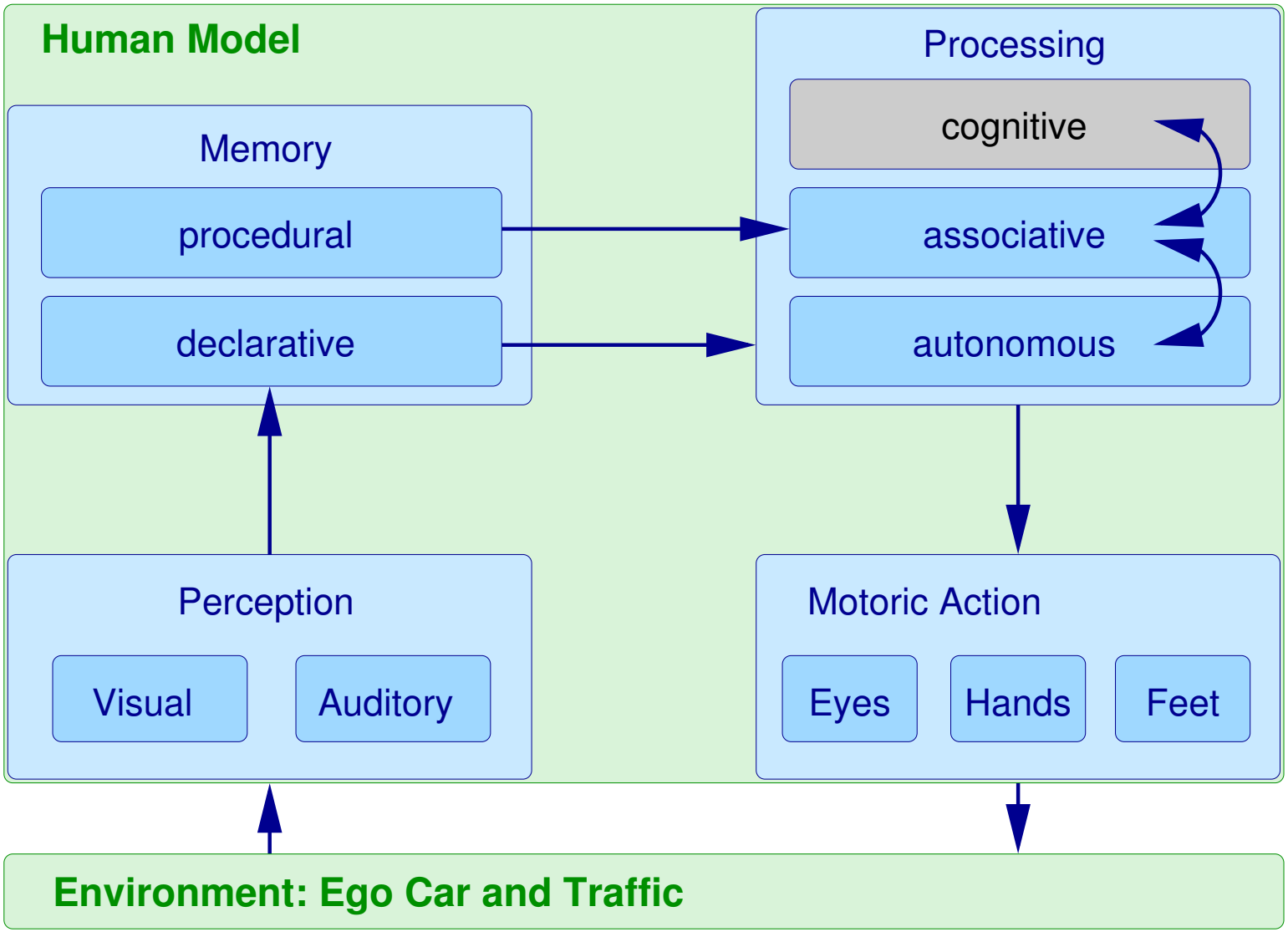
Environment

traffic simulation

differential equations
+ (state–dependent) mode shifts
+ triggered events
= hybrid discrete–continuous systems

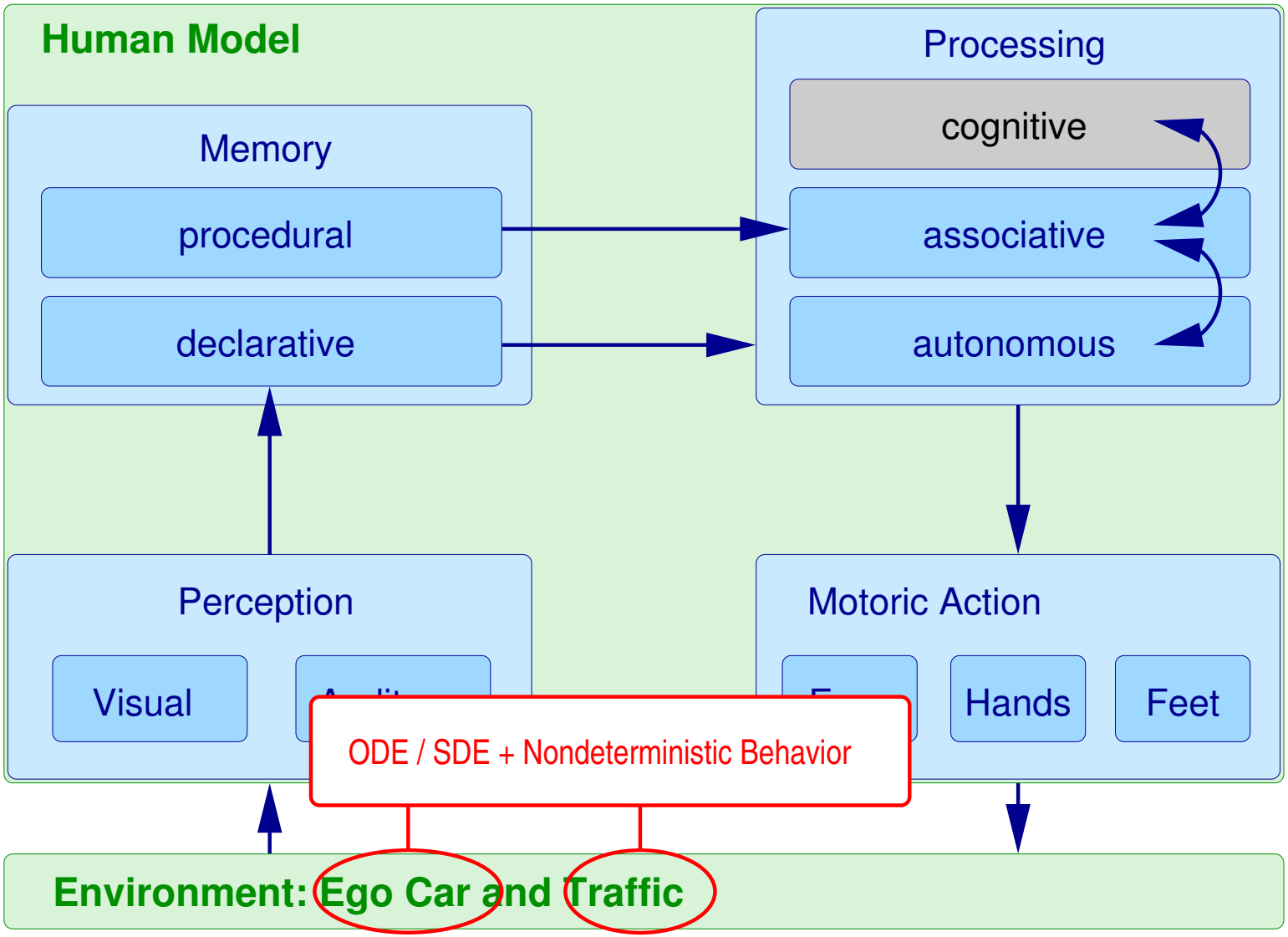
Ingredients of driver-in-the-loop model

[based on cognitive architecture CASCaS; Eilers, Lüdtke, Weber Wortelen 2008–]



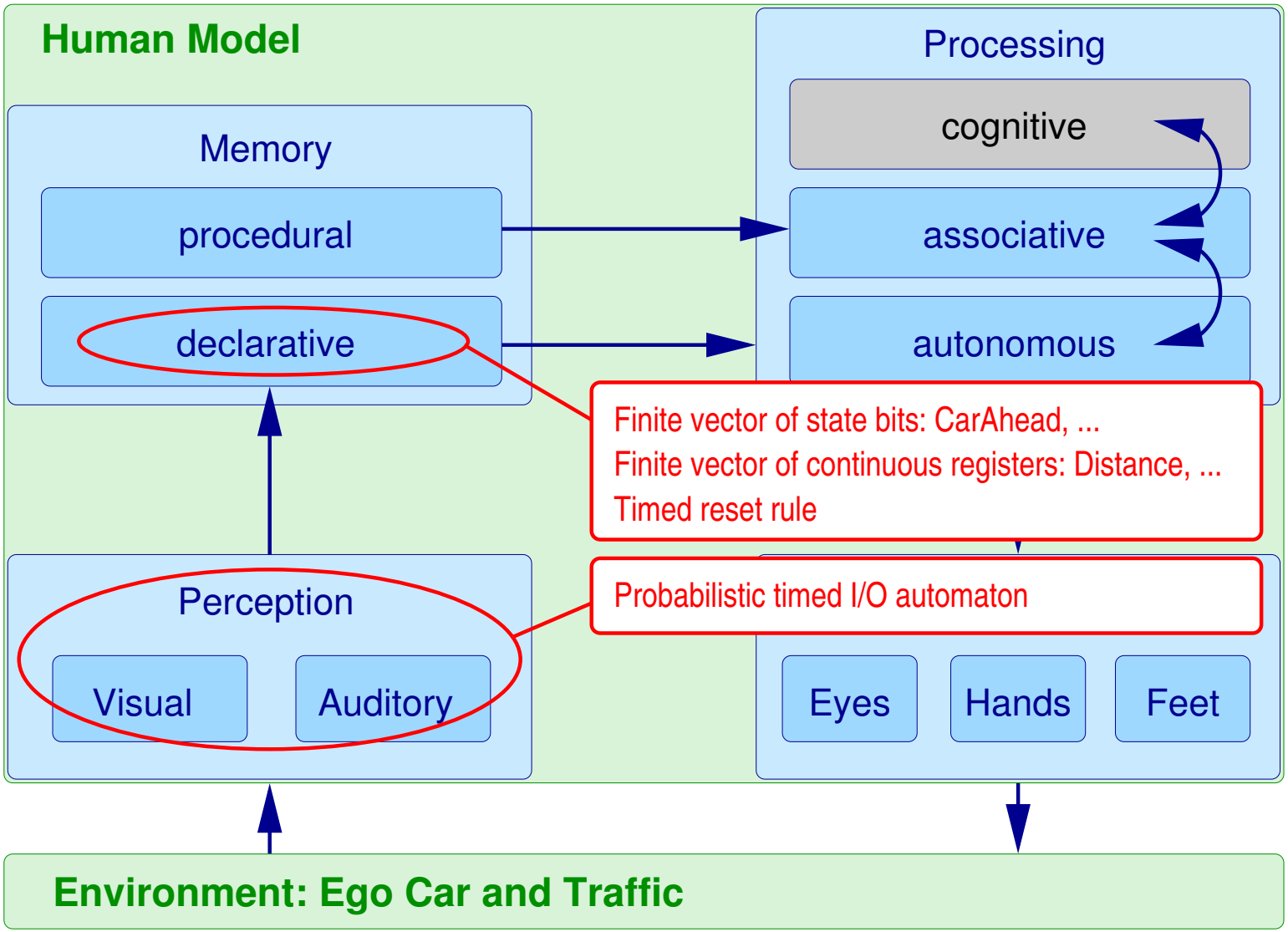
Ingredients of driver-in-the-loop model

[based on cognitive architecture CASCaS; Eilers, Lüdtke, Weber Wortelen 2008–]



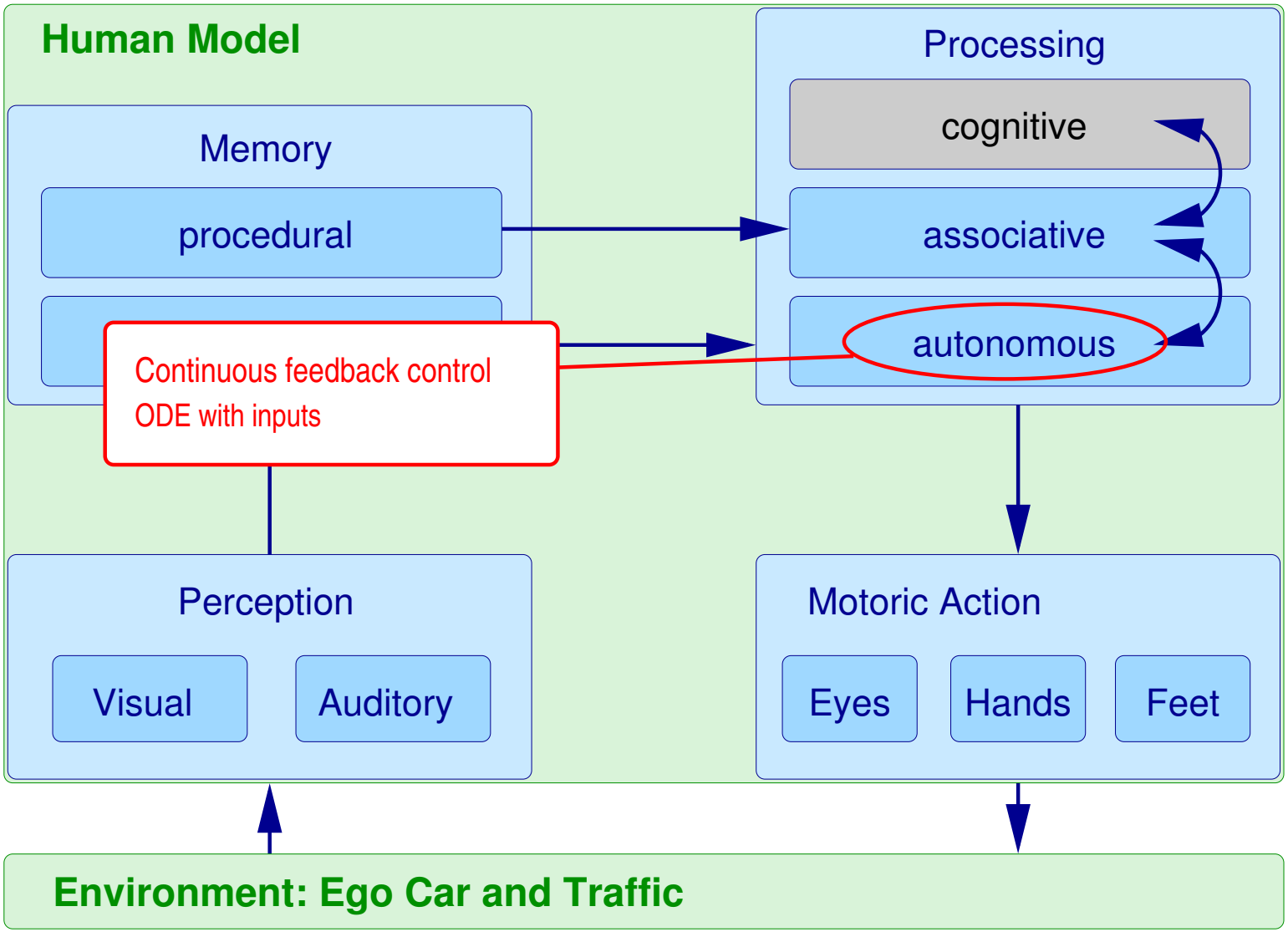
Ingredients of driver-in-the-loop model

[based on cognitive architecture CASCaS; Eilers, Lüdtke, Weber Wortelen 2008–]



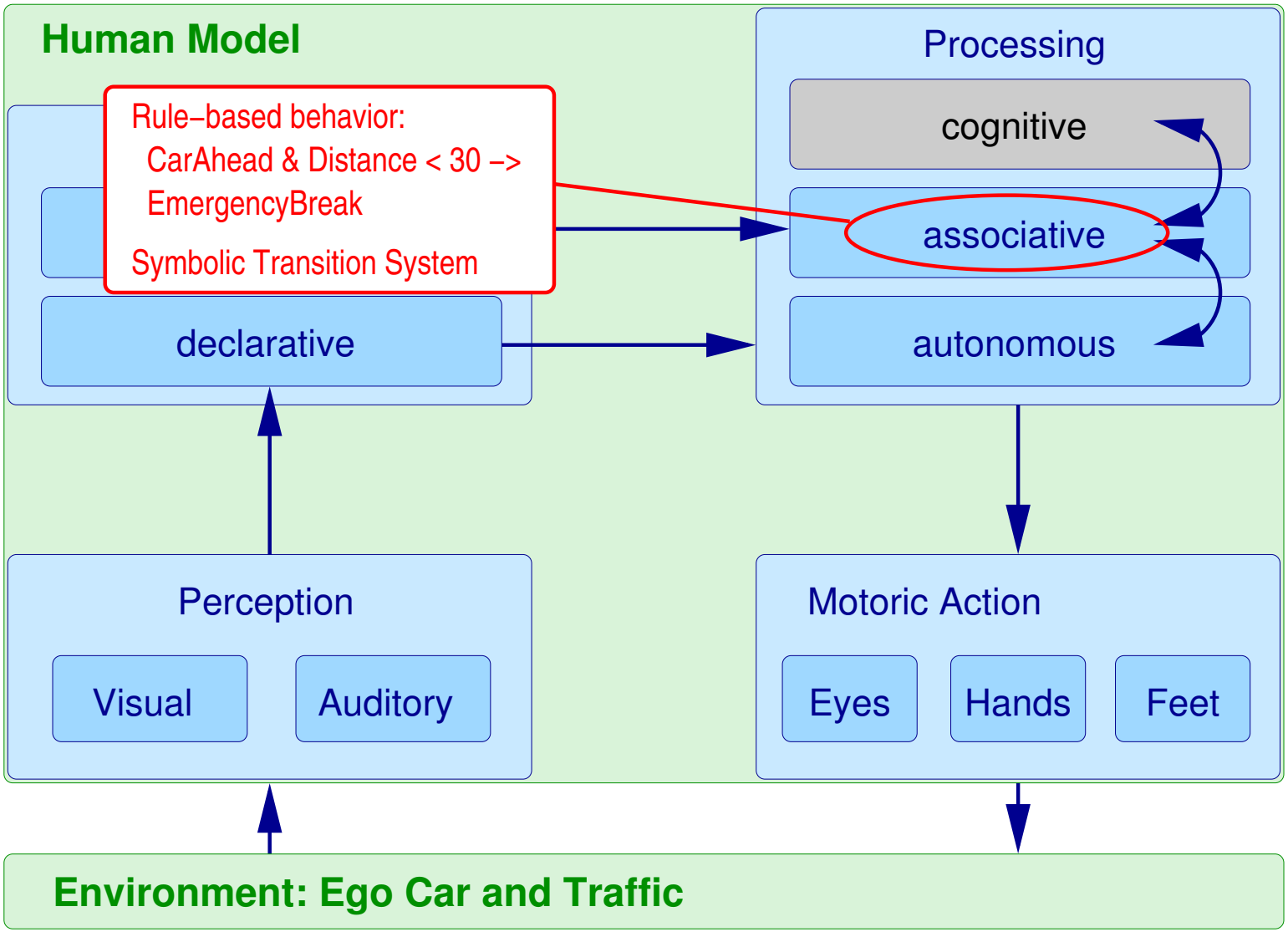
Ingredients of driver-in-the-loop model

[based on cognitive architecture CASCaS; Eilers, Lüdtke, Weber Wortelen 2008–]



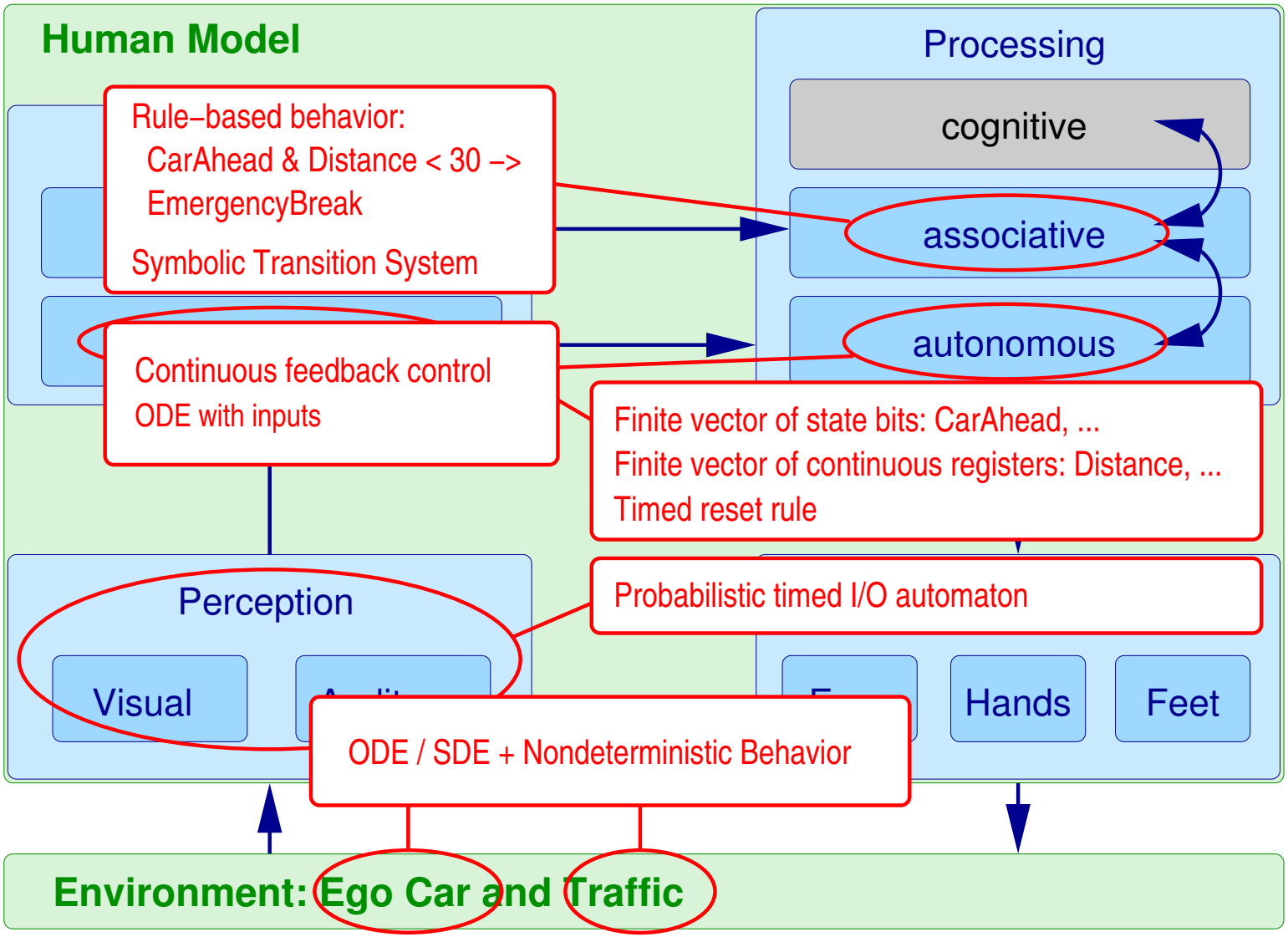
Ingredients of driver-in-the-loop model

[based on cognitive architecture CASCaS; Eilers, Lüdtke, Weber Wortelen 2008–]



Ingredients of driver-in-the-loop model

[based on cognitive architecture CASCaS; Eilers, Lüdtke, Weber Wortelen 2008–]



Analysing the ADAS in the Loop

The model

- essentially is a stochastic hybrid system,
- albeit with extremely large state space,
- residing in a heterogeneous ensemble of COTS simulators (driving simulator, cognitive architecture, Simulink-Stateflow model of ADAS, models of sensors, . . .),
- many of which are black boxes.

Analysing the ADAS in the Loop

The model

- essentially is a stochastic hybrid system,
- albeit with extremely large state space,
- residing in a heterogeneous ensemble of COTS simulators (driving simulator, cognitive architecture, Simulink-Stateflow model of ADAS, models of sensors, . . .),
- many of which are black boxes.

Only reasonable analysis technique consequently is co-simulation

- is i.g. linear in the number of state bits, etc.
- thus cheap and fast
- but covers just one model / trajectory per run
- thus remains inherently incomplete (unless even higher computational cost than in exhaustive search is accepted)
- ? can it answer the following questions *with any kind of confidence*?
  - in a qualitative setting: does system satisfy property?
  - in a stochastic setting: is the probability of satisfaction $> \theta$?

Step I

Setting up a Faithful Co-Simulation

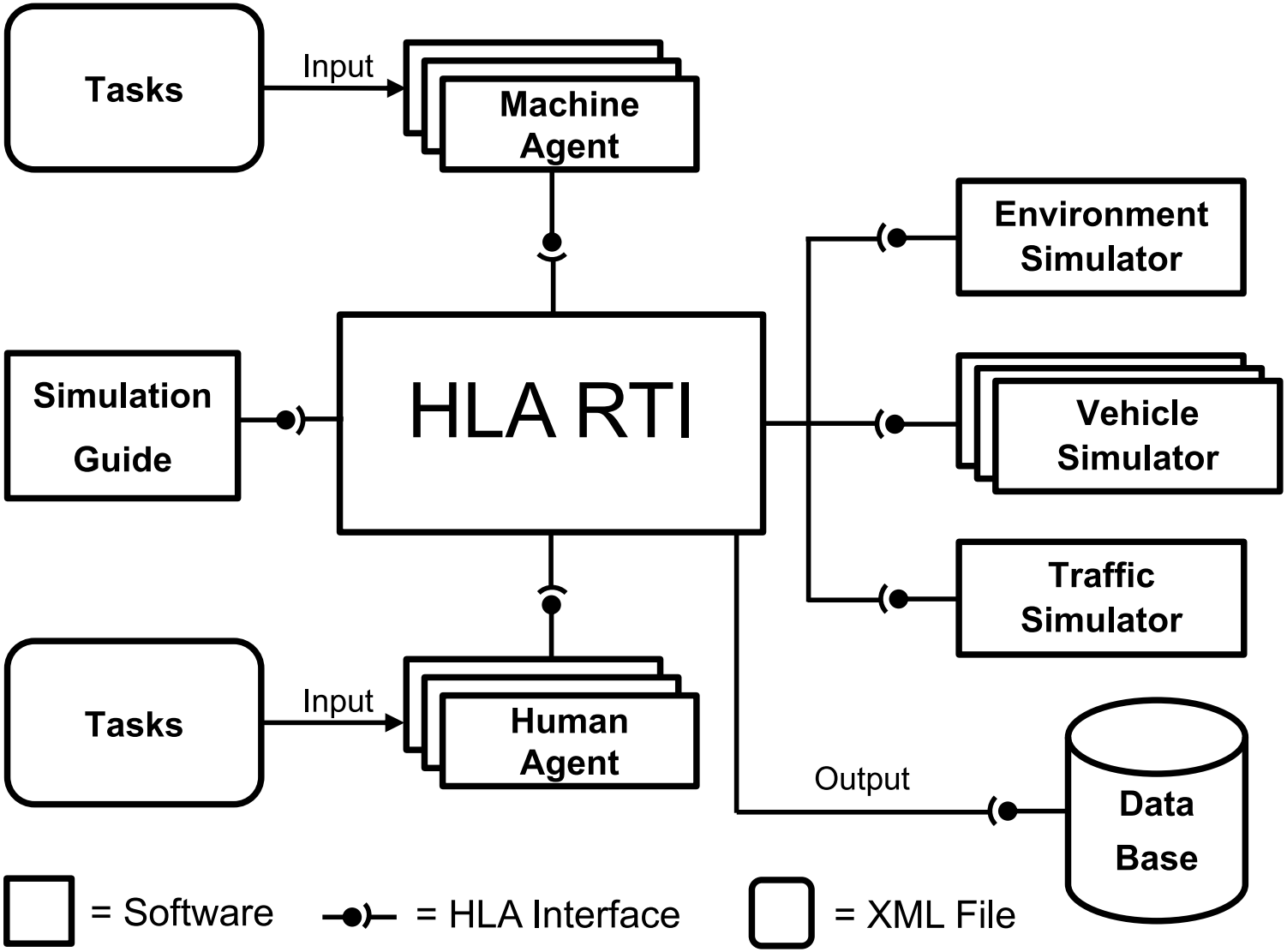
The Task

Problem: Set up a co-simulation that

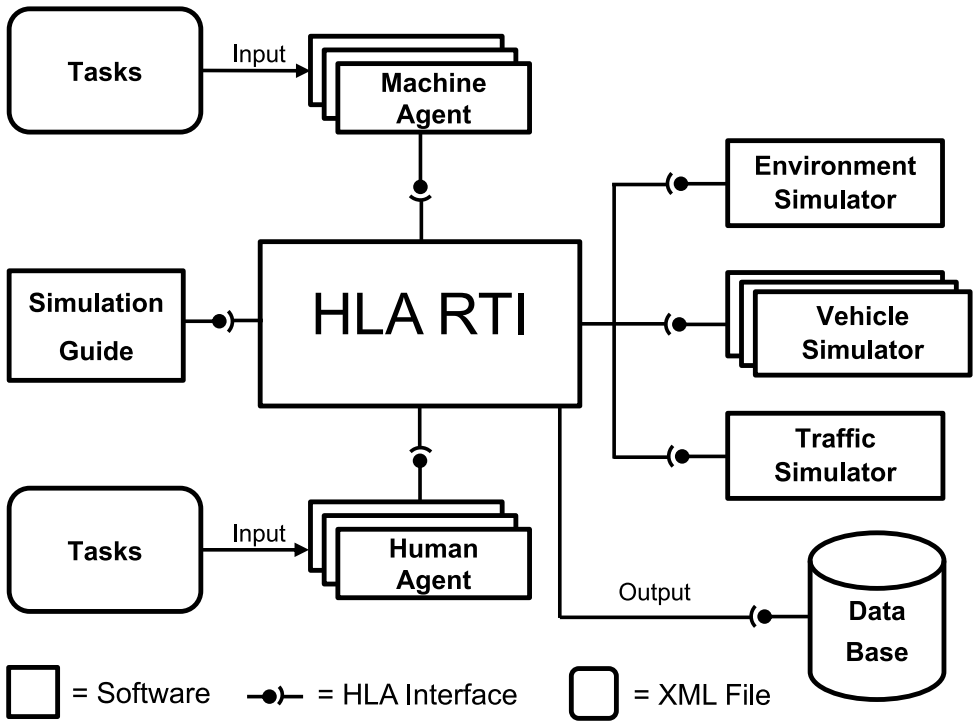
- unifies multiple models of (sub-)system dynamics:
  - Discrete (equidistant) time; continuous time; event-driven dynamics
  - Newtonian or Markovian state dynamics
- bridges simulation time models:
  - real-time (wall-clock) time vs. virtual (simulation) time
- permits component plug-and-play:
  - should support full virtual model (incl. cognitive components)
  - should also work in interactive driving simulation with real driver in the loop.

Solution: Use infrastructure ("bus") mediating transparently between heterogeneous simulators.

Co-simul. of heterogeneous models [Puch et al. 2009–]



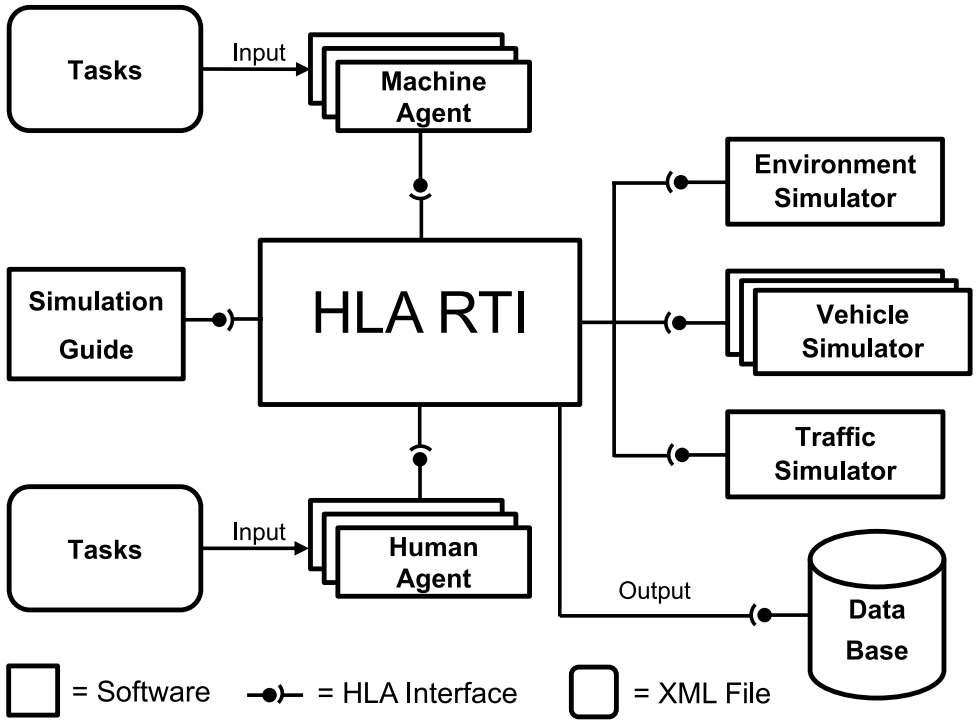
Co-simul. of heterogeneous models [Puch et al. 2009–]



Using HLA [IEEE Std. 1516], the co-simulation

- enforces temporal and state consistency between the individual components, despite heterogeneous time models,
- is input-to-state deterministic
  (when replacing stochastic sources by inputs)

Co-simul. of heterogeneous models [Puch et al. 2009–]



- Scope of temporal and state consistency extends to various analysis tools and experiment data bases.
- For all these, it is transparent whether they are coupled to
  1. an autonomous simulation incorporating a driver model,
  2. an interactive simulation in one of the various driving simulators.

Step II

Statistical Model-Checking — The Very Idea

Statistical Model Checking — the very Idea

In a purely stochastic setting, we can generalize from samples:

- Given a stochastic process P, a random variable $x \in [0,1]$ in P, we approximate the *expected value* E_x of x in P by
  1. taking n random samples (i.e., simulation runs), each yielding a value x_i, $i \in \{1,\ldots,n\}$, for x,
  2. then computing the estimate $\tilde{E}_x = \frac{1}{n}\sum_{i=1}^{n} x_i$.

Statistical Model Checking — the very Idea

In a purely stochastic setting, we can generalize from samples:

- Given a stochastic process P, a random variable $x \in [0,1]$ in P, we approximate the *expected value* E_x of x in P by
  1. taking n random samples (i.e., simulation runs), each yielding a value x_i, $i \in \{1,\ldots,n\}$, for x,
  2. then computing the estimate $\tilde{E}_x = \frac{1}{n}\sum_{i=1}^{n} x_i$.
- The law of large numbers tells that given sufficiently large n, the estimate $\tilde{E}_x$ is unlikely to be far off
  - as a considerable over- or underestimation of E_x would require samples with an accumulation of one-sided errors,
  - which are peculiar samples and thus unlikely.

Statistical Model Checking — the very Idea

In a purely stochastic setting, we can generalize from samples:

- Given a stochastic process P, a random variable $x \in [0,1]$ in P, we approximate the *expected value* E_x of x in P by
  1. taking n random samples (i.e., simulation runs), each yielding a value x_i, $i \in \{1,\ldots,n\}$, for x,
  2. then computing the estimate $\tilde{E}_x = \frac{1}{n}\sum_{i=1}^{n} x_i$.
- The law of large numbers tells that given sufficiently large n, the estimate $\tilde{E}_x$ is unlikely to be far off
  - as a considerable over- or underestimation of E_x would require samples with an accumulation of one-sided errors,
  - which are peculiar samples and thus unlikely.
- The exact figure is given by Hoeffding's inequality: For all $t > 0$,

$$\Pr(\tilde{E}_x - E_x \geq t) \leq e^{-2nt^2}, \qquad \Pr(\tilde{E}_x - E_x \leq -t) \leq e^{-2nt^2}$$

  - independent of P's structural properties, like probability distributions, size of state set, etc.,
  - provided sampling is random in the sense of stochastic independence between draws of individual samples.

Statistical Model Checking [Younes, Simmons 2002–]

Given a property $E_x \leq \theta$, with $\theta \in (0, 1)$,

- e.g. $x = \begin{cases} 1 & \text{iff (simulated) trajectory reaches a bad state,} \\ 0 & \text{else,} \end{cases}$
- such that $E_x \leq \theta$ means risk of misbehavior is at most θ,

let's try to "verify" $E_x \leq \theta$ by random sampling:

1. add a small don't care range t s.t. any answer is acceptable if $E_x \in [\theta - t, \theta + t]$
2. collect n random samples and compute $\varepsilon = \tilde{E}_x - \theta$,
3. test whether $\varepsilon \leq 0$.

Statistical Model Checking [Younes, Simmons 2002–]

Given a property $E_x \leq \theta$, with $\theta \in (0, 1)$,

- e.g. $x = \begin{cases} 1 & \text{iff (simulated) trajectory reaches a bad state,} \\ 0 & \text{else,} \end{cases}$
- such that $E_x \leq \theta$ means risk of misbehavior is at most θ,

let's try to "verify" $E_x \leq \theta$ by random sampling:

1. add a small don't care range t s.t. any answer is acceptable if $E_x \in [\theta - t, \theta + t]$
2. collect n random samples and compute $\varepsilon = \tilde{E}_x - \theta$,
3. test whether $\varepsilon \leq 0$.

Hoeffding's inequality tells us how to interpret the outcome:

- If $\varepsilon \leq 0$ then we can say that the property is satisfied,
- If $\varepsilon > 0$ then we can say that the property is violated

Statistical Model Checking [Younes, Simmons 2002–]

Given a property $E_x \leq \theta$, with $\theta \in (0,1)$,

- e.g. $x = \begin{cases} 1 & \text{iff (simulated) trajectory reaches a bad state,} \\ 0 & \text{else,} \end{cases}$
- such that $E_x \leq \theta$ means risk of misbehavior is at most θ,

let's try to "verify" $E_x \leq \theta$ by random sampling:

1. add a small don't care range t s.t. any answer is acceptable if $E_x \in [\theta - t, \theta + t]$
2. collect n random samples and compute $\varepsilon = \tilde{E}_x - \theta$,
3. test whether $\varepsilon \leq 0$.

Hoeffding's inequality tells us how to interpret the outcome:

- If $\varepsilon \leq 0$ then we can say that the property is satisfied, but only with *confidence* $1 - e^{-2nt^2}$.
- If $\varepsilon > 0$ then we can say that the property is violated but only with *confidence* $1 - e^{-2nt^2}$.

Statistical Model Checking [Younes, Simmons 2002–]

Given a property $E_x \leq \theta$, with $\theta \in (0,1)$,

- e.g. $x = \begin{cases} 1 & \text{iff (simulated) trajectory reaches a bad state,} \\ 0 & \text{else,} \end{cases}$
- such that $E_x \leq \theta$ means risk of misbehavior is at most θ,

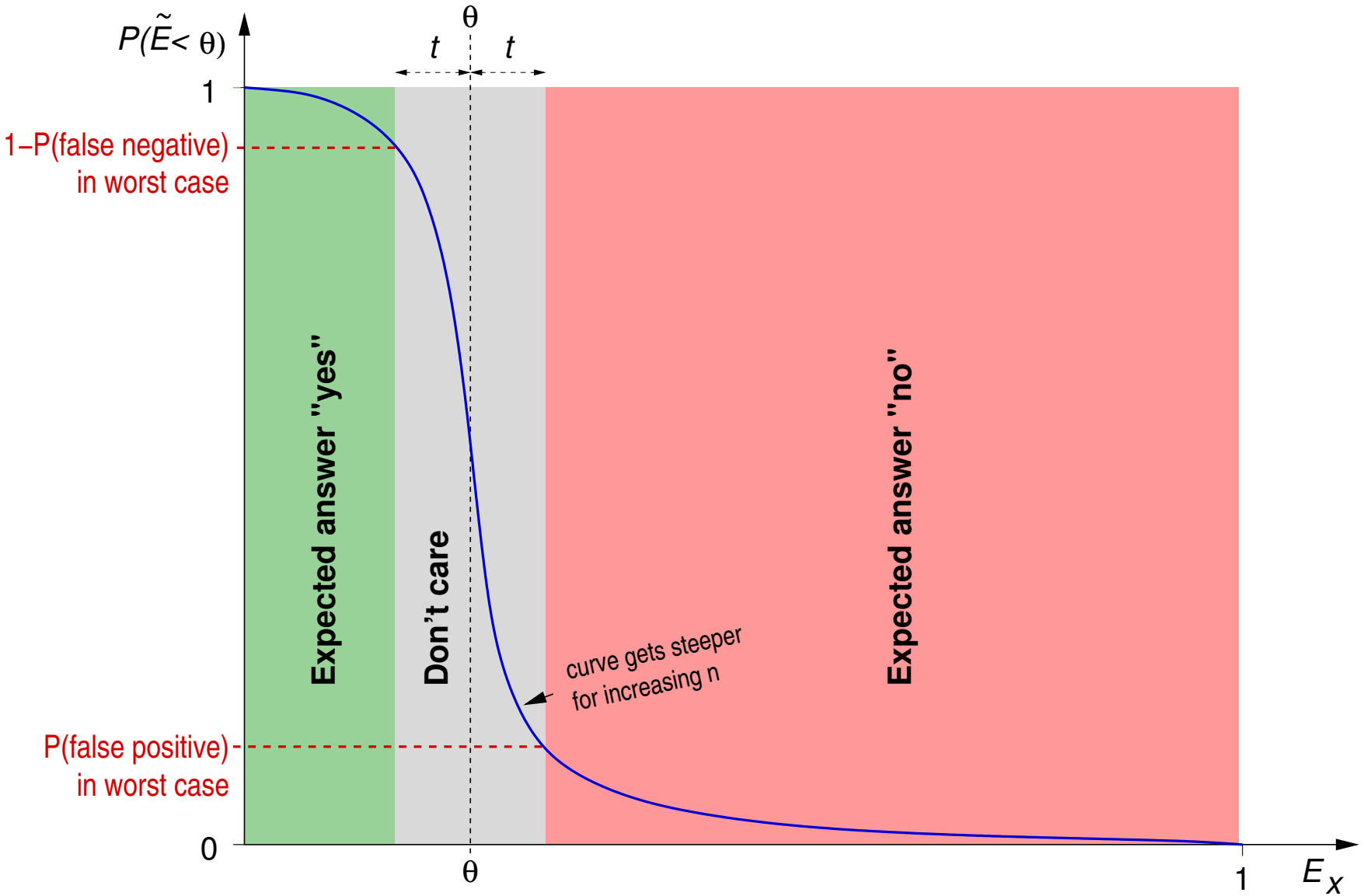
let's try to "verify" $E_x \leq \theta$ by random sampling:

1. add a small don't care range t s.t. any answer is acceptable if $E_x \in [\theta - t, \theta + t]$
2. collect n random samples and compute $\varepsilon = \tilde{E}_x - \theta$,
3. test whether $\varepsilon \leq 0$.

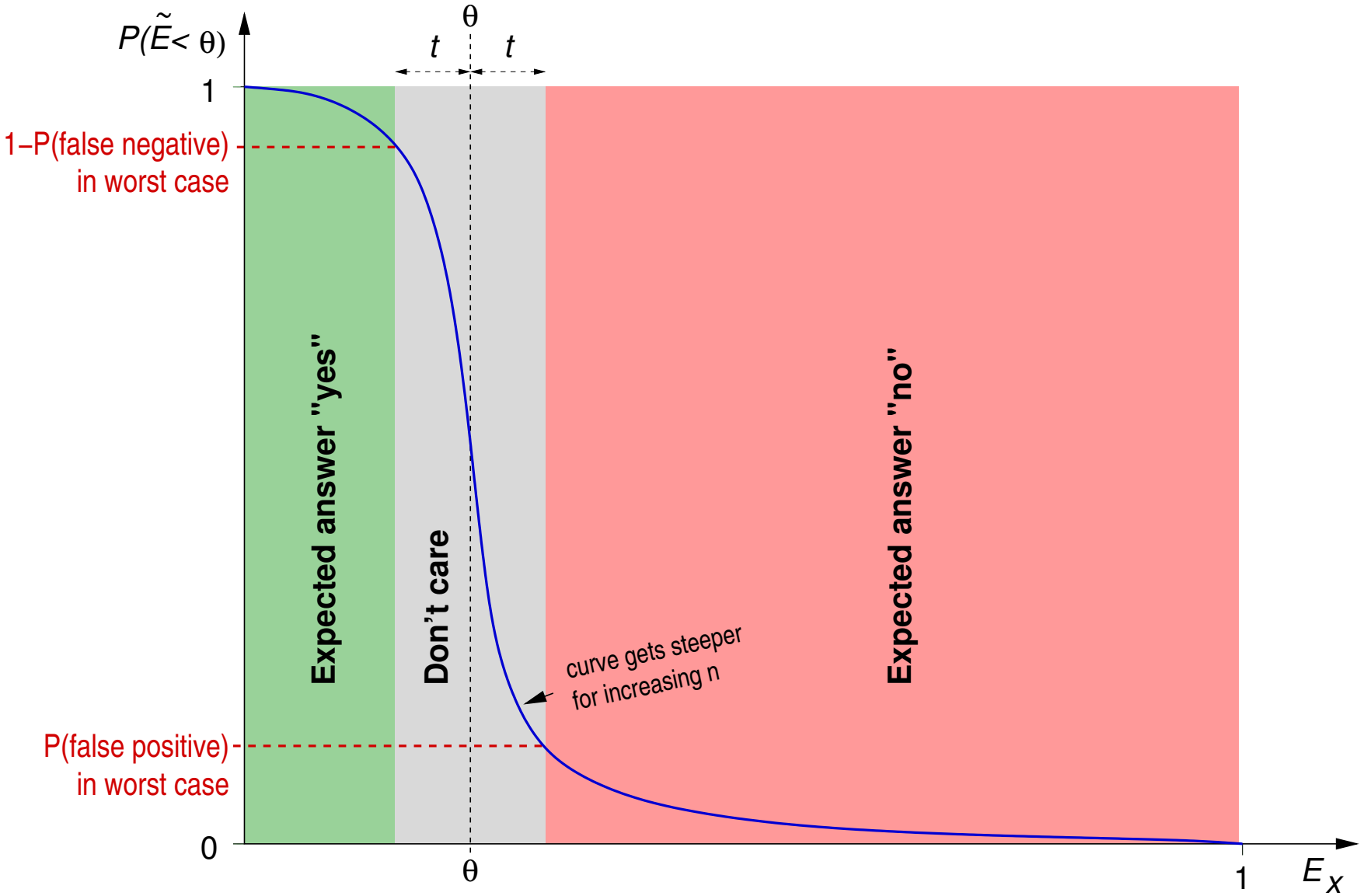
Hoeffding's inequality tells us how to interpret the outcome:

- If $\varepsilon \leq 0$ then we can say that the property is satisfied, but only with *confidence* $1 - e^{-2nt^2}$.
- If $\varepsilon > 0$ then we can say that the property is violated but only with *confidence* $1 - e^{-2nt^2}$.
- which means that we are misled by *false positives / false negatives with probability* e^{-2nt^2}.

Interpretation of result

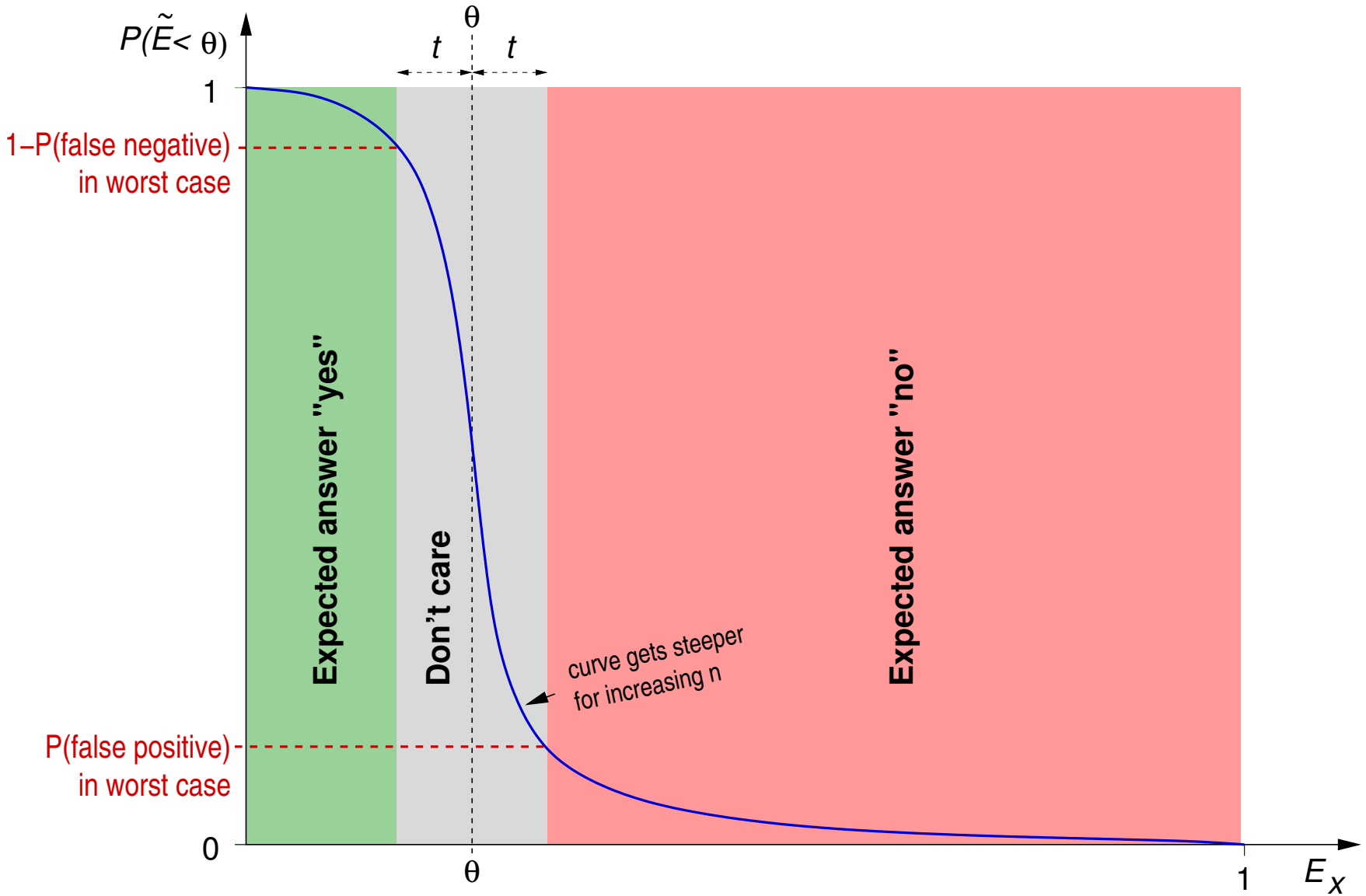


Interpretation of result



Obs.: $\mathrm{P}(\text{false certificate}) \to 0$ if $n \to \infty$ or $t \to \max(\theta, 1-\theta)$.

Interpretation of result



But what if safety targets are high and interesting events are rare?

Hardness: What safety targets are we after?

- Statistically[1], we have one injury per $1.46 \cdot 10^6$km road traffic. If every tenth collision is assumed to lead to some injury, this means one collision every $1.5 \cdot 10^5$km on average.

[1] Ingeborg Vorndran: Unfallstatistik — Verkehrsmittel im Risikovergleich. Statistisches Bundesamt, 12/2010

Hardness: What safety targets are we after?

- Statistically[1], we have one injury per $1.46 \cdot 10^6$km road traffic. If every tenth collision is assumed to lead to some injury, this means one collision every $1.5 \cdot 10^5$km on average.
- I.e., likelihood of collision during filtering in should be of order $5 \cdot 10^{-6}$ to 10^{-5} per maneuver — the latter if we accept filtering in being of above average risk.

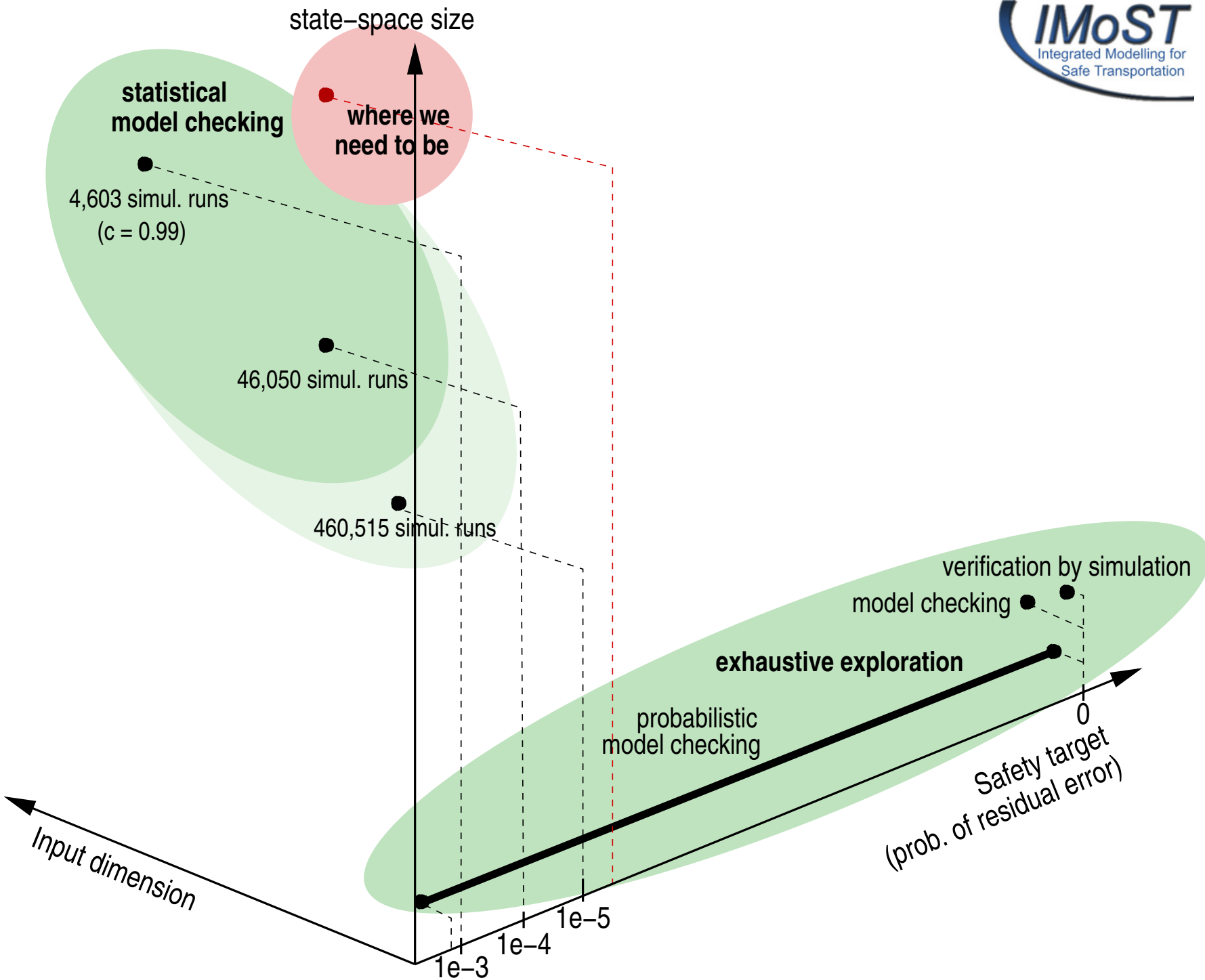
[1] Ingeborg Vorndran: Unfallstatistik — Verkehrsmittel im Risikovergleich. Statistisches Bundesamt, 12/2010

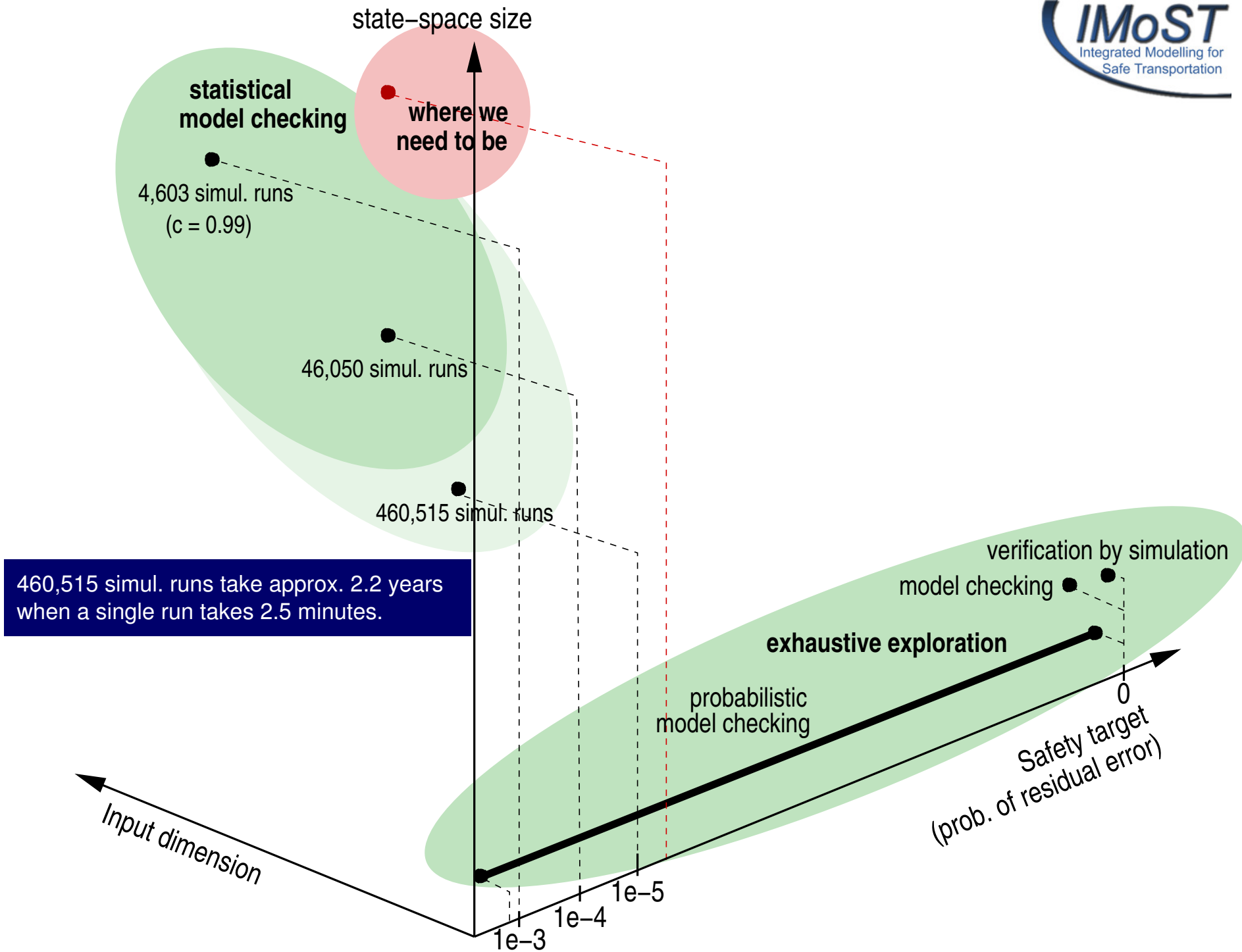
Hardness: What safety targets are we after?

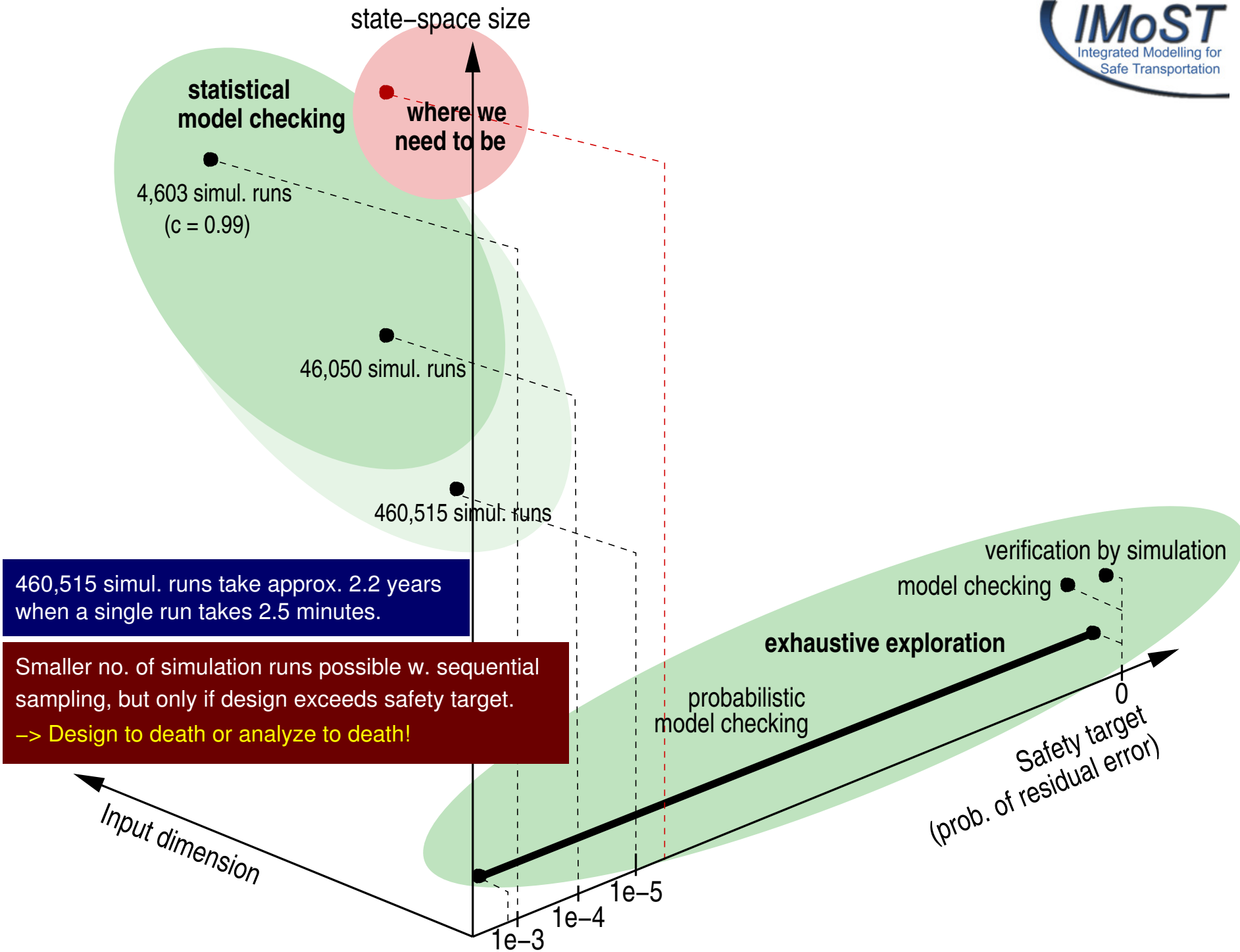
- Statistically[1], we have one injury per $1.46 \cdot 10^6$km road traffic. If every tenth collision is assumed to lead to some injury, this means one collision every $1.5 \cdot 10^5$km on average.
- I.e., likelihood of collision during filtering in should be of order $5 \cdot 10^{-6}$ to 10^{-5} per maneuver — the latter if we accept filtering in being of above average risk.

Can we assess such reliability figures by simulation / SMC?

[1] Ingeborg Vorndran: Unfallstatistik — Verkehrsmittel im Risikovergleich. Statistisches Bundesamt, 12/2010


state–space size
statistical
model checking
where we
need to be
4,603 simul. runs
(c = 0.99)
46,050 simul. runs
460,515 simul. runs
verification by simulation
model checking
exhaustive exploration
probabilistic
model checking
0
Safety target
(prob. of residual error)
Input dimension
1e–3
1e–4
1e–5


state–space size
statistical
model checking
where we
need to be
4,603 simul. runs
(c = 0.99)
46,050 simul. runs
460,515 simul. runs
460,515 simul. runs take approx. 2.2 years
when a single run takes 2.5 minutes.
verification by simulation
model checking
exhaustive exploration
probabilistic
model checking
0
Safety target
(prob. of residual error)
Input dimension
1e–3
1e–4
1e–5


state–space size
statistical
model checking
where we
need to be
4,603 simul. runs
(c = 0.99)
46,050 simul. runs
460,515 simul. runs
460,515 simul. runs take approx. 2.2 years
when a single run takes 2.5 minutes.
Smaller no. of simulation runs possible w. sequential
sampling, but only if design exceeds safety target.
–> Design to death or analyze to death!
verification by simulation
model checking
exhaustive exploration
probabilistic
model checking
0
Safety target
(prob. of residual error)
Input dimension
1e–3
1e–4
1e–5

Step III

Enhancing Statistical Model Checking by Guided Simulation

Cures suggested in the literature

To reduce the number of samples necessary for achieving a given confidence

- Zuliani , Platzer , and Clarke suggests Bayesian Statistical Model Checking [Zuliani , Platzer , Clarke 2010]
- but this is prone to fallacies of Bayesian inference in case of (even moderately) rare events [Younjoo Kim, Moonzoo Kim, Taihyo Kim 2012]

Cures suggested in the literature

To reduce the number of samples necessary for achieving a given confidence

- Zuliani , Platzer , and Clarke suggests Bayesian Statistical Model Checking [Zuliani , Platzer , Clarke 2010]
- but this is prone to fallacies of Bayesian inference in case of (even moderately) rare events [Younjoo Kim, Moonzoo Kim, Taihyo Kim 2012]

To deal with rare events,

- Zuliani, Baier, and Clarke suggest an adaptation of importance sampling to give rare events a boost:

$$\tilde{E}_x = \frac{1}{n} \sum_{i=1}^{n} \frac{p(x_i)}{\hat{p}(x_i)} V(x_i)$$

  where $\hat{p}$ is a modified distribution used for sampling the x_i which emphasizes the rare events [Zuiliani, Baier, Clarke 2012].
- Has been successfully applied to technical models, where the rare events are primary faults (like sensor faults in Simulink's fault-tolerant fuel cell demo) s.t. the necessary modification $p \rightsquigarrow \hat{p}$ is obvious.

Cures suggested in the literature

To reduce the number of samples necessary for achieving a given confidence

- Zuliani , Platzer , and Clarke suggests Bayesian Statistical Model Checking [Zuliani , Platzer , Clarke 2010]
- but this is prone to fallacies of Bayesian inference in case of (even moderately) rare events [Younjoo Kim, Moonzoo Kim, Taihyo Kim 2012]

To deal with rare events,

- Zuliani, Baier, and Clarke suggest an adaptation of importance sampling to give rare events a boost:

$$\tilde{E}_x = \frac{1}{n} \sum_{i=1}^{n} \frac{p(x_i)}{\hat{p}(x_i)} V(x_i)$$

  where $\hat{p}$ is a modified distribution used for sampling the x_i which emphasizes the rare events [Zuiliani, Baier, Clarke 2012].
- Has been successfully applied to technical models, where the rare events are primary faults (like sensor faults in Simulink's fault-tolerant fuel cell demo) s.t. the necessary modification $p \rightsquigarrow \hat{p}$ is obvious.
- Unclear how to apply this to probabilistic decisions in cognitive models.

The need for identifying the important events

In human-in-the-loop models, an obvious monotonicity between the primary stochastic events (e.g., look now or later) and the rare events to be observed (e.g., accidents) is missing:

- Is it more risky to look 20ms earlier rather than later? Or vice versa?
- Is it more risky to watch the side mirror first and then the inner one? Or vice versa?

The need for identifying the important events

In human-in-the-loop models, an obvious monotonicity between the primary stochastic events (e.g., look now or later) and the rare events to be observed (e.g., accidents) is missing:

- Is it more risky to look 20ms earlier rather than later? Or vice versa?
- Is it more risky to watch the side mirror first and then the inner one? Or vice versa?

Before (or while) employing importance sampling,
we first have to learn what events are important and when/how.

Criticality-guided simulation

Idea: Make simulation a daredevil, greedy for risk.

- Good heuristic measures for distance to hazardous situation are often easy to obtain: e.g., estimated time to collision.
- Use these "criticality functions" to attract simulation towards risk:
  - Bias random sources to prefer values with high criticality,
  - thus becoming greedy for risk,
  - while retaining a randomized process eventually covering the signal space.

Criticality-guided simulation

Idea: Make simulation a daredevil, greedy for risk.

- Good heuristic measures for distance to hazardous situation are often easy to obtain: e.g., estimated time to collision.
- Use these "criticality functions" to attract simulation towards risk:
  - Bias random sources to prefer values with high criticality,
  - thus becoming greedy for risk,
  - while retaining a randomized process eventually covering the signal space.

Problem:

- Criticality is naturally measured in terms of the system response rather than the input stimuli s.t. a direct assessment of the available choices usually is impossible.

Criticality-guided simulation

Idea: Make simulation a daredevil, greedy for risk.

- Good heuristic measures for distance to hazardous situation are often easy to obtain: e.g., estimated time to collision.
- Use these "criticality functions" to attract simulation towards risk:
  - Bias random sources to prefer values with high criticality,
  - thus becoming greedy for risk,
  - while retaining a randomized process eventually covering the signal space.

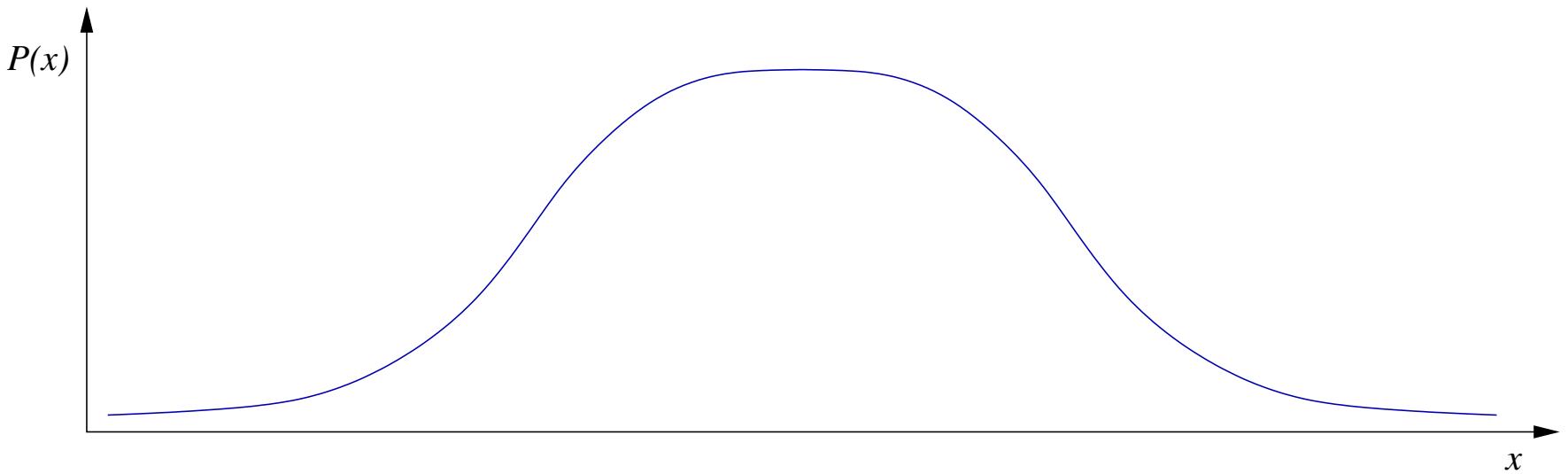
Problem:

- Criticality is naturally measured in terms of the system response rather than the input stimuli s.t. a direct assessment of the available choices usually is impossible.

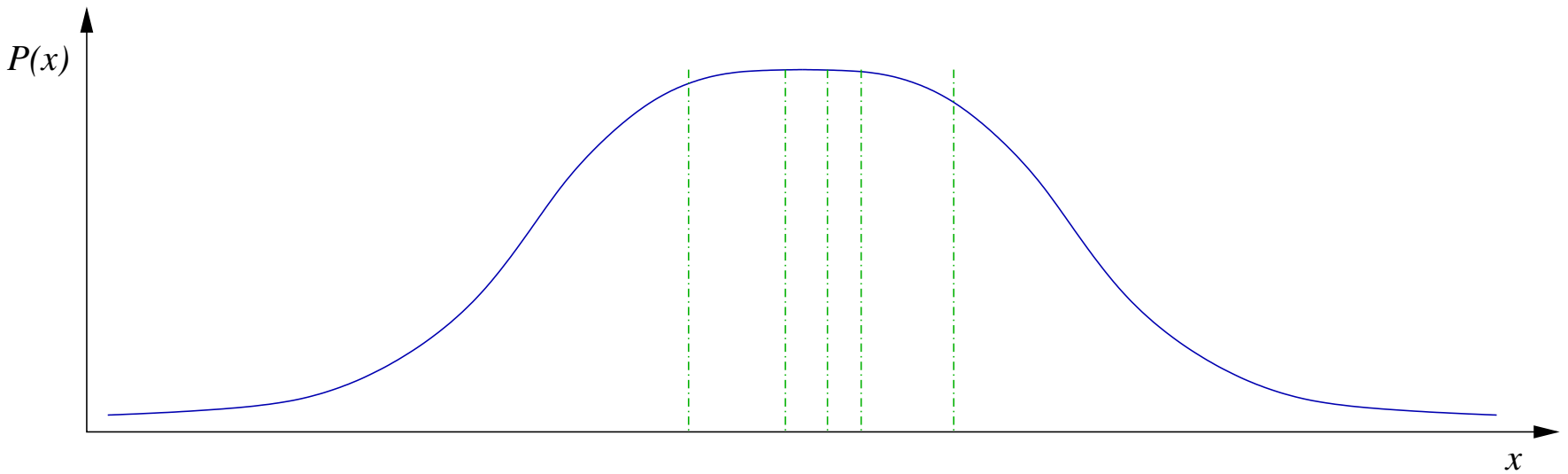
Idea:

- Adaptively fit a criticality function to input stimuli based on observed criticality of system response.
- Use interpolation to assess stimulus values not encountered before.

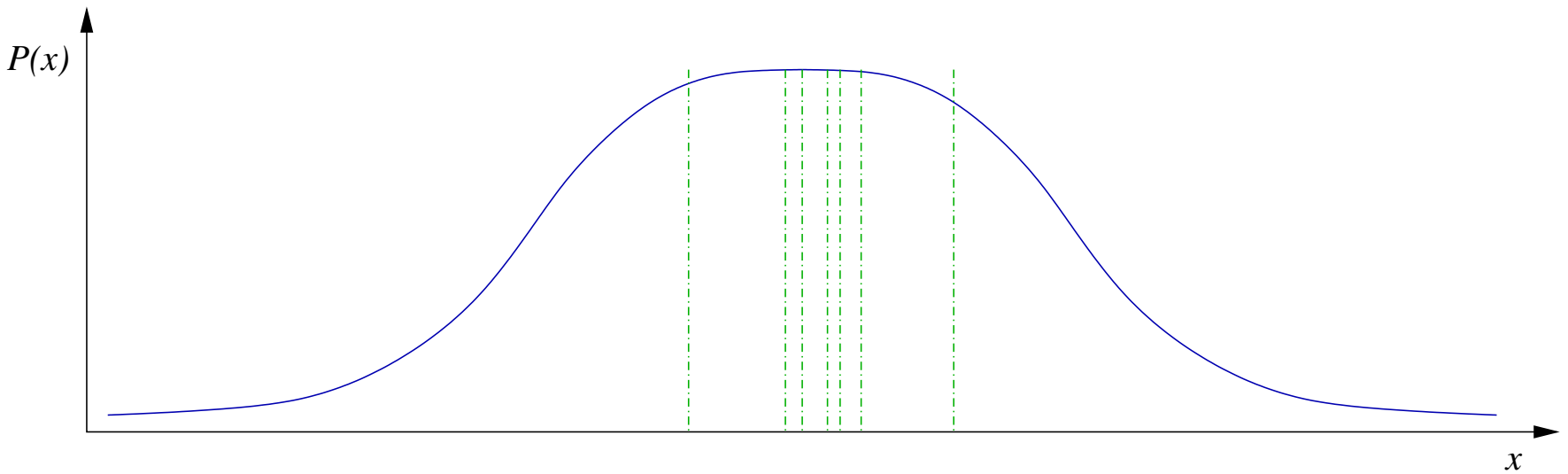
Schematic view: standard randomized simulation



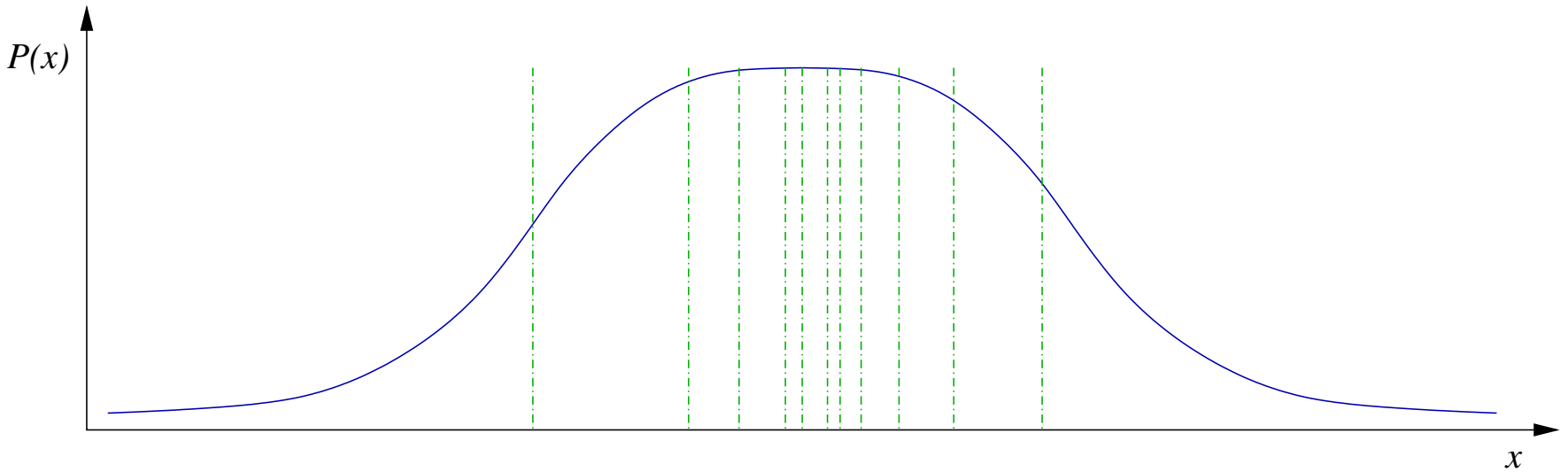
Schematic view: standard randomized simulation



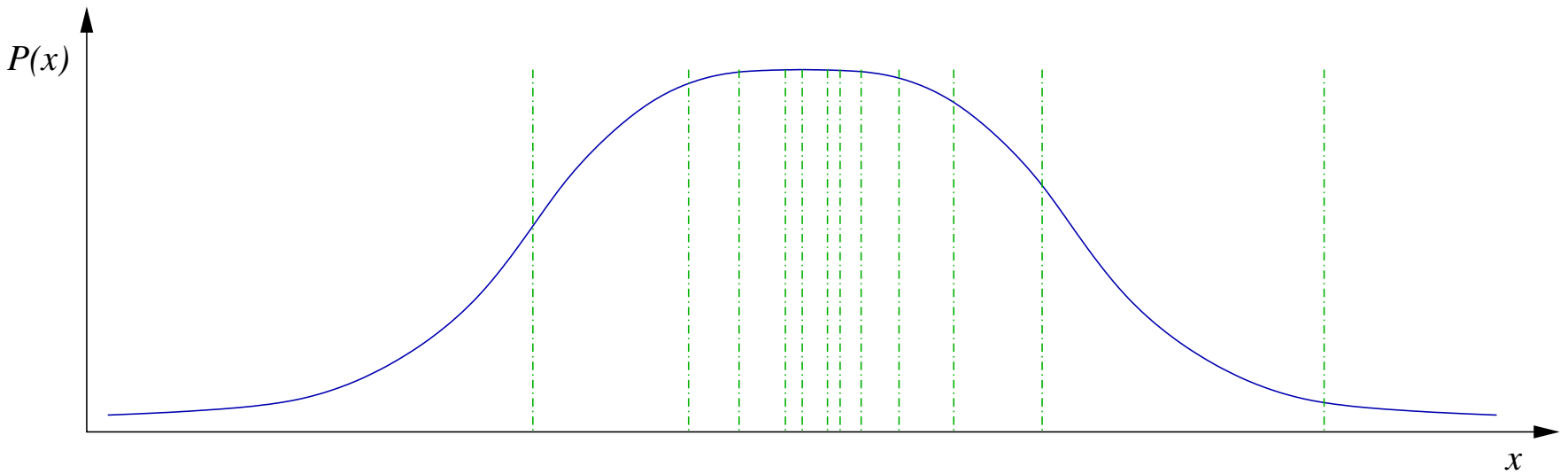
Schematic view: standard randomized simulation



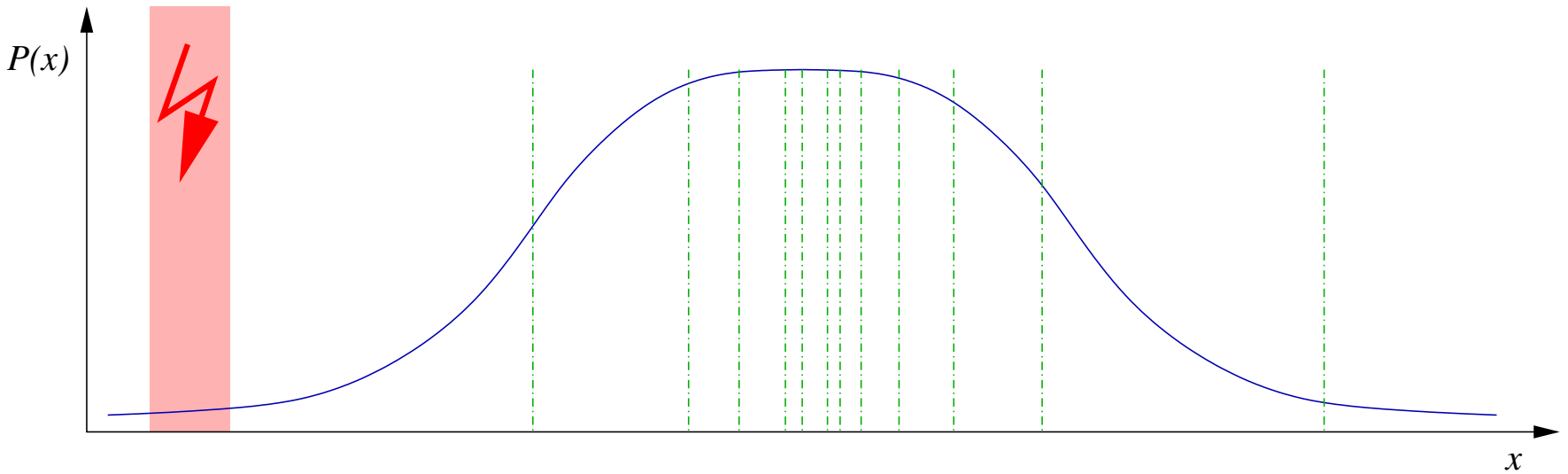
Schematic view: standard randomized simulation



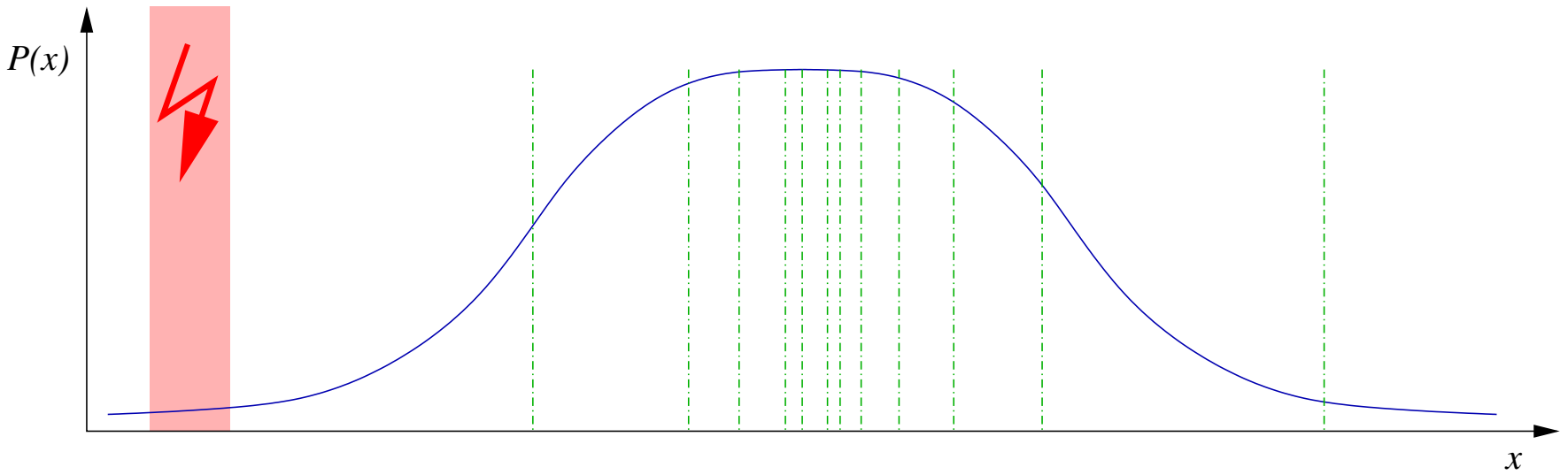
Schematic view: standard randomized simulation



Schematic view: standard randomized simulation

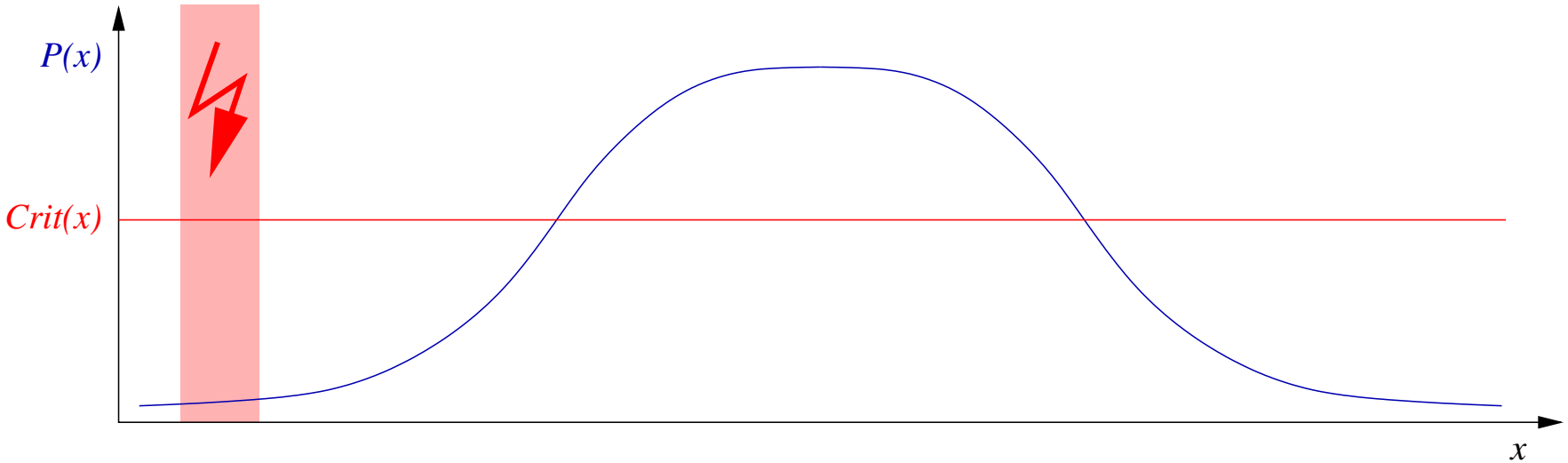


Schematic view: standard randomized simulation

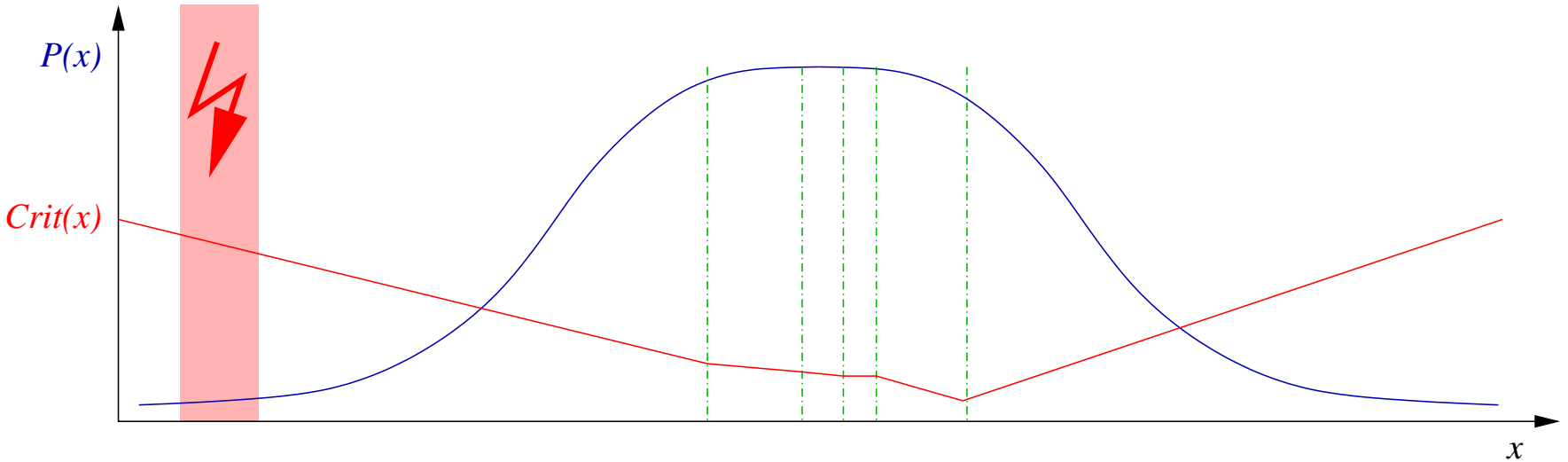


Very unlikely to find hazardous situations, especially in higher-dimensional search spaces.

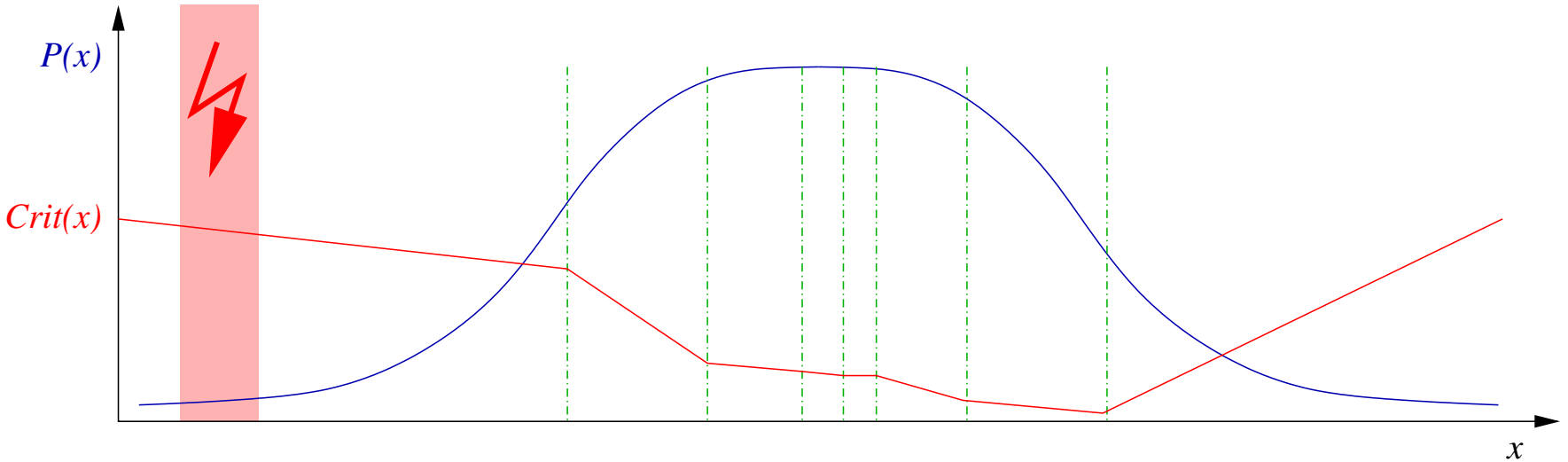
Schematic view: criticality-guided simulation



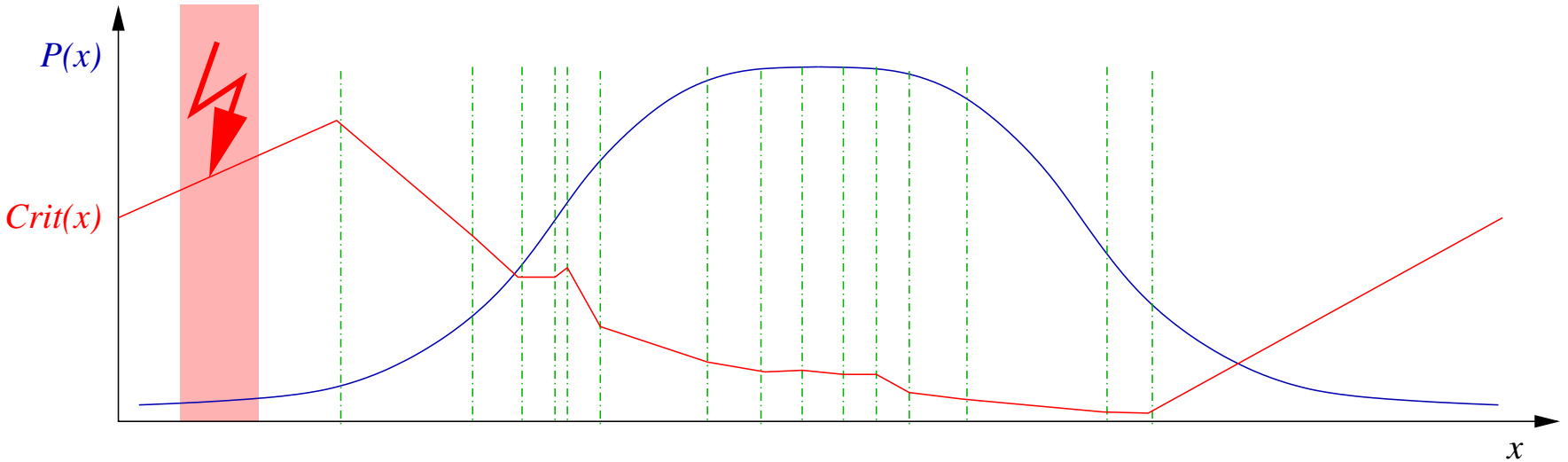
Schematic view: criticality-guided simulation



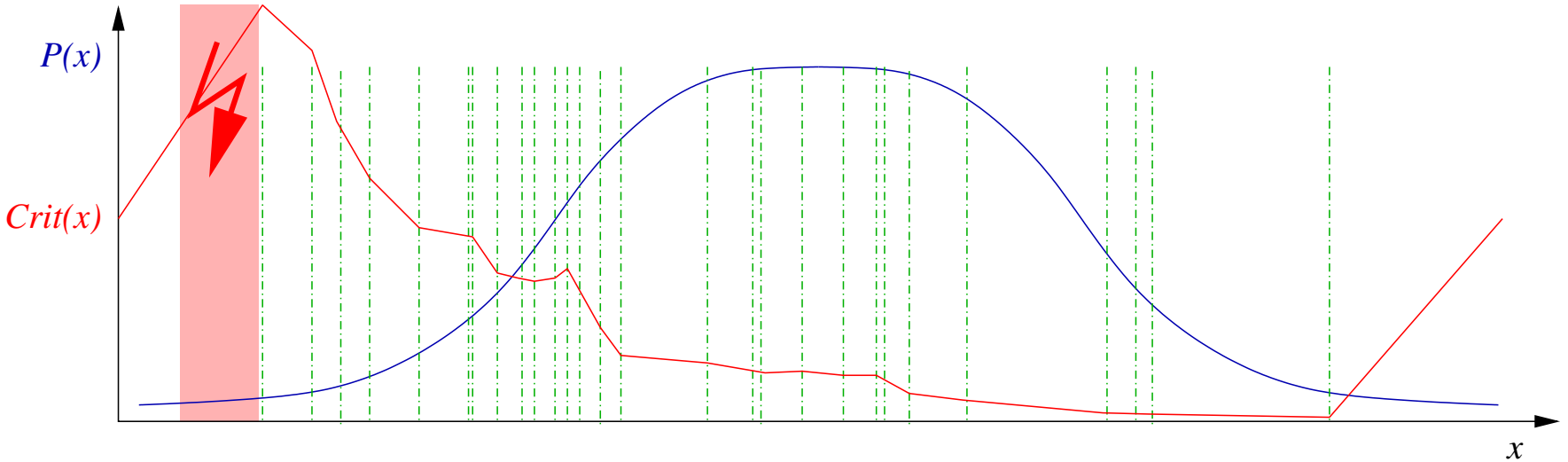
Schematic view: criticality-guided simulation



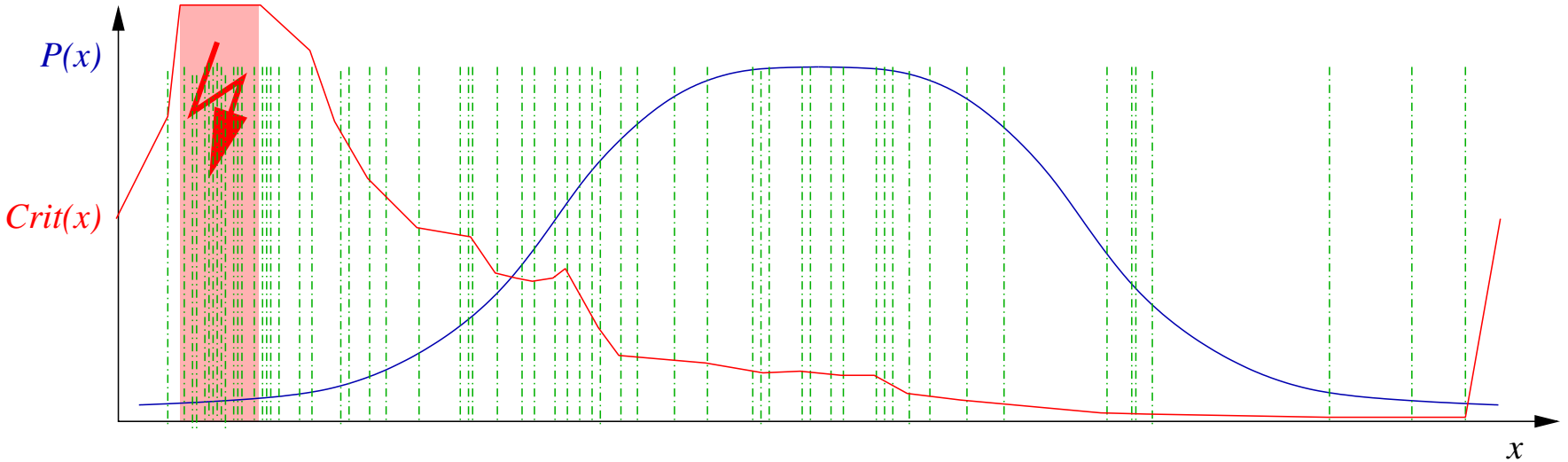
Schematic view: criticality-guided simulation



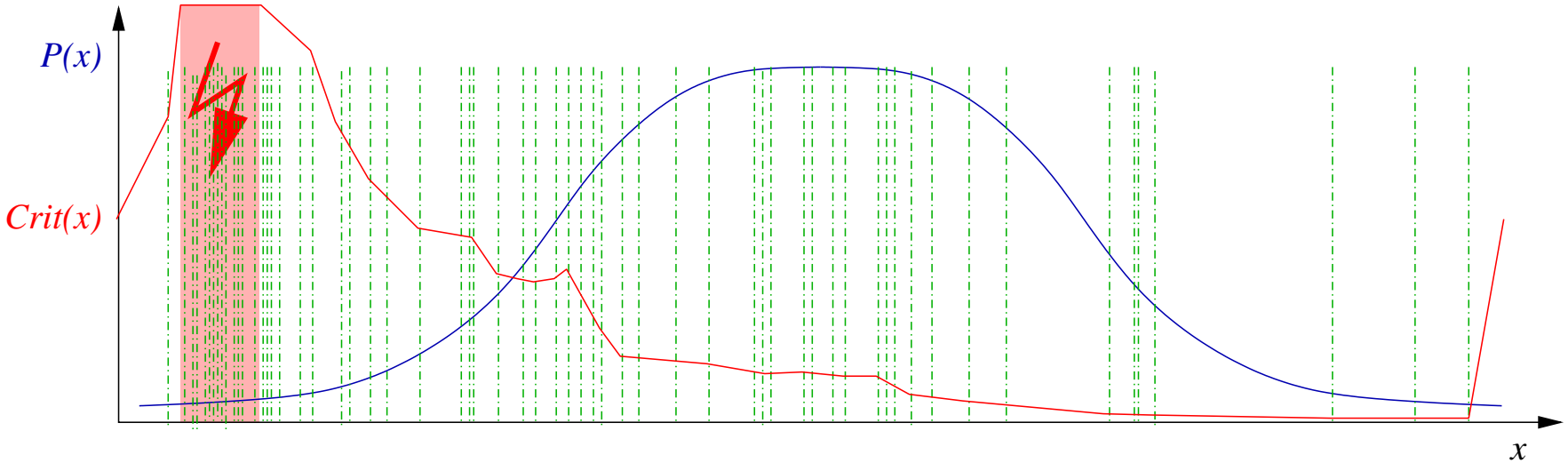
Schematic view: criticality-guided simulation



Schematic view: criticality-guided simulation

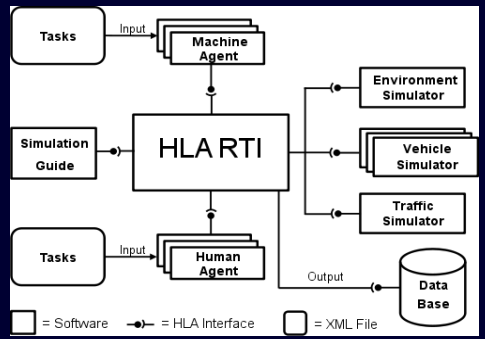


Schematic view: criticality-guided simulation

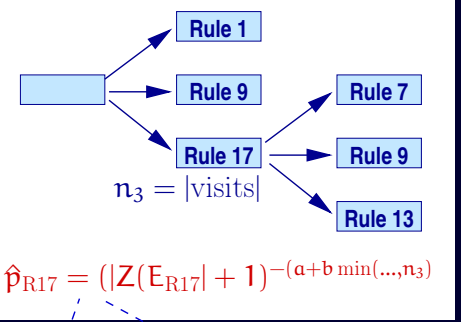


Active guiding towards hazardous situations, provided criticality function yields reasonable heuristic measure.

Simulate

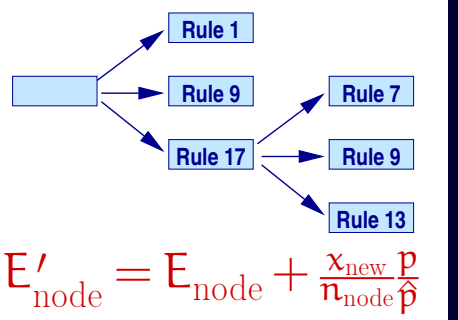


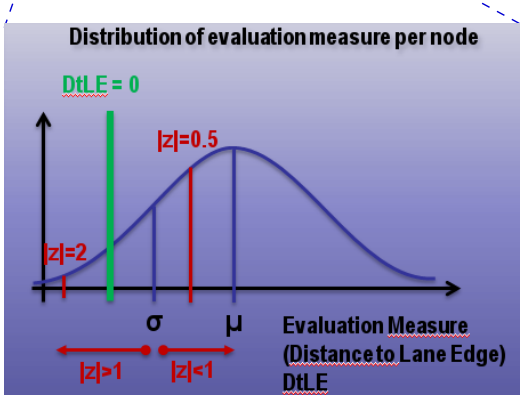
Update branch probabilities



Expand decision tree OTF

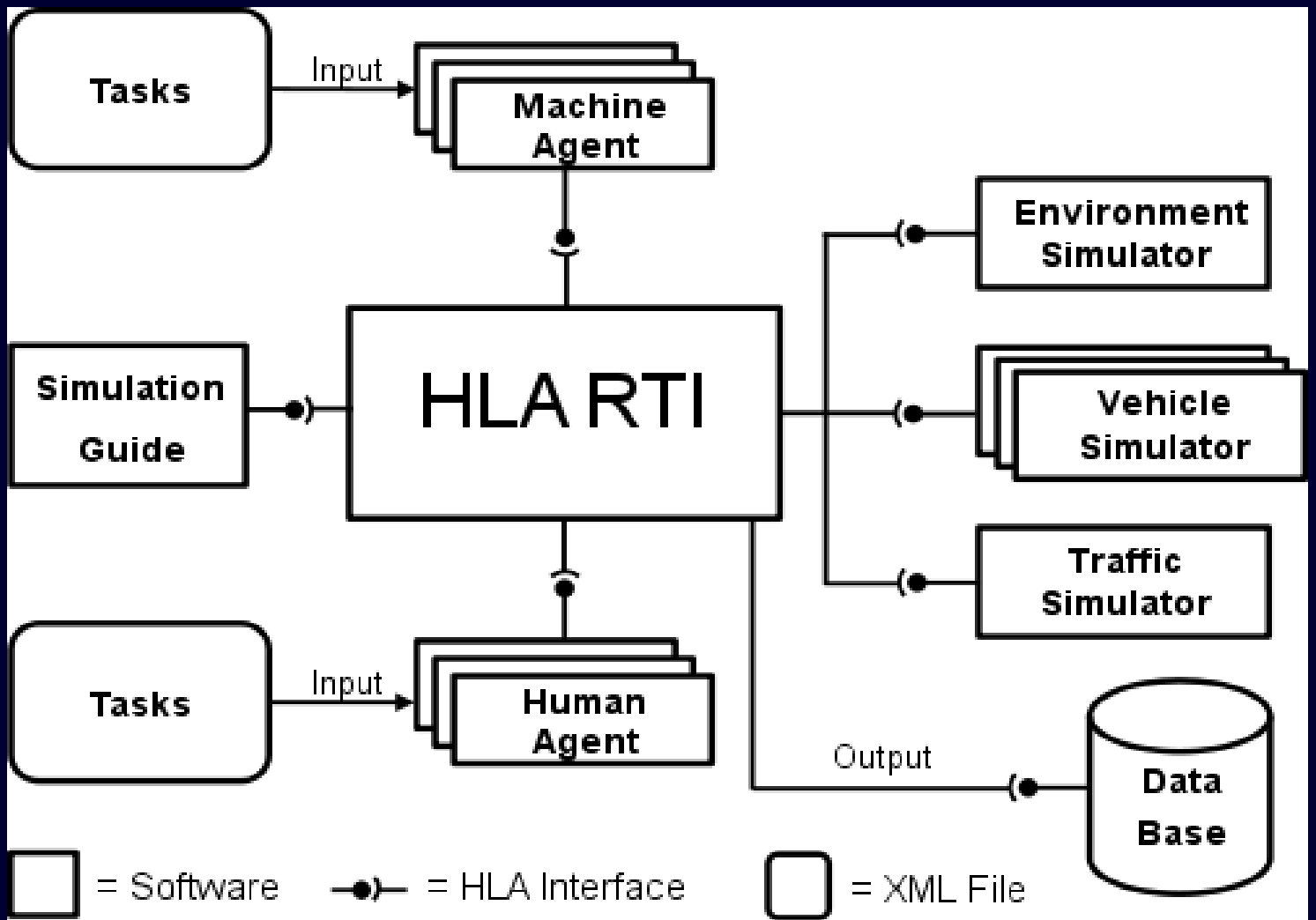
Update expectations



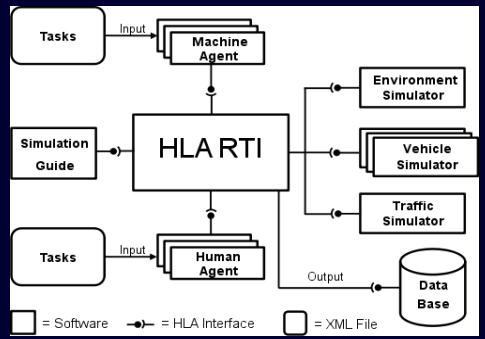


[Puch, Wortelen et al., 2012]

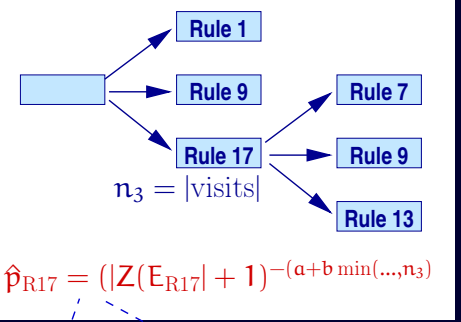
Simulate


Tasks
Input
Machine Agent
Environment Simulator
Simulation Guide
HLA RTI
Vehicle Simulator
Traffic Simulator
Tasks
Input
Human Agent
Output
Data Base
= Software
= HLA Interface
= XML File

Simulate

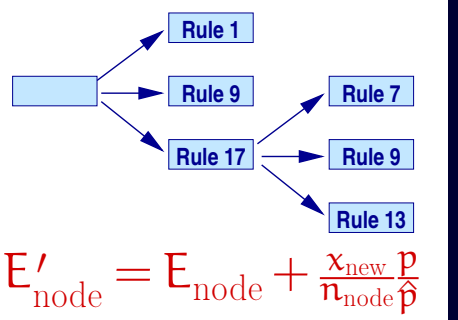


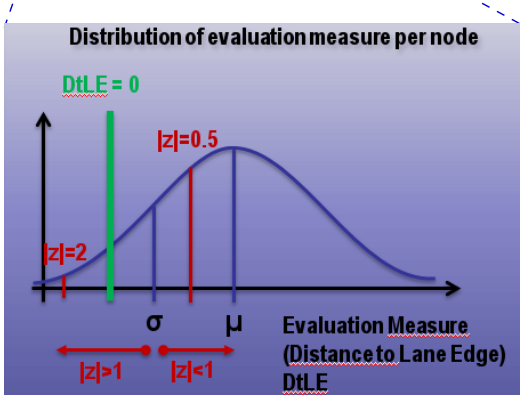
Update branch probabilities



Expand decision tree OTF

Update expectations

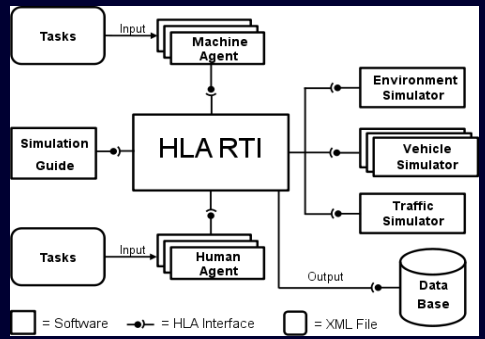




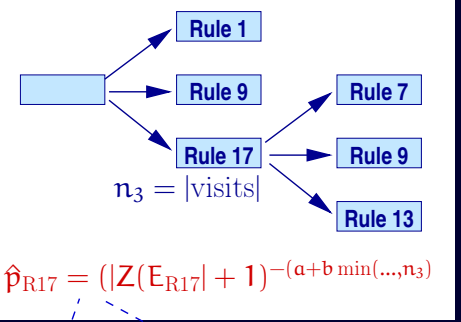
[Puch, Wortelen et al., 2012]

Expand decision tree OTF

Simulate

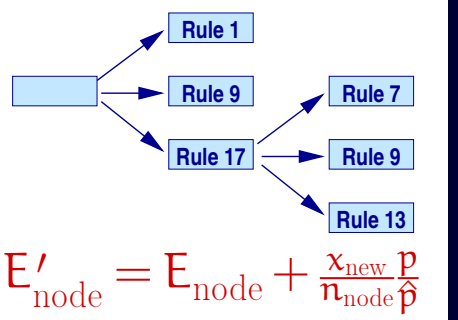


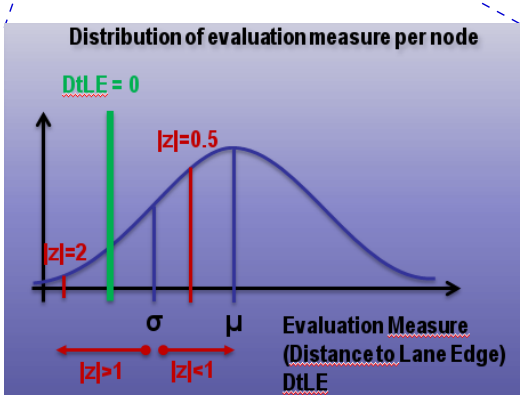
Update branch probabilities



Expand decision tree OTF

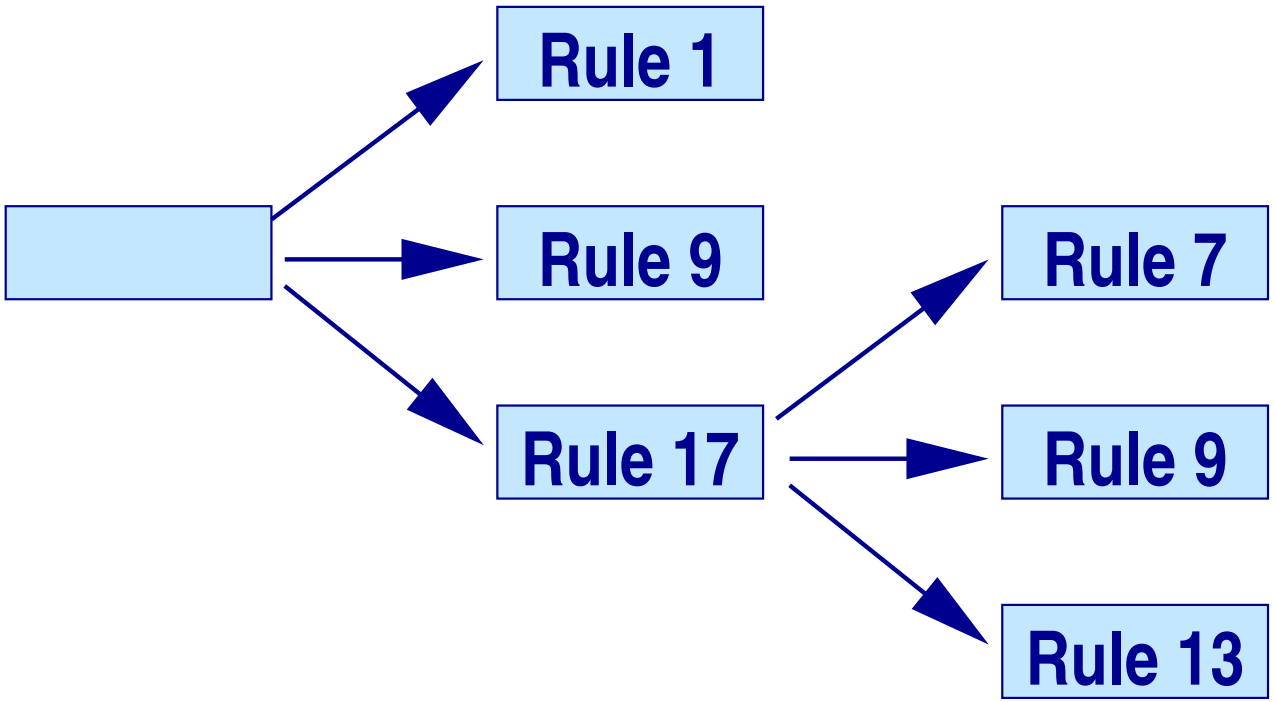
Update expectations





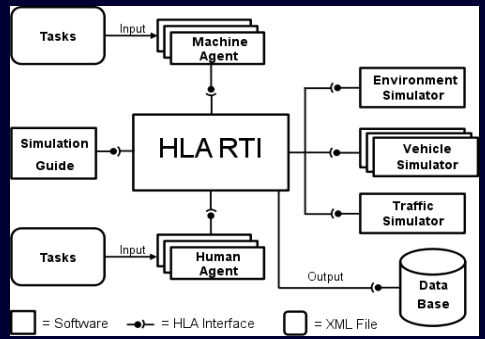
[Puch, Wortelen et al., 2012]

Update expectations

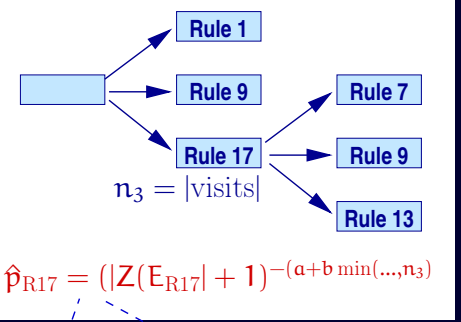


$$E'_{node} = E_{node} + \frac{x_{new}}{n_{node}} \frac{p}{\hat{p}}$$

Simulate

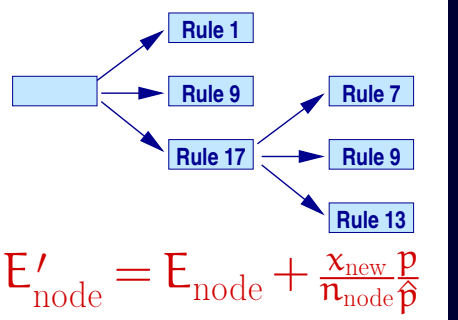


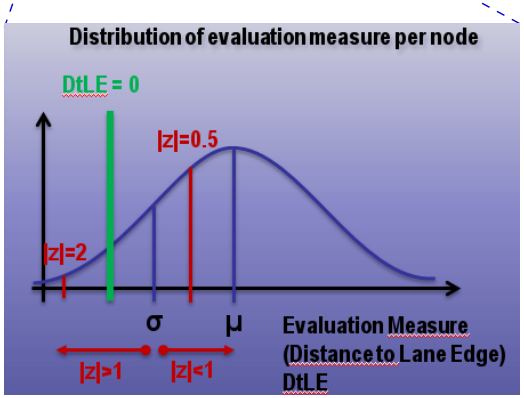
Update branch probabilities



Expand decision tree OTF

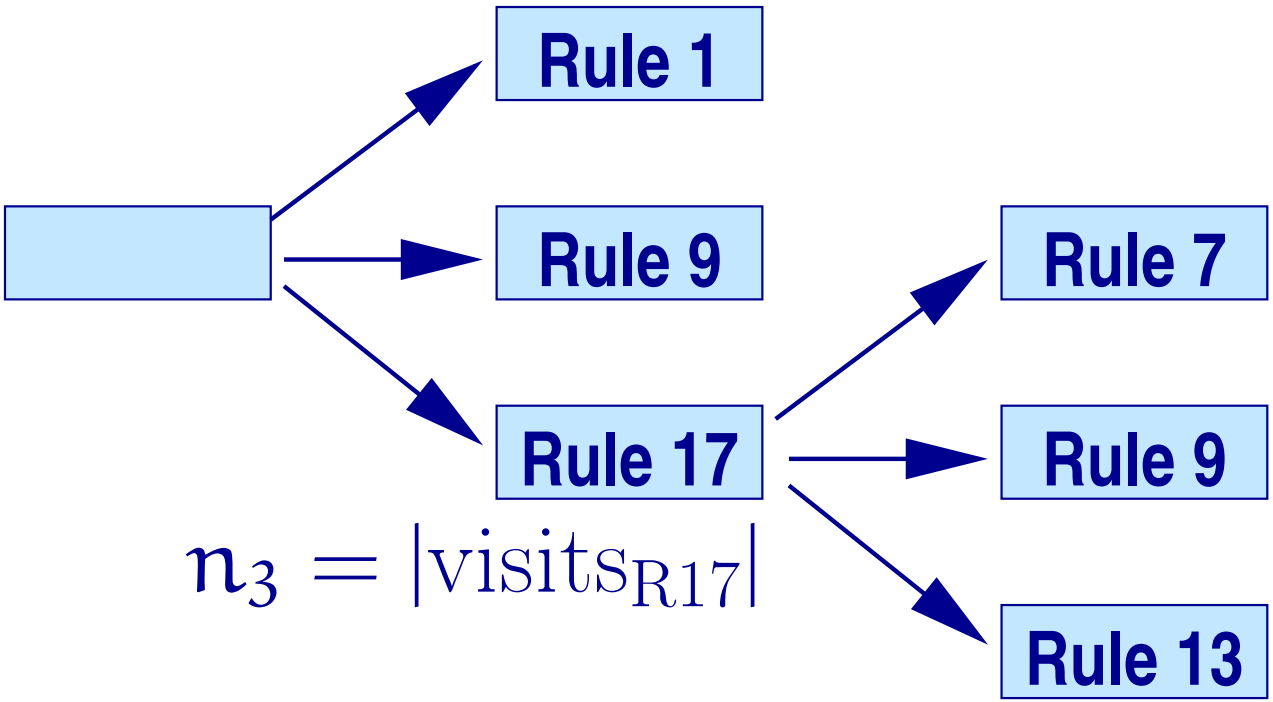
Update expectations





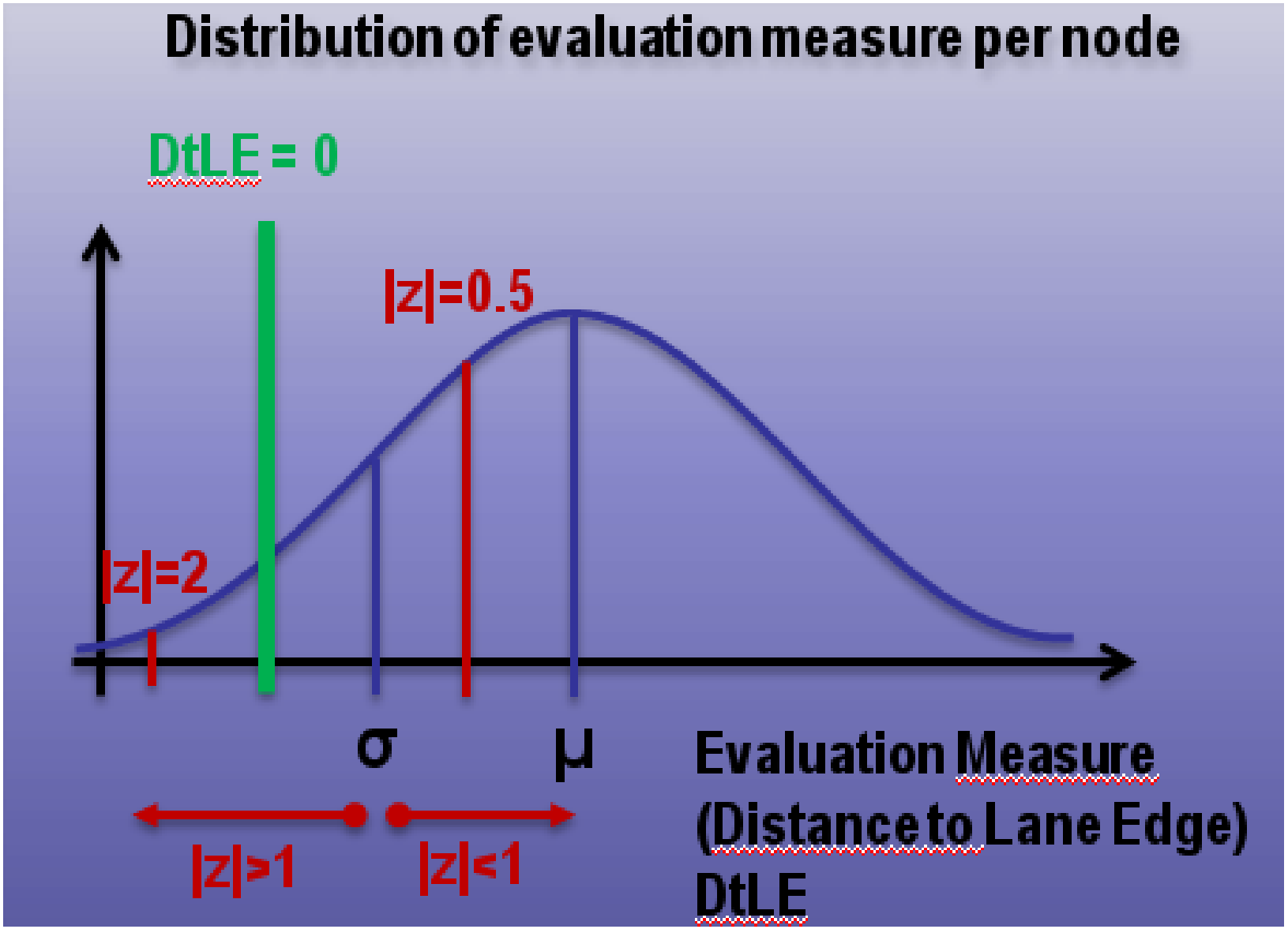
[Puch, Wortelen et al., 2012]

Update branch probabilities

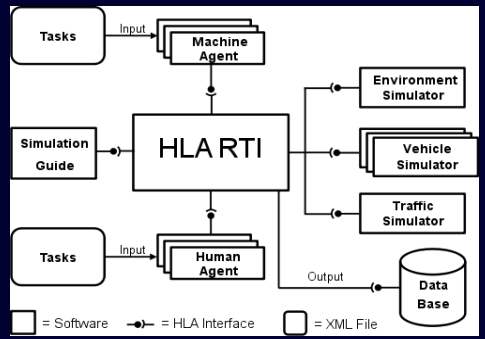


$$n_3 = |\text{visits}_{R17}|$$

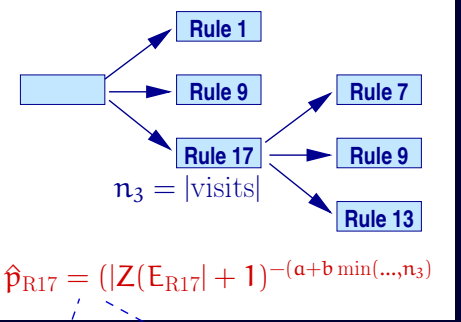
$$\hat{p}_{R17} = (|Z(E_{R17})| + 1)^{-(a+b\min\{\ldots,n_3\})}$$


Distribution of evaluation measure per node
DtLE = 0
|z|=0.5
|z|=2
σ
μ
Evaluation Measure
(Distance to Lane Edge)
DtLE
|z|>1
|z|<1

Simulate

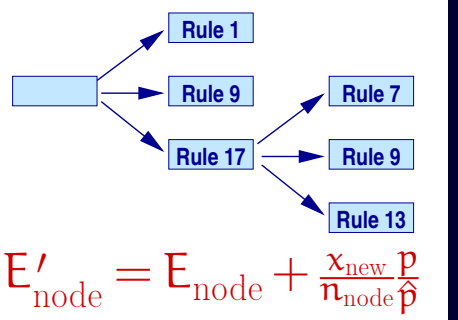


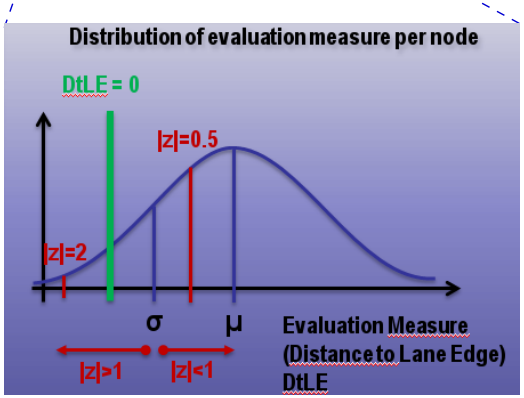
Update branch probabilities



Expand decision tree OTF

Update expectations



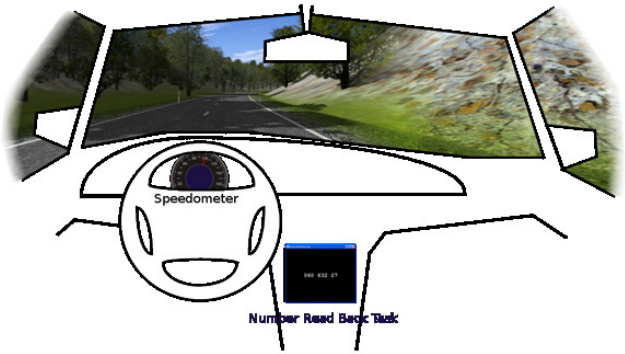


[Puch, Wortelen et al., 2012]

Effect of guiding — benchmark results

Scenario: Driving at a winding road with different curve radii

- Target speed $100\,\frac{\mathrm{km}}{\mathrm{h}}$
- Secondary in-vehicle task: read displayed numbers



Question: How likely is the distraction to cause a near hit of a bridge pillar far down the track?

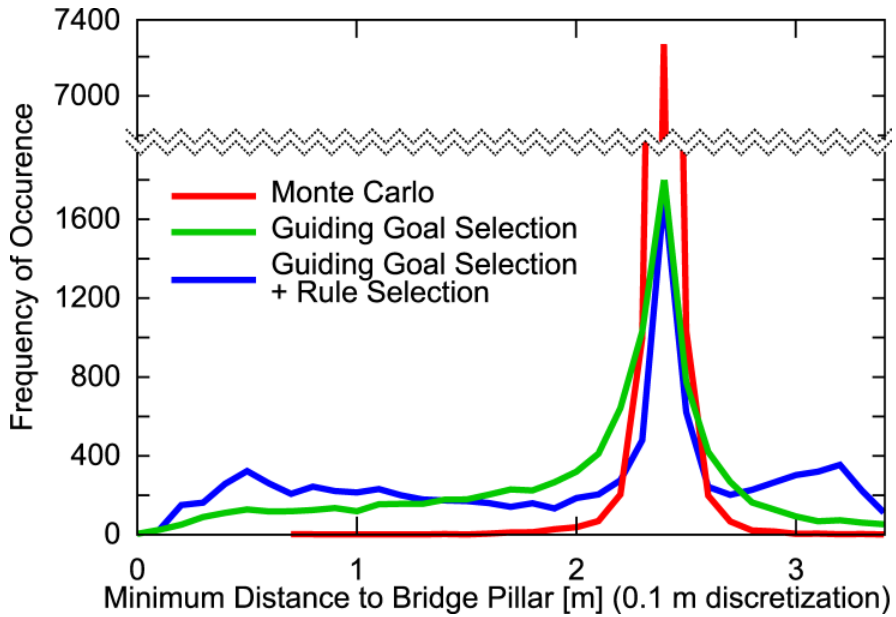
Effect of guiding — benchmark results

Scenario: Driving at a winding road with different curve radii

- Target speed $100\,\frac{\mathrm{km}}{\mathrm{h}}$
- Secondary in-vehicle task: read displayed numbers

Question: How likely is the distraction to cause a near hit of a bridge pillar far down the track?

Result: Within 10k simulations ($\approx$ 1 week simulation time), only guided simulation could provide reasonable yield of near-hits, i.e., a useful statistics



Step IV

Getting the Most out of Simulation Time by Trajectory Recombination

Rationale

Problem: Simulation still is extremely time-consuming:

- 10k simulations $\approx$ 1 week simulation time
- need to get into at least that range:
  - w/o importance sampling: need ≈ 2.5m simulations (safety target $4 \cdot 10^{-6}$ at confidence 99%)
  - with gain factor 1000: still need ≈ 2.5k simulations

$\Rightarrow$ still unsuitable for desktop use

Idea: Enhance simulation coverage (and thus statistics) through recombination (rather than computation) of simulation runs.

Rationale

Problem: Simulation still is extremely time-consuming:

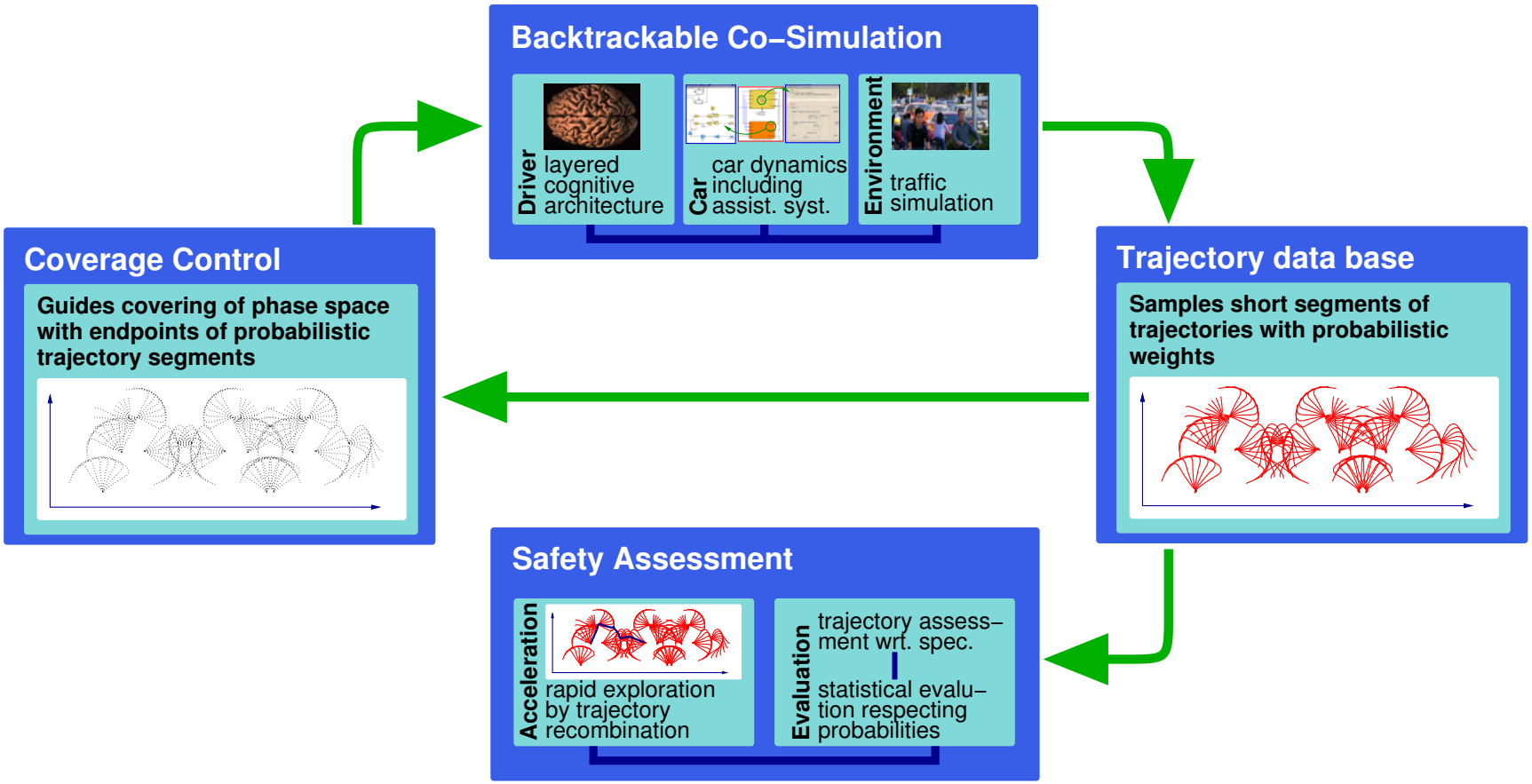
- 10k simulations $\approx$ 1 week simulation time
- need to get into at least that range:
  - w/o importance sampling: need ≈ 2.5m simulations (safety target $4 \cdot 10^{-6}$ at confidence 99%)
  - with gain factor 1000: still need ≈ 2.5k simulations

$\Rightarrow$ still unsuitable for desktop use

Idea: Enhance simulation coverage (and thus statistics) through recombination (rather than computation) of simulation runs.

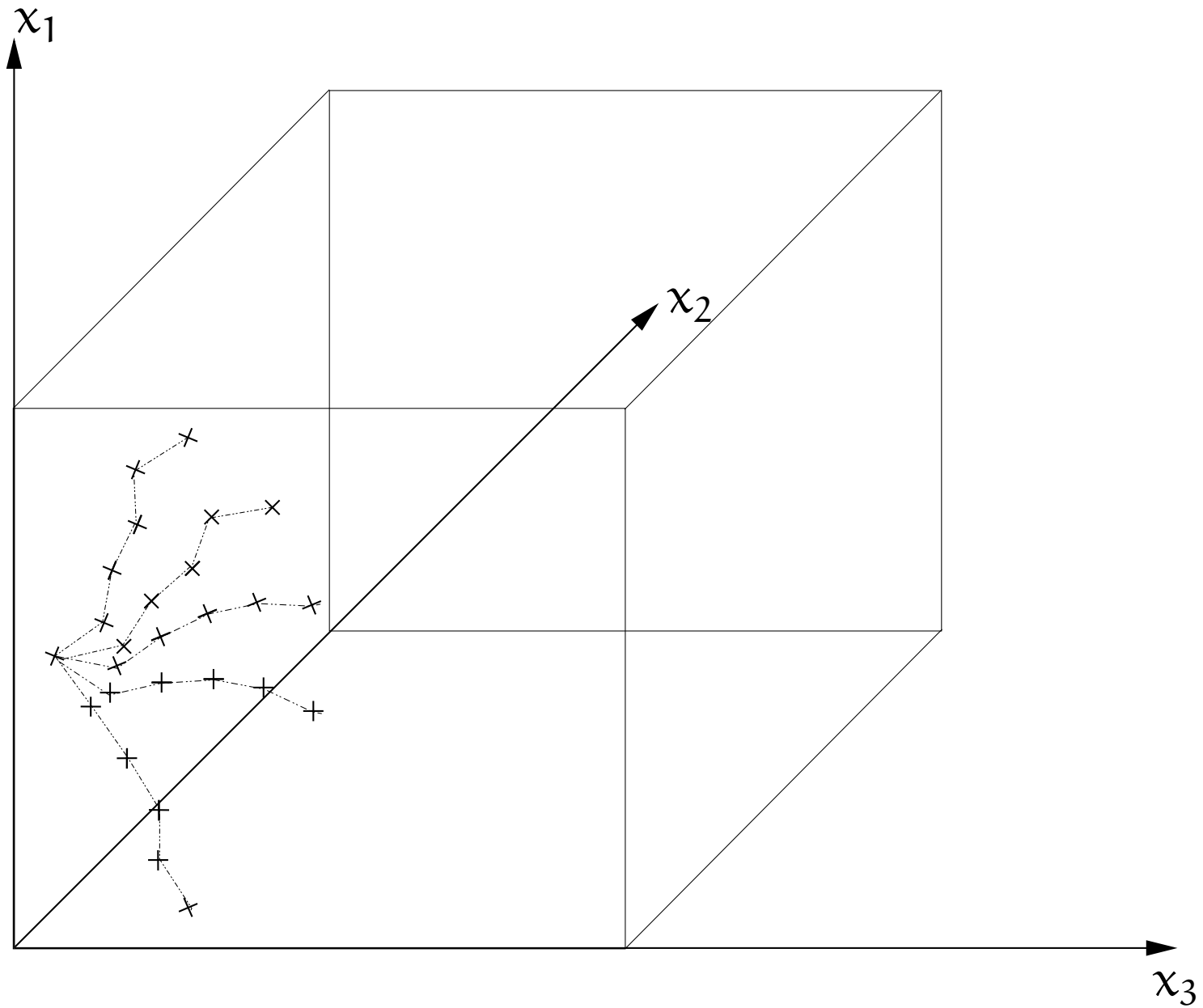
Approach: Collect trajectory segments;
recombine at crossing points (or at near hits).

State-space exploration by rapidly exploring random forests (RRF)

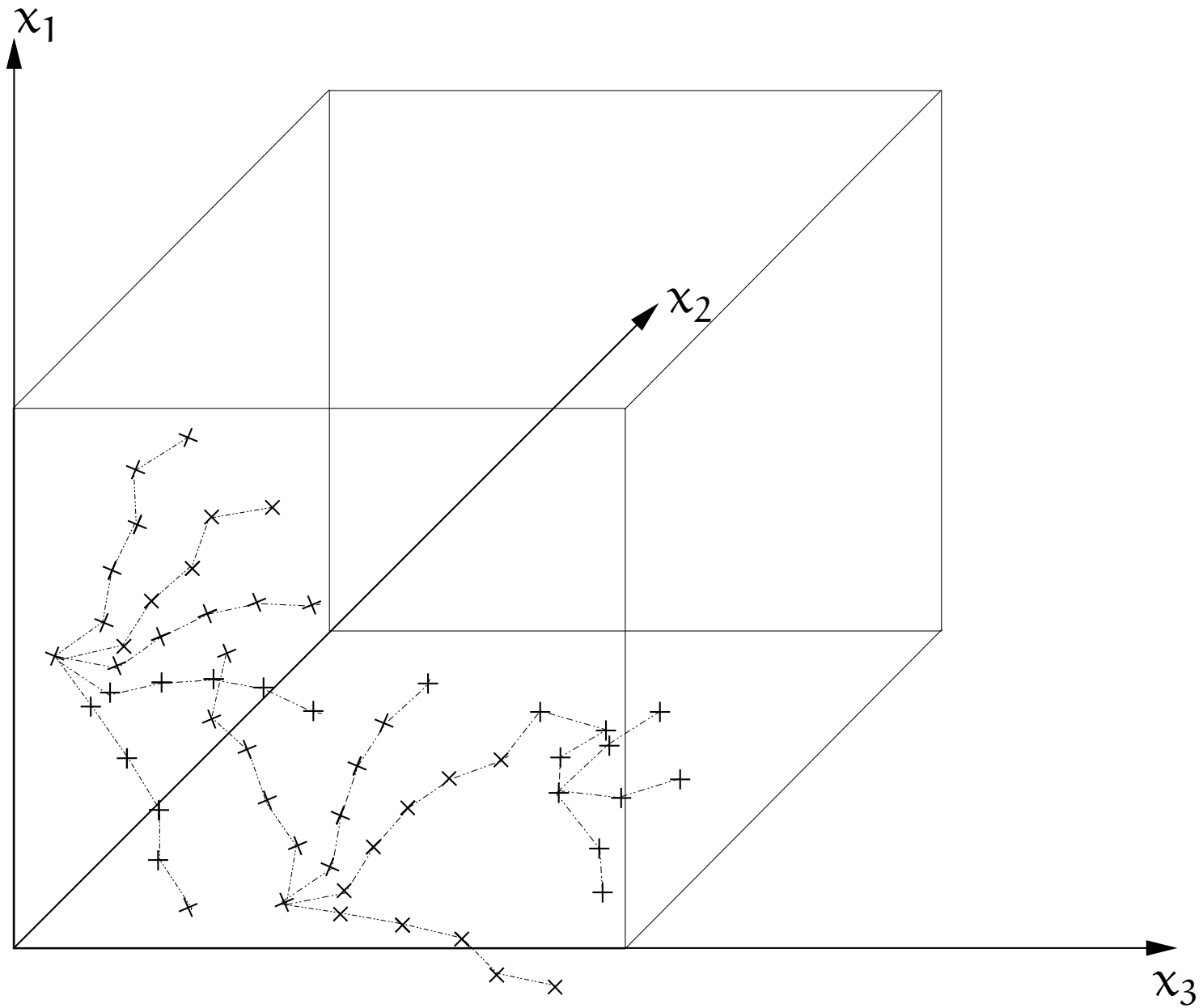


A novel extension of rapidly exploring random trees, as successfully used in robotics [LaValle, Kuffner 2001] and hybrid systems [Nahhal, Dang 2007–] for reachability, to quantitative analysis of stochastic systems.

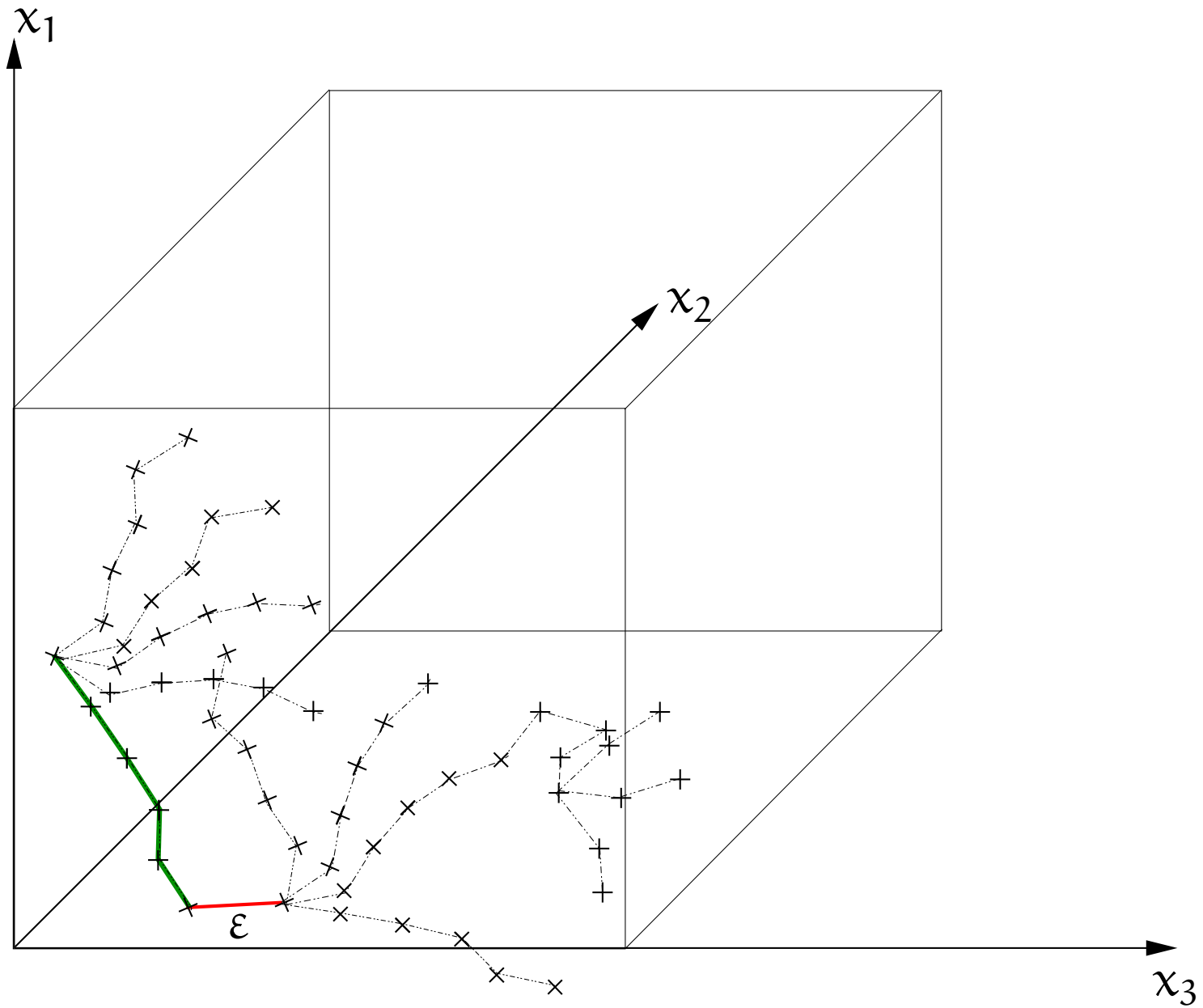
Recombination of trajectory segments from RRF



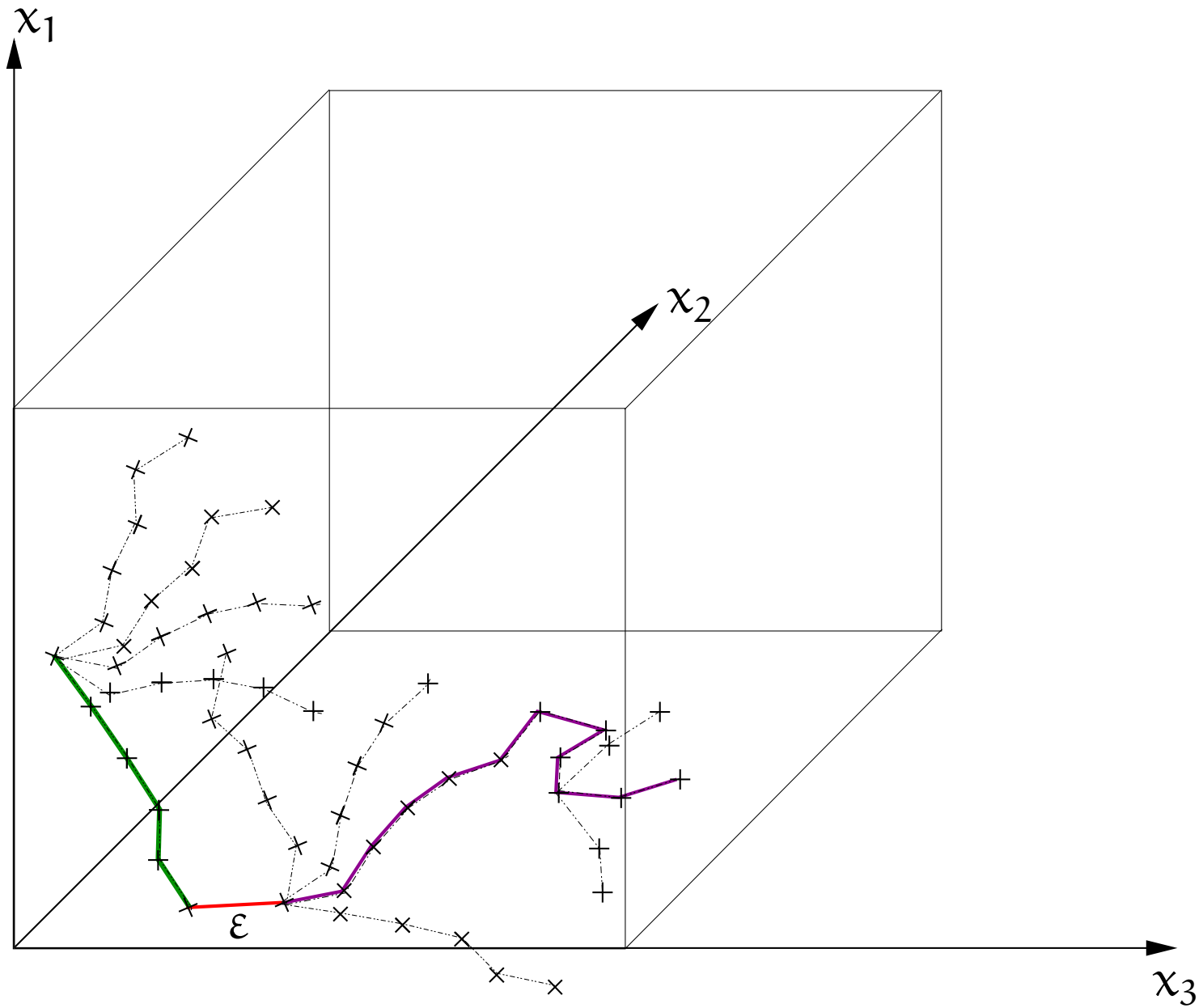
Recombination of trajectory segments from RRF



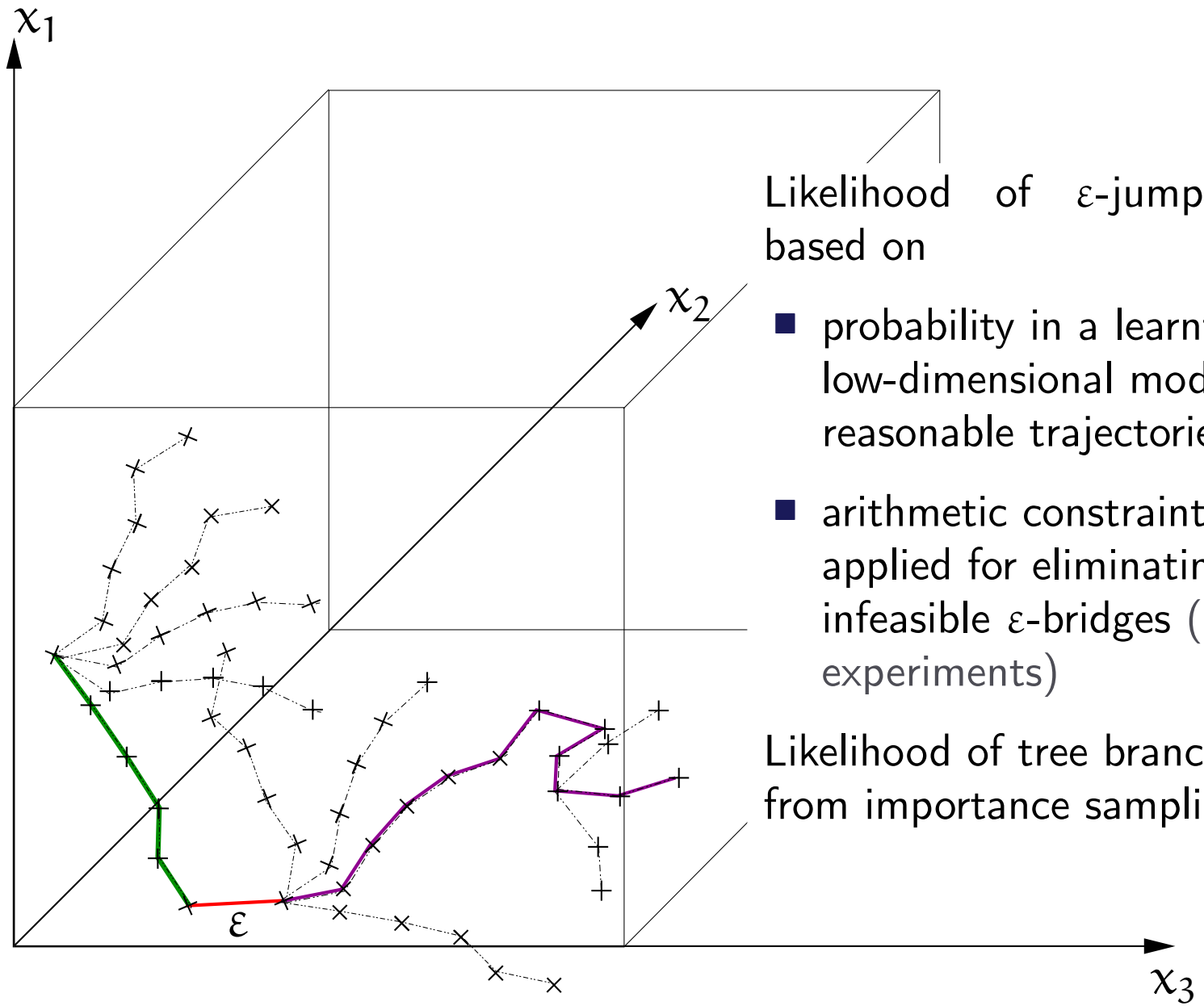
Recombination of trajectory segments from RRF



Recombination of trajectory segments from RRF



Recombination of trajectory segments from RRF

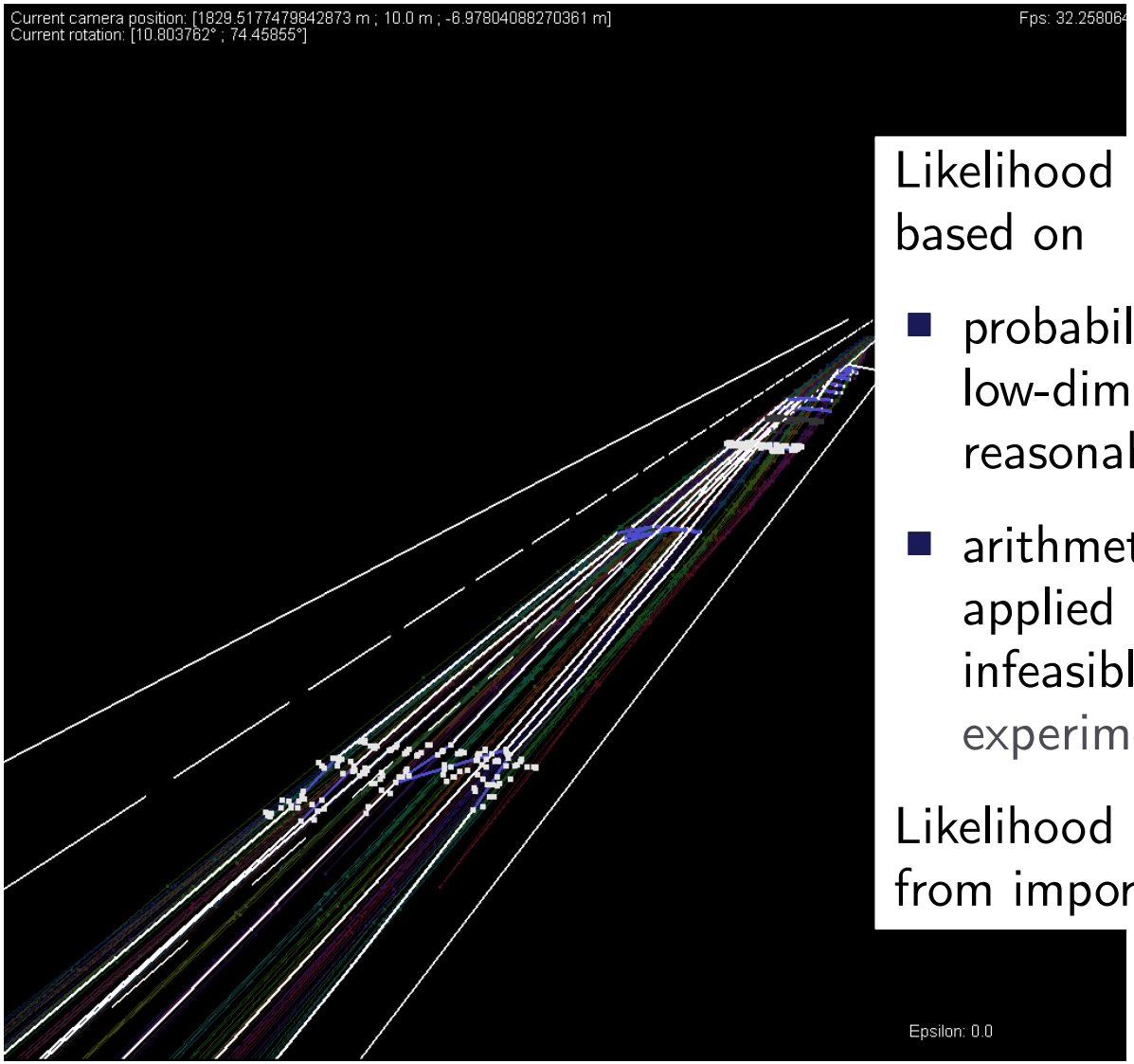


Likelihood of ε-jumps evaluated based on

- probability in a learnt low-dimensional model of reasonable trajectories in traffic
- arithmetic constraint solving applied for eliminating physically infeasible ε-bridges (first experiments)

Likelihood of tree branches inherited from importance sampling.

Recombination of trajectory segments from RRF



Likelihood of ε-jumps evaluated based on

- probability in a learnt low-dimensional model of reasonable trajectories in traffic
- arithmetic constraint solving applied for eliminating physically infeasible ε-bridges (first experiments)

Likelihood of tree branches inherited from importance sampling.

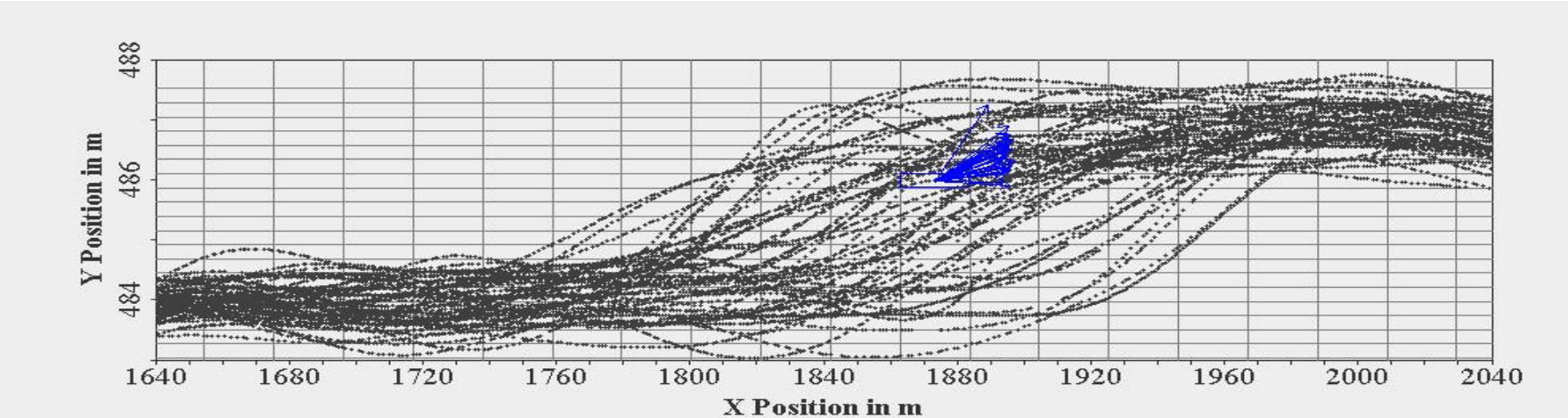
Step V

Mined Models Complementing Mind Models

Constructing stochastic models by data mining: Rationale

1. The cognitive model is a postulate
   - need a "measurable" model of normative behavior to validate (and optimize) it
2. ADAS shall provide help when driver is in need — not domineer over the driver
   - need a quantitative model of risk / controllability / ... for ADAS trigger design
3. Detailed co-simulation covers rather isolated maneuvers (e.g., filtering in) only; i.e., SMC computes conditional probabilities only
   - need to interface to models computing "background" probabilities

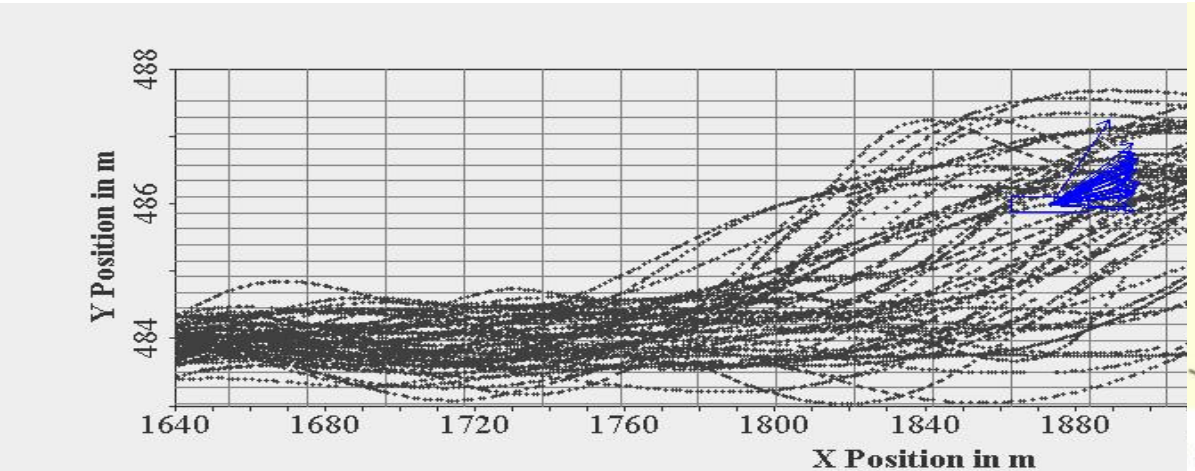
Mining stochastic models: Langevin analysis of human-in-the-loop dynamics [Langner, Peinke 2008–]

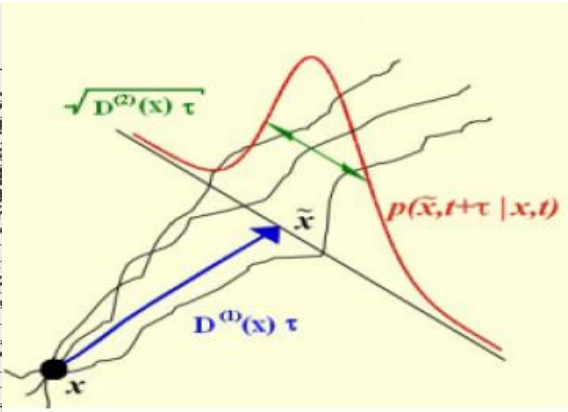


Derives a potential-based model of the joint dynamics of driver and car with or without assistance

- derivation is *automatic from experimental data* using an extension of the Langevin method
- extension is able to deal with scarce and non-equidistant samples [Langner, Peinke 2010]

Mining stochastic models: Langevin analysis of human-in-the-loop dynamics [Langner, Peinke 2008–]



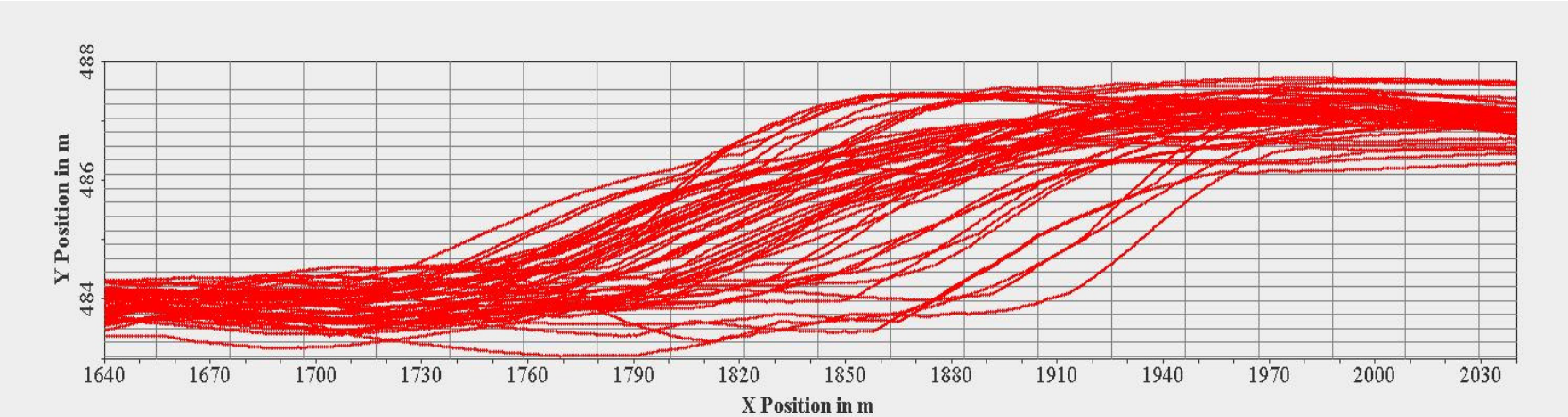


$$x(t) = x(t-\tau) + D^{(1)}(x)\tau + \sqrt{D^{(2)}(x)\tau}\Gamma(t)$$

Derives a potential-based model of the joint dynamics of driver and car with or without assistance

- derivation is *automatic from experimental data* using an extension of the Langevin method
- extension is able to deal with scarce and non-equidistant samples [Langner, Peinke 2010]

Mining stochastic models: Langevin analysis of human-in-the-loop dynamics [Langner, Peinke 2008–]

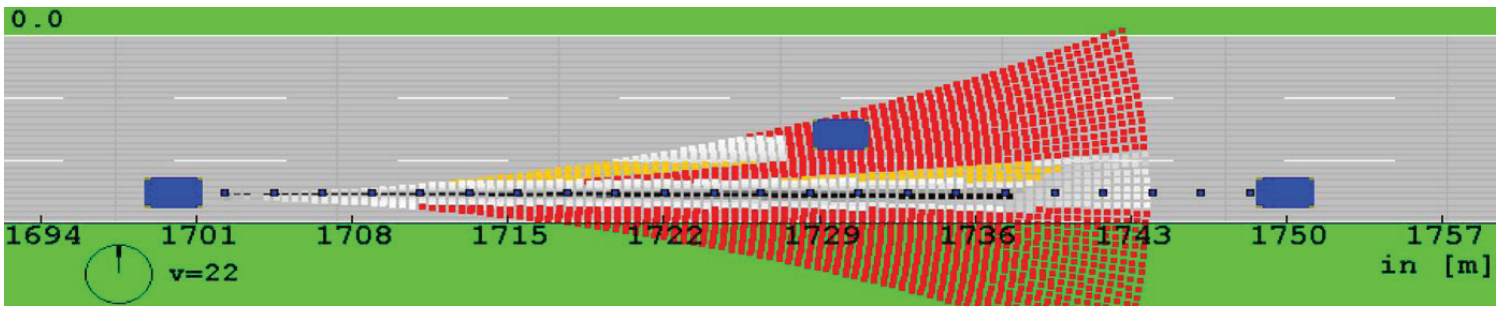


Derives a potential-based model of the joint dynamics of driver and car with or without assistance

- derivation is *automatic from experimental data* using an extension of the Langevin method
- extension is able to deal with scarce and non-equidistant samples [Langner, Peinke 2010]
- results in a stochastic vector field able to faithfully reconstruct global trajectories from a *low-dimensional*, homogeneous, Markovian model
- can be used for assessing the holistic co-simulation

Use of mined model in ADAS design

- Langevin model provides extrapolation of situation
- Can be used for computing (expected) time to collision
- Which can be converted into a risk map:



Risikowerte: Schwarz->kein Risiko; Grau/Weiß->erhöhtes Risiko;

Gelb-> nicht empfohlen; Rot->Unfall unvermeidlich

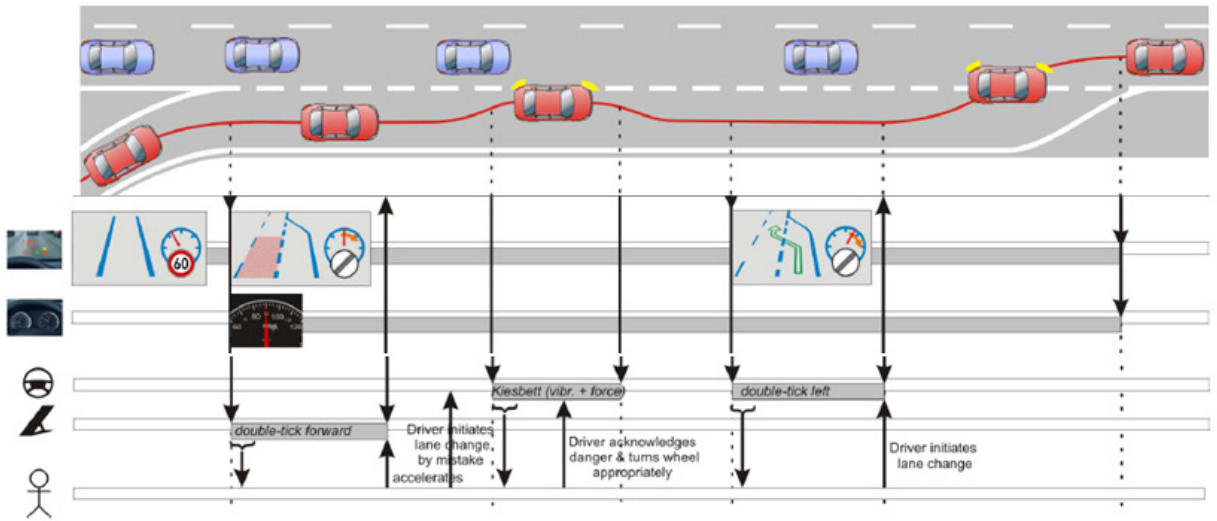
- Provides information on reasonable time/situation for
  - when to trigger the ADAS dialogues,
  - where to guide the driver.

Step VI

Requirements Specification

Visual system specification

Goal: A formal, visual, spatio-temporal logic for concisely expressing movements of traffic agents in space and time



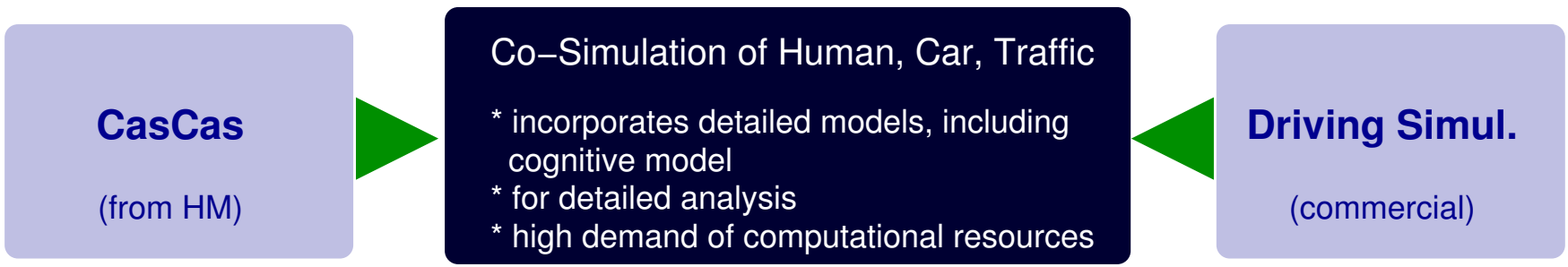
Approach: A spatio-temporal counterpart to MSCs/LSCs, designed to

1. enhance communication between traffic psychologists, system engineers, software engineers
2. permit automatic on-line evaluation of driving experiments / simulations wrt. formal specifications (including animation of spec.)
3. serve as a concise and expressive filter when browsing experiment data bases

Discussion

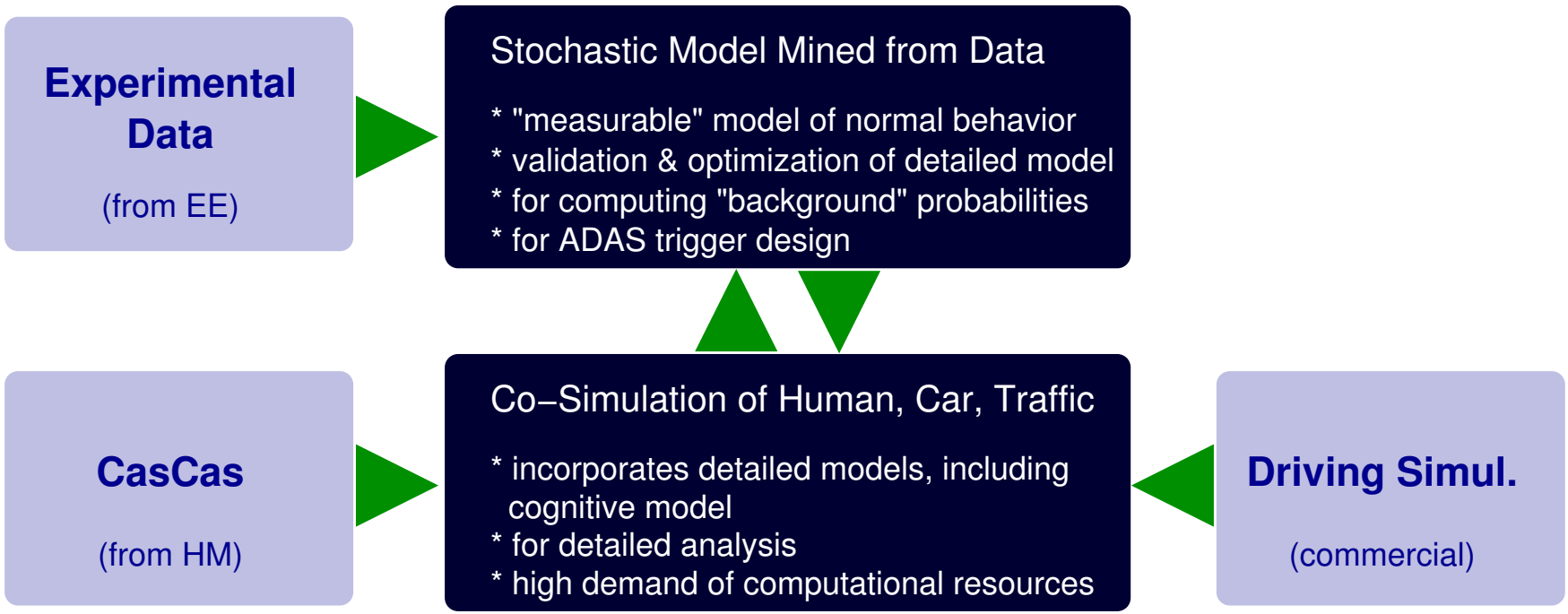
Problems addressed by IMoST AN

1. **Simulation explores only one trajectory per simulation run:**
   - coverage?
   - generation of interesting inputs for open systems?
   - estimation of probability of hazardous behaviour?
2. **Analysis of simulation results:**
   - lacking a mechanism for generating interesting input, hazardous situations can only (if ever) be found by simulating enourmous numbers of different scenarios
   - how to find the needle in the haystack of simulation runs?
3. **Human models inevitably are approximations only:**
   - impact on safety assessment unclear.
4. **Accidents in human-controlled traffic are extremely rare events:**
   - very unlikely to see a statistically relevant number of accidents in any reasonable number of simulation runs.


CasCas
(from HM)
Co–Simulation of Human, Car, Traffic
* incorporates detailed models, including cognitive model
* for detailed analysis
* high demand of computational resources
Driving Simul.
(commercial)

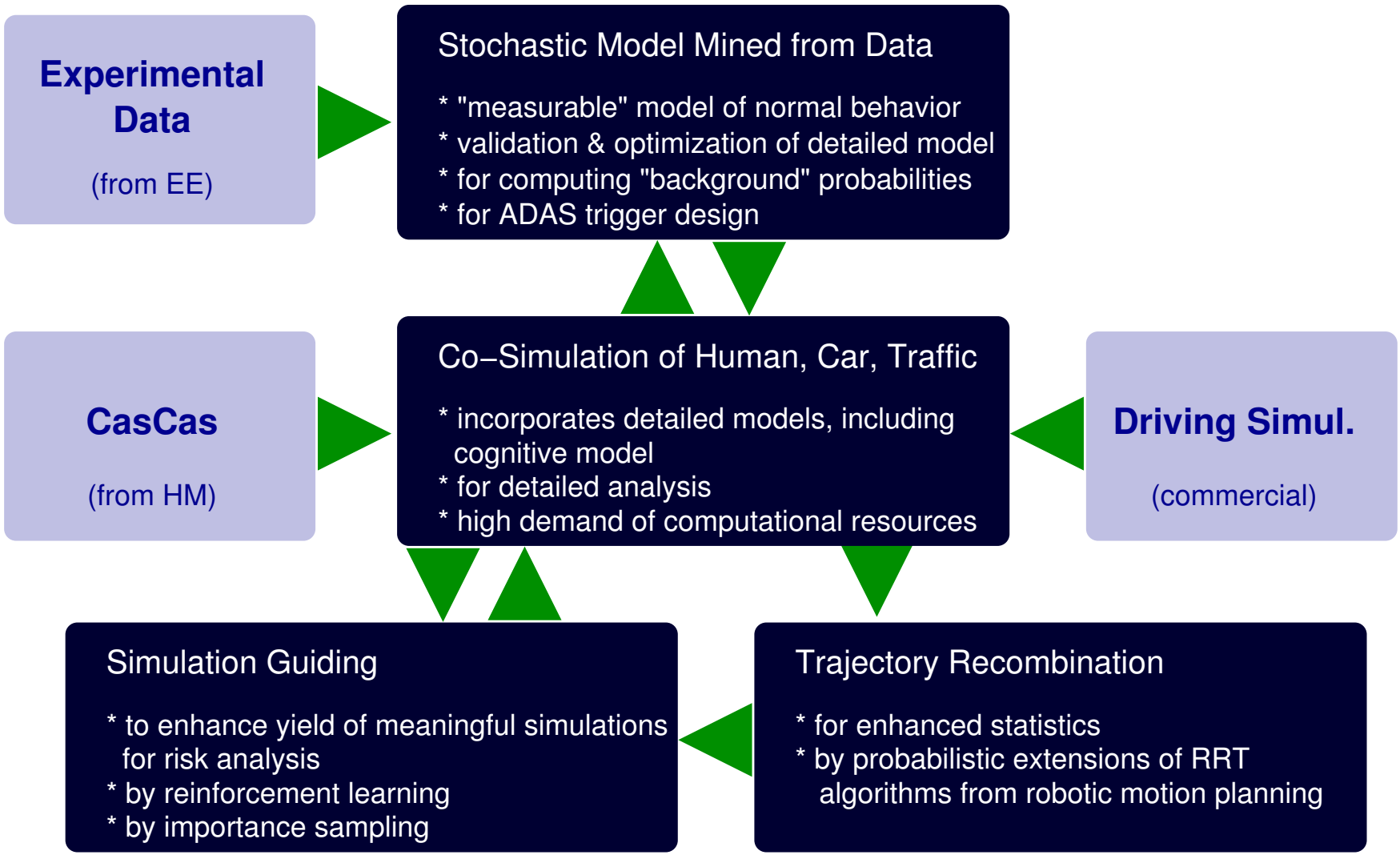
Specification

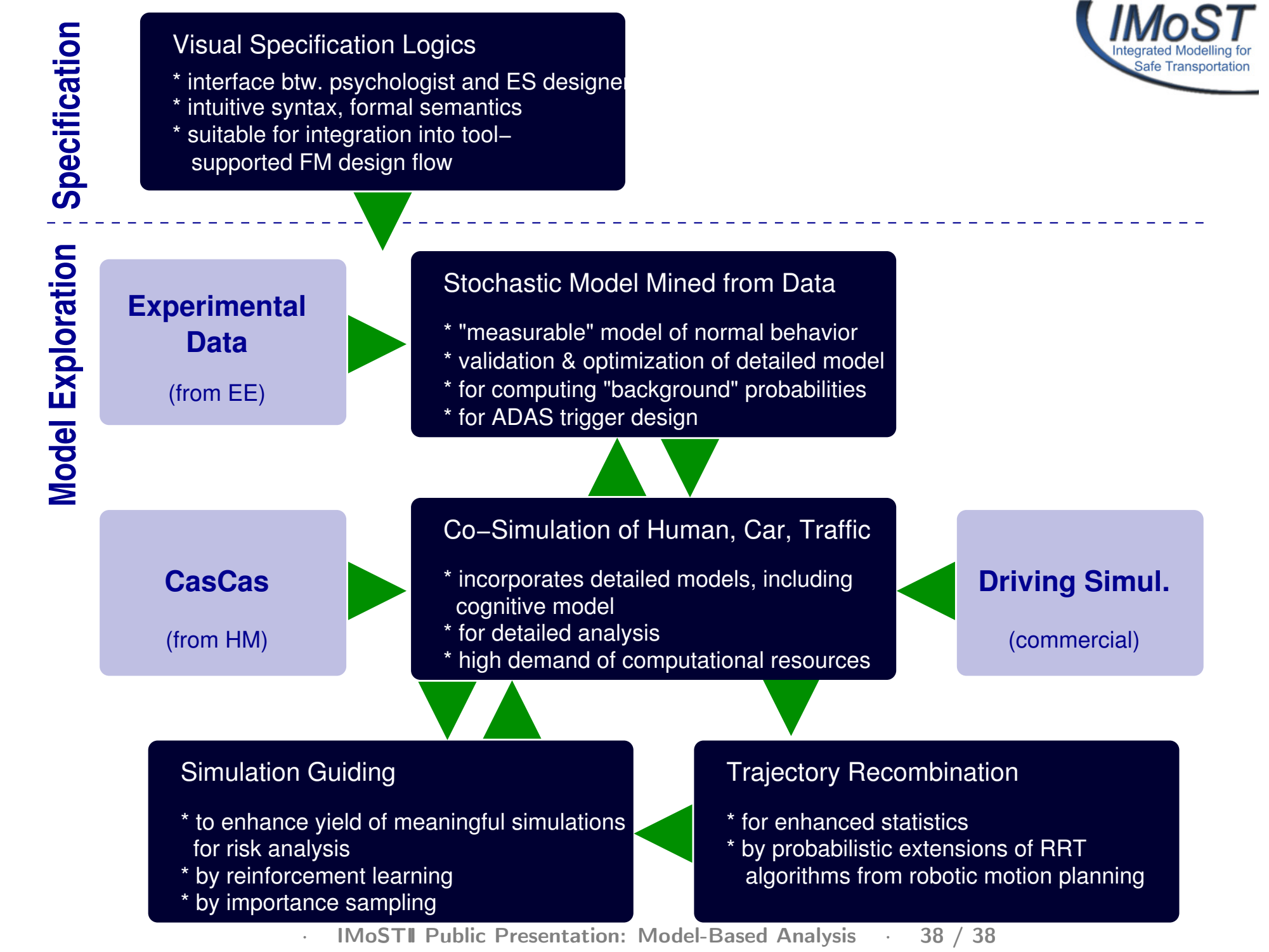
Model Exploration

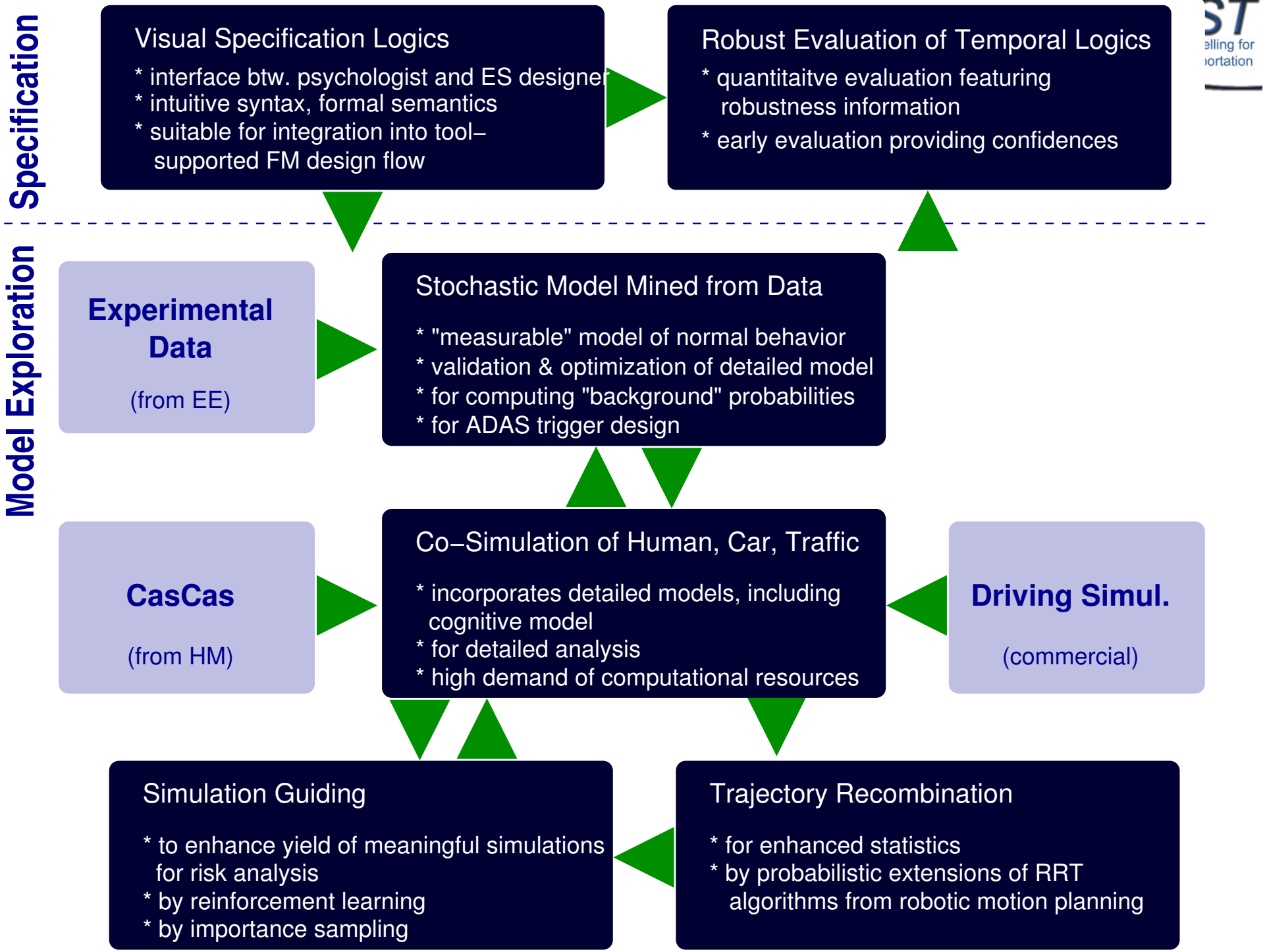


Specification

Model Exploration




Specification
Model Exploration
Visual Specification Logics
* interface btw. psychologist and ES designer
* intuitive syntax, formal semantics
* suitable for integration into tool–supported FM design flow
Experimental Data
(from EE)
Stochastic Model Mined from Data
* "measurable" model of normal behavior
* validation & optimization of detailed model
* for computing "background" probabilities
* for ADAS trigger design
CasCas
(from HM)
Co–Simulation of Human, Car, Traffic
* incorporates detailed models, including cognitive model
* for detailed analysis
* high demand of computational resources
Driving Simul.
(commercial)
Simulation Guiding
* to enhance yield of meaningful simulations for risk analysis
* by reinforcement learning
* by importance sampling
Trajectory Recombination
* for enhanced statistics
* by probabilistic extensions of RRT algorithms from robotic motion planning


Specification
Model Exploration
Visual Specification Logics
* interface btw. psychologist and ES designer
* intuitive syntax, formal semantics
* suitable for integration into tool–supported FM design flow
Robust Evaluation of Temporal Logics
* quantitaitve evaluation featuring robustness information
* early evaluation providing confidences
Experimental Data
(from EE)
Stochastic Model Mined from Data
* "measurable" model of normal behavior
* validation & optimization of detailed model
* for computing "background" probabilities
* for ADAS trigger design
CasCas
(from HM)
Co–Simulation of Human, Car, Traffic
* incorporates detailed models, including cognitive model
* for detailed analysis
* high demand of computational resources
Driving Simul.
(commercial)
Simulation Guiding
* to enhance yield of meaningful simulations for risk analysis
* by reinforcement learning
* by importance sampling
Trajectory Recombination
* for enhanced statistics
* by probabilistic extensions of RRT algorithms from robotic motion planning