Foundations of Resilient Cyber-Physical Systems (FORCES)

Shankar Sastry, UC Berkeley

Larry Rohrbough, UC Berkeley

The FORCES Investigator Team

Alex Bayen, Shankar Sastry, Dawn Song, Claire Tomlin

Saurabh Amin, Hamsa Balakrishnan, Asuman Ozdaglar

Ian Hiskens, Demos Teneketzis

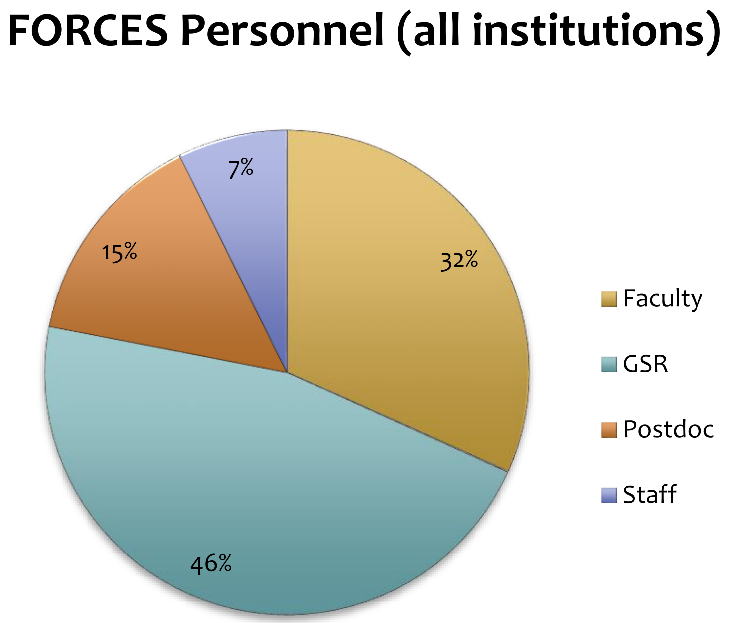
Gabor Karsai, Xenofon Koutsoukous, Janos Sztipanovits

FORCES is supported by the National Science Foundation Award Numbers CNS-1238959 (Vanderbilt), CNS-1238962 (Michigan), CNS-1239054 (MIT), and CNS-1239166 (Berkeley)

The FORCES Team Overall

- Total Participants = 41
  - Graduate Students = 19
  - Faculty = 13
  - Post Docs = 6
  - Staff = 3

- Demographics
  - Female = 22%
  - URM = 2%
  - U.S. Persons = 68%

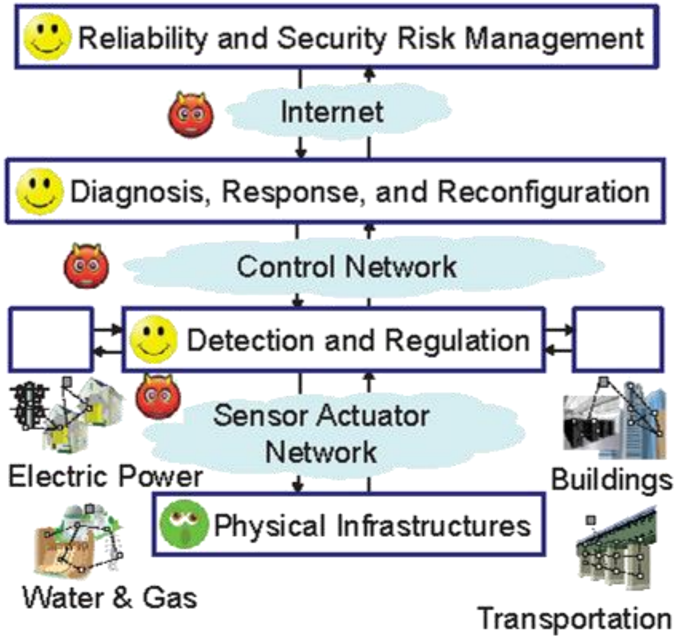


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

FORCES Overview and Approach

Economic Incentives

Game theory // Mechanism design // Interdependent risk management



Resilient CPS Design

Robust Control

Fault/attack diagnostics // Control of ActionWebs // Model-based design

Research Focus Areas

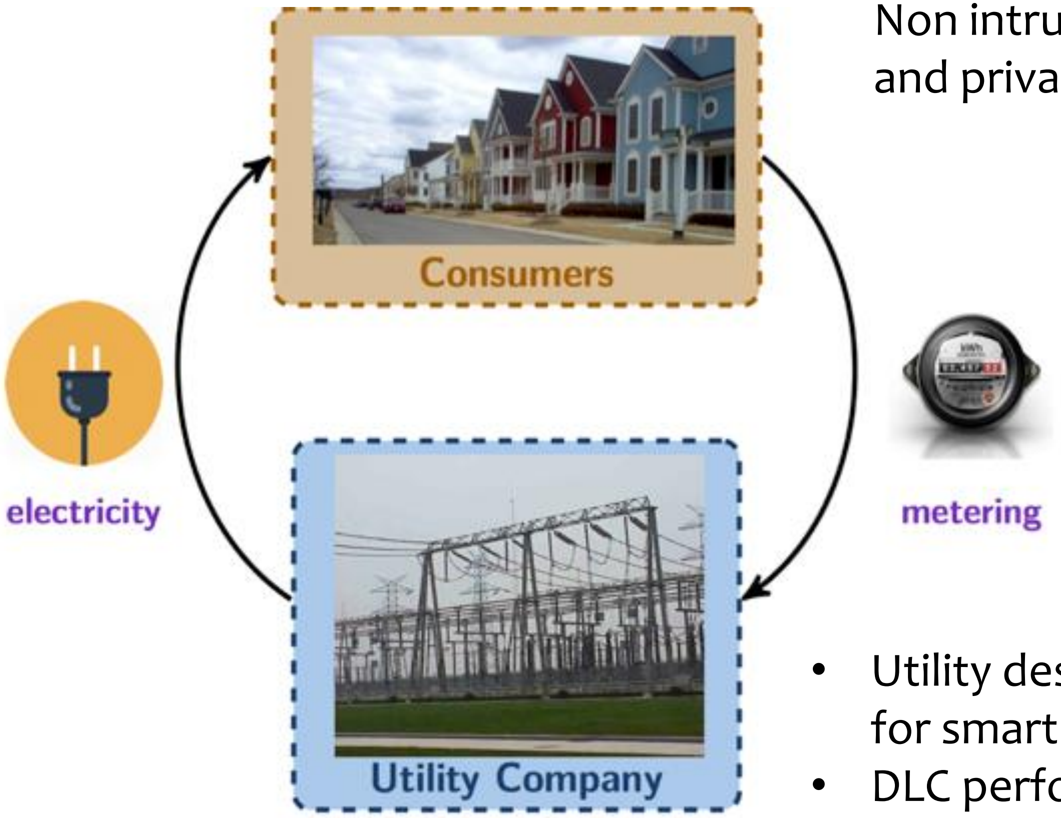
- **Economic Incentives**
  - Game theory
    - Deal with strategic adversaries
    - Model both security failures and reliability failures
  - Mechanism design and theory of incentives
    - Agents contribute to CPS efficiency and safety, while optimizing their individual objectives
    - Joint stochastic control and incentive-theoretic design
- **High Confidence Control**
  - Control for resilience against network-level attacks and faults
  - Including software:
    - Current CPS often run legacy code
    - Protocols often lack security, authentication, or privacy
    - Attacker can extract or control information and computation

