Cyber-Physical Systems

Laura Nenzi

Università degli Studi di Trieste
II Semestre 2020

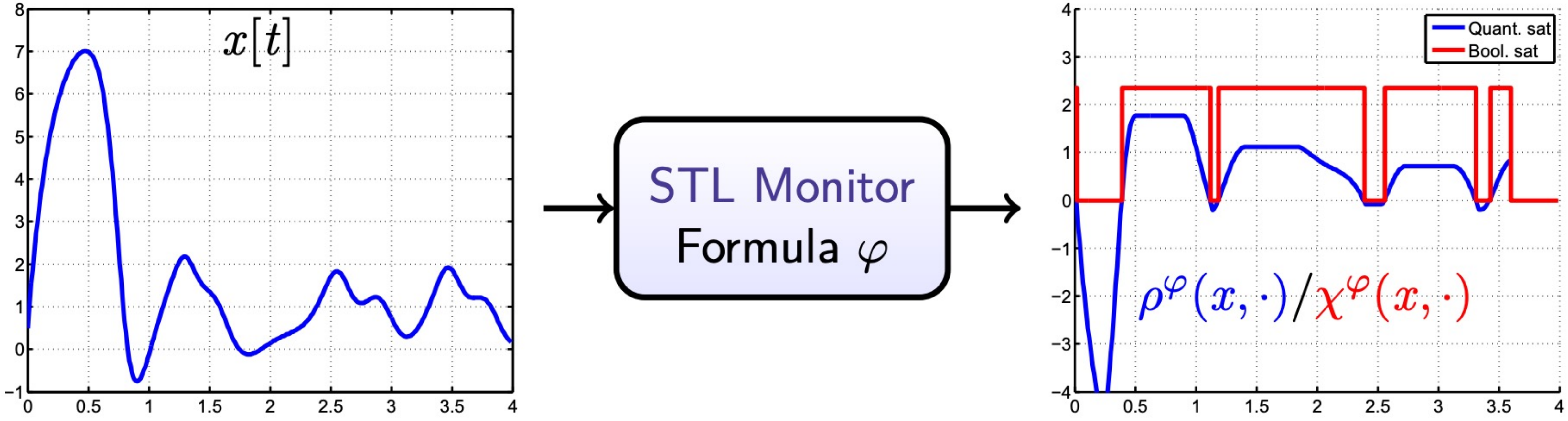
Lecture 14 (second part): STL applications: intro to falsification

[Many Slides due to J. Deshmukh, S. Silvetti]

Terminology

- **Syntax**: A set of syntactic rules that allow us to construct formulas from specific ground terms
- **Semantics**: A set of rules that assign meanings to well-formed formulas obtained by using above syntactic rules
- **Model-checking/Verification**: $M \vDash \phi \iff \forall \mathbf{x} \in trace(M) \;\; s(\varphi, \mathbf{x}, 0) = 1$
- **Monitoring**: computing s for a single trace $\mathbf{x} \in trace(M)$
- **Statistical Model Checking**: “doing statistics” on s$(\varphi, \mathbf{x}, 0)$ for a finite-subset of $trace(M)$

STL Monitor



An STL monitor is a transducer that transforms x into Boolean or a quantitative signal

The many uses of STL

- Requirement-based testing for closed-loop control models
- Falsification Analysis
- Parameter Synthesis
- Mining Specifications/Requirements from Models
- Online Monitoring
- …

Closed-loop Models

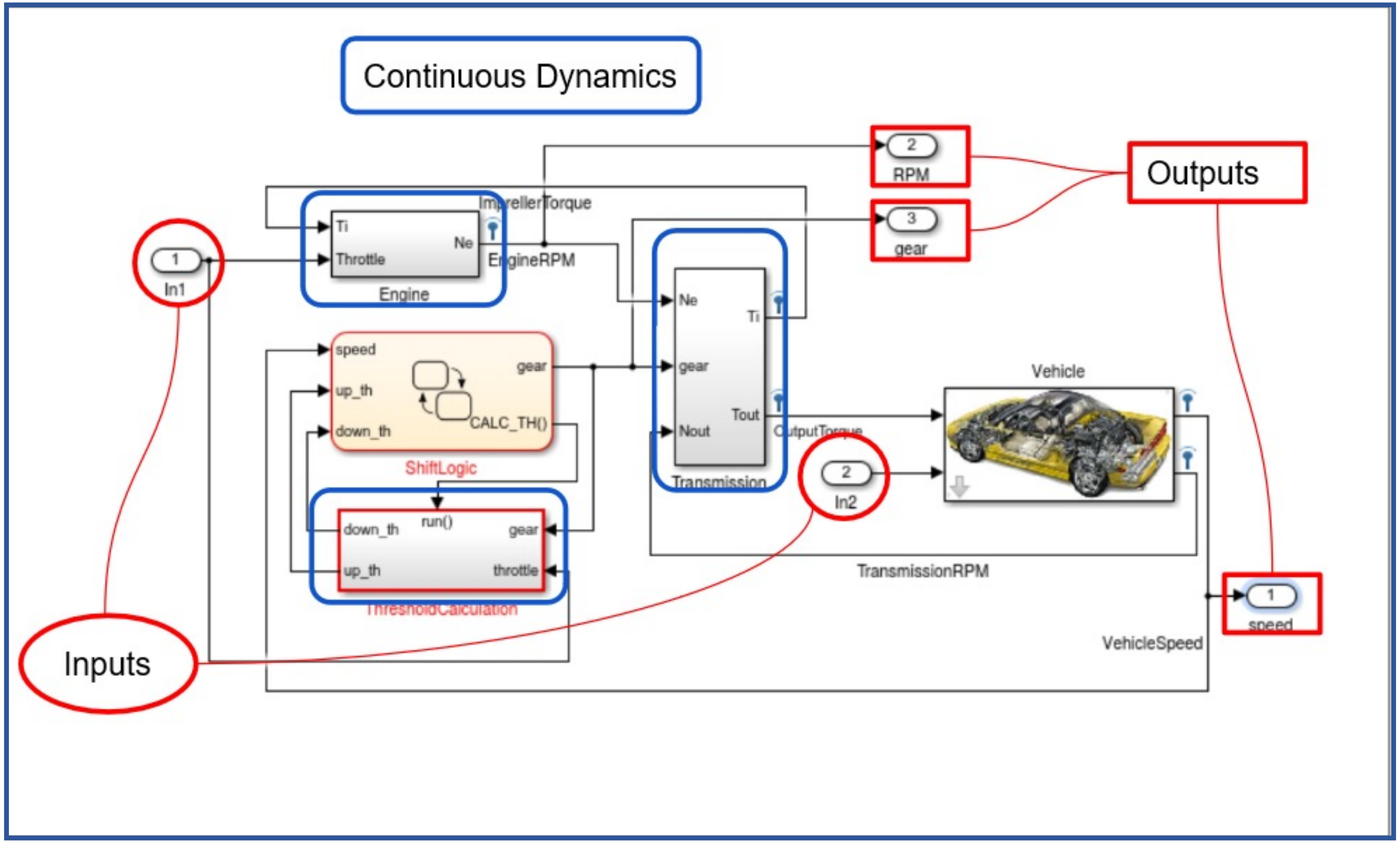
- Closed-loop Models contain:
  - Dynamics describing Physical Processes (Plant)
  - Code describing Embedded Control, Sensing, Actuation
  - Models of connection between plant and controller (hard-wired vs. wired network vs. wireless communication)

Example

Inputs:

Throttle

Brake



Outputs:

