Towards a Theory of Resilient CPS Systems

Shankar Sastry

Dean and Roy W. Carlson Professor of Engineering
University of California, Berkeley

Joint work with Saurabh Amin and Galina A. Schwartz

Outline

Action Webs

Action Webs & Networked Control Systems (NCS)

NCS vulnerabilities

Resilient Control for CPS

1. Threat assessment
2. Attack diagnosis
3. Resilient control

Economic Incentives

Conclusions and future research

Outline

Action Webs

Action Webs & Networked Control Systems (NCS)

NCS vulnerabilities

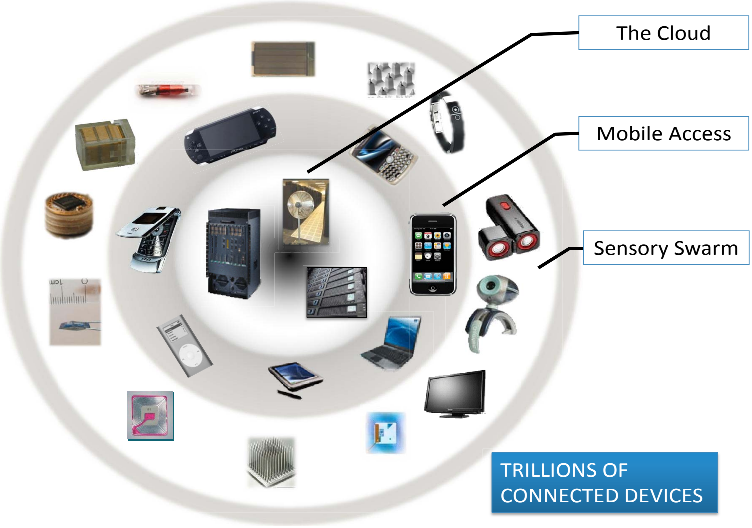
Resilient Control for CPS

1. Threat assessment
2. Attack diagnosis
3. Resilient control

Economic Incentives

Conclusions and future research

The swarm at the edge of the cloud

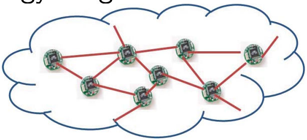


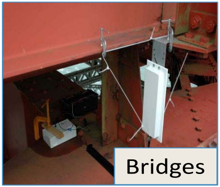
Source: J. Rabaey [ASPDAC'08]

Ubiquitous instrumentation

Wireless Sensor Networks (WSN) for infrastructure monitoring

- Environmental systems
- Structural health
- Construction projects
- Energy usage





Bridges

Snowpack

Soil liquefaction

Smart buildings

Traffic

Vineyards

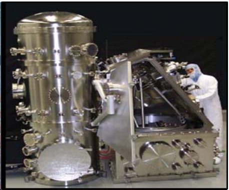
Courtesy: UCB-CEE Systems Faculty

Wireless Sensor webs everywhere

Change detection: Thresholds, phase transitions, anomalies

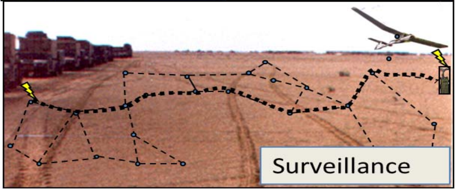
- Security systems
- Health care
- Wildfire detection
- Fault diagnosis
- Tracking & surveillance

Intel Research



Health Care

Fire Response



Surveillance

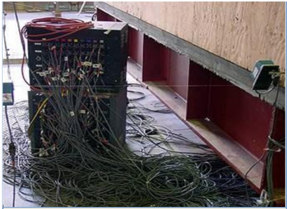
Action Webs in CPS Infrastructures

Supervisory Control & Data Acquisition (SCADA)

- Robust estimation
  - Noisy measurements
  - Lossy communication
- Real-time control
  - Safety
  - Performance

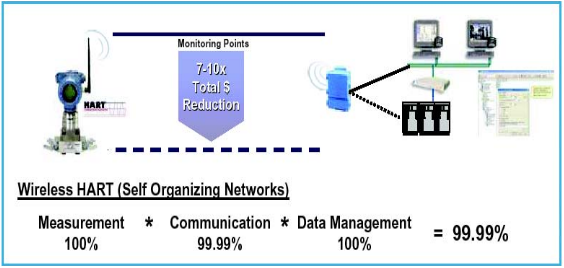
COTS IT for SCADA

- Cost ↓, Reliability ↑
- Digital and IP based: New vulnerabilities!
- Reliability $\not\Rightarrow$ Security



Wired networks are costly to maintain

Typical industrial infrastructure ~ $10B



Wireless HART (Self Organizing Networks)

Measurement 100% * Communication 99.99% * Data Management 100% = 99.99%

Source: Emerson case study

Societal CPS

A complex collection of sensors, controllers, compute nodes, and actuators that work together to improve our daily lives

- From very small: Ubiquitous, Pervasive, Disappearing, Perceptive, Ambient
- To very large: Always Connectable, Reliable, Scalable, Adaptive, Flexible

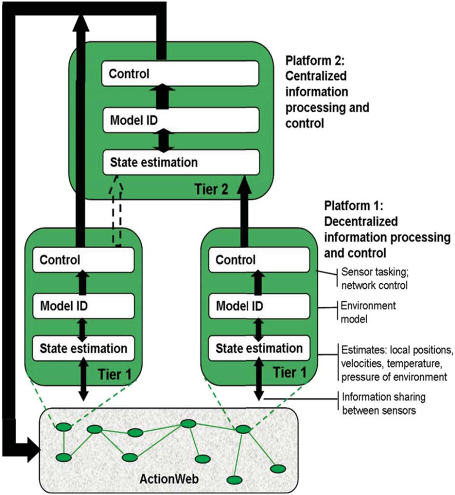
Emerging Service Models

- Building energy management
- Automotive safety and control
- Management of metropolitan traffic flows
- Distributed health monitoring
- Smart Grid

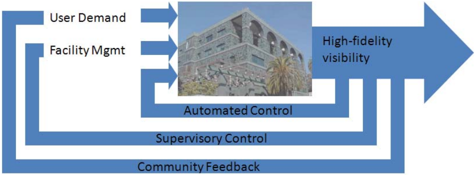
Action Webs

Observe and infer for planning and modifying action

- Dealing with uncertainty
- Tasking sensors
- Programming the ensemble
- Multiple objectives
- Embedding humans


Control
Model ID
State estimation
Tier 2
Platform 2: Centralized information processing and control
Control
Model ID
State estimation
Tier 1
Control
Model ID
State estimation
Tier 1
Platform 1: Decentralized information processing and control
Sensor tasking; network control
Environment model
Estimates: local positions, velocities, temperature, pressure of environment
Information sharing between sensors
ActionWeb

Example: Building energy management

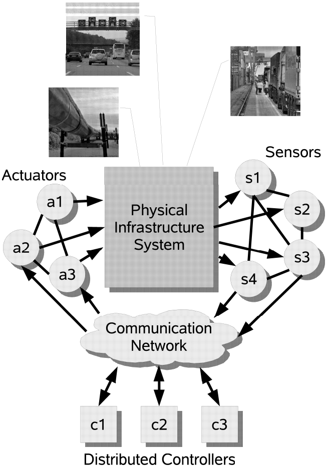


Courtesy: Claire Tomlin

From Action Webs to Resilient CPS

Resilient/High Confidence Networked Control

- Fault-tolerant networked control
  - Limits on stability, safety, & optimality
  - Scalable model predictive control
- Security & Resilient Control
  - Availability, Integrity, & Confidentiality
  - Graceful degradation
- Economic Incentives
  - Incentive Design for investing in security
  - Interdependent Risk Assessment & Cyber Insurance



CPS Attacks

Maroochy Shire sewage plant *(2000)*

Los Angeles traffic control *(2008)*

Tehama Colusa canal system *(2007)*

Cal-ISO power system computers *(2007)*

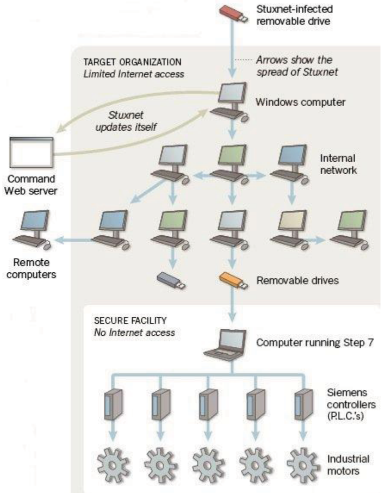
NCS/CPS security concerns

Attackers

- Malicious insiders
- Computer hackers
  - Cyber criminals
  - Cyber warriors
  - Hacktivists
  - Rogue hackers
  - Corporate spies

Stuxnet worm

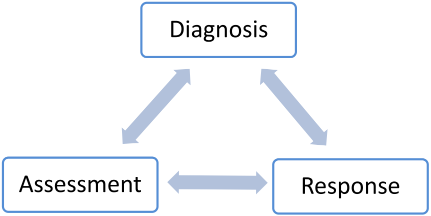
- Targets SCADA systems
- Four zero-day exploits, antivirus evasion techniques, p-2-p updates, network infection routines
- Reprograms *Programmable Logic Controller (PLC)* code



Source: Symantec, NYT

Resilient Control for CPS

1. Threat assessment
   - How to model attacker and his strategy?
   - Consequences to the physical infrastructure
2. Attack diagnosis
   - How to detect manipulations of sensor-control data?
   - Stealthy [undetected] attacks
3. Resilient control
   - Design of resilient control algorithms
   - Tradeoffs between performance and containment



Outline

Action Webs

Action Webs & Networked Control Systems (NCS)

NCS vulnerabilities

Resilient Control for CPS

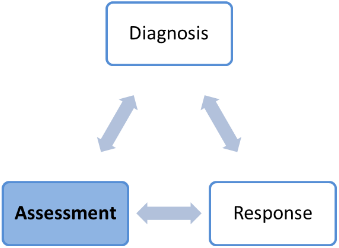
1. Threat assessment
2. Attack diagnosis
3. Resilient control

Economic Incentives

Conclusions and future research

Threat assessment

- How to model attacker and his strategy?
- Consequences to the physical infrastructure



Field operational test on the Gignac canal network
[Amin, Litrico, Sastry, Bayen. HSCC'10]

Models of deception and denial-of-service (DoS) attacks
[Amin, Cárdenas, Sastry. HSCC'09]

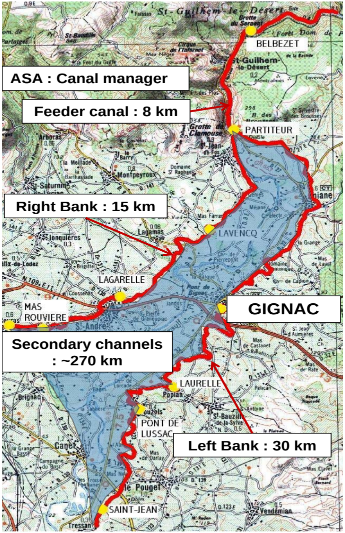
Assessment for Tennessee Eastman process control system (TE-PCS)
[Cárdenas, Amin, Lin, Huang, Sastry. ASIACCS'11]

Gignac water canal network

SCADA components

- Level & velocity sensors
- PLCs & gate actuators
- Wireless communication
- Multiple stakeholders

Communication station



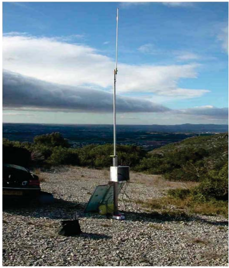
Map of Gignac canal

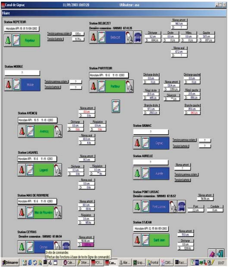
Presented by permission from Cemagref, France

Gignac canal network

Physical infrastructure

Cyber infrastructure





Canal de Gignac 11/09/2003 10:07:20 Utilisateur : asa

Filaire

Station REPETEUR
Horodate API : 10 :01 11/09/2003
Repeteur
Tension panneau solaire 0.10 v
Tension batterie 10.70 v

Station BELBEZET
Dernière connexion : 11/09/03 07:41:35
Belbezet
Niveau amont 146.1 cm D ?
Décharge 9.2 cm D 604 L/s
Droite 0.0 cm D 0 L/s
Milieu 0.0 cm D 0 L/s
Gauche 38.5 cm D 897 L/s
Niveau aval 67.2 cm D ?

Station MOBILE
?
Mobile
Tension panneau solaire ?
Tension batterie ?

Station PARTITEUR
Horodate API : 10 :6 11 /9 /2003
Partiteur
Décharge droite 0.0 cm D 0 L/s
Niveau amont 130.4 cm D 2259 L/s
Décharge gauche 0.0 cm D 0 L/s
Régul droite 28.9 cm D 495 L/s
Déversoir D ** L/s
Régul gauche 21.5 cm D 856 L/s
Branche droite 97.3 cm D 2583 L/s
Branche gauche 85.6 cm D 840 L/s

Station AYENCQ
Horodate API : 10 :5 11 /9 /2003
Avencq
Niveau amont 0.0 cm D 0 L/s
Décharge 0.0 cm D 0 L/s
Régulation 0.9 cm D 0 L/s
Niveau aval 60.0 cm D 4 L/s

Station GIGNAC
?
Gignac
Tension panneau solaire ?
Tension batterie ?

Station LAGAREL
Horodate API : 10 :6 11 /9 /2003
Lagarel
Niveau amont 90.2 cm
Décharge 0.3 cm D 0 L/s
Régulation 0.3 cm D ** L/s
Niveau aval 0.0 cm D 0 L/s

Station AURELLE
?
Aurelle
Niveau amont ?
Tension panneau solaire
Tension batterie

Station MAS DE ROUVIERE
Horodate API : 10 :6 11 /9 /2003
Mas de Rouvière
Niveau amont 80.1 cm D 88 L/s
Régulation 3.8 cm D 165 L/s

Station PONT LUSSAC
Dernière connexion : 11/09/03 07:15:57
Pont Lussac
Niveau amont 54.54 cm
Pont 2.2 cm
Conduite 0 cm

Station CEYRAS
Dernière connexion : 11/09/03 07:00:54
Ceyras
Niveau amont 56.06 cm D [illegible] L/s

Station STJEAN
Horodate API : 12 :15 06/05/2003
Saint Jean
Niveau amont 55.0 cm
Décharge 0.0 cm D 1200 L/s

Invite de commandes
Effectue des fonctions à base de texte (ligne de commande).

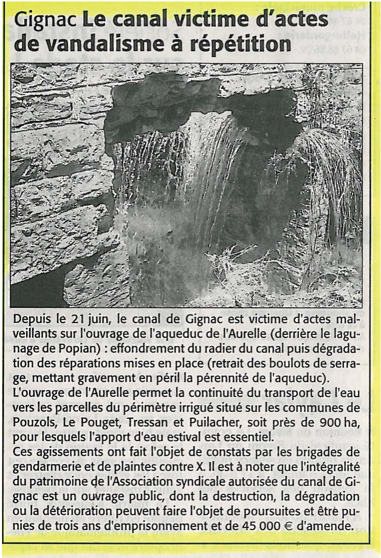
Reported attacks on water SCADA systems

Gignac canal system attacks

- Stealing water by compromising sensors
- Tampering PLCs
- Theft of solar panels

Other SCADA vulnerabilities

- Time between telemetry requests can be used for malicious traffic injection
- Encryption provides confidentiality but does not provide data integrity



Gignac **Le canal victime d'actes de vandalisme à répétition**

Depuis le 21 juin, le canal de Gignac est victime d'actes malveillants sur l'ouvrage de l'aqueduc de l'Aurelle (derrière le lagunage de Popian) : effondrement du radier du canal puis dégradation des réparations mises en place (retrait des boulots de serrage, mettant gravement en péril la pérennité de l'aqueduc).
L'ouvrage de l'Aurelle permet la continuité du transport de l'eau vers les parcelles du périmètre irrigué situé sur les communes de Pouzols, Le Pouget, Tressan et Puilacher, soit près de 900 ha, pour lesquels l'apport d'eau estival est essentiel.
Ces agissements ont fait l'objet de constats par les brigades de gendarmerie et de plaintes contre X. Il est à noter que l'intégralité du patrimoine de l'Association syndicale autorisée du canal de Gignac est un ouvrage public, dont la destruction, la dégradation ou la détérioration peuvent faire l'objet de poursuites et être punies de trois ans d'emprisonnement et de 45 000 € d'amende.

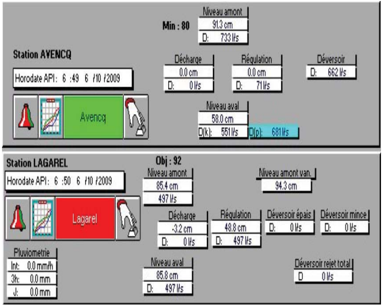
Courtesy: C. Hugodot, Manager

Regulatory control of canal pools

Control objective

- Manipulate gate opening
- Control upstream water level
- Reject disturbances (offtake withdrawals)

SCADA interface



Min : 80

Niveau amont
91.3 cm
D: 733 l/s

Station AVENCQ

Horodate API : 6 :49 6 /10 /2009

Décharge
0.0 cm
D: 0 l/s

Régulation
0.0 cm
D: 71 l/s

Déversoir
D: 662 l/s

Niveau aval
58.0 cm
D(k): 551 l/s
D(p): 681 l/s

Station LAGAREL

Horodate API : 6 :50 6 /10 /2009

Obj : 92

Niveau amont
85.4 cm
497 l/s

Niveau amont van.
94.3 cm

Décharge
-3.2 cm
D: 0 l/s

Régulation
48.8 cm
D: 497 l/s

Déversoir épais
D: 0 l/s

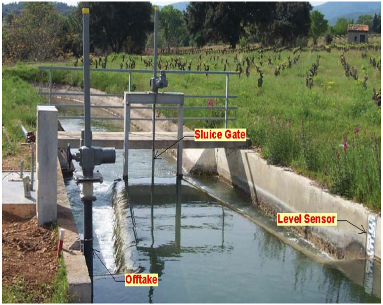
Déversoir mince
D: 0 l/s

Pluviometrie
Int: 0.0 mm/h
3h: 0.0 mm
J: 0.0 mm

Niveau aval
85.8 cm
D: 497 l/s

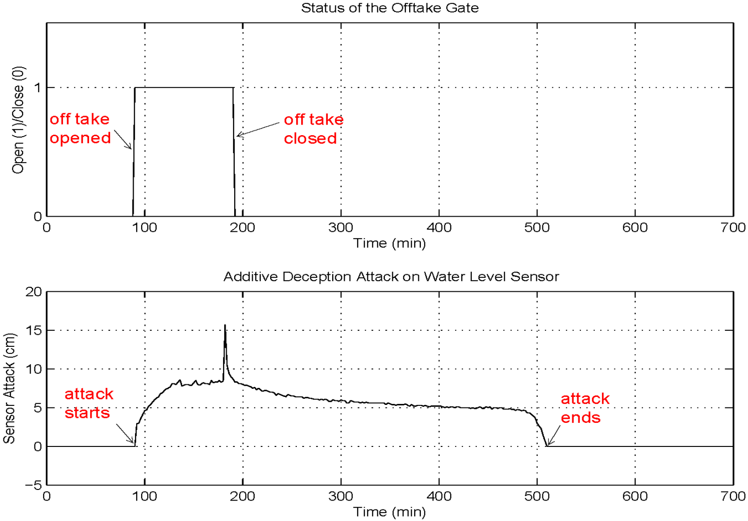
Déversoir rejet total
D 0 l/s

Avencq cross-regulator



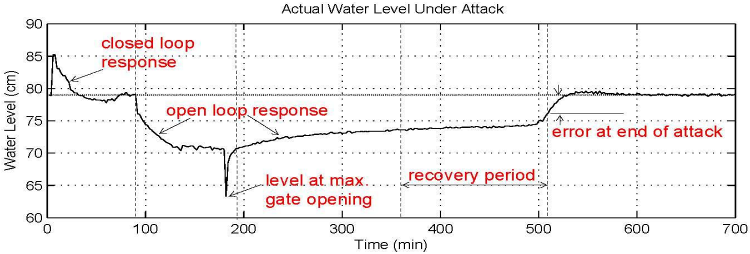
Cyber-attack on the Avencq canal pool

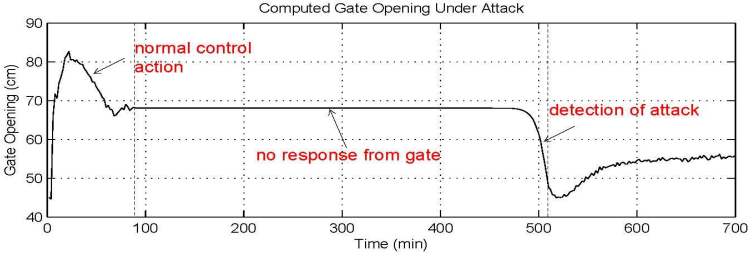
Field operational test (October 12th, 2009)



Cyber-attack on the Avencq canal pool

Successful attack





Taxonomy of Attacks on NCS

Cyber Attacks

SCADA Manager [IT Security] **A6**

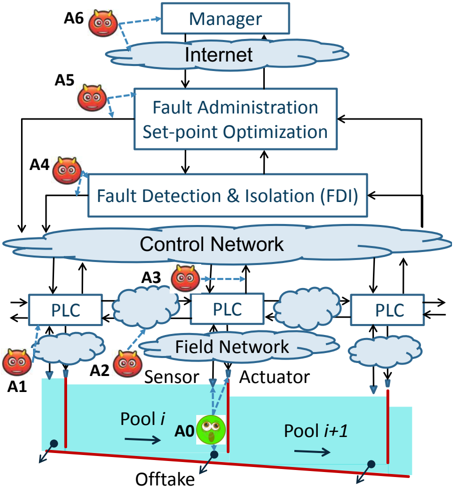
- Unauthorized access, Viruses

Supervisory Control **A3-A5**

- Deception: set-point change, parameter substitution
- Denial-of-Service (DoS): network flooding, process disruption

Regulatory Layer **A1-A2**

- Deception: compromise of measurements & controls, spoofing, replay
- DoS: jamming, ↑ comm. latency

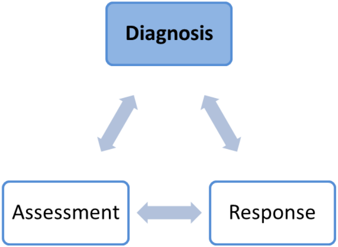


Physical Faults [Control th.] **A0**

- Sensor-actuator faults
- Unauthorized leaks

Attack diagnosis

- How to detect manipulations of sensor-control data?
- Stealthy [undetected] attacks



Observer-based diagnosis for Gignac SCADA system
[Amin, Litrico, Sastry, Bayen. IEEE TCST'11]

Non-parametric CUSUM statistic based diagnosis for TE-PCS
[Cárdenas, Amin, Sastry, et.al. ASIACCS'11]

Study of stealthy attacks on power system state estimators
[Teixeira, Amin, Sandberg, Johansson, Sastry. IEEE CDC'10]

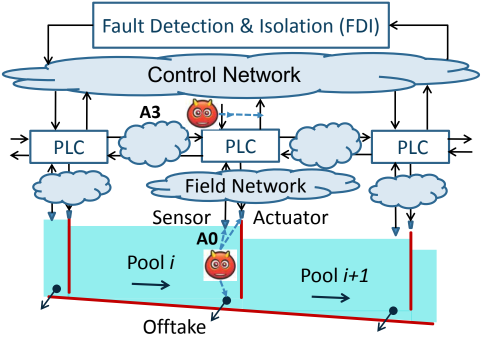
Attacks on supervisory control layer

Supervisory Layer Attacks **A3**

- Deception: set-point change, parameter substitution
- Denial-of-Service (DoS): network flooding, process disruption

Physical Faults/Attacks **A0**

- Sensor-actuator faults
- Unauthorized withdrawals



Design of a model-based diagnosis scheme

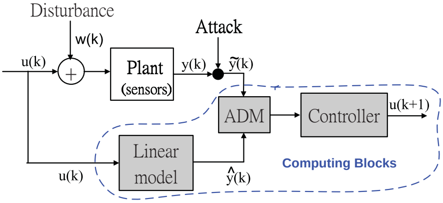
Recommendations on Security Diagnosis

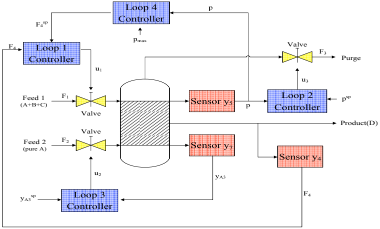
Recommendations to the European Commission on Canal Automation & the Cemagref Research Institute

- Enhanced model (redundancy) improves detection
- Sensors located closer to the offtakes are critical
- Localized sensor attacks do not lead to global degradation
- Multiple pool sensor attacks can evade detection [stealth]

Attack diagnosis for [other] SCADA systems

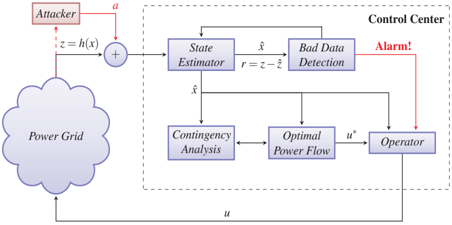
Process control

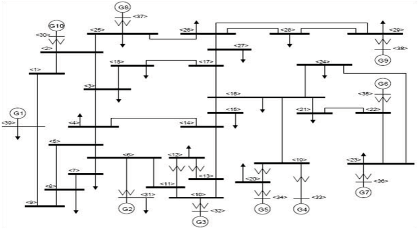




[Cárdenas, Amin, Lin, Huang, Sastry. ASIACCS'11]

Power transmission

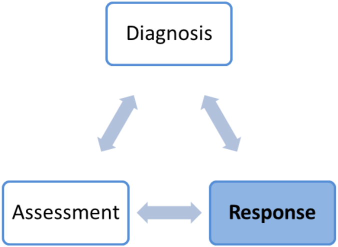




[Teixeira, Amin, Sandberg, Johansson, Sastry. IEEE CDC'10]

Resilient control

- Design of resilient control algorithms?
- Fundamental limitations & interdependent security



Stability of hyperbolic PDEs under switching boundary control
[Amin, Hante, Bayen. IEEE TAC'10]

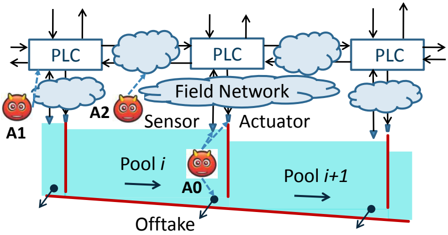
Incentives to secure under network induced interdependent risks
[Amin, Schwartz, Sastry. GameSec'10]

Safety-preserving control for stochastic systems under comm. losses
[Amin, Cárdenas, Sastry. HSCC'09]

Attacks on regulatory control layer

Regulatory layer **A1-A2**

- Deception: compromise of measurements & controls
- DoS: jamming, ↑ latency



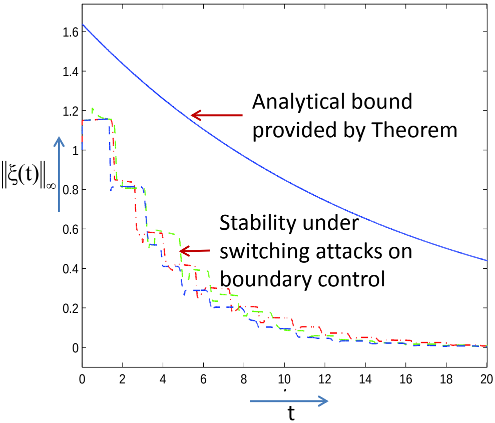
Physical faults or attacks **A0**

- Sensor-actuator faults
- Unauthorized withdrawals

Switching attacks can lead to instability!

Switching attack: characterization of system stability

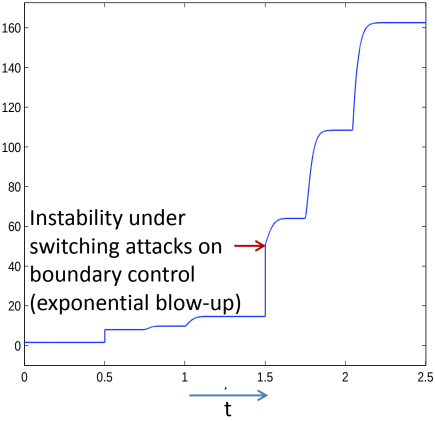
All assumptions of stability thm. hold



Analytical bound provided by Theorem

Stability under switching attacks on boundary control

An assumption of stability thm. violated



Instability under switching attacks on boundary control (exponential blow-up)

Outline

Action Webs

Action Webs & Networked Control Systems (NCS)

NCS vulnerabilities

Resilient Control for CPS

1. Threat assessment
2. Attack diagnosis
3. Resilient control

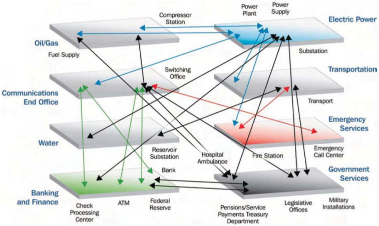
Economic Incentives

Conclusions and future research

Interdependent security (IDS) & incentives to secure

Security interdependencies due to

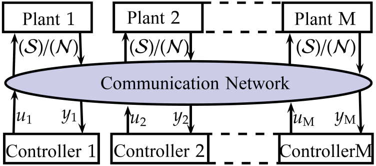
- Network induced risks
  - ⇒ Example: Distributed DOS attacks
- Wide use of COTS IT components
  - ⇒ Expect increased interdependencies



Infrastructure interdependencies

Interdependent security

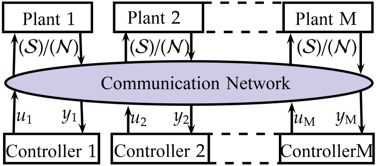
- Goal: Security analysis & implementation of control measures
- Methods: Game theory & Control theory
- Observation: Individual & social incentives differ



Network induced interdependencies

Game Theoretic formulation of Interdependent NCS

Two-stage game of plant-controller systems (players)



Each player

1. Invests in security $[V^i = S$ & incurs $\ell^i > 0]$ or not $[V^i = N]$
2. Chooses inputs u_t^i for NCS:

$$x_{t+1}^i = Ax_t^i + \nu_t^i B u_t^i + w_t^i$$
$$y_t^i = \gamma_t^i C x_t^i + v_t^i$$

where γ_t^i & ν_t^i are Bernoulli packet loss processes

Interdependent failure probabilities

- Failure probabilities:

$$\mathrm{P}[\gamma_t^i = 0 \mid V] = \tilde{\gamma}^i(V), \quad \mathrm{P}[\gamma_t^i = 1 \mid V] = 1 - \tilde{\gamma}^i(V),$$

  - $V := \{V^1, \ldots, V^{\mathrm{m}}\}$ Set of player security choices
- Security choices and failure probabilities:

$$\tilde{\gamma}^i(V) = \underbrace{\mathbf{1}_S^i \bar{\gamma}^i}_{\text{reliability}} + \underbrace{(1 - \mathbf{1}_S^i \bar{\gamma}^i)\beta(\eta^i)}_{\text{security}},$$

  - $\mathbf{1}_S^i$: Indicator function 1 if $V^i = S$
  - η^i: # of insecure players
  - $\beta(\eta^i)$: Interdependence term

$$0 < \beta(\{S, \ldots, S, \underbrace{N \ldots, N}_{\eta \text{ players}}\}) < \beta(\{S, \ldots, S, \underbrace{N \ldots, N}_{\eta+1 \text{ players}}\}) < 1,$$

Multiplayer games with interdependent security

- $V := \left\{V^1, \dots, V^{\mathrm{m}}\right\}$ Set of player security choices
- $U := \{u_t^1, \dots, u_t^{\mathrm{m}} | t \in \mathbb{N}_0\}$ Set of player control input sequences
- Each player minimizes his total cost:

$$J^i(V,U) = J^i_{\mathrm{I}}(V) + J^i_{\mathrm{II}}(V,U),$$

1. Security cost

$$J^i_{\mathrm{I}}(V) := (1 - \mathbf{1}^i_S)\ell^i$$

2. LQG control cost:

$$J^i_{\mathrm{II}}(V,U) := \limsup_{T \longrightarrow \infty} \frac{1}{T} \mathsf{E}\left[\sum_{t=0}^{T-1} {x^i_t}^\top G x^i_t + \nu^i_t {u^i_t}^\top H u^i_t\right]$$

- Social planner minimizes the aggregate cost:

$$J^{\mathsf{SO}}(V,U) = \sum_{i=1}^{\mathrm{m}} J^i(V,U).$$

Increasing and decreasing incentives to secure

2−player game

	S	N
S	$J^*_{\mathbb{I}}(\{S,S\}) + \ell^1$, $J^*_{\mathbb{I}}(\{S,S\}) + \ell^2$	$J^*_{\mathbb{I}}(\{S,N\}) + \ell^1$, $J^*_{\mathbb{I}}(\{N,S\})$
N	$J^*_{\mathbb{I}}(\{N,S\})$, $J^*_{\mathbb{I}}(\{S,N\}) + \ell^2$	$J^*_{\mathbb{I}}(\{N,N\})$, $J^*_{\mathbb{I}}(\{N,N\})$

Increasing incentives

If a player secures, other player gain from securing *increases*:

$$J^*_{\mathbb{I}}(\{N,N\}) - J^*_{\mathbb{I}}(\{S,N\}) \leqslant J^*_{\mathbb{I}}(\{N,S\}) - J^*_{\mathbb{I}}(\{S,S\})$$

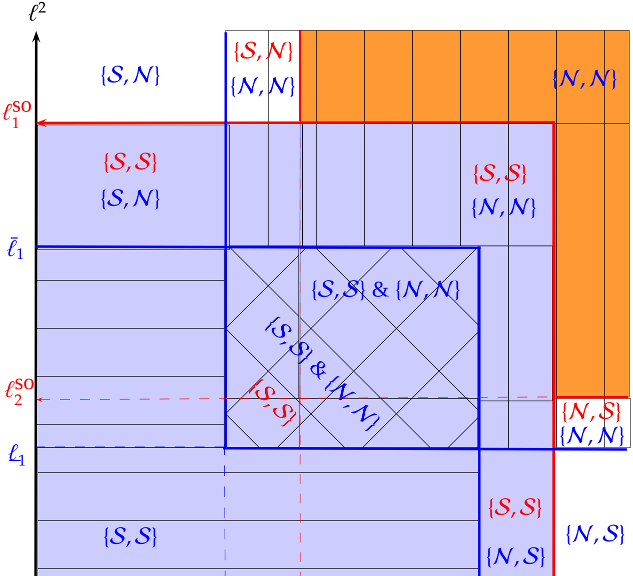
Decreasing incentives

If a player secures, other player gain from securing *decreases*:

$$J^*_{\mathbb{I}}(\{N,N\}) - J^*_{\mathbb{I}}(\{S,N\}) > J^*_{\mathbb{I}}(\{N,S\}) - J^*_{\mathbb{I}}(\{S,S\})$$

Individual optima [Nash equilibria] and social optima

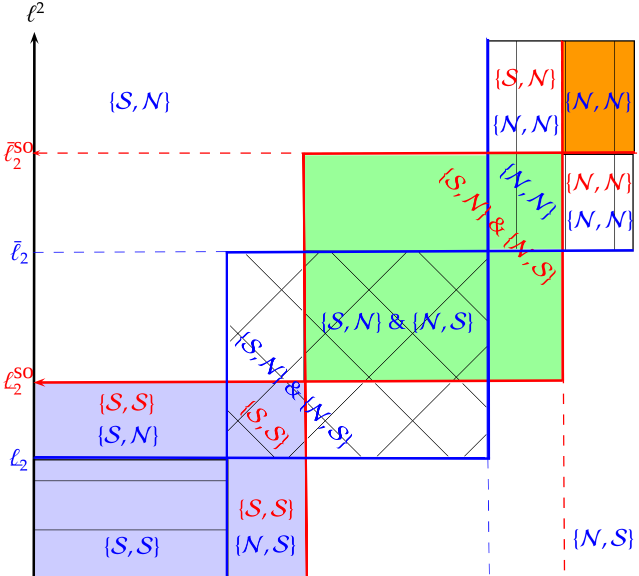
Theorem [Increasing incentive case]



ℓ^2
ℓ_1^{SO}
$\bar{\ell}_1$
ℓ_2^{SO}
$\underline{\ell}_1$
$\{\mathcal{S},\mathcal{N}\}$
$\{\mathcal{S},\mathcal{N}\}$
$\{\mathcal{N},\mathcal{N}\}$
$\{\mathcal{N},\mathcal{N}\}$
$\{\mathcal{S},\mathcal{S}\}$
$\{\mathcal{S},\mathcal{N}\}$
$\{\mathcal{S},\mathcal{S}\}$
$\{\mathcal{N},\mathcal{N}\}$
$\{\mathcal{S},\mathcal{S}\}$ & $\{\mathcal{N},\mathcal{N}\}$
$\{\mathcal{S},\mathcal{S}\}$ & $\{\mathcal{N},\mathcal{N}\}$
$\{\mathcal{S},\mathcal{S}\}$
$\{\mathcal{N},\mathcal{S}\}$
$\{\mathcal{N},\mathcal{N}\}$
$\{\mathcal{S},\mathcal{S}\}$
$\{\mathcal{S},\mathcal{S}\}$
$\{\mathcal{N},\mathcal{S}\}$
$\{\mathcal{N},\mathcal{S}\}$

Individual optima [Nash equilibria] and social optima

Theorem [Decreasing incentive case]



ℓ^2
$\bar{\ell}_2^{\mathrm{SO}}$
$\bar{\ell}_2$
ℓ_2^{SO}
ℓ_2
$\{\mathcal{S},\mathcal{N}\}$
$\{\mathcal{S},\mathcal{N}\}$
$\{\mathcal{N},\mathcal{N}\}$
$\{\mathcal{N},\mathcal{N}\}$
$\{\mathcal{S},\mathcal{N}\}$ & $\{\mathcal{N},\mathcal{S}\}$
$\{\mathcal{N},\mathcal{N}\}$
$\{\mathcal{N},\mathcal{N}\}$
$\{\mathcal{N},\mathcal{N}\}$
$\{\mathcal{S},\mathcal{N}\}$ & $\{\mathcal{N},\mathcal{S}\}$
$\{\mathcal{S},\mathcal{N}\}$ & $\{\mathcal{N},\mathcal{S}\}$
$\{\mathcal{S},\mathcal{S}\}$
$\{\mathcal{S},\mathcal{S}\}$
$\{\mathcal{S},\mathcal{N}\}$
$\{\mathcal{S},\mathcal{S}\}$
$\{\mathcal{N},\mathcal{S}\}$
$\{\mathcal{S},\mathcal{S}\}$
$\{\mathcal{N},\mathcal{S}\}$

Outline

Action Webs

Action Webs & Networked Control Systems (NCS)

NCS vulnerabilities

Resilient Control for CPS

1. Threat assessment
2. Attack diagnosis
3. Resilient control

Economic Incentives

Conclusions and future research

Economic Incentives for Resilient CPS systems

NCS security & reliability

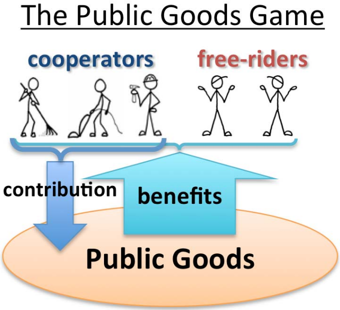
- Security failures (attacks S) and reliability failures (faults R) are difficult or costly to distinguish
- Goal: Model interdependent system failures F

$$\mathrm{Pr}(S \cap R \mid F) \neq \mathrm{Pr}(S \mid F)\mathrm{Pr}(R \mid F)$$

Courtesy: C. Goldschmidt (Symantec)

Negative externalities

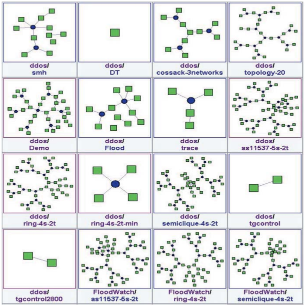
- Public goods game
- Information asymmetries
- Property right deficiencies & high enforcement costs
- Goal: Develop mechanisms to reduce NCS incentive suboptimality



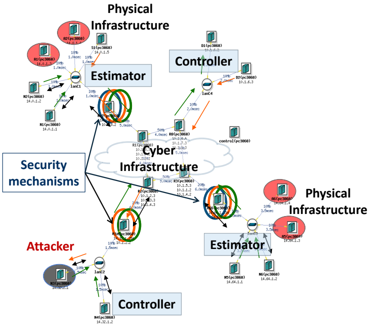
CPS RC + EI experimentation

Experiments for networked infrastructure

- Testing
- Validation



Network topologies



Cyber-Security Testbed with INL

cyber-DEfense Technology Experimental Research (DETER) Testbed

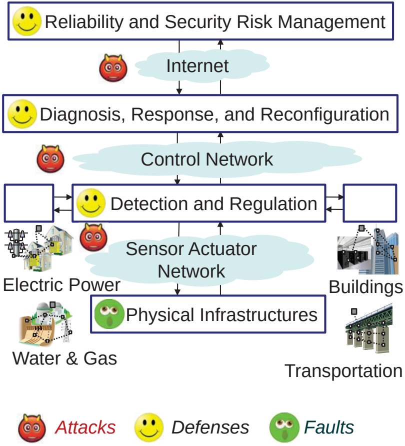
Towards a theory of Resilient CPS

Resilient Control

- Assessment, detection & response
- Networked and fault-tolerant control
- Scalable resilient Control algorithms
- Fundamental Limitations

Economic Incentives

- Incentive Theory for Resilient Systems
- Mechanism Design for reconciling Nash and societal optima
- Interdependent risk assessment
- Cyber Insurance



Reliability and Security Risk Management

Internet

Diagnosis, Response, and Reconfiguration

Control Network

Detection and Regulation

Electric Power

Sensor Actuator Network

Buildings

Physical Infrastructures

Water & Gas

Transportation

Attacks *Defenses* *Faults*

Thank you for your attention

Shankar Sastry
sastry@coe.berkeley.edu