Matrix of Research Projects

CPS for Transportation & Electric Power	Tools Based on High Confidence Control	Tools Based on 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 distribution	Distributed load control	Demand response schemes
Energy efficient building operations	Predictive control of devices	Energy saving incentives

Economic Incentives Highlights (1/4)

Non intrusive load monitoring and privacy compatible design

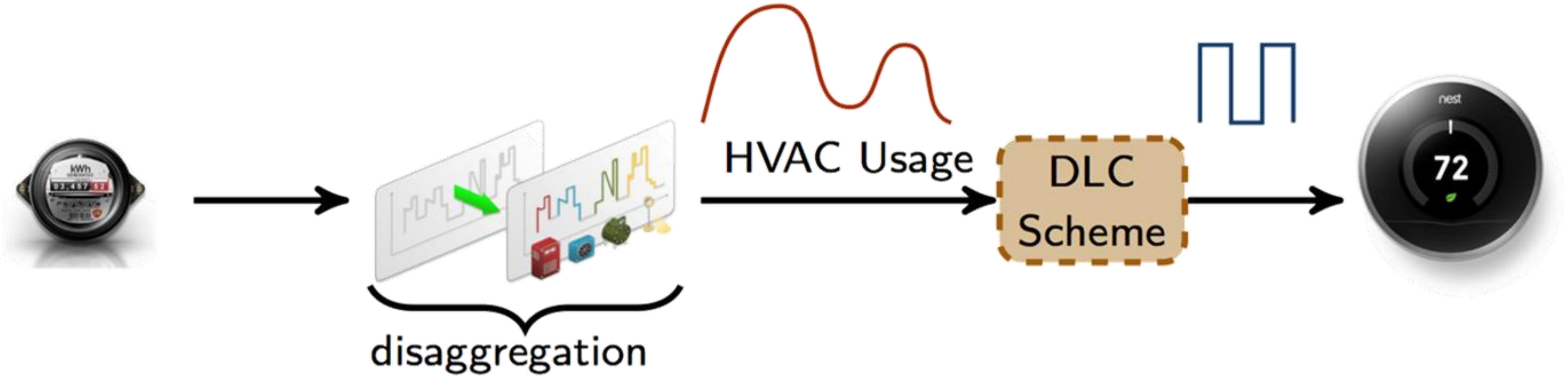


- Utility desires high fidelity data for smart grid operations
- DLC performance degrades as privacy preserving metering is increased

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Economic Incentives Highlights (1/4)

Privacy Contracts for Demand-Side Energy Management (Shankar Sastry)



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

Economic Incentives Highlights (2/4)

Variability and Uncertainty in Power Systems
(Ian Hiskens)

Variability and uncertainty increase power system operating costs, compromise reliability

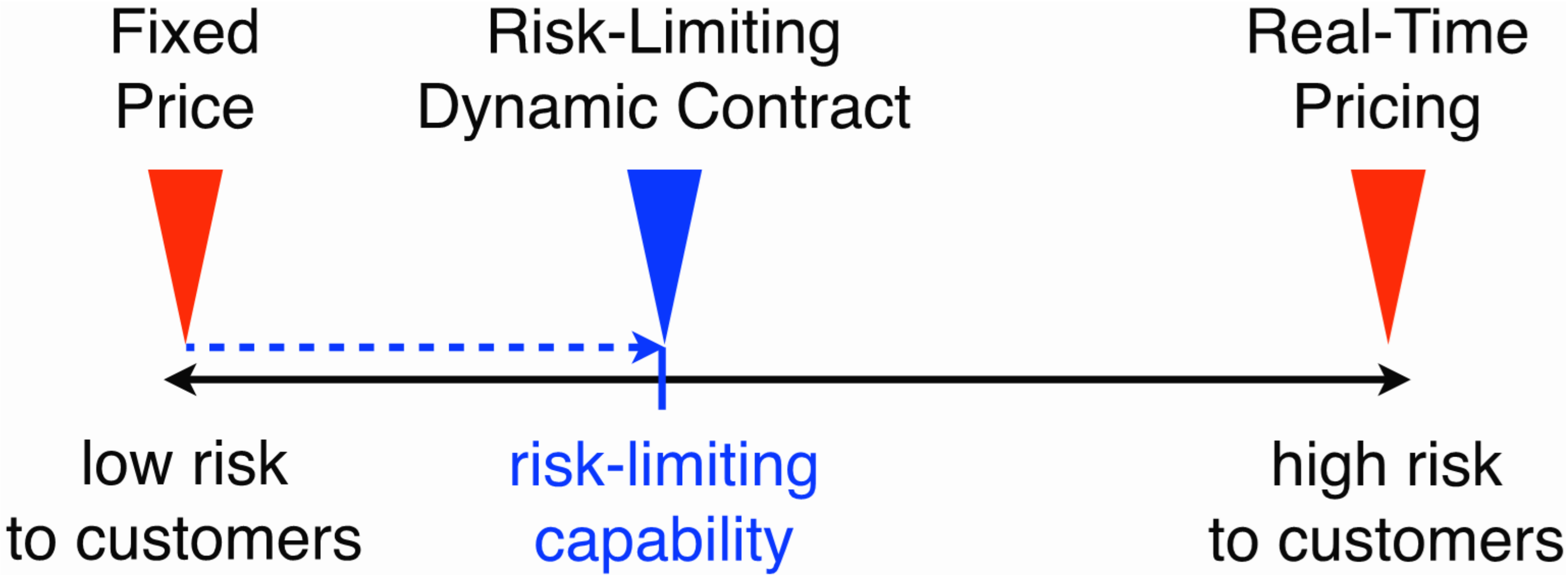
Solutions:

- Technologies
  - Supply-side: fast-start and fast-ramp generators
  - Storage
  - Demand-side flexibility
- New market structures

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Economic Incentives Highlights (3/4)

Dynamic Contracts for Limiting Risk in Direct and Indirect Load Control (Claire Tomlin)



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

Economic Incentives Highlights (3/4)

Economic Incentives for Intermittent Power Generation (Claire Tomlin)

- A demand-side solution to manage the uncertainty of customers' solar and wind generation and loads:

  direct load control for risk management

- Dynamic contracts between a utility and its customers:

  risk-limiting capability

- Theoretic contribution: a solution method for mean-variance constrained-risk sensitive control via dynamic programming

- Demonstration using data (ERCOT, Austin node):

  1. beneficial to both utility and customers
  2. works well under both flat and real-time pricing retail tariffs

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

[Yang, Callaway, Tomlin, 2014]

Economic Incentives Highlights (4/4)

Network Neutrality and Cyber-Physical Systems
(Galina Schwartz)

Retain the Benefits Of Neutrality + Permit QoS for Mission-critical tasks

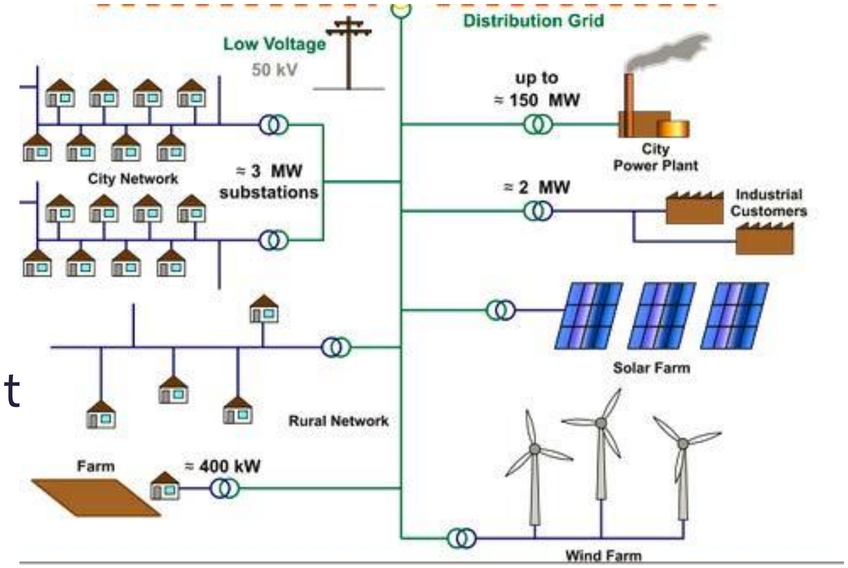
- The goals:
  - Enable service differentiation
    - Enable user discrimination
  - Preserve "Neutral Network"
    - Quasi-neutral network state
- Proposal: To implement x-Model, but only for
  - Specialized mission-critical services (CPS) only
  - (Possibly) only at times of critical emergencies

Resilient Control Highlights (1/4)

Resilient Monitoring and Control Algorithms for Distribution Networks (Saurabh Amin)

CPS Management of distributed generation (DGs) in distribution networks needs introduces new vulnerabilities

- Our focus
  - Worst case attack plans:
    - Denial-of-service (DoS) attacks
    - Manipulation of protection equipment
  - Secure network control
  - Design secure CPS architecture

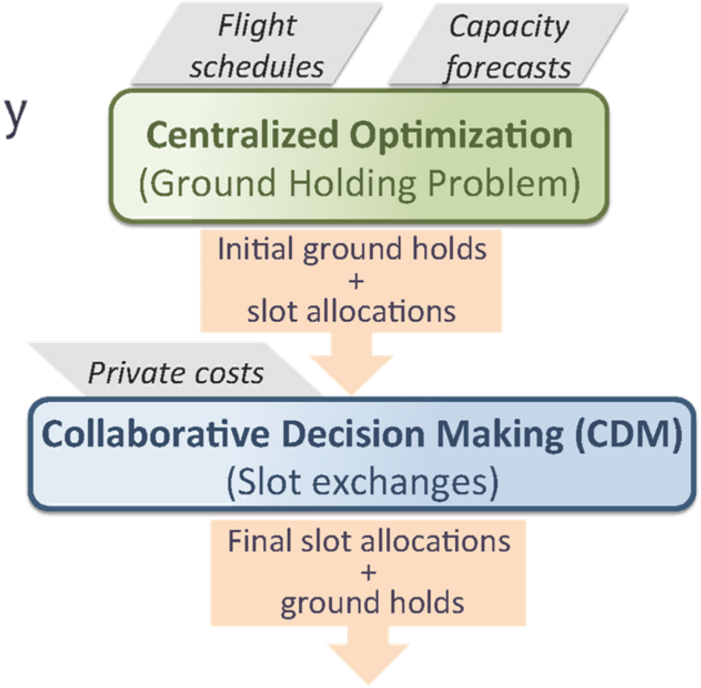


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Control Highlights (2/4)

Modeling and Mitigating Disruptions in Networked, Multi-Agent CPS (Hamsa Balakrishnan)

- Centralized optimization generally **assumes homogeneous delay costs**
- Airport capacity is uncertain, especially a few hours ahead of time
- Stochastic optimization formulations:
  - Static: Single-stage stochastic Integer Program (IP)
  - Dynamic: Multi-stage stochastic IP, differentiates between flights of different durations
  - *Hybrid:* Multi-stage stochastic IP, but does not differentiate between flights of different durations



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Control Highlights (3/4)

Robust Convergence of Distributed Routing with Heterogeneous Population Dynamics (Alex Bayen)

- 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.

Extensions:

- Varying masses.
- Adapt to other problems, such as network consensus.

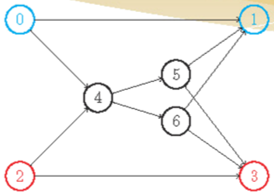


Figure : Example network

- 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: $\ell_i^k(x)$

Routing game with heterogeneous populations

Under unbiased noisy losses, with heterogeneous update rules with $\eta_t^k = \theta_k t^{-\alpha_k}$

$$\mathbb{E}\left[f(x^{(t)})\right] - f^\star = O\left(t^{-\min(\min_k \alpha_k, 1-\max_k \alpha_k)}\right)$$

where f is the Rosenthal potential function

Resilient Control Highlights (4/4)

Supervisory Control Approach to Dynamic Cyber-Security (Demos Teneketzis)

A supervisory control approach for cyber-security from the point of view of the defender with

- progressive attacks,
- defender's imperfect knowledge of the state of the system,
- 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.

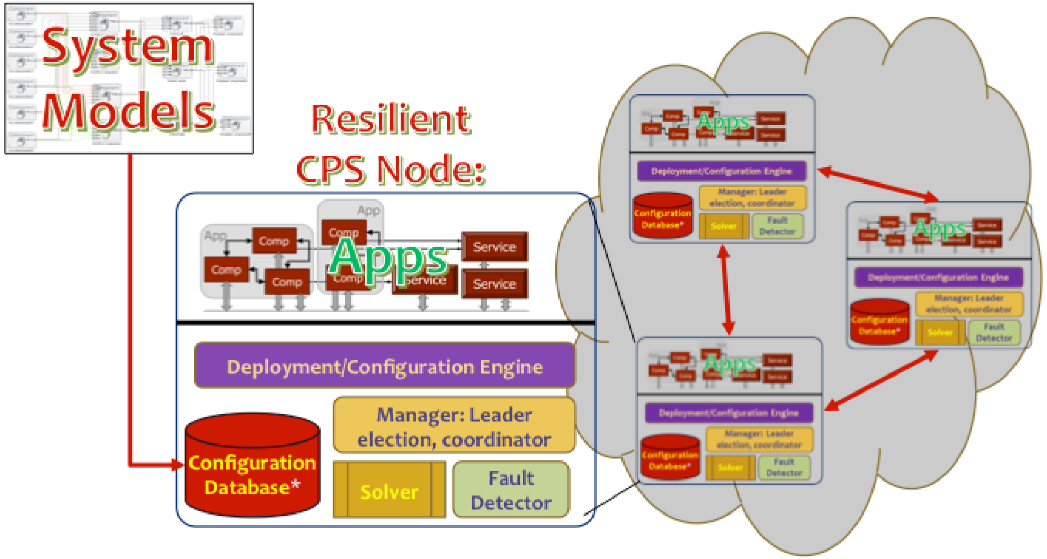
Strengthen resiliency of systems against attacks, intentional and unintentional misuses, and inadvertent failures.

Resilient CPS Design Highlights (1/4)

Resilience Modeling and Model-Based Design for CPS (Gabor Karsai)

Toward implementing resilience

- Models are translated into deployment plans and configuration spaces that are loaded into a configuration database
- The database is *fault tolerant* (via active replication)
- Each node includes:
  - Deployment and configuration engine (software manager)
  - Fault detector (detects local anomalies and remote node loss)
  - Solver (to re-compute configuration solution)
  - Manager (to do leader / controller election and coordination)
- Any node/process/component/link can fail (become compromised) → the system recovers



Resilient CPS Design Highlights (2/4)

Resilience Monitoring of CPS in the Presence of Faults and Adversarial Attacks (Xenofon Koutsoukos)

- Large area to be monitored
- Only a limited number of sensors can be placed
  - cost of deployment and maintenance

WHERE TO PLACE SENSORS?

- An adversary may try to disable some of the sensors
  - cyber attack, physical destruction, wireless jamming, battery exhaustion, etc.
  - sensor placement has to be resilient to such attacks
- Attack model: the adversary removes a limited number of the variables that have been selected

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

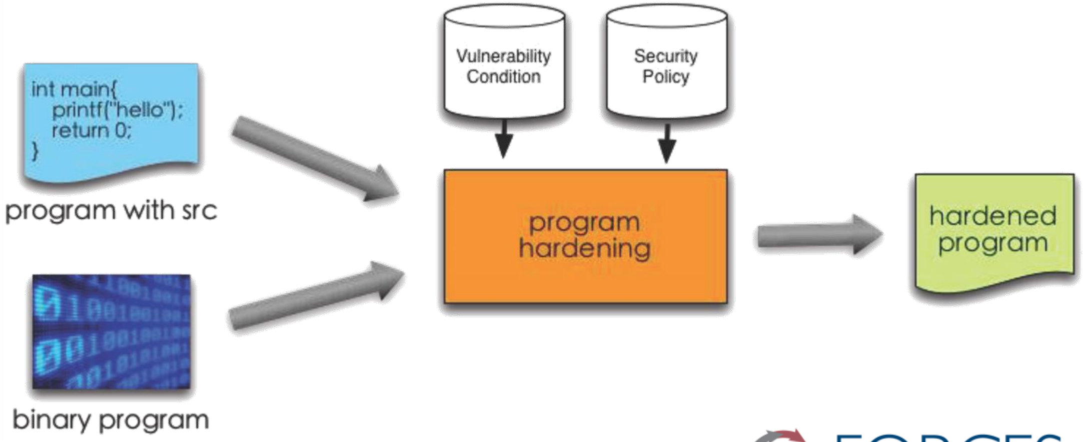
Resilient CPS Design Highlights (3/4)

Program Hardening of CPS Systems
(Dawn Song)

Software inevitably have vulnerabilities.

- human mistakes
- limited resources in CPS

How to protect them from being exploited?



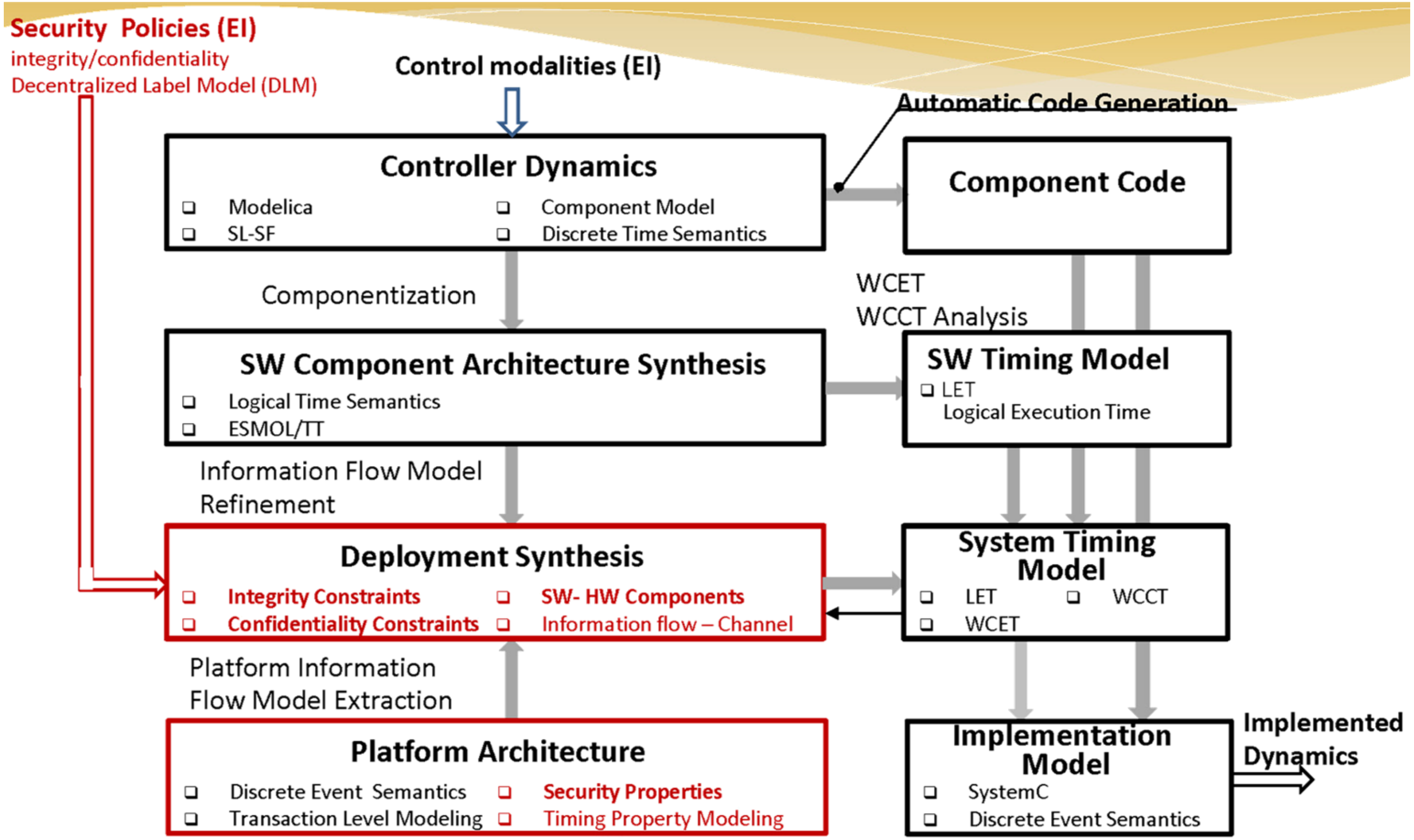
```
int main{
   printf("hello");
   return 0;
}
```

- Fix vulnerabilities
- Deploy security checks

Resilient CPS Design Highlights (4/4)

CPS System-Security Co-Design
(Janos Sztipanovits)

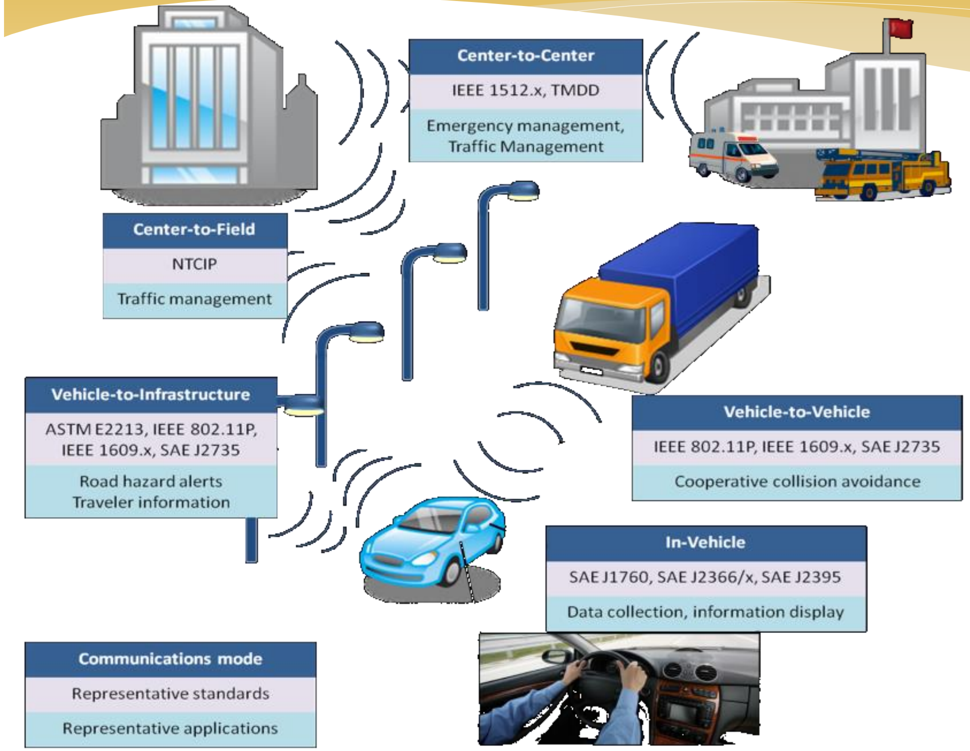
Integrity Attacks // Confidentiality Attacks // Information Flows



FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Road Transportation CPS:

Connected Corridors



Center-to-Center

IEEE 1512.x, TMDD

Emergency management, Traffic Management

Center-to-Field

NTCIP

Traffic management

Vehicle-to-Infrastructure

ASTM E2213, IEEE 802.11P, IEEE 1609.x, SAE J2735

Road hazard alerts
Traveler information

Vehicle-to-Vehicle

IEEE 802.11P, IEEE 1609.x, SAE J2735

Cooperative collision avoidance

In-Vehicle

SAE J1760, SAE J2366/x, SAE J2395

Data collection, information display

Communications mode

Representative standards

Representative applications

Connected Corridors: “next generation” of Integrated Corridor Management is being developed and piloted on a freeway and arterial network in Southern California using freeway ramps and arterial traffic signals.

Cyber Attack
s

C 2 Wind Tunnel for Integrated Testbed

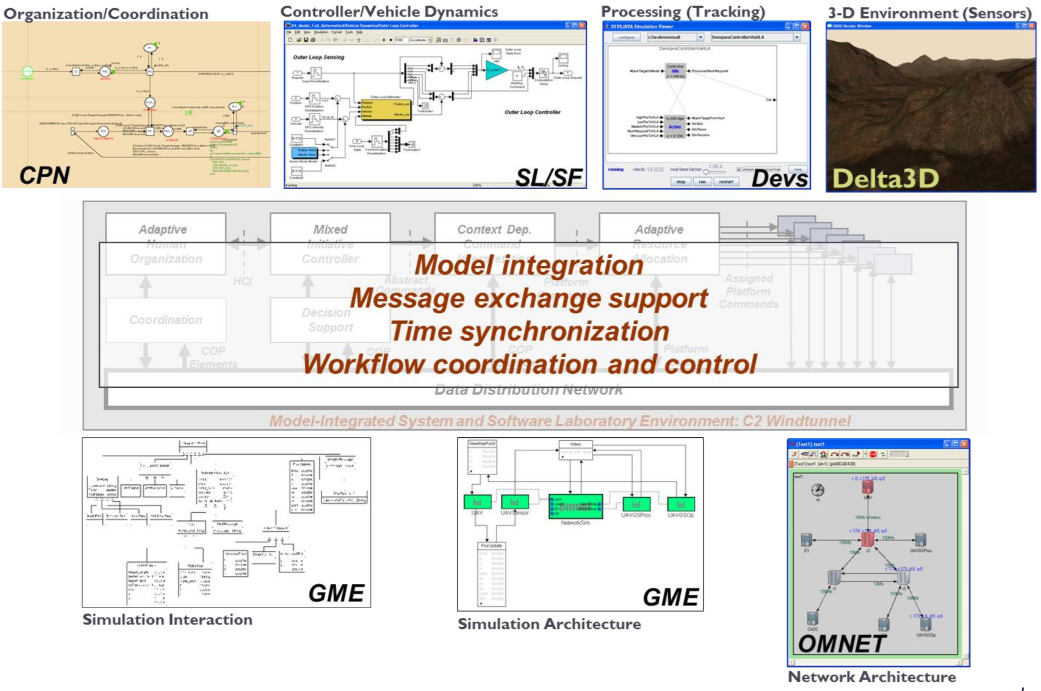
- **Vanderbilt's** Command and Control (C2) Wind Tunnel is a virtual laboratory for experimentation using simulations of both *physical* and *cyber* elements that are tightly coupled and interact
- Used to evaluate C2 systems for the military, to experiment with cyber defenses in industrial control (SCADA) systems

Simulators:

- Matlab/Simulink
- CPN Tools
- DEVS
- Omnet++
- …

Services:

- Message exchange
- Time synchronization
- Message translations


Organization/Coordination
CPN
Controller/Vehicle Dynamics
SL/SF
Processing (Tracking)
Devs
3-D Environment (Sensors)
Delta3D
Adaptive Human Organization
Mixed Initiative Controller
Context Dep. Command
Adaptive Resource Allocation
HCI
Abstract Commands
Platform
Assigned Platform Commands
Coordination
Decision Support
COP Elements
COP
Platform
Model integration
Message exchange support
Time synchronization
Workflow coordination and control
Data Distribution Network
Model-Integrated System and Software Laboratory Environment: C2 Windtunnel
GME
Simulation Interaction
GME
Simulation Architecture
OMNET
Network Architecture

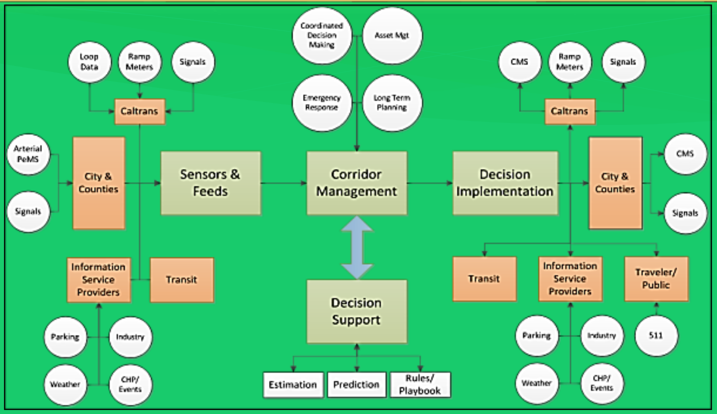
Integrated Testbed for FORCES Traffic

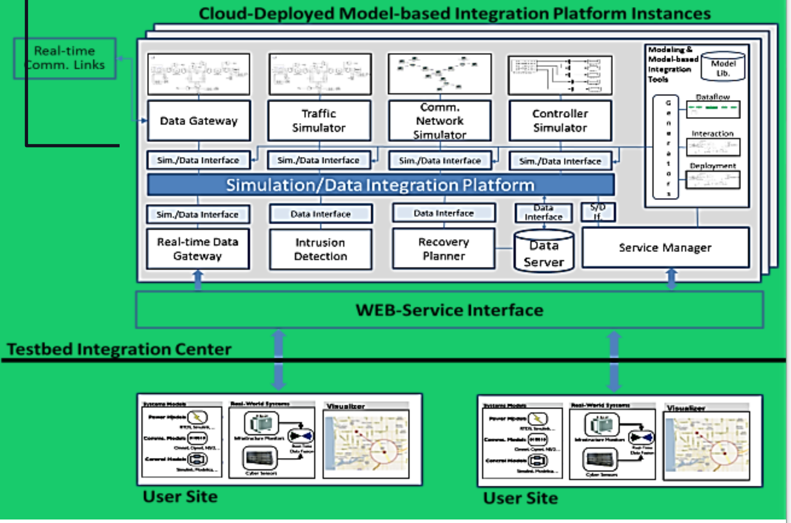
Our Solution:

Connected Corridors (CC)

+

High-fidelity simulation software (C2WT)





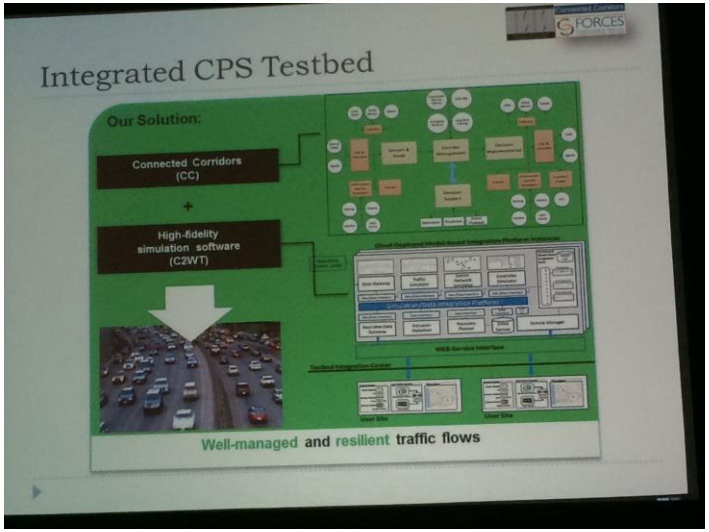
Well-managed and resilient traffic flows

CPS Testbed in the SmartAmerica Challenge

- SmartAmerica Challenge
  - Berkeley/Vanderbilt project on resilient transportation networks, impacts of cyber attacks
  - Integrated demonstration June 11 in Washington, DC

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Smart America Challenge



Integrated CPS Testbed

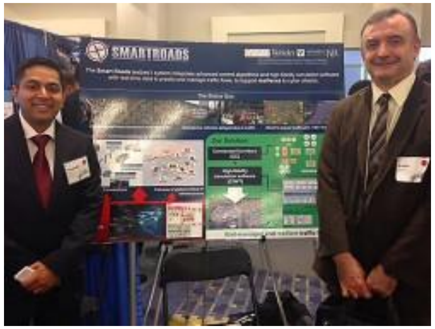
Our Solution:

Connected Corridors (CC)

+

High-fidelity simulation software (C2WT)

Well-managed and resilient traffic flows

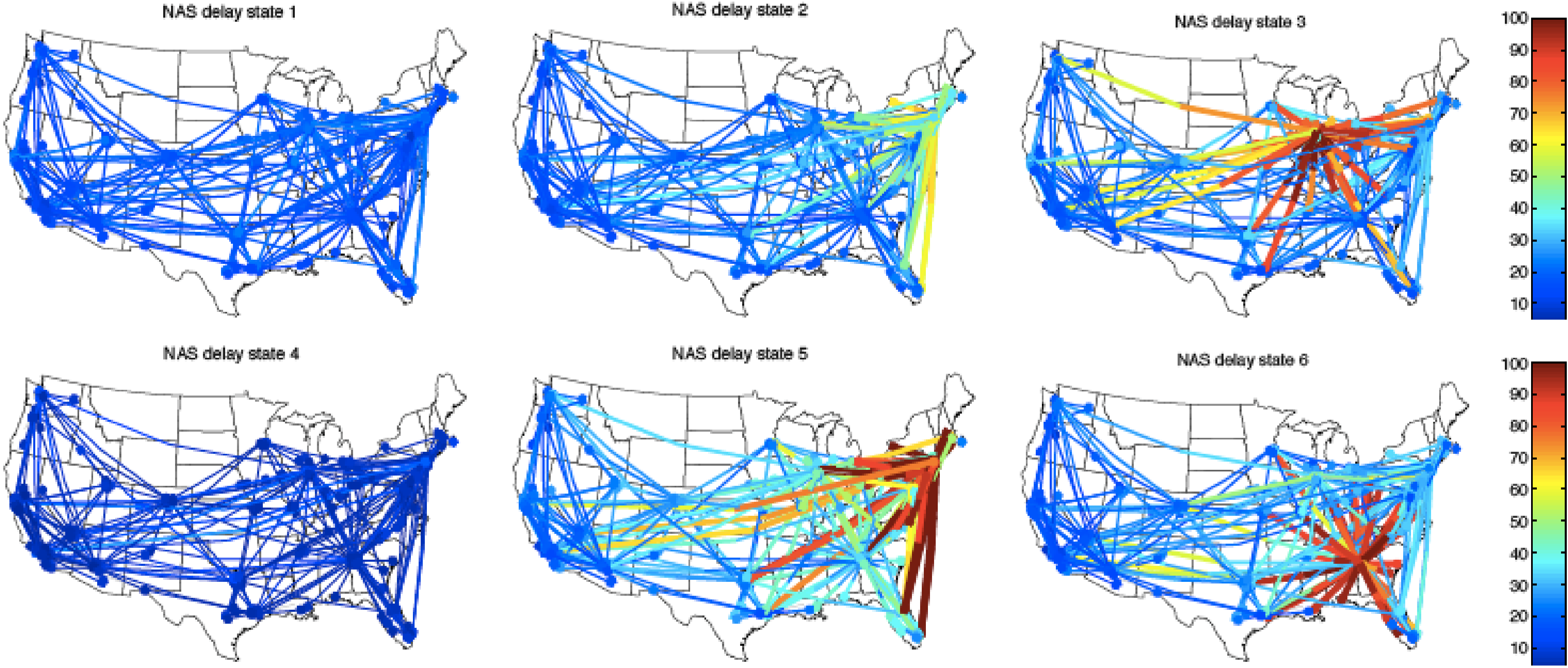


[Karsai, Neema, Bayen 2014]

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Air Transportation Delay: Building in Resilience

- 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 Knowledge Transfer

- Some highlights:
  - CPSWeek 2014: Invited Keynotes by Sastry "Towards a Theory of Resilient Cyber Physical Systems" and Hiskens "A Cyber-Enabled Grid of the Future"
  - Ratliff and Ohlsson workshop: "Big Data Meets CPS" at 2014 IEEE Conference on Decision and Control
  - Amin and Balakrishnan workshop: "Resilient Control of CPS" at 2014 IEEE Conference on Decision and Control
  - Amin and Schwartz summer school: "Cyber-Physical Security" at 2015 Institute for Pure & Applied Mathematics (IPAM)
  - Bayen Fall Program: "Network Infrastructure of Traffic Systems" at 2014 IPAM
  - Practitioner workshops at Caltrans, ITS California to educate community about traffic vulnerabilities

International Partnerships

Resilient Societal-Scale Cyber-Physical Systems
(Larry Rohrbough, Claire Tomlin, Kameshwar Poolla, Anthony Joseph)

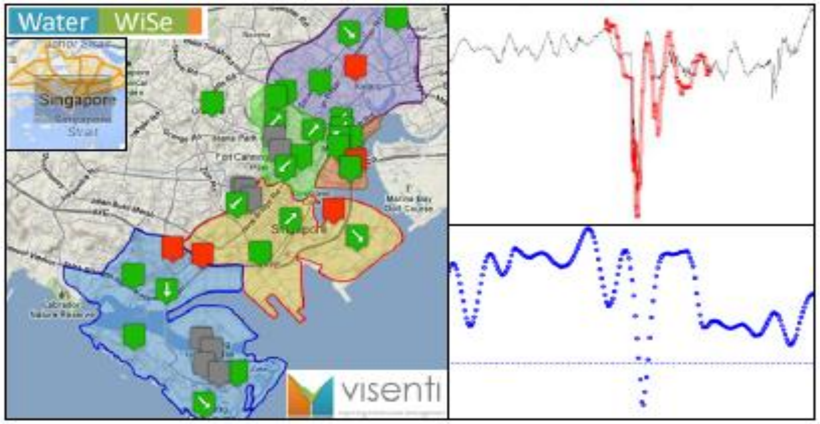
- Republic of the Philippines: Philippine California Advanced Research Institutes (PCARI)
  - Resilient Societal-Scale Cyber-Physical Systems
    - Multi-year research program focused on improving the resilience (faults, failures, attacks) of key Philippine infrastructures--energy, transportation, smart buildings
    - New courses development
    - US-PH graduate student exchanges
  - Partners UC Berkeley (EE, CS, ME) and University of the Philippines (CS, CE), other Philippine physical infrastructure stake holders

COMMISSION ON HIGHER EDUCATION
1994
OFFICE OF THE PRESIDENT OF THE PHILIPPINES
UNIVERSITY OF THE PHILIPPINES
1908

International Partnerships (cont.)

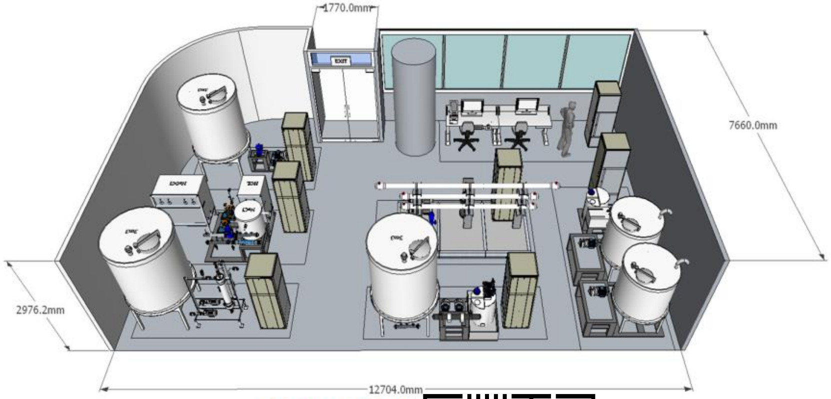
Resilient Water Networks
(Saurabh Amin, Lina Sela)

- **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

SWaT: Secure Water Treatment Test Bed



FLOTECH PROCESS CONTROL & INSTRUMENTATION

SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

FORCES Education: new or revised courses

- **Resilient Infrastructure Networks (MIT/Amin)**
  - (Graduate) Control algorithms and game-theoretic tools to enable resilient operation of large-scale infrastructure networks. Dynamical network flow models, stability analysis, robust predictive control, fault and attack diagnostic tools. Strategic network design, routing games, congestion pricing, demand response, and incentive regulation. Design of operations management strategies for different reliability and security scenarios. Applications to transportation, logistics, electric-power, and water distribution networks.
- **Security of CPS (Vanderbilt/Koutsoukos)**
  - (Graduate) Security requirement for CPS, Vulnerability analysis; Intrusion detection; Security protocols; Assurance.
- **Computer security (Berkeley/Song)**
  - (Undergraduate) General security course with new material in security issues in cyber-physical systems.

FORCES Education: new or revised courses

- **Air Transportation Operations Research (MIT/Balakrishnan)**
  - (Graduate) Covers analytical and algorithmic techniques for air transportation systems; includes discussions of key challenges pertaining to resilience and security of air traffic infrastructure; control, optimization and game-theoretic algorithms for air transportation systems.
- **Stochastic control (Michigan/Teneketzis)**
  - Projects in Stochastic hybrid systems, game theory, decentralized control, mechanism design.
- **Special topics in Mechanism design (Michigan/Teneketzis)**
- **Infrastructure for vehicle electrification (Michigan/Hiskens)**
  - Fundamentals of the physical and cyber infrastructures that will underpin large-scale integration of plug-in electric vehicles. Control strategies are considered for economically and equitably coordinating the charging of large numbers of electric vehicle, whilst ensuring that grid loading limits are respected.
- **Power system dynamics and control (Michigan/Hiskens)**
  - Hybrid dynamical systems perspective in introducing students to the dynamic behavior of power systems; resilient control strategies that enable recovery from large disturbances are considered

FORCES Broadening Participation

MESA Mathematics Engineering Science Achievement

High School Program & Research

- Program to develop the skills and STEM readiness of students in transition to High School
- Based on prior work w/ TRUST-BFOIT: Boutique Program 16 students in 3 years, 4 currently in college in STEM Majors.
- Multiple Research Based Components
  - Focus on Mathematics skill development in Algebra and Calculus
  - Inclusion of parents and school support programs
  - Exposure to career options and multiple STEM Careers
  - Additional focus on leadership and grit
  - The education of counselors and development of tools to help them in their work.

black girls CODE imagine. build. create.

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

FIRST GRADUATE

Berkeley Girls in Engineering

- Summer 2014 we ran the "pilot":
  - 60 middle school girls from east bay
  - 2 2-week sessions at UC Berkeley
  - 3 "modules" a day:
    - Bioengineering, robotics, materials, coding, big data…
    - What is Engineering?
    - Leadership, talks, posters, elevator pitches…
  - Week long project (in groups)
  - Field trips: Lawrence Hall of Science, Pixar
  - All of the instructors (faculty, graduate students, staff, Pixar engineers) were women

Taking Stock of FORCES

- Common themes have emerged:
  - Integration of economic incentives and high confidence control
  - Utility-based privacy: the increasingly important role of privacy in CPS systems
  - Big data meets CPS: decision making in real time
- Application Domains where Impact is being made
  - Air Transportation
  - Road Transportation
  - Energy Infrastructures: Demand Side, Distribution, …
  - Water

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Moving Forward…

- Industry collaboration: UTRC, Honeywell, C3 Energy, SDGE
- Government: FAA, NASA, Federal and State DOTs, EPRI
- Smart America Challenge:
  - FORCES integration of Mobile Millennium and ISIS
- Smart Cities (water)
- Education efforts:
  - Young researcher talks
  - Course modules, UROPs, conference workshops
- Team efforts:
  - Active collaborations between students and faculty of four campuses: First sets of joint papers out
- Outreach: GIRLS IN ENGINEERING! (middle school girls)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS