Verifying Probabilistic Conformance for Cyber-Physical Systems

Yu Wang*, Mojtaba Zarei*, Borzoo Bonakdarpour**, Miroslav Pajic*

*Department of Electrical and Computer Engineering
Duke University

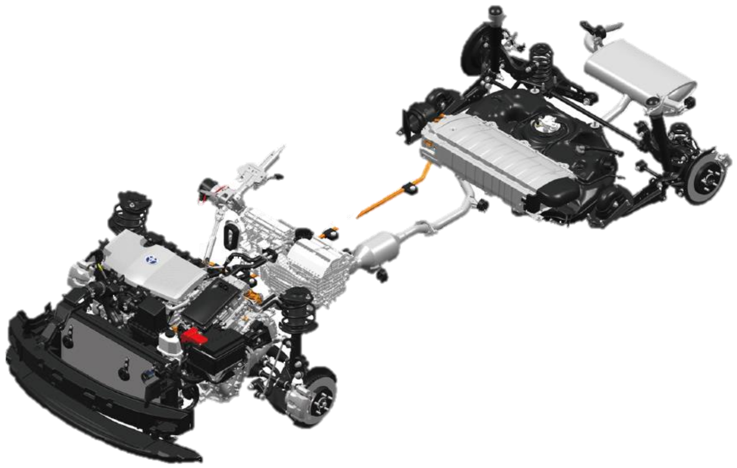
**Department of Computer Science
Michigan State University

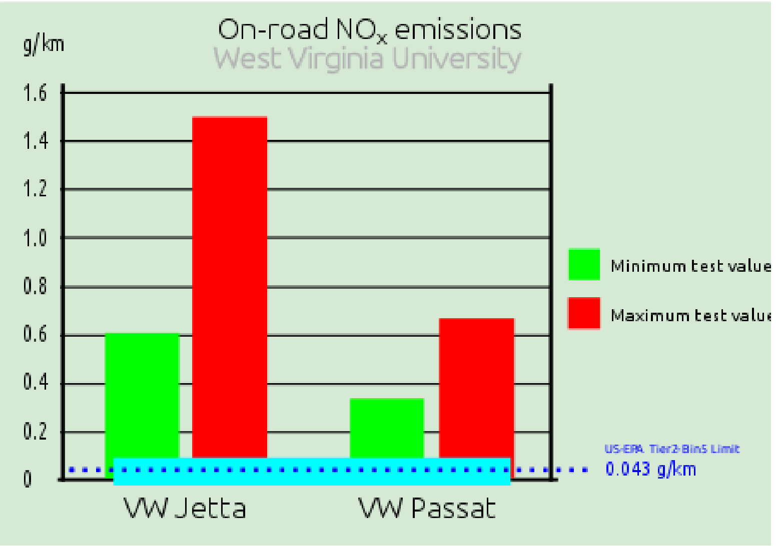
Duke UNIVERSITY | PRATT SCHOOL of ENGINEERING

Conformance of Cyber-Physical Systems (CPS)

Conformance: The behaviors of two CPS models are similar, so that the results from analyzing one model automatically transfer to the other.

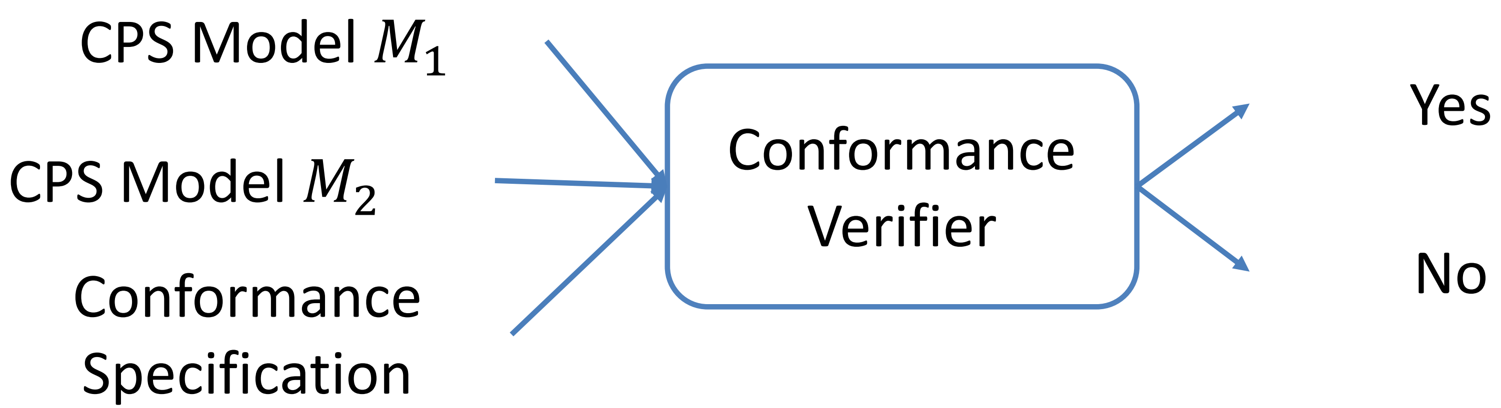
Model Simplification	System Update	System Testing





