The Fourth Component of Societal-Scale CPS: Components That Can Learn

Janos Sztipanovits

ISIS-Vanderbilt

Societal-Scale CPS

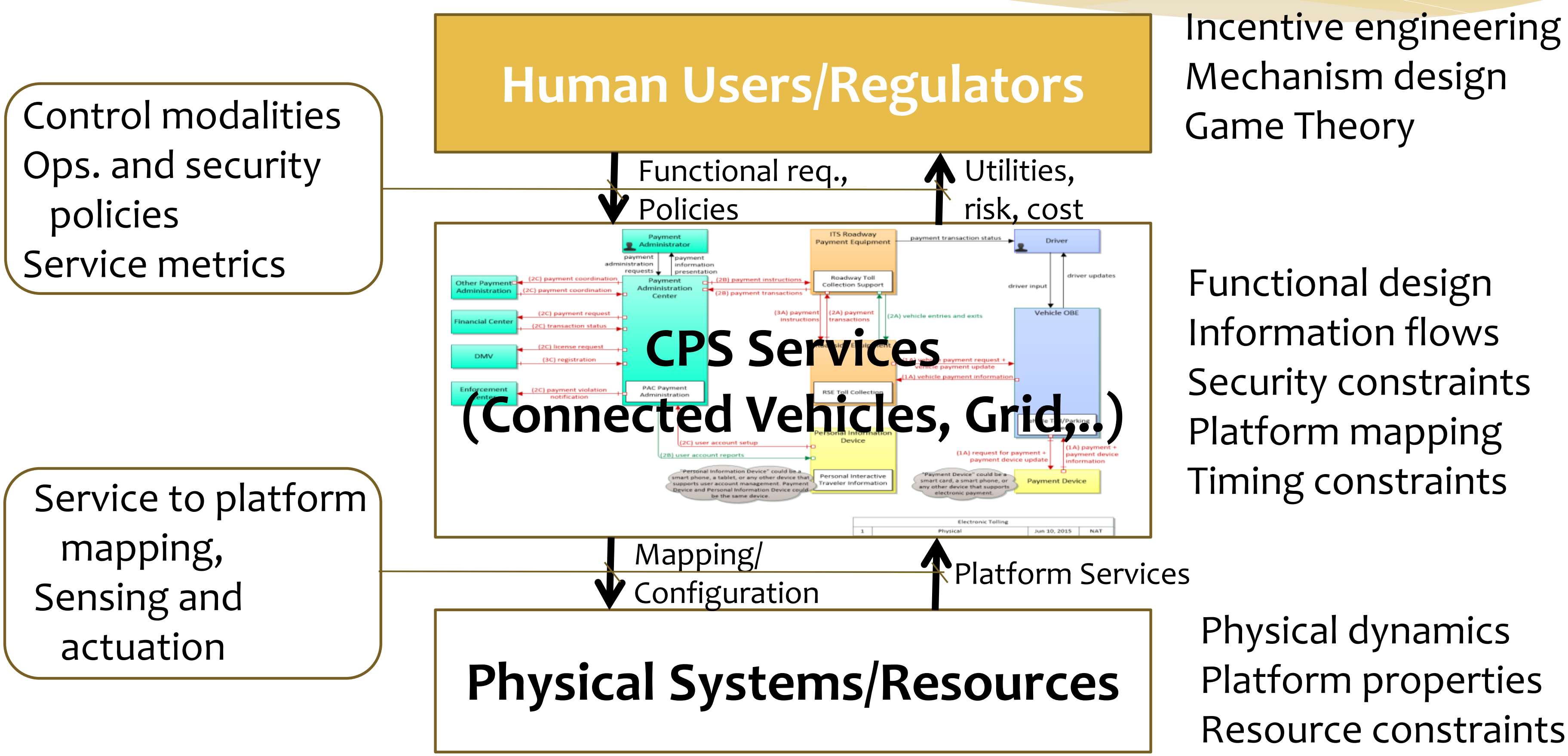
… are enabled by emerging industrial platforms in IoT, II and Fog Computing. Examples addressed by FORCES are:

* Transportation networks
* Air traffic networks
* Energy distribution networks
* Water distribution networks

- Humans are "embedded intelligent agents", human decision making is part of control loops: **H-CPS**
- Massive societal implications trigger conflicting societal expectations and policies: **Policy-aware system design**
- Complexity requires building systems with **Learning Enabled Components: High-confidence system design with components that can learn**

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Modeling and Analysis of Societal-Scale CPS: H-CPS Framework



Approach: Model and Component based design

Policy-Aware System Design

Controversies created by societal-scale systems now extend to regulations, certification, insurance as side-effects of widespread adaptation. Typical conflict issues are:

* Autonomous and Mixed-Use H-CPS (human decision making, automation, social acceptance and liability)
* Privacy (utility of services, costs, personal/institutional privacy)
* Resilience (design complexity, cost, dependability of services)

Example: dynamic, traffic aware routing

Driver incentive: savings in travel time + fuel
Societal gain: better road utilization
Cost: neighborhoods with increased traffic
Who resolves the conflict?

Two sides of the solution approaches:

Adjusting public policy to new technology

Create technology that can be parameterized by societal context

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

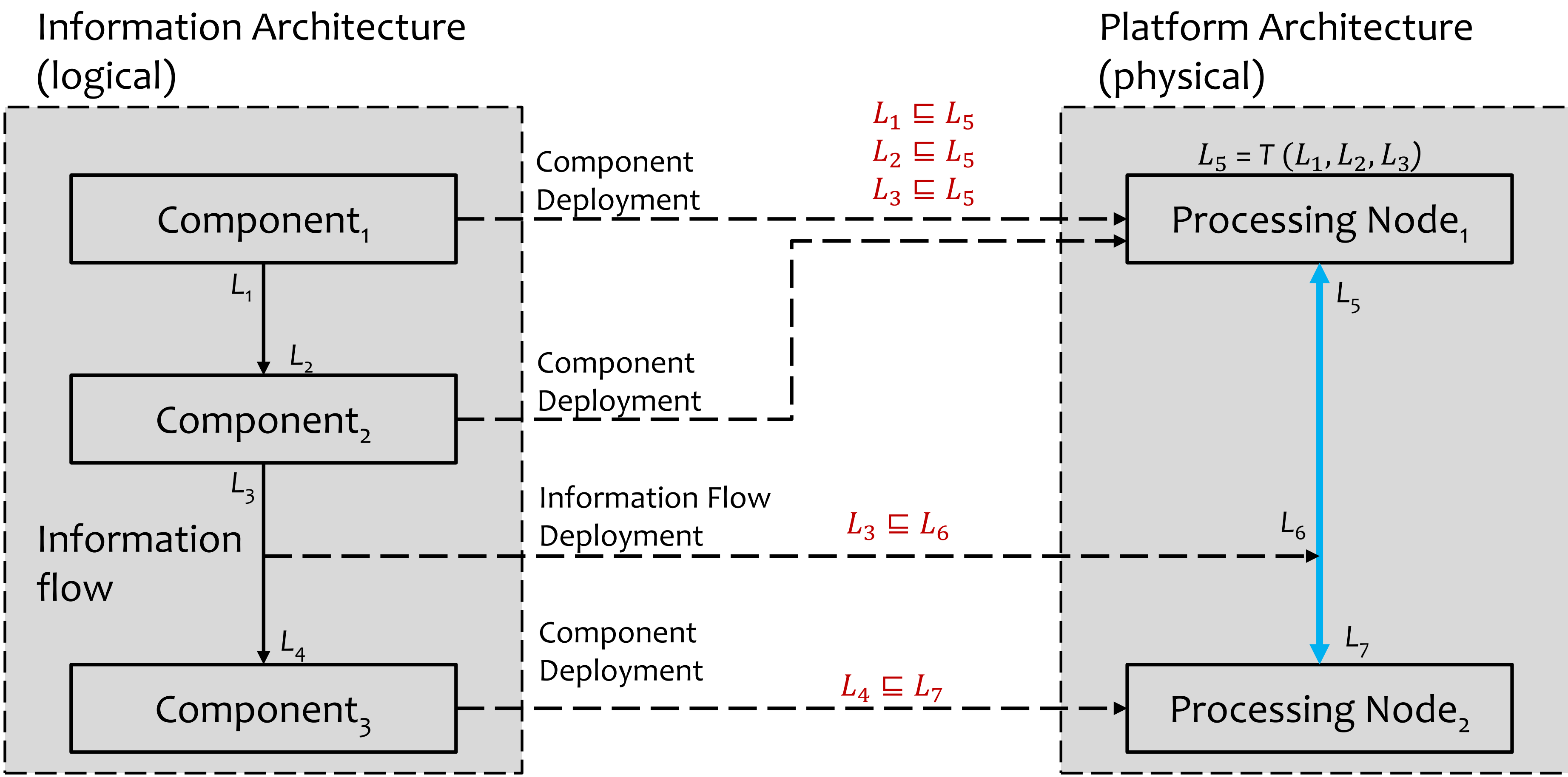
FORCES: Security-Aware System-Level Synthesis

* How to map a logical Information Architecture (components + information flows) on a physical Platform Architecture such that

  - Functional requirements (the information architecture)
  - Performance requirements (timing)
  - Security requirements (confidentiality and integrity)

  are satisfied simultaneously?

Information Architecture Deployed on a Physical Platform



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

High-Confidence System Design with Learning-Enabled Components

High confidence systems require pushing the limits of "correct-by-construction" methods.

– Model-based Technologies

Computational models that predict properties of cyber-physical systems "as designed" and "as built".

Challenge: Develop domain-specific abstraction layers for complex CPS that are evolvable, heterogeneous, yet semantically sound and supported by tools.

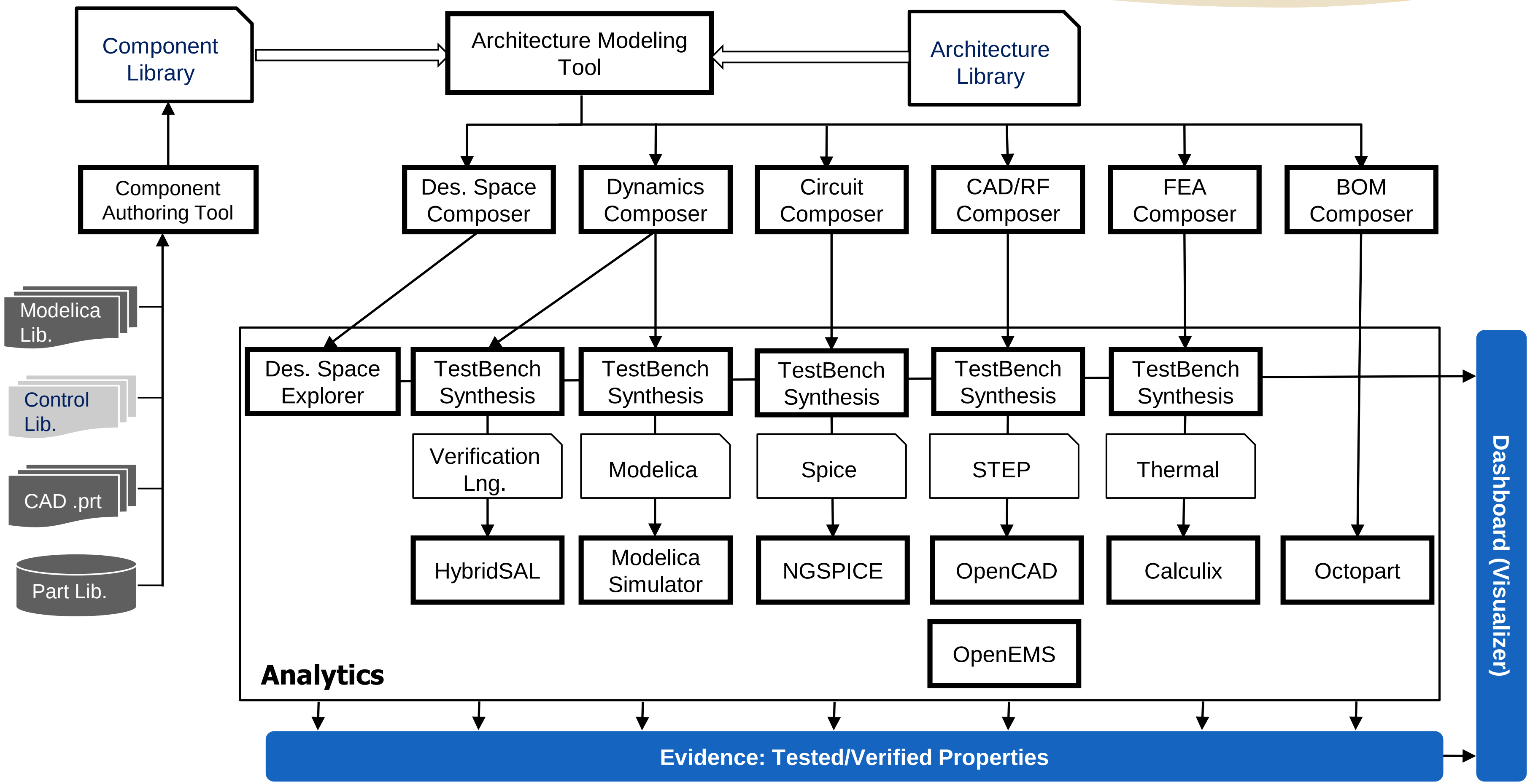
– Component-based Technologies

Reusable units of knowledge (models) and manufactured components.

Challenge: Go beyond interoperability; find and introduce compositional frameworks where system-level properties can be computed from the properties of components

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Example for CPS Design Tool Suite: OpenMETA

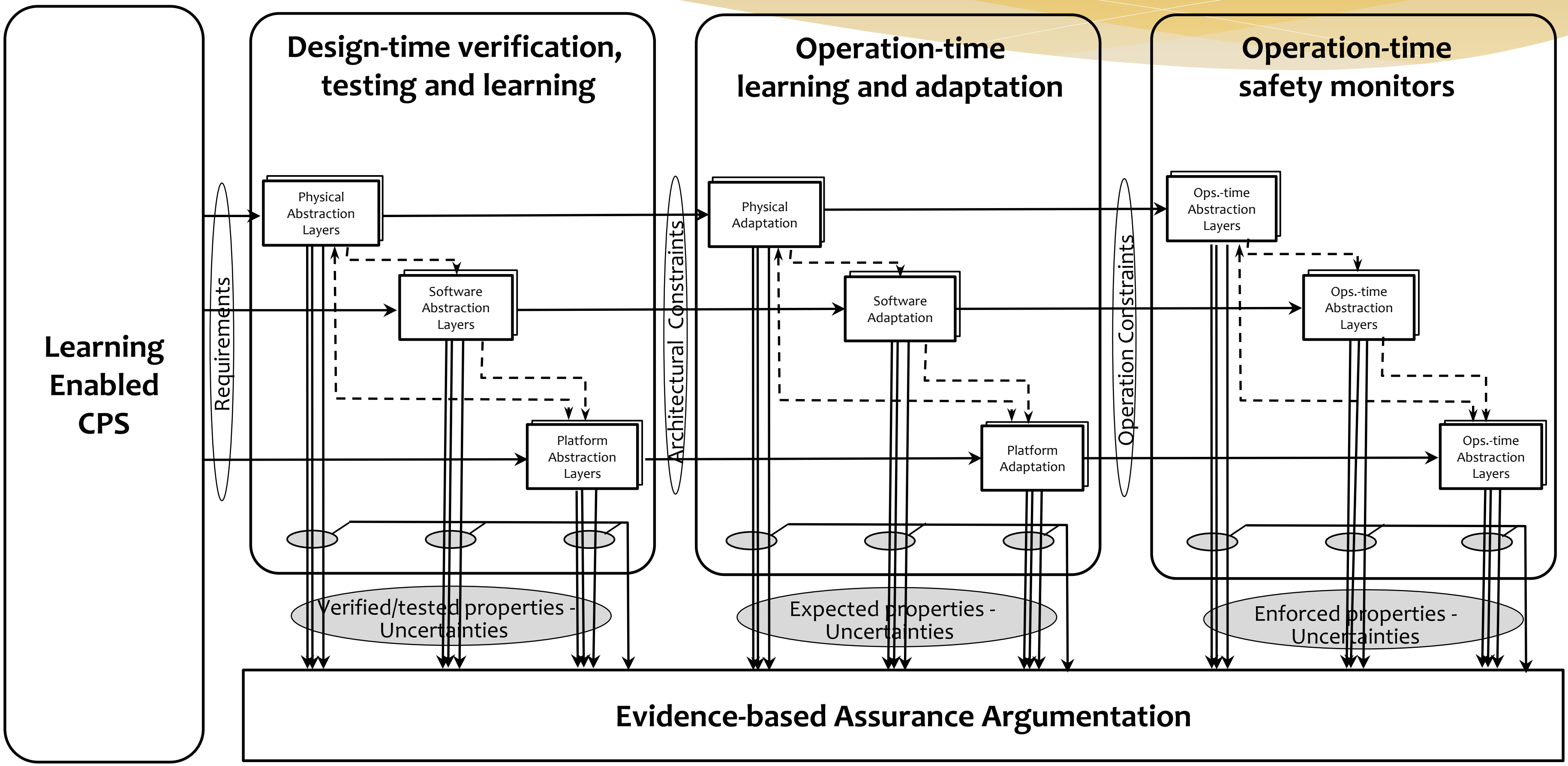


What Are the Problems With Learning Enabled Components?

* **Challenges:**
  a. How to guarantee system-level safety/security properties?
  b. How to identify those system components/behaviors in an overall H-CPS architecture that best be implemented using learning/adaptive methods?
  c. How to make tradeoff between design-time invariant models, design-time learning/adaptation and operation-time learning/adaptation?
  d. In learning/adaptive components what is reusable across different systems?

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Reframing the Model-based Design Approach



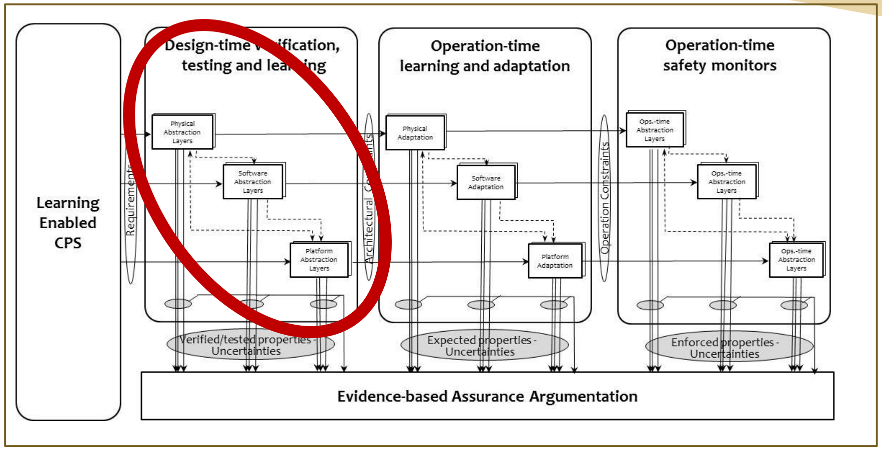
Assurance using design-time (partial) evidence

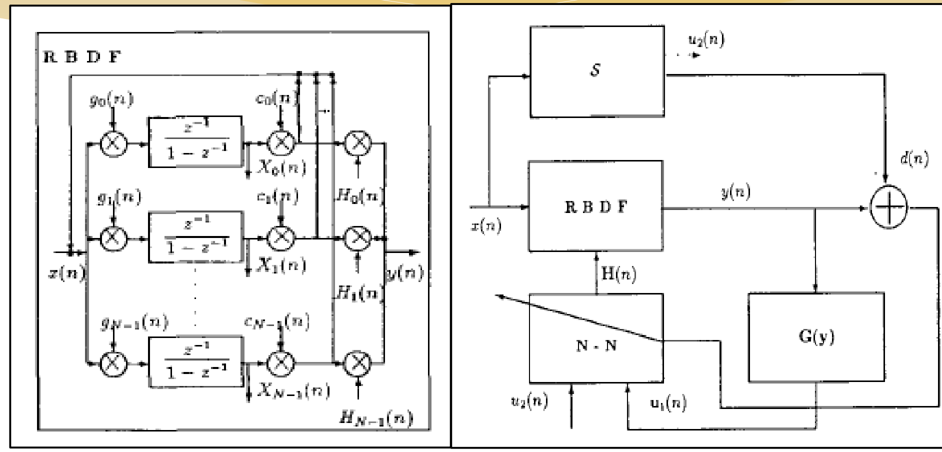
Assurance using operation-time evidence

Assurance using operation-time observations

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Example: Design-time Evidence for Preserving Stability



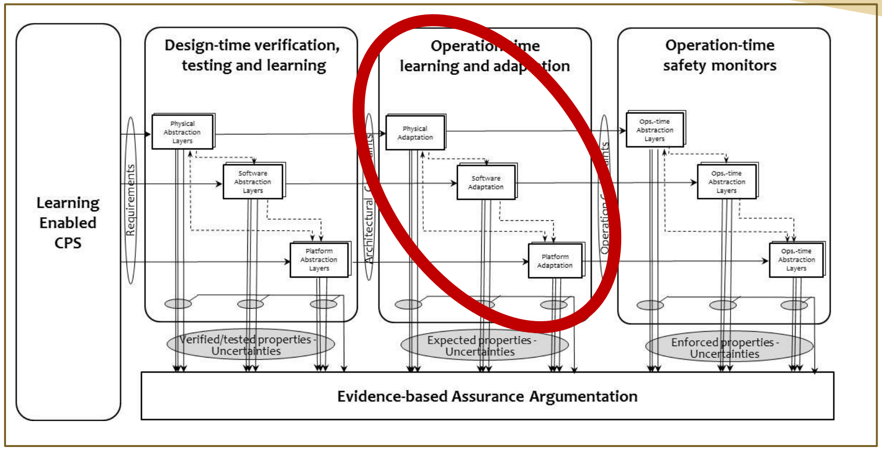


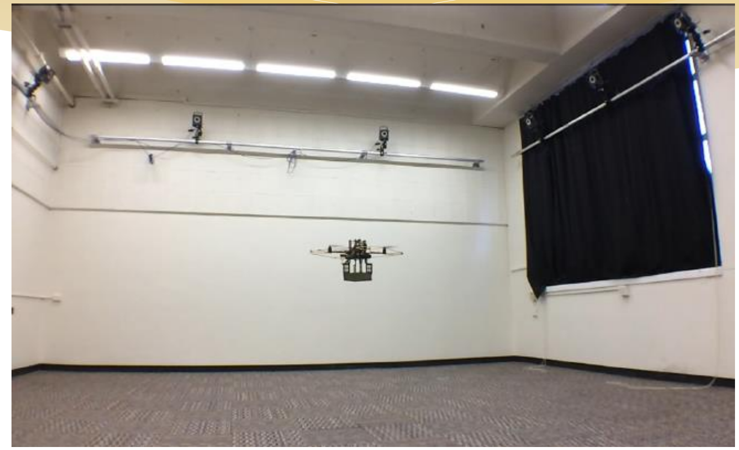
Structurally passive learning enabled dynamics

- **Physical Architecture: Passivity-based design**
  - Method: Passivity-based design (e.g. *Proc. IEEE,Vol.100 No.1, pp. 29-44, 2012*)
    Outcome: Decouples effects of time varying delays on stability caused by computation and networking effects
  - Sztipanovits, J., "Dynamic Backpropagation for Neural Network Controlled Resonator-Banks," IEEE Transactions on Circuits and Systems, Vol. 39, No.2, pp. 99-108
- **SW & Platform: TTA/TTP**
  - Guaranteed deadlock freeness
  - Bounded delay
- **Tradeoff between performance and verification complexity**

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Example: Embedded Safe Learning





* **Safe Learning**
  * Method: Learn unkown dynamics based on a Gaussian Process Model and iteratively approximate the maximal safe set Passivity-based design
    Tomlin et al: Reachability-based safe learning with Gaussian Processes. *Proc. 53rd CDC 2014*
    Chen, Fisac, Sastry, Tomlin: Safe sequential path planning via double obstacle Hamilton Jacobi Isaacs variational inequalities. ECC 2016
    Outcome: Safety is guaranteed during the learning process
* **Learning approaches:**
  * Gaussian process model
  * Deep Neural Nets

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Many Open Problems

* Models of learning-enabled CPS components whose behavior is bounded and composable in open CPS architectures
* Guarantees for Closed Loop Performance of learning-enabled CPS components
* Real time metrics for the performance of learning algorithms
* Extending model-based design methods with precise representation and utilization of partial (but bounded) models in design flows
* Evidence-based assurance argumentation methods that can handle both probabilistic and deterministic methods
* Integrated tool chain and model-based design flow that incorporates learning enabled components

Summary

* Societal-scale CPS are enabled by the new platforms: IoT, II and Fog
* Impact of these systems requires new architecture, offer new capabilities and create new challenges:
  * H-CPS
  * Policy-aware architectures
  * H-CPS with Learning Enabled Components
* Achieving progress in these areas defines the next decade for CPS research

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS