

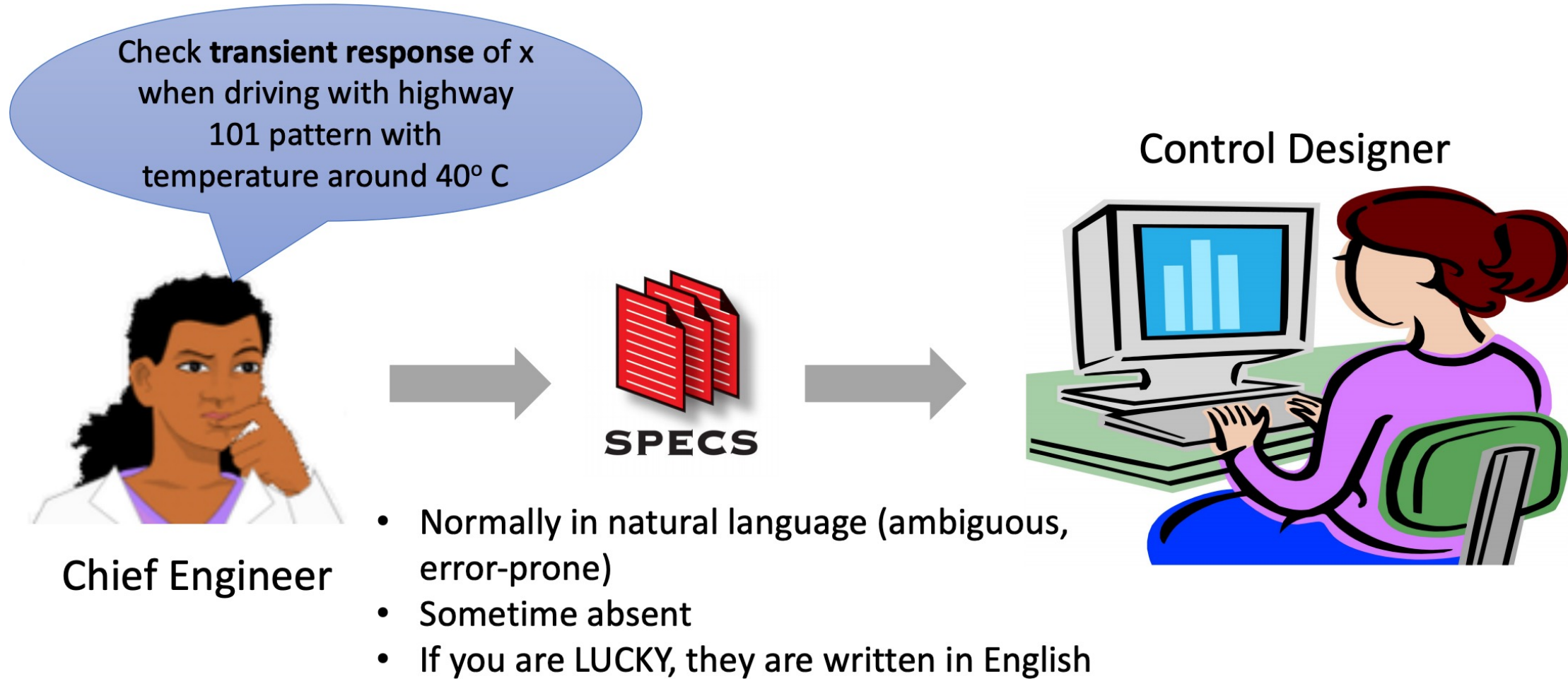
Cyber-Physical Systems

Laura Nenzi

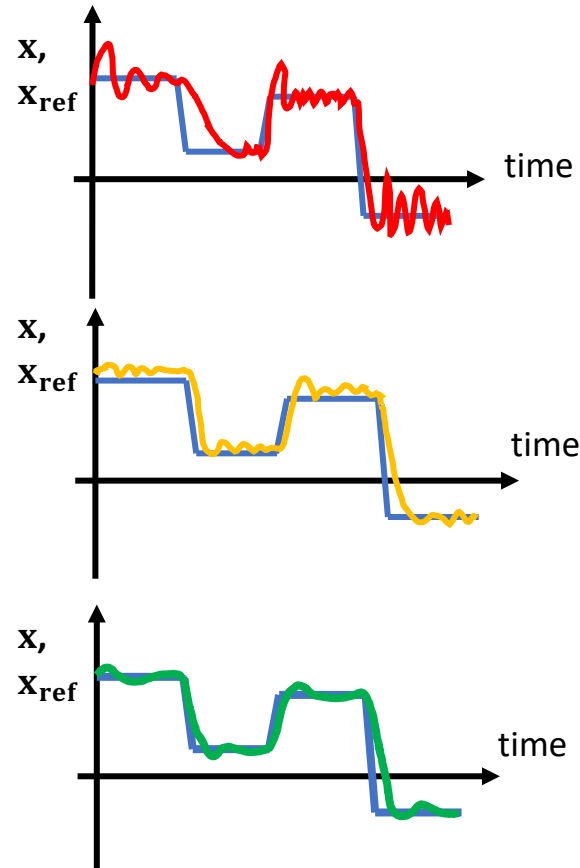
Università degli Studi di Trieste
II Semestre 2022

Lecture 12: Signal Temporal Logic

Typical day in a control designer's life



Typical day in a control designer's life



Uh Oh!

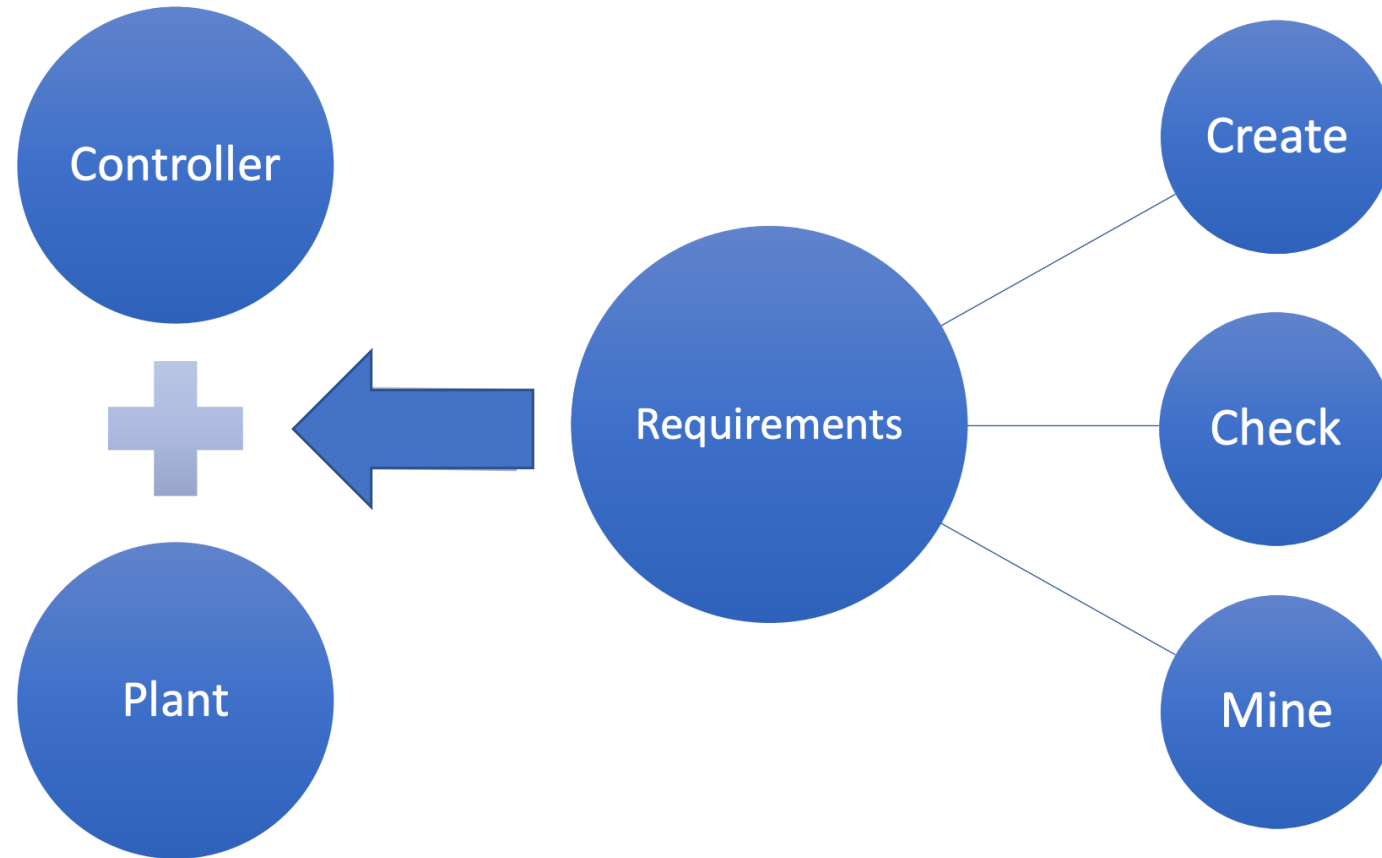
... should be okay

Looks good



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**:

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

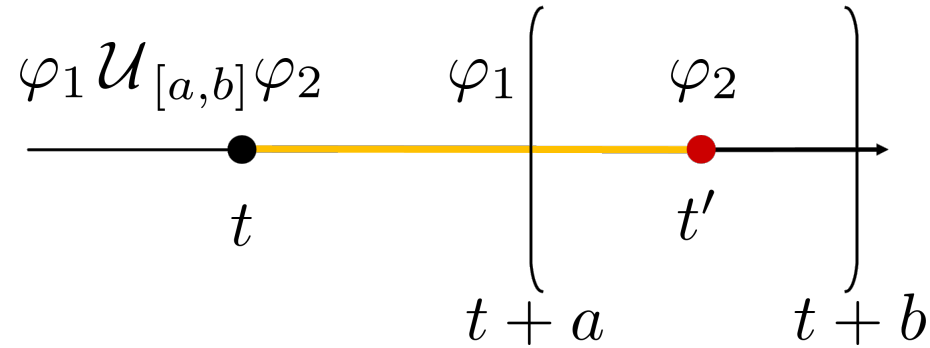
STL Syntax

Syntax of STL

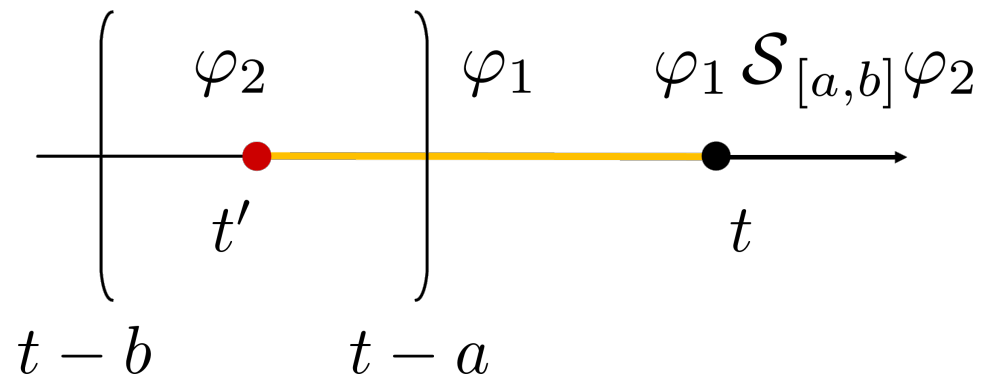
$\varphi ::=$	$f(\mathbf{x}) \sim 0$		$f: \mathbb{D} \rightarrow \mathbb{R}$ is a function over the signal $\mathbf{x}: \mathbb{T} \rightarrow \mathbb{D}$, $\sim \in \{\leq, <, >, \geq, =, \neq\}$
	$\neg \varphi$		Negation
	$\varphi_1 \wedge \varphi_2$		Conjunction
	$\mathbf{F}_{[a,b]} \varphi$		At some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

Since and Until Operators

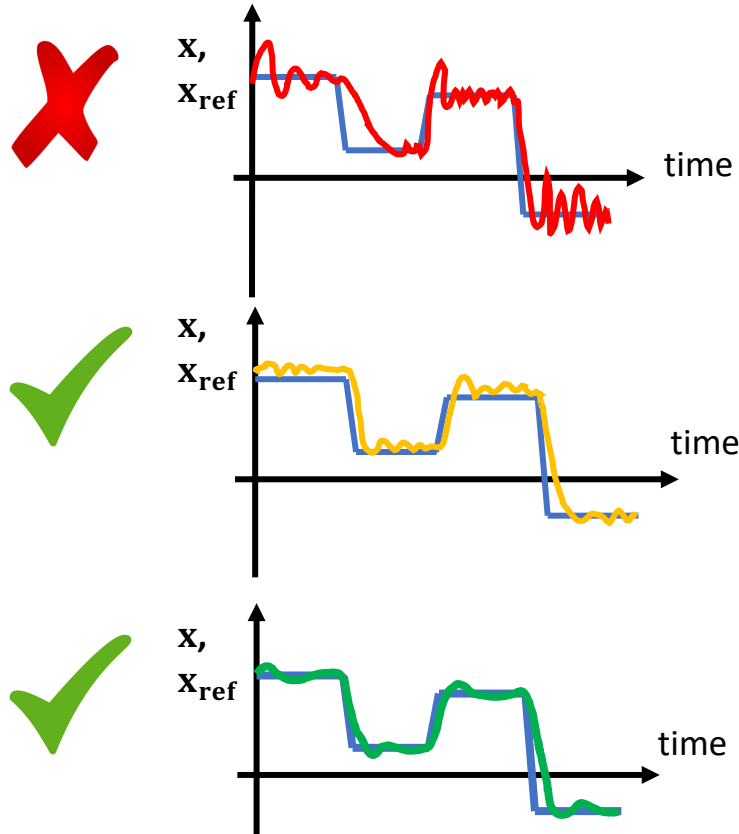
- Until



- Since



Can we express our engineer's requirements?



Uh Oh!

... should be okay

Looks good

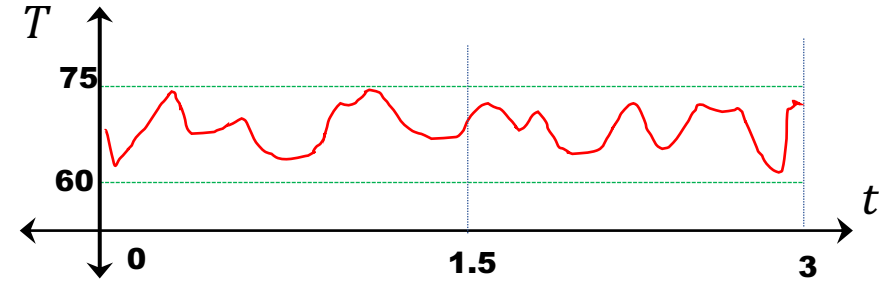


$$\varphi \equiv \text{Alw}_{[0,10]}(|x - x_{ref}| < 0.05)$$

Expressing specifications in STL

Always_[0,3] ($60 < T < 75$)

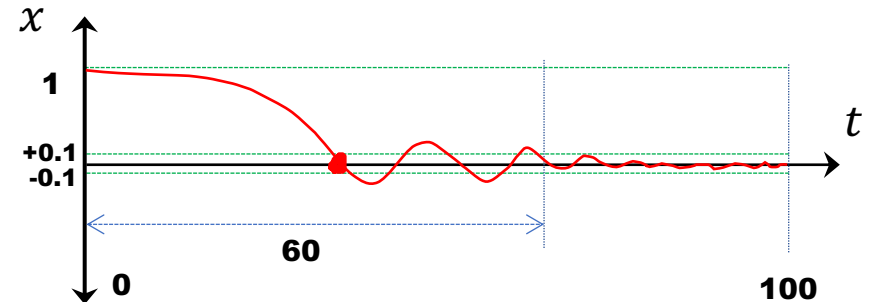
Always between time 0 and 3



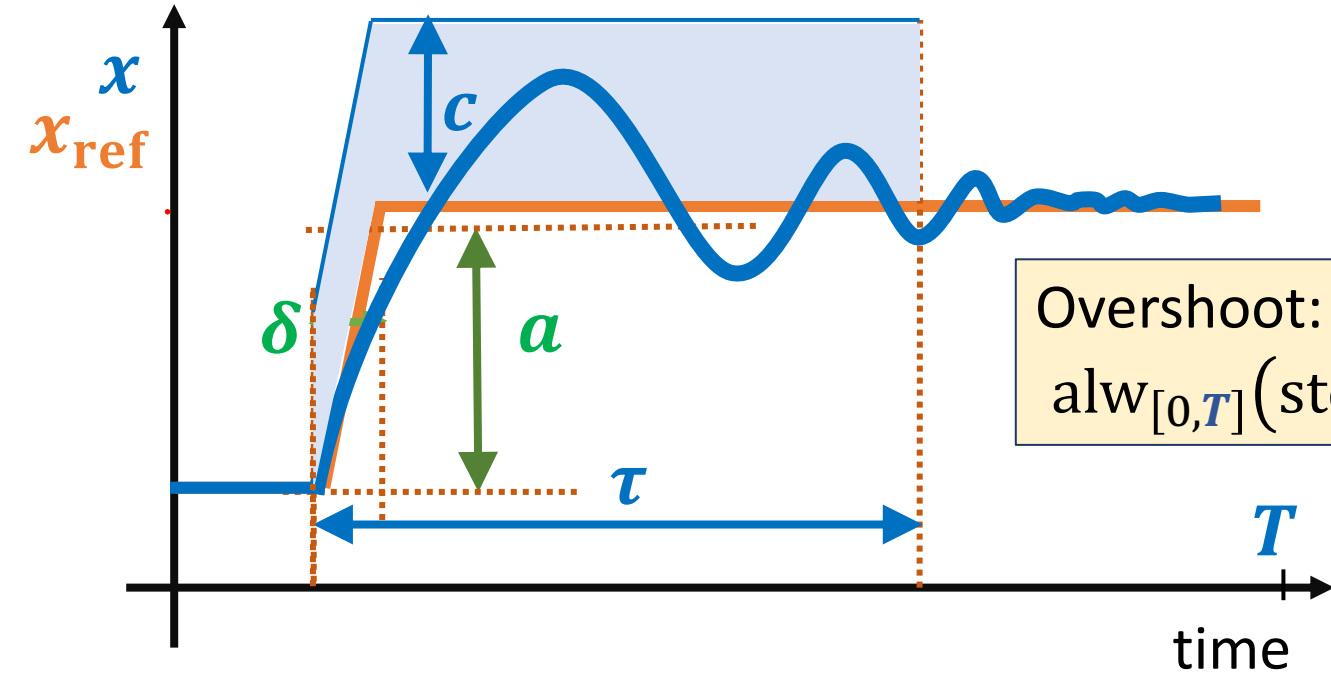
Eventually_[0,60] (**Always** ($|x| < 0.1$))

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



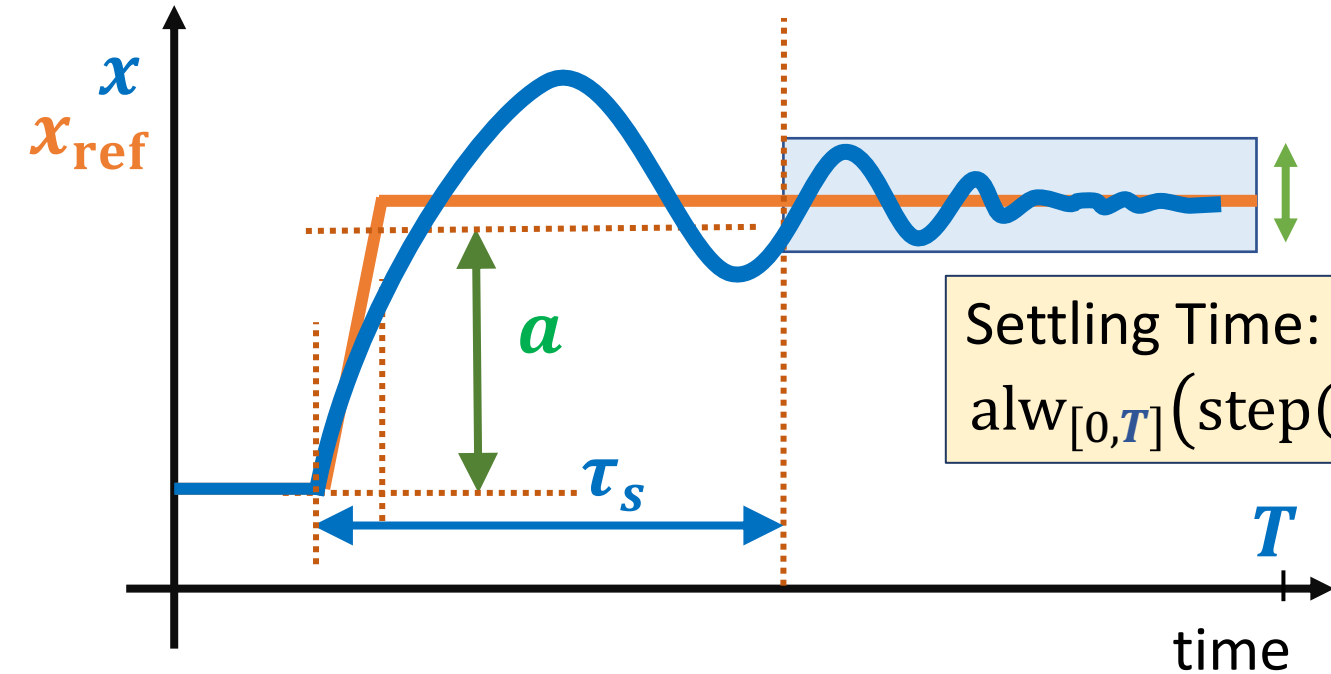
Step:

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

Overshoot:

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

Example STL formulas: Settling Time



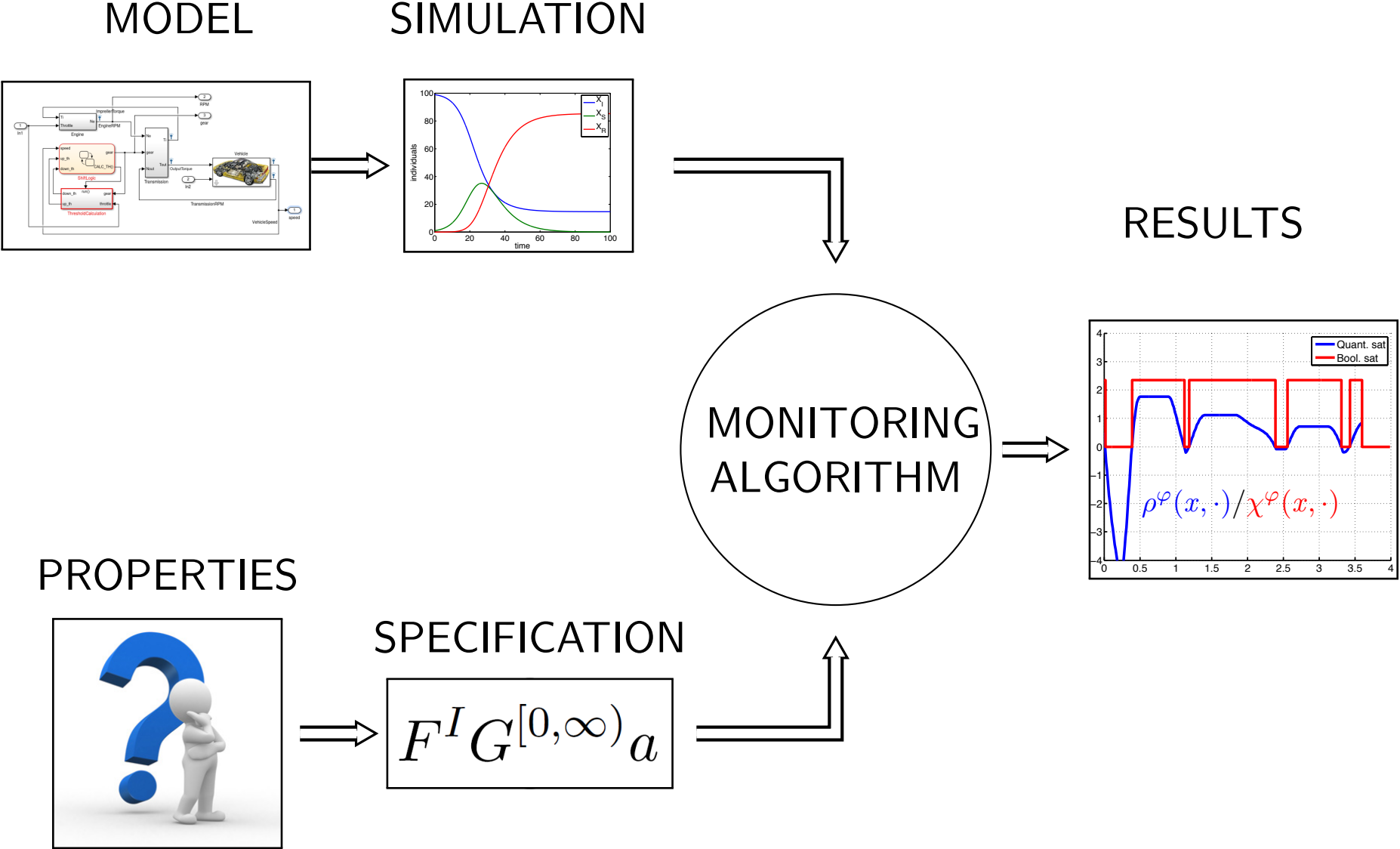
Step:

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

Settling Time:

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

Specification-based Monitoring



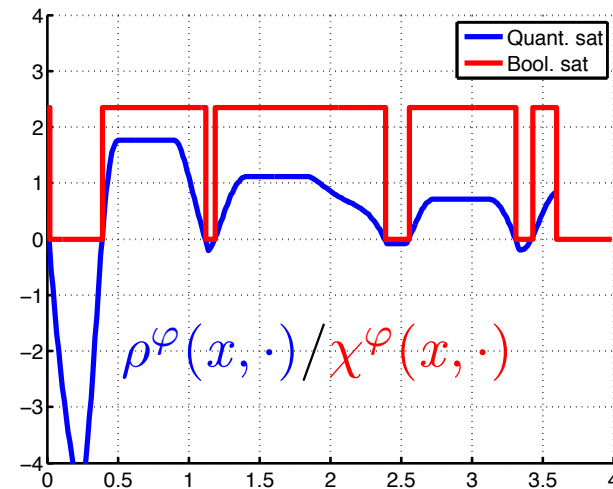
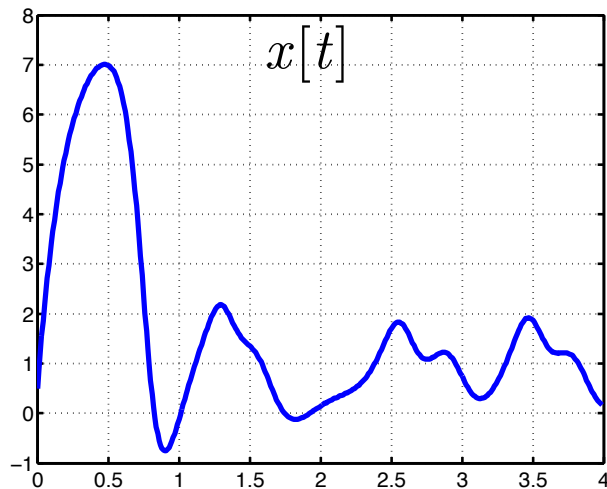
Specification-based Monitoring

Boolean Signal

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

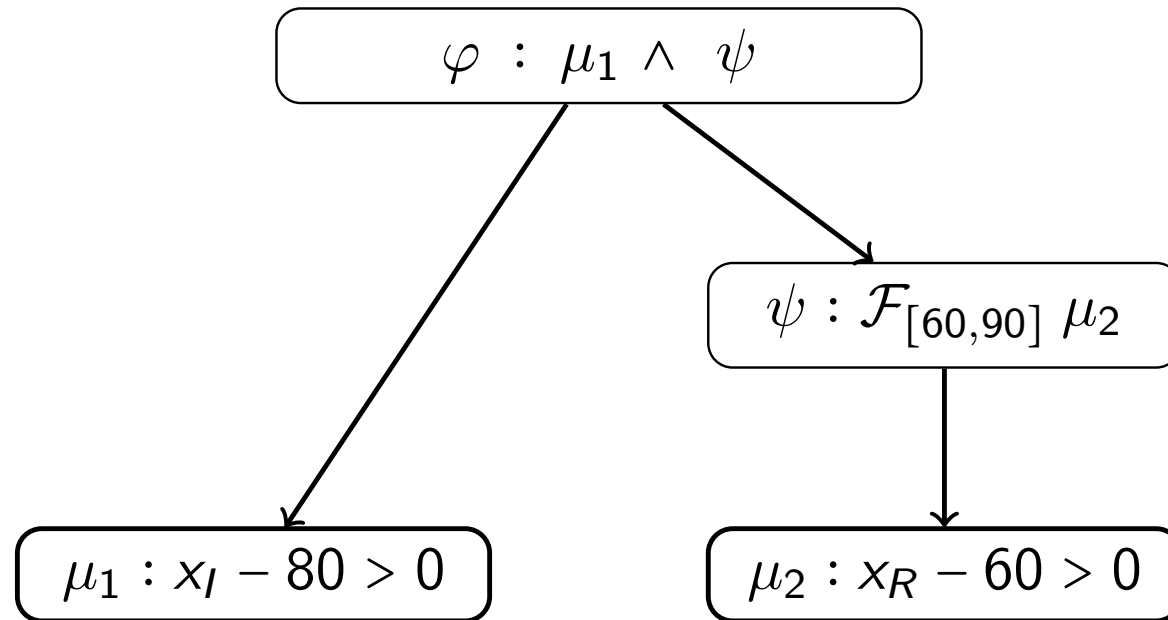
Quantitative Signal

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

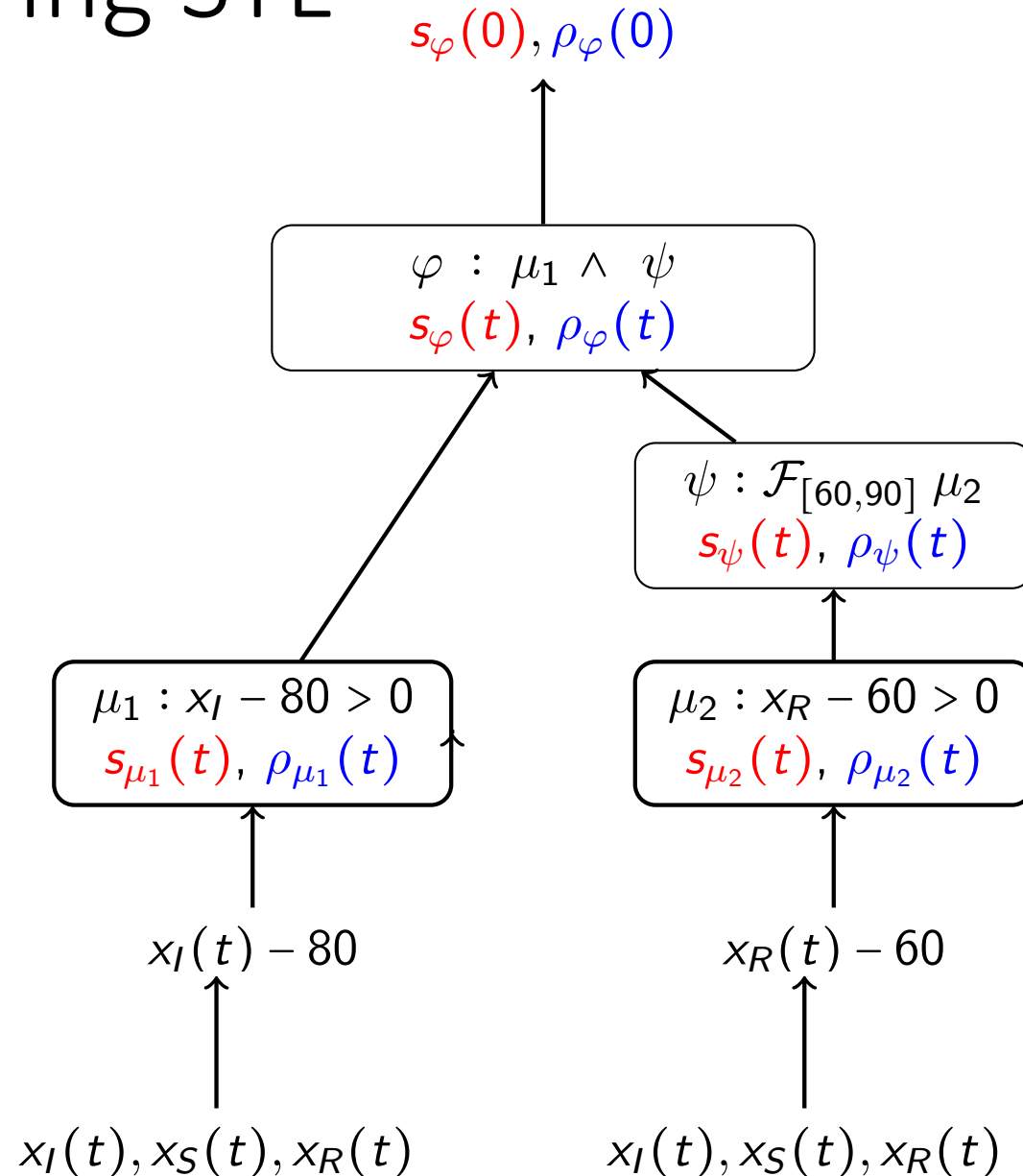


Monitoring STL

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



Monitoring STL



Boolean satisfaction

Quantitative satisfaction

Boolean signals

Quantitative signals

Secondary signals

Primary signals



Recursive Boolean Semantics of STL

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

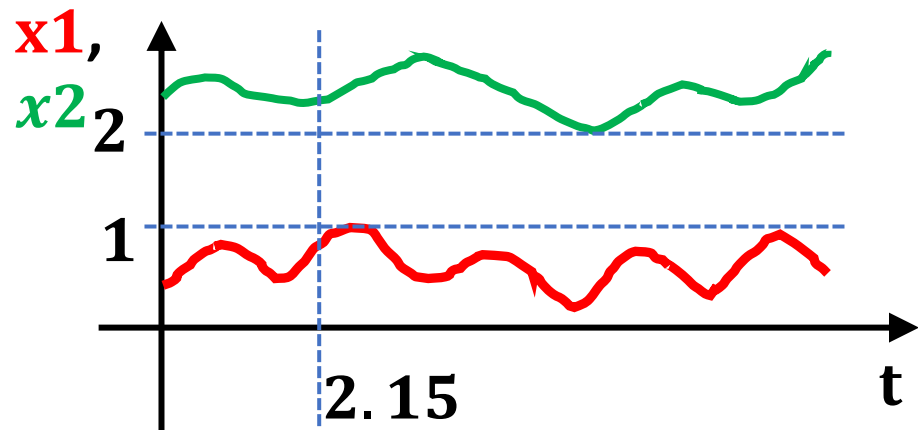
$$s(\varphi, \mathbf{x}) = s(\varphi, \mathbf{x}, 0)$$

STL semantics

- ▶ Semantics of STL specified recursively over a signal $\mathbf{x}: \mathbb{T} \rightarrow \mathbb{D}$ 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
 $s(\varphi, \mathbf{x}, t) = \text{true}$ iff $f(\mathbf{x}(t)) > 0$



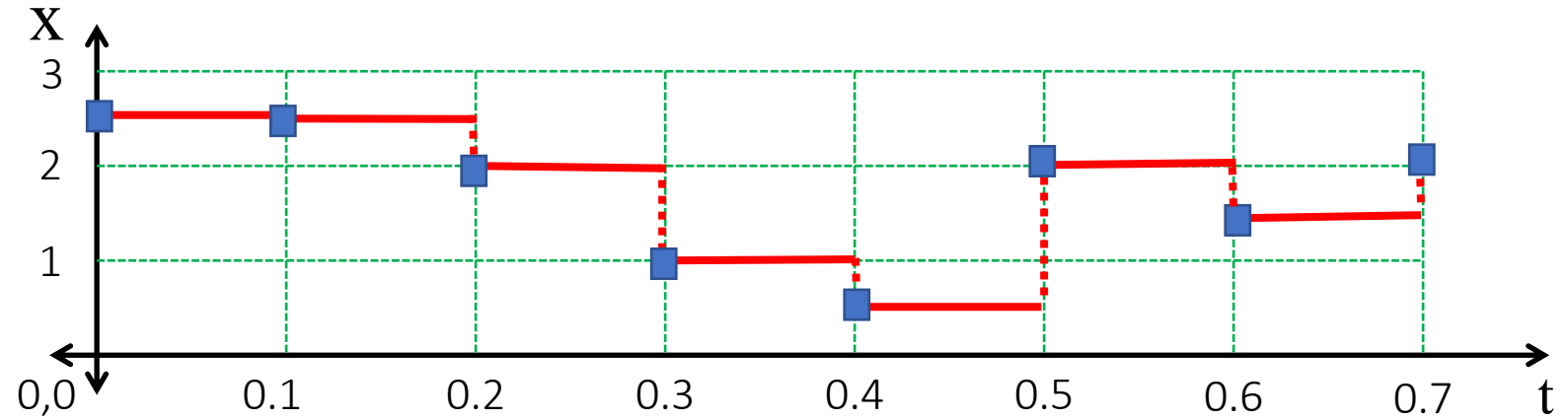
$$\mathbf{x} = (x_1, x_2)$$

$$f = x_2 - x_1 - 1$$

$$s(f(\mathbf{x}) > 0, \mathbf{x}, 2.15)?$$

Recursive Boolean Semantics of STL

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



$x(t) - 1.5 > 0$	T	T	T	F	F	T	T	T
$\mathbf{F}_{[0,0.2]} \mu$	T	T	T	T	T	T		
$\mathbf{G}_{[0,0.7]} \mathbf{F}_{[0,0.2]} \mu$	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 tto some real value
- ▶ We can interpret robustness as “distance to violation” of a given formula

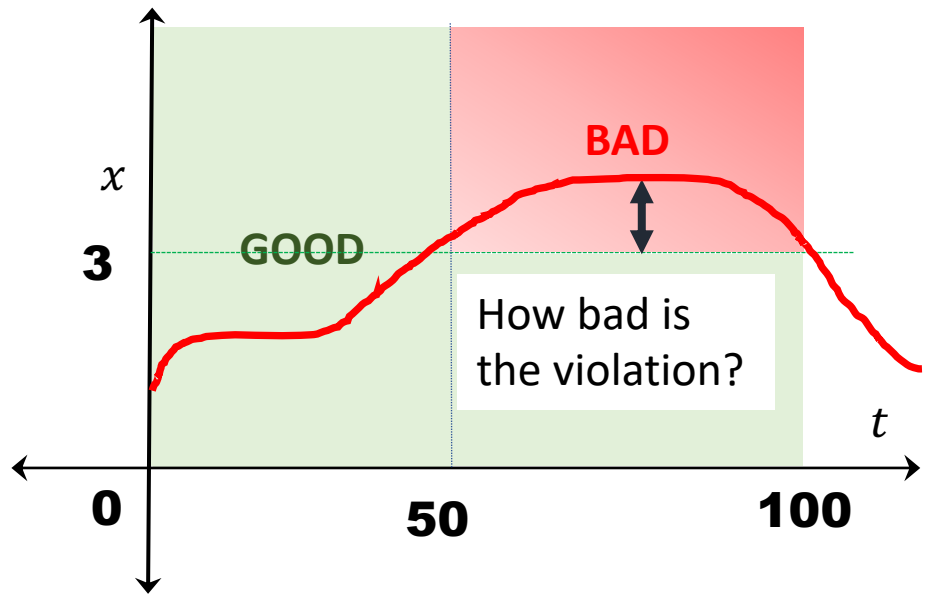
Recursive Quantitative Semantics

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

.

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

Distance to violation/satisfaction



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

Property of Robust Satisfaction Signal

- ▶ Sign indicates satisfaction status (soundness):

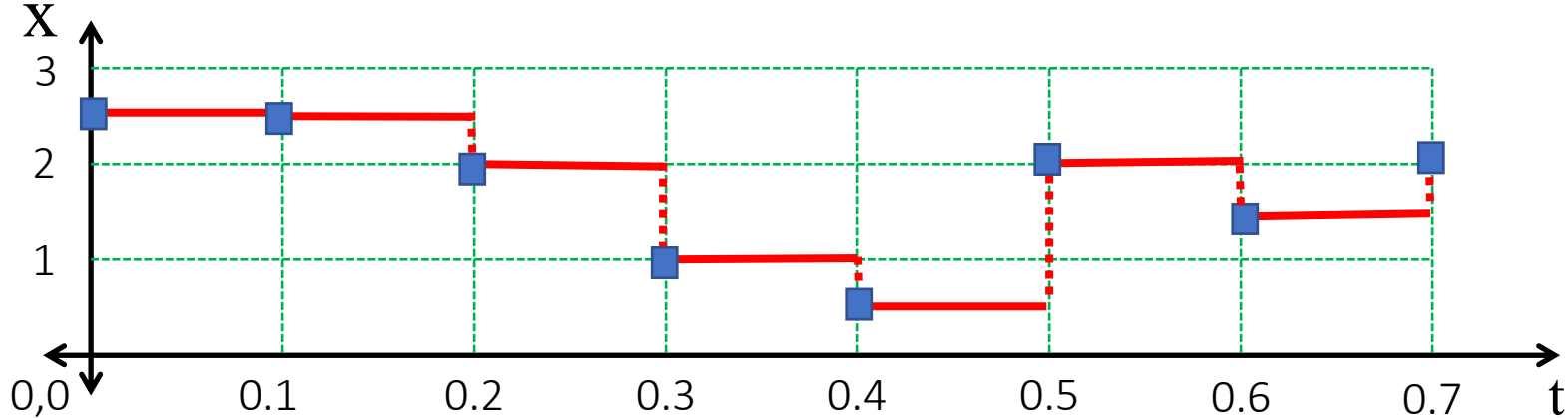
$$\begin{aligned}\rho(\varphi, \mathbf{x}, t) > 0 &\Rightarrow \beta(\varphi, \mathbf{x}, t) = 1 \\ \rho(\varphi, \mathbf{x}, t) < 0 &\Rightarrow \beta(\varphi, \mathbf{x}, t) = 0\end{aligned}$$

- ▶ Absolute value indicates tolerance (correctness)

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

Robustness computation example

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



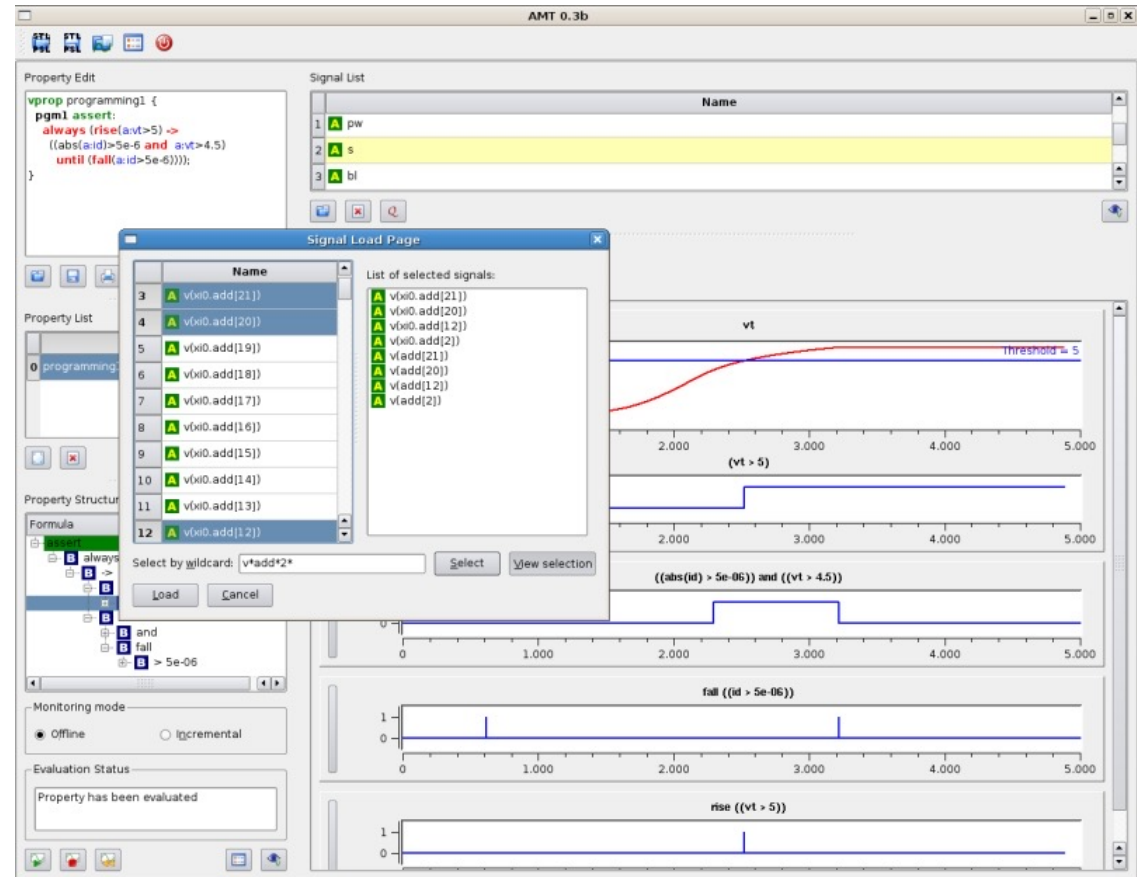
$x(t) - 1.5$	1	1	0.5	-0.5	-1	0.5	0	0.5
$\mathbf{F}_{[0,0.2]} \mu$	1	1	0.5	0.5	0.5	0.5		
$\mathbf{G}_{[0,0.7]} \mathbf{F}_{[0,0.2]} \mu$	0.5							

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

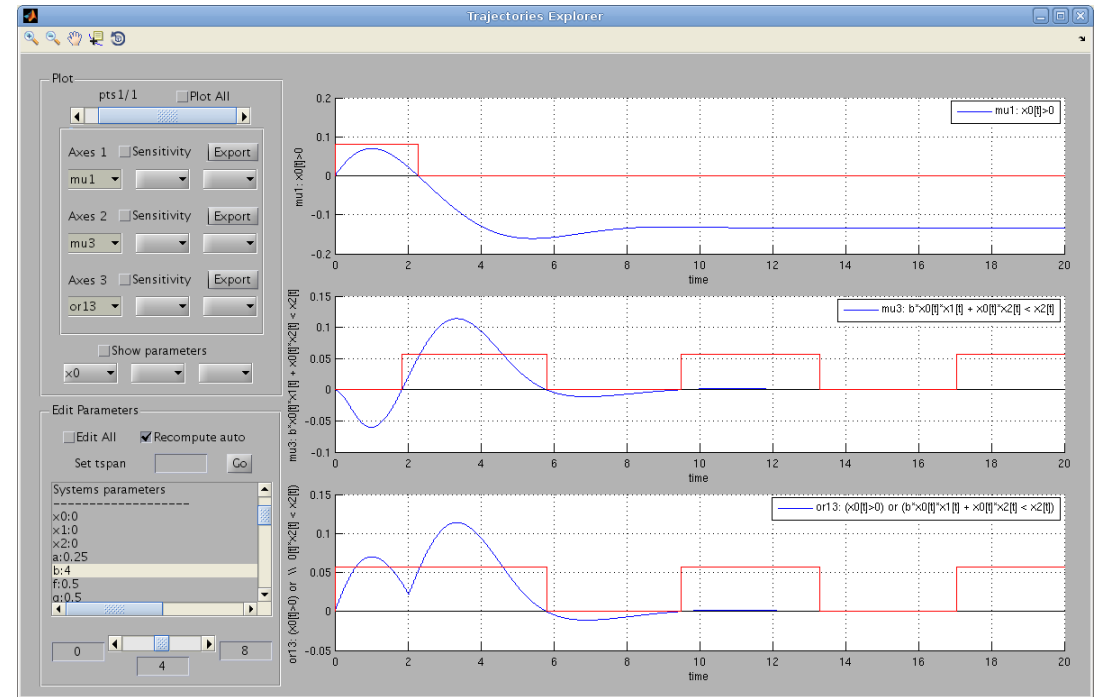
- ▶ Java toolbox
- ▶ STL with qualitative semantics
 - ▶ Correctness
- ▶ Offline monitoring



Breach

<https://github.com/decyphir/breach>

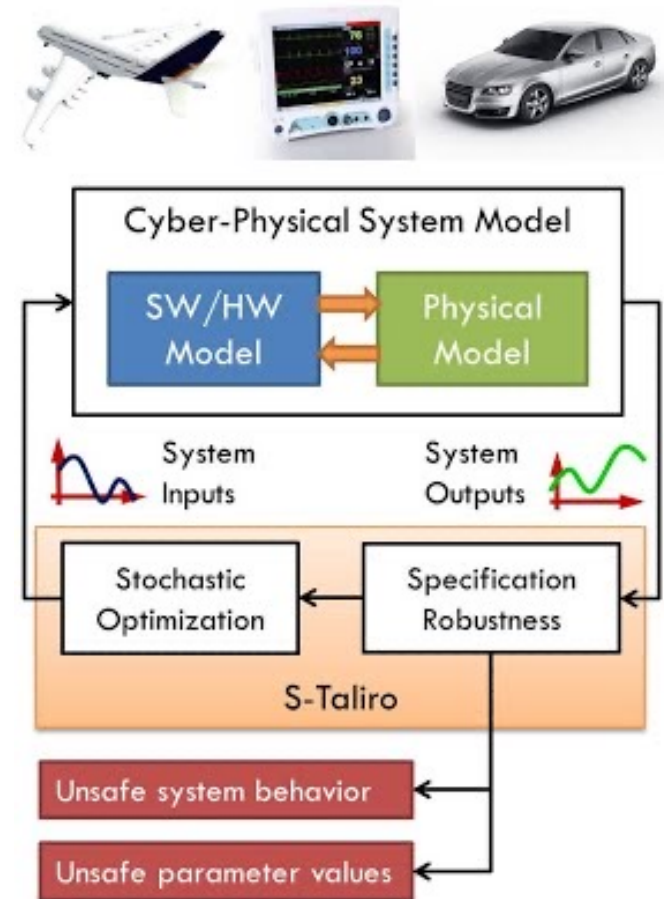
- ▶ MATLAB toolbox for
 - ▶ Simulation
 - ▶ Monitoring of temporal properties
 - ▶ Reachability
- ▶ STL with qualitative and quantitative semantics
 - ▶ Correctness
 - ▶ Robustness
- ▶ Offline and Online monitoring



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 entropy
- ▶ MTL with quantitative semantics
 - ▶ Robustness
- ▶ Offline and Online monitoring



Moonlight

<https://github.com/MoonLightSuite/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.