Formal Verification of Conformance

Can we design a software tool to verify conformance?



Need for Formal Methods:
1. How to model cyber-physical systems?
2. How to formally express conformance specifications?
3. How to develop mathematically-rigorous algorithms to verify?

Q1: How to Model CPS?

Duke PRATT SCHOOL *of* ENGINEERING

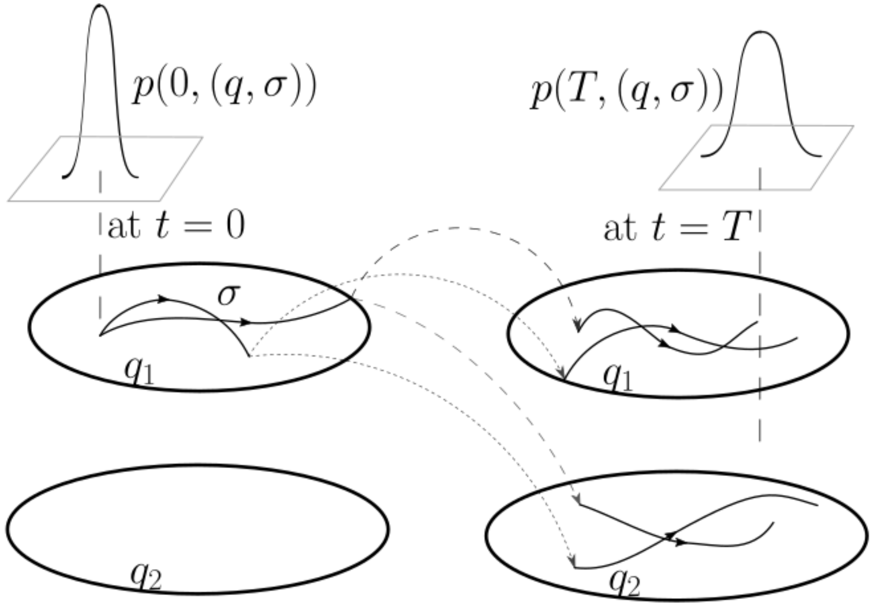
Probabilistic uncertain models (PUM): $\mathcal{S} = (\mathcal{X}, X^{init}, F, D, AP, L)$ where

- (Hybrid) state space $\mathcal{X}$, Initial state $X^{\text{init}} \in \mathcal{X}$
- Time-varying parameter $D(t)$ from **unknown** random processes
- (Hybrid) dynamics $X^+ = F(X(t), D(t))$
- *AP* is a set of labels, $\mathrm{L}: \mathcal{X} \rightarrow 2^{AP}$ is a labeling function

The PUM allows capturing

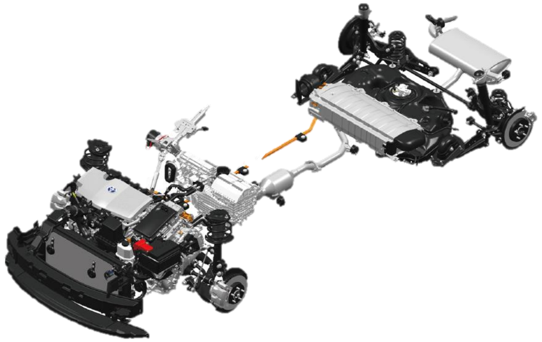
- Hybrid automata with probabilistic parameters (e.g., powertrain)
- Continuous-time Markov chains (e.g., queueing networks)

CPS dynamics are typically **hybrid** and **probabilistic**.

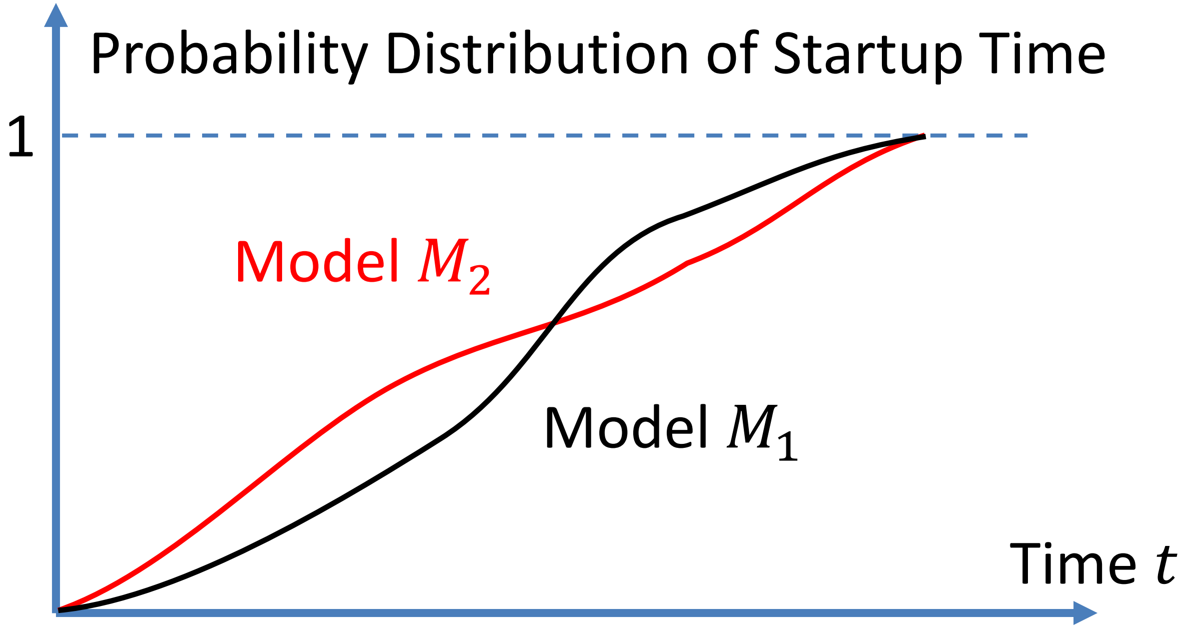


Q2: How to Formally Express Conformance?

Conformance is a **meta-specifications** of (infinitely) many simple specifications.



- M_1: Detailed Dynamical Model
- M_2: Simplified Dynamical Model



Probabilistic Conformance in Startup Time: If the probability of startup by time t is (almost) equal **for any t** for both models M_1 and M_2.

Specify Conformance by Parametrized STL Formulas

Traditionally, **simple specifications** are formally expressible by **STL** formulas.

We express **meta-specifications** for conformance by **parametrized STL** formulas.

Signal Temporal Logic (STL):

$$\varphi ::= a \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi\,\mathcal{U}_{[t_1,t_2]}\varphi$$

- a: atomic proposition,
- $t_1, t_2 \in \mathbb{Q}$ with $t_2 > t_1 \geq 0$.

Probabilistic Conformance in Startup Time:
$\forall t > 0, \left|\mathbf{Pr}_{\sigma_1 \sim \mathcal{M}_1}\left(\sigma_1 \vDash \Diamond_{[0,t]}\, \text{started}\right) - \mathbf{Pr}_{\sigma_2 \sim \mathcal{M}_2}\left(\sigma_2 \vDash \Diamond_{[0,t]}\, \text{started}\right)\right| < c$

Examples

- Reach to goal: $\Diamond_{[t_1,t_2]}\,\text{goal} = \mathtt{True}\,\mathcal{U}_{[t_1,t_2]}\text{goal}$
- Stay Safe: $\Box_{[t_1,t_2]}\text{safe} = \neg\left(\Diamond_{[t_1,t_2]} \neg\, \text{safe}\right)$

Q3: How to Verify Conformance?

Probabilistic Conformance in Startup Time:
$\forall t > 0, \left|\mathbf{Pr}_{\sigma_1 \sim \mathcal{M}_1}\left(\sigma_1 \vDash \Diamond_{[0,t]} \text{started}\right) - \mathbf{Pr}_{\sigma_2 \sim \mathcal{M}_2}\left(\sigma_2 \vDash \Diamond_{[0,t]} \text{started}\right)\right| < c$

Challenge: Traditional verification methods can only handle unparametrized STL formulas.

Conformance Definition: For a constant $c > 0$, if $\forall \vec{d}.\ \ |\mathbf{Pr}_{\sigma_1 \sim \mathcal{M}_1}(\sigma_1 \vDash \phi_{\vec{d}}) - \mathbf{Pr}_{\sigma_2 \sim \mathcal{M}_2}(\sigma_2 \vDash \phi_{\vec{d}})| < c.$

We develop a new verification method for **monotonically** parametrized STL formulas.

Statistical Verification of Probabilistic Conformance

The parametrized STL formula $\phi_{\vec{d}}$ is monotonic if and only if $\mathbf{Pr}_{\sigma_i \sim \mathcal{M}_i}(\sigma_i \vDash \phi_{\vec{d}})$ for $i = 1,2$ increases/decreases with the entries of $\vec{d}$.

PUM M_1

PUM M_2

Monotonically parametrized STL formula ϕ_d

Statistical Verifier

Significance level (error probability) $\alpha > 0$

Yes

No

Advantages:

- Tolerate Unknowns
- Scalability
- Probabilistic Guarantee

For any pre-given $\alpha > 0$, the result is correct with probability at least $1 - \alpha$.

Step 1: Hypothesis Testing on Distribution Difference

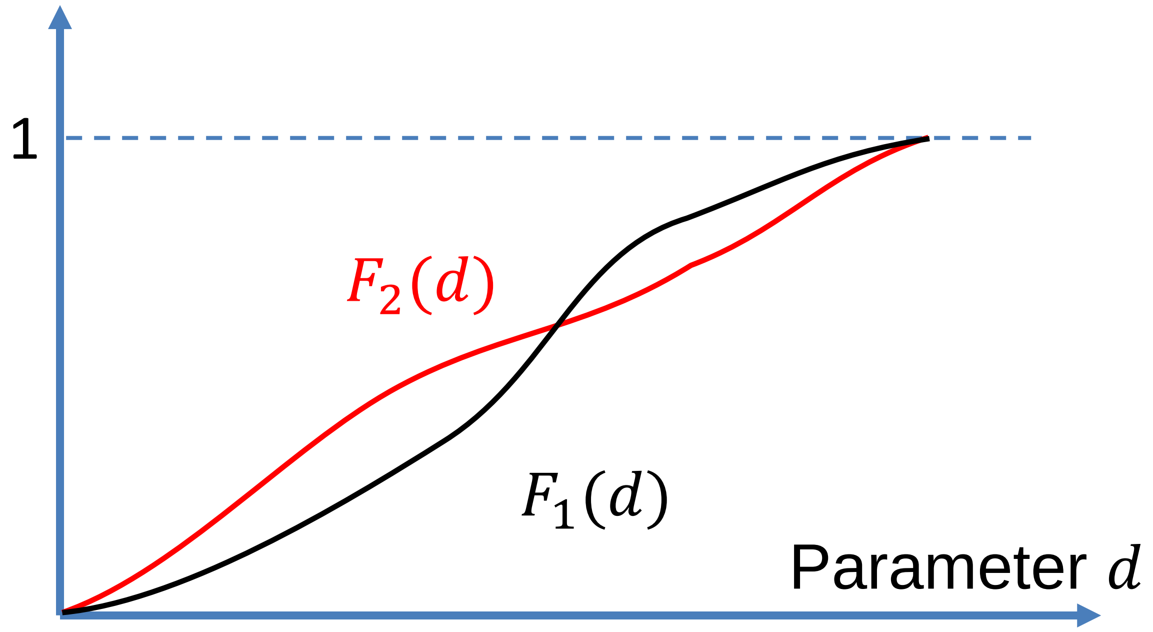
For simplicity, let the parameter d be a scalar.

If ϕ_d is monotonically parametrized, then $F_i(d) = \mathbf{Pr}_{\sigma_i \sim \mathcal{M}_i}(\sigma_i \vDash \phi_d)$ are two cumulative distribution functions.

Conformance requires $\|F_1 - F_2\|_\infty < c$.

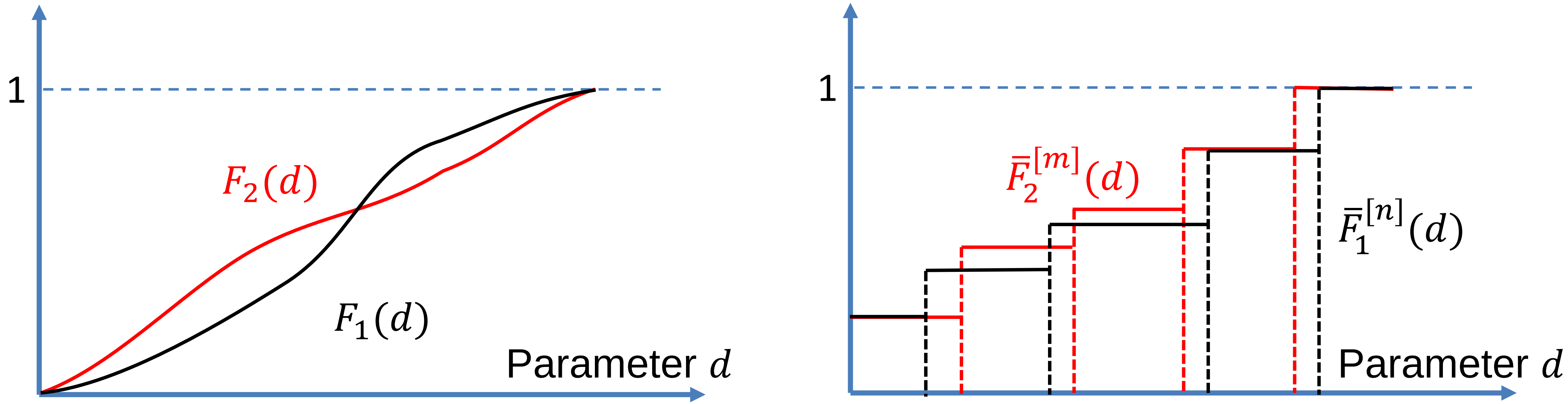
Hypothesis Testing:

$$\begin{cases} H_0\colon \|F_1 - F_2\|_\infty < c \\ H_1\colon \|F_1 - F_2\|_\infty \geq c \end{cases}$$



Step 2: Estimated Distribution Difference from Samples

F_1, F_2 are estimable by empirical distributions $\bar{F}_1, \bar{F}_2$



$\bar{F}_1^{[n]}(d) = \frac{1}{n}\sum_{i=1}^{n} \mathbf{I}\left(X^{(i)} \leq d\right)$ and $\bar{F}_2^{[m]}(d) = \frac{1}{m}\sum_{i=1}^{m} \mathbf{I}\left(Y^{(i)} \leq d\right)$

$$\left\|\bar{F}_1^{[n]} - \bar{F}_2^{[m]}\right\|_\infty \to \|F_1 - F_2\|_\infty \text{ as } n, m \to \infty$$

Step 3: Bounding Finite-Sample Estimation Error

Let $\delta_{n,m} = \|(\bar{F}_1^{[n]} - F_1) - (\bar{F}_2^{[m]} - F_2)\|_\infty$,
then $\left\|\bar{F}_1^{[n]} - \bar{F}_2^{[m]}\right\|_\infty - \|F_1 - F_2\|_\infty \in [-\delta_{n,m}, \delta_{n,m}]$

Theorem 1: $\delta_{n,m}\sqrt{mn/(m+n)}$ obeys the Kolmogorov-Smirnov distribution $\boldsymbol{KS}$, which **is independent of** the form of F_1, F_2

The estimation error of $\left\|\bar{F}_1^{[n]} - \bar{F}_2^{[m]}\right\|_\infty$ for $\|F_1 - F_2\|_\infty$ is statistically bounded even if we don't know F_1, F_2!

If $\left\|\bar{F}_1^{[n]} - \bar{F}_2^{[m]}\right\|_\infty = \lambda < c$, then $\|F_1 - F_2\|_\infty < c$ with significance level

$$\alpha_{n,m} = 1 - \boldsymbol{KS}\left((\lambda - c)\sqrt{mn/(m+n)}\right)$$

Step 4: Conformance Verification Algorithm

Algorithm to check conformance $\|F_1 - F_2\|_\infty < c$:

Input Desired significance level $\alpha > 0$

Do drawing new samples from F_1, F_2.

Until $\alpha_{n,m} > \alpha$

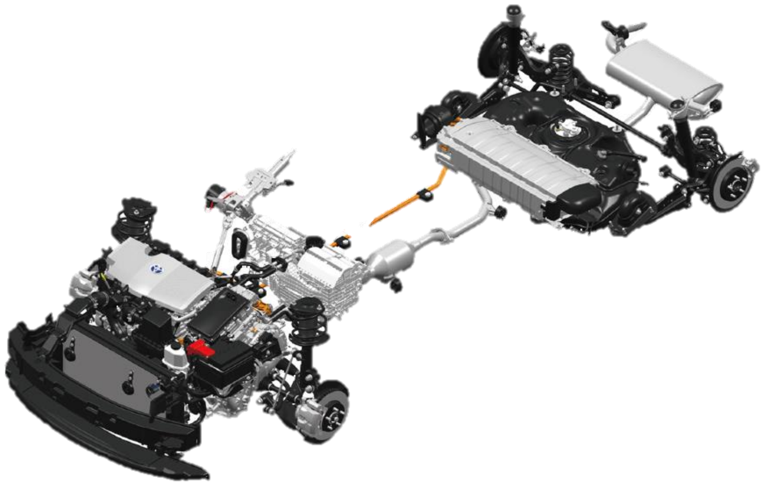
Return True If $\left\|\bar{F}_1^{[n]} - \bar{F}_2^{[m]}\right\|_\infty < c$ and **False** otherwise.

Theorem 2: **Algorithm** terminates with probability 1 if $\|F_1 - F_2\|_\infty \neq c$.

Theorem 3: **Algorithm**'s return has significance level α.

Case Study I: Toyota Powertrain Benchmark

Duke
PRATT SCHOOL of ENGINEERING



Powertrain = Car Engine + Embedded Controller

- $\mathcal{M}_d$: Detailed PUM with **nonlinear** engine dynamics
- $\mathcal{M}_s$: Simplified PUM with **polynomial** engine dynamics (by Taylor expansion)

Conformance in Startup Time of Detailed/Simplified models of $\mathcal{M}_d/\mathcal{M}_s$ powertrain system.

$$\forall \tau \geq 0. \left| \mathbf{Pr}_{\sigma_s \sim \mathcal{M}_s}\left(\sigma_s \vDash \Diamond_{[0,\tau]}(e_{A/F} < 0.05)\right) - \mathbf{Pr}_{\sigma_d \sim \mathcal{M}_d}\left(\sigma_d \vDash \Diamond_{[0,\tau]}(e_{A/F} < 0.05)\right) \right| < c$$

Case Study I: Results

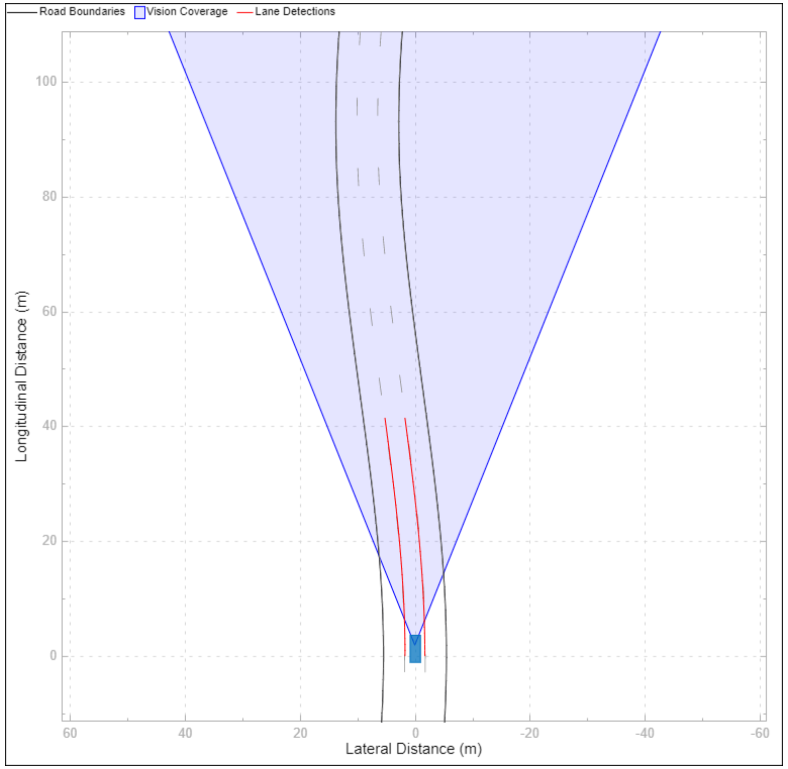
Duke PRATT SCHOOL of ENGINEERING

Conformance in Startup Time of Detailed/Simplified models of $\mathcal{M}_d/\mathcal{M}_s$ powertrain system.

$$\forall \tau \geq 0.\ \left|\mathbf{Pr}_{\sigma_s \sim \mathcal{M}_s}\left(\sigma_s \vDash \Diamond_{[0,\tau]}(e_{A/F} < 0.05)\right) - \mathbf{Pr}_{\sigma_d \sim \mathcal{M}_d}\left(\sigma_d \vDash \Diamond_{[0,\tau]}(e_{A/F} < 0.05)\right)\right| < c$$

c	Confidence	Samples	Time (s)	Result
0.40	0.99	3.9e+01	1.8e-02	F
0.40	0.95	1.9e+01	4.4e-03	F
0.25	0.99	2.5e+01	4.6e-03	F
0.25	0.95	1.3e+01	2.2e-03	F
0.10	0.99	1.8e+01	3.6e-03	F
0.10	0.95	9.0e+00	1.6e-03	F
0.05	0.99	1.6e+01	2.8e-03	F
0.05	0.95	8.0e+00	1.3e-03	F

Case Study II: Lane-Keeping Controller



System = Car + Lane-Keeping Controller (for a detected lane).

- $\mathcal{M}_{\mathrm{MPC}}$: PUM of a car with (tradition) model predictive controller
- $\mathcal{M}_{\mathrm{NN}}$: PUM of a car with neural network controller

Conformance in Track Error of $\mathcal{M}_{\mathrm{MPC}}$/$\mathcal{M}_{\mathrm{NN}}$-based Lane-Keeping Controllers.

$$\forall \tau \geq 0.\ \left|\mathbf{Pr}_{\sigma_1 \sim \mathcal{M}_{\mathrm{NN}}}(\sigma_1 \vDash \Diamond_{[0,\tau]}(|e_y^{\mathrm{NN}}| < \gamma)) - \mathbf{Pr}_{\sigma_2 \sim \mathcal{M}_{\mathrm{MPC}}}(\sigma_2 \vDash \Diamond_{[0,\tau]}(|e_y^{\mathrm{MPC}}| < \gamma))\right| < c$$

Case Study II: Results

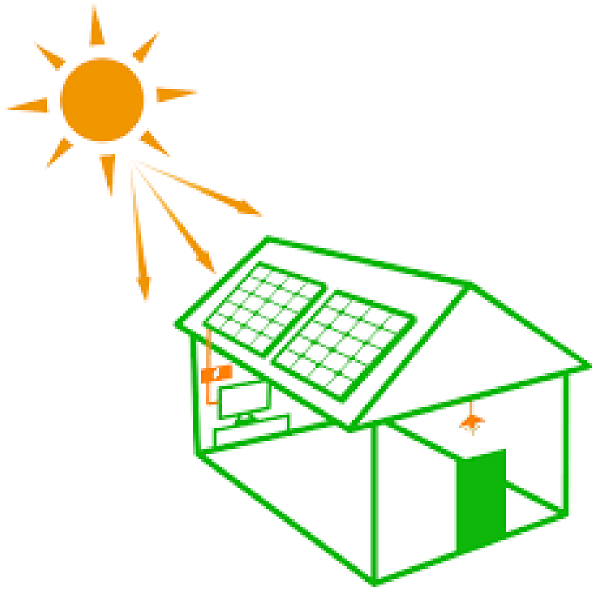
Duke PRATT SCHOOL of ENGINEERING

Conformance in Track Error of MPC/NN-based Lane-Keeping Controllers.

$$\forall \tau \geq 0.\ \left|\mathbf{Pr}_{\sigma_1 \sim \mathcal{M}_{\mathrm{NN}}}(\sigma_1 \vDash \Diamond_{[0,\tau]}(|e_y^{\mathrm{NN}}| < \gamma)) - \mathbf{Pr}_{\sigma_2 \sim \mathcal{M}_{\mathrm{MPC}}}(\sigma_2 \vDash \Diamond_{[0,\tau]}(|e_y^{\mathrm{MPC}}| < \gamma))\right| < c$$

c	Confidence	Samples	Time (s)	Result
0.40	0.99	1.0e+04	9.6e+00	T
0.40	0.95	3.6e+03	2.0e+00	T
0.25	0.99	9.5e+02	3.2e-01	F
0.25	0.95	2.5e+02	5.9e-02	F
0.10	0.99	2.1e+02	4.2e-02	F
0.10	0.95	1.2e+02	2.2e-02	F
0.05	0.99	1.3e+02	2.5e-02	F
0.05	0.95	7.3e+01	1.4e-02	F

Case Study III: Power System



Power System = 100kW Photovoltaic Array + 25kV Power Grid + DC-DC Boost Converter + Voltage Source Converter.

- $\mathcal{M}_{\mathrm{d}}$: PUM with **detailed** dynamics
- $\mathcal{M}_{a}$: PUM with **average** dynamics (by filtering out high-frequency responses)

Conformance in Voltage Deviation of Detailed/Simplified models $\mathcal{M}_d/\mathcal{M}_a$ of Power Converter.

$$\forall \gamma \geq 0.\ \left|\mathbf{Pr}_{\sigma_d \sim \mathcal{M}_d}(\sigma_d \vDash \square_{[0.5,2]}(|e_{vdc_d}| < \gamma)) - \mathbf{Pr}_{\sigma_a \sim \mathcal{M}_a}(\sigma_a \vDash \square_{[0.5,2]}(|e_{vdc_a}| < \gamma))\right| < c$$

Case Study III

Duke PRATT SCHOOL of ENGINEERING

Conformance in Voltage Deviation of Detailed/Simplified models $\mathcal{M}_d/\mathcal{M}_a$ of Power Converter.

$$\forall\gamma \geq 0.\ \left|\mathbf{Pr}_{\sigma_d\sim\mathcal{M}_d}(\sigma_d \vDash \square_{[0.5,2]}(\,|e_{vdc_d}| < \gamma)) - \mathbf{Pr}_{\sigma_a\sim\mathcal{M}_a}(\sigma_a \vDash \square_{[0.5,2]}(\,|e_{vdc_a}| < \gamma))\right| < c$$

c	Confidence	Samples	Time (s)	Result
0.40	0.99	3.9e+01	1.0e-02	F
0.40	0.95	1.9e+01	6.9e-03	F
0.25	0.99	2.5e+01	5.3e-03	F
0.25	0.95	1.3e+01	3.3e-03	F
0.10	0.99	1.8e+01	3.8e-03	F
0.10	0.95	9.0e+00	1.8e-03	F
0.05	0.99	1.8e+01	3.2e-03	F
0.05	0.95	8.0e+00	1.3e-03	F

Thank you

Code: https://gitlab.oit.duke.edu/cpsl/conformance