FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Societal-Scale CPS:
Policy Awareness and Provably Correct Behavior for Systems with Learning Enabled Components

Janos Sztipanovits

ISIS-Vanderbilt

Berkeley UNIVERSITY OF CALIFORNIA

Massachusetts Institute of Technology

NSF

MICHIGAN

VANDERBILT UNIVERSITY

Societal-Scale CPS

Examples addressed by FORCES are:

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

Key enablers for deployment are emerging industrial platforms:

* Industrial Internet – IIC 2014
* Fog Computing – OpenFog Consortium 2016
* IoT platforms – several major companies

Key barriers for deployment are lack of foundations to guarantee system-level properties

* Safety
* Security
* Resilience

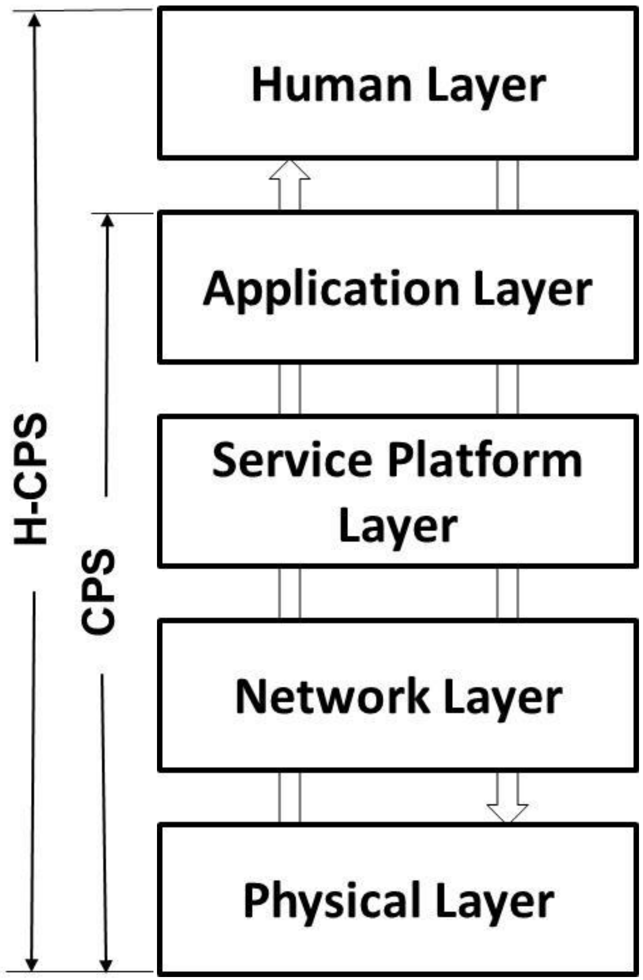
Many Roles of Humans in H-CPS

* Direct components of large systems (e.g. drivers of Connected Vehicles)
* Supervisors of systems operation via monitoring aggregate performance metrics and changing operational policies (e.g. adjusting market rules in Transactive Energy)
* Designers making investment decisions, design tradeoffs and selecting performance metrics

- 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

Layers of H-CPS



Incentive engineering
Mechanism design
Game Theory

Functional design
Use of interacting services
Coordination, timing

Information flows
Security, privacy constraints
Resource constraints

Throughput/delay
Availability
Security

Physical dynamics
Platform properties
Resource constraints

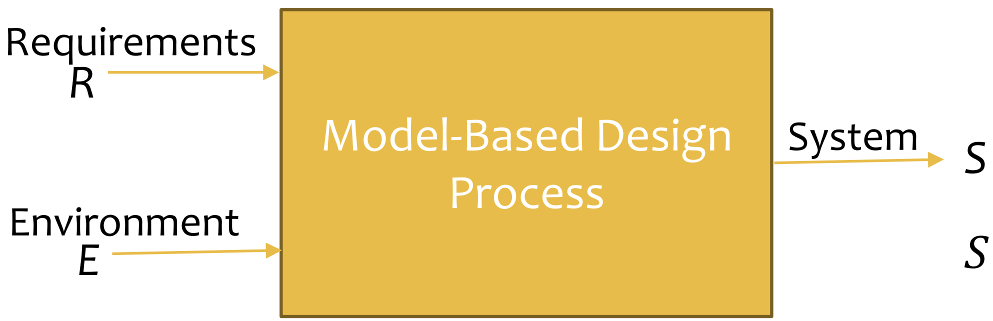
What Are the Fundamentally New Challenges?

- **Policy Aware System Design:**
  Making societal-scale systems adaptable to social context

- Designing high-confidence systems that can learn
  Theory for high confidence system design with Learning Enabled Components

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Policy-Aware System Design



$$S \parallel E \models R$$

Societal-scale systems are motivated by societal needs (*R*), must conform to social norms and respond to expectations (*E*).

Examples for conflicts and differences:

Dynamic, traffic aware routing
- Driver's gain: travel time, fuel
- Societal gain: road utilization
- Cost: neighborhoods with increased traffic
- **Who resolves the conflict?**

Life-and-death decisions and autonomy
- US: open for societal discourse
- Germany: leaving live-and death decision to machine is unconstitutional
- **Who is right?**

Potential Solutions

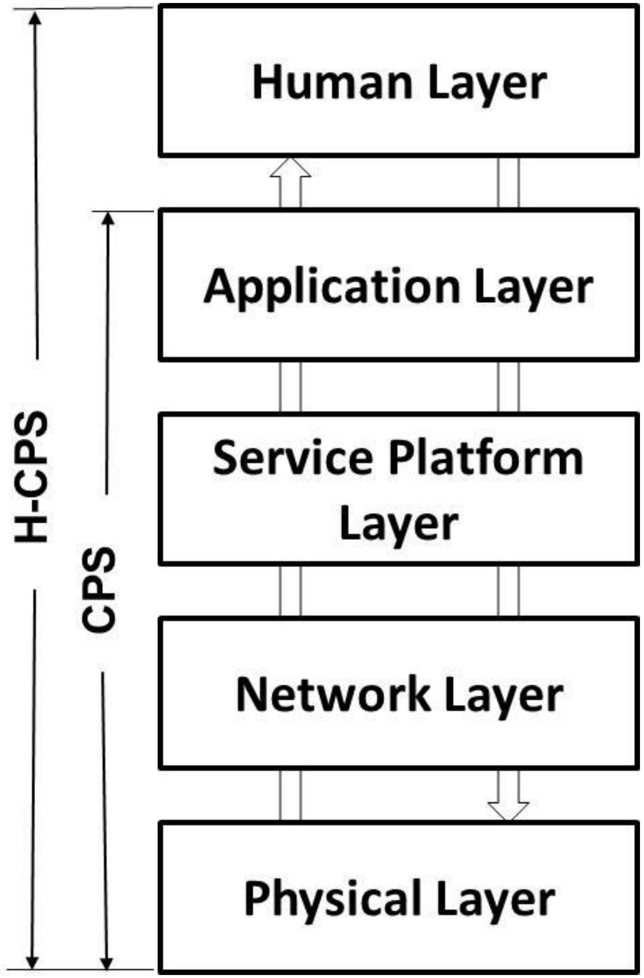
* Adjusting public policy to new technology
  Complex, unstable, leaves industry exposed to policy changes and costly differences on the international market

* **Constructing H-CPS systems that can be "parameterized" by social context.**
  Missing foundations for creating this technology

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Research on Parameterized Architectures

Vanderbilt, Berkeley
TU Munich, U. Oldenburg



Incentive Eng.	On-line Conflict Resolution	Policy aware synthesis	Auditing
Incentive structure Mechanism design Nash equilibria	Prob. reachability properties Resource utilization Goal aggregation Situation dependent goals State dependent goals	Confidentiality and integrity, DLM Modeling security properties System-level synthesis	Policy-driven monitoring Data usage control Audit-log data mining

FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

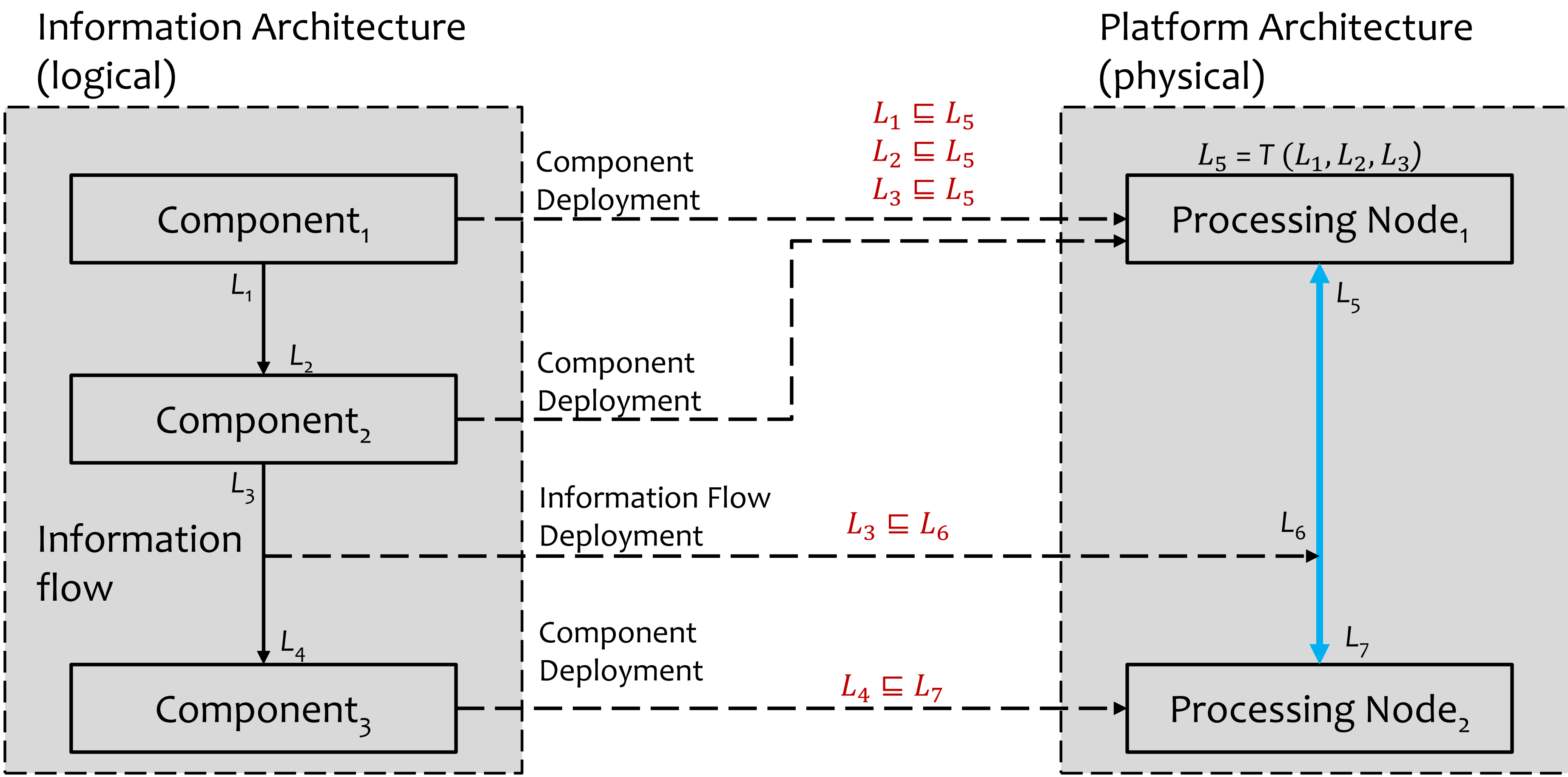
FORCES: Policy-Aware System-Level Synthesis

* 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

What Are the Fundamentally New Challenges?

* Policy Aware System Design:

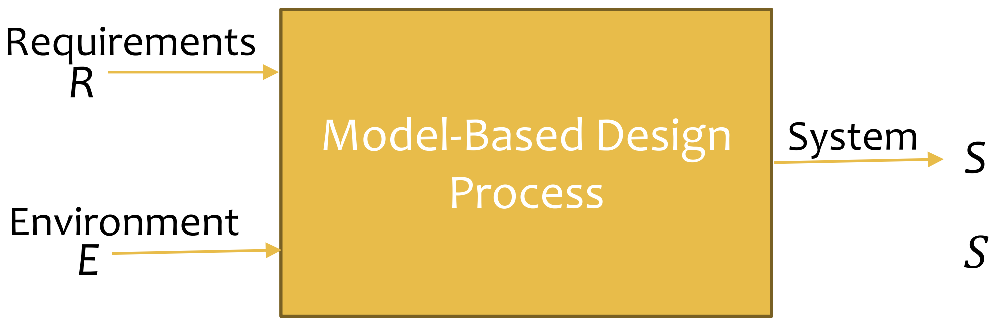
  Making societal-scale systems adaptable to social context

* **Designing high-confidence systems that can learn**

  Theory for high confidence system design with Learning Enabled Components

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

High-Confidence Design with Learning Enabled Components



$S \parallel E \vDash R$

In model- and component-based design *R*, *E* and *S* are formally modeled and the design process is a combination of synthesis and verification steps. *The goal of synthesis is to synthesize S from a class of systems* $\mathbb{C}_S$ *such that* $S \parallel E \vDash R$.

Barriers in societal –scale CPS/H_CPS:

SID methodology for formal verification (Seshia, 2015):

- Abstraction-Based Model Checking
- Synthesis of *R* (STL formula) from sim. traces..

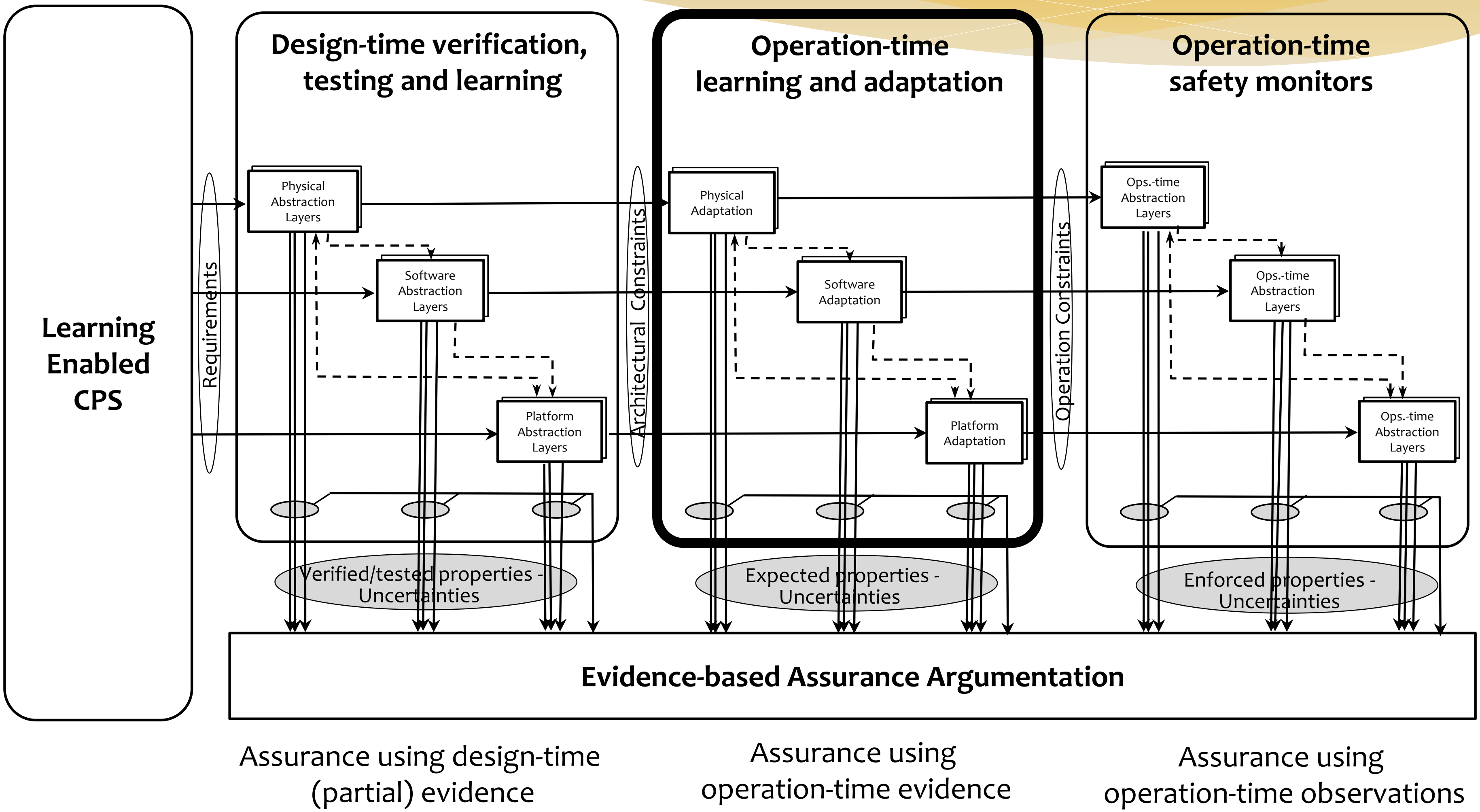
Scalability remains limited for CPS.

Modeling uncertainty in physical systems

- **Aleatoric** uncertainties: irreducable, rooted in physics
- **Epistemic** uncertainties: lack of knowledge

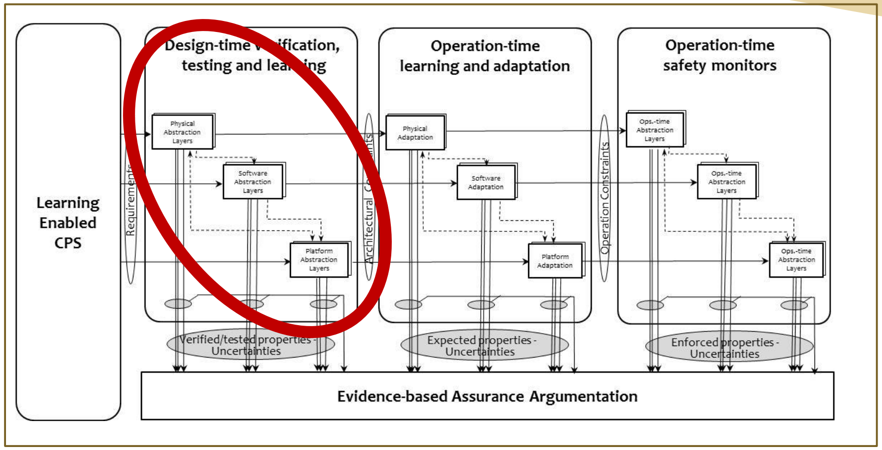
Role of epistemic uncertainties dominates.

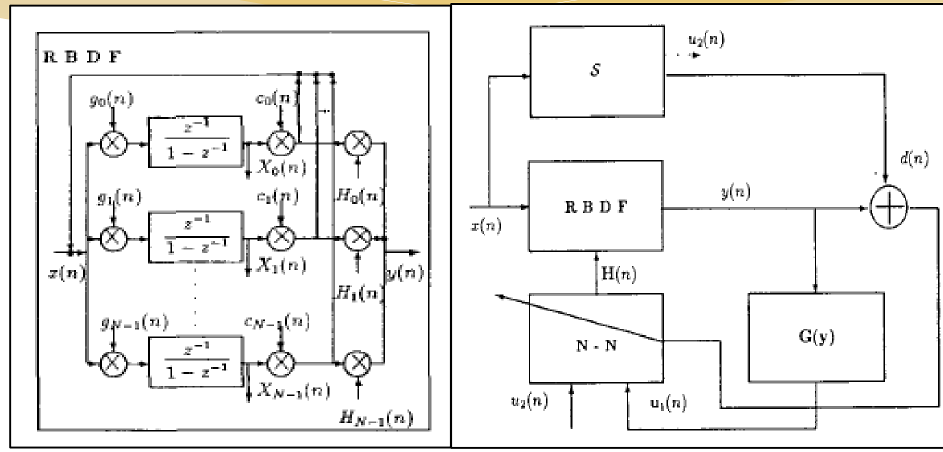
Addressing Epistemic Uncertainties with Learning and Adaptation



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Example: Design-Time Evidence for Stability Preservation

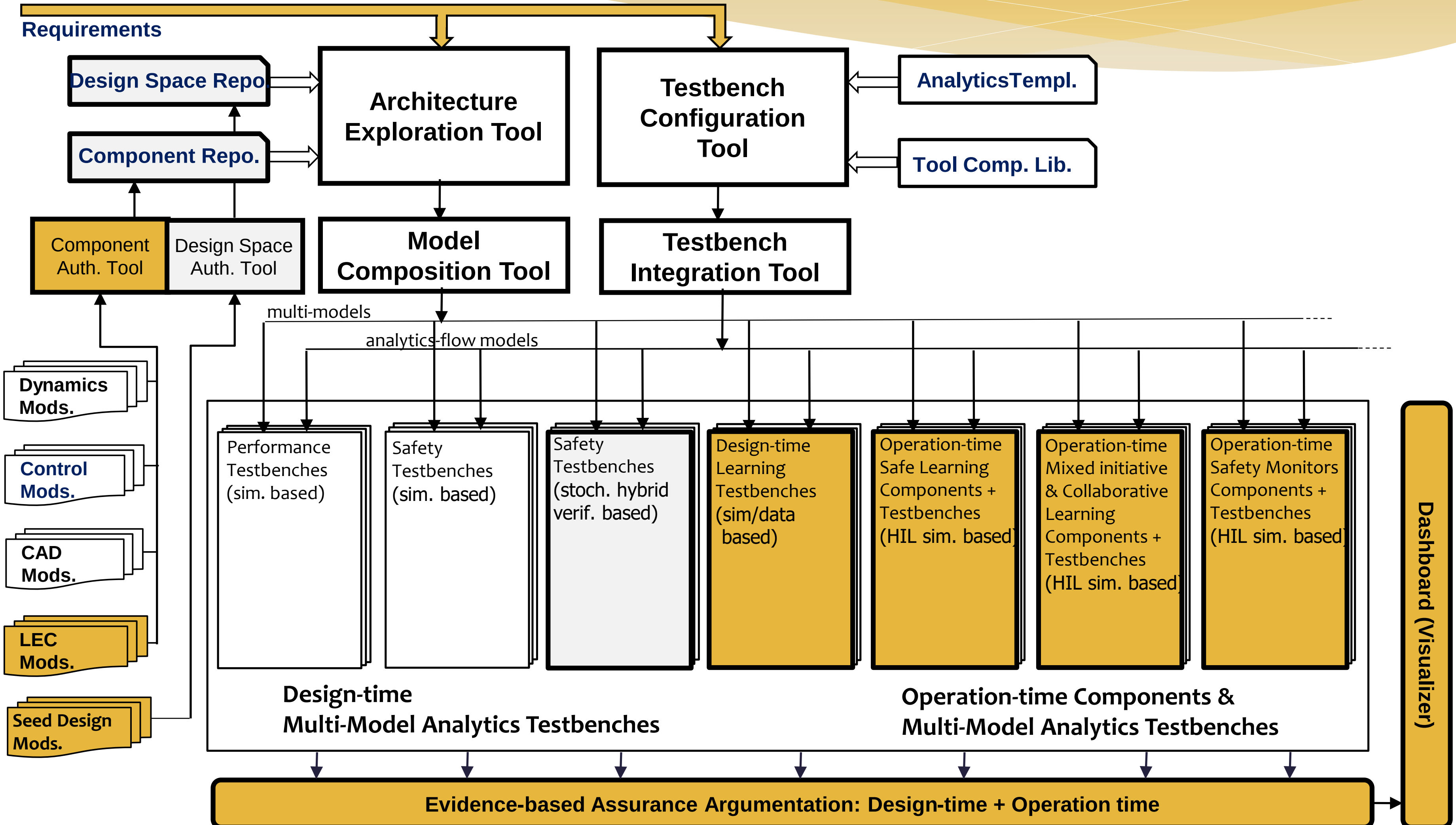




Structurally passive learning enabled dynamics

- **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**

Revisiting CPS Design Tool Chains



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The Emerging Agenda

Industry Perception
(Gartner's View on Technology Trends)

* **Transparently immersive experiences**
  Technology becomes more adaptive, contextual and fluid
* **The perceptual smart machine age**
  CPS fusion with AI
* **Platform revolution**
  Ecosystem-enabling platforms

Academic Perception:
(Current Academic Research Trends)

* **Policy awareness**
  How to build H-CPS that can be parameterized with societal context?

- **Learning Enabled Components**
  How to deliver assurance?
- **Platforms with safety, security and performance guarantees**
  How to build platforms and application development tools that enforce platform constraints (and preferably free)?

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

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

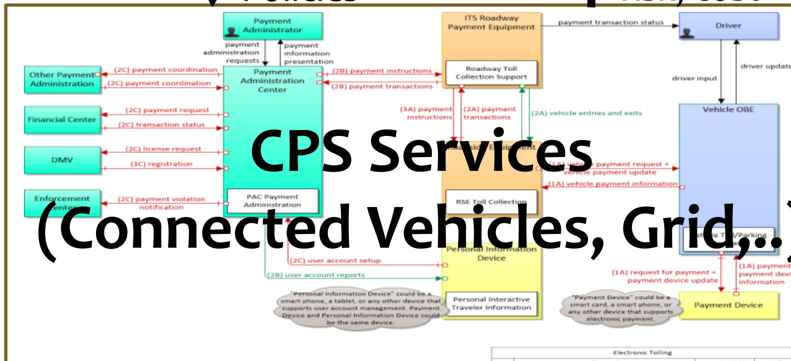
Control modalities
Ops. and security policies
Service metrics

Human Users/Regulators

Incentive engineering
Mechanism design
Game Theory

Functional req., Policies

Utilities, risk, cost



CPS Services (Connected Vehicles, Grid,..)

Functional design
Information flows
Security constraints
Platform mapping
Timing constraints

Service to platform mapping,
Sensing and actuation

Mapping/ Configuration

Platform Services

Physical Systems/Resources

Physical dynamics
Platform properties
Resource constraints

Approach: Model and Component based design