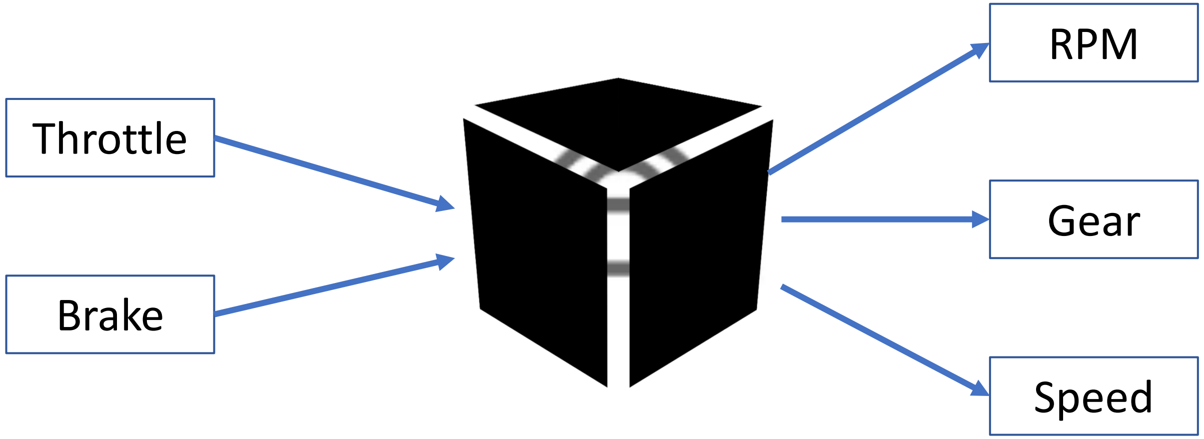
RPM

Gear

Speed

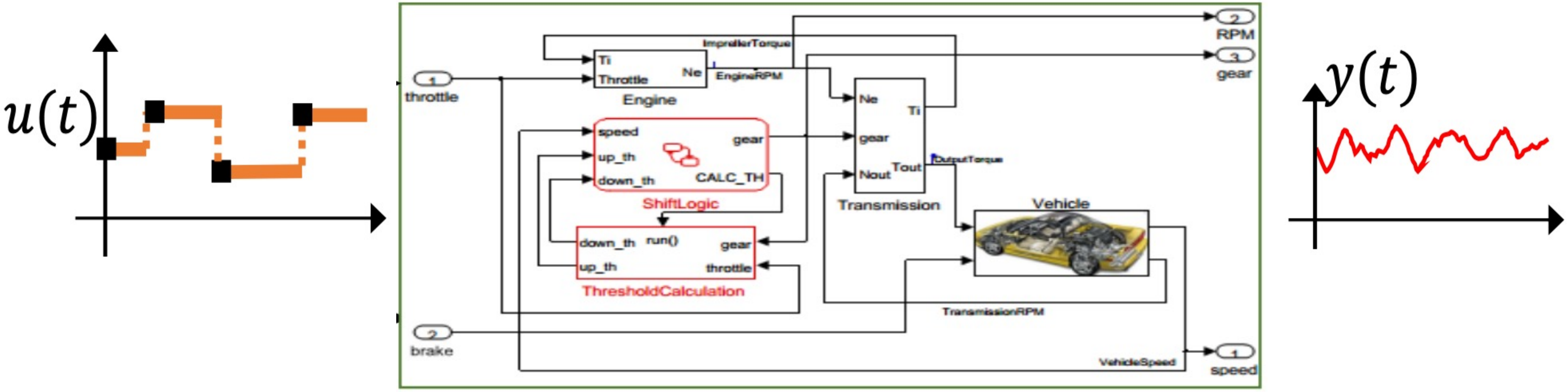
Simulink model of a Car Automatic Gear Transmission Systems

Black Box Assumption



Black Box Assumption

- For simplicity, consider the composed plant model, controller and communication to be a model M that is excited by an input signal $\mathbf{u}(t)$ and produces some output signal $\mathbf{y}(t)$



Verification vs. Testing

- For simplicity, $\mathbf{u}$ is a function from $\mathbb{T}$ to $\mathbb{R}^m$; let the set of all possible functions representing input signals be U
- Verification Problem:

  Prove the following: $\forall \mathbf{u} \in U: \big(\mathbf{y} = M(\mathbf{u})\big) \vDash \varphi(\mathbf{u}, \mathbf{y})$
- Falsification/Testing Problem:

  Find a witness to the query: $\exists \mathbf{u} \in U : \big(\mathbf{y} = M(\mathbf{u})\big) \nvDash \varphi(\mathbf{u}, \mathbf{y})$
- These formulations are quite general, as we can include the following "*model uncertainties*" as input signals: Initial states, tunable parameters in both plant and controller, time-varying parameter values, noise, etc.,

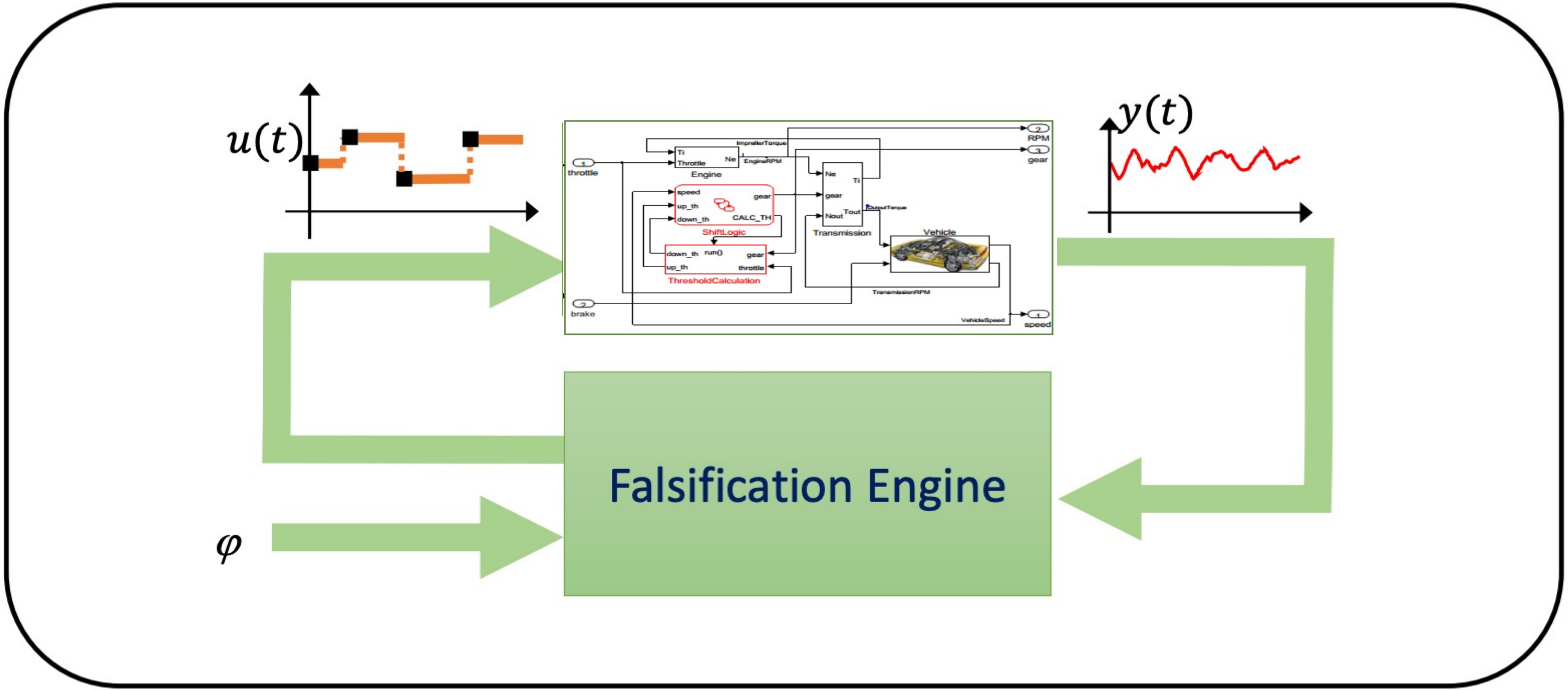
Challenges with real-world systems

- If plant model, software and communication is simple (e.g. linear models), then we can do formal analysis

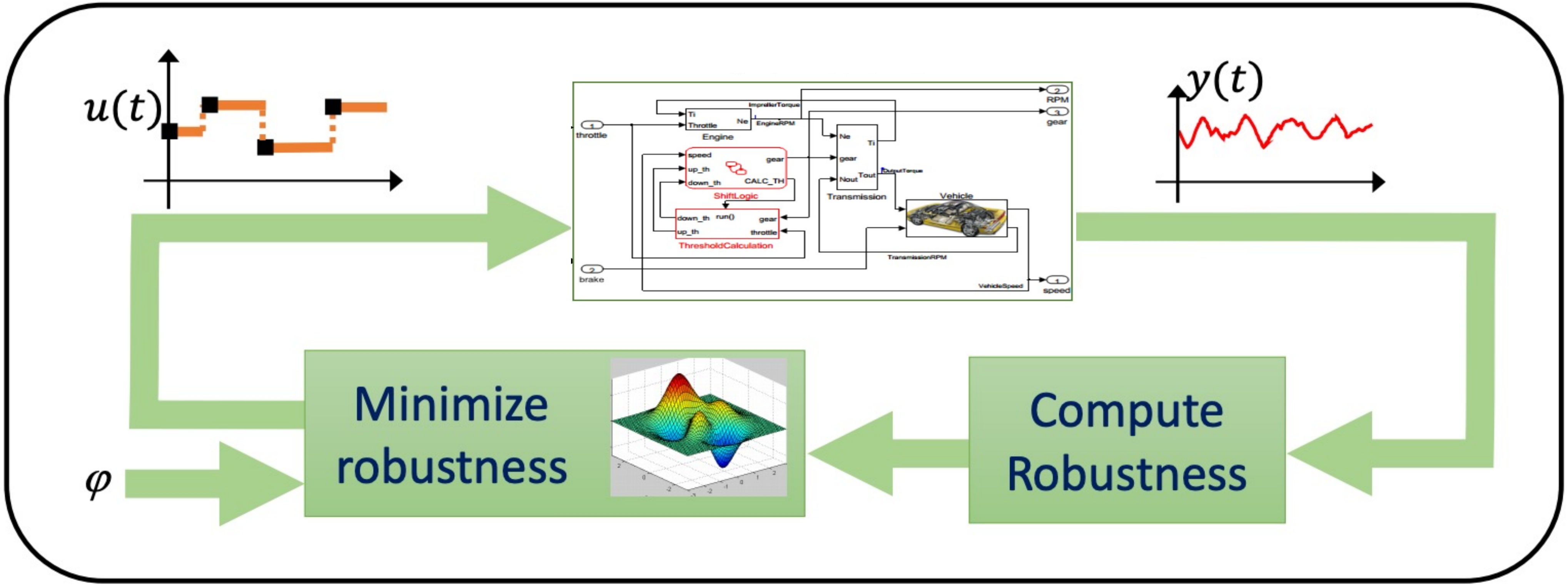
- Most real-world examples have very complex plants, controllers and communication!

- Verification problem, in the most general case is ***undecidable***
  - it is proved to be impossible to construct an algorithm that always leads to a correct yes-or-no answer to the problem

Falsification/Testing



Falsification by optimization



Use robustness as a cost function to minimize with Black-box/Global Optimizers

Falsification/Testing

- Falsification or testing attempts to find one or more $\mathbf{u}$ signals such that $\neg\varphi(\mathbf{u}, M(\mathbf{u}))$ is true.

- In verification, the set $\mathbb{T}$ (the time domain) could be unbounded, in falsification or testing, the time domain is necessarily bounded, i.e. $\mathbb{T} \subseteq [0, T]$, where T is some finite numeric constant

- In verification the co-domain of $\mathbf{u}$, could be an unbounded subset of $\mathbb{R}^m$, in falsification, we typically consider some compact subset of $\mathbb{R}^m$

- For the i^{th} input signal component, let D_i denote its compact co-domain. Then the input signal $\mathbf{u}$: $\mathbb{T}$ -> $D_1 \times \cdots \times D_m$, where $\mathbb{T} \subseteq [0, T]$
In simple words: input signals range over bounded intervals and over a bounded time horizon

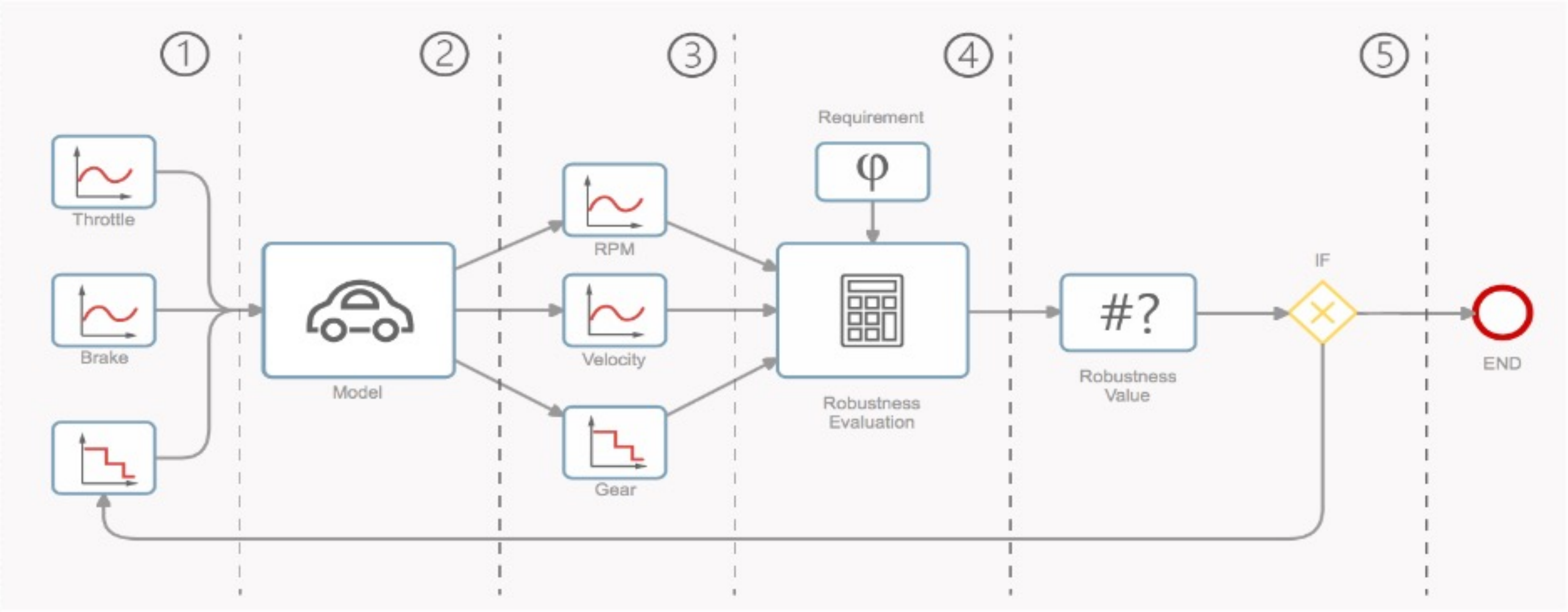
Falsification re-framed

Given:

- Set of all such input signals : U
- Input signal $\mathbf{u} : \mathbb{T} \rightarrow D_1 \times \cdots \times D_m,$ where $\mathbb{T} \subseteq [0, T]$
- Model M that maps $\mathbf{u}$ to some signal $\mathbf{y}$ with the same domain as $\mathbf{u}$, and co-domain some subset of $\mathbb{R}^n$
- Property φ that can be evaluated to true/false over given $\mathbf{u}$ and $\mathbf{y}$

Check: $\exists \mathbf{u} \in U : \left(\mathbf{y} = M(\mathbf{u})\right) \vDash \neg\varphi(\mathbf{u}, \mathbf{y})$

Falsification CPS



Goal:

Find the inputs (1) which falsify the requirements (4)

Problems:

- Falsify with a low number of simulations — Active Learning
- Functional Input Space — Adaptive Parameterization