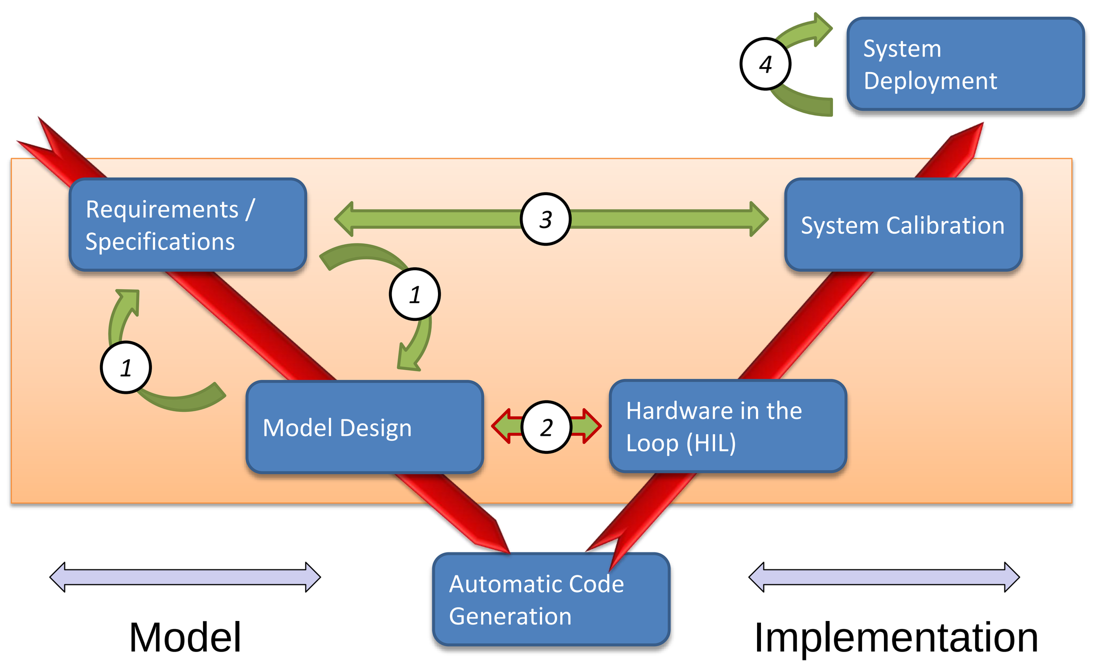
Conformance Testing as Falsification for Cyber-Physical Systems

Houssam Abbas(1), Bardh Hoxha(1), Georgios Fainekos(1), Jyotirmoy Deshmukh(2), James Kapinski(2) and Koichi Ueda(2)

(1) Arizona State University, CPS Lab (2) MBD Toyota Technical Center

Sponsors: CNS 1116136, CNS 1319560, IIP-0856090
Center for Embedded Systems, an NSF Industry/University Cooperative Research Center

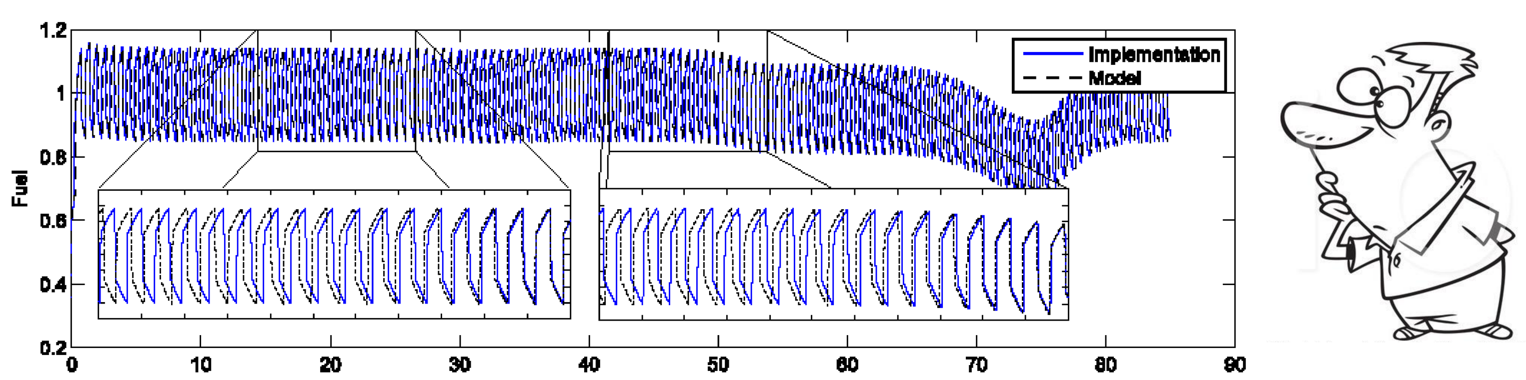
Model-Based Design V Process



Problem:
- How to formalize the notion that the outputs of the Implementation (right-hand side) "look like" those of the Model (left-hand side), both in signal values and timing characteristics?
- How to compute such a closeness measure?
- What can we infer about satisfied properties?

A generic conformance notion

In general, determining that the outputs of the Model and the Implementation are "close enough", i.e. conformant, is application-dependent and relies on expertise and ad-hoc rules.



We propose (T,J,τ,ε)-closeness as a generic conformance notion. This notion is appropriate for continuous-time, discrete-time, and hybrid-time systems.

Benefits of (T,J,τ,ε)-closeness as a generic notion of conformance:
- Only requires the ability to simulate the system – black boxes O.K.
- Can be tested early in the design cycle before all the instrumentation is in place for more targeted testing.
- Captures differences in timing characteristics as well as signal values
- Real-valued: can speak of a conformance degree and rank Implementations based on how well they conform to the Model.

Related work: distance between systems

- Input-Output Conformance (Tretmans) for discrete Labeled Transition Systems and Hybrid IOCO (Van Osch) for Hybrid Transition Systems.
- Woehrle et al. verify *conformance to a specification* (and not between systems)
- Modeling by Discrete Action Systems (Brandl et al.)
- Directional Haussdorf distance (Abate et al.)
- (τ,ε)-similar traces (Quesel)
- Skorokhod metrics with bijective re-timings (Caspi et al.) or set-valued re-timings (Davoren)
- Approximate synchronization and bisimulation (Julius et al.)

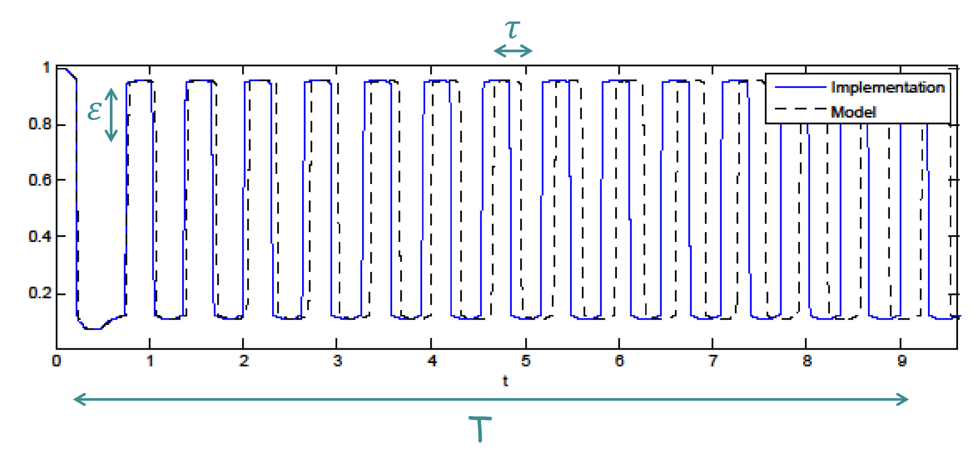
J.-D. Quesel. *Similarity, Logic, and Games: Bridging Modeling Layers of Hybrid Systems*. PhD thesis, Carl Von Ossietzky Universitat Oldenburg, 2013.
A.A. Julius and G.J. Pappas. Approximate equivalence and approximate synchronization of metric transition systems, *CDC 2006*

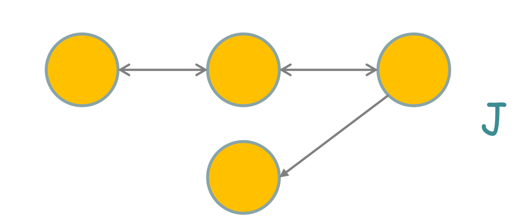
(T,J,τ,ε)-closeness

Consider two trajectories $\boldsymbol{y}$, and $\boldsymbol{y}'$ of Σ and Σ', respectively. Given $T>0$, $J>0, \tau>0$, and $\varepsilon>0$, we say $\boldsymbol{y}$ and $\boldsymbol{y}'$ are (T,J,τ,ε)–close if:

a) For all (t,j) in the support of $\boldsymbol{y}$ s.t. $t\le T$ and $j\le J$, there exists (s,j) in the support of $\boldsymbol{y}'$, such that $|t-s|<\tau$ and $||y(t,j)-y'(s,j)||<\varepsilon$

b) For all (t,j) in the support of $\boldsymbol{y}'$, s.t. $t\le T$ and $j\le J$, there exists (s,j) in the support of $\boldsymbol{y}$, such that $|t-s|<\tau$ and $||y'(t,j)-y(s,j)||<\varepsilon$

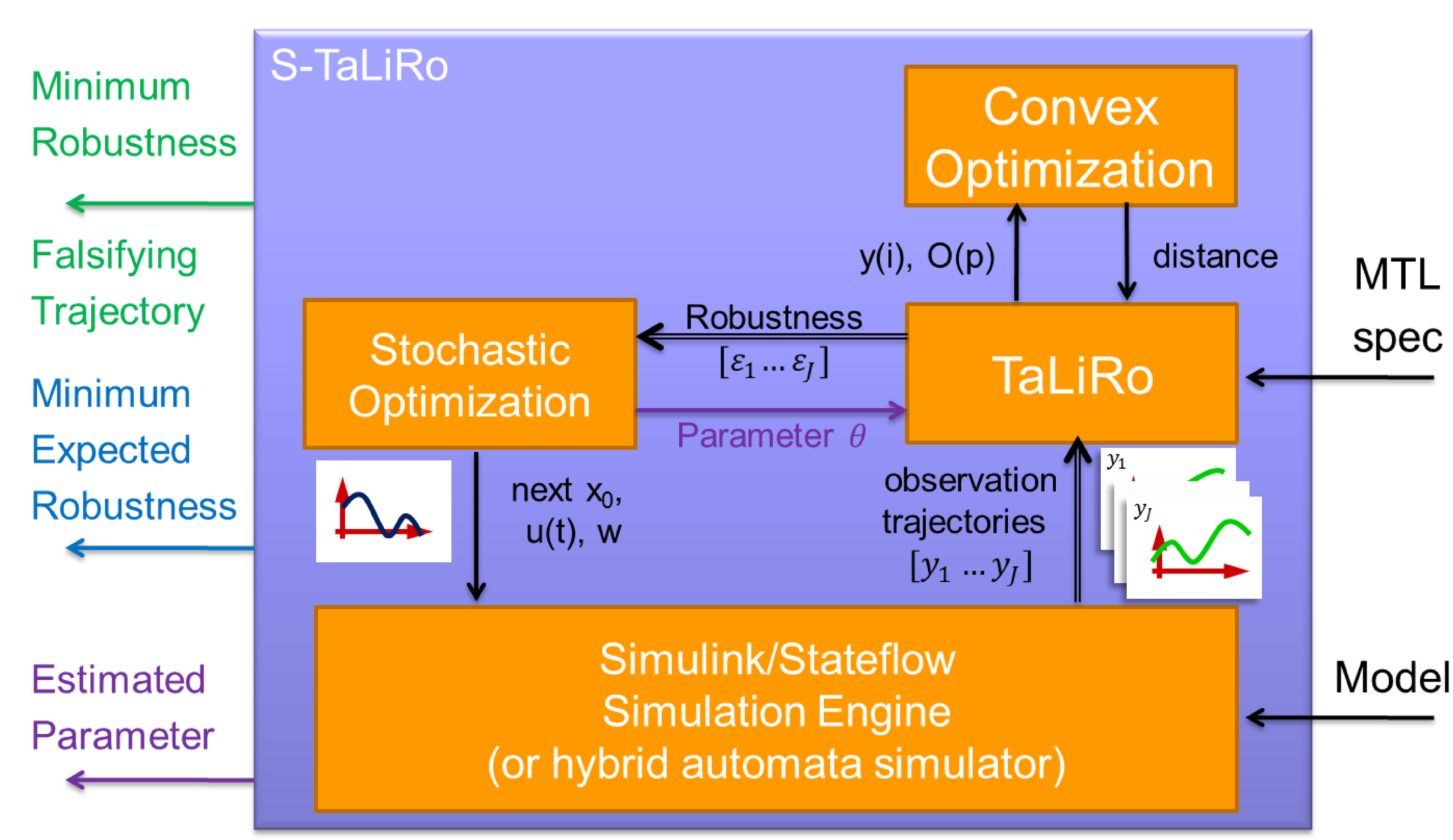




The largest (τ,ε) such that all trajectories of Σ and Σ' are (T,J,τ,ε)–close is the conformance degree between Σ and Σ'.

R. Goebel and A.R. Teel. Solutions to hybrid inclusions via set and graphical convergence with stability theory applications. *Automatica*, 2006.
R. G. Sanfelice and A. R. Teel. Dynamical properties of hybrid systems simulators. *Automatica*, 2010.

Implemented in the S-TaLiRo Toolbox



www.tinyurl.com/Staliro

High-fidelity engine model

56 state variables and black boxes

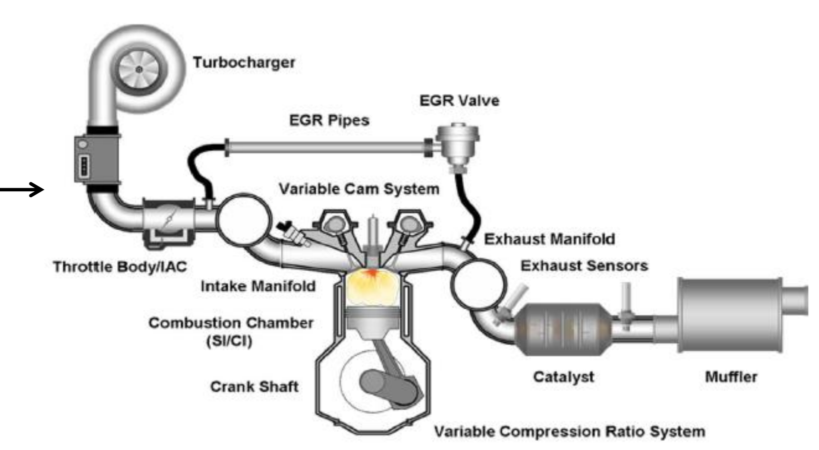
Modeling from physics first principles

LUTs, FSMs and regression models

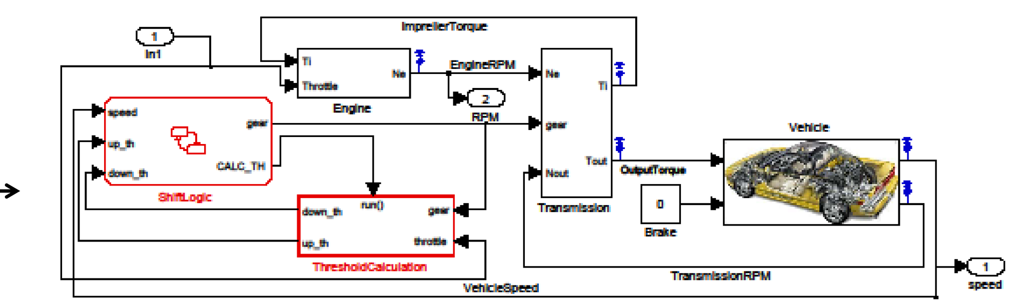
Input signal

Nonlinear dynamics

LUTs and FSMs



SimuQuest® engine model



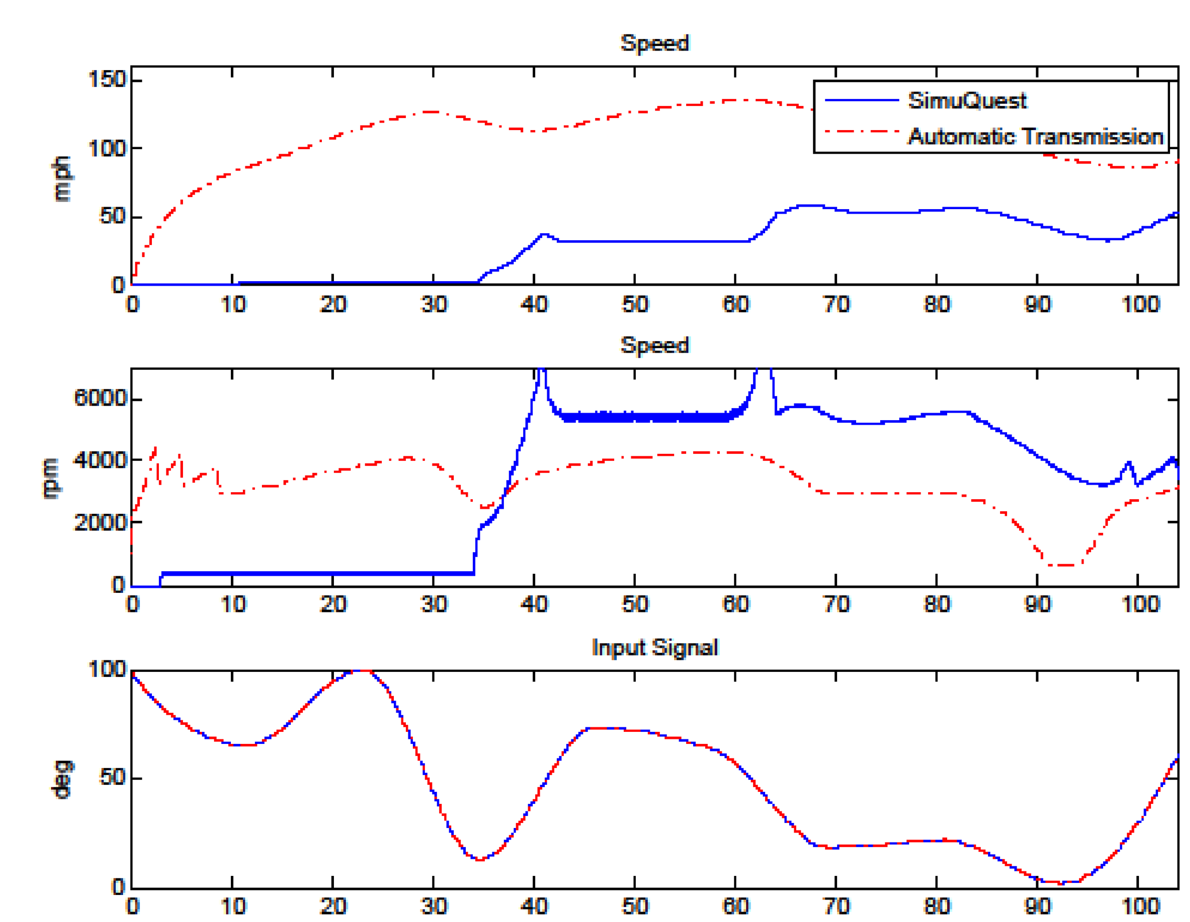
MathWorks® Automatic Transmission model

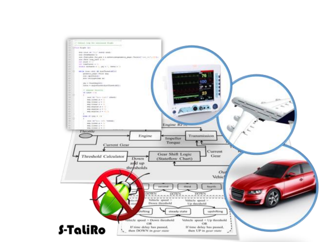
Conformance testing results

The (τ,ε) pairs are partially ordered, so must fix one parameter and optimize the other.
We fix τ and maximize ε, for pre-defined values of the horizon (T,J).

We use Simulated Annealing to maximize ε: it is a stochastic, global, derivative-free optimizer. It converges in probability to the global maximum with known bounds on the convergence rate.

H. Haario and E. Saksman. Simulated annealing in general state space. *Advances in Applied Probability*, 23:866–893, 1991.





Sample result: the two systems are $(104, J_{MAX}, 5*10^{-4}, 1)$–close with high probability.
This constitutes a *lower bound* on the true conformance degree.