AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

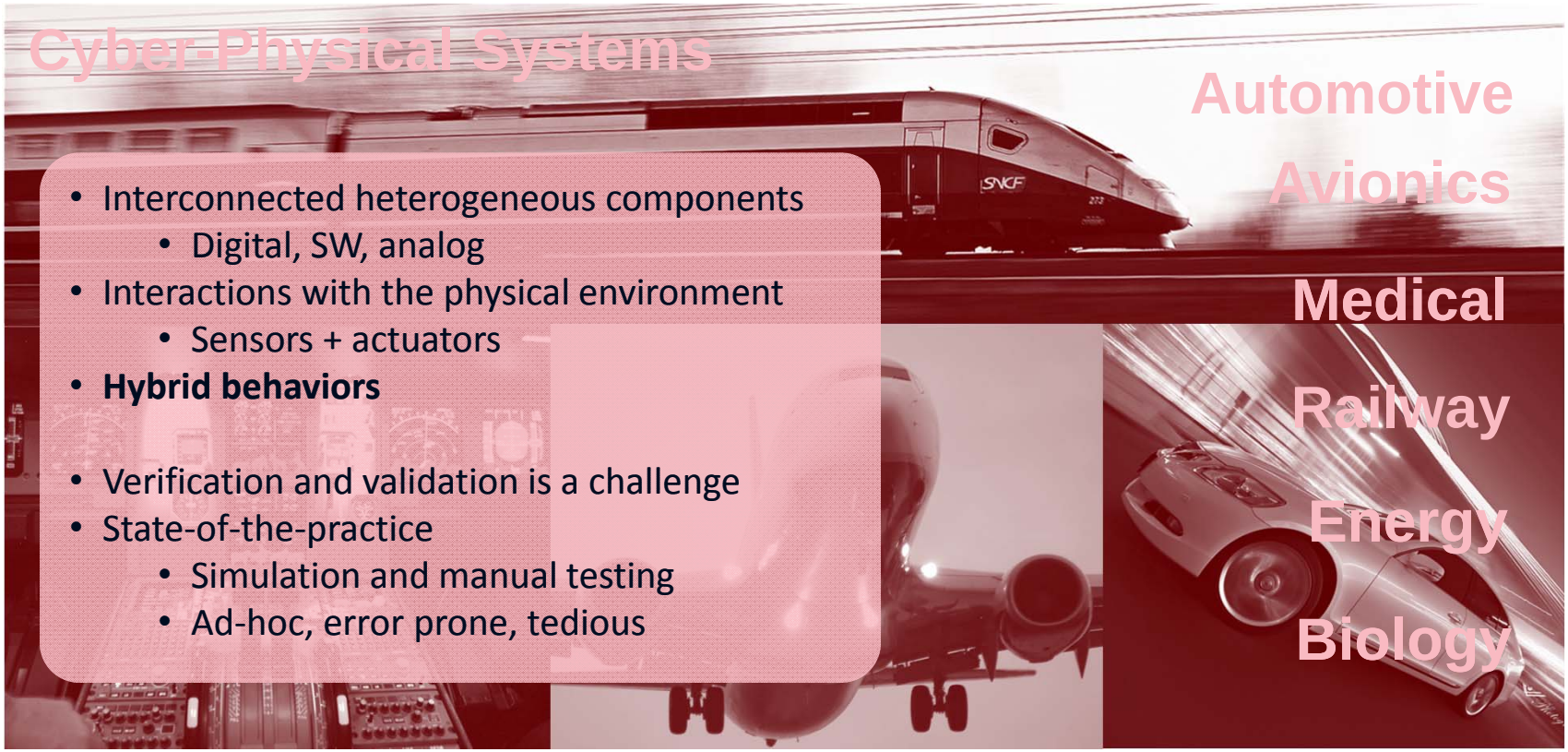
Monitoring and Measuring Hybrid Behaviors

Tutorial

Dejan Ničković

AIT Austrian Institute of Technology GmbH.

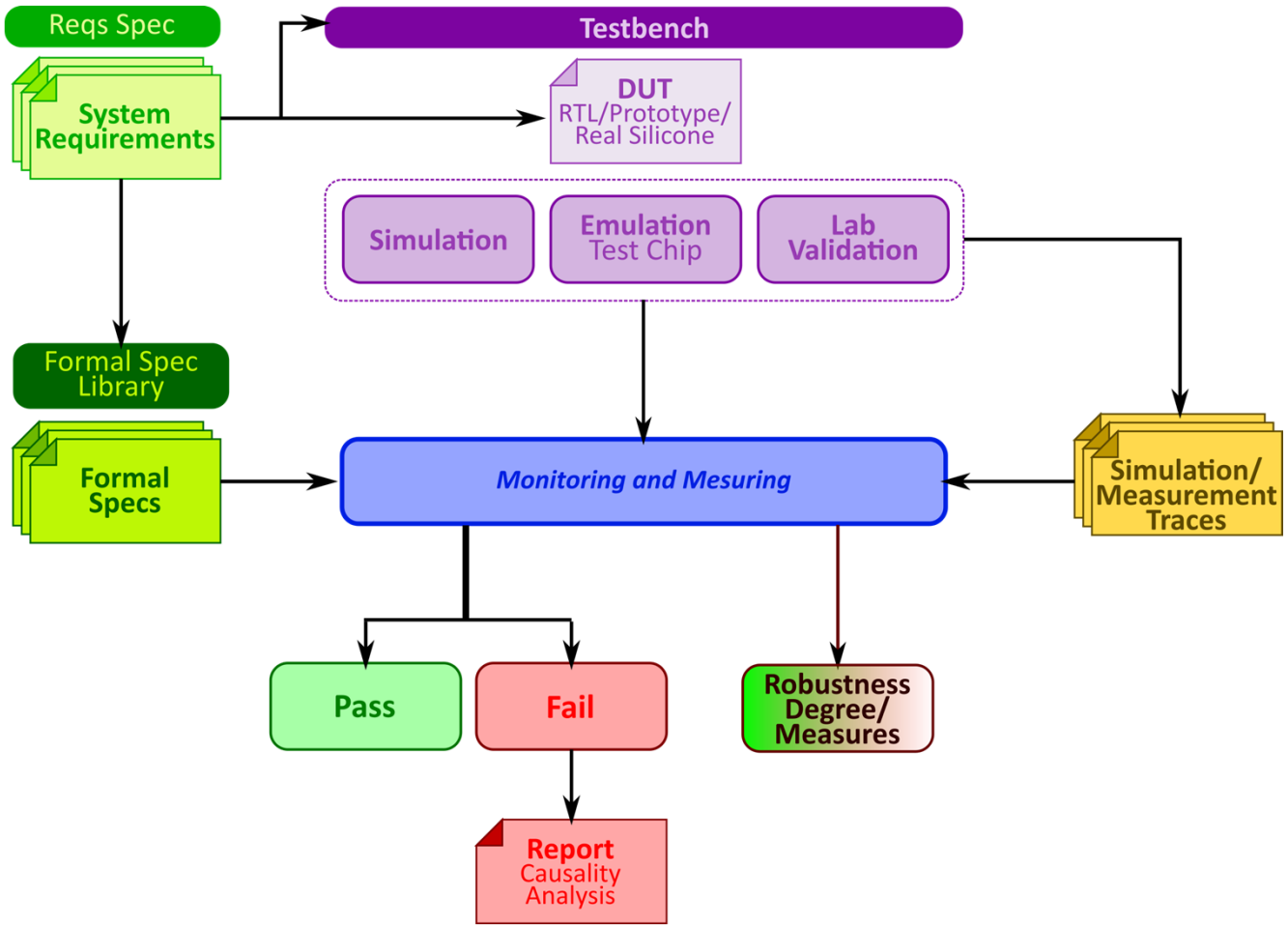
Introduction



- Interconnected heterogeneous components
  - Digital, SW, analog
- Interactions with the physical environment
  - Sensors + actuators
- **Hybrid behaviors**

- Verification and validation is a challenge
- State-of-the-practice
  - Simulation and manual testing
  - Ad-hoc, error prone, tedious

Monitoring and Measuring Technology

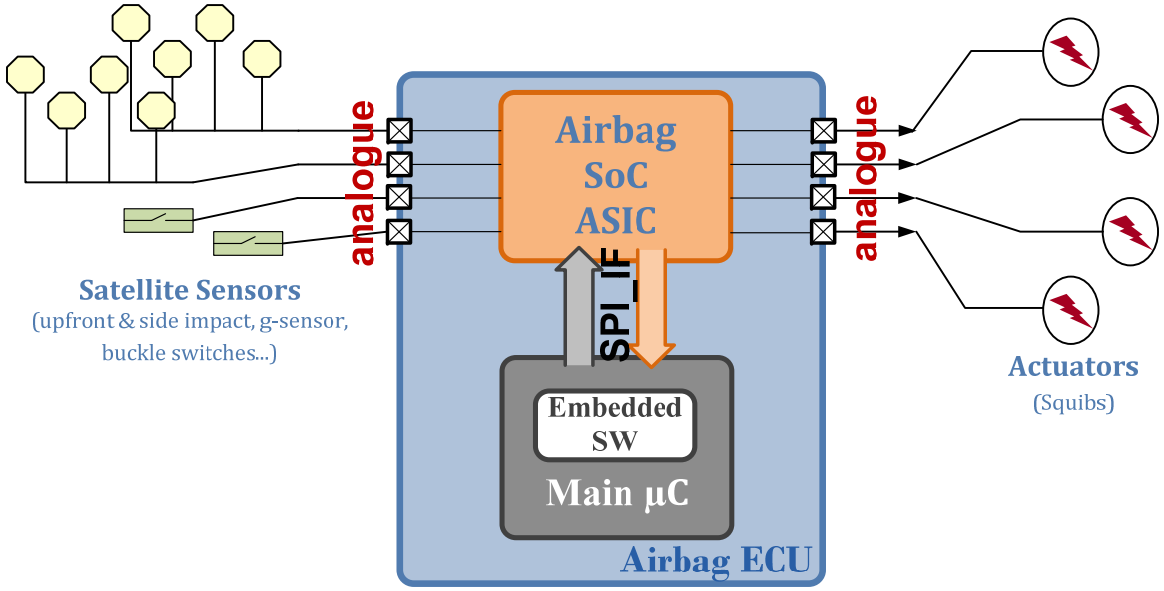


- Rigourous
- Not ambiguous
- Automatic
- Scalable
- Reusable

Motivating Example

Distributed Systems Interface (DSI3)

- Automotive bus standard



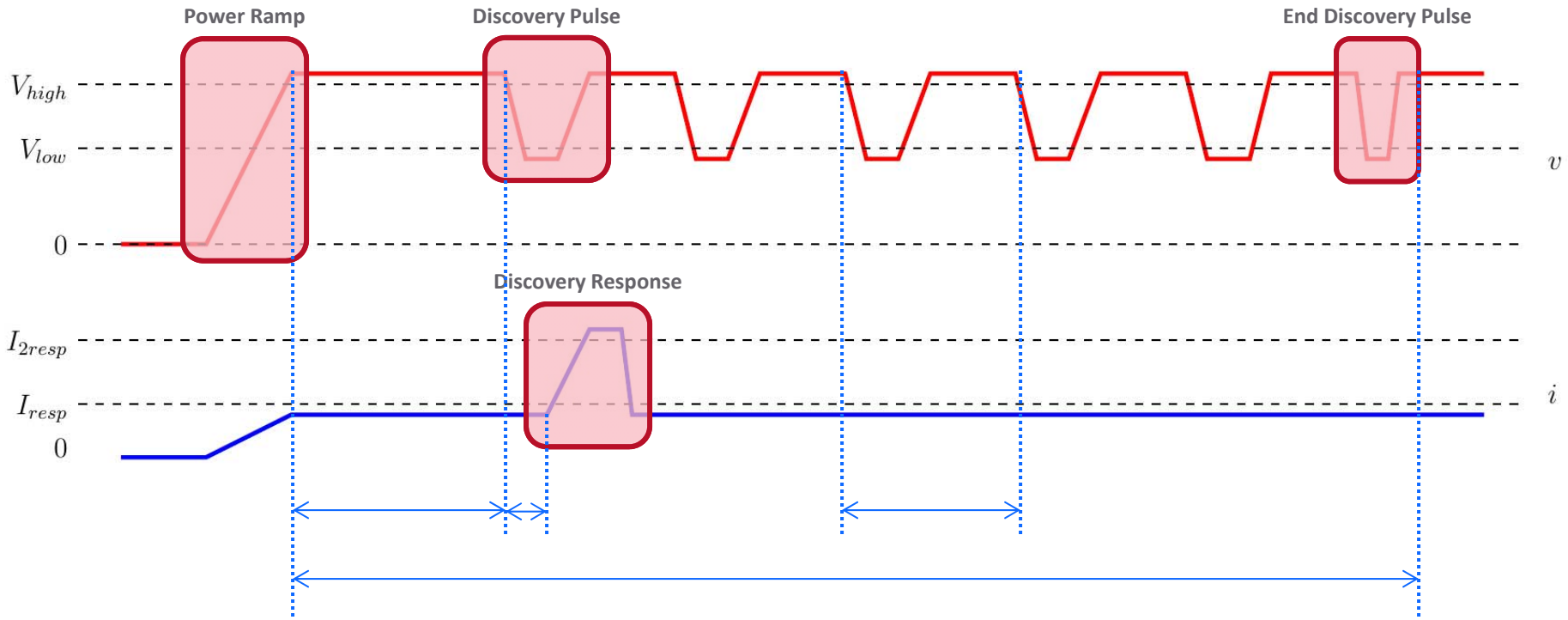
Airbag System Overview

(Sensors <--> Controller <--> Actuators)

- Communication via **voltage** and **current** lines

Motivating Example

Distributed Systems Interface (DSI3) – Discovery Mode



Outline

- Specification Languages
  - Signal Temporal Logic
  - Timed Regular Expressions
- Monitoring and Measuring Algorithms
  - STL with qualitative and quantitative semantics
  - STL with Quantitative semantics
  - Pattern matching TRE
- Beyond Signal Temporal Logic and Timed Regular Expressions
- Tools and Applications
- Future Perspectives

Specification Languages

Signal Temporal Logic

- High-level specification language
  - Continuous interpretation of time
  - Predicates over real-valued variables

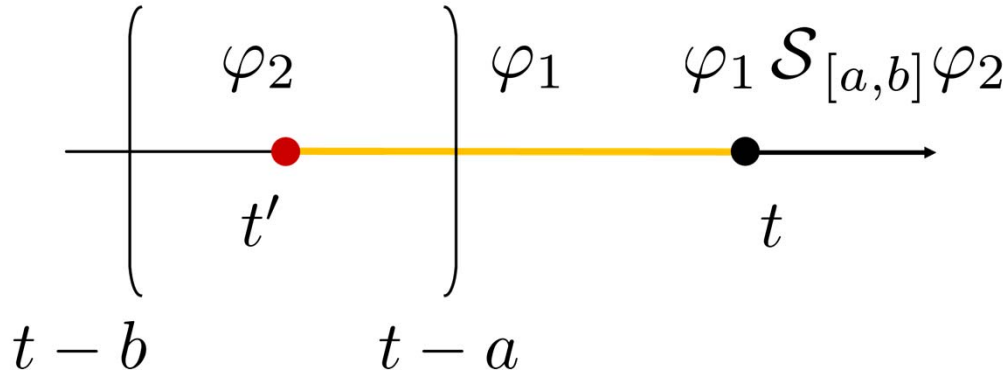
$$\alpha \quad := \quad p \mid x < c \mid x \leq c$$

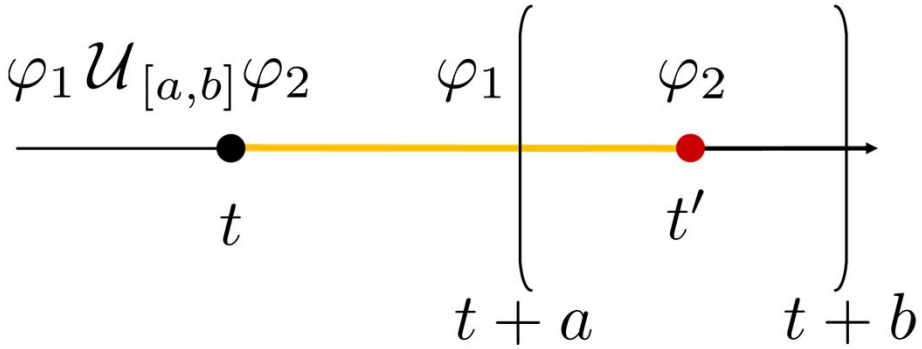
$$\varphi \quad := \quad \alpha \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \mathcal{U}_I \varphi_2 \mid \varphi_1 \mathcal{S}_I \varphi_2$$

- [MN04,MN13]

Signal Temporal Logic

Semantics





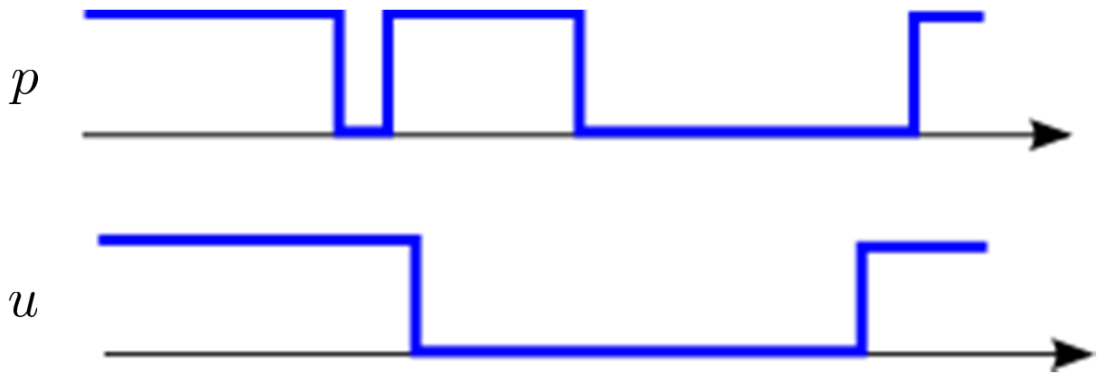
Signal Temporal Logic

Satisfaction Signals

- For every STL formula φ and behavior w, we associate a satisfaction signal u that has the following property.

$$u(t) = 1 \leftrightarrow (w, t) \models \varphi$$

- Satisfaction signal u for the formula $\Diamond_I p$



Signal Temporal Logic

Derived Operators

- Timed **always**, **eventually**, **historically** and **once**

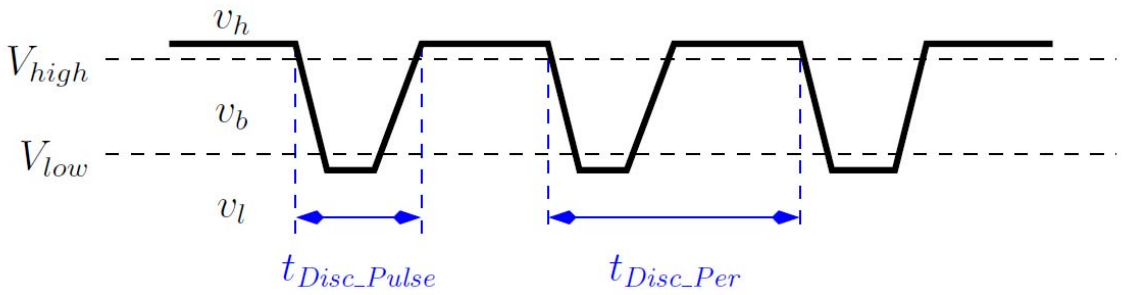
$$
\begin{aligned}
\Diamond_I \varphi &\equiv True\ \mathcal{U}_I\ \varphi \\
\Box_I \varphi &\equiv \neg \Diamond_I \neg \varphi \\
\diamondminus_I \varphi &\equiv True\ \mathcal{S}_I\ \varphi \\
\boxminus_I \varphi &\equiv \neg \diamondminus_I \neg \varphi
\end{aligned}
$$

- Events – **rising** and **falling edges**

$$
\begin{aligned}
\uparrow \varphi &\equiv (\varphi \wedge (\neg\varphi\, \mathcal{S}\, True)) \vee (\neg\varphi \wedge (\varphi \mathcal{U}\, True)) \\
\downarrow \varphi &\equiv (\neg\varphi \wedge (\varphi\, \mathcal{S}\, True)) \vee (\varphi \wedge (\neg\varphi \mathcal{U}\, True))
\end{aligned}
$$

Signal Temporal Logic

Formalization of DSI3 Requirements



$$
\begin{aligned}
v_l &\equiv v \leq V_{low} \\
v_b &\equiv V_{low} \leq v \leq V_{high} \\
v_h &\equiv v \geq V_{high}
\end{aligned}
$$

- Discovery pulse

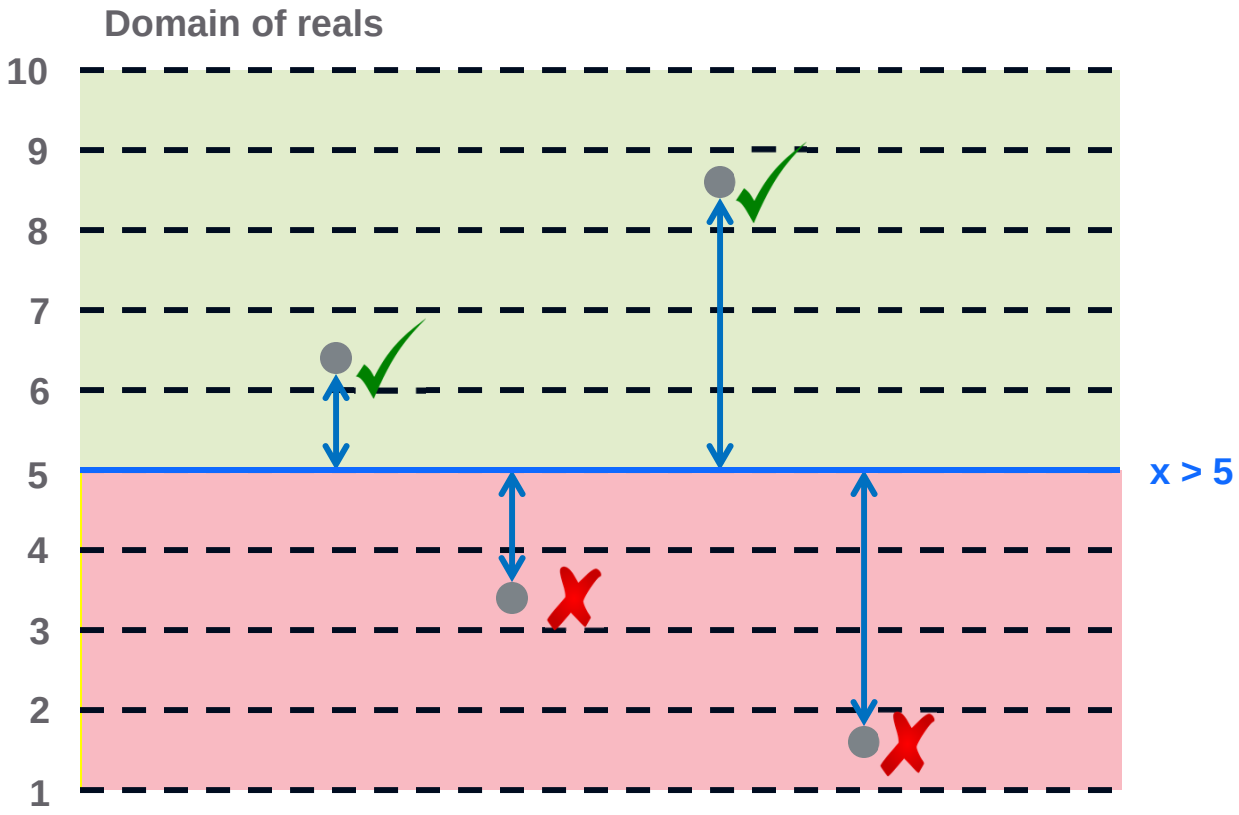
$$
\begin{aligned}
\varphi_{shape} &\equiv \downarrow v_h \wedge (v_b \mathcal{U} v_l \mathcal{U} v_b \mathcal{U} v_h) \\
\varphi_{dur} &\equiv \downarrow v_h \wedge (\neg v_h \mathcal{U}_{I_{Disc\_Pulse}} \uparrow v_h) \\
\varphi_{pulse} &\equiv \varphi_{shape} \wedge \varphi_{dur}
\end{aligned}
$$

- Distance between consecutive discovery pulses

$$\Box(\varphi_{pulse} \rightarrow ((\neg\varphi_{pulse} \mathcal{U}_{I_{Disc\_per}} \varphi_{pulse}) \vee \Box(\neg\varphi_{pulse})))$$

Signal Temporal Logic

Quantitative Semantics - Motivation



Signal Temporal Logic

Quantitative Semantics

- From satisfaction relation to **robustness degree**

$$(w,t) \models \varphi_1 \vee \varphi_2 \quad \leftrightarrow \quad (w,t) \models \varphi_1 \text{ or } (w,t) \models \varphi_2$$

$$\rho(\varphi_1 \vee \varphi_2, w, t) \quad = \quad \max\{\rho(\varphi_1, w, t), \rho(\varphi_2, w, t)\}$$

$$(w,t) \models \Diamond_I \varphi \quad \leftrightarrow \quad \exists t' \in (t+I) \cap \mathbb{T} \text{ st. } (w,t') \models \varphi$$

$$\rho(\Diamond_I \varphi, w, t) \quad = \quad \sup_{t' \in (t+I) \cap \mathbb{T}} (\rho(\varphi, w, t'))$$

- **Spatial** quantitative semantics
- [FP09]

Timed Regular Expressions

Syntax and Semantics

- Extension of regular expressions with real-time constraints [ACM97]
- Syntax

$$\alpha \quad := \quad \epsilon \mid \theta \mid \alpha_1 \cdot \alpha_2 \mid \alpha_1 \cup \alpha_2 \mid \alpha_1 \cap \alpha_2 \mid \alpha^* \mid \langle \alpha \rangle_I$$

- Semantics

$$\begin{array}{lll}
(w,t,t') & \models \epsilon & \leftrightarrow \quad t = t' \\
(w,t,t') & \models \theta & \leftrightarrow \quad t < t' \text{ and } \forall\, t < t'' < t',\, \pi_\theta(w)[t''] = 1 \\
(w,t,t') & \models \alpha_1 \cdot \alpha_2 & \leftrightarrow \quad \exists\, t \le t'' \le t',\, (w,t,t'') \models \alpha_1 \text{ and } (w,t'',t') \models \alpha_2 \\
(w,t,t') & \models \langle \alpha \rangle_I & \leftrightarrow \quad t' - t \in I \text{ and } (w,t,t') \models \alpha
\end{array}$$

- Match set

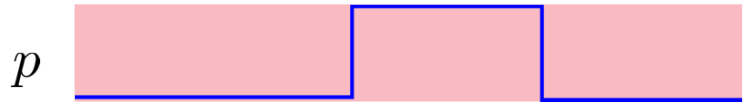
$$\mathcal{M}(\alpha, w) = \{(t,t') \in \mathbb{R}^2 \mid (w,t,t') \models \alpha\}$$

Timed Regular Expressions

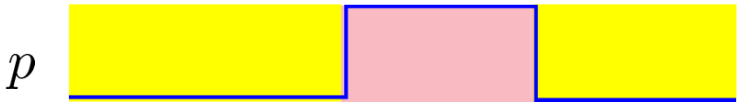
Conditional Expressions and Events

- Conditional Expressions

$$(w,t,t') \models \alpha_1 \,?\, \alpha_2 \leftrightarrow (w,t,t') \models \alpha_2 \text{ and } \exists t'' \leq t,\ (w,t'',t) \models \alpha_1$$
$$(w,t,t') \models \alpha_1 \,!\, \alpha_2 \leftrightarrow (w,t,t') \models \alpha_1 \text{ and } \exists t'' \geq t',\ (w,t',t'') \models \alpha_2$$



$\neg p \cdot p \cdot \neg p$



$\neg p \,?\, p \,!\, \neg p$

- Events

$$\uparrow\theta \equiv \neg\theta \,?\, \epsilon \,!\, \theta$$
$$\downarrow\theta \equiv \uparrow\neg\theta$$

Timed Regular Expressions

Mesurement Specification Language

- Event-bounded timed regular expressions

$$\psi := \uparrow p \mid \psi_1 \cdot \alpha \cdot \psi_2 \mid \psi_1 \cup \psi_2 \mid \psi_1 \cap \alpha$$

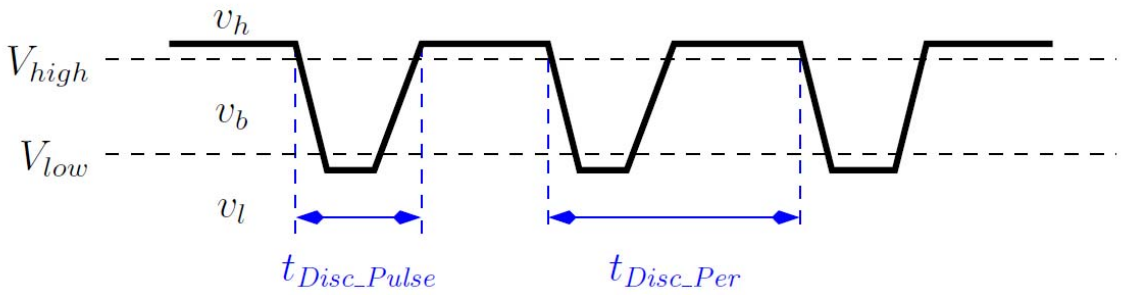
- Mesurement language

$$\begin{aligned}
[\![\mathsf{time}(\uparrow p)]\!]_w &= \{t \,:\, (t,t) \in \mathcal{M}(\uparrow p, w)\} \\
[\![\mathsf{value}_x(\uparrow p)]\!]_w &= \{\pi_x(w)[t] \,:\, (t,t) \in \mathcal{M}(\uparrow p, w)\} \\
[\![\mathsf{duration}(\alpha)]\!]_w &= \{t' - t \,:\, (t,t') \in \mathcal{M}(\alpha, w)\} \\
[\![\mathsf{inf}_x(\alpha)]\!]_w &= \{\min_{t \le \tau \le t'} \pi_x(w)(\tau) \,:\, (t,t') \in \mathcal{M}(\alpha, w)\} \\
[\![\mathsf{sup}_x(\alpha)]\!]_w &= \{\max_{t \le \tau \le t'} \pi_x(w)(\tau) \,:\, (t,t') \in \mathcal{M}(\alpha, w)\} \\
[\![\mathsf{integral}_x(\alpha)]\!]_w &= \{\int_t^{t'} \pi_x(w)(\tau) d\tau \,:\, (t,t') \in \mathcal{M}(\alpha, w)\} \\
[\![\mathsf{average}_x(\alpha)]\!]_w &= \{\tfrac{1}{t'-t} \int_t^{t'} \pi_x(w)(\tau) d\tau \,:\, (t,t') \in \mathcal{M}(\alpha, w)\}
\end{aligned}$$

- [FMN+15]

Timed Regular Expressions

Formalization of DSI3 Requirements



$$v_l \equiv v \leq V_{low}$$
$$v_b \equiv V_{low} \leq v \leq V_{high}$$
$$v_h \equiv v \geq V_{high}$$

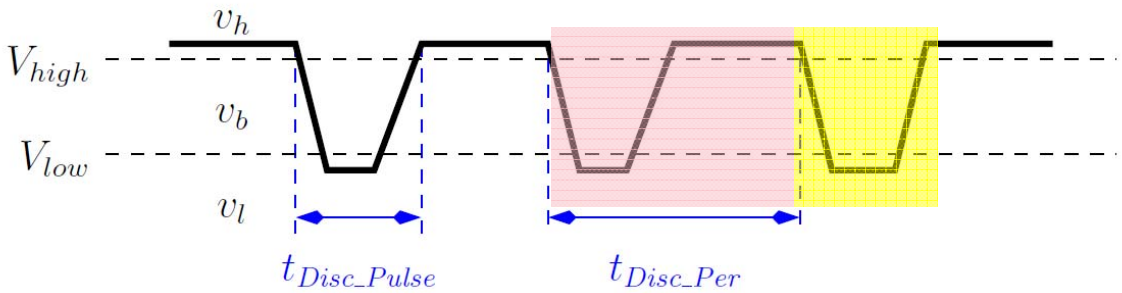
- Discovery pulse

$$\alpha_{pulse} \equiv \downarrow (v_h) \cdot \langle v_b \cdot v_l \cdot v_b \rangle_{I_{Disc\_Pulse}} \cdot \uparrow (v_h)$$

- Distance between consecutive discovery pulses
  - Cannot be expressed
    - No negation
    - No universal quantification over time

Timed Regular Expressions

Formalization of DSI3 Requirements - Measurements



$$
\begin{aligned}
v_l &\equiv v \leq V_{low} \\
v_b &\equiv V_{low} \leq v \leq V_{high} \\
v_h &\equiv v \geq V_{high}
\end{aligned}
$$

- Segment between two consecutive discovery pulses

$$
\begin{aligned}
\alpha_1 &\equiv \epsilon \\
\psi &\equiv \alpha_{pulse} \cdot v_h \cdot \downarrow (v_h) \\
\alpha_2 &\equiv \alpha_{pulse} \\
\alpha &\equiv \alpha_1 \,?\, \psi \,!\, \alpha_2
\end{aligned}
$$

- Average duration between consecutive discovery pulses

$$
\begin{aligned}
\mathcal{D} &= \mathsf{duration}(\alpha) \\
avg &= \frac{\Sigma_{\delta \in \mathcal{D}}\ \delta}{|\mathcal{D}|}
\end{aligned}
$$

Summary

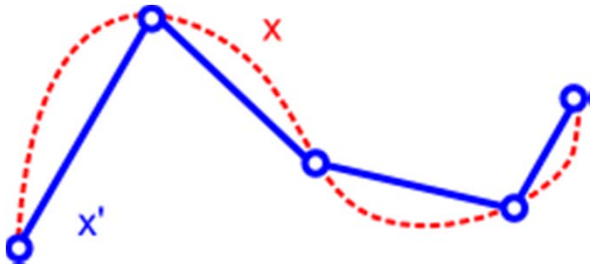
- Signal temporal logic
  - Patterns could be formalized
    - Difficult
  - Temporal relations could be formalized
    - Easy
  - No measurement specifications

- Timed regular expressions
  - Patterns could be formalized
    - Easy
  - Temporal properties could not be formalized
    - No negation
  - Measurement specifications

Monitoring and Measuring Algorithms

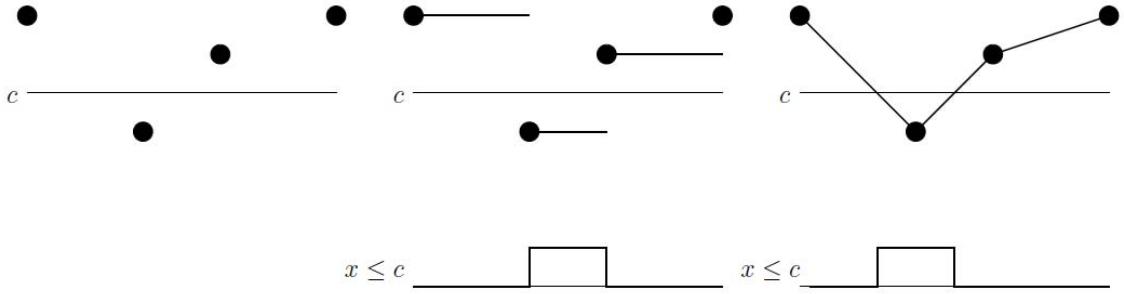
Handling Numerical Predicates

- Specification formalisms defined with respect to ideal mathematical behaviors
  - Function from continuous-time to real valued domain



- Simulator provide imperfect approximation of behaviors
  - Collection of timestamp-value pairs

- Interpolation
  - Step, linear, etc.



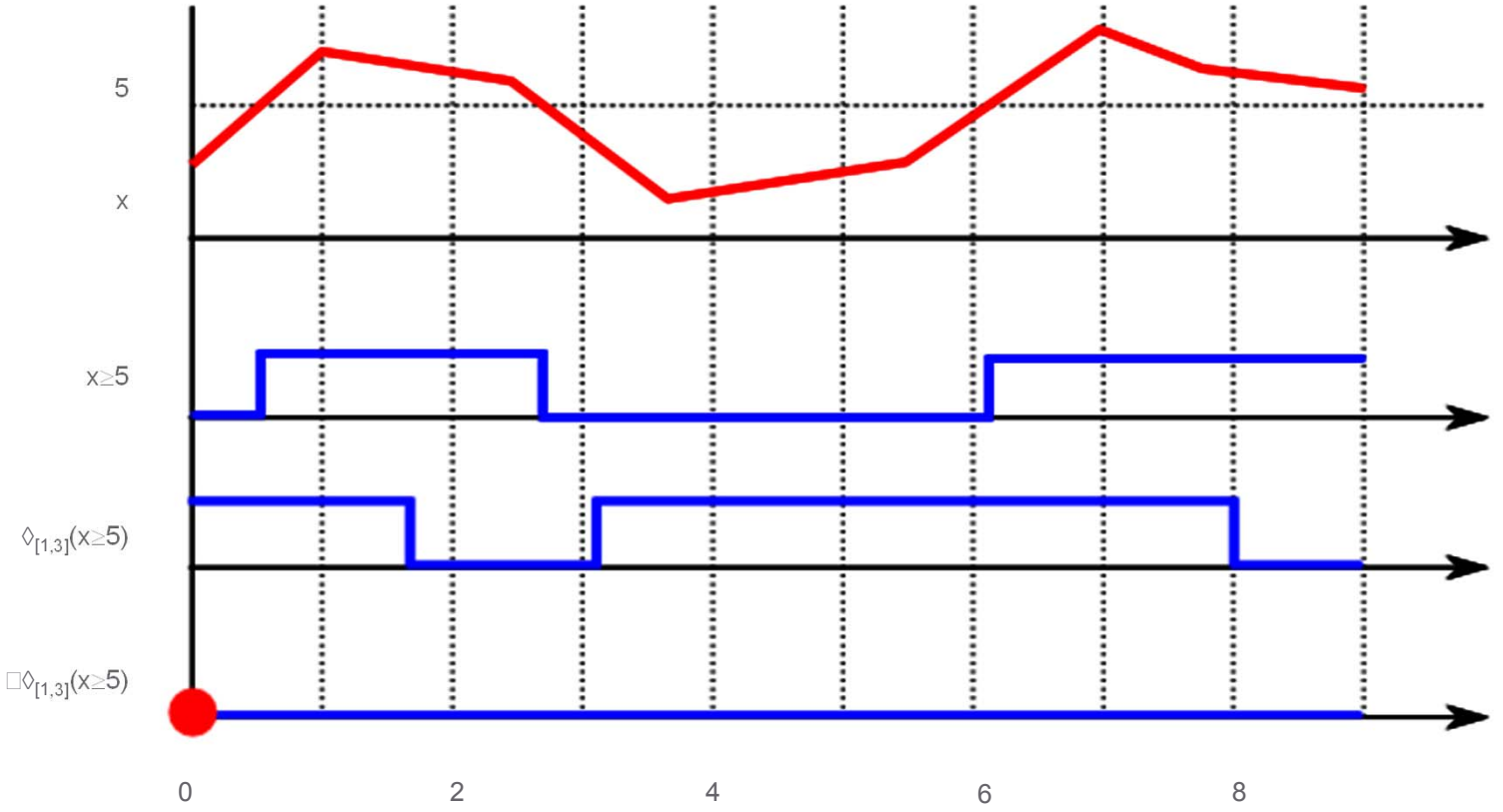
Monitoring Signal Temporal Logic

- **Marking:** a procedure that computes the satisfaction signal or the robustness degree of each sub-formula of an STL specification
  - Doubly-recursive procedure, on time and the structure of the formula
  - Procedure directly applied on signals, no automata

- Algorithms for monitoring STL properties
  - **Offline marking:** input is fully available
  - **Incremental marking:** input is dynamically observed
  - **Quantitative marking:** computation of robustness degree

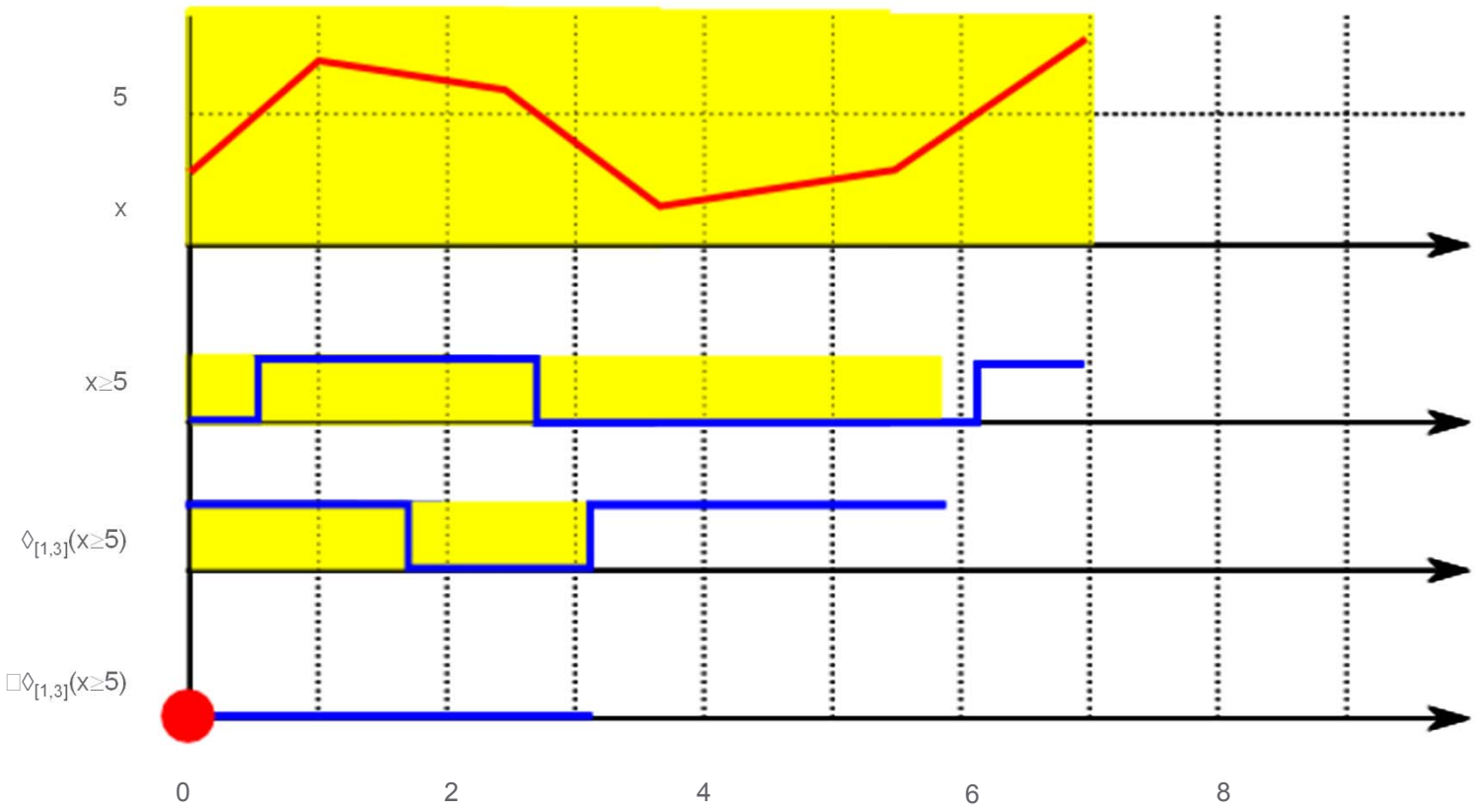
Monitoring Signal Temporal Logic

Offline Qualitative



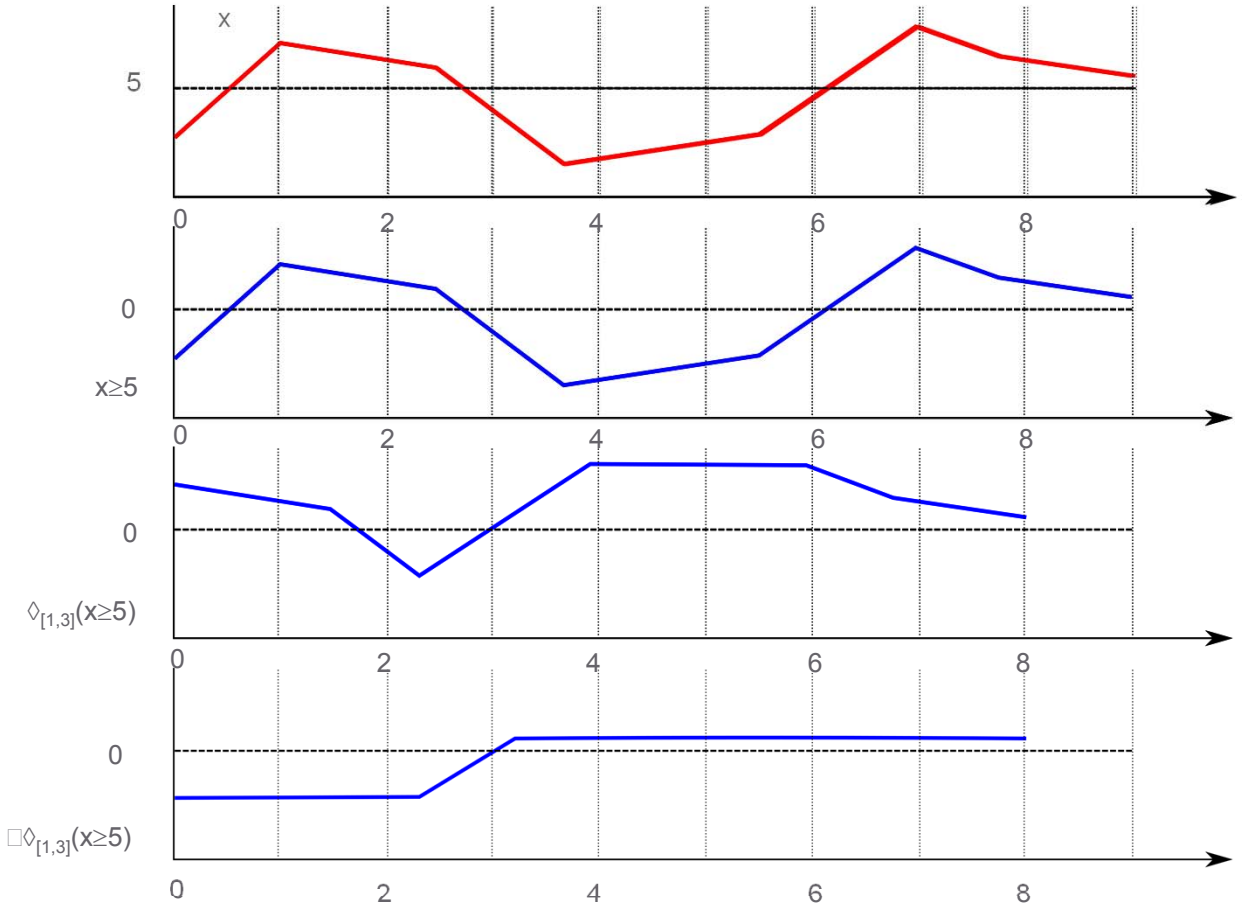
Monitoring Signal Temporal Logic

Incremental Qualitative



Monitoring Signal Temporal Logic

Quantitative



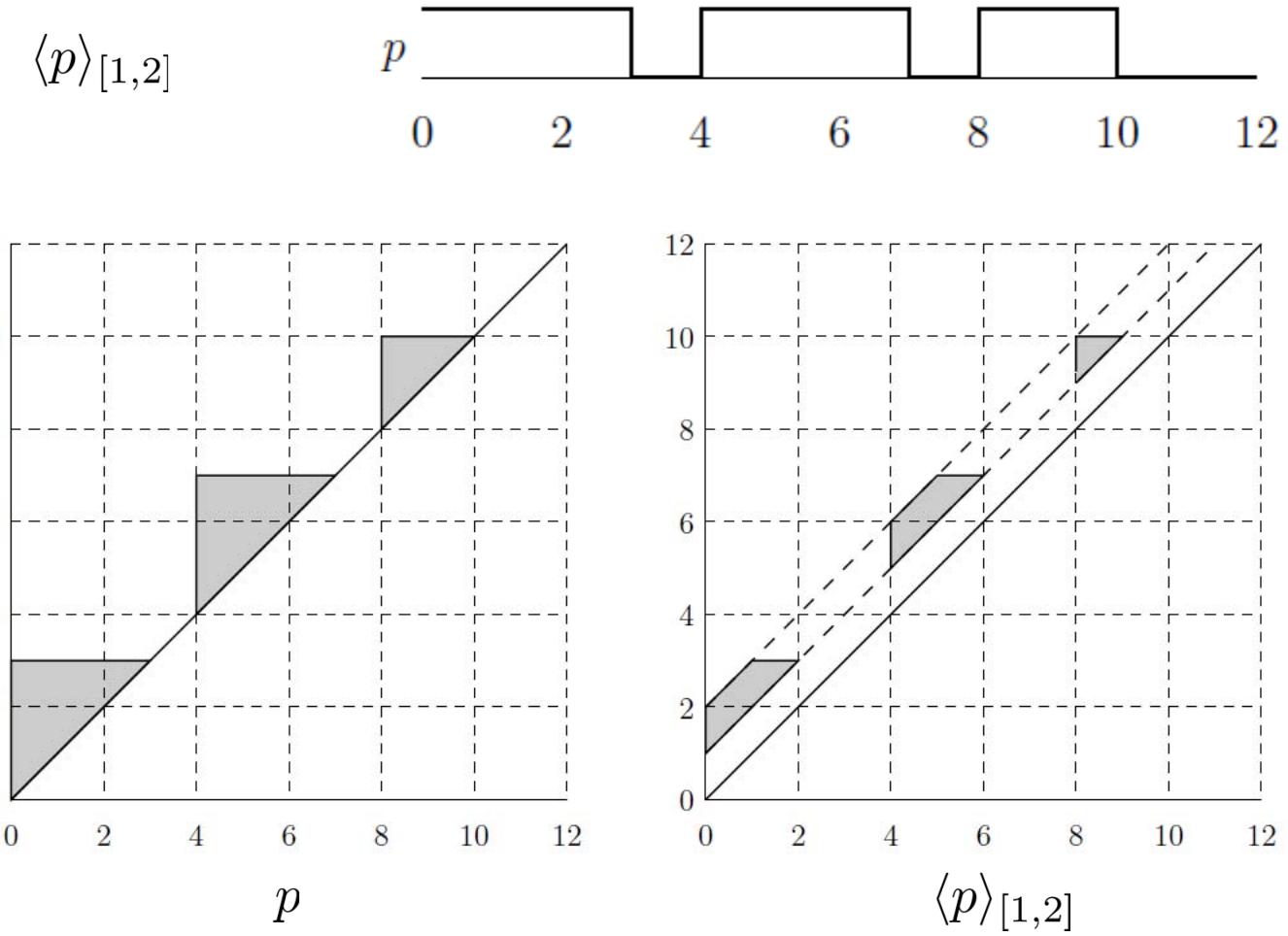
Pattern Matching Timed Regular Expressions

- Computing the **match set** of an expression
  - Finite union of 2-dimensional **zones**

- Timed regular expression operators
  - Operations on zones

- [UFA+14]

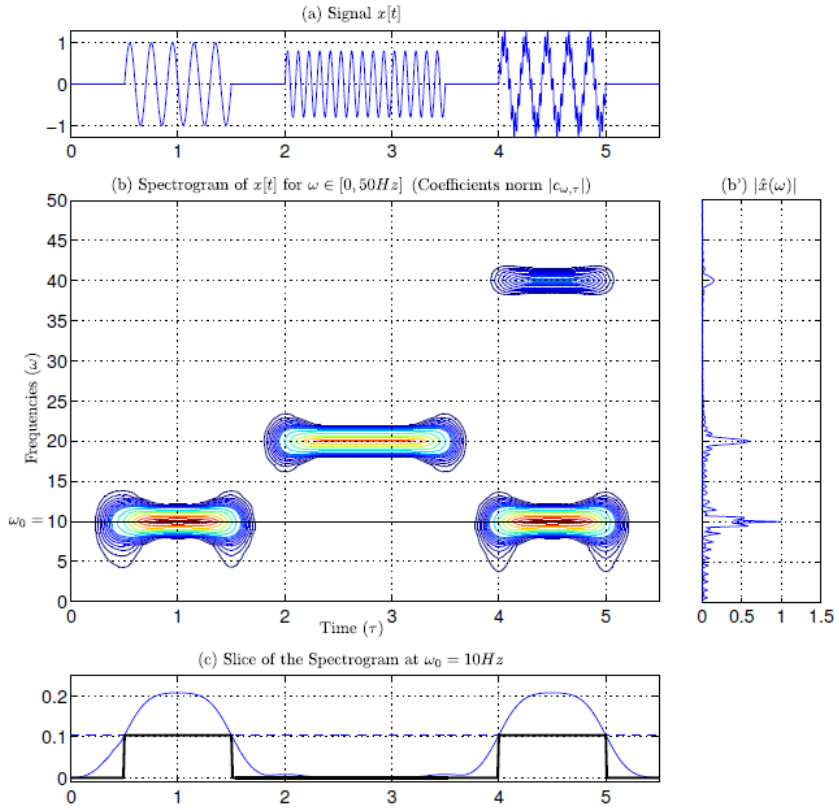
Pattern Matching Timed Regular Expressions



Beyond Signal Temporal Logic and Timed Regular Expressions

Time-Frequency Logic

- Specification language that captures
  - Time-domain
  - Frequency-domain properties
- Extends STL with frequency domain predicates
  - Short-time Fourier transform
- [DMB+12]



Signal Temporal Logic with Freeze Quantifiers

- STL with freezing operator
  - Freeze a value in the behavior when a sub-property evaluates to true
  - Use it for comparison in another sub-property
- Powerful mechanism
  - Similar to local variables in PSL and SVA
  - Similar to TPTL
- Qualitative and quantitative semantics
- [BDS+14]

Parametric Signal Temporal Logic

- Signal Temporal Logic with **magnitude** and **time parameters**

$$\Box_{[0,s_1]} \Diamond_{[0,s_2]} (x < p)$$

- s_1, s_2 and p are parameters

- Given an STL formula with timing and magnitude parameters and a behavior of a system, find the range of parameters that makes the formula satisfied with respect to the behavior

- Two algorithms
  - Quantifier elimination
  - Approximation of Pareto fronts

- [ADM+11]

Spatio Temporal Logic

- SpaTeL – unification of
  - Signal Temporal Logic
  - Tree Spatial Superposition Logic
- Specification of spatial patterns that evolve over time
- Distributed and networked systems
- Quantitative semantics + statistical model checking
- [HJK+15]

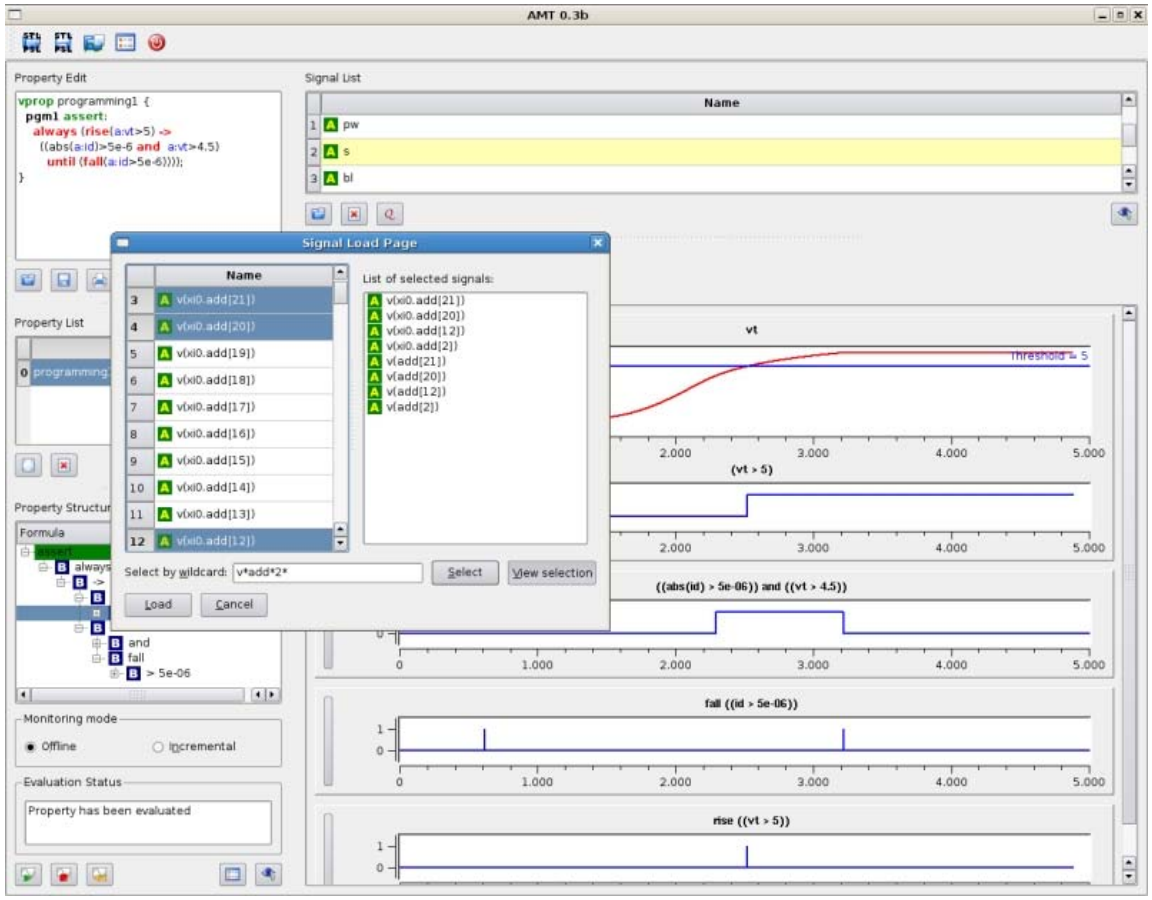
Tools and Applications

Analog Monitoring Tool

http://www-verimag.imag.fr/DIST-TOOLS/TEMPO/AMT/content.html

- STL with qualitative semantics
  - Correctness
- Offline monitoring
- Incremental monitoring

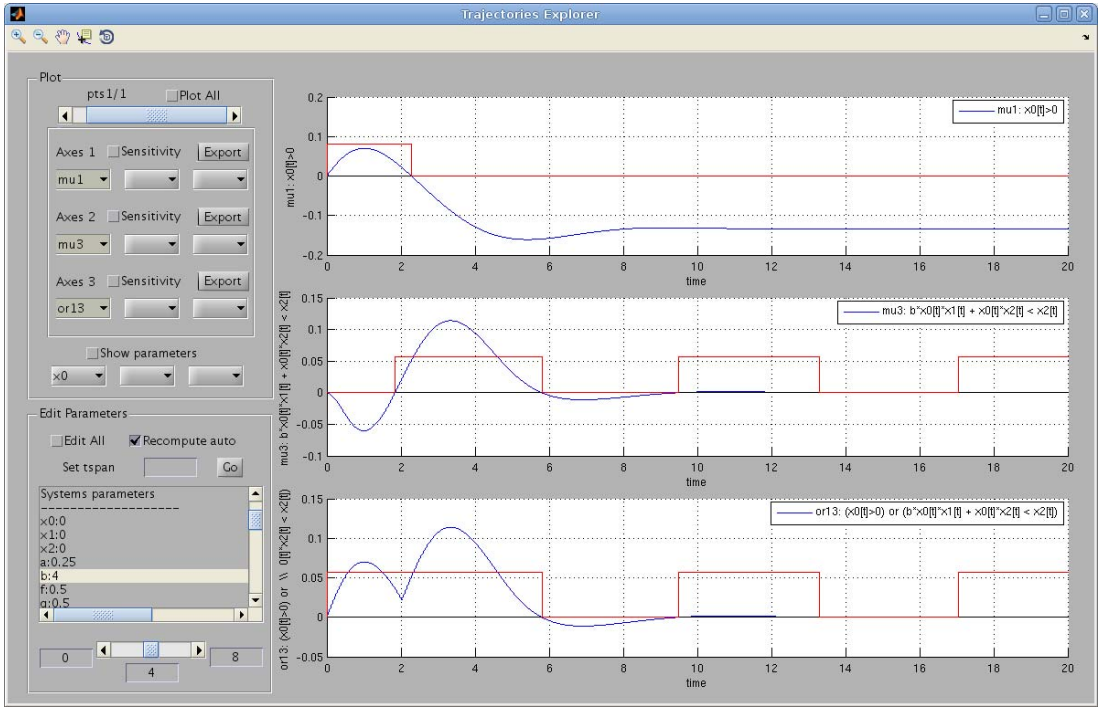
- [NM07]



Breach

http://www.eecs.berkeley.edu/~donze/breach_page.html

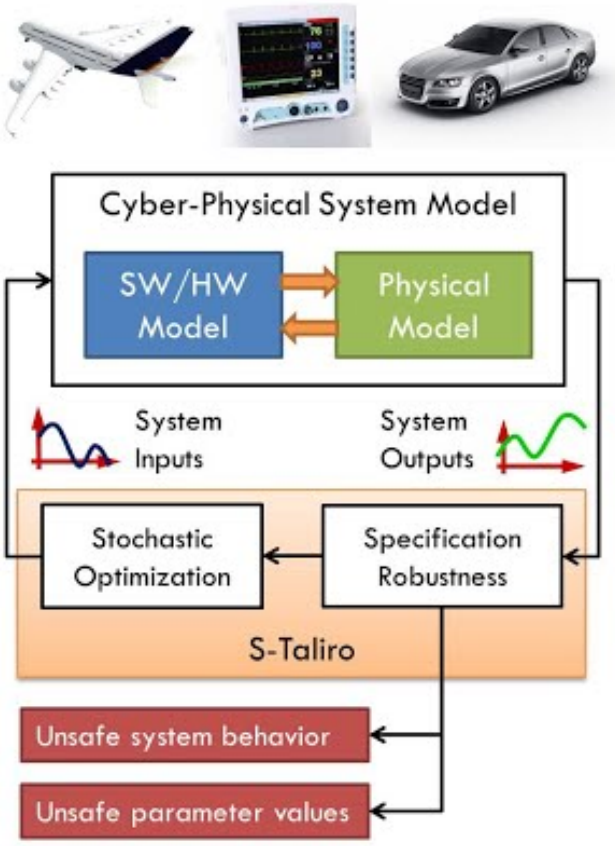
- MATLAB toolbox for
  - Simulation
  - Verification of temporal properties
  - Reachability
- STL with qualitative and quantitative semantics
  - Correctness
  - Robustness
- [Don10]



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
- [FSU+12]



CPSGrader

http://cpsgrader.org/

- Auto grader for laboratory courses
  - STL-based *test benches*
  - Monitor simulation traces of student solutions for faults
- STL with quantitative semantics
  - Robustness
- [JDJ+14]

U-Check

- Model checking and parameter synthesis for STL against stochastic dynamical systems
  - Machine learning techniques
  - Tutorial this afternoon

- [BMS15]

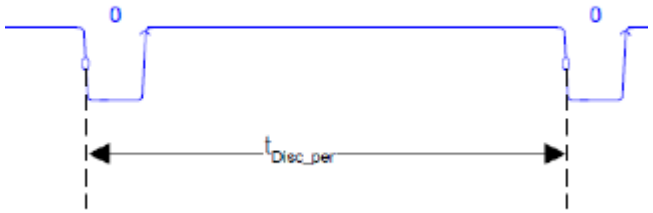
Applications

- Automotive
  - Correctness of DSI3 protocol implementation
  - Measuring DSI3 quantitative properties
  - Directed testing of powertrain control system
  - Robustness checking (S-TaLiRo) of
    - automatic transmission
    - powertrain control system
    - port fuel injected spark ignition systems
- Analog and mixed signal circuits
  - Correctness of DDR3 and Flash memory interfaces
- Music
  - Time-frequency domain properties
- Biology
  - Design of synthetic biological circuits
  - Logical characterization of an oscillator of the circadian clock in Ostreococcus Tauri
  - Qualitative properties of the behavior of cellular mechanisms with STL
  - Robust STL semantics for biological systems
    - Schlögl system
    - Incoherent type 1 feed-forward loops
    - Repressilator – synthetical biology clock
- Medical
  - Insuline pump usage parameter synthesis
  - Assisted ventilation
  - Discrimination of cardiac malfunction in ECG

Future Perspectives

Specification Languages

- Gap between informal requirements and formal languages



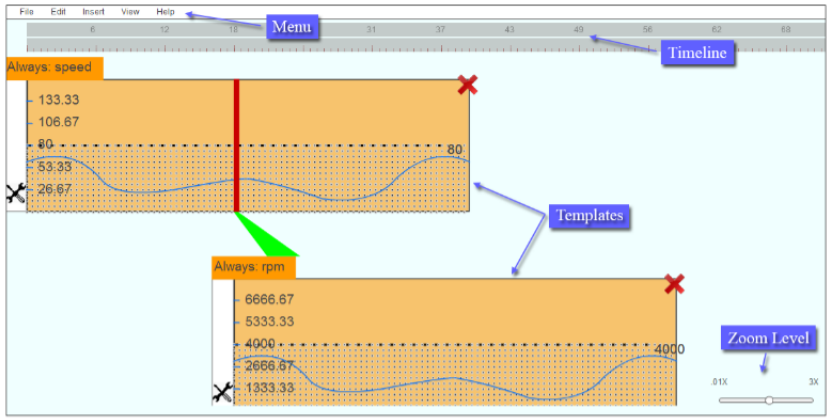
$$
\begin{aligned}
v_l &\equiv v \leq V_{low} \\
v_b &\equiv V_{low} \leq v \leq V_{high} \\
v_h &\equiv v \geq V_{high}
\end{aligned}
$$

$$
\begin{aligned}
\varphi_{shape} &\equiv \downarrow v_h \wedge (v_b \mathcal{U} v_l \mathcal{U} v_b \mathcal{U} v_h) \\
\varphi_{dur} &\equiv \downarrow v_h \wedge (\neg v_h \mathcal{U}_{I_{Disc\_Pulse}} \uparrow v_h) \\
\varphi_{pulse} &\equiv \varphi_{shape} \wedge \varphi_{dur}
\end{aligned}
$$

$$
\square(\varphi_{pulse} \rightarrow ((\neg\varphi_{pulse} \mathcal{U}_{I_{Disc\_per}} \varphi_{pulse}) \vee \square(\neg\varphi_{pulse})))
$$

- Steep learning curve for non-experts
- ViSpec

[DHF15]



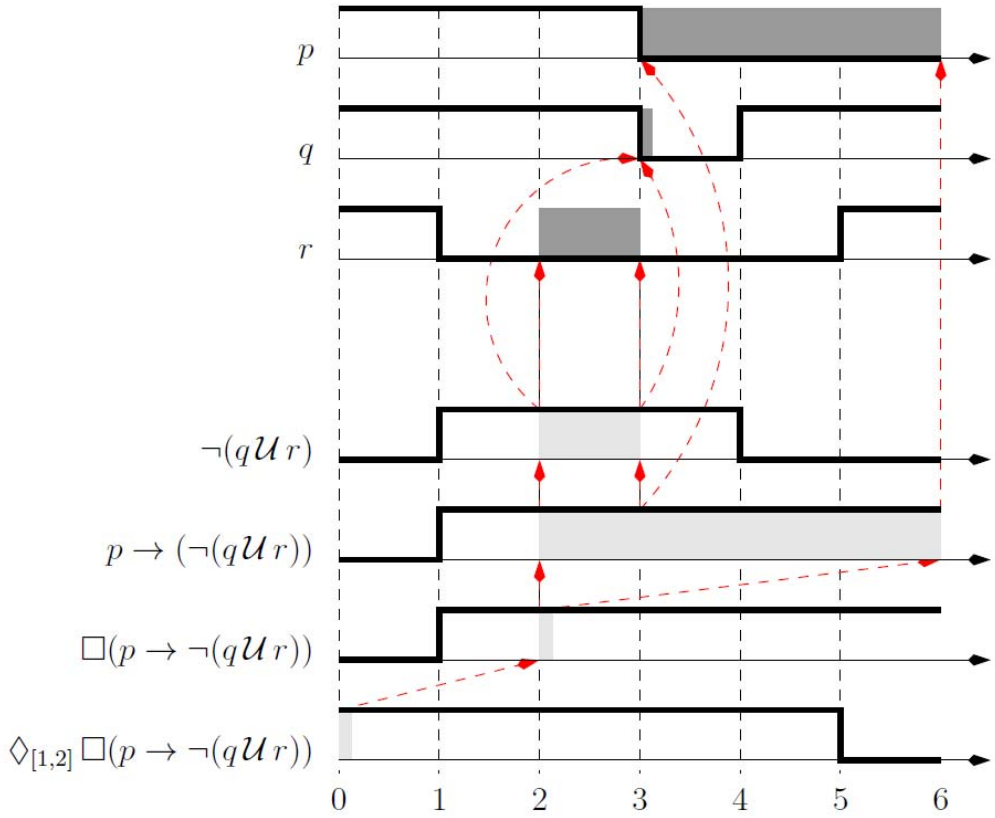
Specification Languages

- Specification libraries
  - Reuse
    - Same design, different phases
    - Same design, different context
  - Parameterization

- Expressiveness
  - Slew rates
  - Data integrity
  - Etc.

Fault Explanation and Localization

- Violation found!
  - How to help debugging?
- Automatic explanation and localization of faults
- Recent work [FMN15]
  - Idea of implicants
  - Computation of small implicants



Monitors Implemented on Hardware

- Monitoring + simulation is very scalable
  - Not always true!!!

- Mixed-signal simulation at SPICE level
  - Several ms of real time = hours to days of simulation time
  - A simulation trace size = hundreds of MB to tens of GB

- Solution:
  - Design emulation on FPGA HW
    - Precision vs. Efficiency

- Need for monitors implemented on FPGA hardware

HARMONIA Project

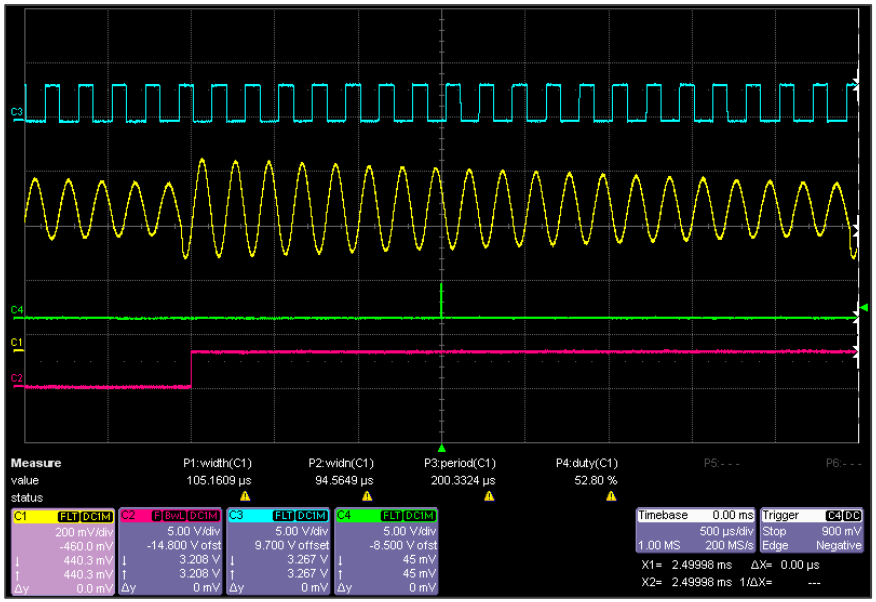
- Asserion-based Hardware Monitoring for Automotive Applications

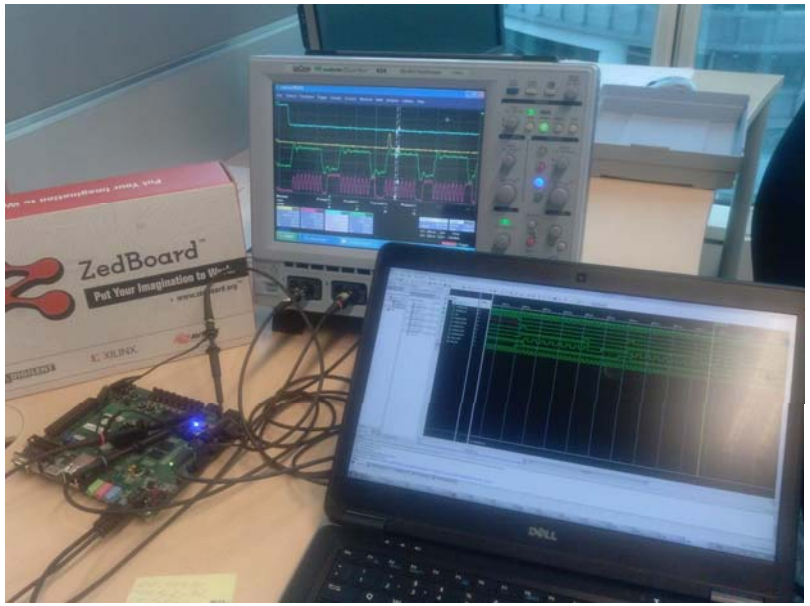
- National Austrian project
  - 2014 - 2017
  - AIT, Infineon Technologies AG, TU Wien
  - 2 PhD students

- STL monitors implemented on FPGA hardware
  - Qualitative and quantitative semantics
- Diagnosis
- Large automotive case study

HARMONIA Project

- Preliminary results





[JBG+15]

References

[MN04] O. Maler and D. Nickovic. Monitoring temporal properties of continuous signals. FORMATS/FTRTFT 2004.

[MN13] O. Maler and D. Nickovic. Monitoring properties of analog and mixed-signal circuits. STTT 2013.

[FP09] G. Fainekos and G. Pappas. Robustness of temporal logic specifications for continuous-time signals. Theor. Comput. Sci., 2009.

[ACM97] E. Asarin, P. Caspi and O. Maler. A Kleene theorem for timed automata. LICS, 1997.

[FMN+15] T. Ferrère, O. Maler, D. Nickovic and D Ulus. Measuring with timed patterns. CAV 2015

[UFA+14] D. Ulus, T. Ferrere, E. Asarin and O. Maler. Timed pattern matching. FORMATS 2014.

[DMB+12] A. Donzé, O. Maler, E. Bartocci, D. Nickovic, R. Grosu and S. Smolka. On temporal logic and signal processing. ATVA 2012.

[BDS+14] L. Brim, P. Dluhos, D. Safranek and T. Vejpustek. STL: Extending Signal Temporal Logic with signal-value freezing operator. Inf. Comput. 2014.

[ADM+11] E. Asarin, A. Donze, O. Maler and D. Nickovic. Parametric identication of temporal properties. RV 2011.

[HJK+15] I. Haghighi, A. Jones, Z. Kong, E. Bartocci, R. Grosu and C. Belta. SpaTeL: a novel spatial-temporal logic and its applications to networked systems. HSCC 2015.

References

[NM07] D. Nickovic and O. Maler. AMT: A property-based monitoring tool for analog systems. FORMATS 2007.

[Don10] A. Donzé. Breach, A toolbox for verication and parameter synthesis of hybrid systems. CAV 2010.

[FSU+12] G. Fainekos, S. Sankaranarayanan, K. Ueda, and H. Yazarel. Verication of automotive control applications using S-TaLiRo. ACC 2012.

[BMS15] L. Bortolussi, D. Milios and G. Sanguinetti. U-check: Model checking and parameter synthesis under uncertainty. QEST 2015.

[JDJ+14] G. Juniwal, A. Donzé, J. Jensen and S. Seshia. CPS-Grader: Synthesizing temporal logic testers for auto-grading an embedded systems laboratory. EMSOFT, 2014

[DHF15] A. Dokhanchi, B. Hoxha and G. Fainekos. Metric Interval Temporal Logic Specification Elicitation and Debugging, MEMOCODE, 2015.

[FMN15] T. Ferrère, O. Maler and D. Nickovic. Trace Diagnostics using Temporal Implicants. ATVA, 2015.

[JBG+15] S. Jaksic, E. Bartocci, R. Grosu, R. Kloibhofer, T. Nguyen and D. Nickovic. From Signal Temporal Logic to FPGA Monitors. MEMOCODE, 2015.