

Cyberphysical Systems: Compositionality and Opacity

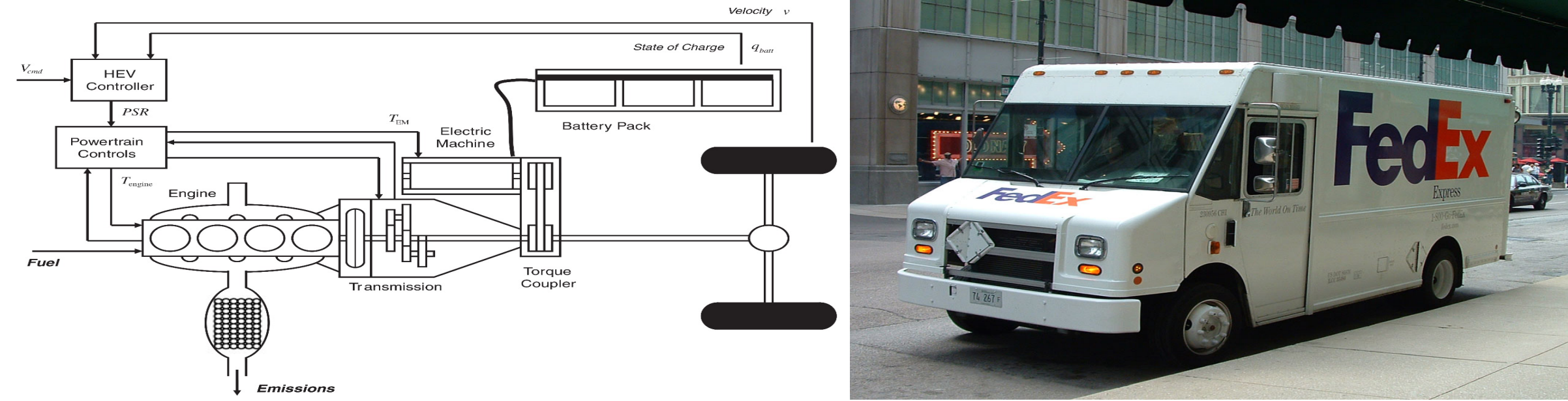
James Ferlez, Bhaskar Ramasubramanian, Rance Cleaveland, and Steven I. Marcus



INSTITUTE FOR
SYSTEMS RESEARCH
A. JAMES CLARK SCHOOL OF ENGINEERING

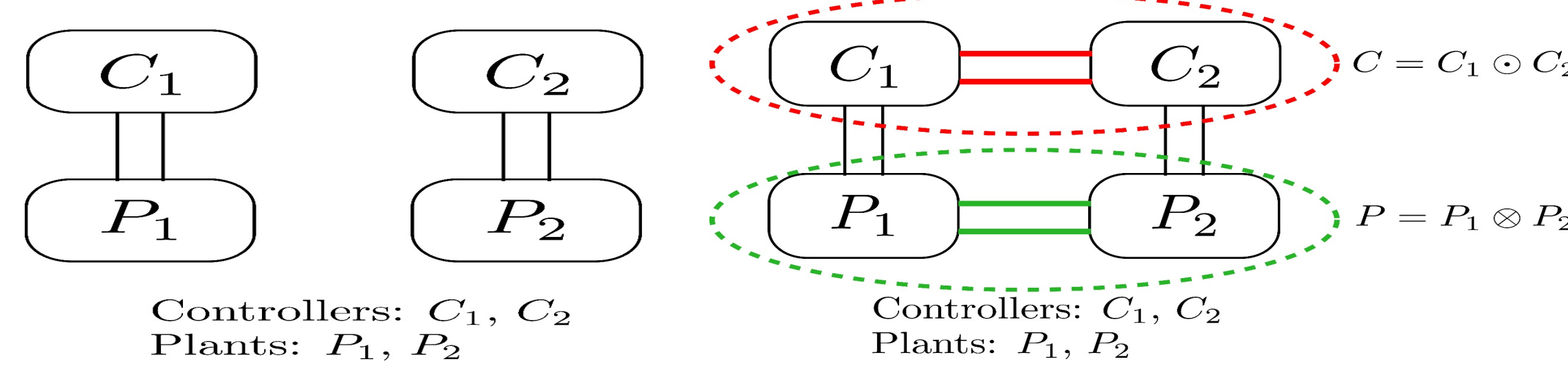
Cyberphysical Systems are Compositional

- For example, hybrid powertrains (see e.g. [3]):



Compositional Reasoning for CPSs

Need to reason about a complicated system based on models/behaviors of components:



- Can the composed system be analyzed in a rigorous way?

Algebraic Composition of Transition Systems

Famously, Milner [2] devised synchronization trees for labeled transition systems (subsequently known as **Process Algebra**):

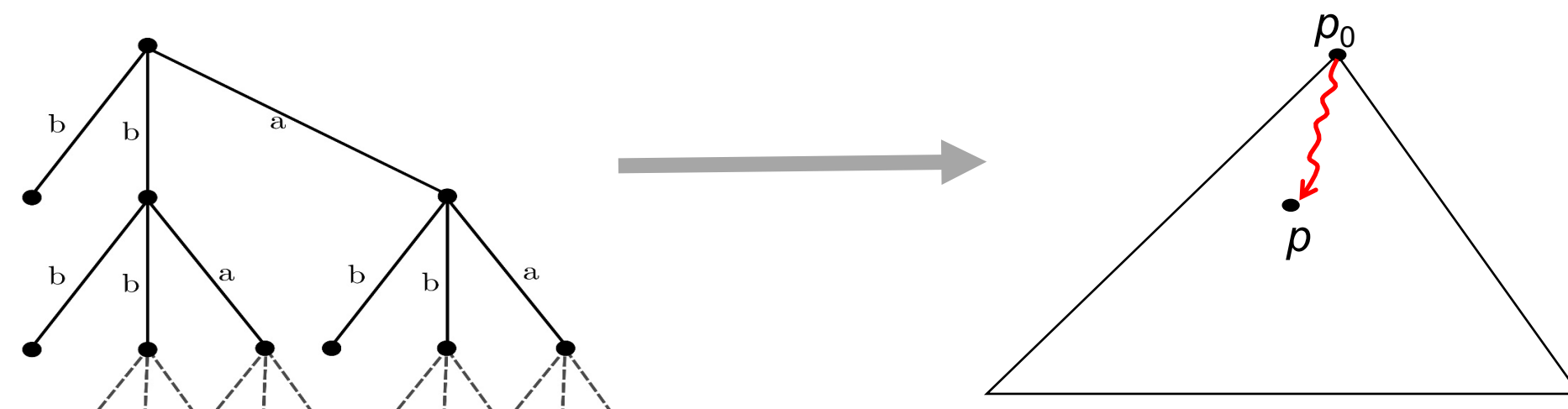
Definition:

A **Synchronization Tree (ST)** over a set of labels L is a tuple (V, E, \mathcal{L}) where (V, E) is an undirected, connected, acyclic graph with a specially identified root node r and \mathcal{L} is a function $\mathcal{L}: E \rightarrow L \cup \{\varepsilon\}$.

- Bisimulation** is a natural (observational) notion of equivalence between trees.
- Composition:** algebraic operations on synchronization trees. E.g. SOS rules:

$$\frac{P \xrightarrow{a} P' \quad a \notin S}{P|S|Q \xrightarrow{a} P'|S|Q} \quad \frac{Q \xrightarrow{a} Q' \quad a \notin S}{P|S|Q \xrightarrow{a} P|S|Q'} \quad \frac{P \xrightarrow{a} P' \quad Q \xrightarrow{a} Q' \quad a \in S}{P|S|Q \xrightarrow{a} P'|S|Q'}$$

- Idea:** generalize synchronization trees to enable algebraic treatment of CPSs.



Generalized Synchronization Trees (GSTs)

Definition:

A **tree** is a partially ordered set (P, \leq) with the following two properties:

- 1) There is a $p_0 \in P$ s.t. $p_0 \leq p$ for all $p \in P$. p_0 is the root of the tree.
- 2) For each $p \in P$, the set $\{p' \in P \mid p' \leq p\}$ is linearly ordered by \leq .

Definition:

A **Generalized Synchronization Tree (GST)** [1] over a set of labels L is a tree (P, \leq) along with a labeling function $\mathcal{L}: P \setminus \{p_0\} \rightarrow L$.

Different Notions of Bisimulation for GSTs

Let $G_P = (P, p_0, \leq_P, \mathcal{L}_P)$ and $G_Q = (Q, q_0, \leq_Q, \mathcal{L}_Q)$ be two GSTs. Furthermore, let $(p, p') \stackrel{\text{def}}{=} \{r \in P \mid p \leq r \leq p'\}$.

Definition:

G_P **weakly simulates** G_Q if there is a relation $R \subseteq P \times Q$ such that $(p_0, q_0) \in R$ and for any $(p, q) \in R$ and $q' \geq q$, there is a $p' \geq p$ such that $(p', q') \in R$, and there is an order-preserving bijection $\lambda: (p, p') \rightarrow (q, q')$.

A new, semantically different kind of simulation for GSTs [1]:

Definition:

G_P **strongly simulates** G_Q if there is a relation $R \subseteq P \times Q$ such that $(p_0, q_0) \in R$ and for any $(p, q) \in R$ and $q' \geq q$, there is a $p' \geq p$ s.t. $(p', q') \in R$, and there is an order-preserving bijection $\lambda: (p, p') \rightarrow (q, q')$ such that $\forall r \in (p, p'). (r, \lambda(r)) \in R$.

Bisimulation and Hennessy-Milner Logic

Definition:

Hennessy-Milner Logic (HML) is a set of formulas defined inductively by the rule:

$$\varphi ::= \perp \mid \varphi_1 \rightarrow \varphi_2 \mid \Box \varphi.$$

HML has a special connection to bisimulation between STs:

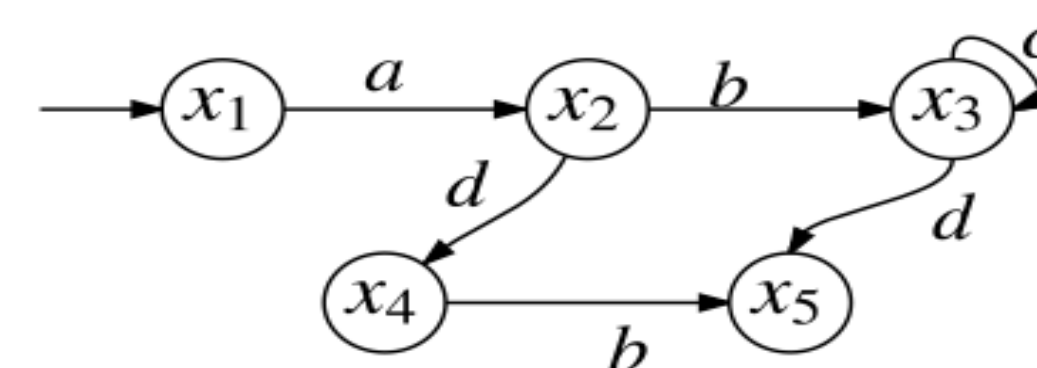
- If two STs are bisimilar, then they satisfy the same HML formulas;
- If two *image-finite* STs satisfy the all of the same HML formulas, then they are bisimilar.

Similar relationships are currently being investigated for weak and strong bisimulation.

CPS Security: Motivation

- Information critical to nominal operation must be safeguarded.
- CPSs integrate communication, control, and computation with physical processes.
- \Rightarrow remote cyber attacks can cause physical damage to the system.
- Opacity** [4]: Can a passive adversarial observer infer a “secret” of the system by observing the system behavior?
- Current state of the art:** Opacity for Discrete Event Systems (DESs) [5].
- Limitation:** States in a DES are discrete.
- Present Work:** formulated centralized and decentralized notions of opacity for continuous state systems.
- Future:** extend to nonlinear and hybrid systems.

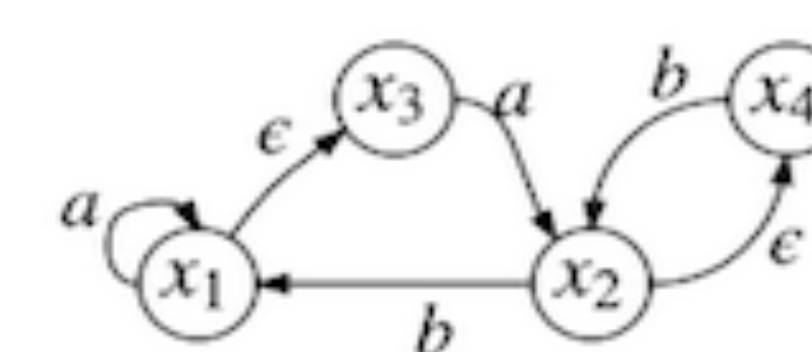
Opacity in Discrete Event Systems



$$\Sigma_o = \{a, b, c\}$$

$$\text{LBO: } L_s = \{abd\}, L_{ns} = \{abcc^*d, adb\}$$

$$\text{Not LBO: } L_s = \{abcd\}, L_{ns} = \{adb\}$$



$$\Sigma_o = \{a, b\}$$

$$\text{ISO: } X_s = \{x_3\}, X_{ns} = X \setminus X_s$$

$$\text{Not ISO: } X_s = \{x_1\}, X_{ns} = X \setminus X_s$$

Language Based Opacity (LBO) \equiv Initial State Opacity (ISO) [5]

Opacity for Linear Systems: 1 Adversary

- A new framework for opacity in continuous state CPSs [6]:

$$x(t+1) = Ax(t) + Bu(t)$$

$$x(0) = x_0 \in X_0$$

$$y(t) = Cx(t)$$

- $\mathcal{K} \subseteq \mathbb{Z}_+$: times at which adversary observes system.
- $X_s, X_{ns} \subseteq X_0$: sets of initial secret, nonsecret states.
- $A \in \mathbb{R}^{n \times n}, B \in \mathbb{R}^{n \times m}, C \in \mathbb{R}^{p \times n}$.

Definition:

Given $X_s, X_{ns} \subseteq X_0$ and $k \in \mathcal{K}$, X_s is **strongly k-initial state opaque (k-ISO)** with respect to X_{ns} if for every $x_s(0) \in X_s$ and admissible controls $u_s(0), \dots, u_s(k)$, there exists $x_{ns}(0) \in X_{ns}$ and admissible controls $u_{ns}(0), \dots, u_{ns}(k)$, such that $y_s(k) = y_{ns}(k)$. X_s is **strongly \mathcal{K} -ISO** w.r.t. X_{ns} if X_s is strongly k-ISO w.r.t. X_{ns} for all $k \in \mathcal{K}$.

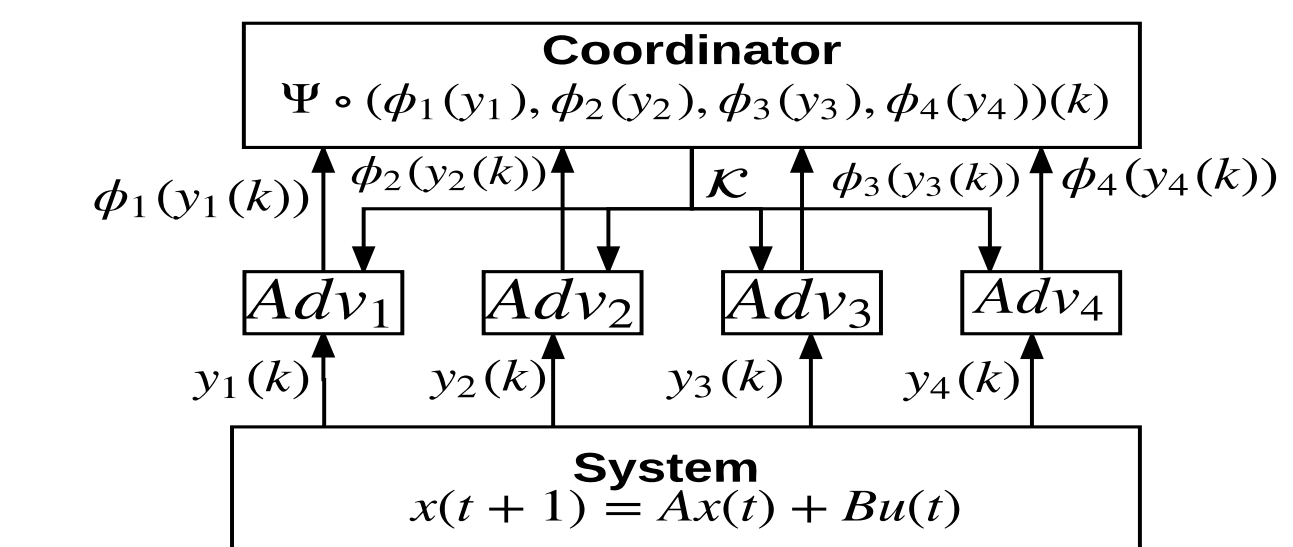
- Adversary must determine $x(0)$ from only snapshots of output.
 - \triangleright Might not want to reveal its presence.
 - \triangleright Might not have resources to make continuous observations.

Theorem:

1. Verifying k-ISO \Leftrightarrow checking membership of $y(k)$ in a set of states reachable at time k , starting from X_s and X_{ns} .
2. k-ISO (under mild additional assumptions) \Leftrightarrow output controllability.

Opacity for Linear Systems: > 1 Adversary

- Notions of **decentralized opacity** distinguished by [7]:
 - \triangleright Presence/ absence of centralized coordinator.
 - \triangleright Presence/ absence of collusion among adversaries.



- The Road Ahead:**

- \triangleright Opacity for switched and nonlinear systems [8.]
- \triangleright Tools and techniques for opacity verification.

References

1. J. Ferlez, R. Cleaveland, and S. I. Marcus. *Generalized synchronization trees*. In FOSSACS 2014, vol. 8412 of LNCS. Grenoble, France, 2014.
2. R. Milner. *A Calculus of Communicating Systems*. Number 92 in Lecture Notes in Computer Science. Springer-Verlag, 1980.
3. E. D. Tate Jr, J. W. Grizzle, and H. Peng. *Shortest path stochastic control for hybrid electric vehicles*. Int. J. Robust Nonlinear Control, December 2007.
4. L. Mazaré. *Using unification for opacity properties*. Proc. IFIP, 2004.
5. Y.-C. Wu, and S. Laforge. *Comparative analysis of related notions of opacity in centralized and coordinated architectures*. Discrete Event Dynamic Systems 23(3): 307-339, 2013.
6. B. Ramasubramanian, R. Cleaveland, and S. I. Marcus. *A framework for opacity in linear systems*. Proc. American Control Conference, pp. 6337-6344, 2016.
7. B. Ramasubramanian, R. Cleaveland, and S. I. Marcus. *A framework for decentralized opacity in linear systems*. Proc. Annual Allerton Conference on Communication, Control, and Computing, 2016.
8. B. Ramasubramanian, R. Cleaveland, and S. I. Marcus. *Opacity for switched linear systems: Notions and characterization*. Submitted.

Research supported by NSF via Grant CNS1446665