Foundations Of Resilient CybEr-physical Systems (FORCES)

Shankar Sastry[1], Saurabh Amin[2], Hamsa Balakrishnan[2],
Alexandre Bayen[1], Ian Hiskens[3], Gabor Karsai[4], Xenofon Koutsoukos[4],
Asuman Ozdaglar[2], Galina Schwartz[1], Dawn Song[1],
Janos Sztipanovits[4], Claire Tomlin[1], Demosthenis Teneketzis[3]

[1]University of California, Berkeley
[2]Massachusetts Institute of Technology
[3]University of Michigan, Ann Arbor
[4]Vanderbilt University

NSF FORCES Kickoff, April 12th, 2013

Motivation: Resilient CPS

Attributes

1. Functional correctness by design
2. Robustness to reliability failures (faults)
3. Survivability against security failures (attacks)

Tools [Traditionally disjoint]

- Resilient Control (RC) over sensor-actuator networks
- Economic Incentives (EI) to influence strategic interaction of individuals within systemic societal institutions

CPS integrated with human decision makers [Tightly coupled RC & EI]

- Spatio-temporal and hybrid dynamics
- Large number of strategic interactions with network interdependencies
- Inherent uncertainties, both public and private

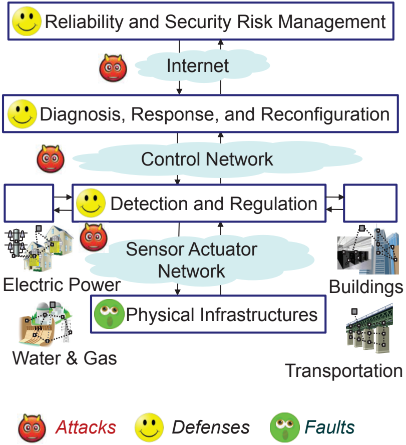
Towards a theory of Resilient CPS

Resilient Control (RC)

- Threat assessment & detection
- Fault-tolerant networked control
- Real-time / predictive response
- Fundamental limits of defenses

Economic Incentives (EI)

- Incentive Theory for resilience
- Mechanisms to align Nash allocations with socially optima
- Interdependent risk assessment
- Insurance & risk redistribution



Functional layers: Regulatory, Supervisory, Management levels

EI-aware RC design

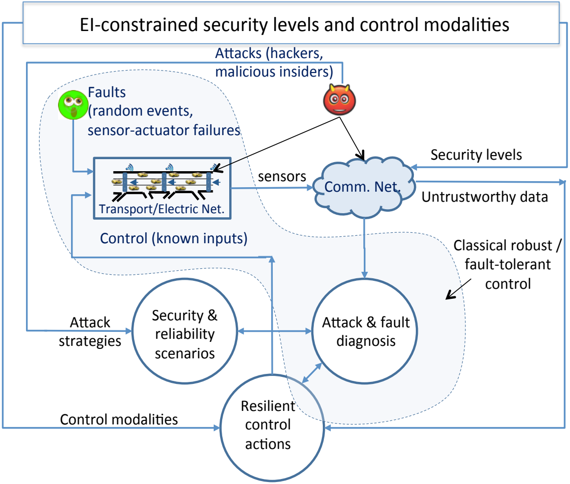
Attack model

- Learn CPS parameters
- Unauthorized access
- DoS / Deception
- Max damage / gain yet evade detection

RC design problem

Max performance subject to

- Security levels & control modalities
- CPS dynamics
- Safety constraints
- Attack / fault hypotheses

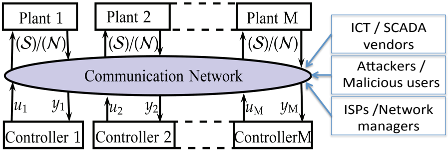


RC with insecure and unreliable cyber (ICT) components

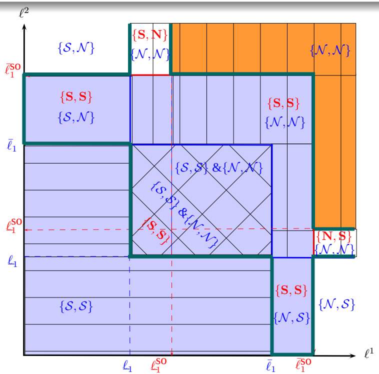
RC-aware EI design

EI for CPS security & reliability

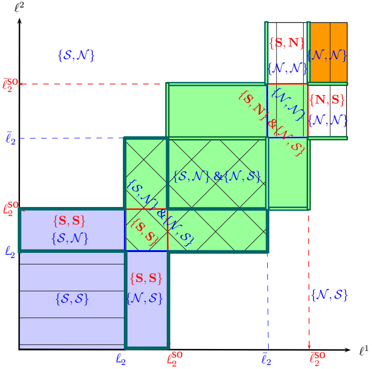
- Network externalities
- Mechanisms design: implement in NE/BNE the social welfare maximizing correspondences



Interdependent security



Increasing incentives



Decreasing incentives

RC+EI: Multi-layer integrated design

Network Games: externalities, investment incentives, residual risk

- Players: Attacker(s), Defenders (CPS owners / Government)
- Failure models: Random, Strategic, Correlated, Byzantine
- Network topologies: Transportation, Electricity T&D, Buildings

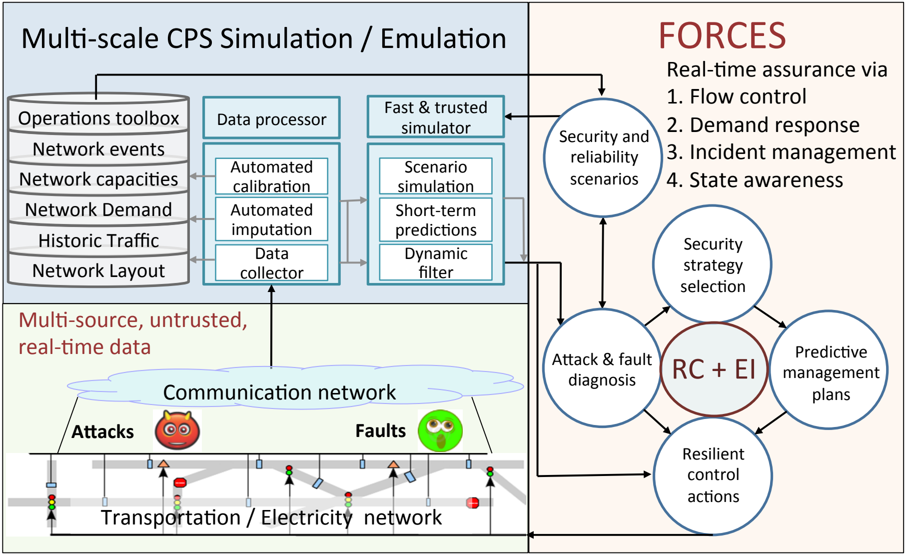
Stochastic Control: learning, minimax control, performance benchmark

- Players: Regulators, System operators, CPS managers
- Public uncertainties: Joint distribution of reliability failures (natural events) and security failures (strategic network attacks)
- Control design: Anomaly / intrusion detection, Safety-preserving (switching) control, Supervisory response (reconfiguration / rerouting)

Incentive theory: Mechanism design, mean-field games (static & dynamic)

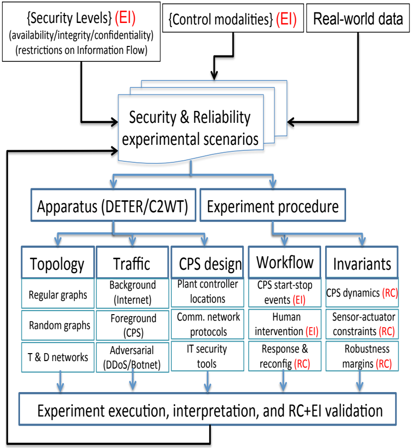
- Players: Distributors, Large population of travelers / consumers
- Private uncertainties: Individual utilities, asymmetric information
- Mechanisms: Public good provision, Demand response / Pricing

Validation approach

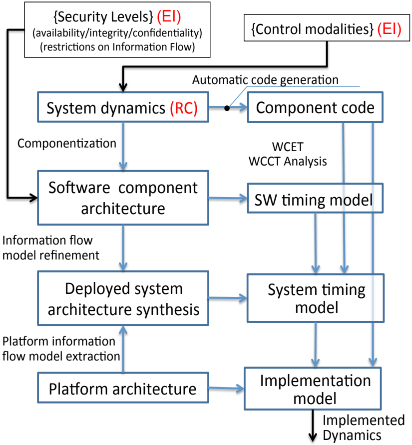


CPS control-security co-experimentation & co-design

Co-experimentation



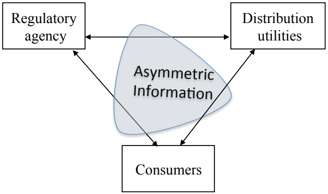
Co-design



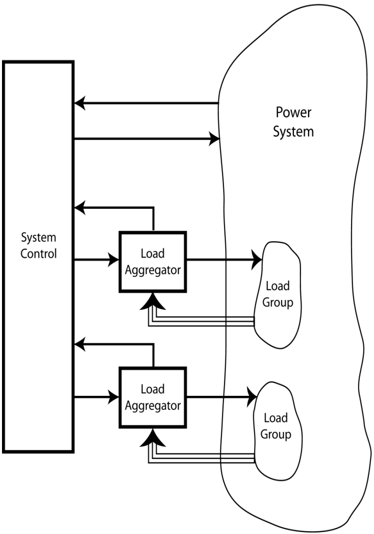
Electricity Transmission and Distribution (T&D)

Wide-area control & Demand response (DR)

- Data: NASPInet (PMUs), NESCOR, IEC & IEEE models, power system simulators
- RC tools: distributed load control, load aggregation (mean-field), balancing (esp. renewables), PHEV charging
- EI tools: DR pricing schemes, T&D regulation, ↓ (non-)technical losses



Regulated electricity distribution

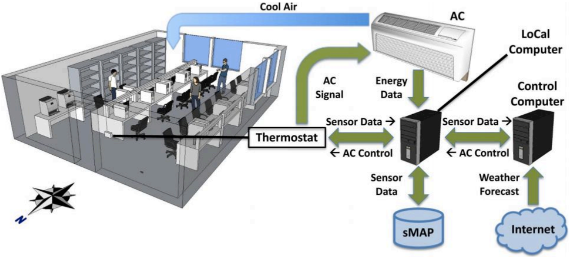


Distributed load control

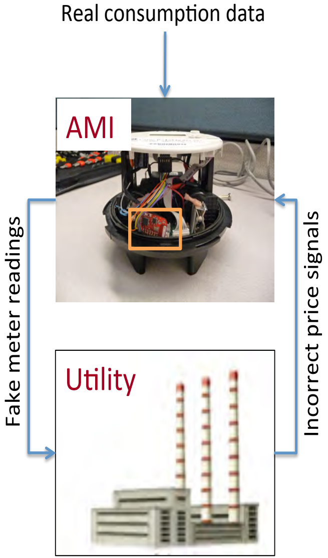
Smart meters and utility networks

Building energy management & DR incentives

- Data: Utility pricing, building operations and loads, consumption patterns
- RC tools: Data fusion, model estimation, integrating occupancy, price, & weather predictions, model-predictive control
- EI tools: Residential DR, AMI security & privacy, ↓ electricity theft/non-payment



BRITE testbed at UCB

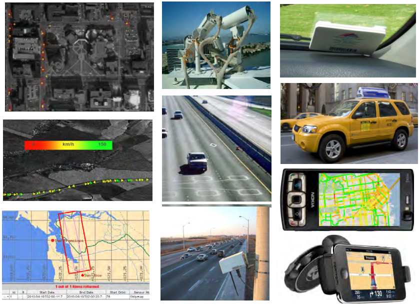


Attacks to AMIs

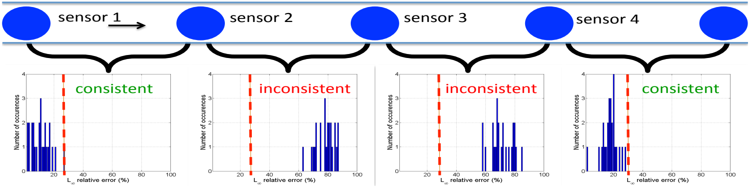
Road Traffic Operations

Mobile Millennium System

- Industry grade platform
- 60 million data points/day
- Tools: Data fusion & consistency, privacy preserving sampling, nowcast, routing, operational control, traveler incentive design
- Real security & reliability scenarios



Traffic data sources

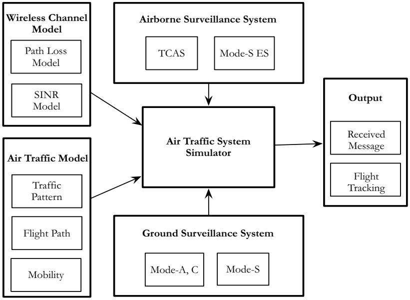


Diagnostics and intrusion detection for traffic information systems

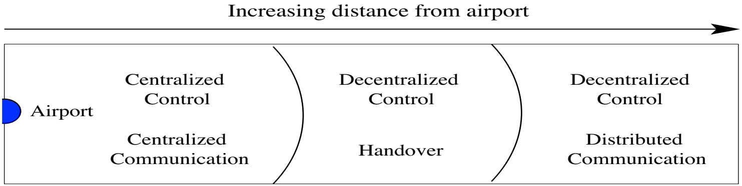
Air Traffic Operations

National Airspace System

- Data: Airport operations, aircraft trajectories, aviation weather
- Airport: Algorithms for ATC choice modeling, scheduling, congestion control, and resource re-allocation
- Airspace: Methods for surveillance (conformance monitoring, threat detection), sectorization, re-routing
- NextGen security & reliability

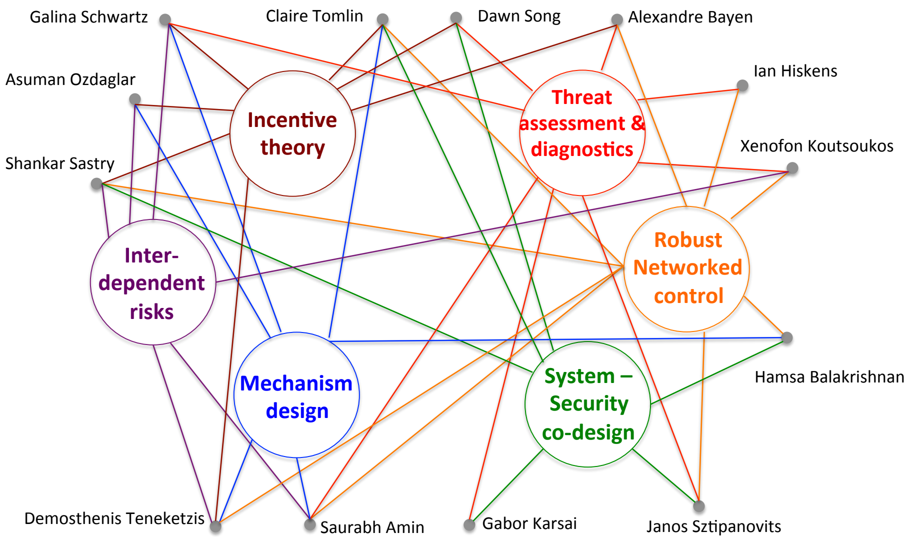


Air traffic system simulation



Varying degrees of EI+RC integration for air traffic control and comm. systems

Integration among individual researchers



Choice of Projects and Coordination

- *Monthly Coordination Telcons:*
    - RC + EI integration for power systems (GS and IM), visitor Catherine Rosenberg (Waterloo), air transportation Systems (HB) so far
    - Game Theory advances (SA) so far
    - CPS VO and inter-agency coordination (XK, JS, SS)
- *Exchange of Students and Research Staff*
    - Student of HB from MIT have spent time at Berkeley
    - GS has spent time at MIT with AO and SA
- *HiCONS and RCSS Conferences*
    - LR and Linda Bushnell (Washington) co-PC chairs for HiCONS, CPS Week, Philadelphia 2013, XK for 2014?
    - LR will host RCSS in August 2013 in San Francisco
- *Industry Coordination*
  JS and SS will work with industry partners (UTRC, Honeywell, GE) to develop FORCES industrial advisory board.