FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

FORCES
Summary and Lessons Learned

FORCES research team
(compiled by Saurabh Amin)

November 14th, 2014

Berkeley
UNIVERSITY OF CALIFORNIA

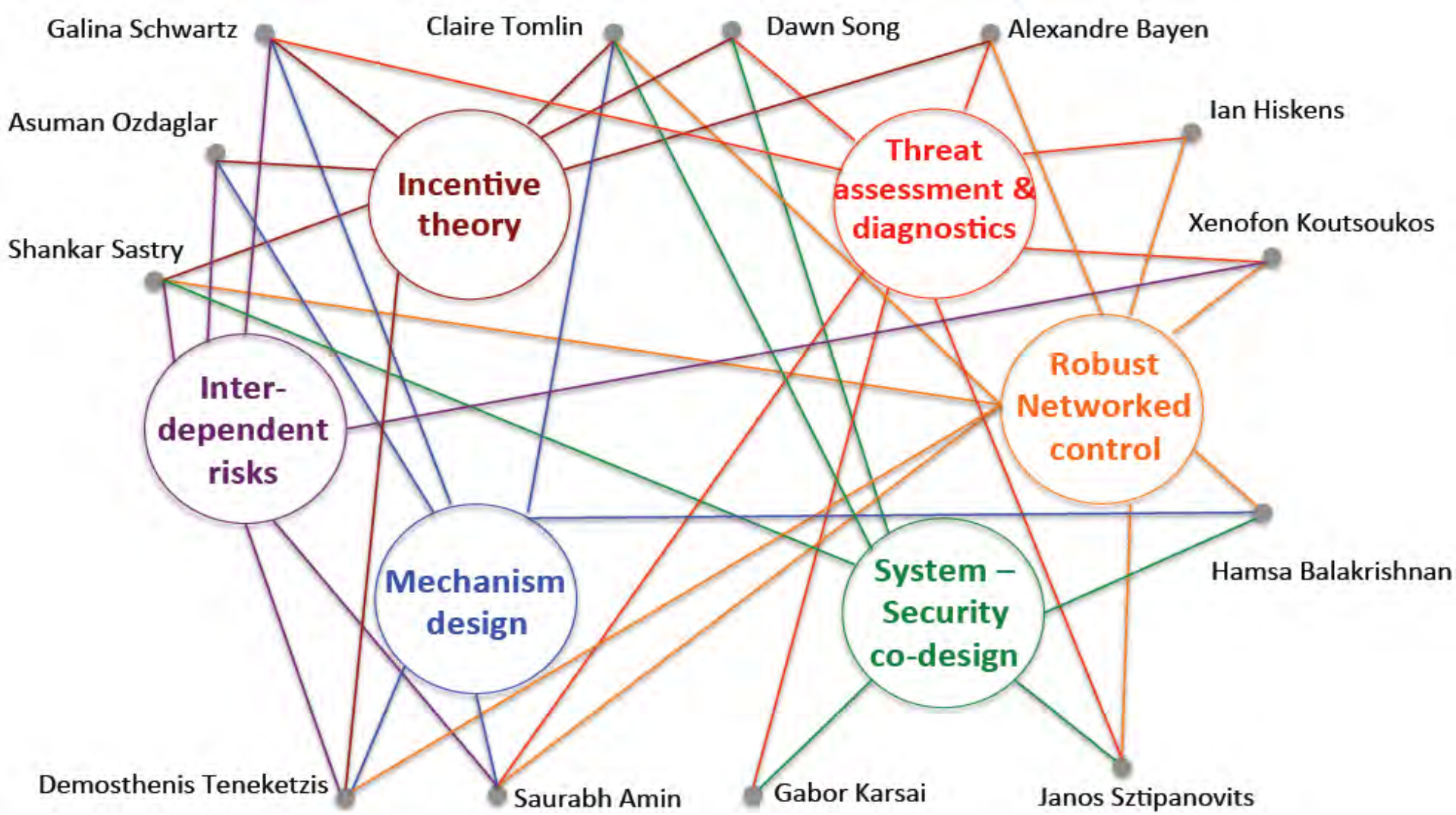
Massachusetts Institute of Technology

NSF

MICHIGAN

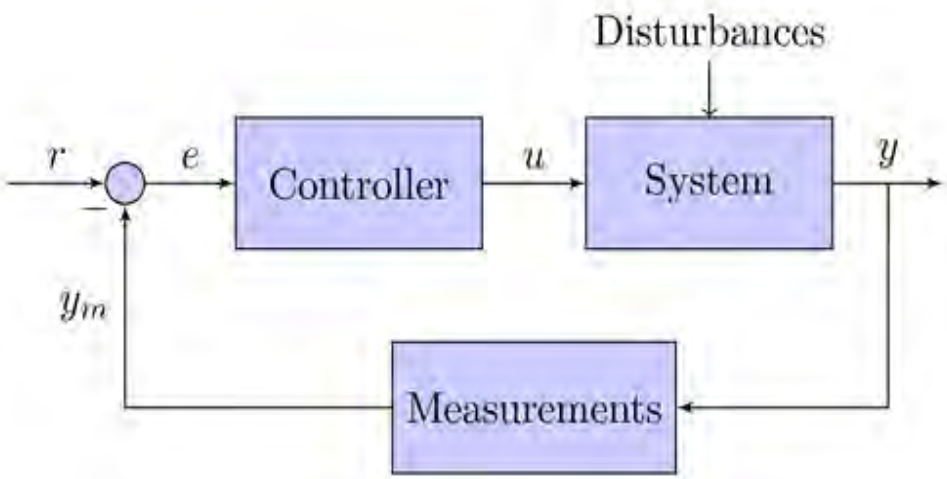
VANDERBILT UNIVERSITY

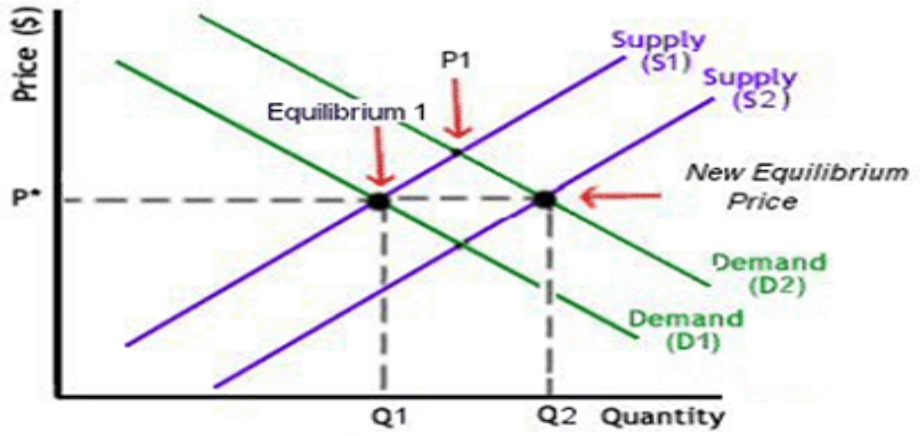
Our **initial** starting point



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Initial barrier 1: Two academic training paths



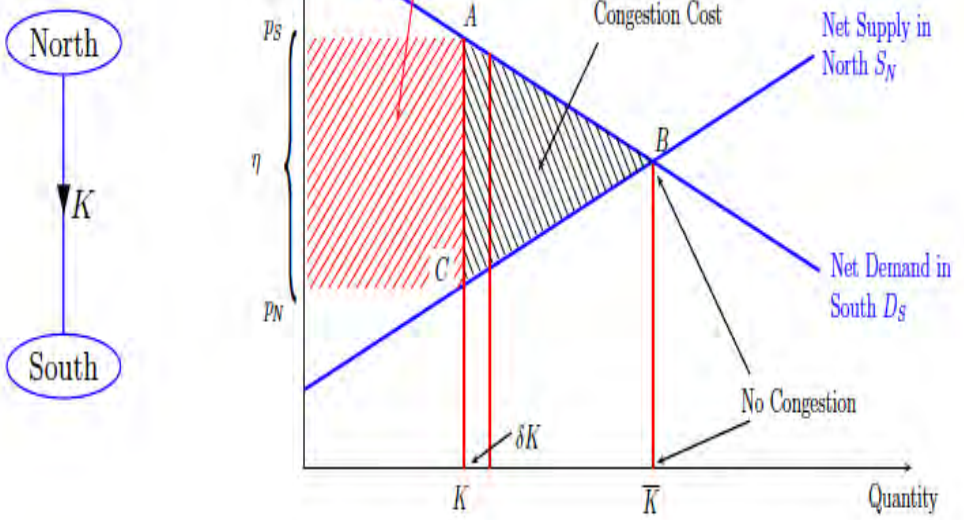


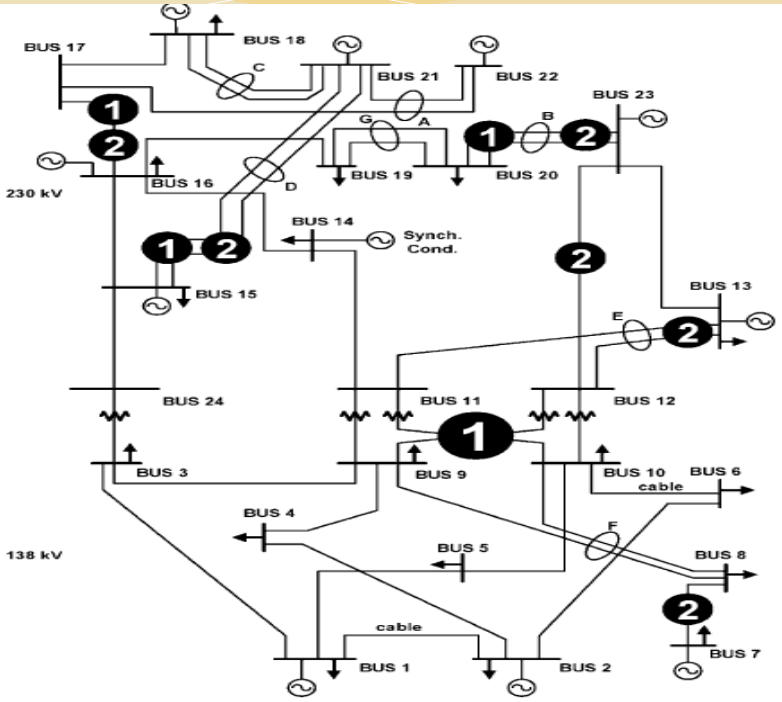
- **Systems and Control**
  - Linear and nonlinear control
  - Convex optimization
  - Theory of optimal control
  - Random processes and stochastic control
  - **Hybrid and embedded systems**
  - **Dynamic non-cooperative games**

- **Economics [markets, regulation]**
  - Microeconomics I and II
  - Macroeconomics
  - Game theory
  - Industrial organization
  - Market design
  - Econometrics

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Initial barrier 2:
Two ways to approach same problem





Joskow and Tirole:
Merchant transmission investment

Baldick, Wood, Salmeron:
Electricity transmission interdiction

How to include tech. & physical constraints in economic models?

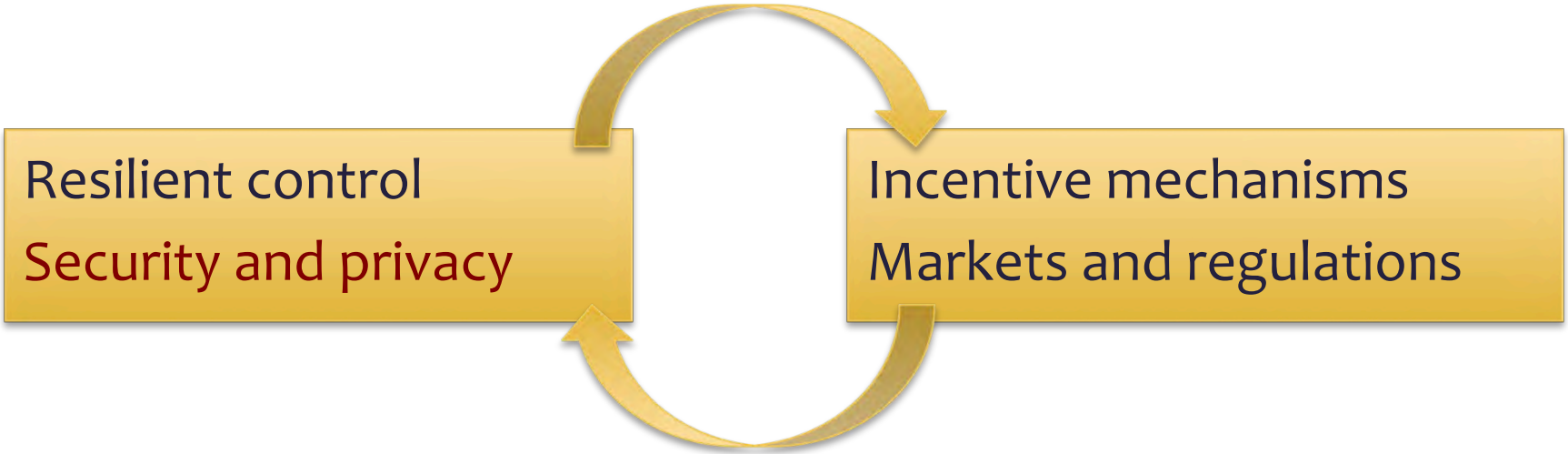
How to include strategic & info. effects in CPS control models?

Our **actual** starting point

"Obviously that poor guy has never heard of TechNote Time's Ohms Law watches! Never fumble for an Ohm's law formula again!"

h-CPS

* Key attributes: CPSs are multi-agent systems, where
  * Agents (players) are strategic, utility-maximizing entities
  * Incomplete and also asymmetric (private) information is present
  * CPSs are subject to security failures and reliability failures
  * Defense strategies include both control and IT security tools
  * Players face regulatory impositions for ensuring efficiency & safety



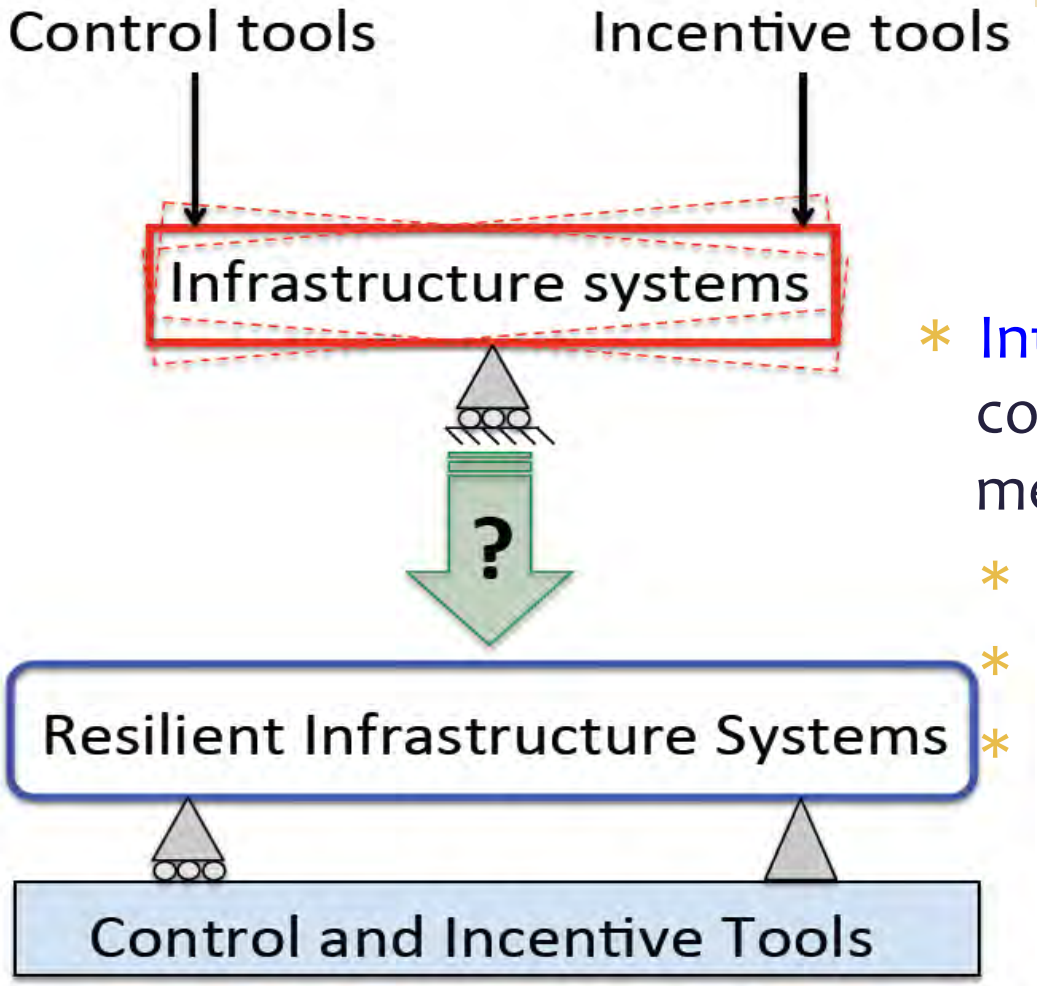
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Matrix of FORCES projects

CPS for Transportation & Electric Power	Tools Based on High Confidence Control	Tools Based on Game theory and Theory of Incentives
Active road traffic management	Distributed sensing and control	Congestion pricing and incentives
NextGen air traffic operations	Robust scheduling and routing	Strategic resource re-allocation
Smart electricity and water [gen & dist.]	Distributed load control, DG & renewable manag.	Demand response schemes, market design
Efficient buildings	Predictive control	Energy saving incentives

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

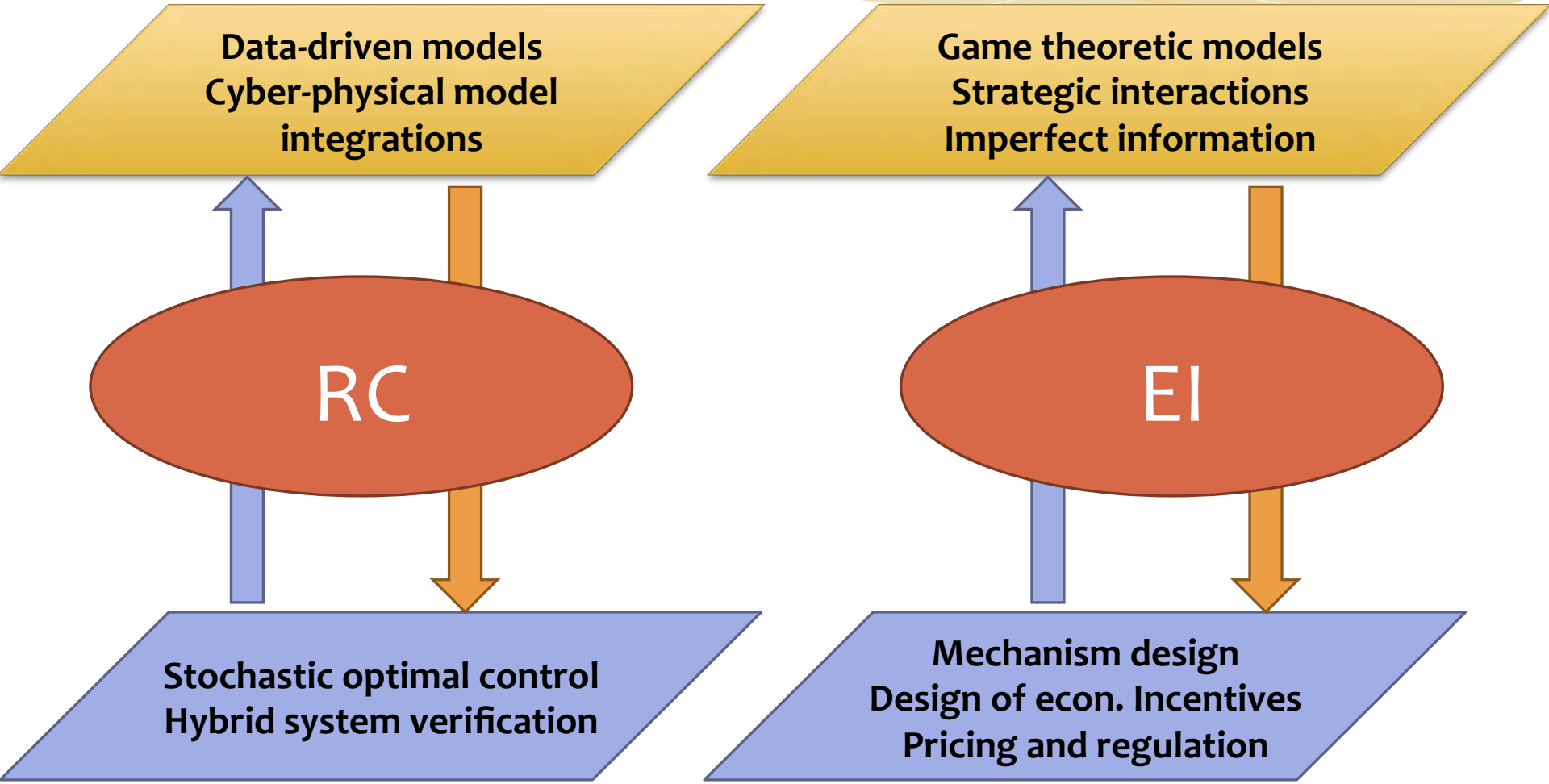
FORCES goal



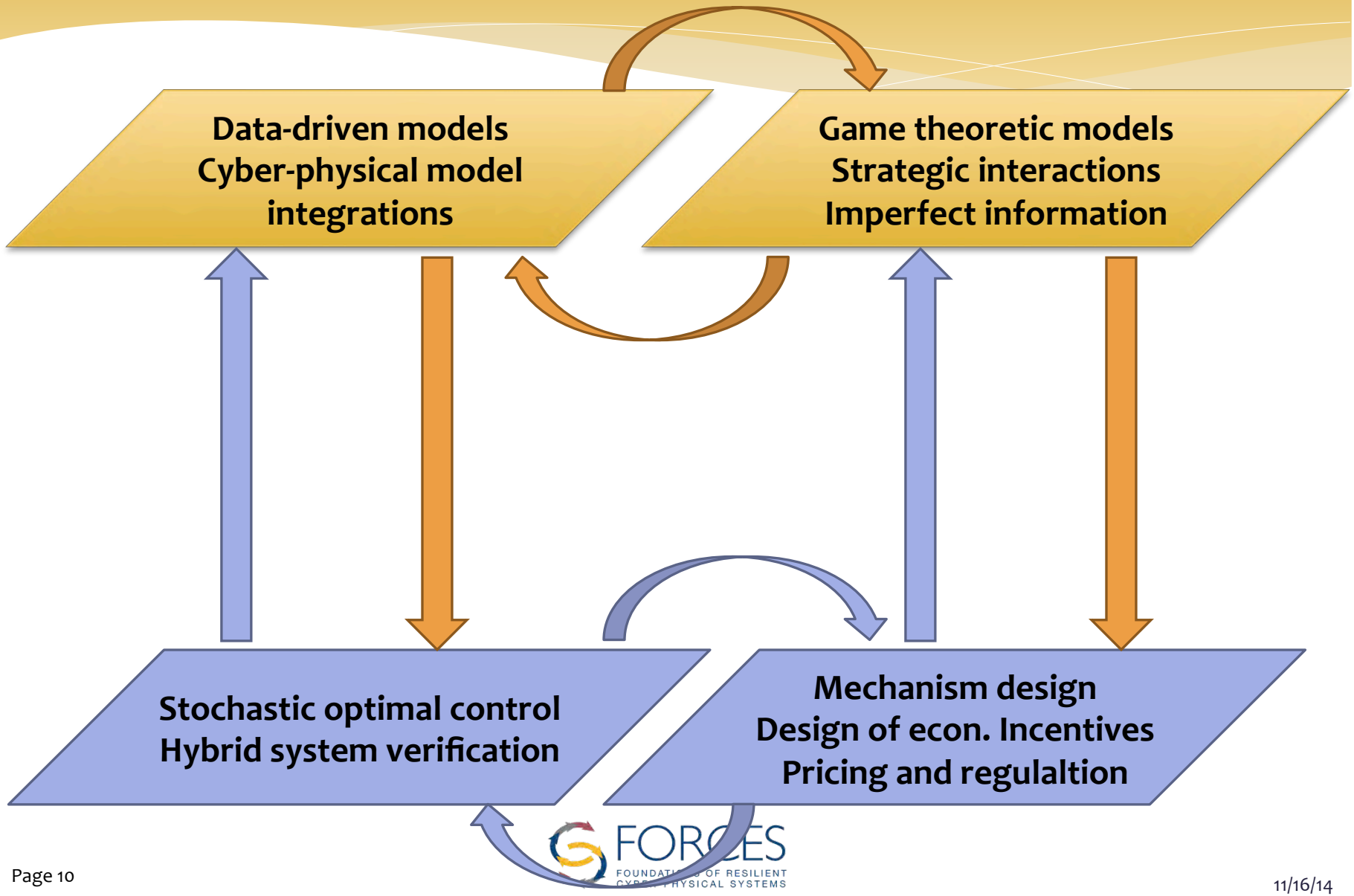
* Integrated design of resilient control and economic incentive mechanisms for improving:
  * Efficiency
  * Security and fault tolerance
  * Operational resilience

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

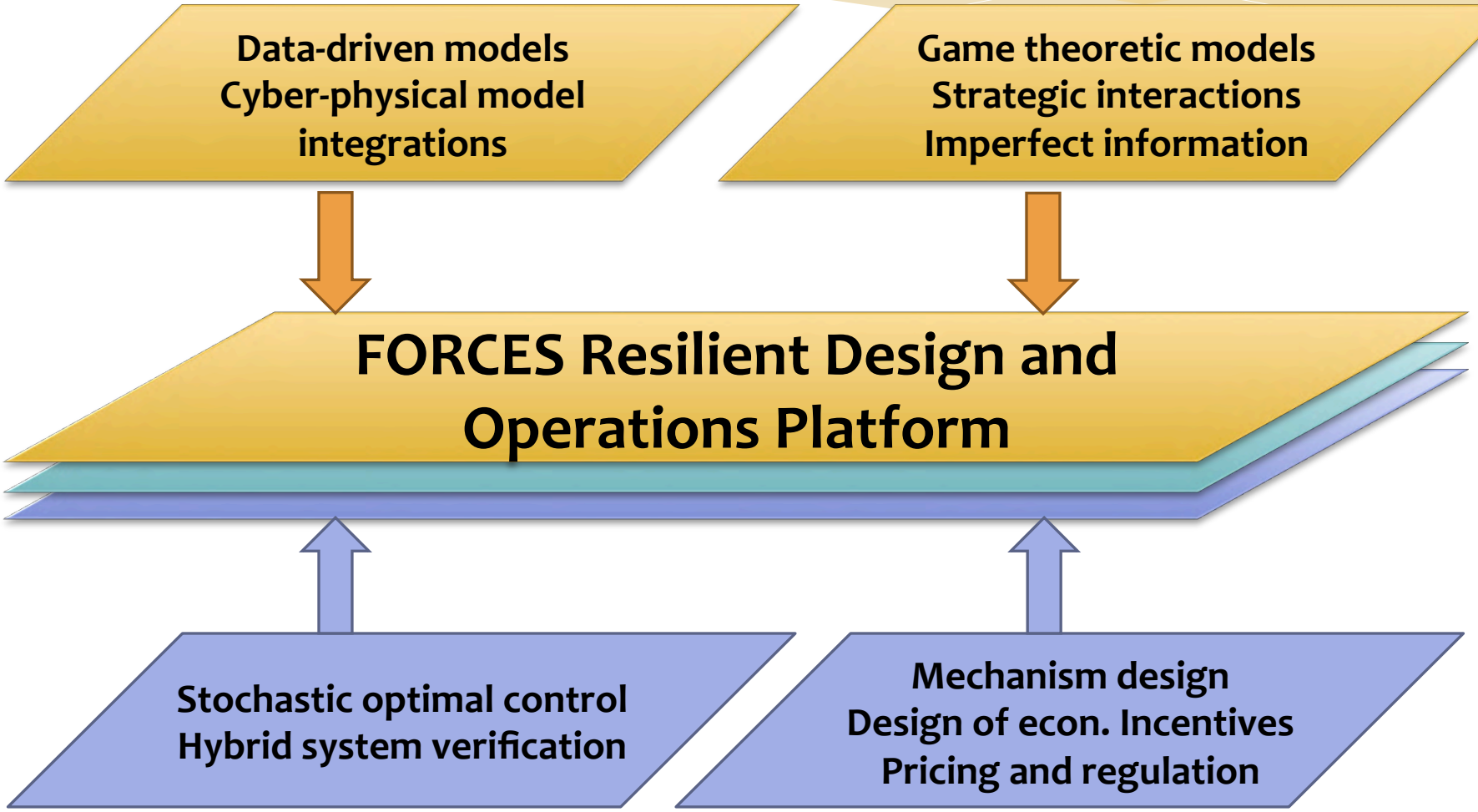
Status Quo


Data-driven models
Cyber-physical model integrations
Game theoretic models
Strategic interactions
Imperfect information
RC
EI
Stochastic optimal control
Hybrid system verification
Mechanism design
Design of econ. Incentives
Pricing and regulation

Our **intermediate** goal



Our final goal



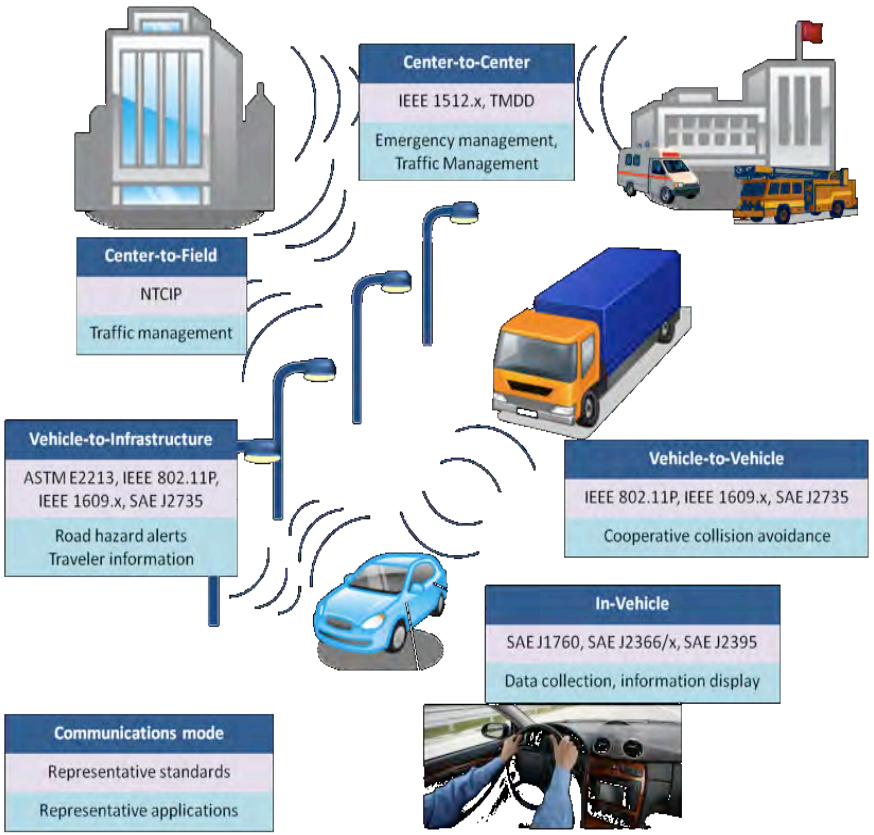
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Good news 1: CPS domain specific courses exist

- **Road and public transportation systems**
  - Transportation Systems Analysis: Performance and Optimization
  - Transportation Systems Analysis: Demand and Economics
- **Electricity systems**
  - Power system dynamics and control
  - Restructured electricity markets: LMP and Market power
- **Air transportation systems**
  - Air transportation operations research
  - Air transportation Infrastructure and Economics

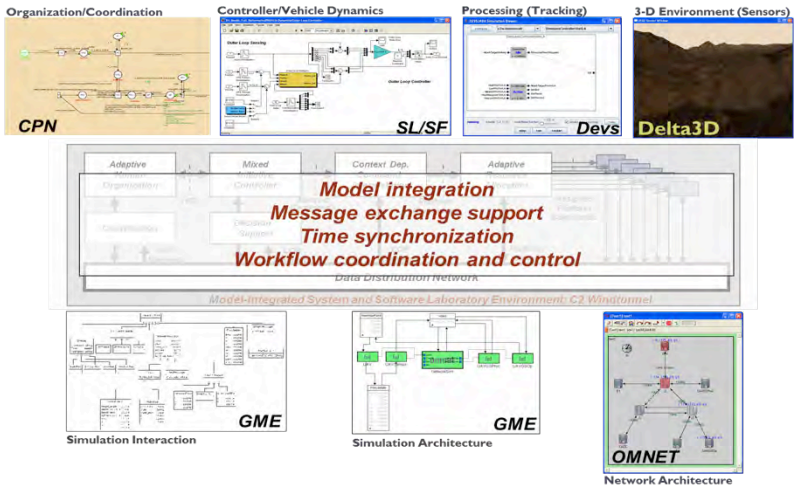
Good news 2:
CPS Testbeds and field experiments

Connected corridors



Water transmission and distribution

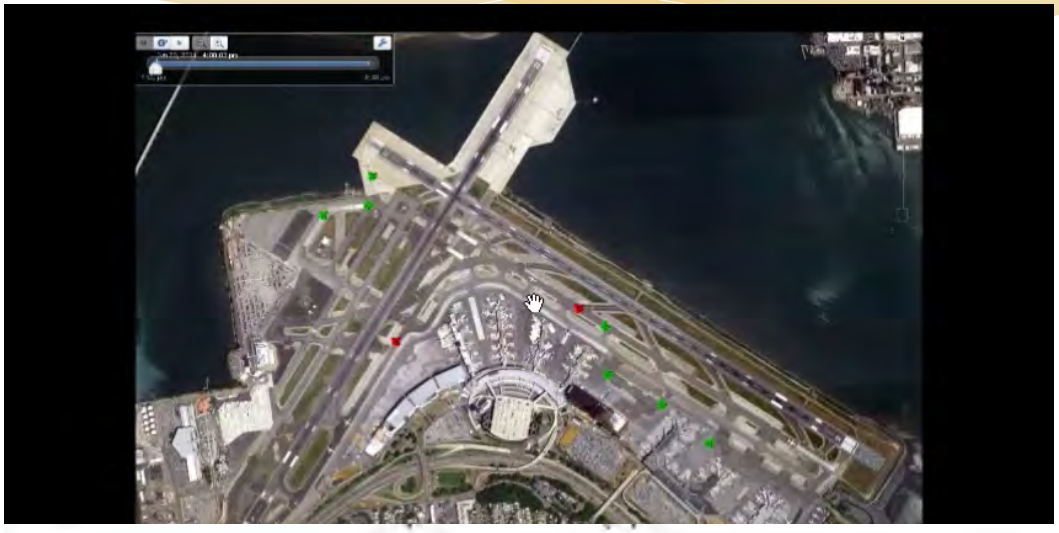
C 2 Wind Tunnel for Integrated Test Bed

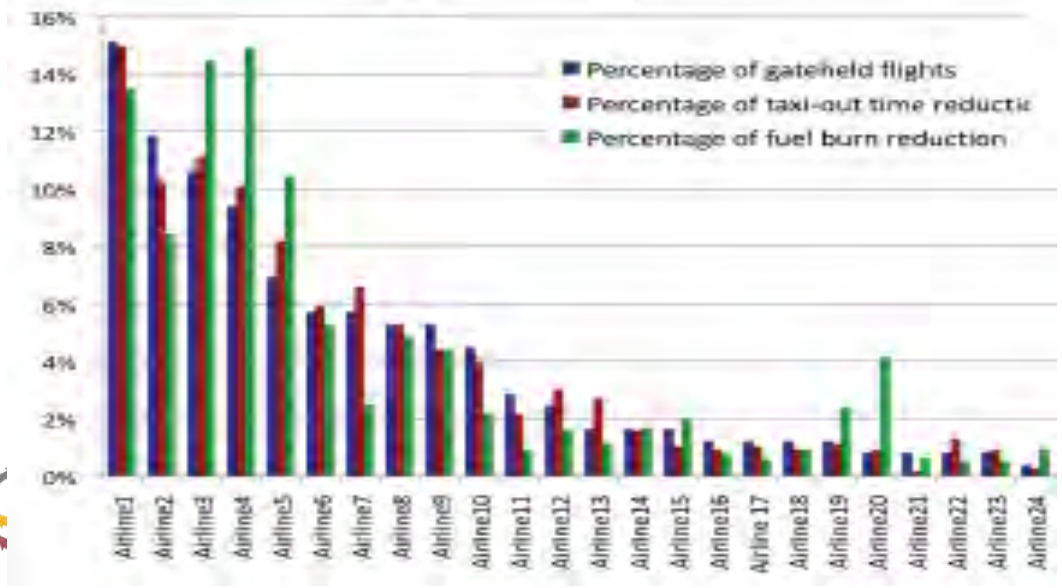


FORCE
FOUNDATIONS OF RES
CYBER-PHYSICAL SYS

Good news 3:
Data from real-world operations [My precious!]

* **Data driven modeling**
  * Queuing model of airport operations => Robust prediction performance
  * Design, field testing, and evaluation of control algorithms





Data from real users
[Also precious!]

* Traces of traffic data from commuters
* Consumption patterns and responses to pricing signals
  * Both residential and commercial issues

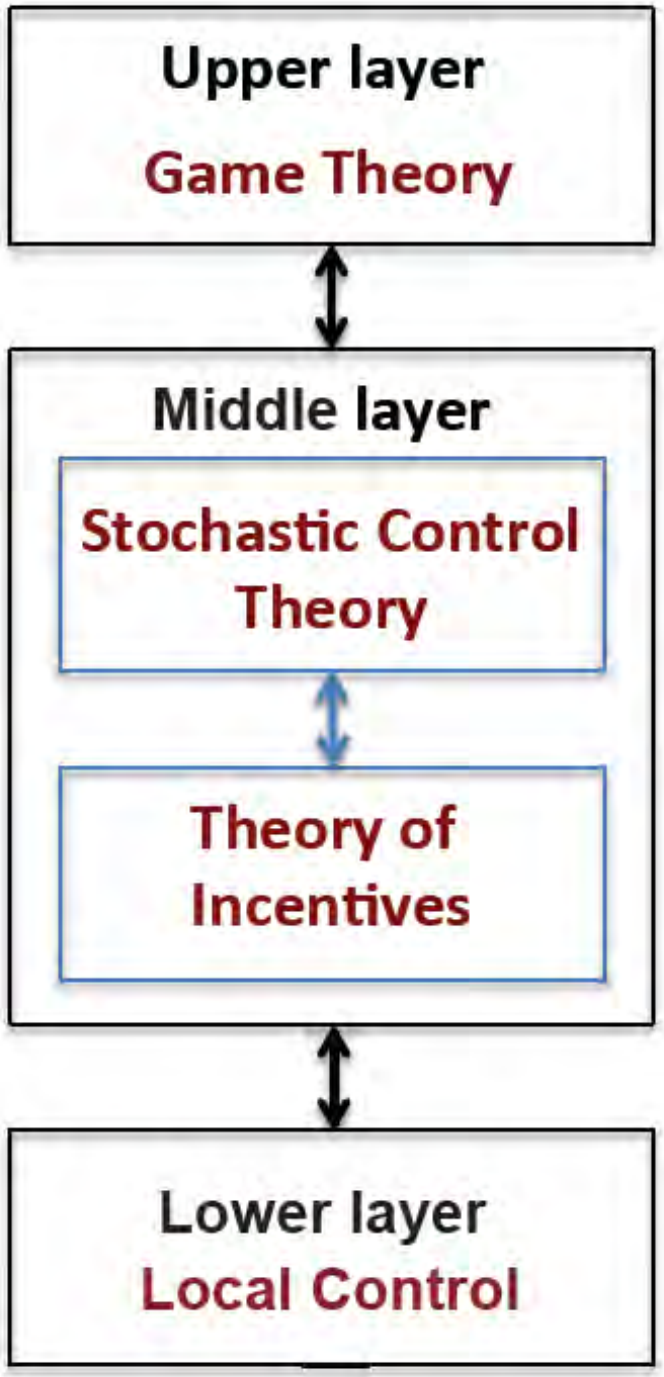
* New models of user behavior
* New trade-offs between
  * Security vs privacy
  * Privacy vs usability
  * Security vs performance
  * …..

Hierarchical approach

* **Layer 1: Game theory**
  * Attacker-defender games
  * Games between strategic entities
  [complete and incomplete info.]

* **Layer 2: Mechanism design & Theory of incentives**
  * Design for networked environments
  * Design for environments strategic entities and incomplete information

* **Layer 3: Resilient control**
  * Network-level (Supervisory)
  * Local-level (regulatory)



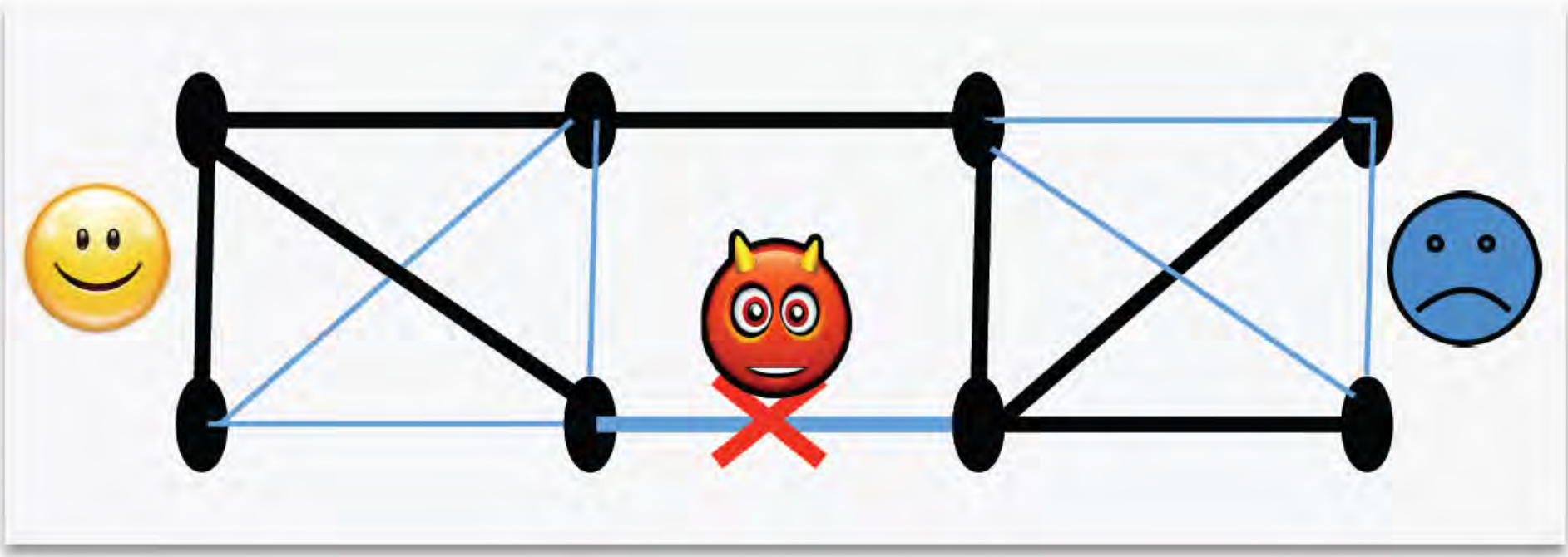
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Hierarchical approach

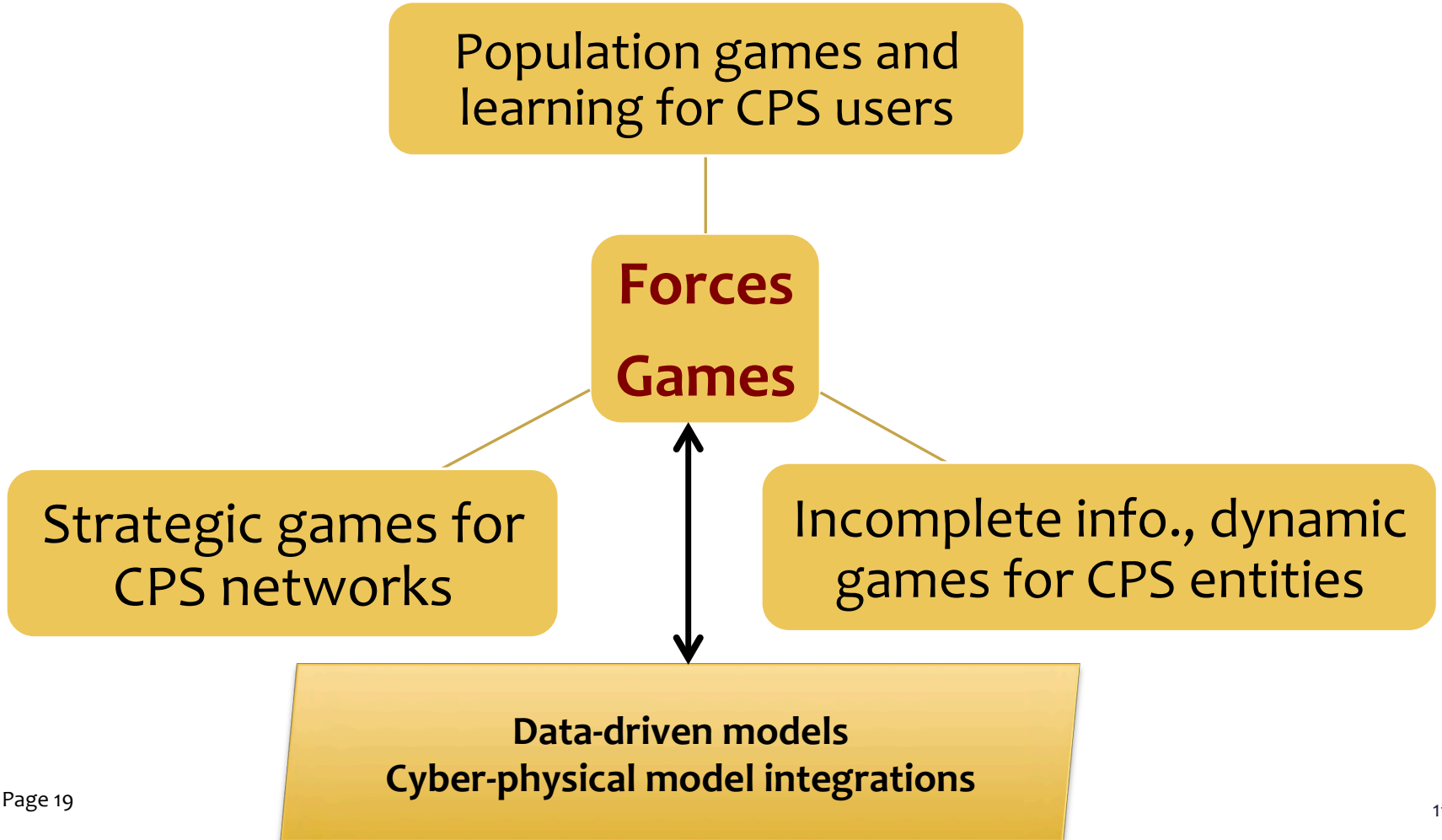
* **Layer 1: Game theory**
  * How the collection of CPS's agents deal with strategic adversary(-ies)
  * Network games that model both security failures and reliability failures
* **Layer 2: Mechanism design and theory of incentives**
  * How strategic agents contribute to CPS efficiency and safety, while protecting their conflicting individual objectives
  * Joint stochastic control and incentive-theoretic design, coupled with the outcome of the upper layer game
* **Layer 3: Resilient network control**
  * Control at each individual agent's site.
  * Control for resilience against network-level attacks and/or faults

Layer 1: Game theory

* How the collection of CPS's agents deal with strategic adversary(-ies)
* Network games that model both security failures and reliability failures

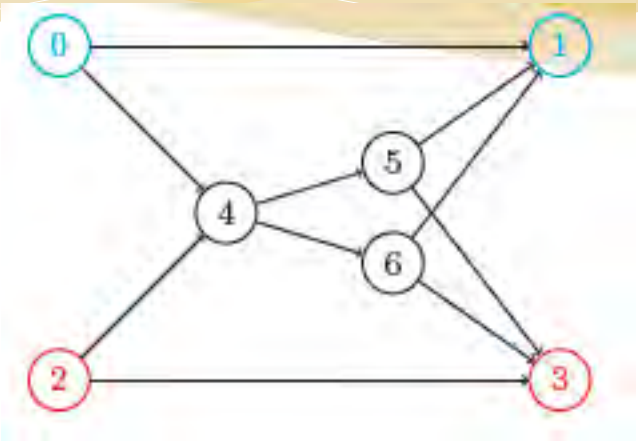


Our focus on Game theoretic analysis



Model1: Distributed routing with heterogeneous population dynamics

- Directed graph (V, E)
- Population k: paths $\mathcal{P}_k$
- Population distribution over paths $x_{\mathcal{P}_k} \in \Delta^{\mathcal{P}_k}$
- Loss on path i of population k: $\ell_i^k(x)$



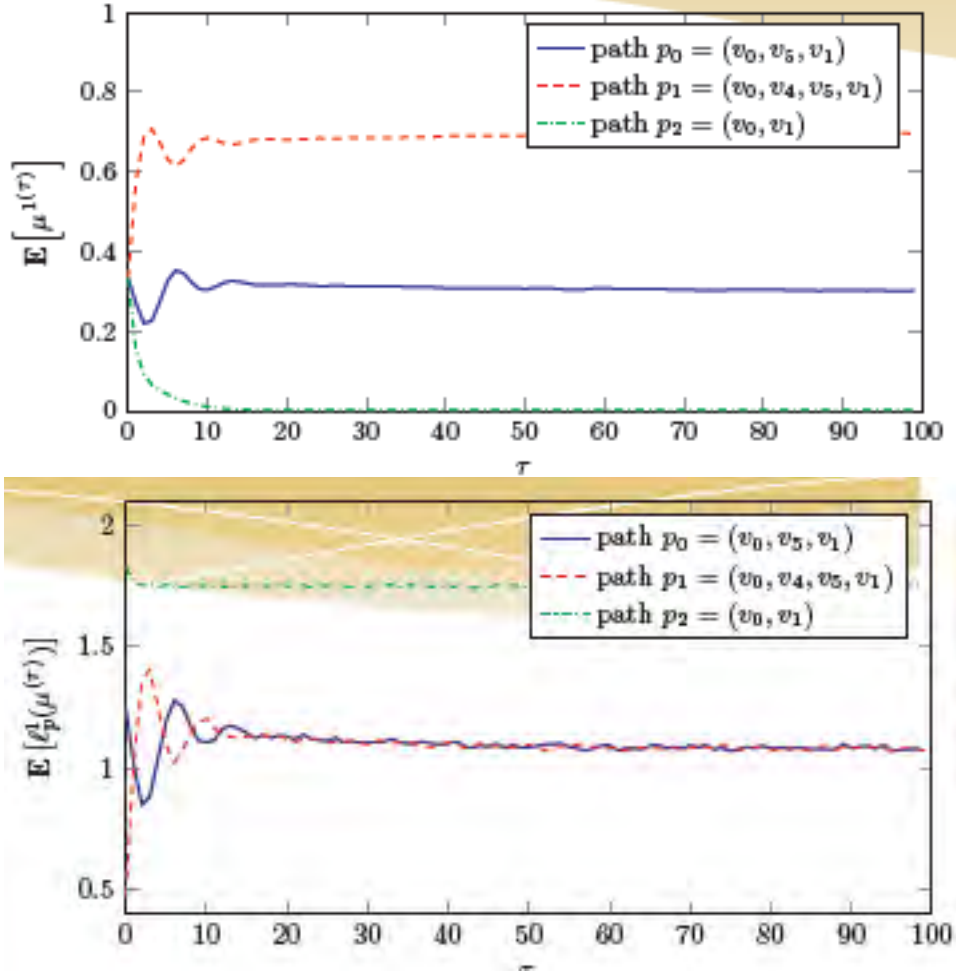
- How do players arrive at equilibrium?
- How fast?
- Stability?
- Robustness (noisy measurements)?

Link collapses

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Distributed routing: main results

* Class of algorithms which are guaranteed to converge, convergence rates.
* Robust to unbiased perturbation, e.g. when losses are not known but estimated.
* Provides a model of population dynamics for optimal control problems, e.g. tolling.



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Model 2: Network Design Game for CPS

A problem of information deficiency

Due to prohibitive costs of determining the cause of a failure, reliability and security failures are frequently indistinguishable.

Game with reliability-security failures

- Network: Undirected weighted graph $G = (V, E, w)$
- Network manager: defender
- Failures:
  - Reliability failure R: Due to *Nature*/random fault (π)
  - Security failure S: Due to a strategic attack ($1 - \pi$)
- How should defender design his defenses?

[G. Schwartz, S. Amin, et al.]

Network Design Game

Attacker-Defender subgame

- Defender: chooses a spanning tree $t \in \mathcal{T}$
- Attacker: chooses an edge $e \in E$

Nature-Defender subgame

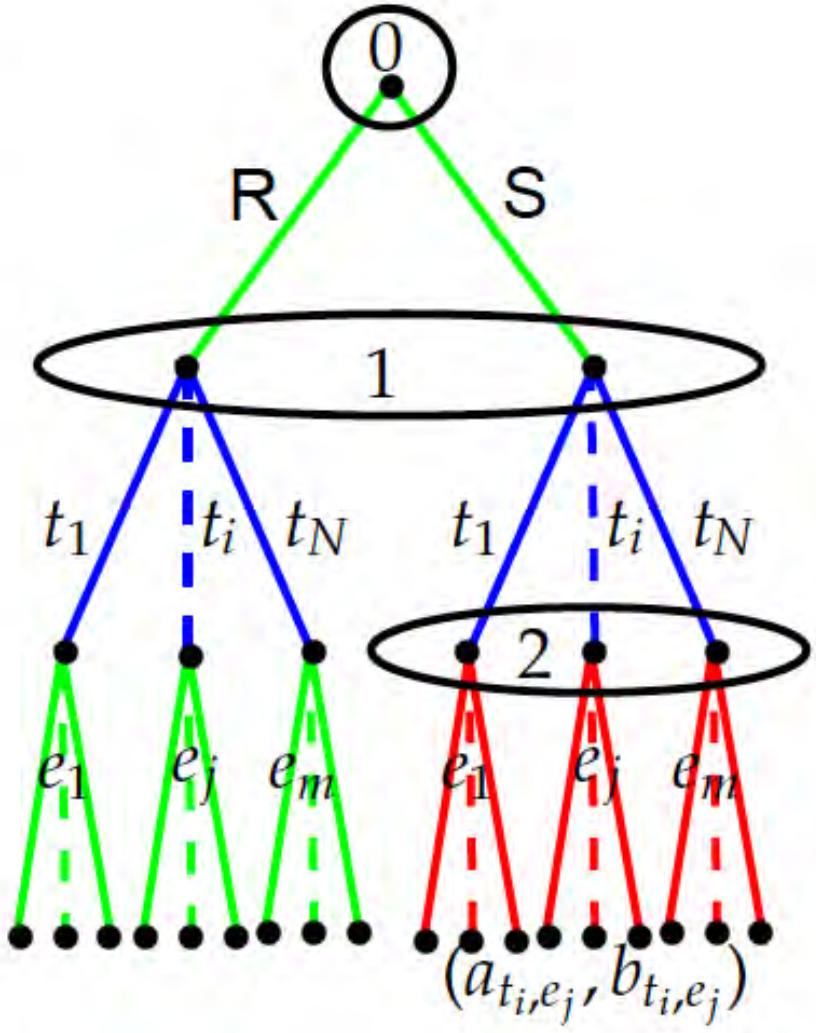
- Defender: chooses a spanning tree $t \in \mathcal{T}$
- Nature: given failure prob. γ_e over edges

Attacker-Nature-Defender game

- Imperfect information: defender faces aggregate failure probabilities:

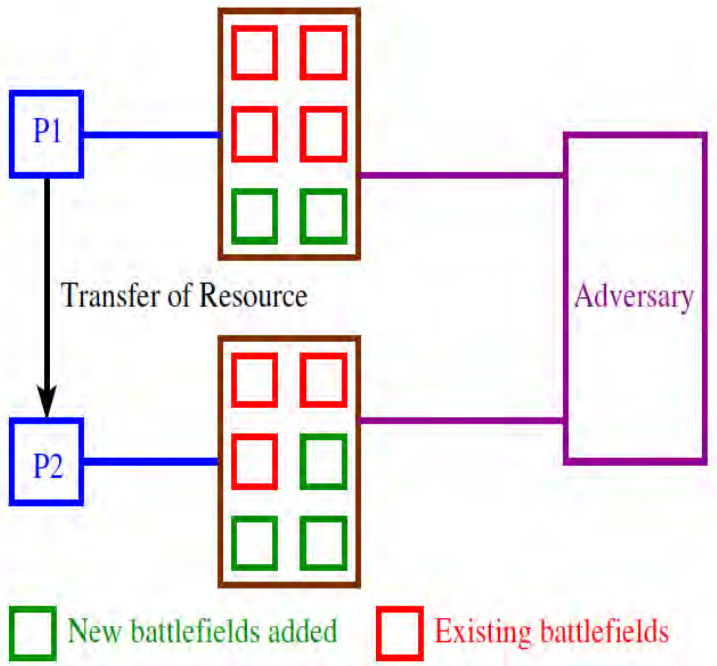
$$P(f_e) = \underbrace{\pi\gamma_e}_{\text{reliability}} + \underbrace{(1-\pi)\beta_e}_{\text{security}}$$

- Common knowledge: π and γ.
- How does Nash Eq. depend on π & γ?



Model 3: Resource allocation [Blotto] games

* Resource allocation in strategic multi-battlefield conflicts
  * possibility to add extra fields and alliances
  * possibility to form alliances (cooperation)
* Offers key insights in strategic resource allocation
* Nash Eq. only in mixed strategies
* Interesting dimensions: Adding battlefields, voluntary coalitions

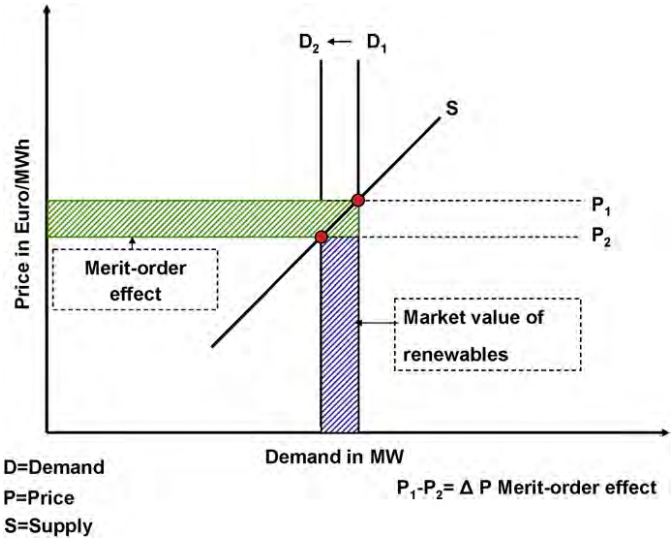


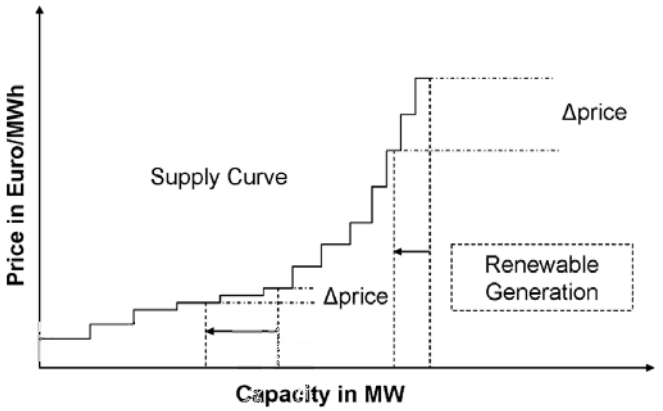
Coalitional Colonel Blotto with Endogenous Battle Fields

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Model 4: Competition with renewable sources

* Oligopolistic competition between partially diversified conventional energy companies & other renewable sources
* Study of the merit order effect (MoE) (reduction in spot price due to renewable penetration). ***MoE is reduced when conventional companies diversify.***
* Characterization of equilibrium under incomplete information about renewable availability (*arbitrary correlation structure*).
* ***Price and consumption volatility are lower when renewable energy availability across plants are mor correlated.***





[Acemoglu, Kakhbod, Ozdaglar 14]

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

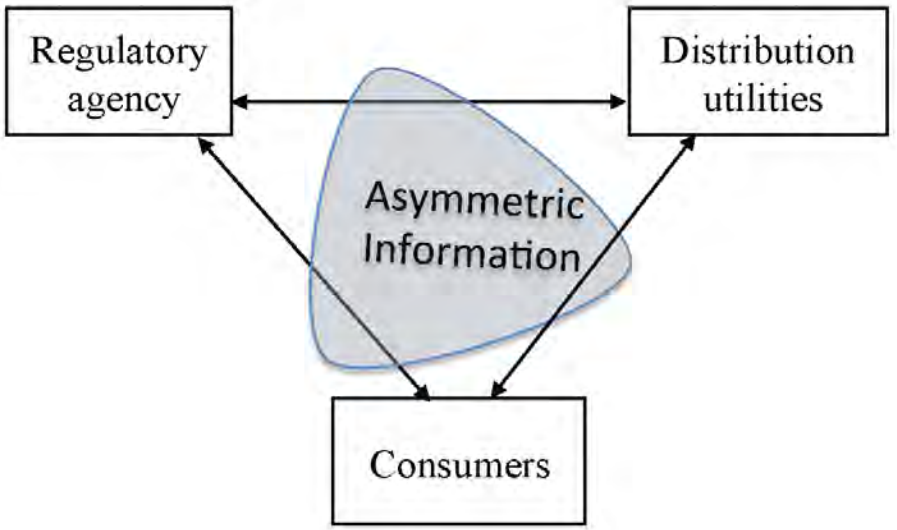
Competition with renewable resources

Ongoing work includes:

* Effect of “network structure" of wind farms on price volatility.
* Optimal pricing when renewable generators have incentive to hold back their supply:
  * Oligopoly pricing with stochastic and correlated capacity constraints:
  * Market design to reduce prices and price volatility.
* Incorporate transmission constraints

Model 5: Security against theft (Distribution side)

* Theft and security in electricity distribution
  * Question: What are the incentives for electricity theft / insecurities under regulatory constraints?
  * Researchers: S. Amin, G. Schwartz, A. Cardenas (UT Dallas)
  * Related work: L. Ratliff, H. Ohlsson, R. Dong, S. Sastry (Berkeley),
  * C3Energy revenue protection project

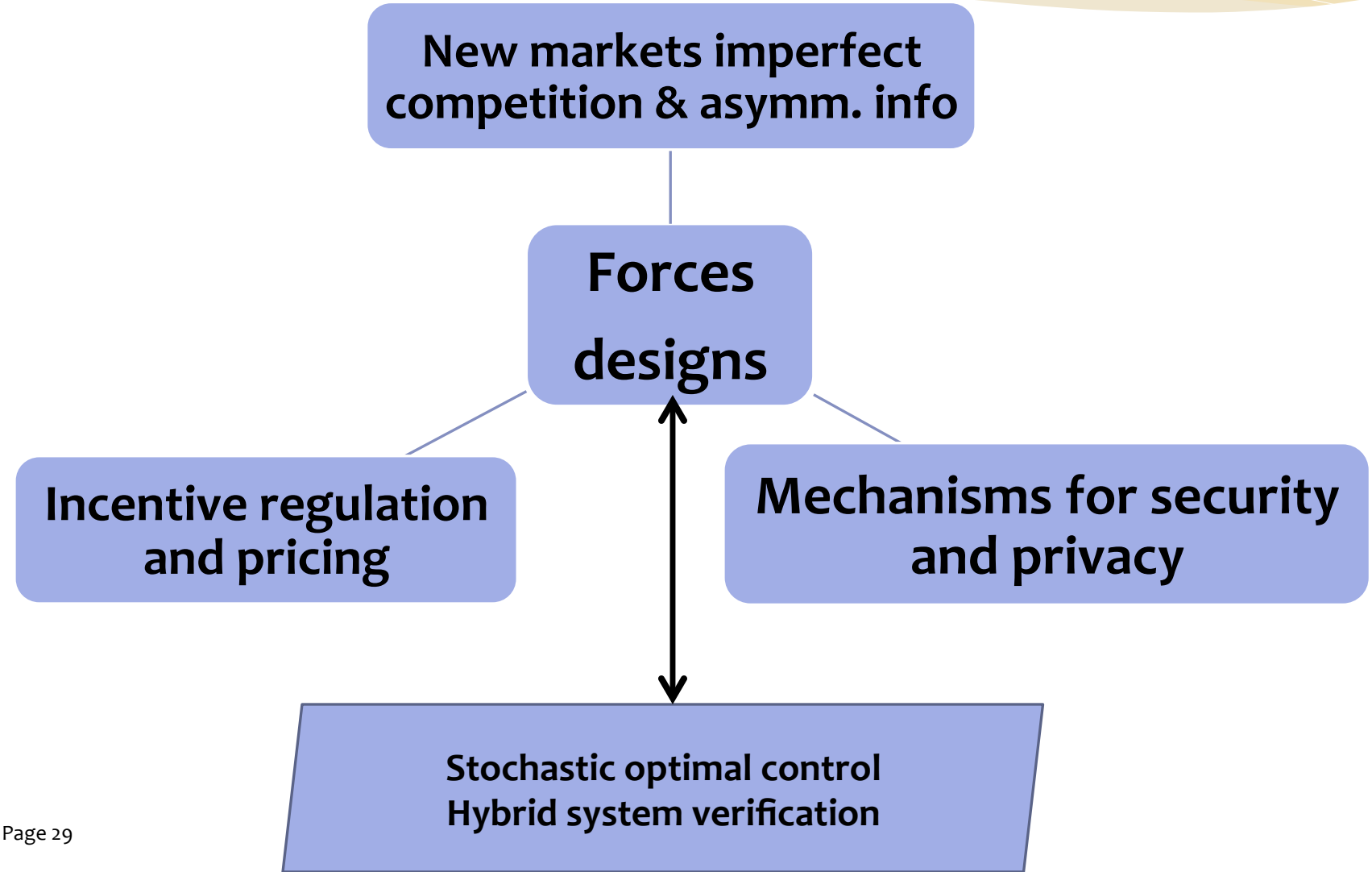


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Contribution: Motoring and enforcement policies for theft management

- Ideas from detection theory and incentive regulation
- Persistent electricity theft in some jurisdictions, but not others. This is the first game theoretic analysis so far!
- Findings:
  - For certain regulatory regimes, electricity distributors make sub-optimal investment in monitoring
  - User steals less when (i) fines are higher (ii) detection probability is higher
  - Distributor invests more in monitoring when (i) costs of monitoring lower (ii) user stealing higher

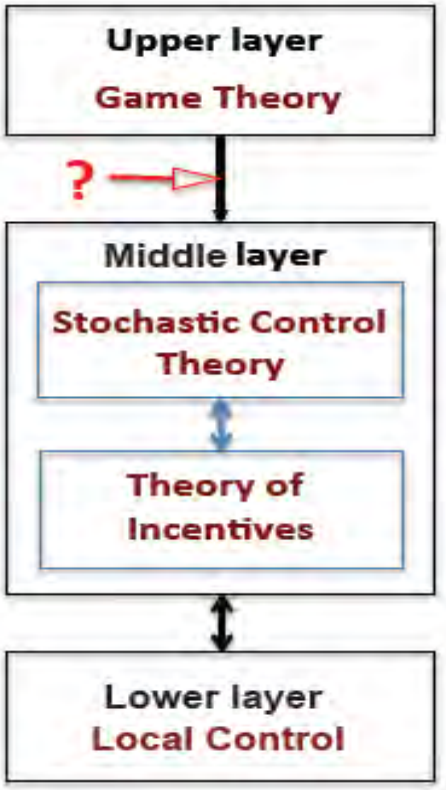
Our focus on mechanism design and its integration with control



Layer 2: Theory of Incentives and Mechanism design

* How strategic agents contribute to CPS efficiency and safety, while protecting their conflicting individual objectives
* Joint stochastic control and incentive-theoretic design, coupled with the outcome of the upper layer game

How to embed the outcomes of upper layer into the middle layer failure models for the design of resilient CPS strategies using stochastic control and incentive-theoretic formulations?

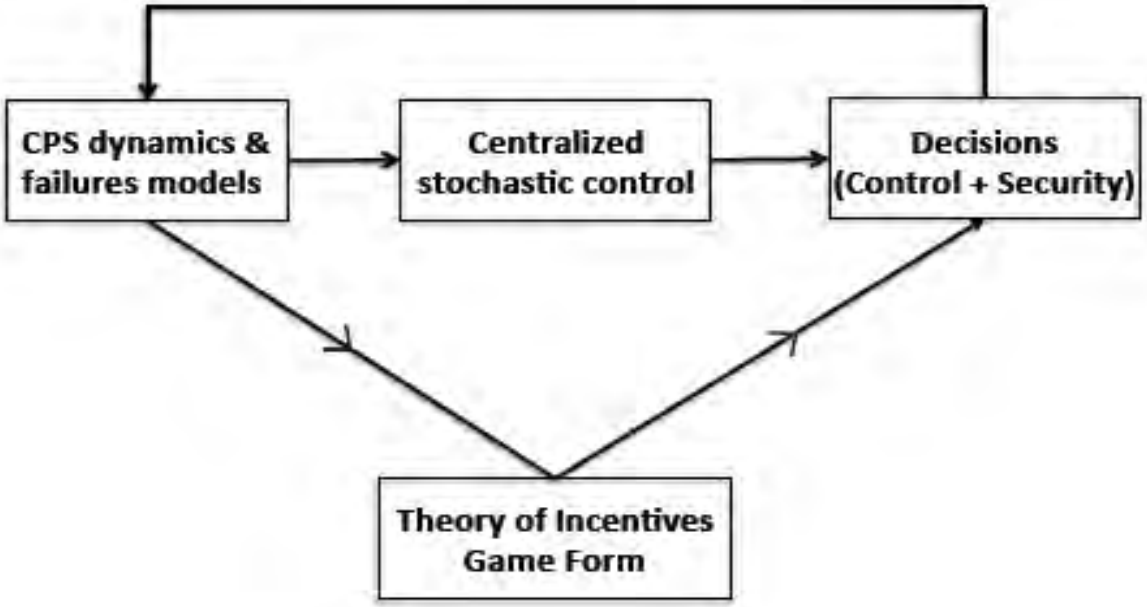


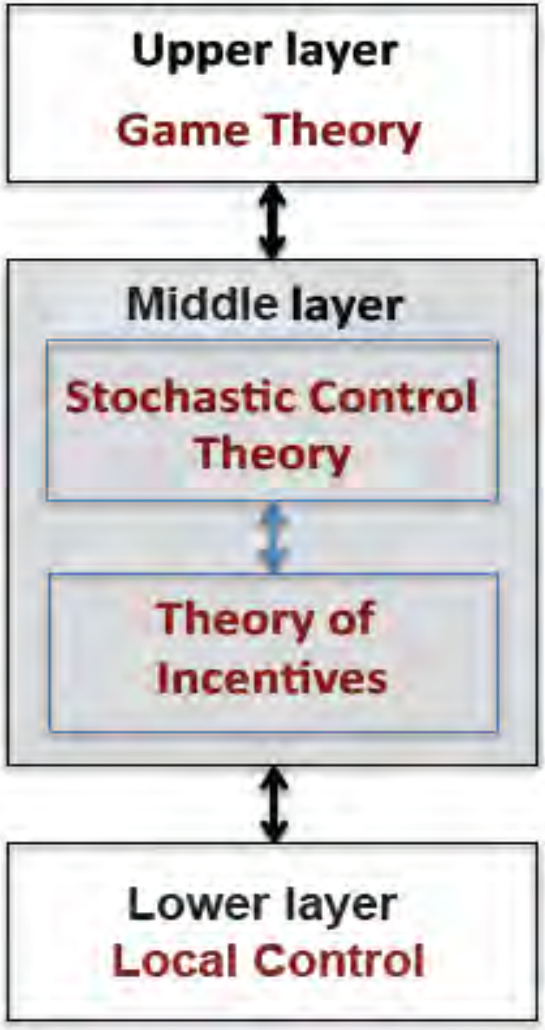
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Middle hierarchical layer

Stochastic control and incentives

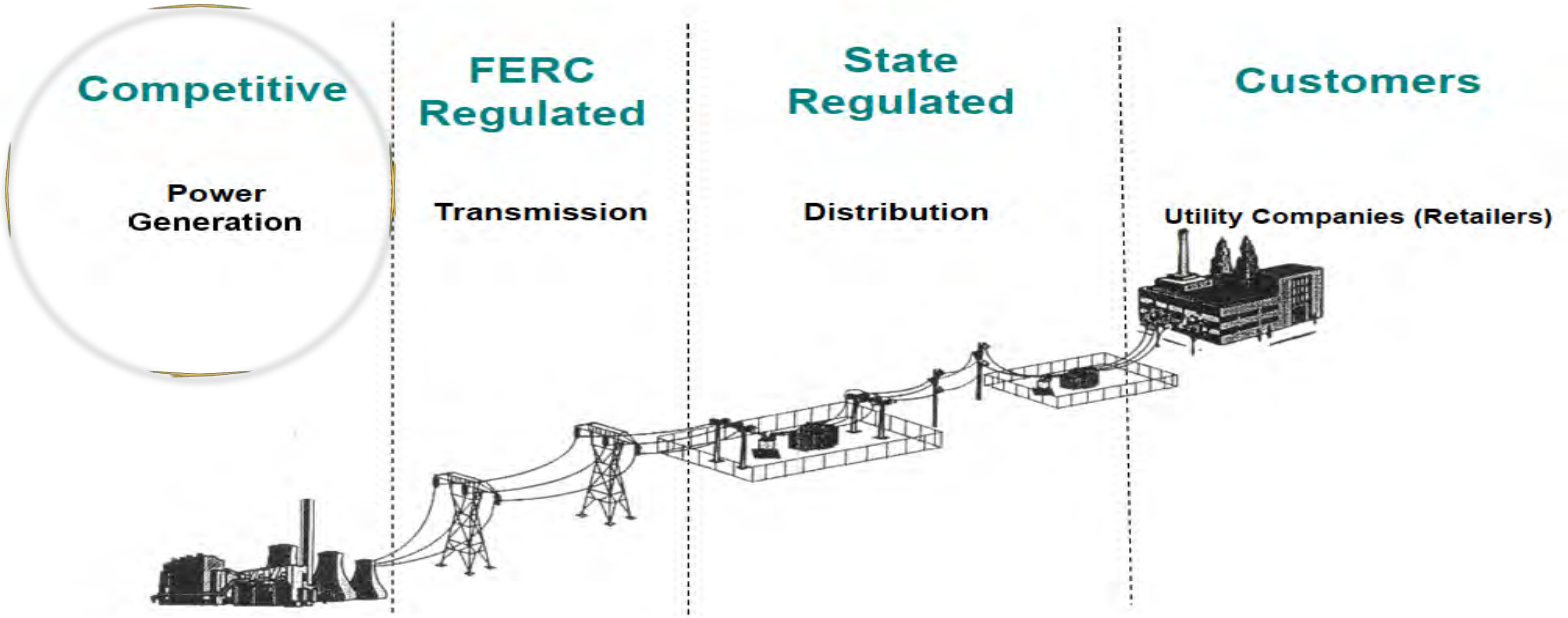
- Stochastic control: Performance benchmark against CPS failures
- Theory of Incentives: implement in appropriate equilibria the optimal control strategies of the stochastic control problem





Design 1: Electricity pooling markets

* Market mechanism for electricity pooling markets
* With strategic producers possessing asymmetric information
* Researchers: M. Rasouli and D. Teneketzis (U of Michigan)



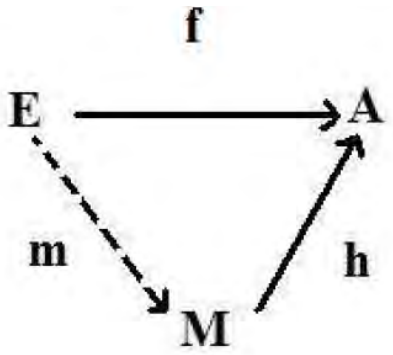
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Common market structure: Supply function model

* Producers bid price-production curves to the ISO
* ISO runs uniform /discriminatory price auction; clears the market
  * Example: California ISO, MISO, PJM, British Markets
* Challenges: Producers may manipulate the market because of
  1. their strategic behavior
  2. private information: production cost function
  3. => markets power due to oligopolistic nature of industry and technical/market features mentioned before
  * Example: 2000 California electricity crisis

Contribution: Novel market mechanism

* Mechanism for electricity pooling market that implements the optimal social welfare correspondence in Nash equilibrium.

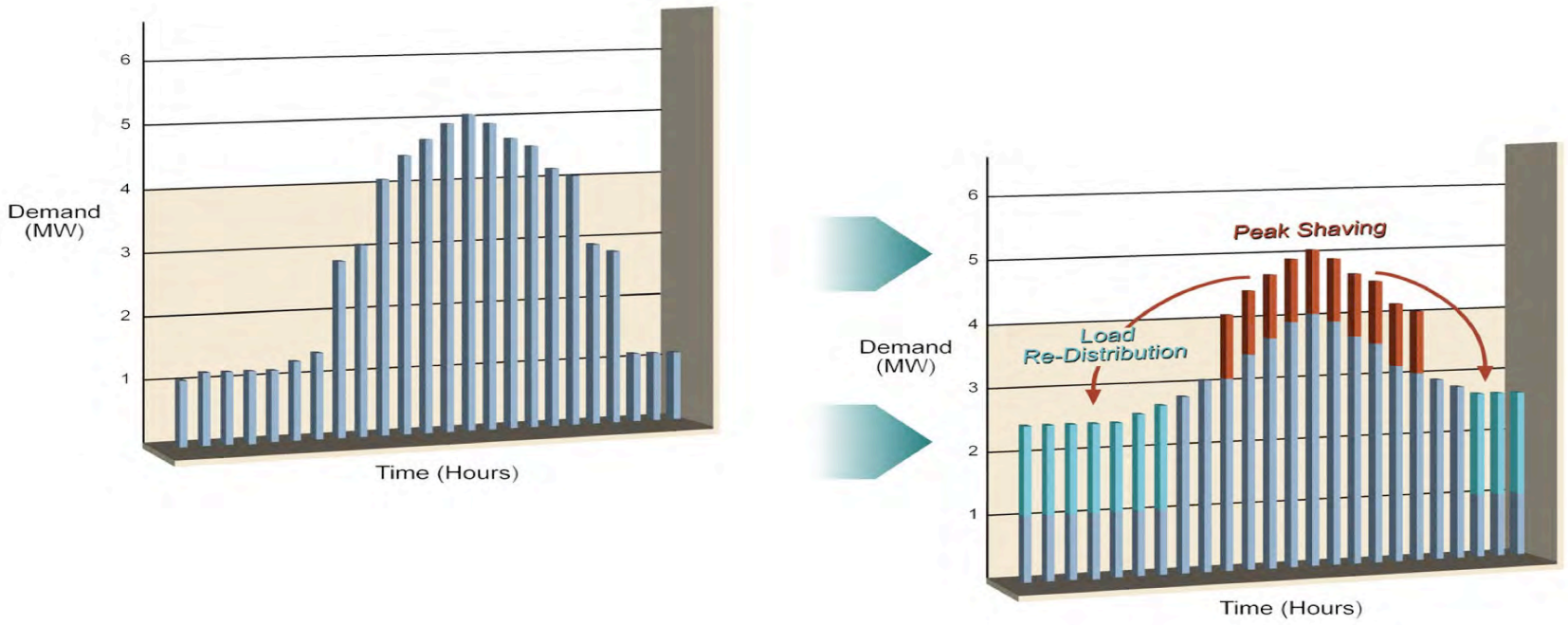


* The mechanism is
  * price efficient (price at equilibrium is marginal cost of production),
  * individually rational,
  * budget balanced.
* Every producer reports one price and one production value.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Design 2: Incentives for Demand management (Distribution side)

* Reward-based demand response for electricity distribution
  * Question: How to incentivize consumers to partly shift/reduce demand?
  * Researchers: G. Schwartz (Berkeley), S. Amin (MIT), H. Tembine (Supélec), S. Sastry (Berkeley)
  * Related work: Direct load control (algorithms + contracts): Tomlin and Hiskens

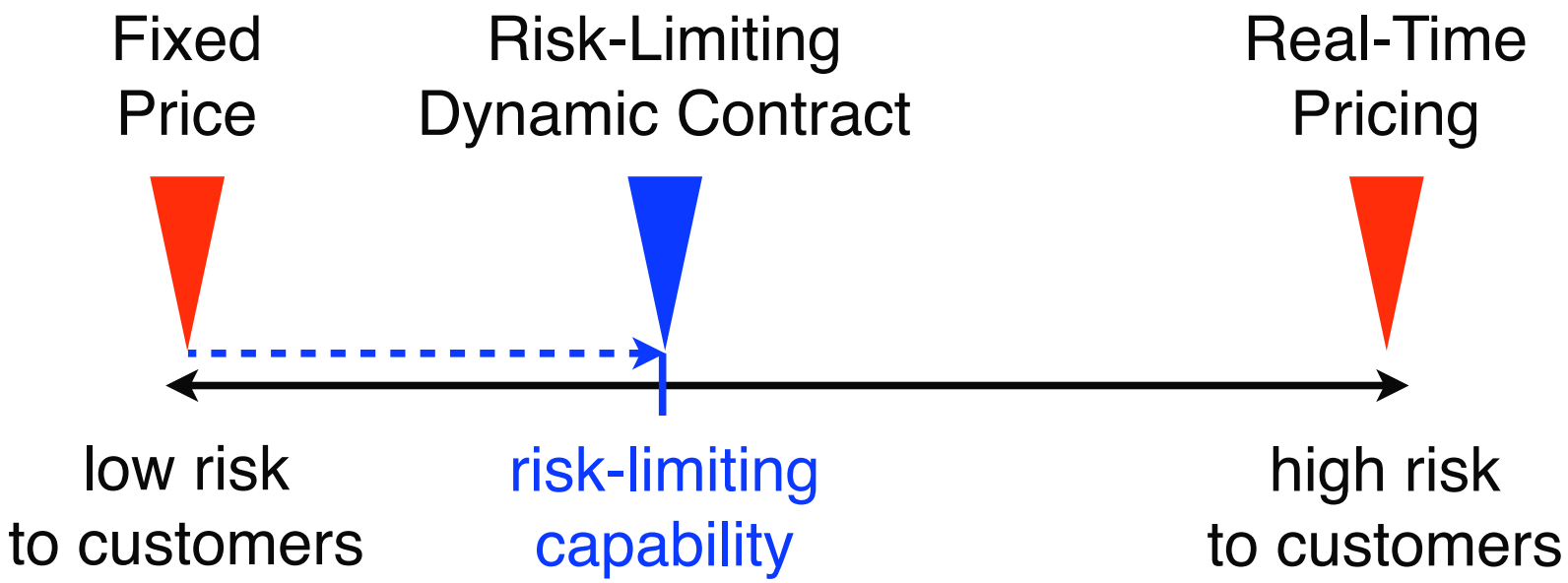


Reward-based demand response mechanism

* Ideas from economics of public good provisioning
* Incentive mechanism: Randomized reward (lottery):
  * user participation is voluntary
  * expected reward of a participating user is proportional to his contribution to the total public good (total shifted demand)
  * users and utility share risks of demand variability (in contrast to real time pricing where risk of demand fluctuations is shifted to users)
  * each user bears risk when it is the cheapest for him
  * both consumers and distribution utility are strictly better off using / employing the incentive mechanism

Design 3: Dynamic contracts for limiting risks in direct and indirect load control

Researchers: Insoon Yang, Claire Tomlin, and Duncan Callaway

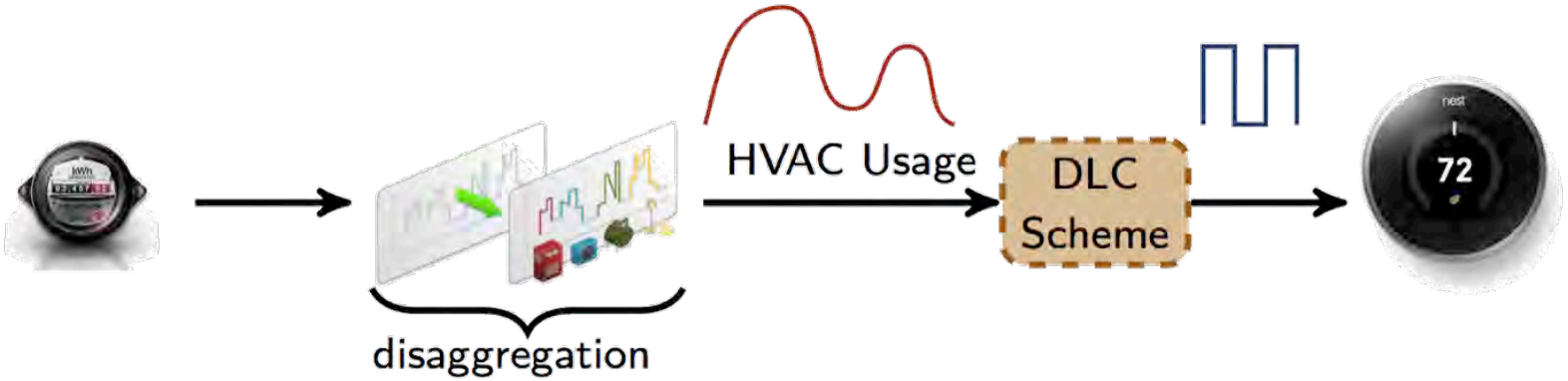


Key Idea: Direct load control + Contract theory

Goal: Capture the benefits of real-time pricing, but manage concerns over risk for intermittent sources of power: wind and solar

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Design 4: Privacy controls for demand management



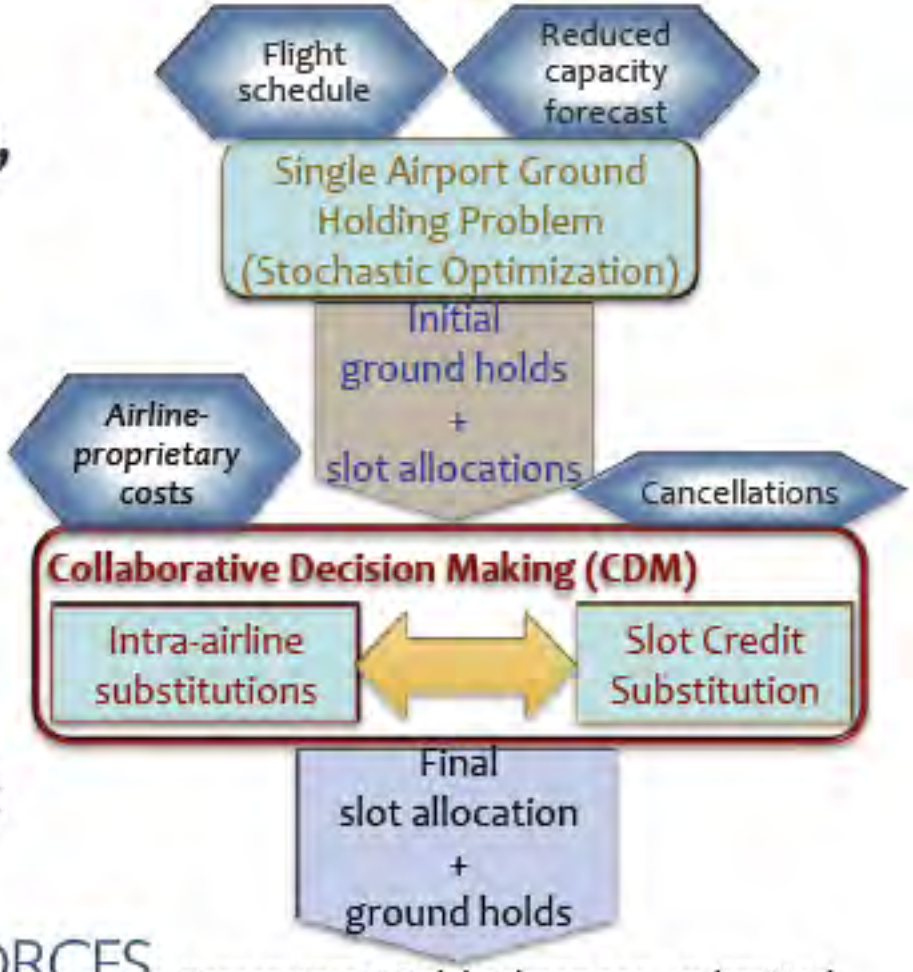
Offer service contracts differentiated according to privacy…

- Utility determines the optimal contract for each privacy type by minimizing its objective subject to:
  - individual rationality
  - incentive compatibility
- Individual Rationality ensures that there is voluntary participation in the contract
- Incentive Compatibility ensures that the consumer's reveal their type truthfully

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Design 5: Evaluation of incentives in collaborative decision making

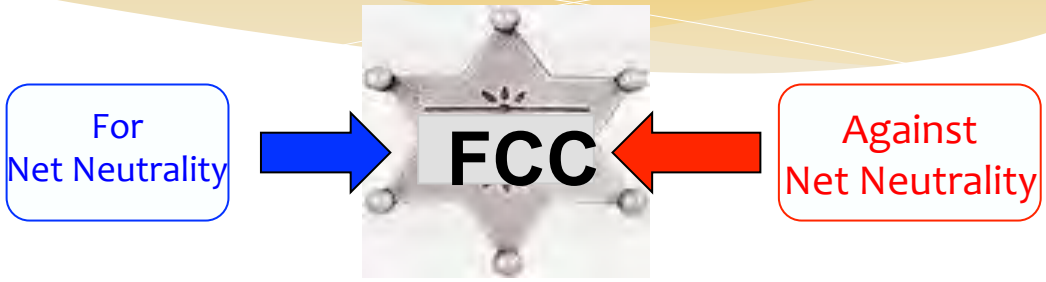
- Simulations of (re)allocation mechanisms with **realistic demand, capacity and operating cost data**
- LGA case study
  - 10-hr Ground Delay Program
  - 27 airlines
  - 20% coefficient of variation in delay costs
  - Demonstrate a tradeoff between adaptability (ability to dynamically replan) and flexibility (available slot swaps for airline)



Ramanujam & Balakrishnan 2013, submitted

Design 6: Network Neutrality

How to harmonize conflicting interests?

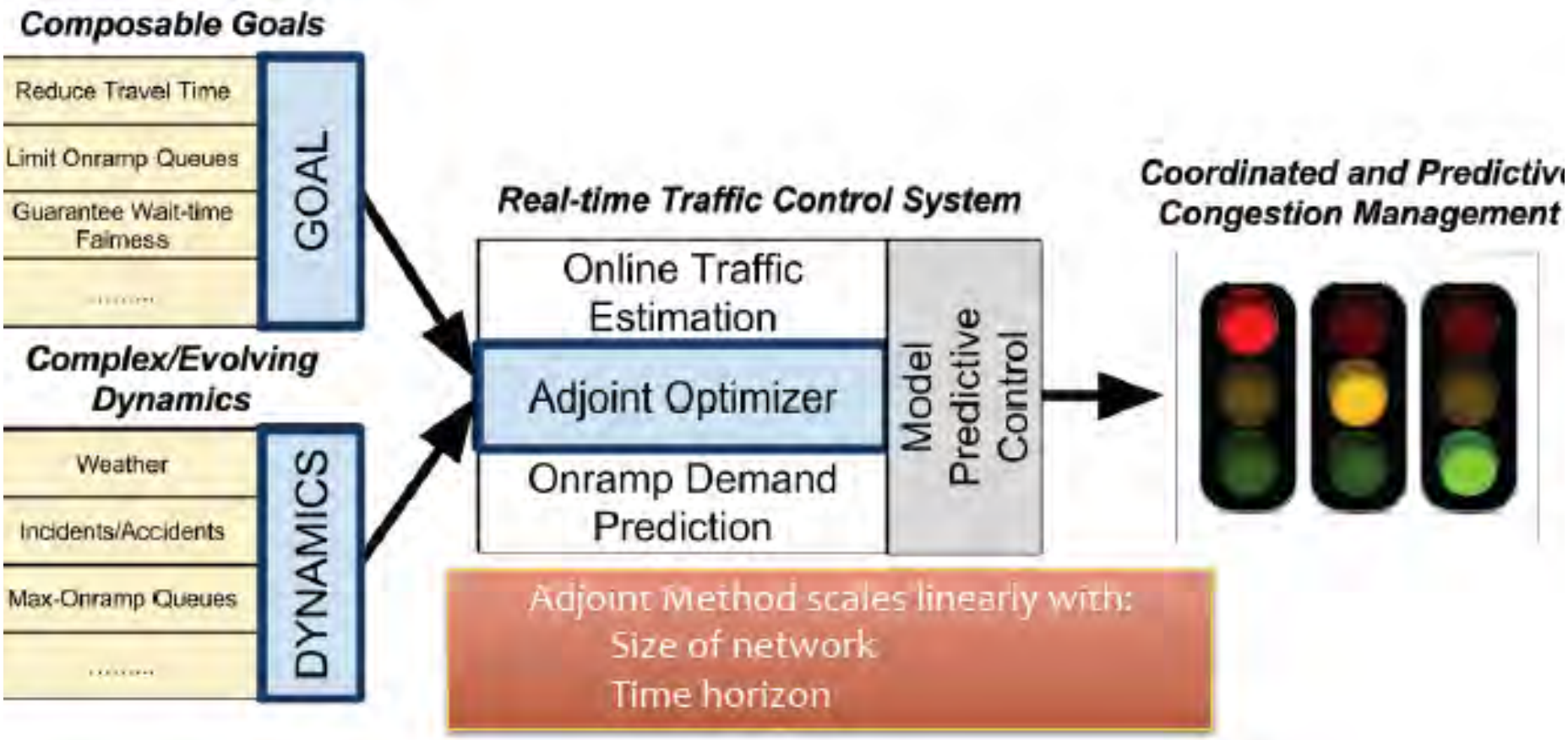


Goals:

1. Enable service differentiation :
   Enable user discrimination
2 Preserve "Neutral Network" :
   quasi-neutral network state

Proposal: To implement x-Model, but only for
- specialized mission-critical services (CPS) only
- (possibly) only at times of critical emergencies

Tool 1: Resilient freeway operations

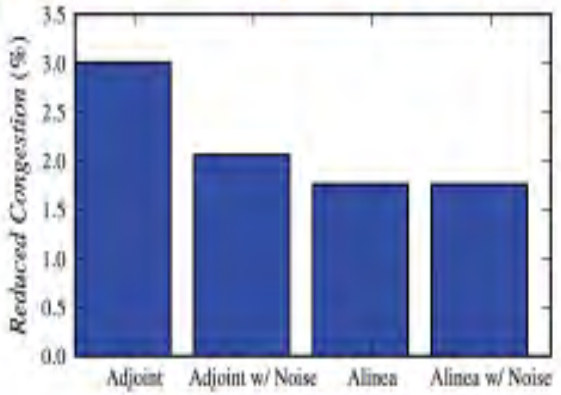


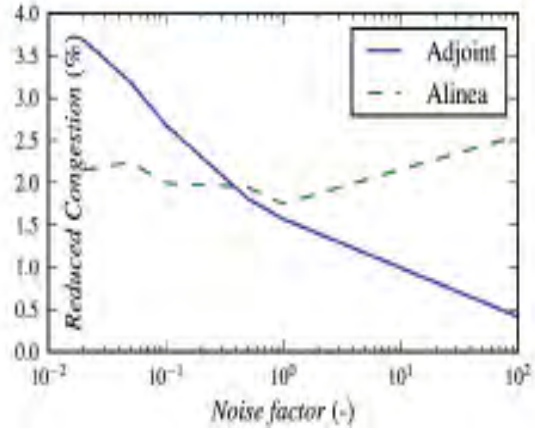
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Adjoint control on I15 simulation

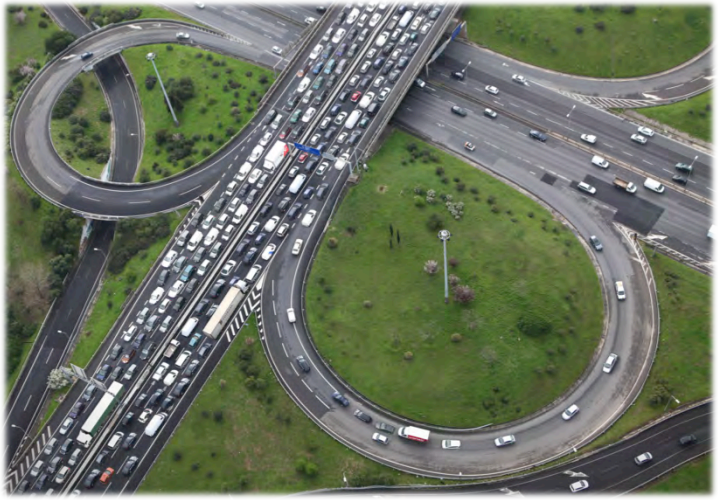
- San Diego I15 Freeway Simulation.

- Overall **reduction** of total travel time over existing feedback-based methods.
- **Robustness** to sensor/prediction noise and model errors.





Resilient Observation Selection using Gaussian Processes



- Large area to be monitored
- Only a limited number of sensors can be placed
  - Cost of deployment and maintenance
  - Where to place the sensors?

- **Observation Selection**

Y predictor variable

$\mathcal{V} = \{X_1, \ldots, X_M\}$ set of possible sensor locations

$$\min_{\mathcal{S} \subset \mathcal{V}: |\mathcal{S}| = N} \sigma^2_{Y|\mathcal{S}}; \quad \sigma^2_{Y|\mathcal{S}} = \sigma^2_Y - \Sigma_{Y\mathcal{S}} \Sigma^{-1}_{\mathcal{S}\mathcal{S}} \Sigma_{\mathcal{S}Y}$$

- **An attacker may try to disable some of the sensors**
  - Sensor placement has to be resilient to such attacks

$$\min_{\mathcal{S} \subset \mathcal{V}: |\mathcal{S}| = N} \max_{\mathcal{A} \subset \mathcal{S}: |\mathcal{A}| = K} \sigma^2_{Y|(\mathcal{S} \setminus \mathcal{A})}$$

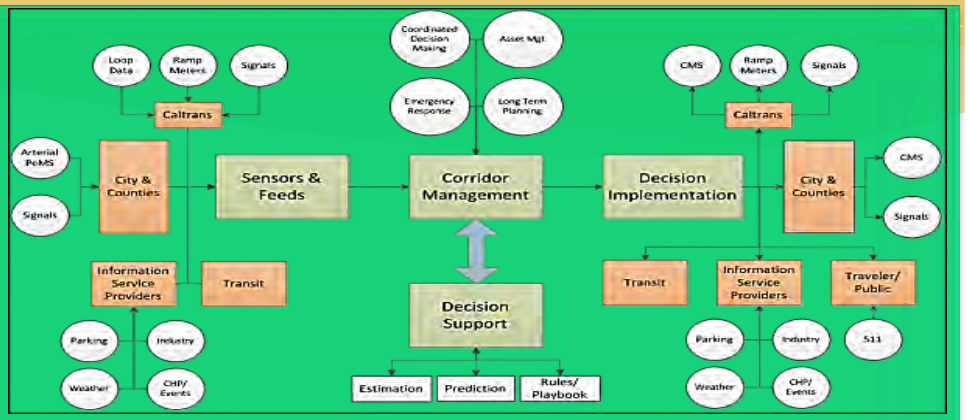
Resilient road traffic networks

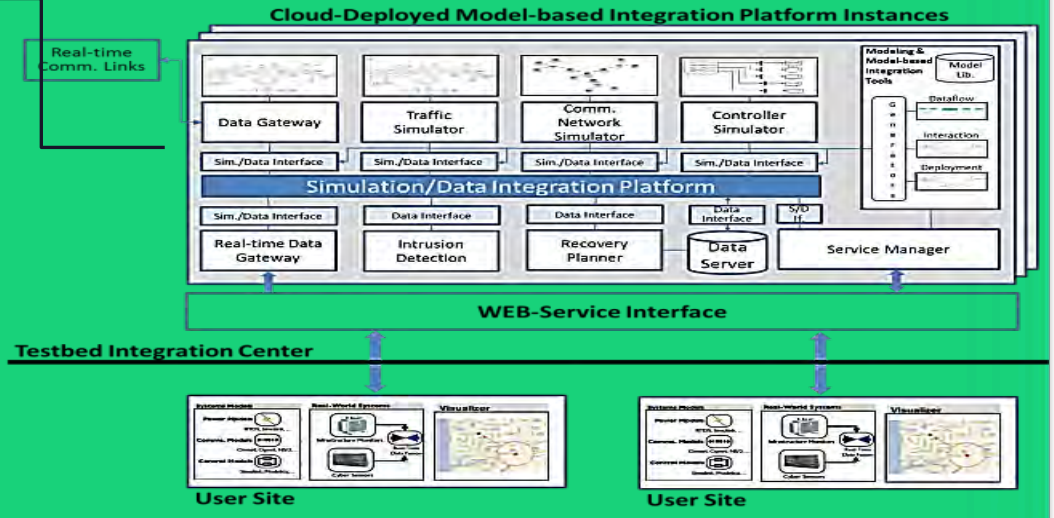
Our Solution:

Connected Corridors (CC)

+

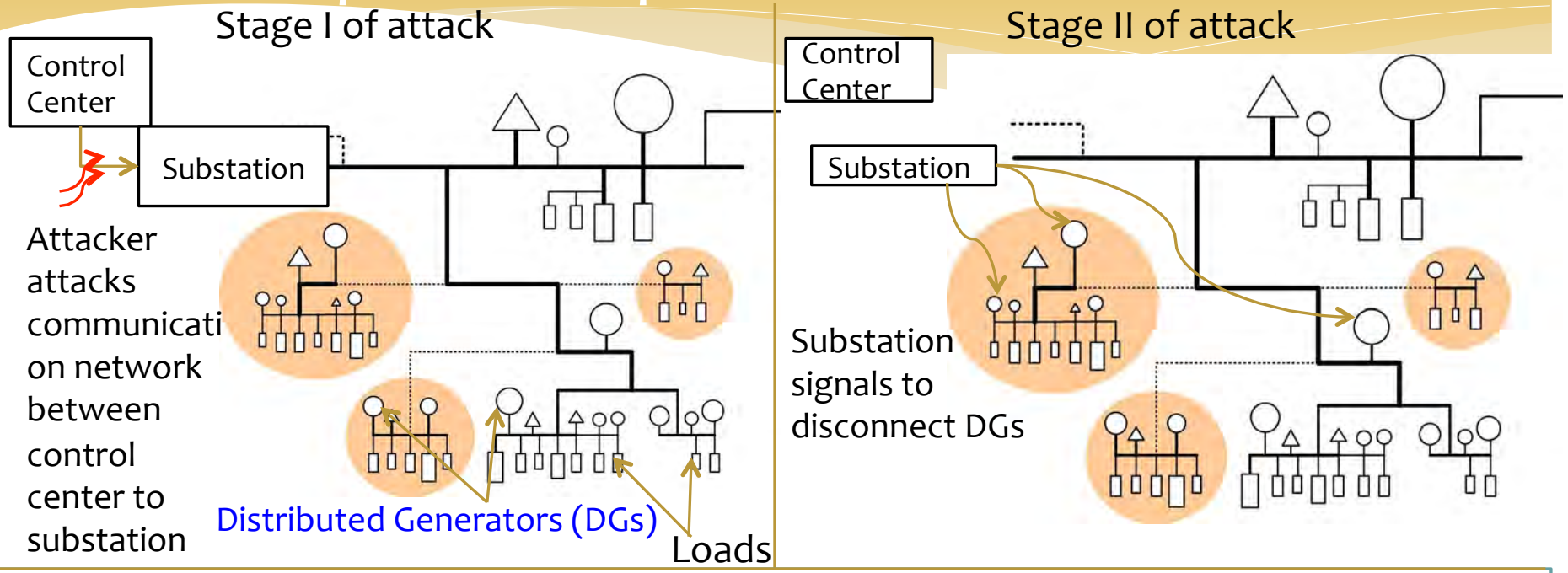
High-fidelity simulation software (C2WT)





Well-managed and resilient traffic flows

Tool 2: Resilient electricity network operations
Optimal response under attacks



Researchers: D. Shelar and S. Amin (joint with EPRI researchers + EDF)
Related works: Attacks to road sensors and controllers: Alex Bayen
Resilient consensus on tree networks: Xenofon Kousoukos

Approach:

i) Model attacker's objectives of load-shedding, equipment damage.

ii) Compute worst-case attack plans and determine optimal response.

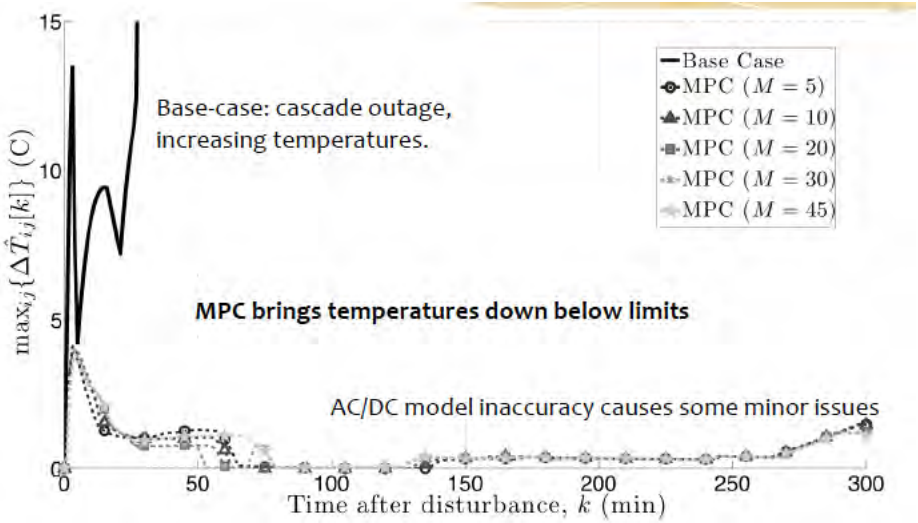
Optimal response under cascading failures

* MPC for cascade mitigation:
  * Assume the system is transiently (10 second timeframe) stable.
  * Exploit thermal inertia inherent in transmission line conductors.
* Use MPC to
  * Control generation, electrical energy storage, wind-spill, FACTS, load.
  * Subject to ramp-rate limits, physical limits
* Hierarchical control
  * Level 1: optimal power flow (with energy storage).
  * Level 2: MPC drives to set-points determined by Level 1.
* Hierarchical control
  * Linear formulation, currently use "DC power flow" for network model.
  * Convex relaxation of quadratic losses, provably tight at optimal.

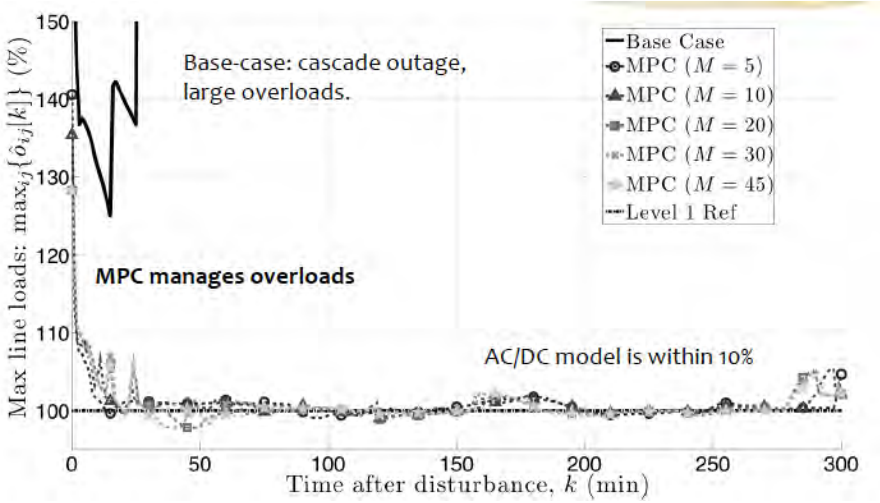
Lead researcher: Ian Hiskens

Test cases: performance results

Max line temperatures



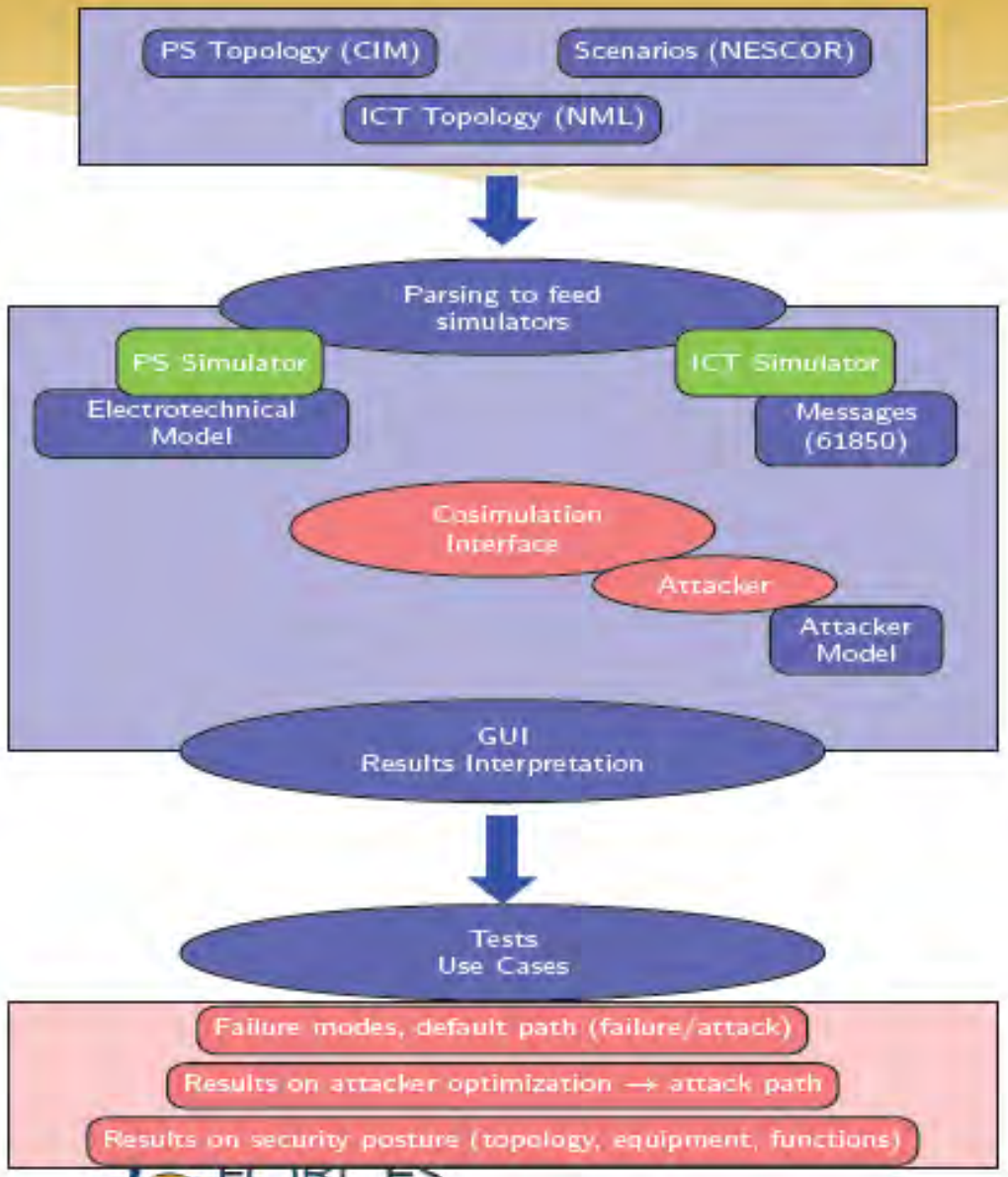
Max line power overloads



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

GRIDNet-D co-simulation testbed

- Inputs
  - Power System
  - ICT
  - Scenarios: Which scenarios to simulate?
- Models
  - Simulations
- Outputs
  - Failure Modes
  - Optimization
  - Security



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Tool 3: Resilient water network operations

* **Resilient Water CPS in Sinapore**
  * MIT, SMART-CENSAM,
  * Visenti Pte., PUB, NRF

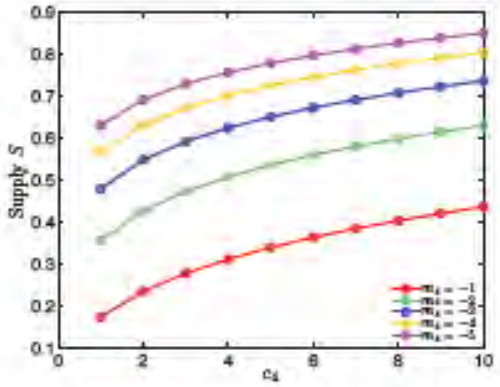
* **SWaT: Secure Water Treatment**
  * Funded by: Ministry of Defense
  * Design review: PUB and SUTD
  * Extensions: water storage and distribution
* **FORCES research contributions**
  * Network control
  * Vulnerability assessment
  * Resilient monitoring and diagnostics

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

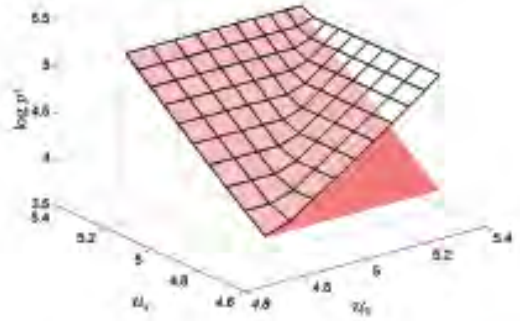
Application

Sensitivity analysis

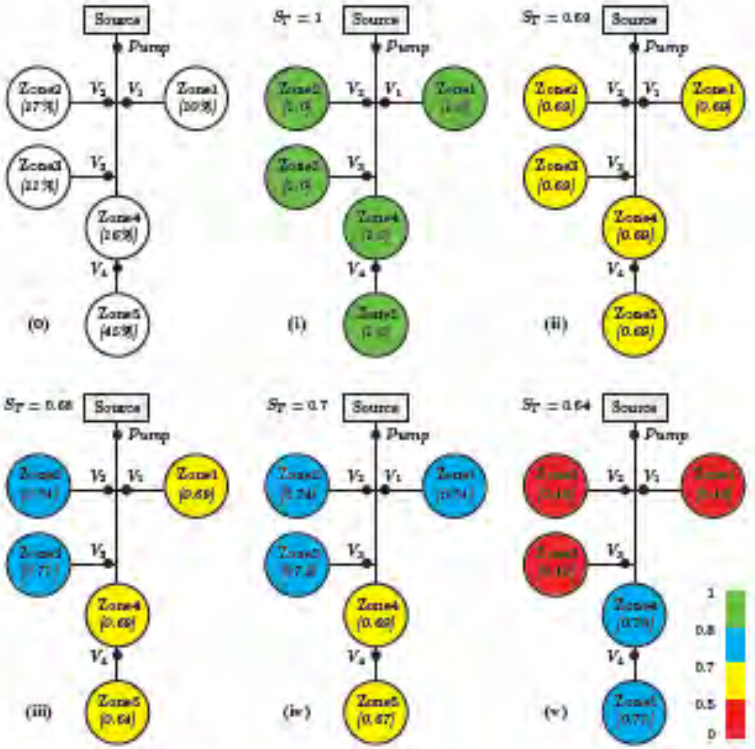
Tradeoff curves:
Demand shedding vs. cost



Perturbation analysis



Demand shedding

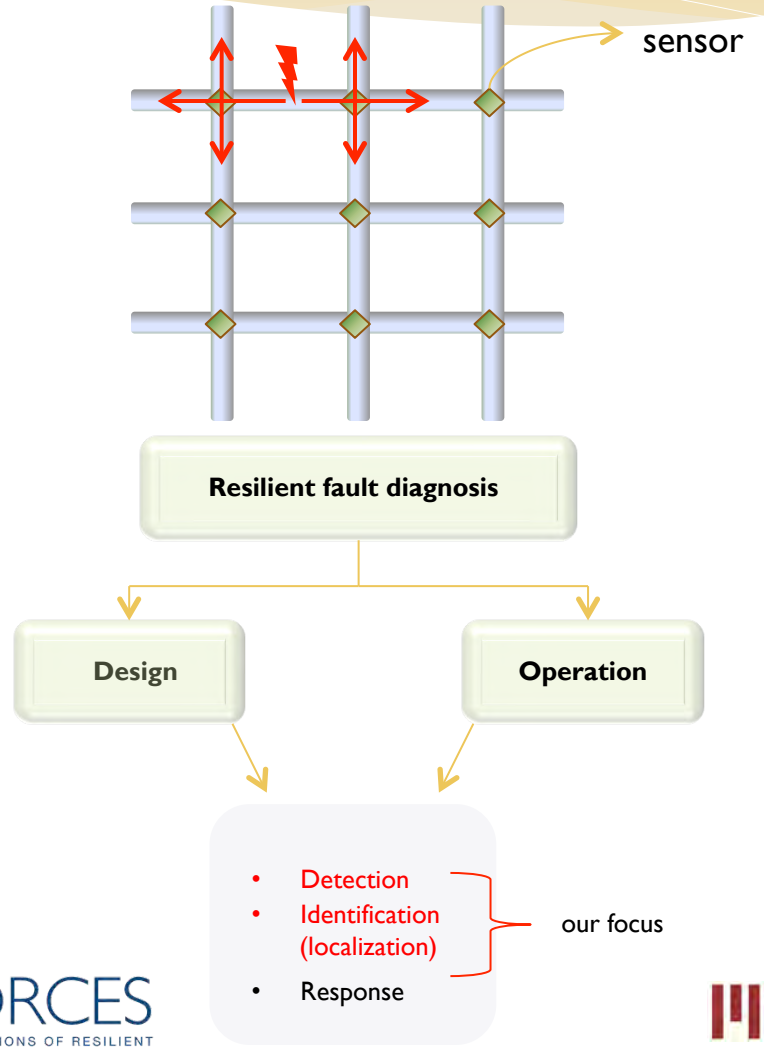


(i) Zero demand shedding
(ii) Limited resources and collective demand shedding
(iii) Limited resources and individual demand shedding with low penalties
(iv) As (iii) with high penalties
(v) As (iii) with mixed penalties

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Fault diagnosis in Flow Networks

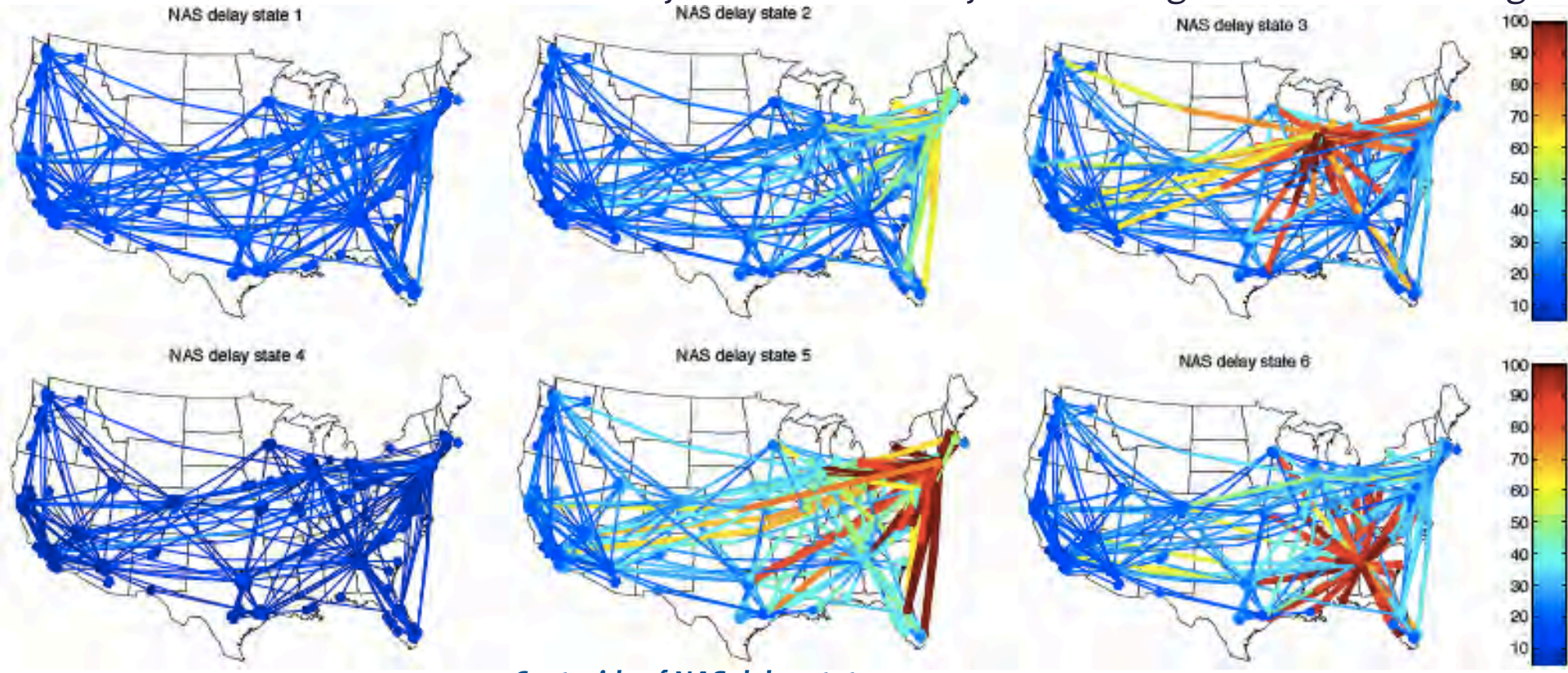
* Objective: For a given flow network, the goal is to distribute the minimum number of sensors that can
  1. Detect a link failure
  2. Localize a link failure (uniquely identify a link failure)
* Approach: Sensor network design for the detection and identification of faults
* Methods: System (flow network, faults, sensor) model, combinatorial optimization
* Performance evaluation: Resilience to random sensor faults and adversarial attacks



[Sela, Abbas, Koutsoukos, and Amin]

Tool 4: Resilient air traffic operations Modeling air Transportation Delays

* Identification of characteristic delay states of entire system through k-means clustering

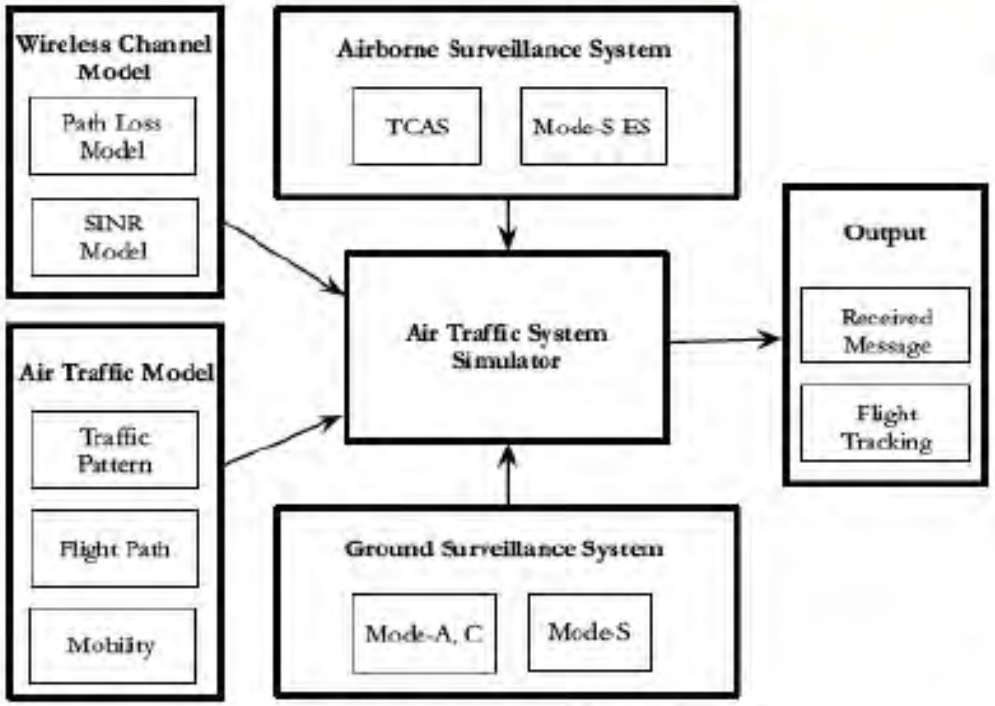


Centroids of NAS delay states.
Color represents median link departure delay over 2-hr time-window

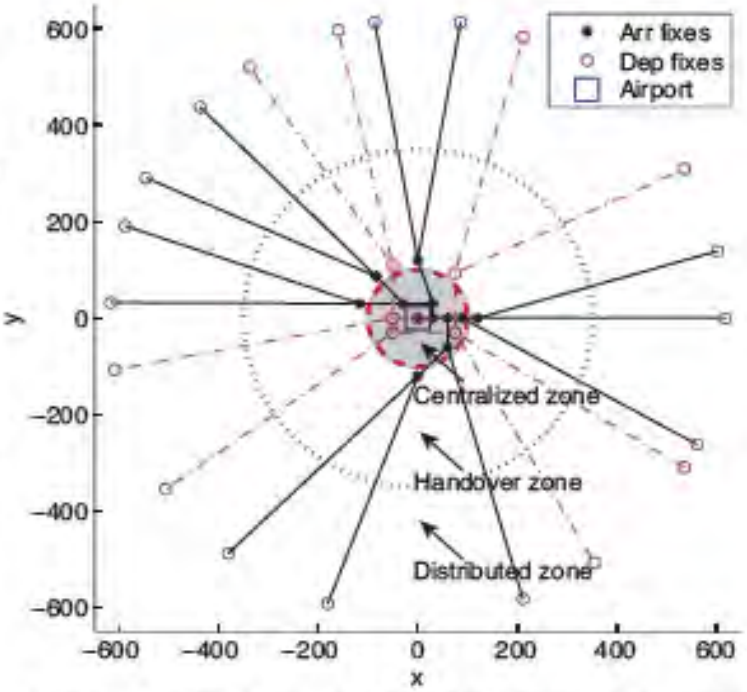
Median link delay in min

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Simulation of Control-Communication Integration



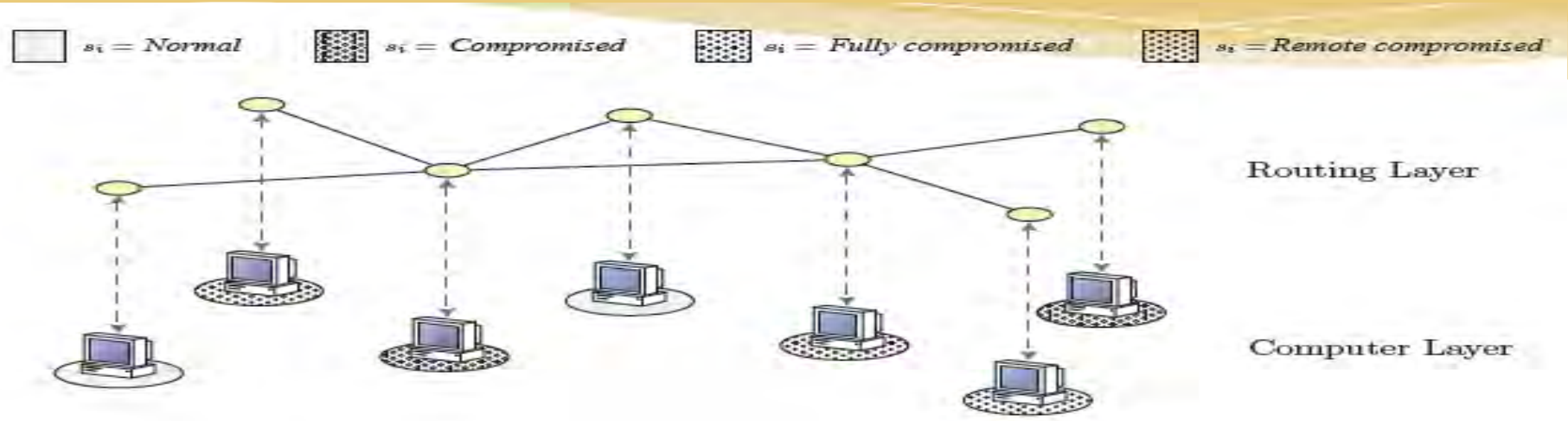
Park and Tomlin, ICCPS 2012



Park et al., IEEE Trans. on Intelligent Transp. Sys. 2013

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Tool 5: Secure control and CPS security



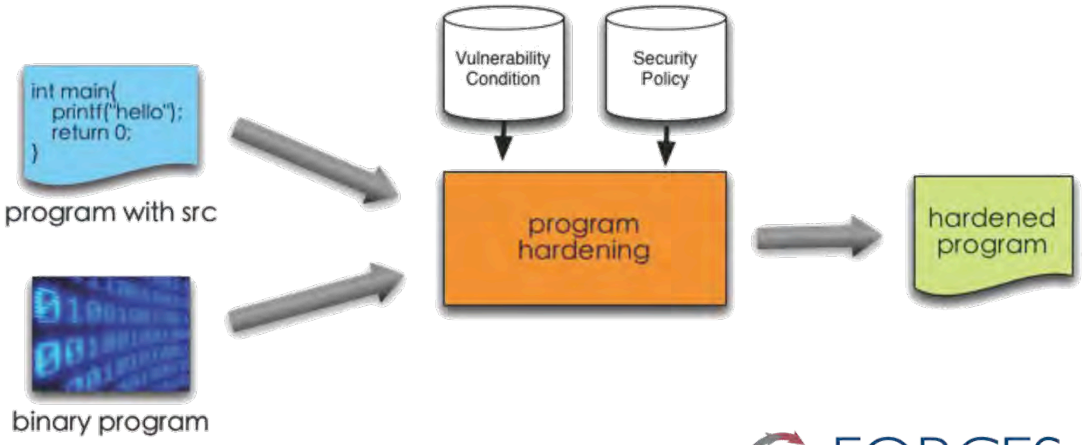
- A supervisory control approach for cyber-security from the defender's viewpoint with
  - progressive attacks,
  - defender's imperfect knowledge of the state,
  - dynamic defense,
  - conservative approach to security,
  - quantification of the cost incurred at every possible state of the system and every possible defender action,
- that achieves
  - quantification of the performance of various defender policies,
  - determination of the defender's optimal control policy (within a restricted set of policies) for a min-max performance criterion.

Program hardening of CPS software

Software inevitably have vulnerabilities.

- human mistakes
- limited resources in CPS

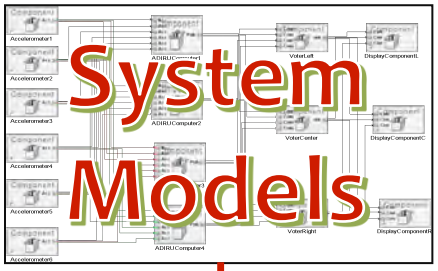
How to protect them from being exploited?



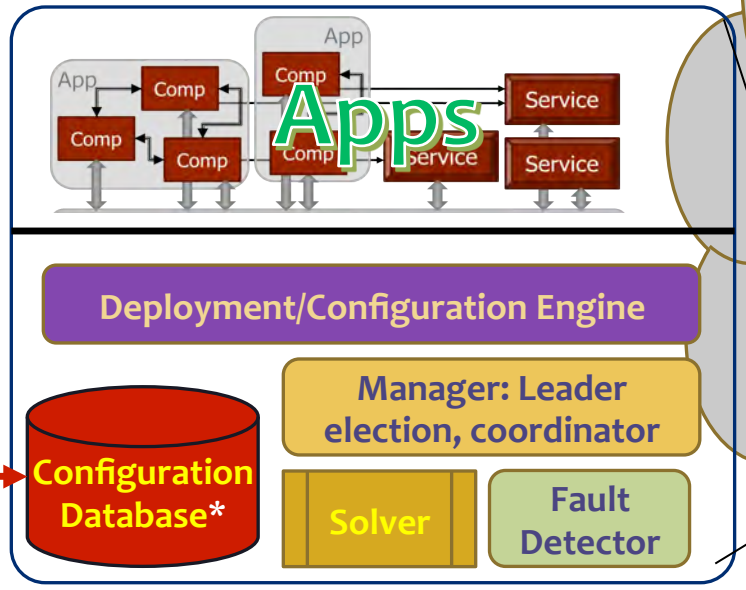
- Fix vulnerabilities
- Deploy security checks

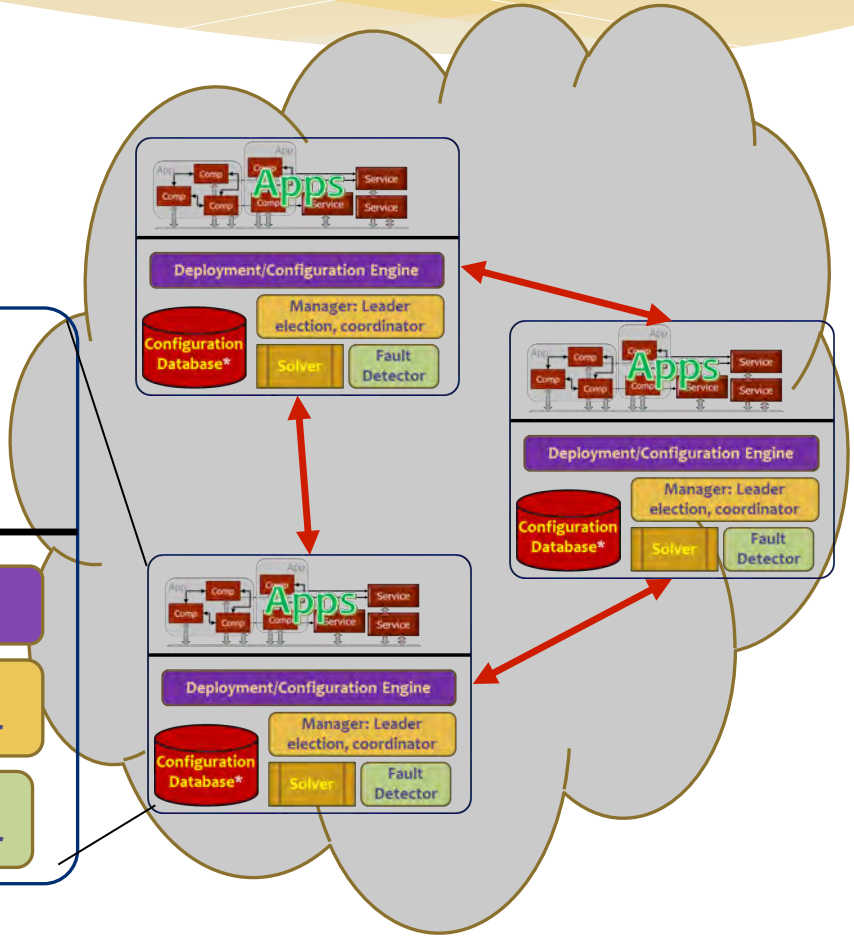
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Towards implementing resilience



Resilient CPS Node:



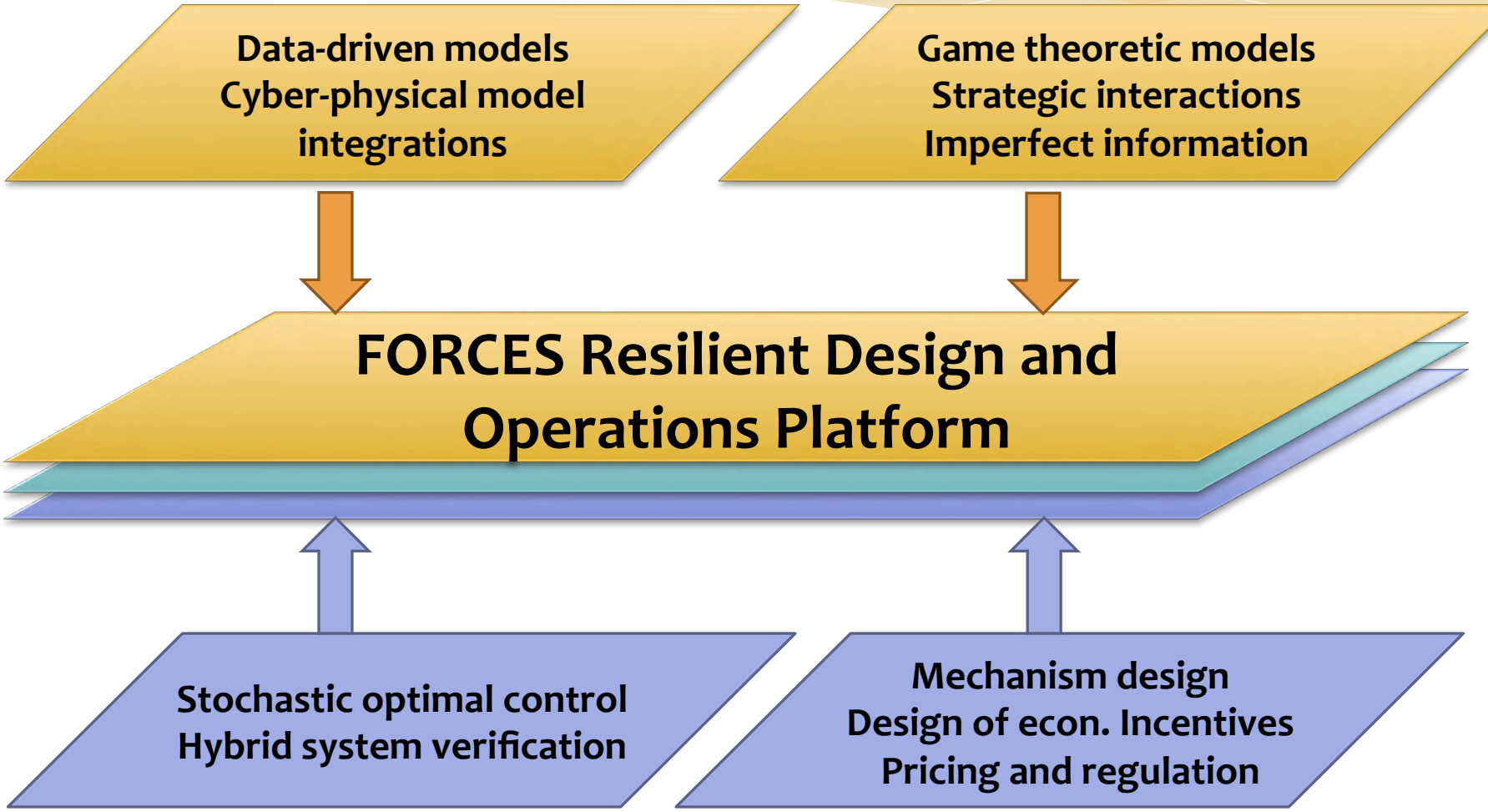


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Embedding Reconfiguration policies in tools: Re-synthesize implementation architecture

* Provide interface for changing required security policies
* Provide models of information flows required to be implemented
* Provide models for security and performance characteristics of communication links and computing devices
* Provide precise specification for the reconfiguration space
* Develop methods for remapping the information architecture to the implementation architecture subject to functional, performance, timing and security constraints

Our final goal



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS