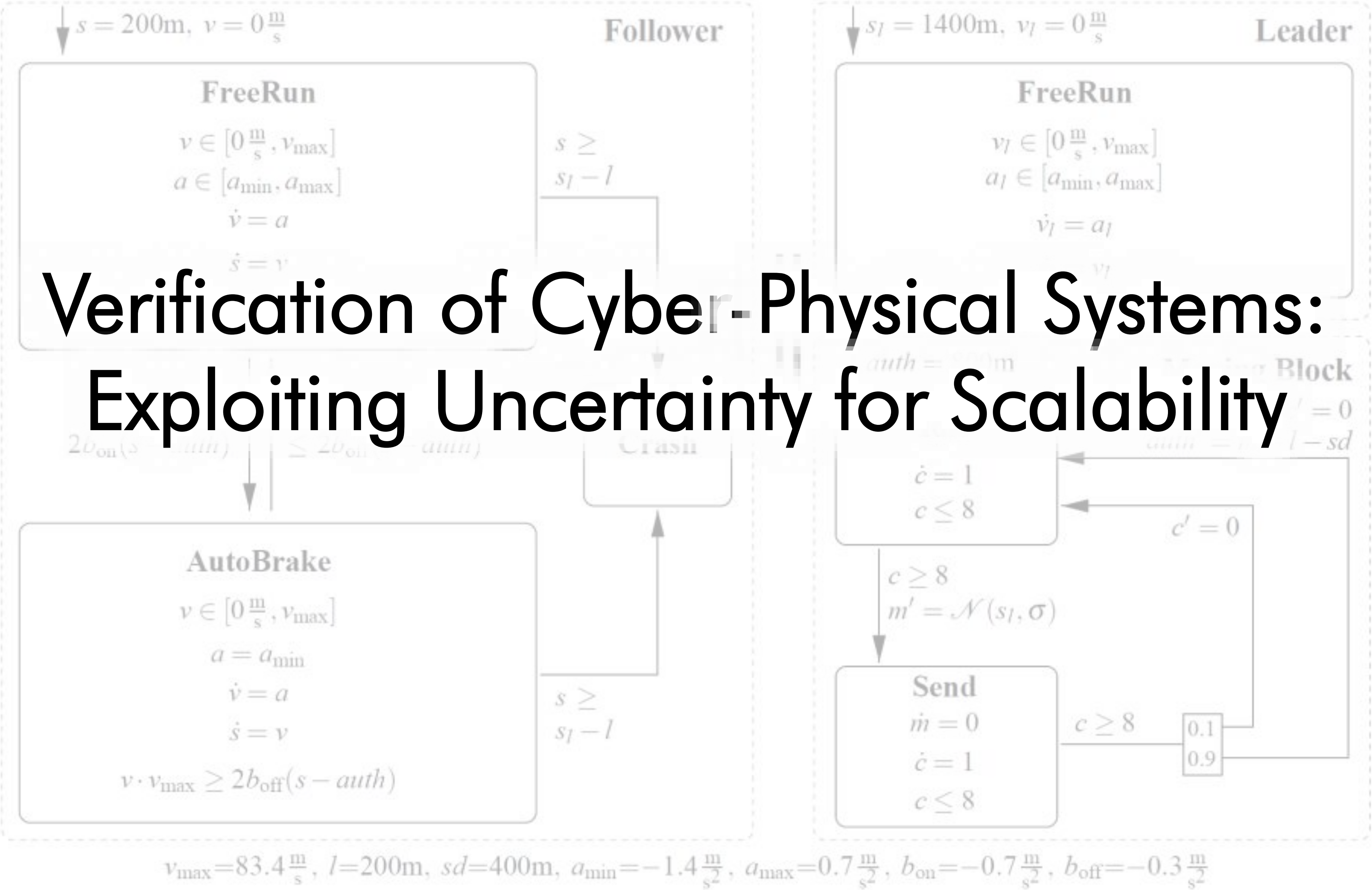
VENI 2017 PROPOSAL

Verification of Cyber-Physical Systems: Exploiting Uncertainty for Scalability


$s = 200\text{m},\ v = 0\frac{\text{m}}{\text{s}}$
Follower
FreeRun
$v \in [0\frac{\text{m}}{\text{s}}, v_{\max}]$
$a \in [a_{\min}, a_{\max}]$
$\dot{v} = a$
$\dot{s} = v$
$s \geq s_l - l$
Crash
AutoBrake
$v \in [0\frac{\text{m}}{\text{s}}, v_{\max}]$
$a = a_{\min}$
$\dot{v} = a$
$\dot{s} = v$
$v \cdot v_{\max} \geq 2b_{\text{off}}(s - auth)$
$s \geq s_l - l$
$s_l = 1400\text{m},\ v_l = 0\frac{\text{m}}{\text{s}}$
Leader
FreeRun
$v_l \in [0\frac{\text{m}}{\text{s}}, v_{\max}]$
$a_l \in [a_{\min}, a_{\max}]$
$\dot{v}_l = a_l$
Block
$l - sd$
$\dot{c} = 1$
$c \leq 8$
$c' = 0$
$c \geq 8$
$m' = \mathcal{N}(s_l, \sigma)$
Send
$\dot{m} = 0$
$\dot{c} = 1$
$c \leq 8$
$c \geq 8$
0.1
0.9
$v_{\max}=83.4\frac{\text{m}}{\text{s}},\ l=200\text{m},\ sd=400\text{m},\ a_{\min}=-1.4\frac{\text{m}}{\text{s}^2},\ a_{\max}=0.7\frac{\text{m}}{\text{s}^2},\ b_{\text{on}}=-0.7\frac{\text{m}}{\text{s}^2},\ b_{\text{off}}=-0.3\frac{\text{m}}{\text{s}^2}$

Arnd Hartmanns

Formal Methods and Tools, University of Twente

Cyber-Physical Systems

fly-by-wire airplanes

self-driving vehicles

Internet of things

smart grids

industrial automation

⇨ safety-critical **cyber-physical systems**

Cyber-Physical Systems

fly-by-wire airplanes

self-driving vehicles

Internet of things

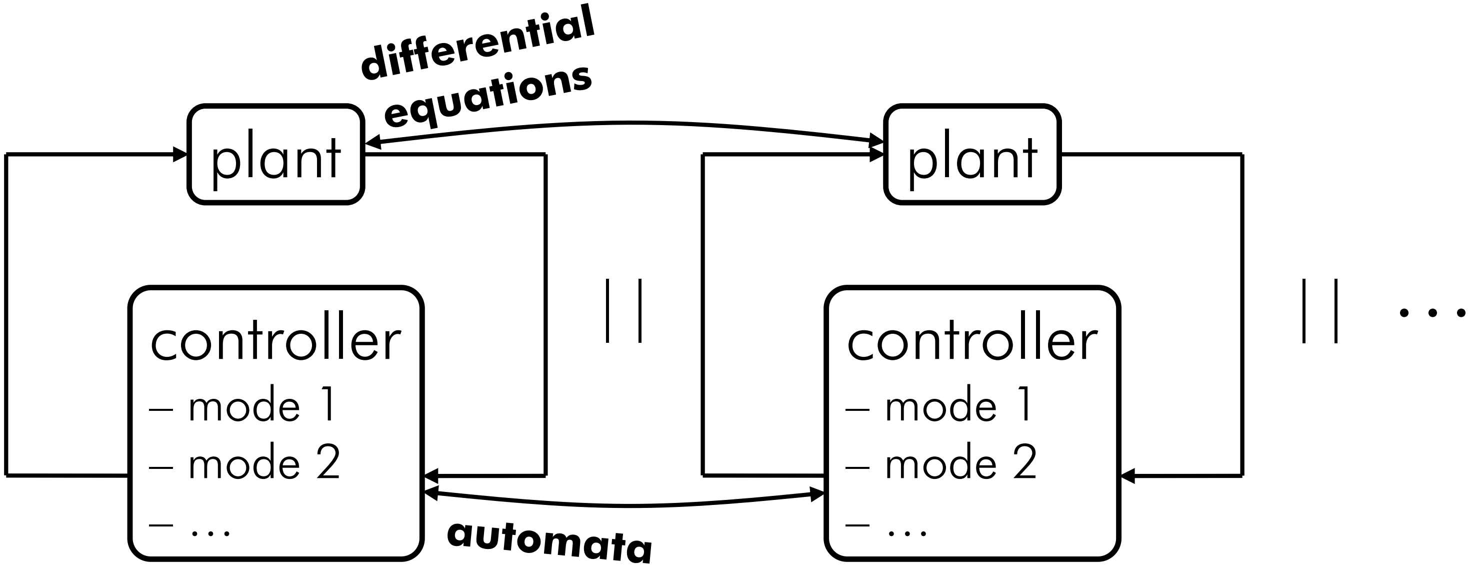
smart grids

industrial automation

⇨ safety-critical **cyber-physical systems**

physical continuous

discrete control logic software



Cyber-Physical Systems

fly-by-wire airplanes

self-driving vehicles

Internet of things

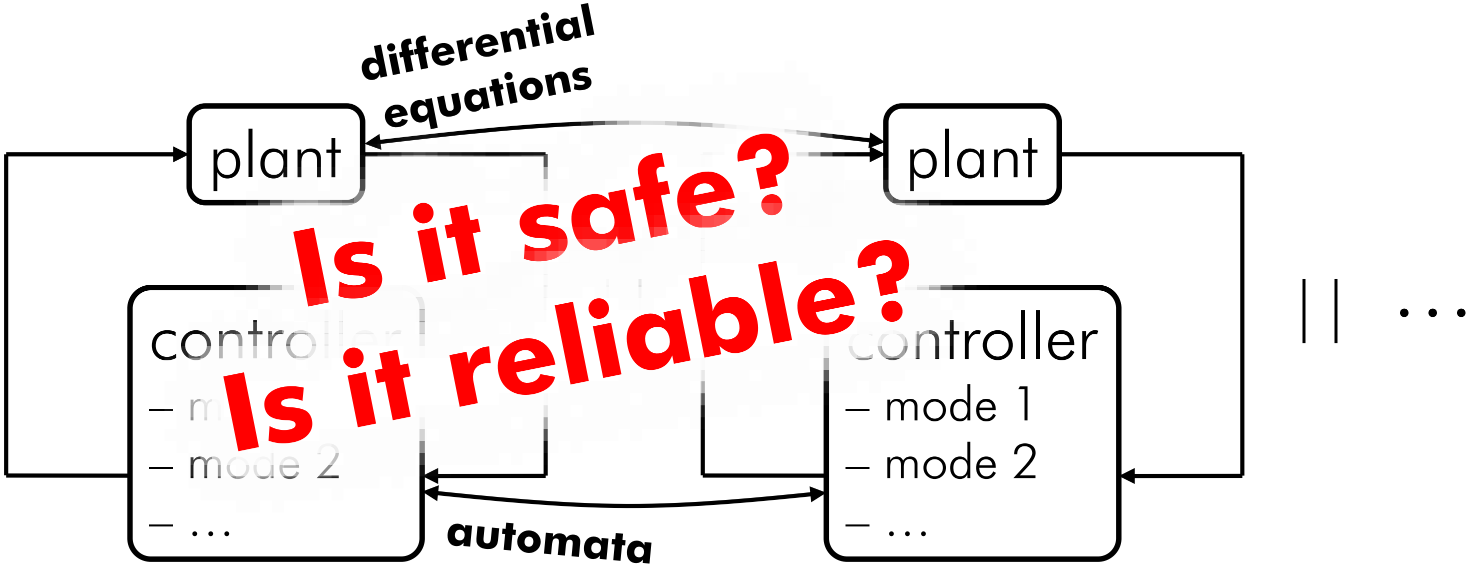
smart grids

industrial automation

⇒ safety-critical **cyber-physical systems**

physical continuous

discrete control logic software



differential equations

plant

plant

controller

– m

– mode 2

– …

controller

– mode 1

– mode 2

– …

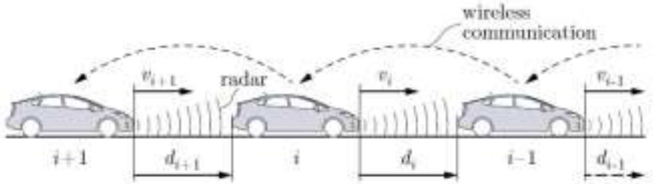
automata

|| …

Is it safe?

Is it reliable?

Uncertainty



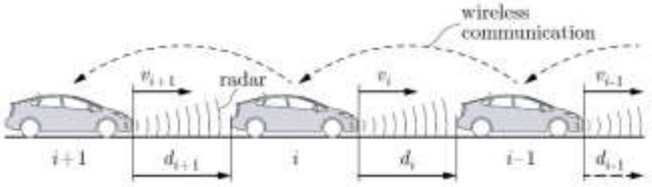
? measurement errors,
randomised algorithms, …

? safety for any leading vehicle behaviour **(within its physical limits)**

⇨ **uncertain** safety-critical cyber-physical systems

↳ **quantified and unquantified uncertainty**

Uncertainty



? measurement errors,
randomised algorithms, …

? safety for any leading vehicle behaviour **(within its physical limits)**

⇨ **uncertain** safety-critical cyber-physical systems

↳ **quantified and unquantified uncertainty**

verification:

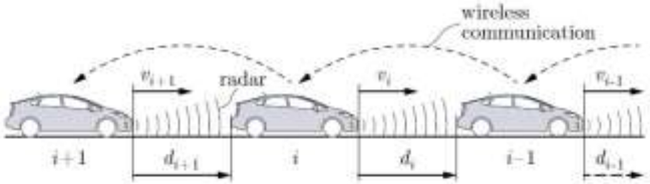
Will the cars ever collide? Yes. ☹

What is the probability within a single trip? $< 10^{-16}$ ☺

⇨ safety **proof**

⚡ simulation

Uncertainty



? measurement errors, randomised algorithms, …

? safety <u>for any</u> leading vehicle behaviour **(within its physical limits)**

⇨ **uncertain** safety-critical cyber-physical systems

↳ **quantified and unquantified uncertainty**

verification:

Will the cars ever collide? Yes. ☹

What is the probability within a single trip? $< 10^{-16}$ ☺

⇨ safety **proof**

⚡ simulation

state of the art

undecidable

Uncertainty = complication on top of classic verification problem

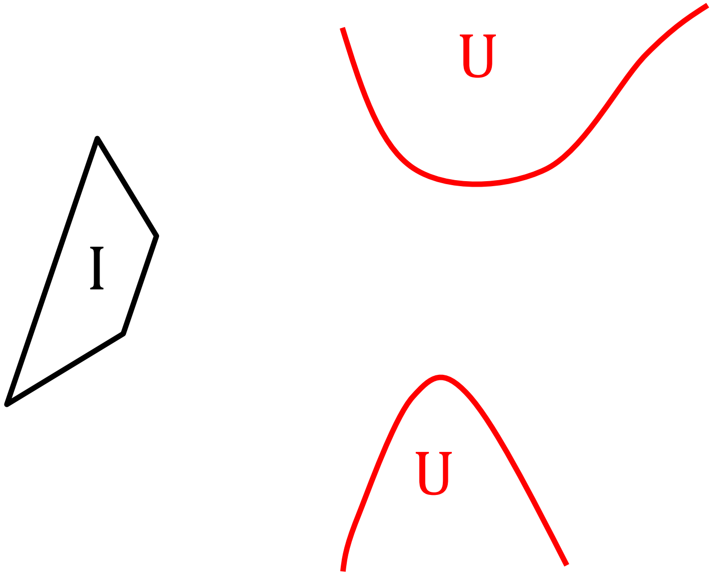
Exploiting Uncertainty

challenge

good approximations + abstractions, effective refinement strategies

⚖ *prove safety ⇔ computational effort*

time + memory



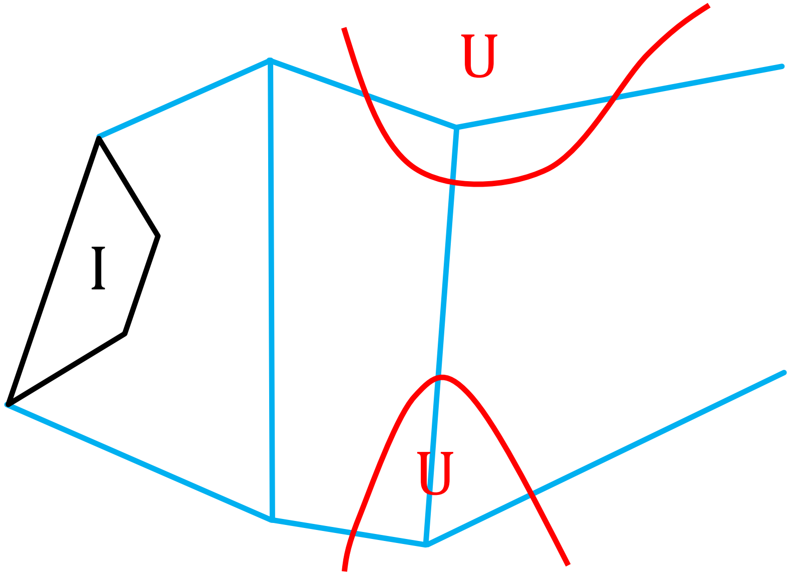
Exploiting Uncertainty

challenge

good approximations + abstractions, effective refinement strategies

⚖ *prove safety ⇔ computational effort*

time + memory



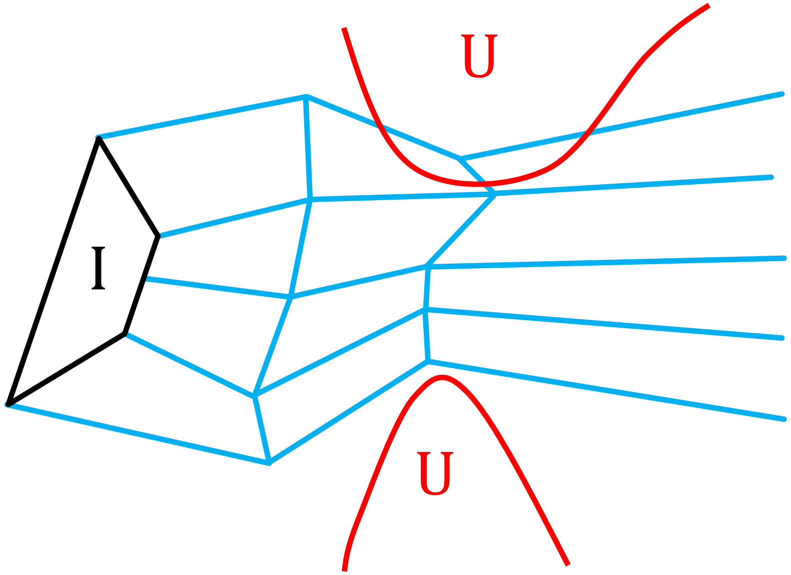
Exploiting Uncertainty

challenge

good approximations + abstractions, effective refinement strategies

⚖ *prove safety ⇔ computational effort*

time + memory



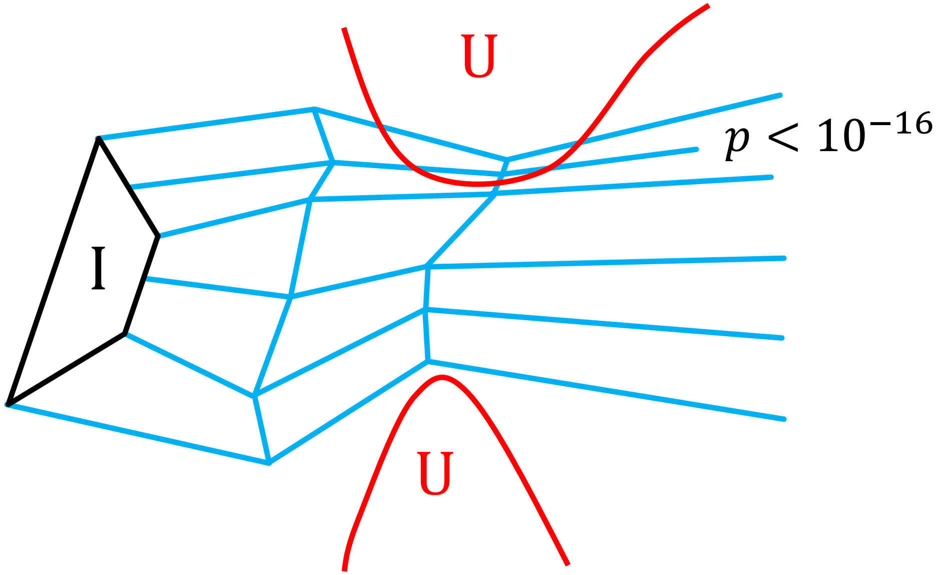
Exploiting Uncertainty

challenge

good approximations + abstractions, effective refinement strategies

⚖ *prove safety ⇔ computational effort*

time + memory



Exploiting Uncertainty

challenge

good approximations + abstractions, effective refinement strategies

⚖ *prove safety* ⇔ *computational effort*

time + memory

my idea

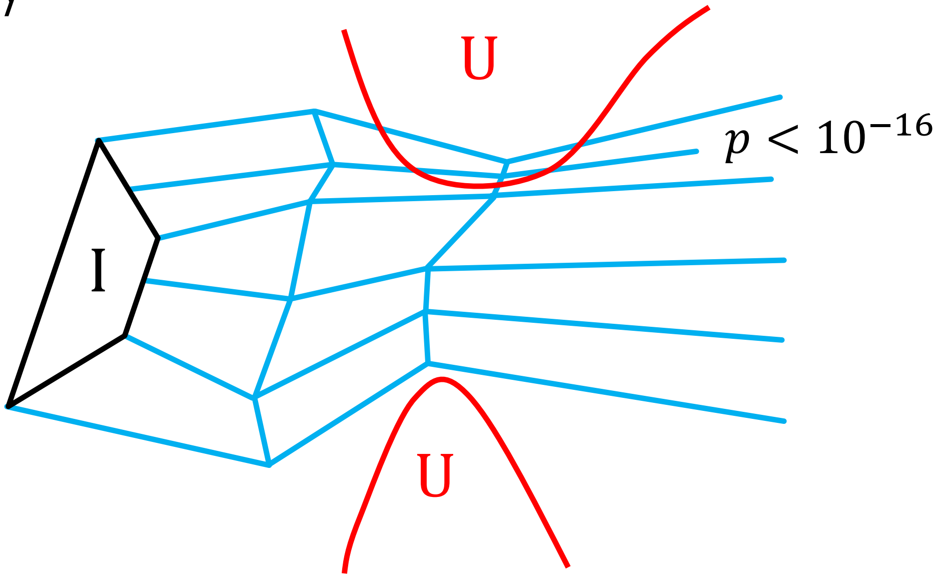
exploit the presence of uncertainty: make use of the extra information!

– focus on likely behaviours
– trade accuracy for scalability
– guided refinement
– …

WP1 algorithms & strategies

WP2 semantics & patterns

WP3 case studies & tools



Applications

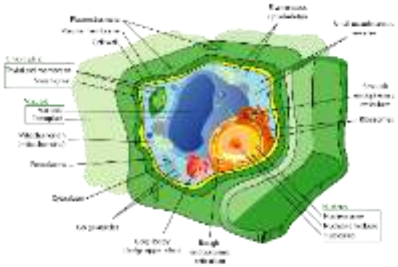
implementation in the Modest Toolset

distributed control of photovoltaic panels
(my thesis)

survivability of critical infrastructures
(University of Münster)

light electric vehicles
(Saarland University)

learning to drive autonomously
(TU Delft)



biological cell signaling
(University of Twente)

nanosatellite scheduling
(Saarland University)

⇨ in collaborations with external experts

The Proposal

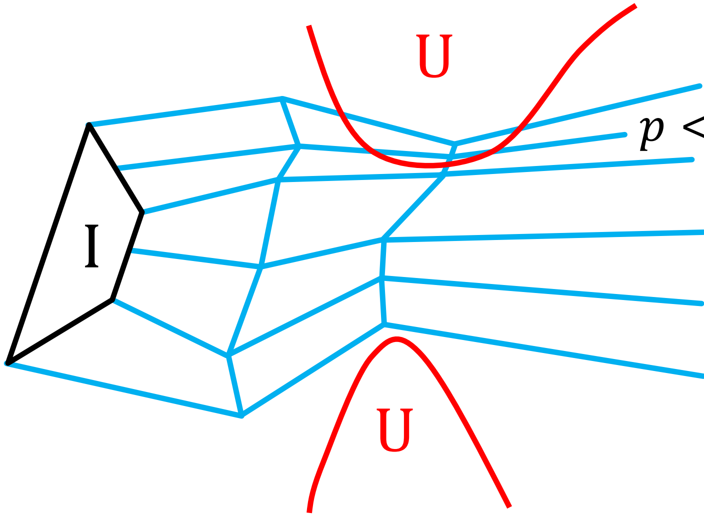
my expertise:

algorithms and tools for quantitative verification

exploiting uncertainty

scalable verification of cyber-physical systems by exploiting uncertainty

new theory, tools and case studies

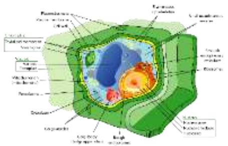


$$P_{\max}(\text{unsafe}) \in [10^{-16}, 10^{-14}]$$

Modest Toolset +

distributed control of photovoltaic panels
(my thesis)

light electric vehicles
(Saarland University)

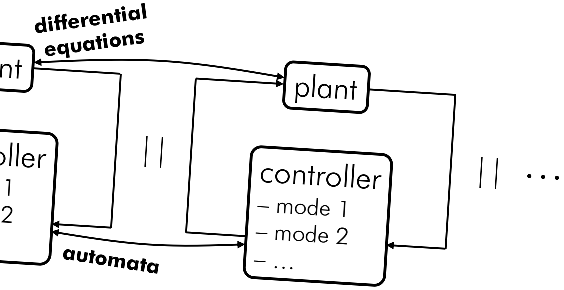


biological cell signaling
(University of Twente)

survivability of critical infrastructures
(University of Münster)

learning to drive autonomously
(TU Delft)

nanosatellite scheduling
(Saarland University)



differential equations
nt
plant
ller
1
2
||
controller
– mode 1
– mode 2
– ...
automata
|| ...