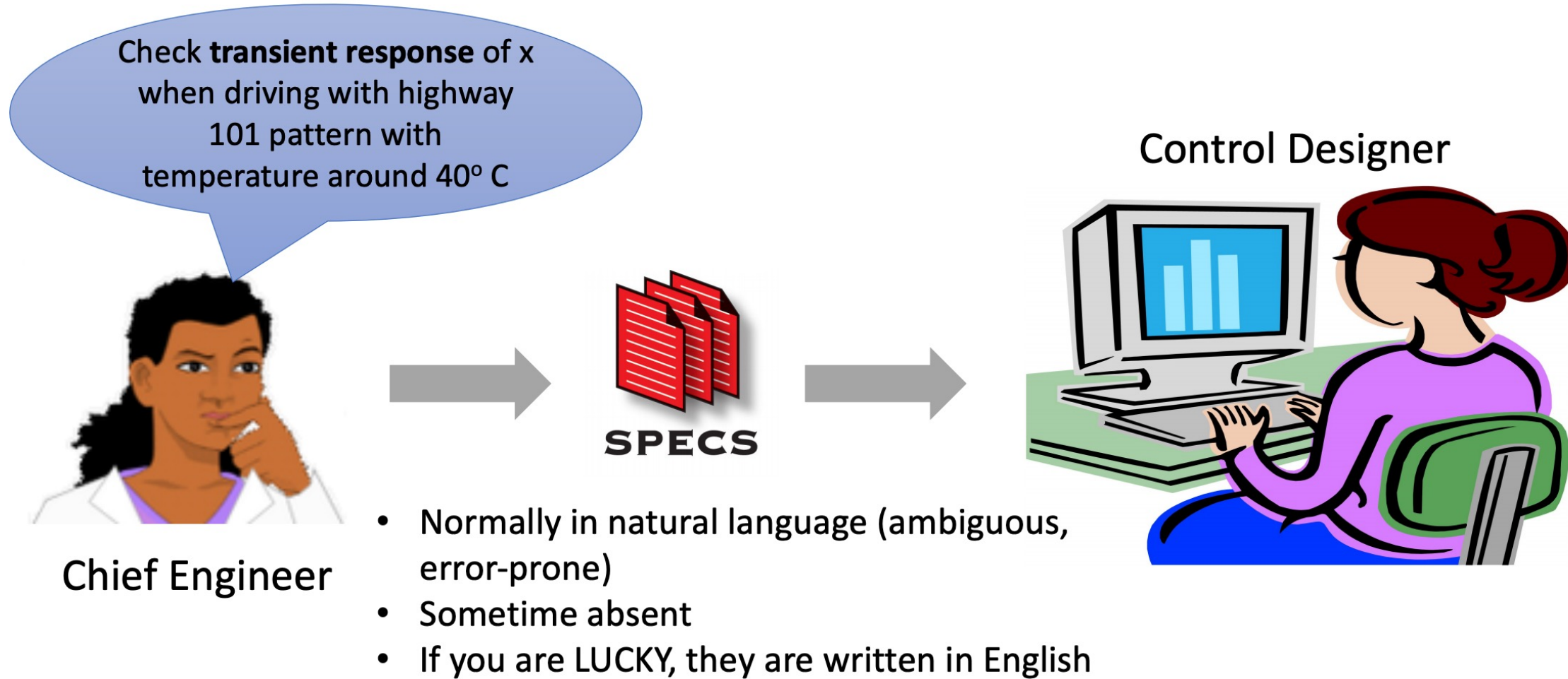# Cyber-Physical Systems

Laura Nenzi
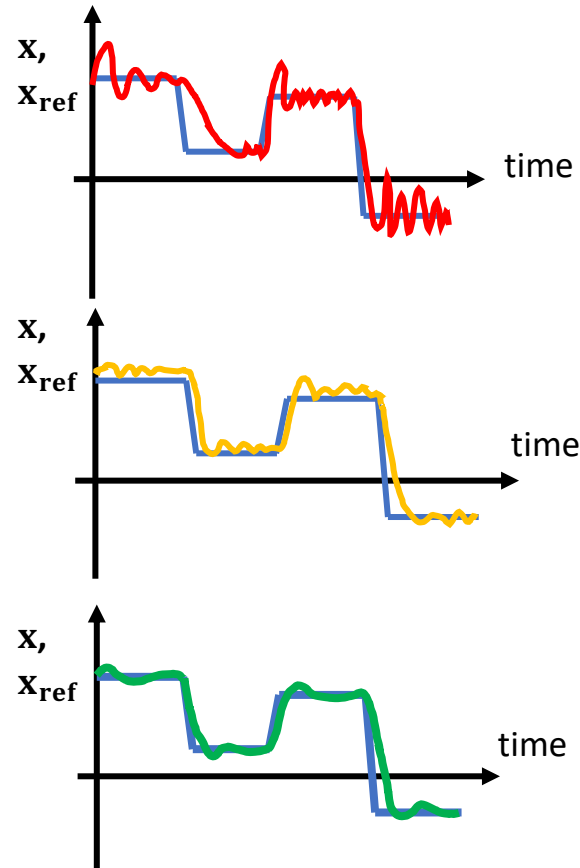
Università degli Studi di Trieste
II Semestre 2020

Lecture 14: Signal Temporal Logic and its Quantitative Semantics

[Many Slides due to J. Deshmukh, A. Donzé]

Typical day in a control designer's life

Check **transient response** of x when driving with highway 101 pattern with temperature around 40° C

Control Designer

Chief Engineer

SPECS

- Normally in natural language (ambiguous, error-prone)
- Sometime absent
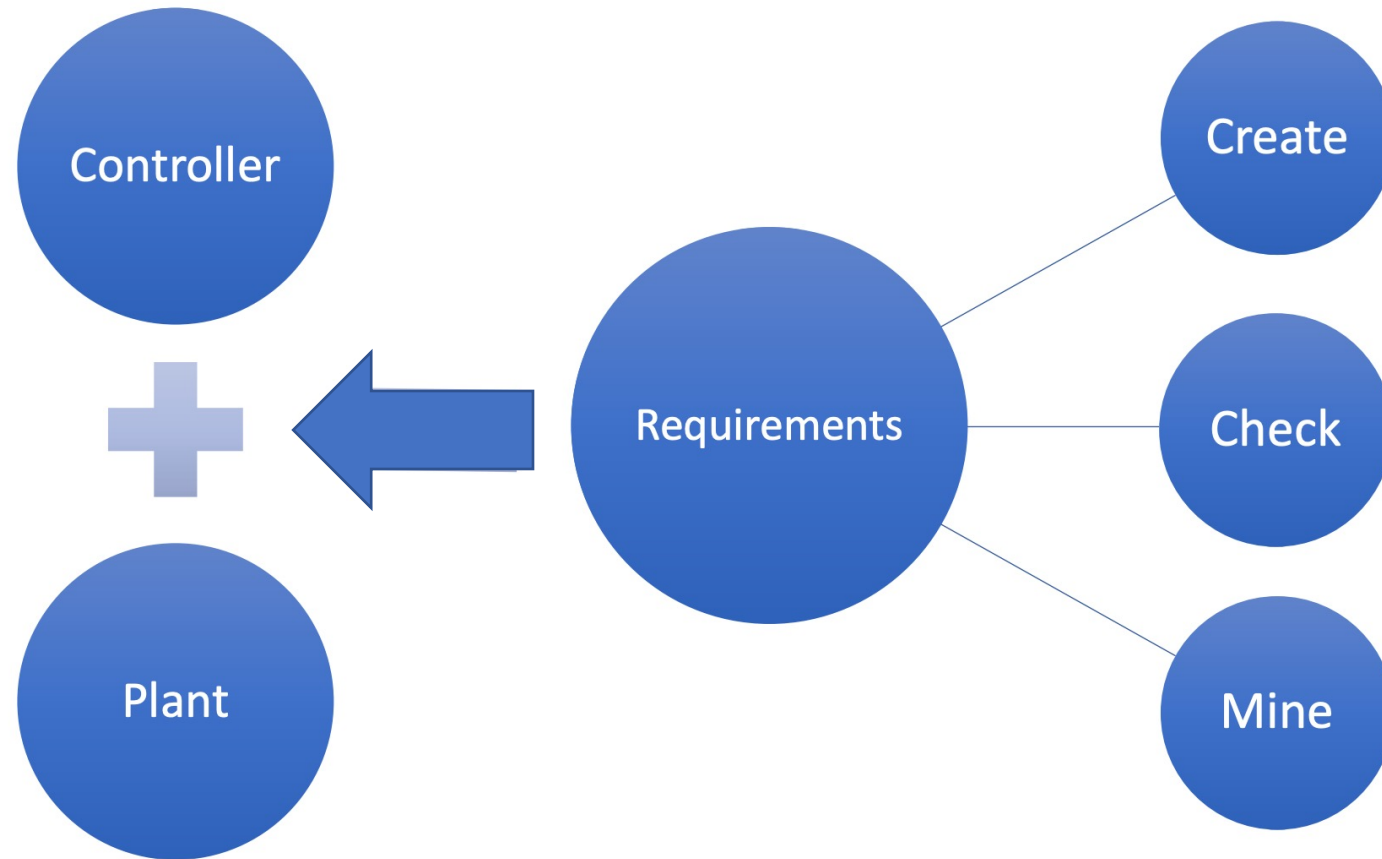- If you are LUCKY, they are written in English

Typical day in a control designer's life

Requirements Driving Design

Requirements **formally** capture what it means for a system to operate correctly in its operating environment

Linear Temporal Logic (LTL) specification

It is a logic interpreted over infinite discrete-time traces

E.g. **For the next 3 days** the highest temperature will be below 75 degree and the lowest temperature will be above 60 degree

$X (p \wedge q) \wedge X X (p \wedge q) \wedge X X X (p \wedge q)$ with p = T<75, q=T>60

Metric Interval Temporal Logic (STL)

Invented by R. Alur, T.Feder, T.A. Henzinger (1991)
It extended LTL by adding **dense time intervals**:

$$G_{[0,3]}(p \wedge q)$$

Signal Temporal Logic (STL)

Invented by D. Nickovic and O. Maler from Verimag (2004)
It extended MITL by having **signal predicates over real values as atomic formulas**:

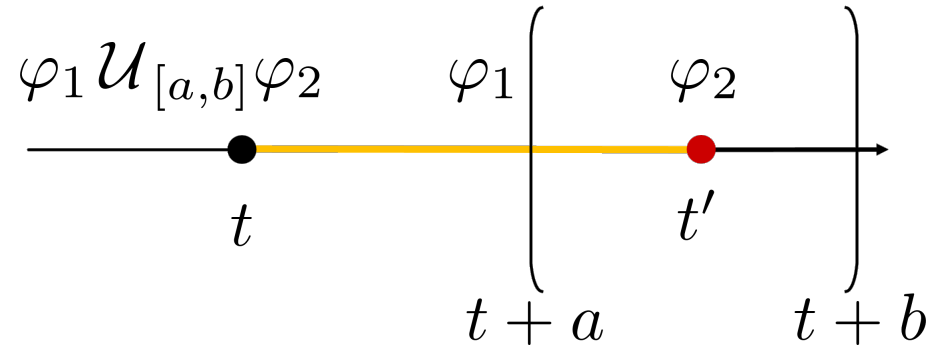$$G_{[0,3]}(T < 75 \wedge T > 60)$$
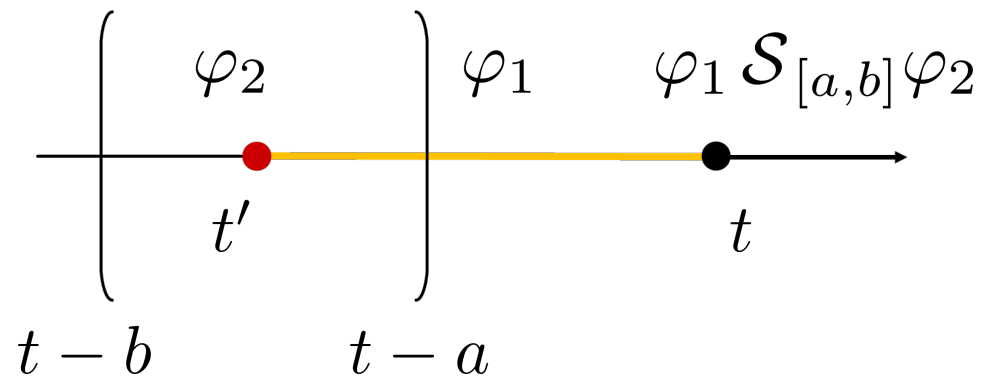
STL Syntax

Syntax of STL	
$\varphi ::= \qquad f(\mathbf{x}) \sim 0 \quad |$	$f: \mathbb{D} \to \mathbb{R}$ is a function over the signal $\mathbf{x}: \mathbb{T} \to \mathbb{D}$, $\sim \in \{\leq, <, >, \geq, =, \neq\}$
$\neg \varphi \quad |$	Negation
$\varphi_1 \wedge \varphi_2 \quad |$	Conjunction
$\mathbf{F}_{[a,b]} \varphi \quad |$	At some **F**uture step in the interval $[a, b]$
$\mathbf{G}_{[a,b]} \varphi \quad |$	**G**lobally in all times in the interval $[a, b]$
$\varphi_1 \, \mathbf{U}_{[a,b]} \, \varphi_2 \quad |$	In all steps **U**ntil in interval $[a, b]$
$\varphi_1 \, \mathbf{S}_{[a,b]} \, \varphi_2 \quad |$	In all steps **S**ince in interval $[a, b]$

Since and Until Operators

- Until

- Since

Can we express our engineer's requirements?

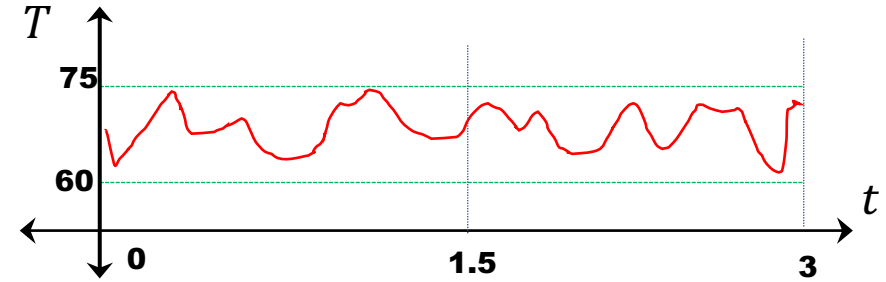

$$\varphi \equiv \text{Alw}_{[0,10]}\left(\left|x - x_{ref}\right| < 0.05\right)$$

Expressing specifications in STL
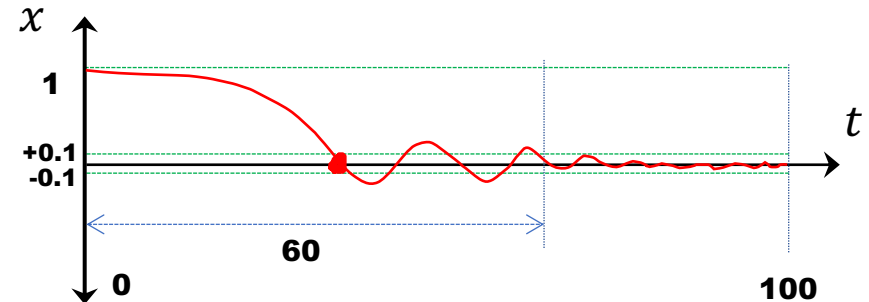
Always$_{[0,3]}$ $(60 < T < 75)$

Always between time 0 and 3
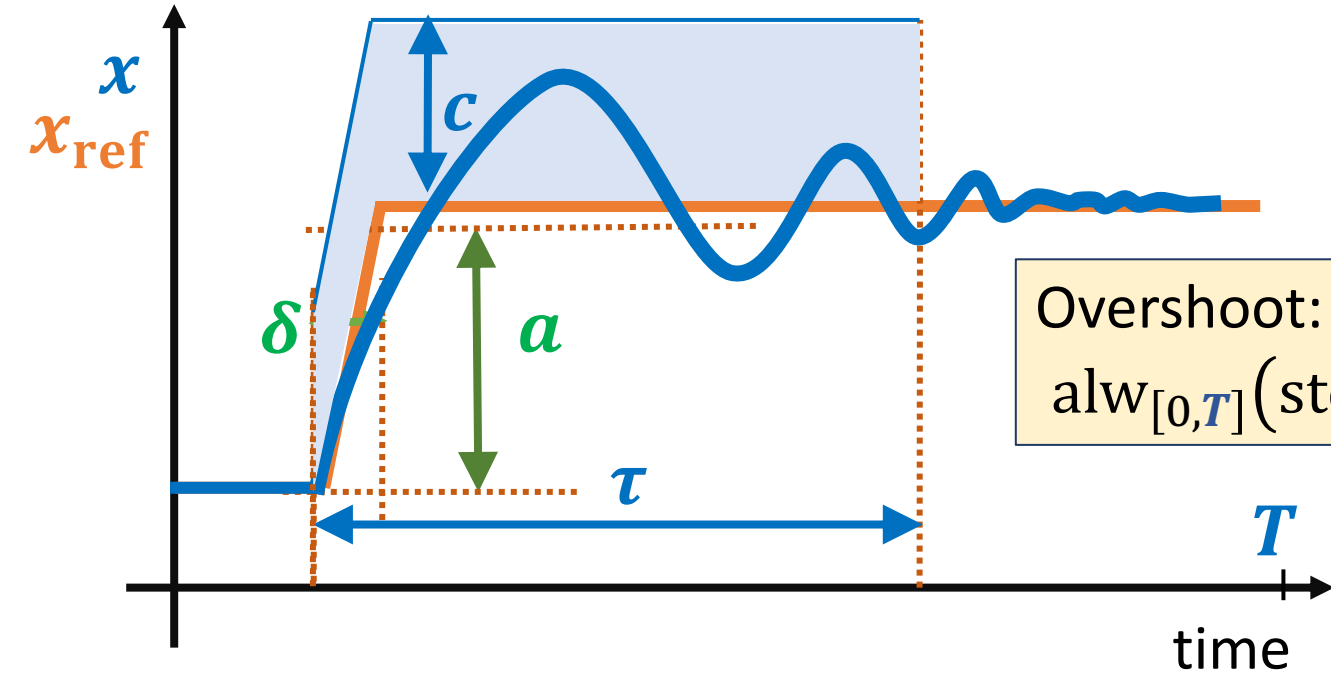

Eventually$_{[0,60]}$(**Always** $(|x| < 0.1)$)

Eventually at **some time** t between time 0 and 60

From that time t, always till the end of the signal trace
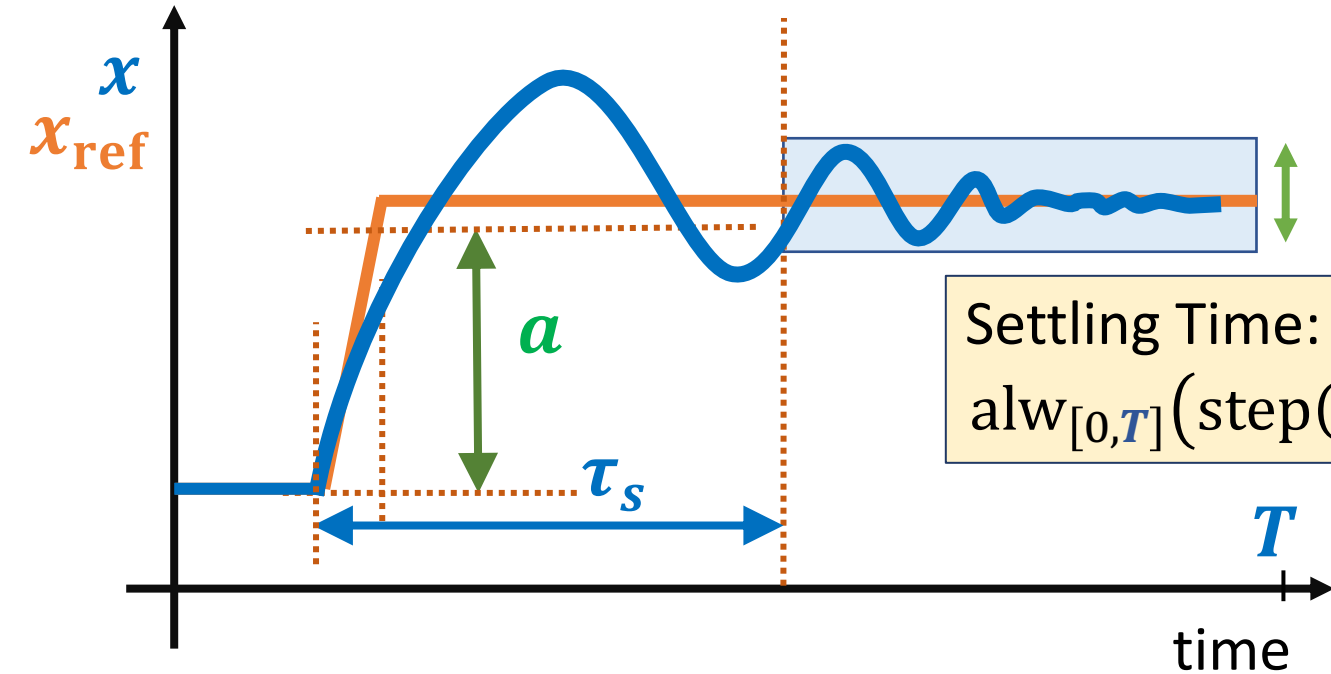
Example STL formulas: Overshoot

Step:
$$\text{step}(y, t) := y(t + \tau) - y(t) > a$$

Overshoot:
$$\text{alw}_{[0,T]}\big(\text{step}(x_{\text{ref}}, t) \Rightarrow \text{alw}_{[0,\tau]}(x(t) - x_{\text{ref}}(t) < c)\big)$$

Example STL formulas: Settling Time

Step:
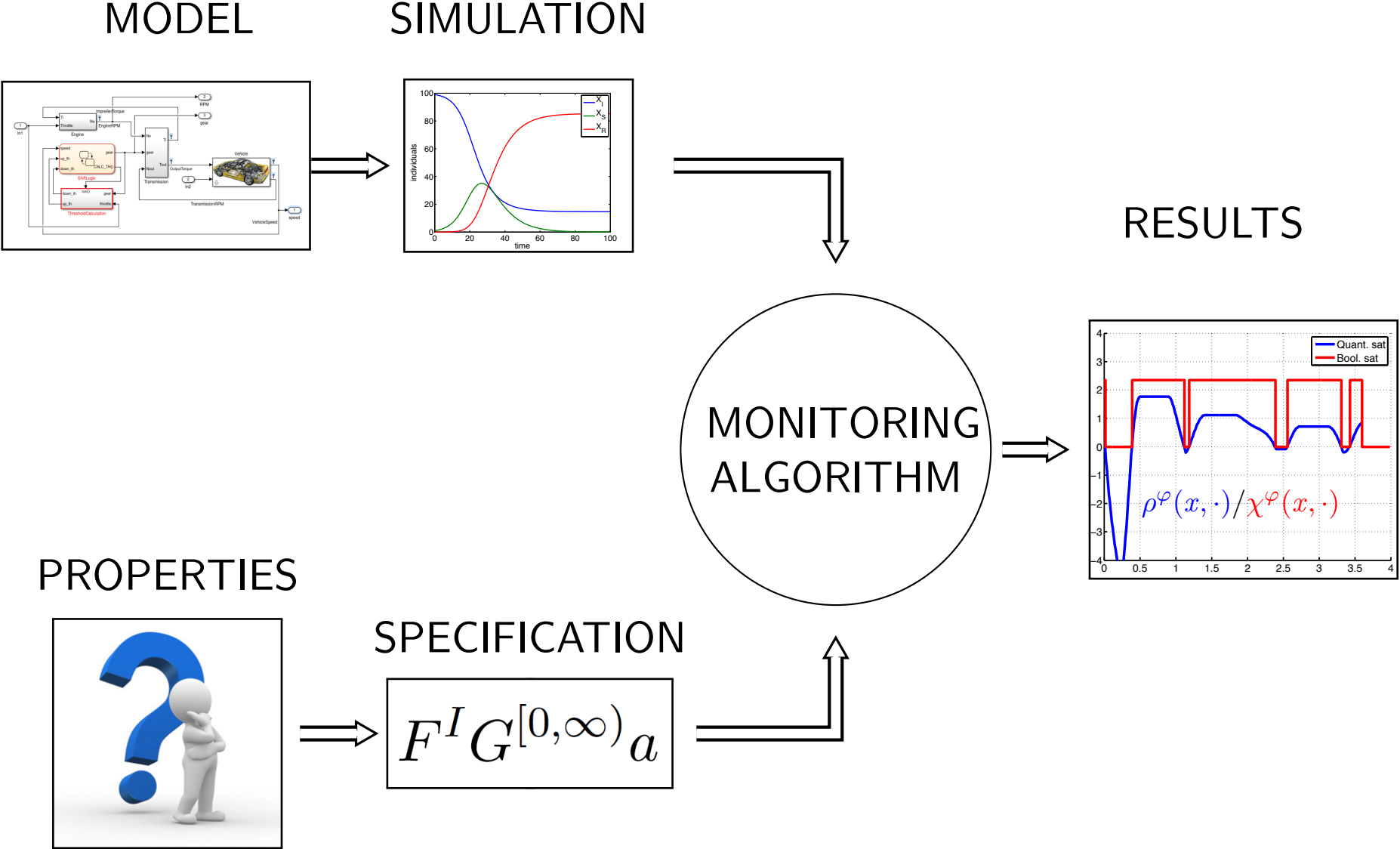$$\text{step}(y, t) := y(t + \delta) - y(t) > a$$

Settling Time:
$$\text{alw}_{[0,T]}\big(\text{step}(x_{\text{ref}}, t) \Rightarrow \text{alw}_{[\tau_s, \infty]}(|x(t) - x_{\text{ref}}(t)| < \epsilon)\big)$$

Specification-based Monitoring

MODEL   SIMULATION

RESULTS

$$\rho^\varphi(x,\cdot)/\chi^\varphi(x,\cdot)$$

MONITORING
ALGORITHM

PROPERTIES

SPECIFICATION

$$F^I G^{[0,\infty)} a$$

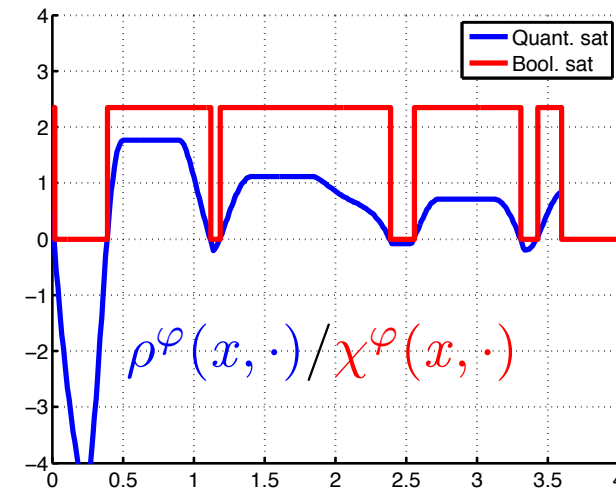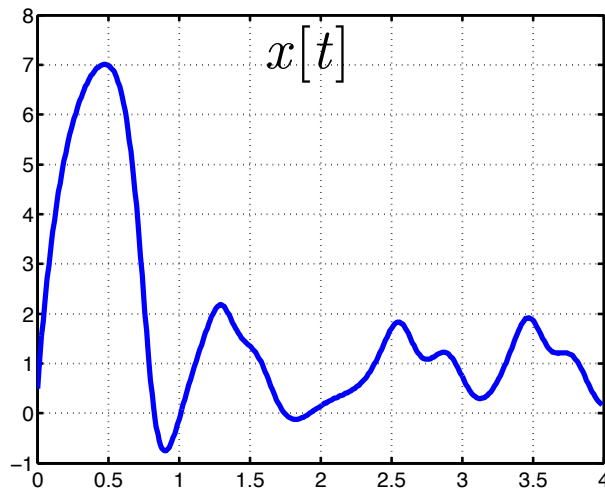# Specification-based Monitoring

Boolean Signal

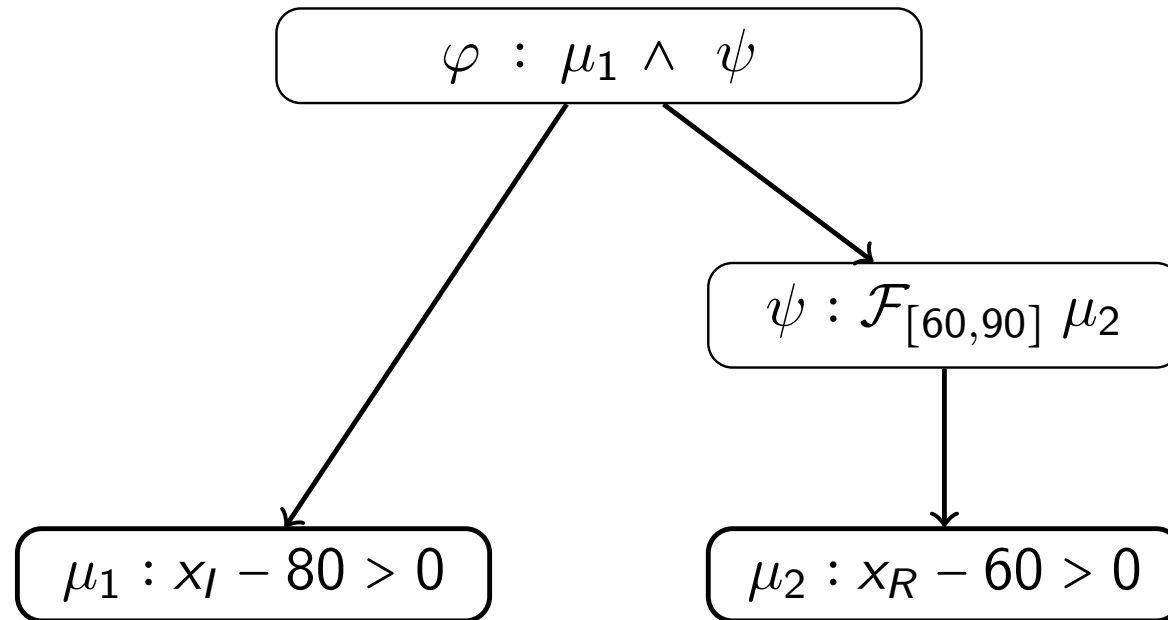$$s_\varphi : [0, T] :\to \{0, 1\} \text{ s.t. } s_\varphi(t) = 1 \Leftrightarrow (\vec{x}, t) \models \varphi$$

Quantitative Signal

$$\rho_\varphi : [0, T] :\to \mathbb{R} \cup \{\pm\infty\} \text{ s.t. } \rho_\varphi(t) = \rho(\varphi, \vec{x}, t)$$

Monitoring STL

$$\varphi : (x_I > 80) \wedge \mathcal{F}_{[60,90]} (x_R > 60)$$

Monitoring STL

$s_\varphi(0), \rho_\varphi(0)$

Boolean satisfaction
Quantitative satisfaction

$\varphi : \mu_1 \wedge \psi$
$s_\varphi(t), \rho_\varphi(t)$

$\psi : \mathcal{F}_{[60,90]} \mu_2$
$s_\psi(t), \rho_\psi(t)$

$\mu_1 : x_I - 80 > 0$
$s_{\mu_1}(t), \rho_{\mu_1}(t)$

$\mu_2 : x_R - 60 > 0$
$s_{\mu_2}(t), \rho_{\mu_2}(t)$

Boolean signals
Quantitative signals

$x_I(t) - 80$

$x_R(t) - 60$

Secondary signals

$x_I(t), x_S(t), x_R(t)$

$x_I(t), x_S(t), x_R(t)$

Primary signals

Recursive Boolean Semantics of STL

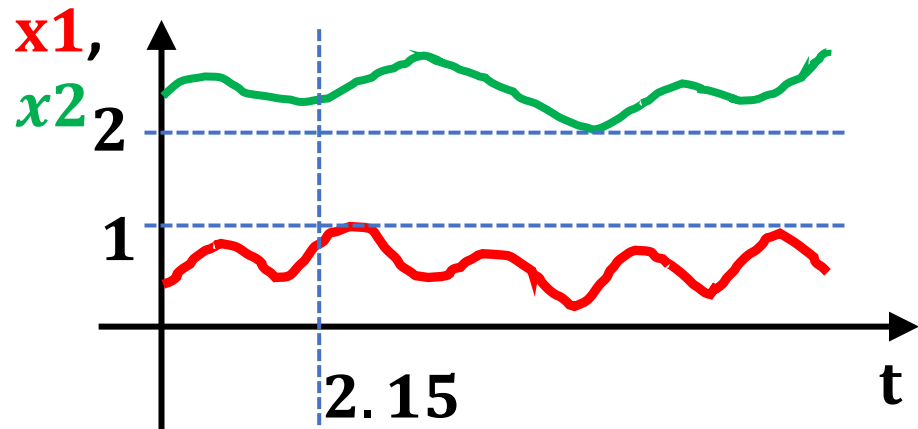| φ	$s(\varphi, \mathbf{x}, t)$
$f(\mathbf{x}) \sim 0$	$f(\mathbf{x}(t)) \sim 0 , \qquad \sim \in \{\leq, <, >, \geq, =, \neq\}$
$\neg\varphi$	$\neg s(\varphi, \mathbf{x}, t)$
$\varphi_1 \wedge \varphi_2$	$s(\varphi_1, \mathbf{x}, t) \wedge s(\varphi_2, \mathbf{x}, t)$
$\mathbf{F}_{[a,b]}\varphi$	$\exists \tau \in [t+a, t+b] \; s(\varphi, \mathbf{x}, \tau)$
$\mathbf{G}_{[a,b]}\varphi$	$\forall \tau \in [t+a, t+b] \; s(\varphi, \mathbf{x}, \tau)$
$\varphi \, \mathbf{U}_{[a,b]} \, \psi$	$\exists \tau \in [t+a, t+b] \left(s(\psi, \mathbf{x}, \tau) \wedge \forall \tau' \in [t, \tau) \; s(\varphi, x, \tau') \right)$
$\varphi \, \mathbf{S}_{[a,b]} \, \psi$	$\exists \tau \in [t-a, t-b] \left(s(\psi, \mathbf{x}, \tau) \wedge \forall \tau' \in (\tau, t] \; s(\varphi, x, \tau') \right)$

$$s(\varphi, \mathbf{x}) = s(\varphi, \mathbf{x}, 0)$$

STL semantics

▶ Semantics of STL specified recursively over a signal $\mathbf{x}: \mathbb{T} \to \mathbb{D}$ at each time,

For each STL formula φ, here's how we define it's semantics:

▶ If φ is the signal predicate $\mu = f(\mathbf{x}) > 0$, then
$s(\varphi, \mathbf{x}, t) = true$ iff $f(\mathbf{x}(t)) > 0$
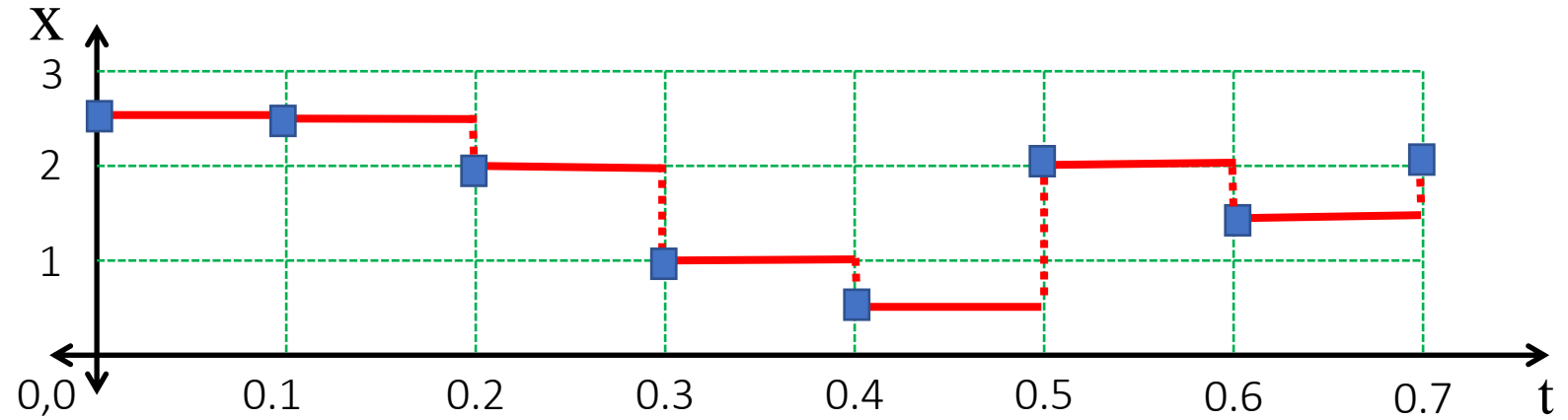

$$\mathbf{x} = (x1, x2)$$
$$f = x2 - x1 - 1$$
$$s(f(\mathbf{x}) > 0, \mathbf{x}, 2.15)?$$

Recursive Boolean Semantics of STL

$$\varphi \equiv F_{[0,0.2]}(x(t) \geq 1.5)$$

$x(t) - 1.5 > 0$	T	T	T	F	F	T	T	T
$F_{[0,0.2]} \mu$	T	T	T	T	T	T		
$G_{[0,0.7]} F_{[0,0.2]} \mu$	T							

STL has quantitative semantics

▶ Quantitative semantics defined using the notion of a *Robust Satisfaction Value*, or *Robustness Value*

▶ Robustness ρ is a function that maps

  ▶ a given trace $\mathbf{x}(t)$,

  ▶ a formula φ,

  ▶ and a time t

  to some real value

▶ We can interpret robustness as "distance to violation" of a given formula
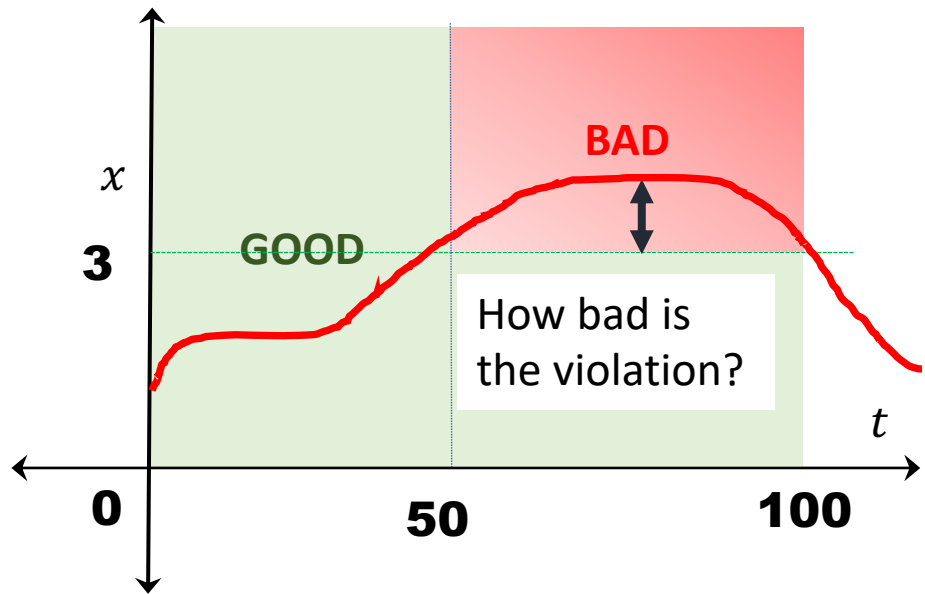
Recursive Quantitative Semantics

φ	$\rho(\varphi, \mathbf{x}, t)$
$f(\mathbf{x}) > 0 \, , f(\mathbf{x}) \geq 0$	$f(\mathbf{x}(t))$
$\neg\varphi$	$-\rho(\varphi, \mathbf{x}, t)$
$\varphi_1 \wedge \varphi_2$	$\min\big(\rho(\varphi_1, \mathbf{x}, t) \wedge \rho(\varphi_2, \mathbf{x}, t)\big)$
$\mathbf{F}_{[a,b]}\varphi$	$\sup\limits_{\tau \in [t+a, t+b]} \rho(\varphi, \mathbf{x}, \tau)$
$\mathbf{G}_{[a,b]}\varphi$	$\inf\limits_{\tau \in [t+a, t+b]} \rho(\varphi, \mathbf{x}, \tau)$
$\varphi \, \mathbf{U}_{[a,b]} \, \psi$	$\sup\limits_{\tau \in [t+a, t+b]} \Big(\min \big(\rho(\psi, \mathbf{x}, \tau), \inf\limits_{\tau' \in [t,\tau)} \rho(\varphi, \mathbf{x}, t) \big) \Big)$

$\rho(\varphi, \mathbf{x}) = \rho(\varphi, \mathbf{x}, 0)$

Distance to violation/satisfaction

GOOD

BAD

How bad is the violation?

3

GOOD

BAD

How far is bad?

3

$$\mathbf{G}_{[50,100]}(x(t) < 3)$$

Property of Robust Satisfaction Signal

▶ Sign indicates satisfaction status (soundness):

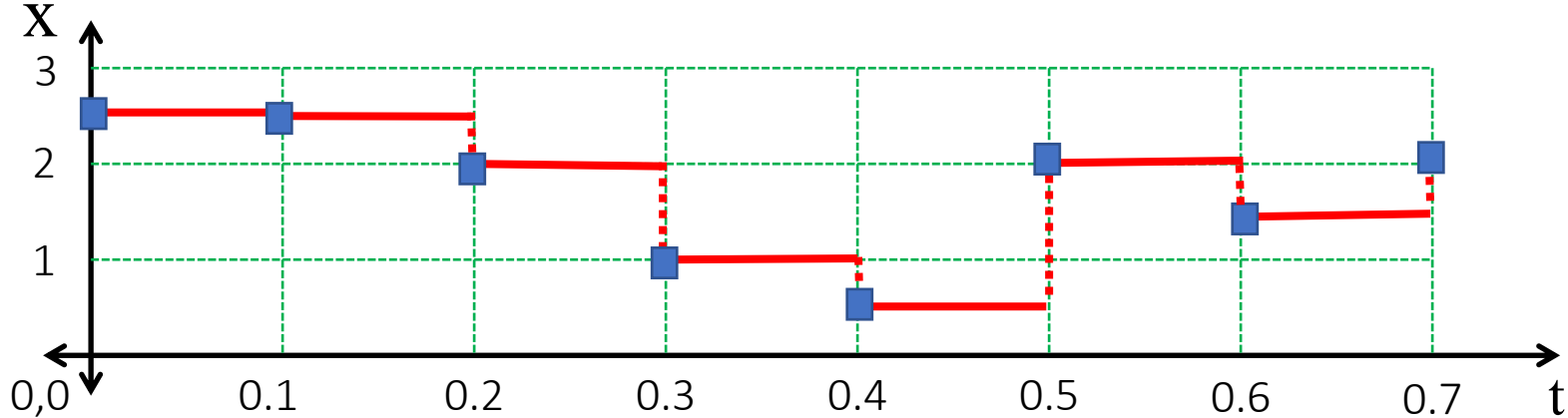$$\rho(\varphi, \mathbf{x}, t) > 0 \quad \Rightarrow \quad s(\varphi, \mathbf{x}, t) = 1$$
$$\rho(\varphi, \mathbf{x}, t) < 0 \quad \Rightarrow \quad s(\varphi, \mathbf{x}, t) = 0$$

▶ Absolute value indicates tolerance (correctness)

$$\left|\left|\mathbf{x} - \mathbf{x}'\right|\right|_\infty < \rho(\varphi, \mathbf{x}, t) \quad \Rightarrow \quad s(\varphi, \mathbf{x}, t) = s(\varphi, \mathbf{x}', t)$$

Robustness computation example

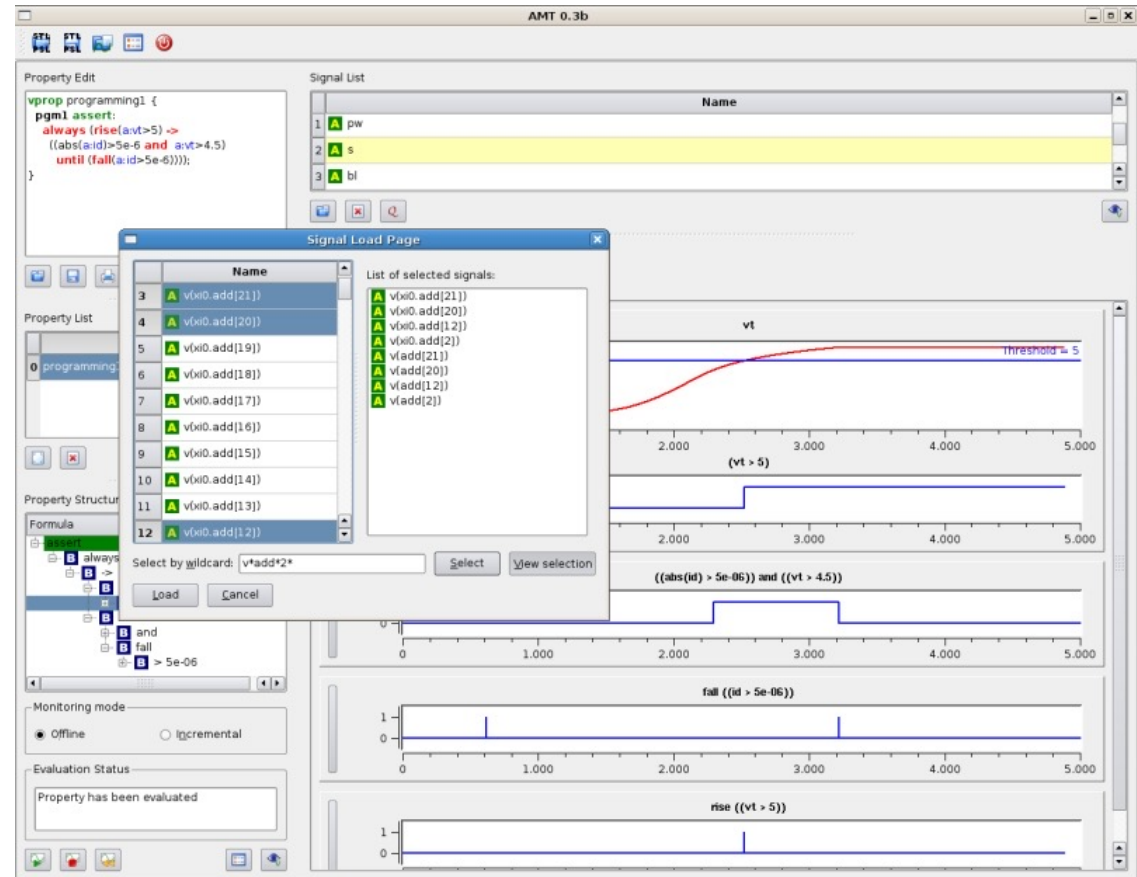$$\varphi \equiv \mathbf{G}_{[0,0.7]}\mathbf{F}_{[0,0.2]}(x(t) > 1.5)$$

$x(t) - 1.5$	1	1	0.5	-0.5	-1	0.5	0	0.5
$\mathbf{F}_{[0,0.2]}\,\mu$	1	1	0.5	0.5	0.5	0.5		
$\mathbf{G}_{[0,0.7]}\mathbf{F}_{[0,0.2]}\,\mu$	0.5							

$\mathrm{f}(x(t)) > 0$ at time t	$f(x(t))$
$\mathrm{F}_{[a,b]}\,\varphi$ at time t	Maximum over robustness of φ for $t' \in t \oplus [a,b]$
$\mathrm{G}_{[a,b]}\varphi$ at time t	Minimum over robustness of φ for $t' \in t \oplus [a,b]$

Analog Monitoring Tool (AMT)
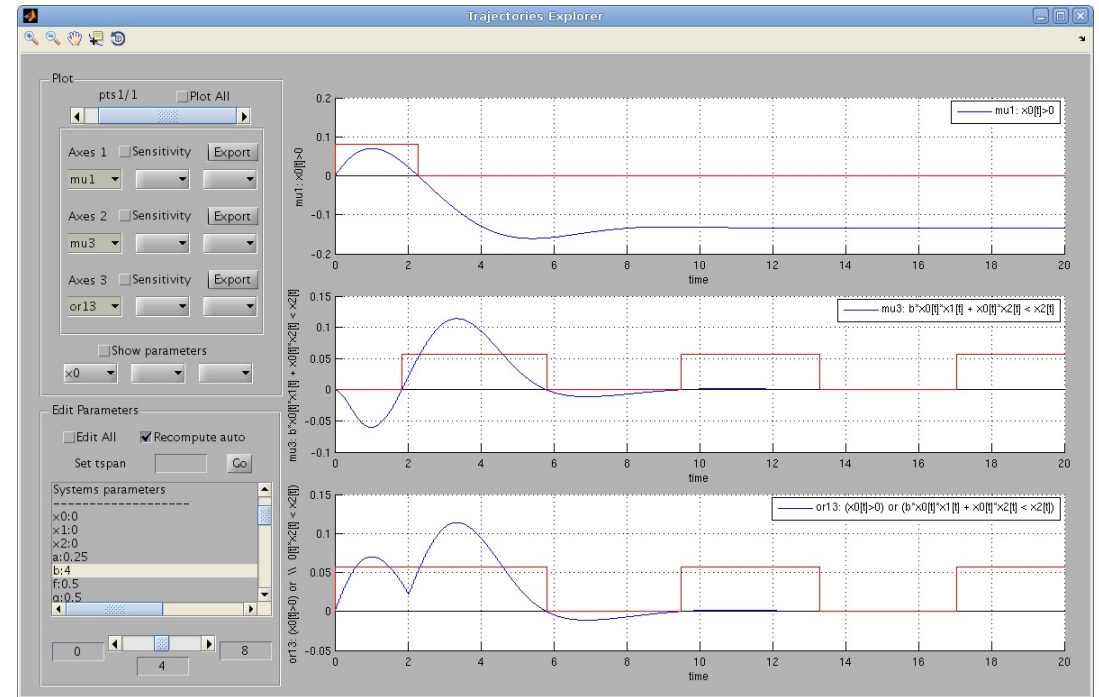
http://www-verimag.imag.fr/DIST-TOOLS/TEMPO/AMT/content.html

- Java toolbox
- STL with qualitative semantics
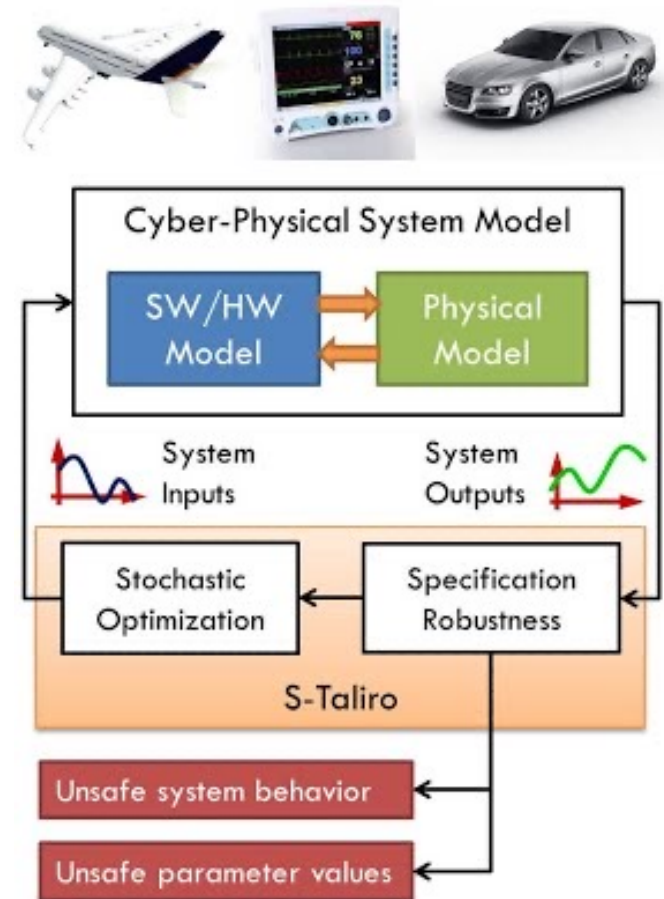 - Correctness
- Offline monitoring

Breach

- MATLAB toolbox for
  - Simulation
  - Monitoring of temporal properties
  - Reachability

- STL with qualitative and quantitative semantics
  - Correctness
  - Robustness

- Offline and Online monitoring

S-TaLiRo

https://sites.google.com/a/asu.edu/s-taliro/s-taliro

- MATLAB toolbox for searching trajectories with minimal robustness
    - Randomized testing
        - Monte-Carlo simulation
        - Ant-colony optimization
        - Simulated annealing
        - Genetic algorithms
        - Cross enthopy

- MTL with quantitative semantics
    - Robustness

- Offline and Online monitoring

Moonlight

▶Java-toolbox + Matlab (and Python) interface for:

▶ Monitoring of temporal properties

▶STL + spatial operator with qualitative and quantitative semantics

▶Correctness

▶Robustness

▶Offline monitoring

Bibliography

1. G. Fainekos, and G. J. Pappas. *Robustness of temporal logic specifications for continuous-time signals*. Theoretical Computer Science 2009.

2. Maler, Oded, and Dejan Nickovic. "Monitoring temporal properties of continuous signals." Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems. Springer, Berlin, Heidelberg, 2004. 152-166.

3. Donzé, Alexandre, and Oded Maler. "Robust satisfaction of temporal logic over real-valued signals." International Conference on Formal Modeling and Analysis of Timed Systems. Springer, Berlin, Heidelberg, 2010.