Cyber-Physical Systems, Smart Grids and Why Should You Care

Ahmad F. Taha

Email: ahmad.taha@utsa.edu

Webpage: http://engineering.utsa.edu/~taha

November 6, 2015

Speaker Bio: Background & Interests

- Born and raised in Beirut, Lebanon
- Undergrad education: American University of Beirut '2011, B.E., ECE
- Interned @ Argonne National Lab, UofT, MIT
- Finished my Ph.D. in ECE from Purdue University in August 2015
- Assistant Professor, ECE Department @ UTSA
- Research interests: Uncertain CPSs

How Can We Make 'Em More Secure?

My Ultimate Objective

Understand how complex systems operate and utilize this knowledge to create tools & algorithms that can be leveraged to social challenges

Essentially, this should improve the quality of our lives...Hopefully!

Seminar Outline

1. CPSs: past, present, & future
2. CPS application: dynamic state estimation in smart power grids
3. Future of research in CPSs
4. Open research problems

Part I — Cyber-Physical Systems: History and Introduction

...And why should I care?

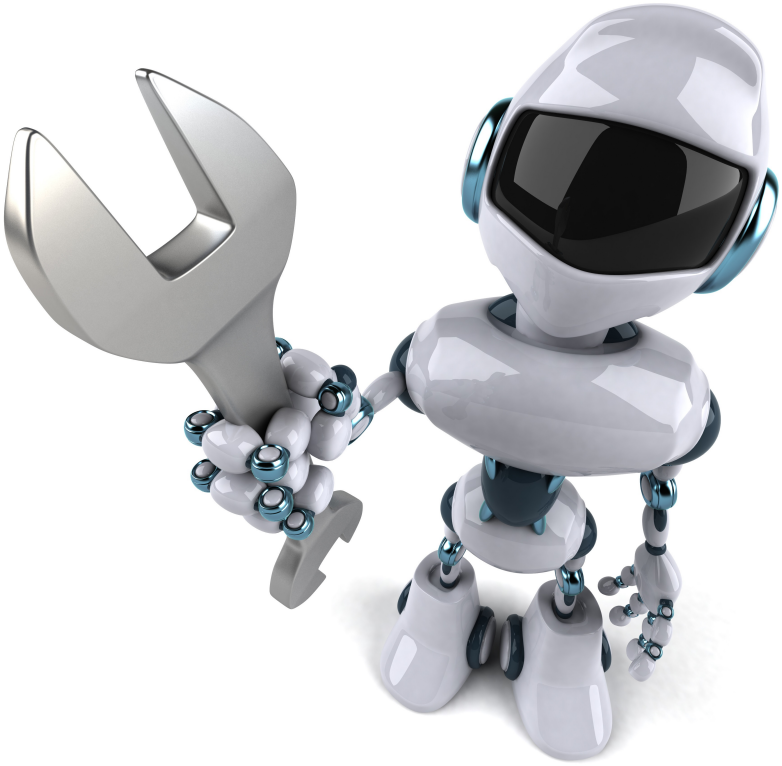
Cyber-Physical Systems — The *Ubiquity is Real!*

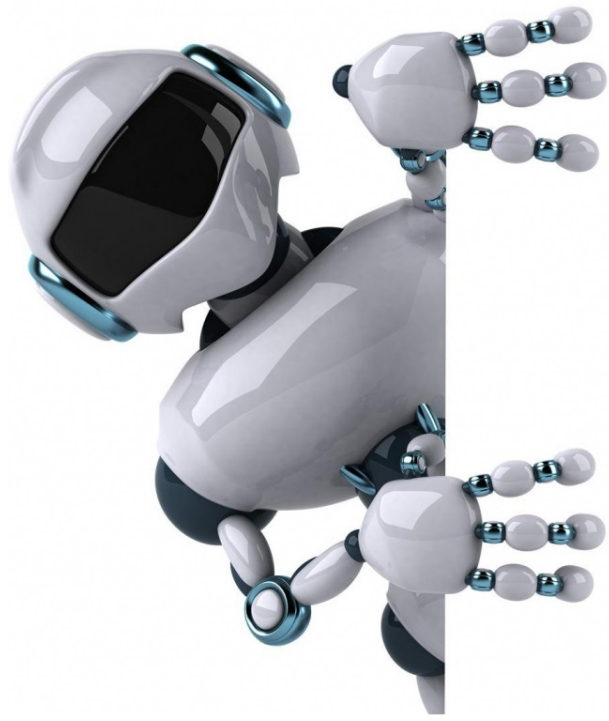
- CPSs: integrating computing, data analysis, communication, & control with physical processes
- Infrastructures are reliant on CPS-techs & communication networks
  - The Physics and The Cyber: Intertwined Responsibilities

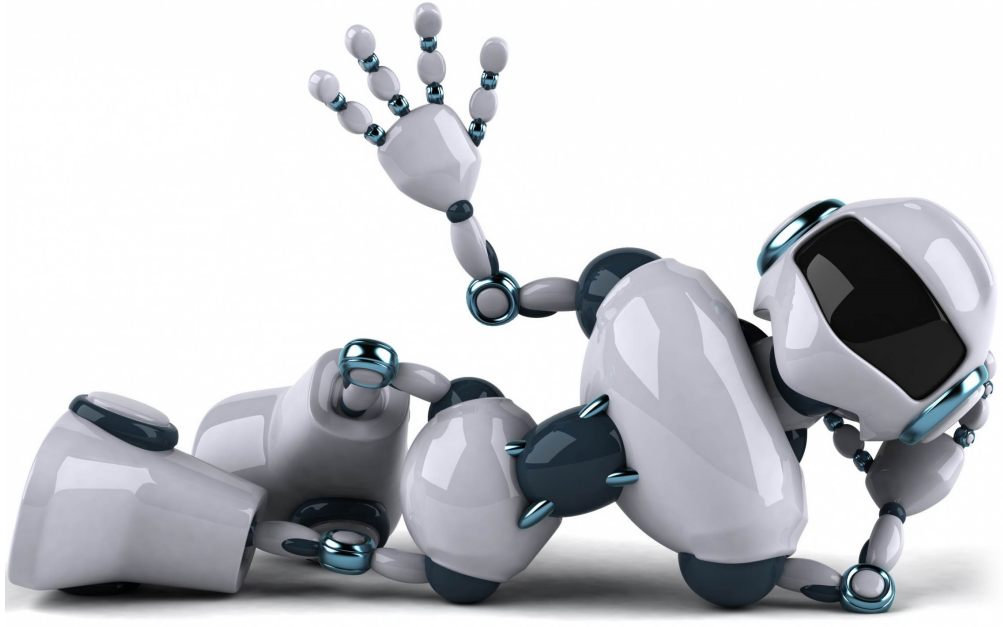
- CPSs are *inherently uncertain*; *vulnerable* to hackers & natural adversities

#TrustIssues

Can we trust computers to manage, control, and optimize physics?








music


08:37
7
12

CPS History [Jeschke, 2013]

1898: Nikola Tesla's Radio-Controlled Boat — *Teleautomaton*

CPS History [Jeschke, 2013]

1898: Nikola Tesla's Radio-Controlled Boat — *Teleautomaton*

1948: Norbert Wiener's Cybernetics

CPS History [Jeschke, 2013]

1898: Nikola Tesla's Radio-Controlled Boat — *Teleautomaton*

↓

1948: Norbert Wiener's Cybernetics

↓

1961: Charles Draper — Apollo Guidance Computer

CPS History [Jeschke, 2013]

1898: Nikola Tesla's Radio-Controlled Boat — *Teleautomaton*

↓

1948: Norbert Wiener's Cybernetics

↓

1961: Charles Draper — Apollo Guidance Computer

↓

1999: Kevin Ashton's Internet of Things

CPS History [Jeschke, 2013]

1898: Nikola Tesla's Radio-Controlled Boat — *Teleautomaton*

↓

1948: Norbert Wiener's Cybernetics

↓

1961: Charles Draper — Apollo Guidance Computer

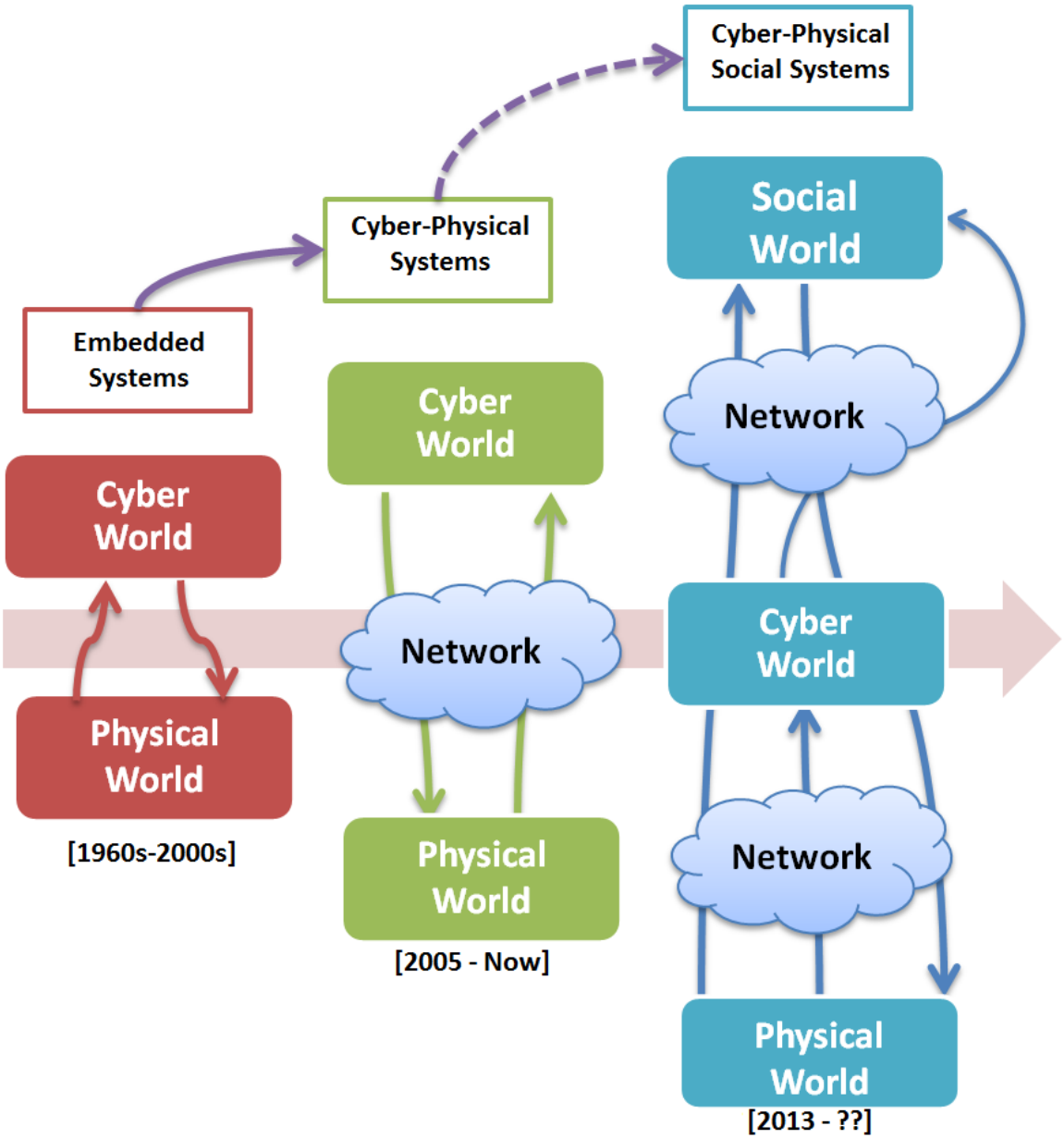
↓

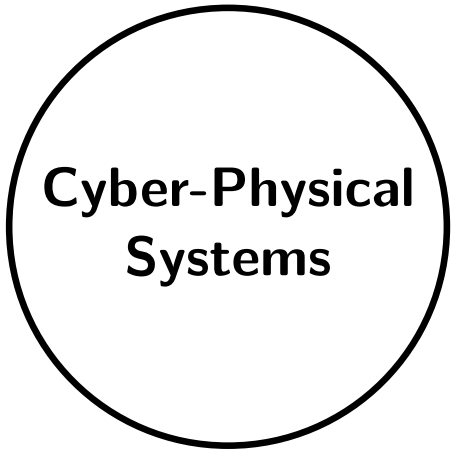
1999: Kevin Ashton's Internet of Things

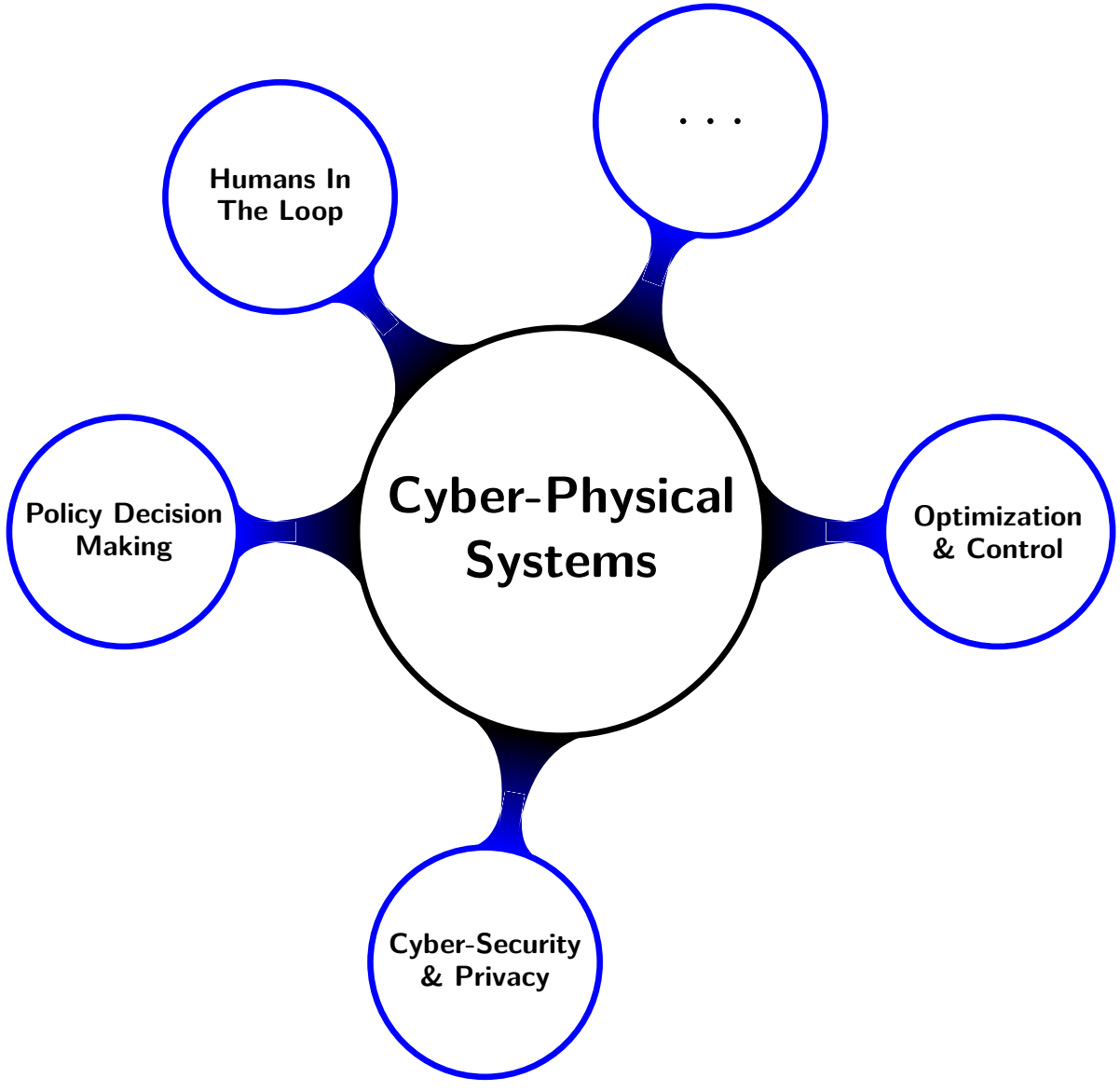
↓

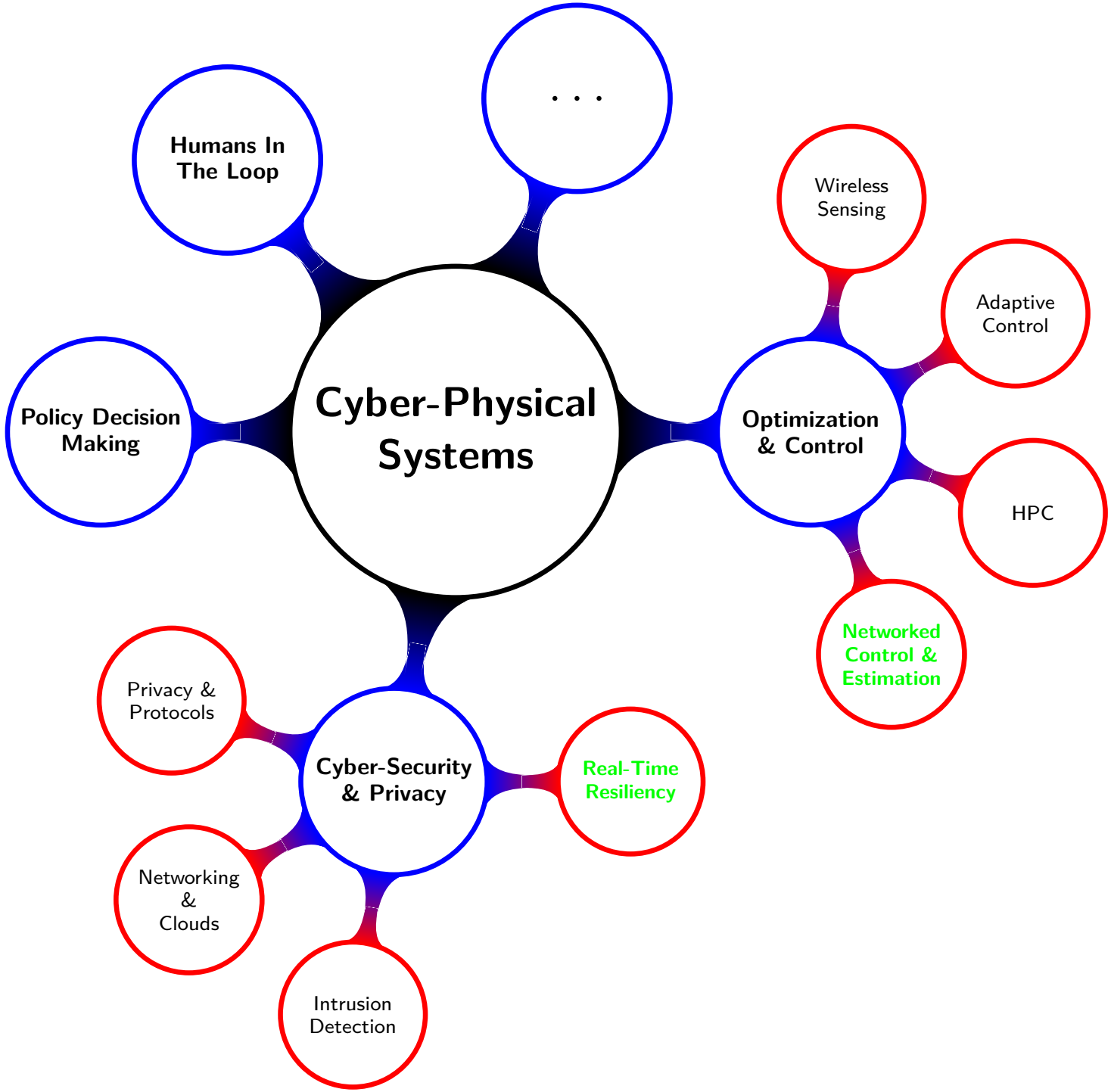
2006: Helen Gill's CPS Definition

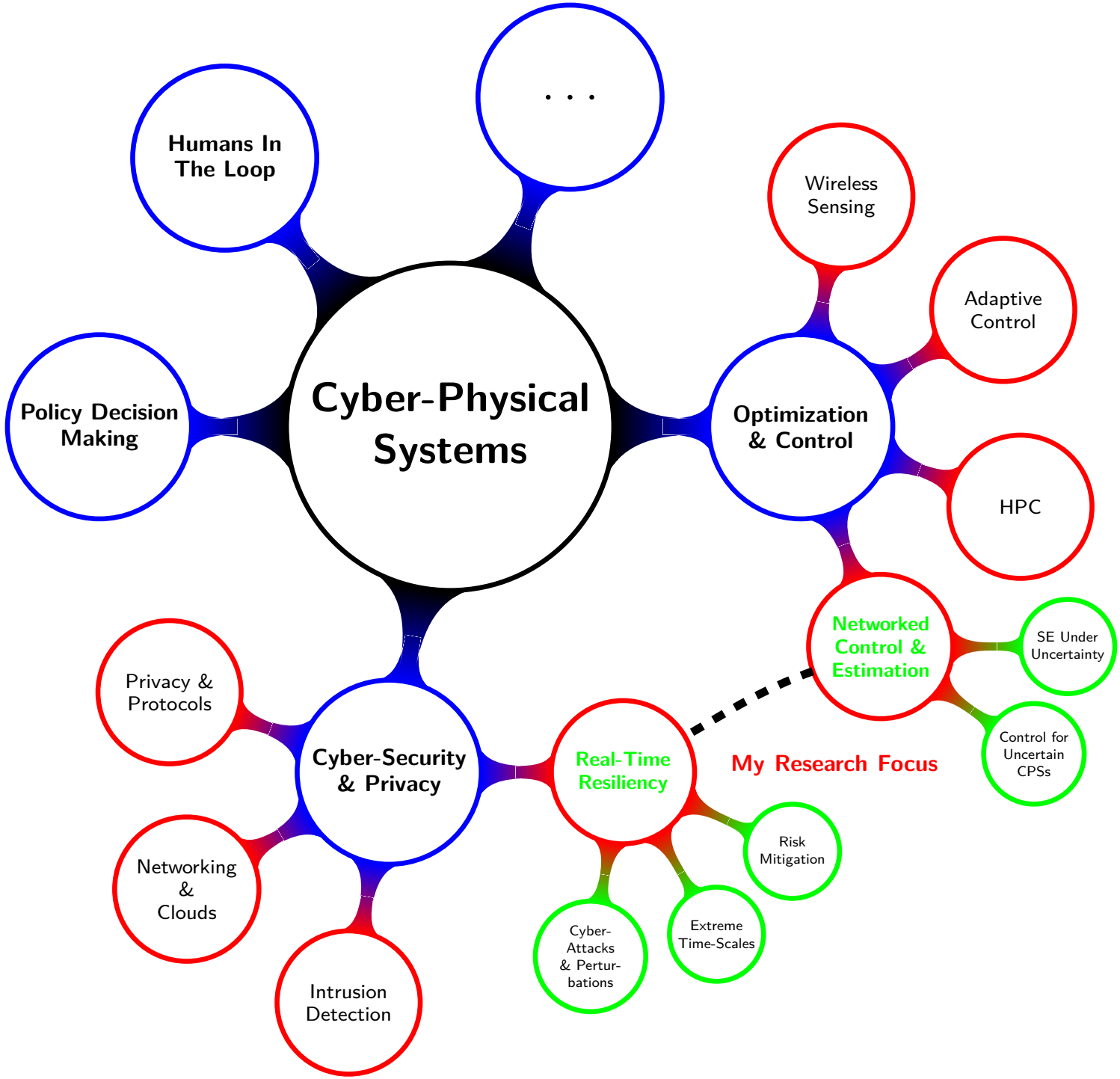
CPS & CPSS Evolution




Cyber-Physical
Systems


Humans In
The Loop
. . .
Policy Decision
Making
Cyber-Physical
Systems
Optimization
& Control
Cyber-Security
& Privacy


Cyber-Physical Systems
Humans In The Loop
. . .
Policy Decision Making
Optimization & Control
Wireless Sensing
Adaptive Control
HPC
Networked Control & Estimation
Cyber-Security & Privacy
Privacy & Protocols
Real-Time Resiliency
Networking & Clouds
Intrusion Detection


Cyber-Physical Systems
Humans In The Loop
. . .
Policy Decision Making
Optimization & Control
Wireless Sensing
Adaptive Control
HPC
Networked Control & Estimation
SE Under Uncertainty
Control for Uncertain CPSs
My Research Focus
Real-Time Resiliency
Risk Mitigation
Extreme Time-Scales
Cyber-Attacks & Perturbations
Cyber-Security & Privacy
Privacy & Protocols
Networking & Clouds
Intrusion Detection

CPS Vision & Mission

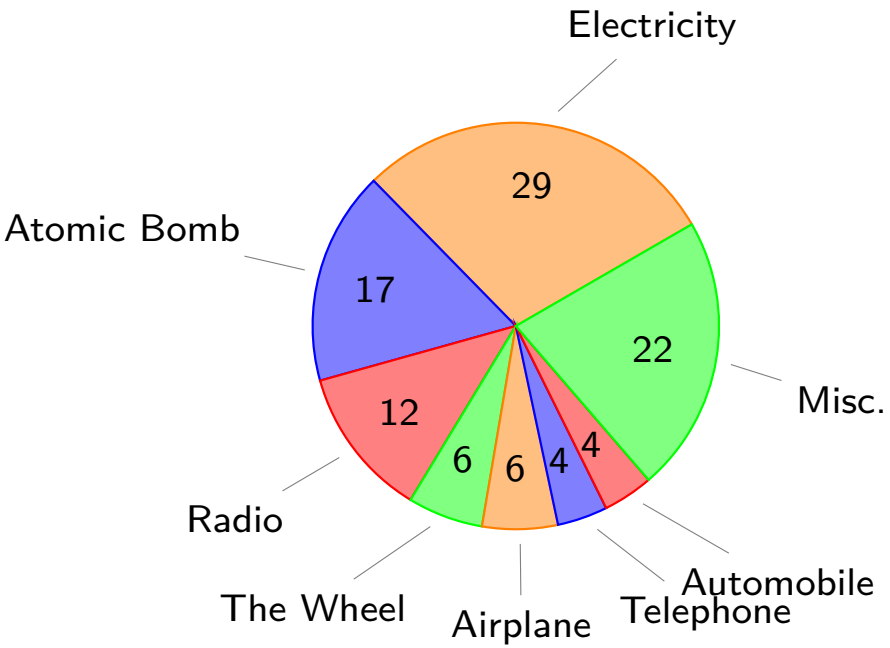
- **Vision**: *building* ***secure & resilient critical infrastructures***
- ***Mission***: *leading efforts to secure infrastructure by* ***managing risk & enhancing resilience*** *through open collaborations* — a DHS mission [DHS, 2015]

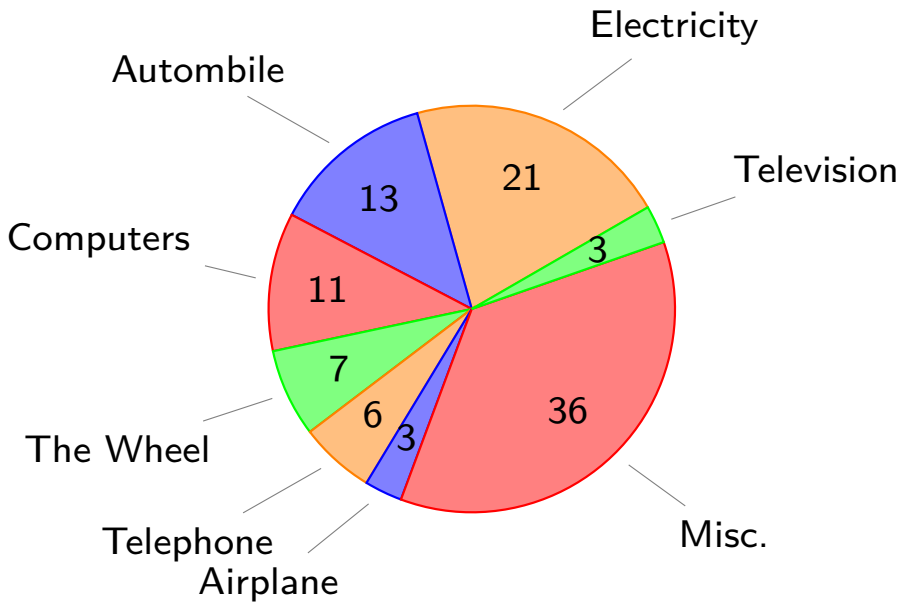
Research **Focus**

Developing secure computational methods for uncertain CPSs with applications to dominant CPS applications

Polls of Greatest Inventions

- Polls of greatest inventions ever made — in 1947 & 2005 [Gallup, 2005]
- Most are CPSs: varying in complexity and size





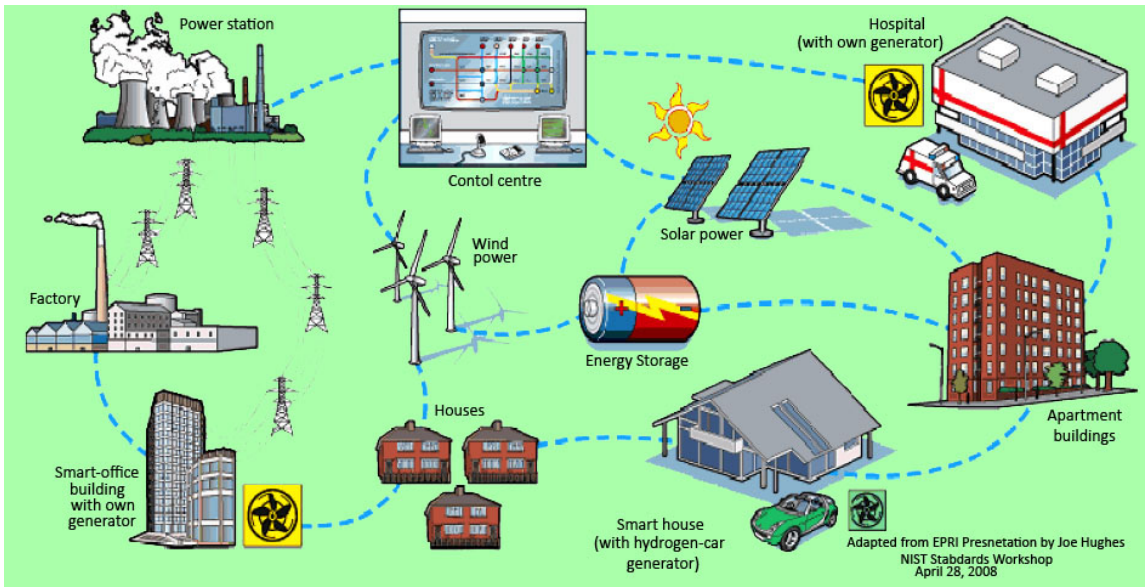
- Electricity remains on top
- With increasing role of **networks**, security has been identified as one of the main issues [Sridhar et al., 2012]

Part II — CPS Application: Smart Grids

Smart Grids: The Most Complex CPS?

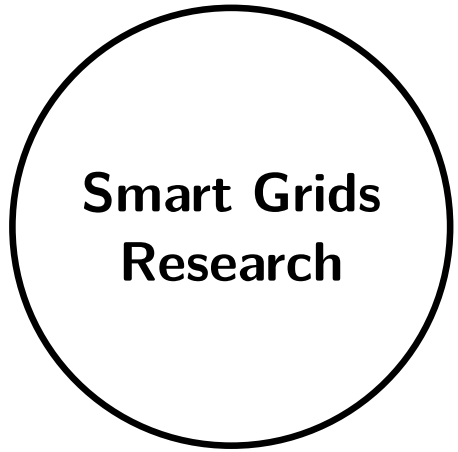
What is a Smart Grid?

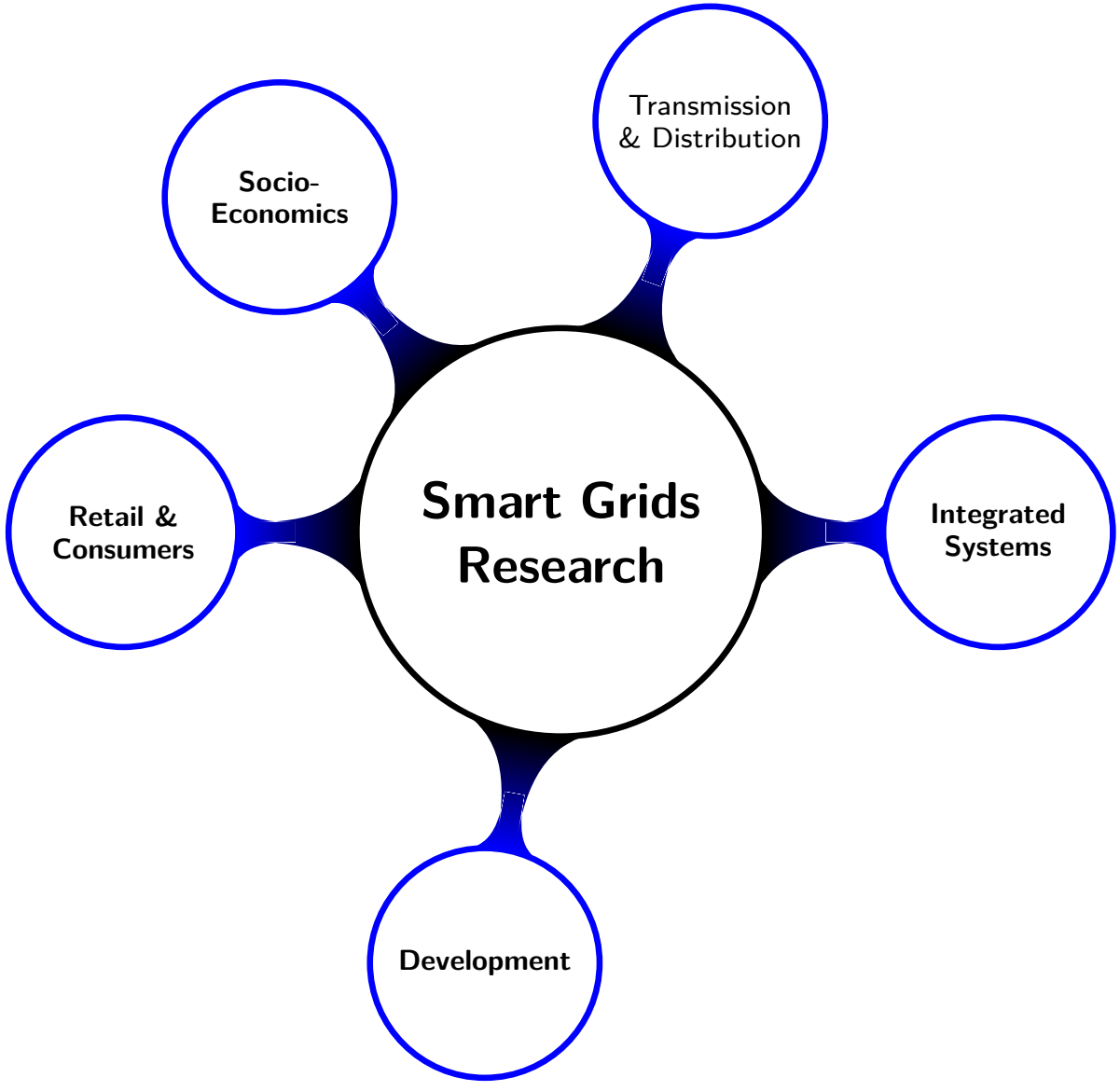
- Modernized electrical grid, uses communications to gather & act on data such as:
  - Consumers' & suppliers' behaviors and preference, market competition, pricing

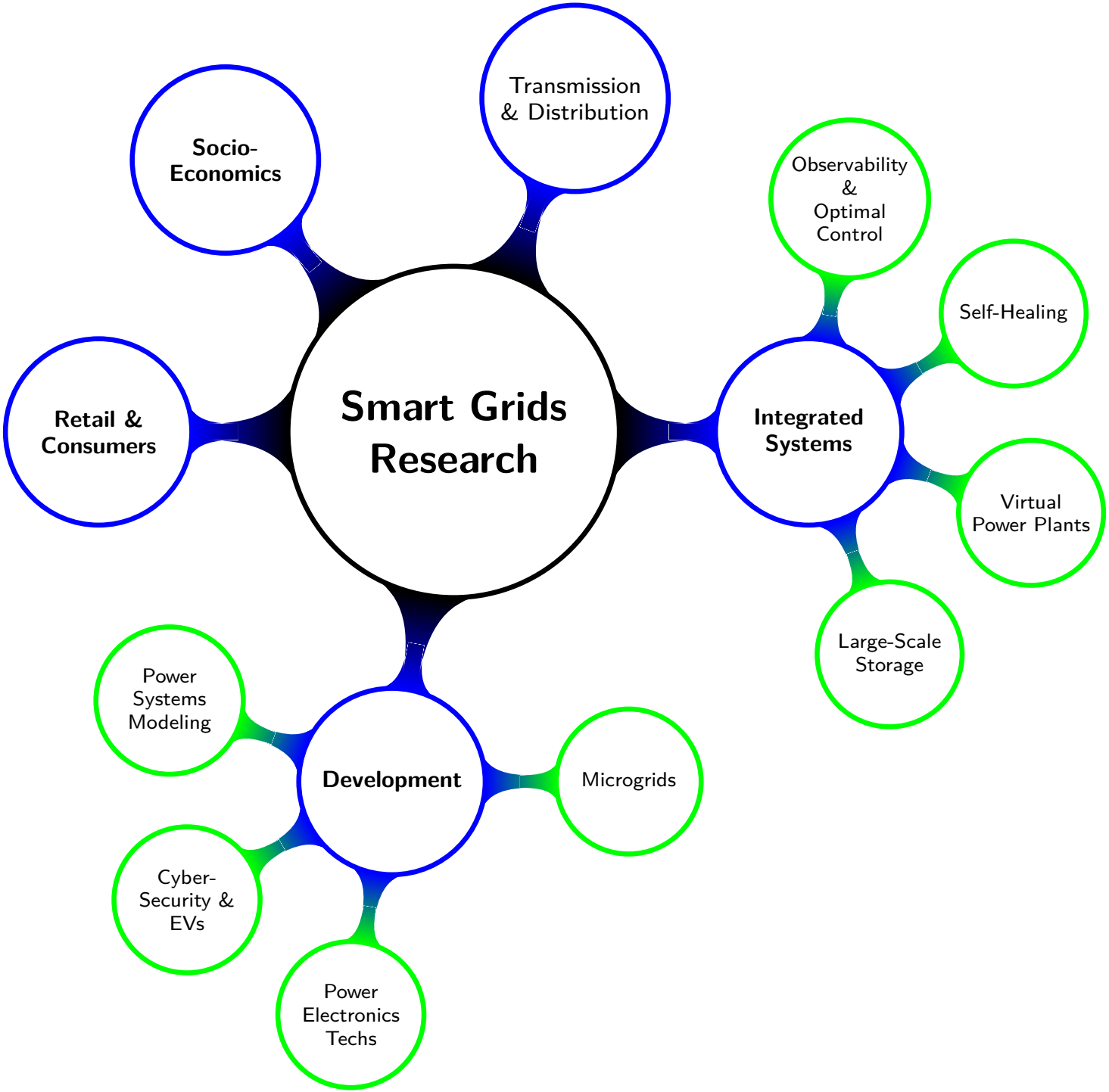


SMART-GRIDS SHOULD **coordinate** NEEDS & CAPABILITIES OF **all market stakeholders** TO OPERATE PARTS OF THE SYSTEM AS **efficiently** AS POSSIBLE, MINIMIZING COSTS & ENVIRONMENTAL IMPACTS WHILE MAXIMIZING SYSTEM RELIABILITY, **resilience & stability**.[1]

[1] Technology Road-map, International Energy Agency, 2011.


Smart Grids
Research


Smart Grids Research
Transmission & Distribution
Socio-Economics
Retail & Consumers
Integrated Systems
Development


Smart Grids Research
Socio-Economics
Transmission & Distribution
Retail & Consumers
Integrated Systems
Observability & Optimal Control
Self-Healing
Virtual Power Plants
Large-Scale Storage
Development
Power Systems Modeling
Microgrids
Cyber-Security & EVs
Power Electronics Techs

CPS & Smart-Grid Research: Dynamic State Estimation

- What is *dynamic state estimation* (DSE)?
  - Accurately depicting what's happening inside a system
- Precisely: estimating internal system states
  - In circuits: *voltages and currents*
  - Water networks: *amount of water flowing*
  - Chemical plants: *concentrations*
  - Robots and UAVs: *location & speed*
  - Humans: *temperature, blood pressure, glucose level*
- *So how does having estimates help me?*
  - Well, if you have estimates, you can do control
  - And if you do good control, you become better off!
- In power systems: DSE can tell me what's happening to generators & lines

$$\Rightarrow \textsc{Preventing/Predicting Blackouts!}$$

Research Question

What is a secure DSE method for power systems under attacks & unknown inputs?

- Research @ Argonne National Lab, supported by DoE

Why Dynamic State Estimation?

- Because static state estimators may not detect *anomalies*
- Availability of real-time data from PMUs $\Rightarrow$ utilize DSE methods...

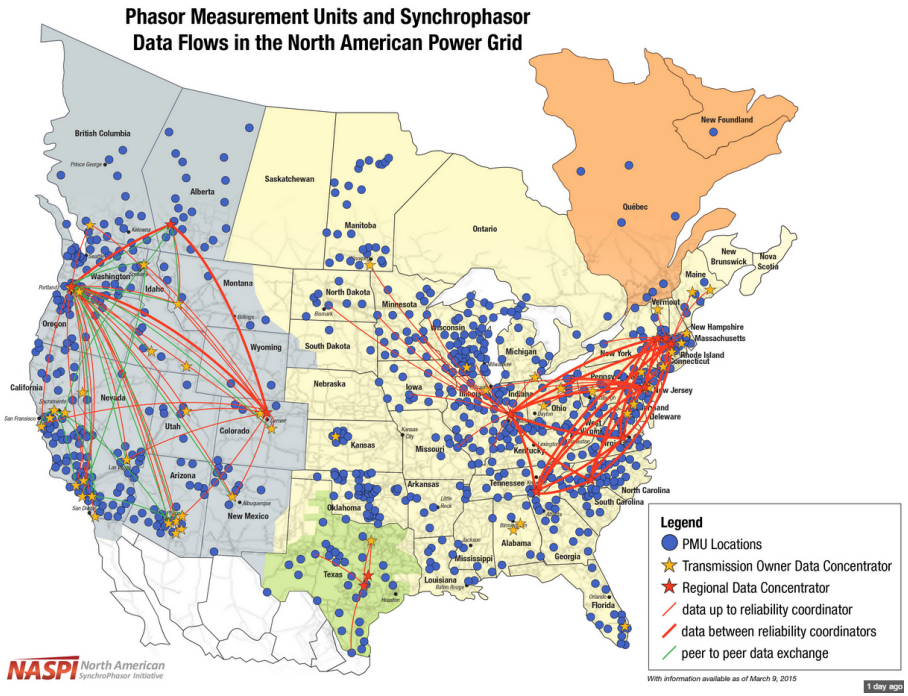


Figure from: https://www.naspi.org

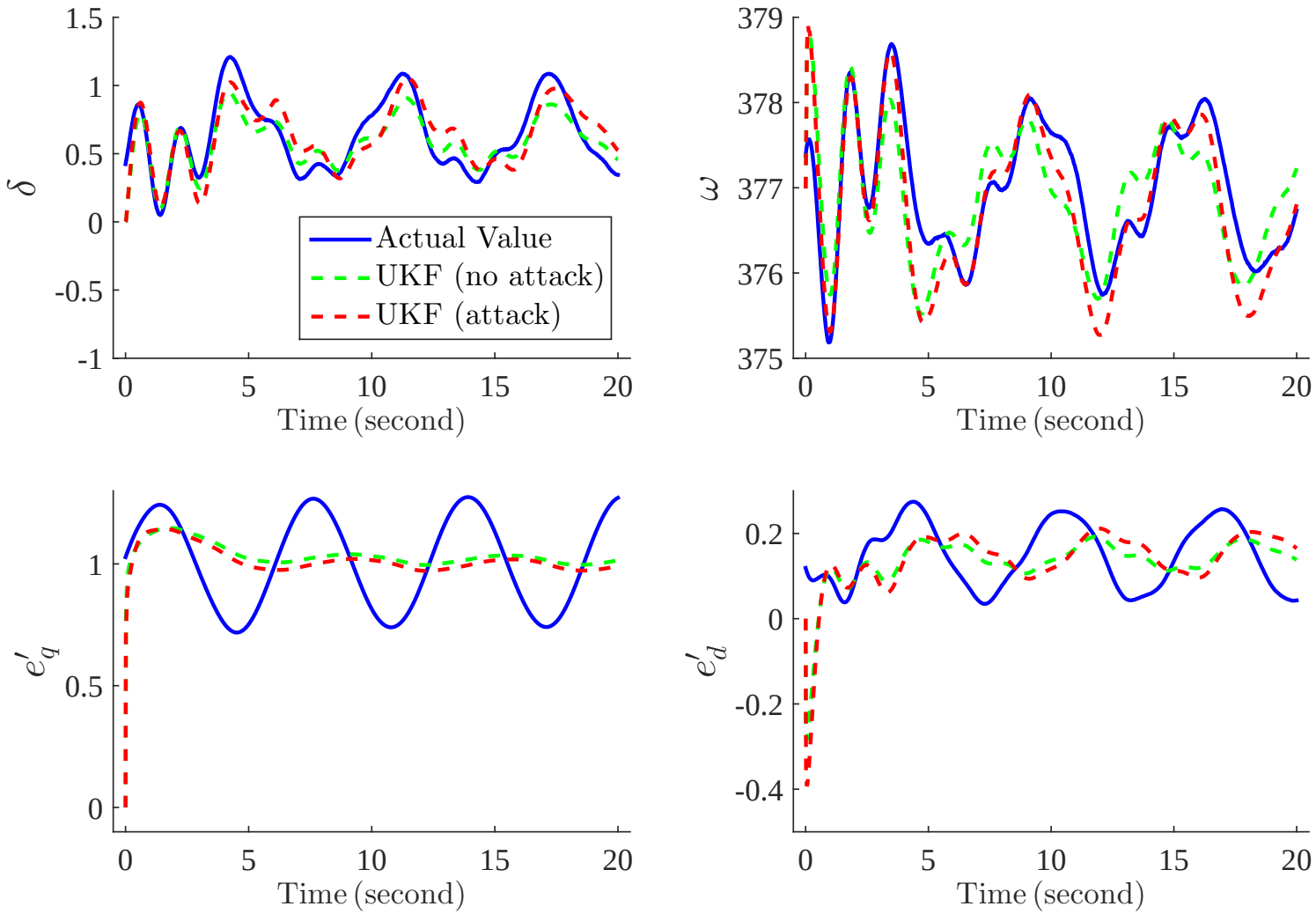
- ...But PMUs can be subject to disturbances, malfunctions
- Failure scenarios [EPRI, 2014]:
  - WAMPAC.4: *Measurement Data Compromised*
  - WAMPAC.6: *Communications Compromised between PMUs & Control Center*

Research Gap

Recent DSE studies can not deal with unknown inputs & potential attack vectors

Current Methods: Tested Under Attacks & Unknown Inputs

- Unscented Kalman Filter [Wang et al., 2012; Singh & Pal, 2014] state-estimation

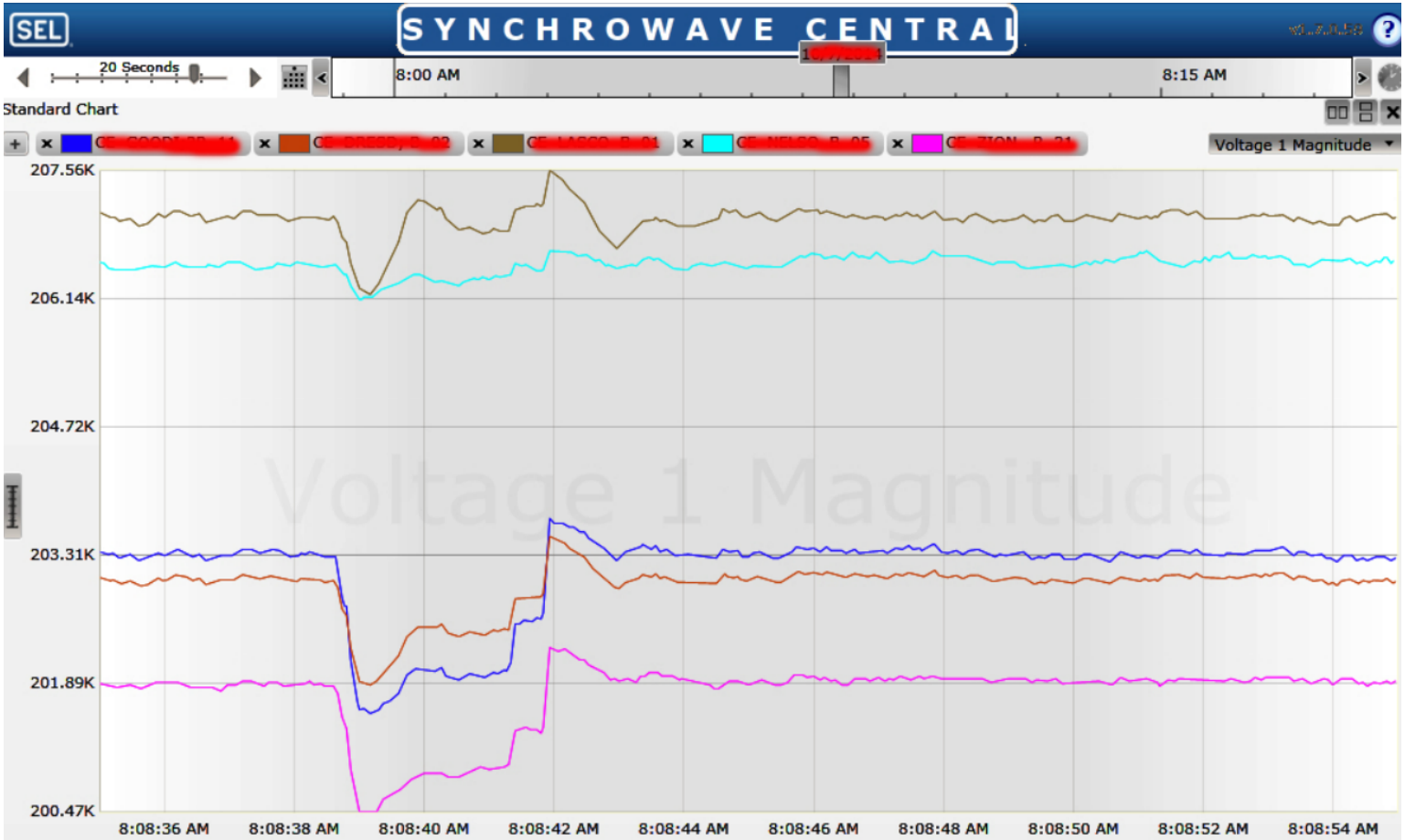


The Poor Ol' Squirrel...And the 12kV Bus[2]

- Picture is self-explanatory
- Squirrel should have been elsewhere ☹

[2] Credits to Commonwealth Edison (ComEd — largest utility in Illinois) for sharing the pictures.

PMU Measurements — Lesson Learned



- PMU detected the **significant** transients due to the squirrel *bite*
- ComEd/Argonne work: better models + **improved DSE** + event detection

Current DSE Methods

Power systems DSE has been implemented by:

- Stochastic estimators:
  - EKF, UKF, PF [Ghahremani & Kamwa, 2011; Singh & Pal, 2014; Ghahremani & Kamwa, 2015]
  - Methods perform poorly in higher dimensions & under attack vectors
- Deterministic linear observers [Pasqualetti et al., 2011; Teixeira et al., 2010]

Our DSE Objective

Objective 1

Present DSE alternatives that address major limitations of current DSE methods such as:

- Tolerance to state-disturbances & attack-vectors
- Unknown initial conditions
- Guaranteed convergence

Objective 2

Perform comparative study and **recommend** DSE methods for uncertain CPSs

Single-Machine Infinite Bus (SMIB) System Dynamics

- SMIB: simplification of a power system — benchmark in DSE studies [Tripathy et al., 2010; Singh & Pal, 2014; Ghahremani & Kamwa, 2015]
- Nominal SMIB nonlinear dynamics:

$$\dot{\boldsymbol{x}}(t) = \underbrace{\boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t)}_{\text{linear terms}} + \underbrace{\boldsymbol{\phi}(\boldsymbol{x}, \boldsymbol{u})}_{\text{nonlinear interconnections}}$$

$$\boldsymbol{x} = \begin{bmatrix} \delta \\ \omega \\ e'_q \\ e'_d \end{bmatrix}, \boldsymbol{u} = \begin{bmatrix} T_m \\ E_{f_d} \end{bmatrix}, \boldsymbol{A} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -\frac{K_D}{2H} & 0 & 0 \\ 0 & 0 & -\frac{1}{T'_{do}} & 0 \\ 0 & 0 & 0 & -\frac{1}{T'_{qo}} \end{bmatrix}$$

$$\boldsymbol{B} = \begin{bmatrix} 0 & 0 \\ \frac{\omega_0}{2H} & 0 \\ 0 & \frac{1}{T'_{do}} \\ 0 & 0 \end{bmatrix}, \boldsymbol{\phi}(\boldsymbol{x}, \boldsymbol{u}) = \begin{bmatrix} -\omega_0 \\ \frac{\omega_0}{2H}\left(-T_e(\boldsymbol{x}, \boldsymbol{u}) + K_D\right) \\ -\frac{x_d - x'_d}{T'_{do}} i_d(\boldsymbol{x}, \boldsymbol{u}) \\ \frac{x_q - x'_q}{T'_{qo}} i_q(\boldsymbol{x}, \boldsymbol{u}) \end{bmatrix}$$

Proposal I: Stochastic Estimation — Cubature Kalman Filter (CKF)

- EKF & UKF can suffer from the curse of dimensionality
- CKF: scalable computations of multivariate moments [Arasaratnam & Haykin, 2009]
- We utilize CKF for DSE in power systems
- SMIB nonlinear system can be written in discrete-time form:

$$\boldsymbol{x}_k = \boldsymbol{f}(\boldsymbol{x}_{k-1}, \boldsymbol{u}_{k-1}) + \boldsymbol{q}_{k-1}$$
$$\boldsymbol{y}_k = \boldsymbol{h}(\boldsymbol{x}_k, \boldsymbol{u}_k) + \boldsymbol{r}_k$$

  - $\boldsymbol{q}_{k-1} \sim N(0, \boldsymbol{Q}_{k-1})$ and $\boldsymbol{r}_k \sim N(0, \boldsymbol{R}_k)$: process & measurement noise
  - $\boldsymbol{Q}_{k-1}$ and $\boldsymbol{R}_k$: covariance of $\boldsymbol{q}_{k-1}$ & $\boldsymbol{r}_k$

Proposal II: Deterministic Estimation — Dynamic Observers

- **Question:** What if statistical distributions are unavailable or inaccurate?
- **Answer:** Use deterministic estimators
- Nonlinear term in the dynamics $\boldsymbol{\phi}(\boldsymbol{x}, \boldsymbol{u})$ is:
  - One-sided Lipschitz:

$$\langle \boldsymbol{\phi}(\boldsymbol{x}, \boldsymbol{u}) - \boldsymbol{\phi}(\boldsymbol{z}, \boldsymbol{u}), \boldsymbol{x} - \boldsymbol{z} \rangle \leq k_1 \|\boldsymbol{x} - \boldsymbol{z}\|^2$$

  - Quadratically inner-bounded:

$$(\boldsymbol{\phi}(\boldsymbol{x}, \boldsymbol{u}) - \boldsymbol{\phi}(\boldsymbol{z}, \boldsymbol{u}))^\top (\boldsymbol{\phi}(\boldsymbol{x}, \boldsymbol{u}) - \boldsymbol{\phi}(\boldsymbol{z}, \boldsymbol{u})) \leq k_2 \|\boldsymbol{x}-\boldsymbol{z}\|^2 + k_3 \langle \boldsymbol{\phi}(\boldsymbol{x}, \boldsymbol{u}) - \boldsymbol{\phi}(\boldsymbol{z}, \boldsymbol{u}), \boldsymbol{x}-\boldsymbol{z} \rangle$$

  - Legitimate assumptions for power systems [Siljak et al., 2002; Kalsi, 2010]
  - Example: if $\boldsymbol{\phi}(\boldsymbol{x}) = \sin(\boldsymbol{x})$, then $\rho = 1$

Observer Design

- Plant dynamics under unknown inputs & attack-vectors:

$$\begin{aligned} \dot{\boldsymbol{x}}(t) &= \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{\phi}(\boldsymbol{x}, \boldsymbol{u}) + \boldsymbol{D}\boldsymbol{d}(t) \\ \boldsymbol{y}(t) &= \boldsymbol{C}\boldsymbol{x}(t) + \boldsymbol{v}(t) \end{aligned}$$

- Observer dynamics [Zhang et al., 2012]:

$$\dot{\hat{\boldsymbol{x}}}(t) = \boldsymbol{A}\hat{\boldsymbol{x}}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{\phi}(\hat{\boldsymbol{x}}, \boldsymbol{u}) + \boldsymbol{L}(\boldsymbol{y}(t) - \boldsymbol{C}\hat{\boldsymbol{x}}(t))$$

- Matrix-gain $\boldsymbol{L}$ determined as follows:
  1. Given k_1, k_2, k_3, solve this LMI for $\epsilon_1, \epsilon_2, \sigma$ and $\boldsymbol{P} = \boldsymbol{P}^\top \succ \boldsymbol{O}$:

$$\begin{bmatrix} \boldsymbol{A}^\top \boldsymbol{P} + \boldsymbol{P}\boldsymbol{A} + (\epsilon_1 k_1 + \epsilon_2 k_2)\boldsymbol{I}_n - \sigma \boldsymbol{C}^\top \boldsymbol{C} & \boldsymbol{P} + \dfrac{k_3\epsilon_2 - \epsilon_1}{2}\boldsymbol{I}_n \\ \left(\boldsymbol{P} + \dfrac{k_3\epsilon_2 - \epsilon_1}{2}\boldsymbol{I}_n\right)^\top & -\epsilon_2 \boldsymbol{I}_n \end{bmatrix} < 0$$

  2. Compute observer gain $\boldsymbol{L}$:

$$\boldsymbol{L} = \frac{\sigma}{2}\boldsymbol{P}^{-1}\boldsymbol{C}^\top$$

- **Extension**: reduced-order DSE

Numerical Results – A Comparative Study

- SMIB parameters from PST toolbox [Chow & Cheung, 1992]
- Initial conditions:

$$\begin{aligned} \boldsymbol{x}(0) &= \begin{bmatrix} 0.4233 & 377.3780 & 1.0277 & 0.1190 \end{bmatrix}^\top \\ \hat{\boldsymbol{x}}(0) &= \begin{bmatrix} 0 & \omega_0 & 0 & 0 \end{bmatrix}^\top \end{aligned}$$

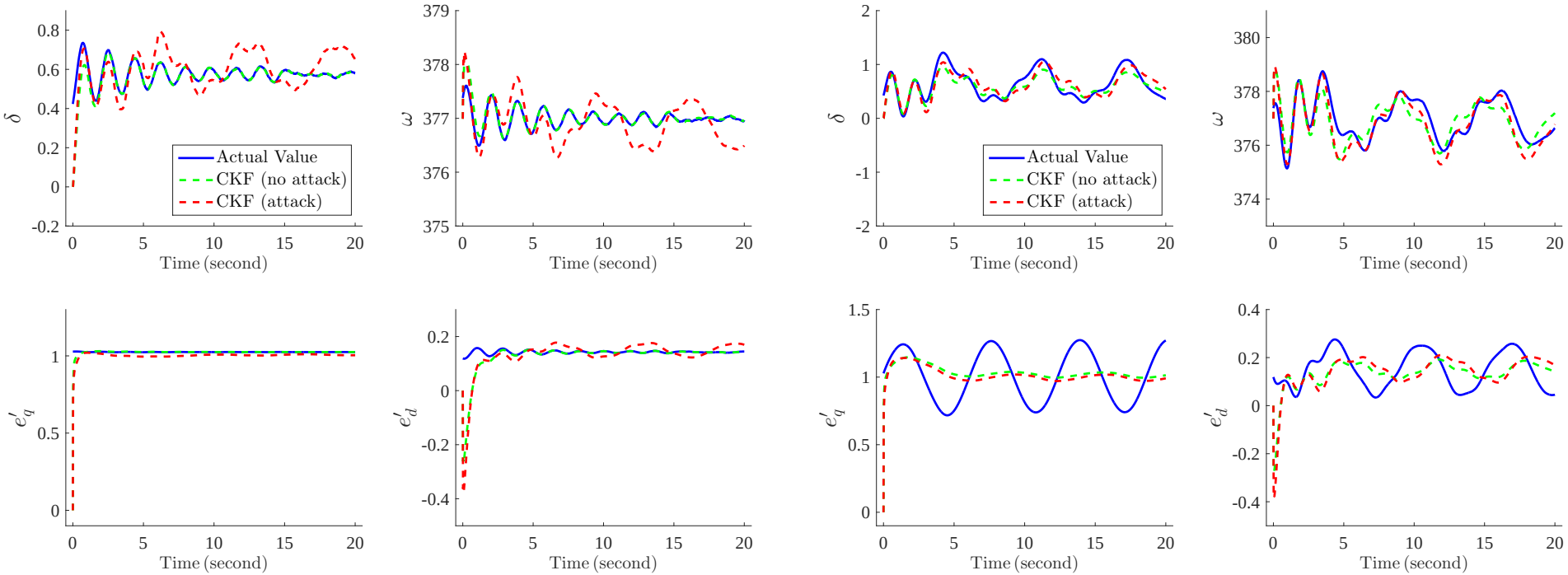
- $\boldsymbol{D}$ is randomly chosen (2 UIs); unknown input vector: $\boldsymbol{d}(t) = 0.01\cos(t)$
- Attack vector, $\boldsymbol{v}(t)$:

$$\begin{aligned} v_1(t) &= 0.2\sin(t) \\ v_2(t) &= \begin{cases} 0.5\sin(2t) + \frac{5}{t^2} & 5 < t < 6 \\ 0 & \text{otherwise} \end{cases} \\ v_3(t) &= 0.3\cos(t) \\ v_4(t) &= 0.2 \end{aligned}$$

- Gaussian process & measurement noise are added

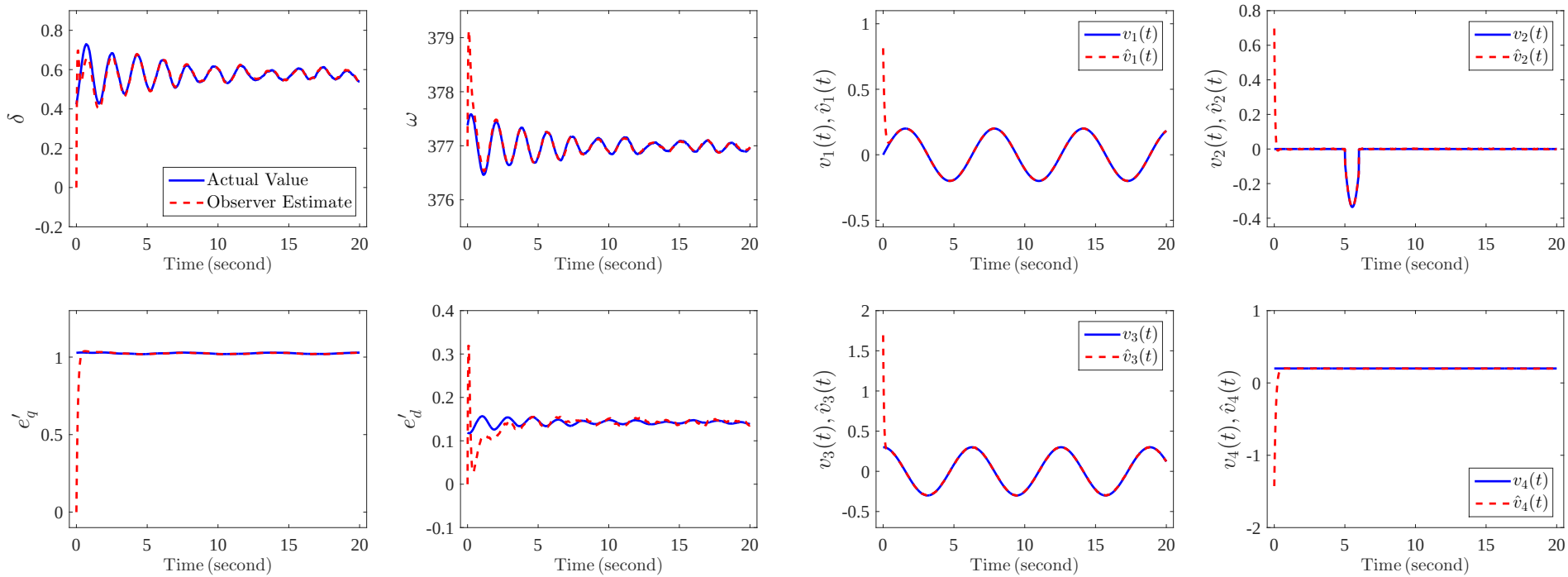
DSE Results: Stochastic Estimation — CKF

- CKF estimates converge in the absence of attack-vectors & unknown inputs (left figure)
- Under noise, unknown inputs & attacks, CKF estimates fail to converge (right figure)



DSE Results: Determinstic Estimation — Dynamic Observer

- Under noise, unknown inputs & attacks, observer estimates rapidly converge (left figure)
- Attack-vector estimator accomplishes near-perfect disturbance estimation (right figure)



DSE for Power Systems: *The Good, the Bad & the Ugly*

#TeamObservers

Functionality/Characteristic	**Kalman Filter Derivatives**			
	EKF	UKF	CKF	Observer
System's Nonlinearities	✗	✓	✓	✓
Tolerance to Different Initial Conditions	✗	✗	✗	✓
Tolerance to Unknown Inputs	✗	✗	✗	✓
Tolerance to Cyber-Attacks	✗	✗	✗	✓
Tolerance to Process & Measurement Noise	✓	✓	✓	✓
Guaranteed Convergence	—	—	—	✓
Computational Complexity	$\mathcal{O}(n^3)$	$\mathcal{O}(n^3)$	$\mathcal{O}(n^3)$	$\mathcal{O}(n^3)$

- Running time:

Initial Conditions	Running Time (seconds)		
	CKF	UKF	Observer
$\hat{\boldsymbol{x}}(0) = [0\ \omega_0\ 0\ 0]^\top$	3.28	6.30	0.76
$\hat{\boldsymbol{x}}'(0) = [3\ \omega_0\ 0\ 0]^\top$	3.27	6.27	0.76

Contributions

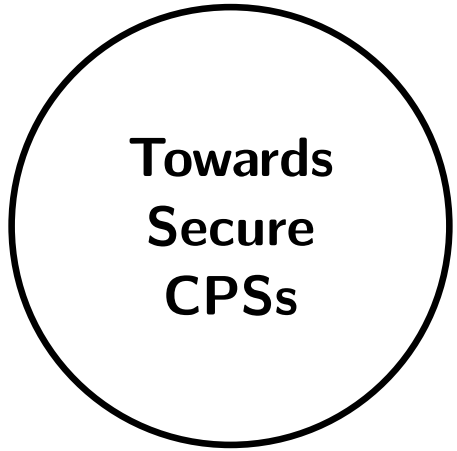
- Current DSE methods: intolerant to attack-vectors & unknown inputs

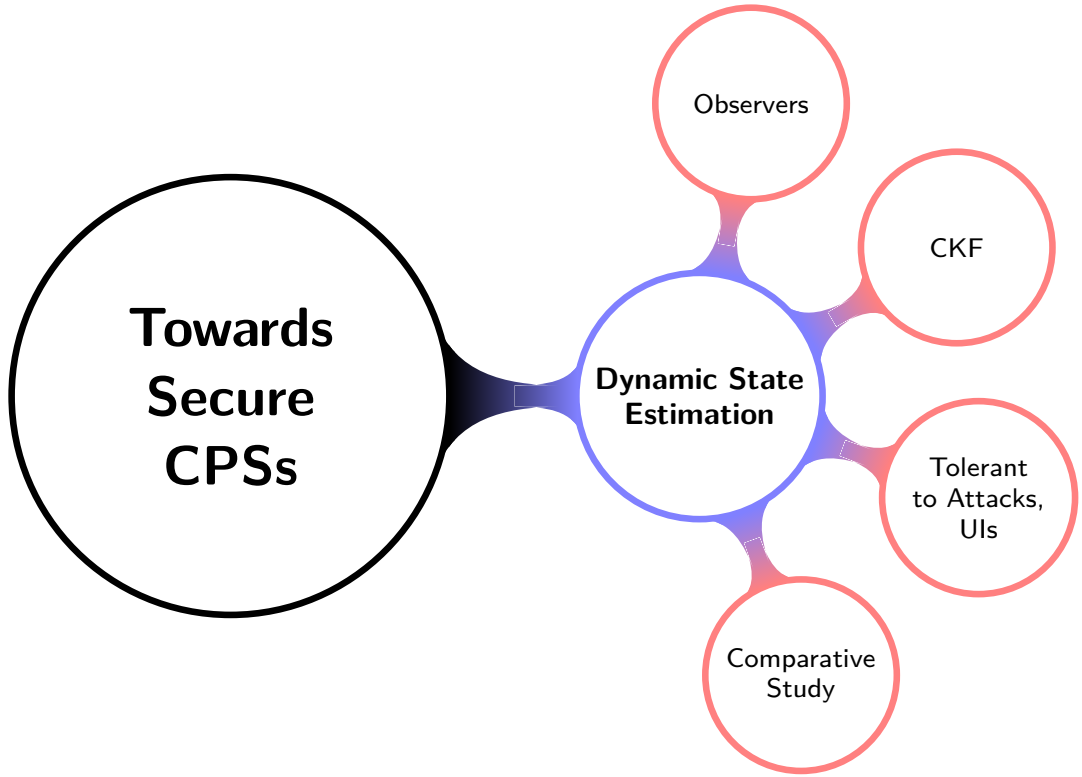
Contributions:

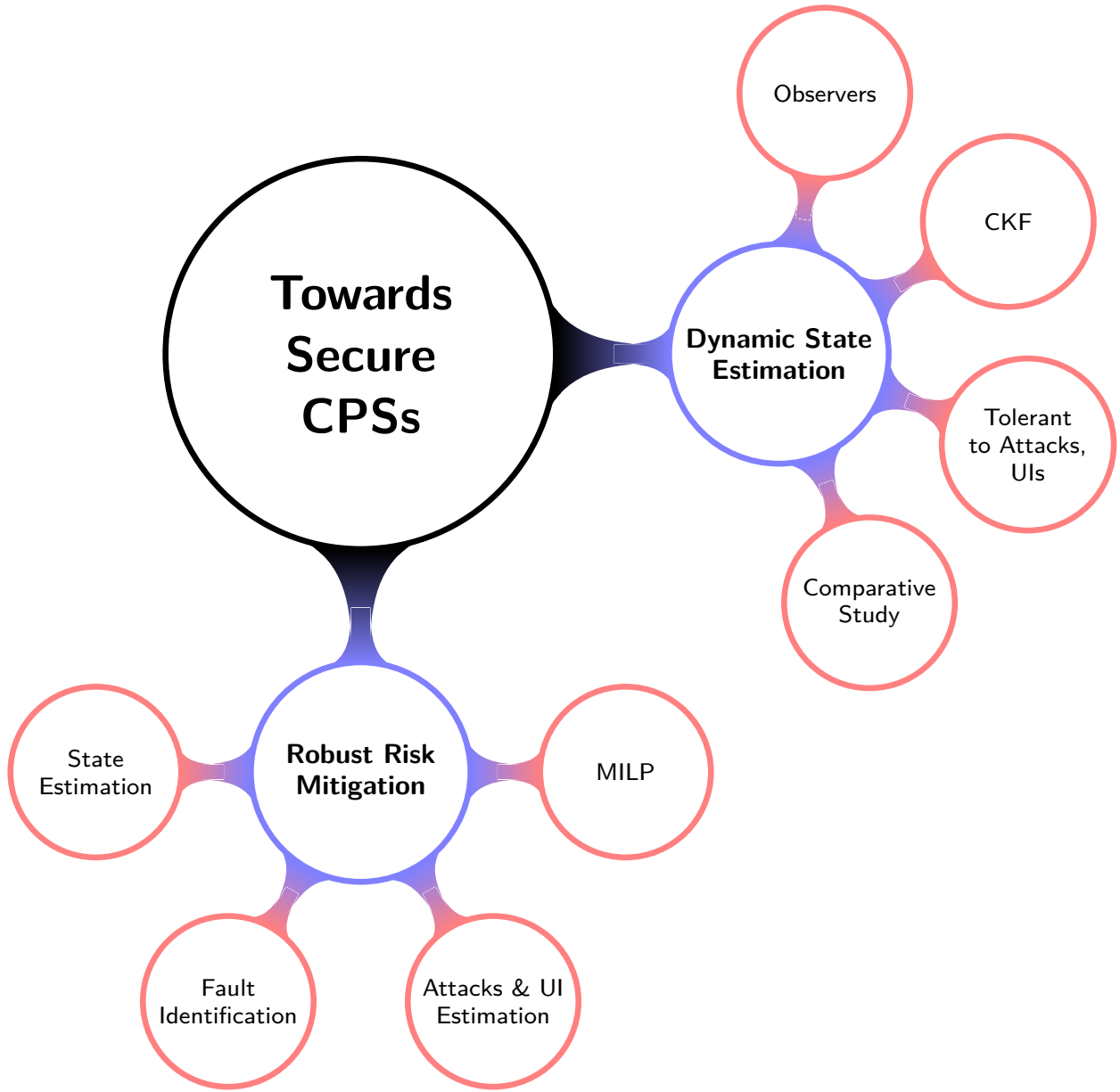
1. Introduce deterministic estimators for nonlinear, uncertain power systems
2. Perform a comparative study of DSE methods for uncertain CPSs & provide recommendations

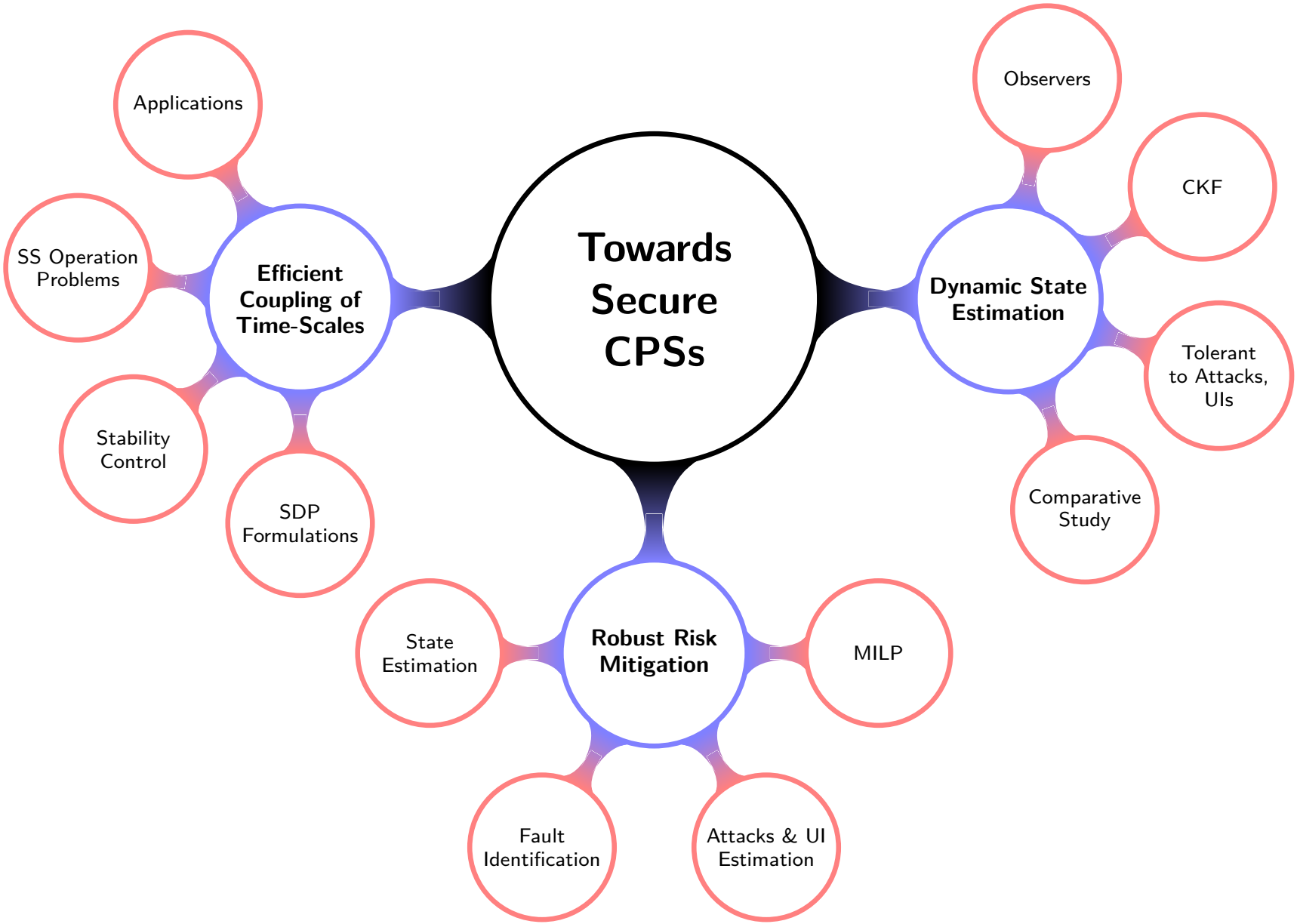
- **Generalization:** under one-sided Lipschitz assumption of $\boldsymbol{\phi}(\boldsymbol{x}, \boldsymbol{u})$, results can be extended to various uncertain CPSs

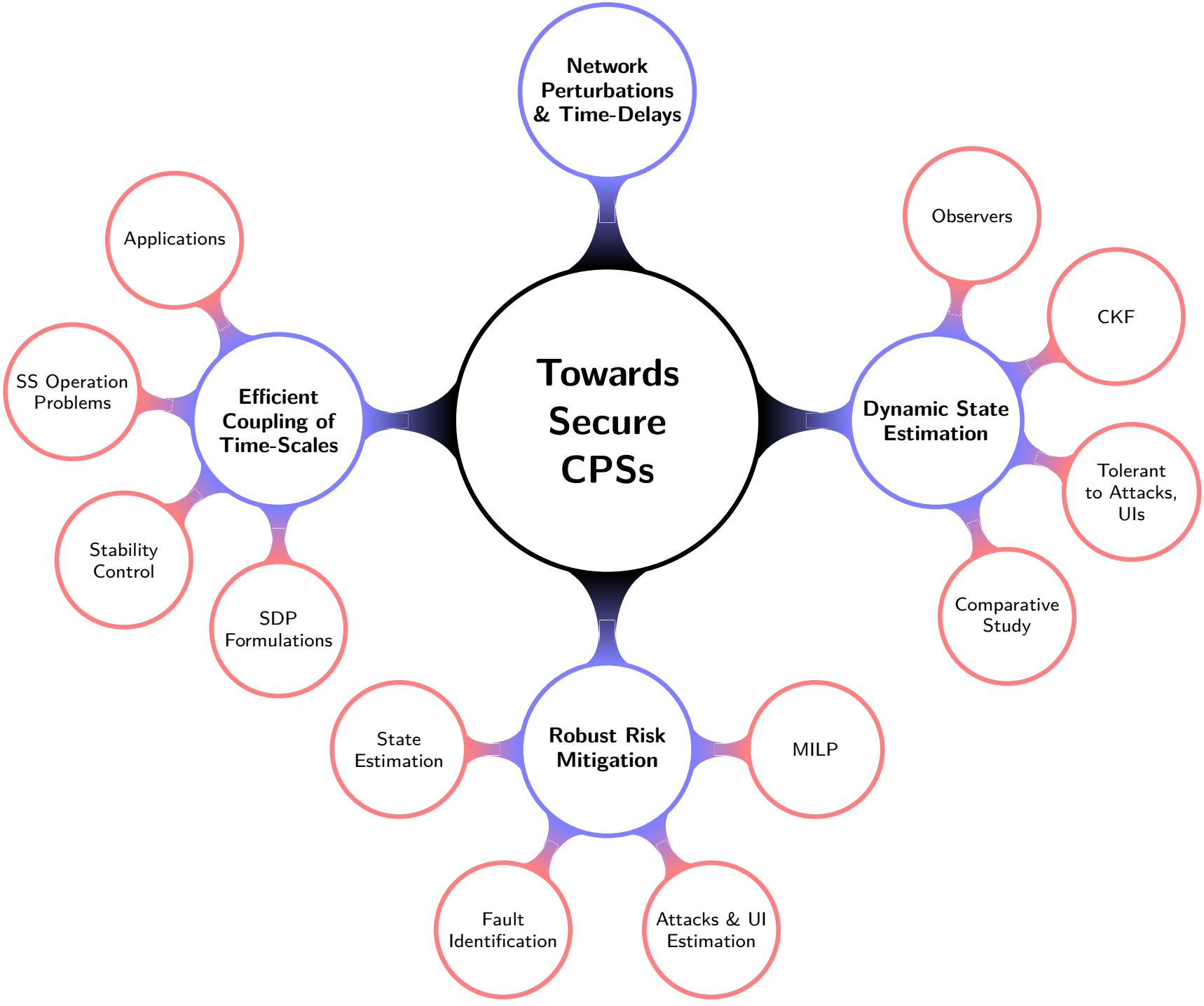
Part III — Future of Research in CPSs, My Interests

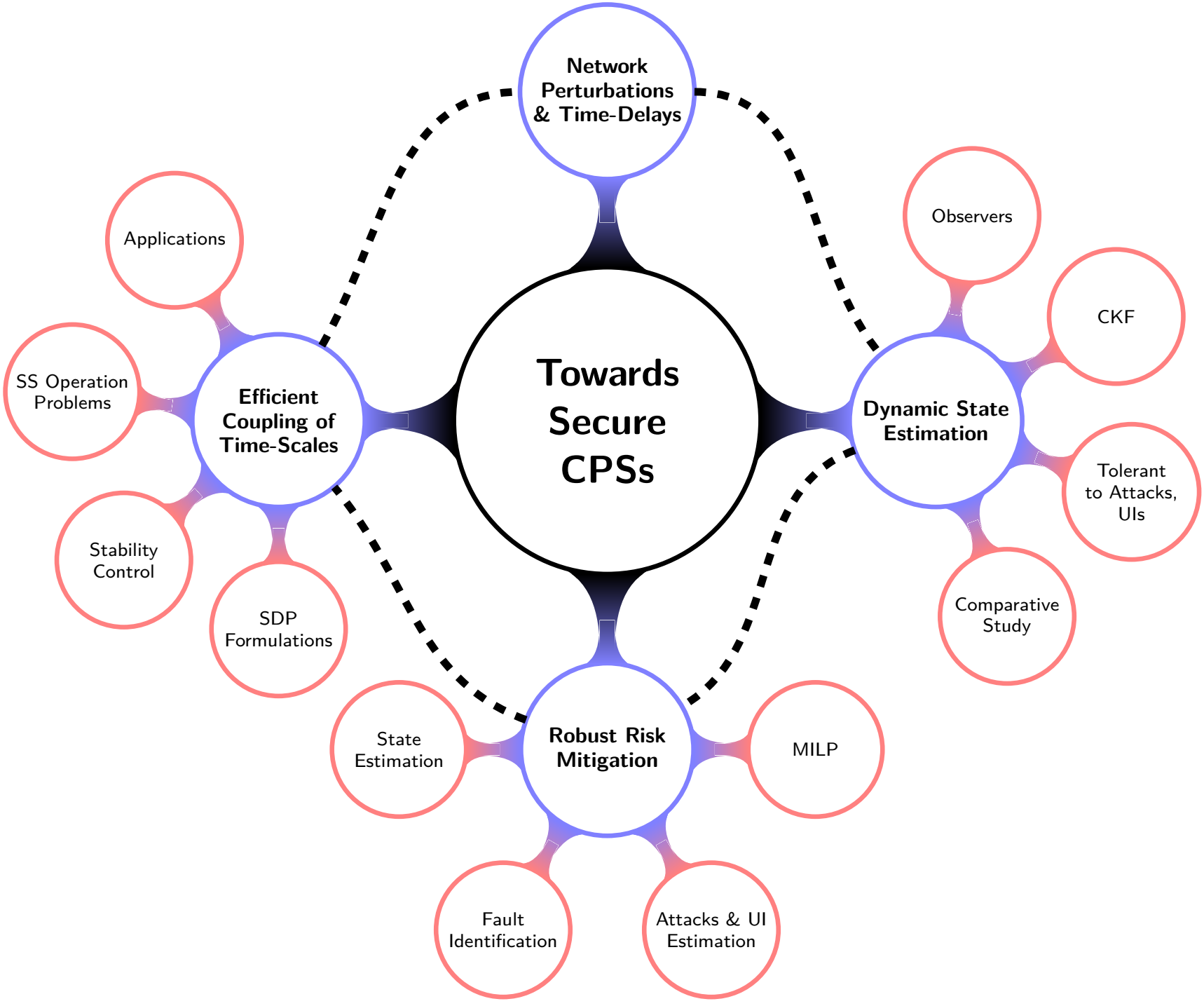

Towards
Secure
CPSs


Towards Secure CPSs
Dynamic State Estimation
Observers
CKF
Tolerant to Attacks, UIs
Comparative Study


Towards Secure CPSs
Dynamic State Estimation
Observers
CKF
Tolerant to Attacks, UIs
Comparative Study
Robust Risk Mitigation
State Estimation
MILP
Fault Identification
Attacks & UI Estimation

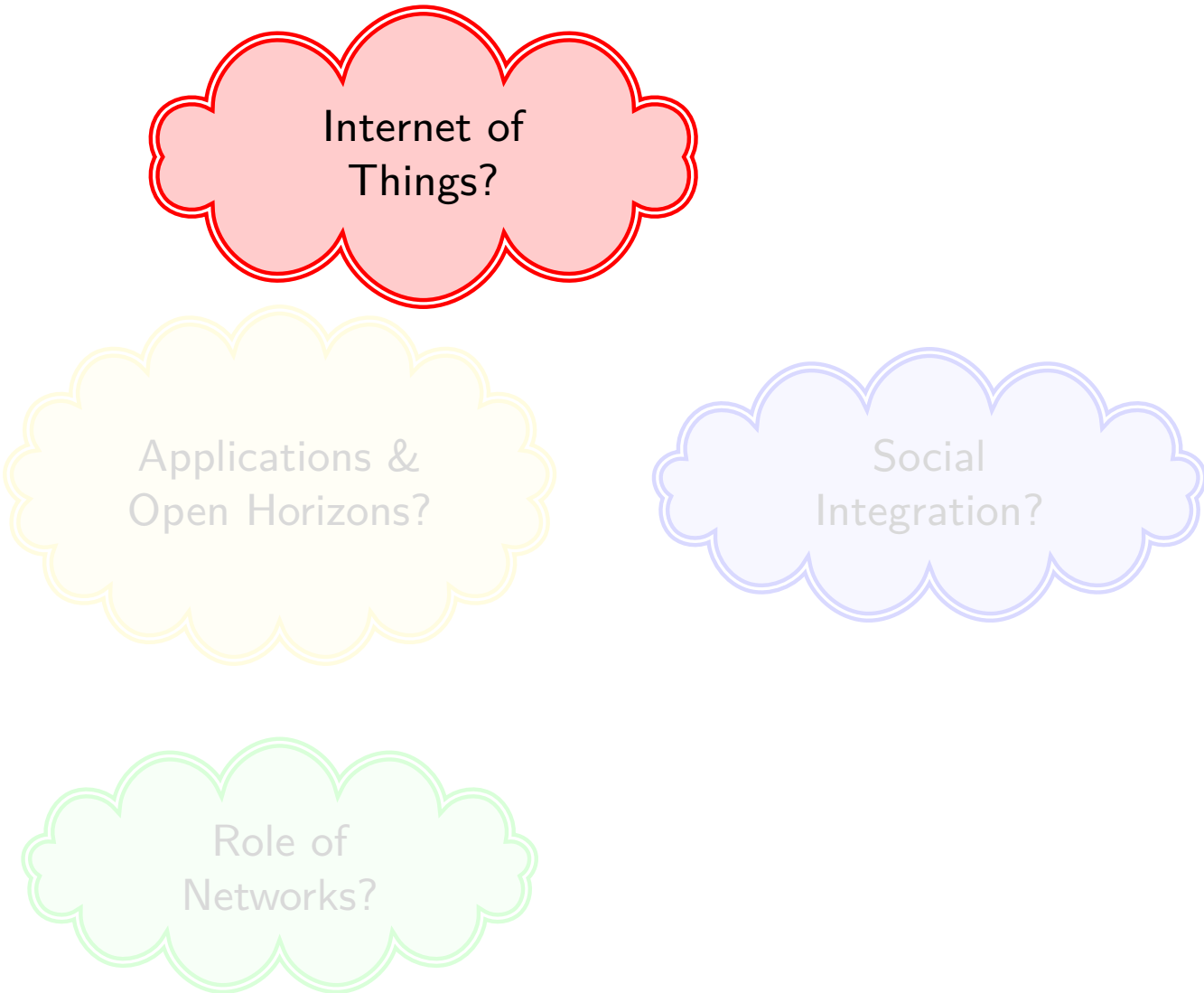

Towards Secure CPSs
Efficient Coupling of Time-Scales
Applications
SS Operation Problems
Stability Control
SDP Formulations
Dynamic State Estimation
Observers
CKF
Tolerant to Attacks, UIs
Comparative Study
Robust Risk Mitigation
State Estimation
MILP
Fault Identification
Attacks & UI Estimation


Towards Secure CPSs
Network Perturbations & Time-Delays
Efficient Coupling of Time-Scales
Applications
SS Operation Problems
Stability Control
SDP Formulations
Dynamic State Estimation
Observers
CKF
Tolerant to Attacks, UIs
Comparative Study
Robust Risk Mitigation
State Estimation
MILP
Fault Identification
Attacks & UI Estimation

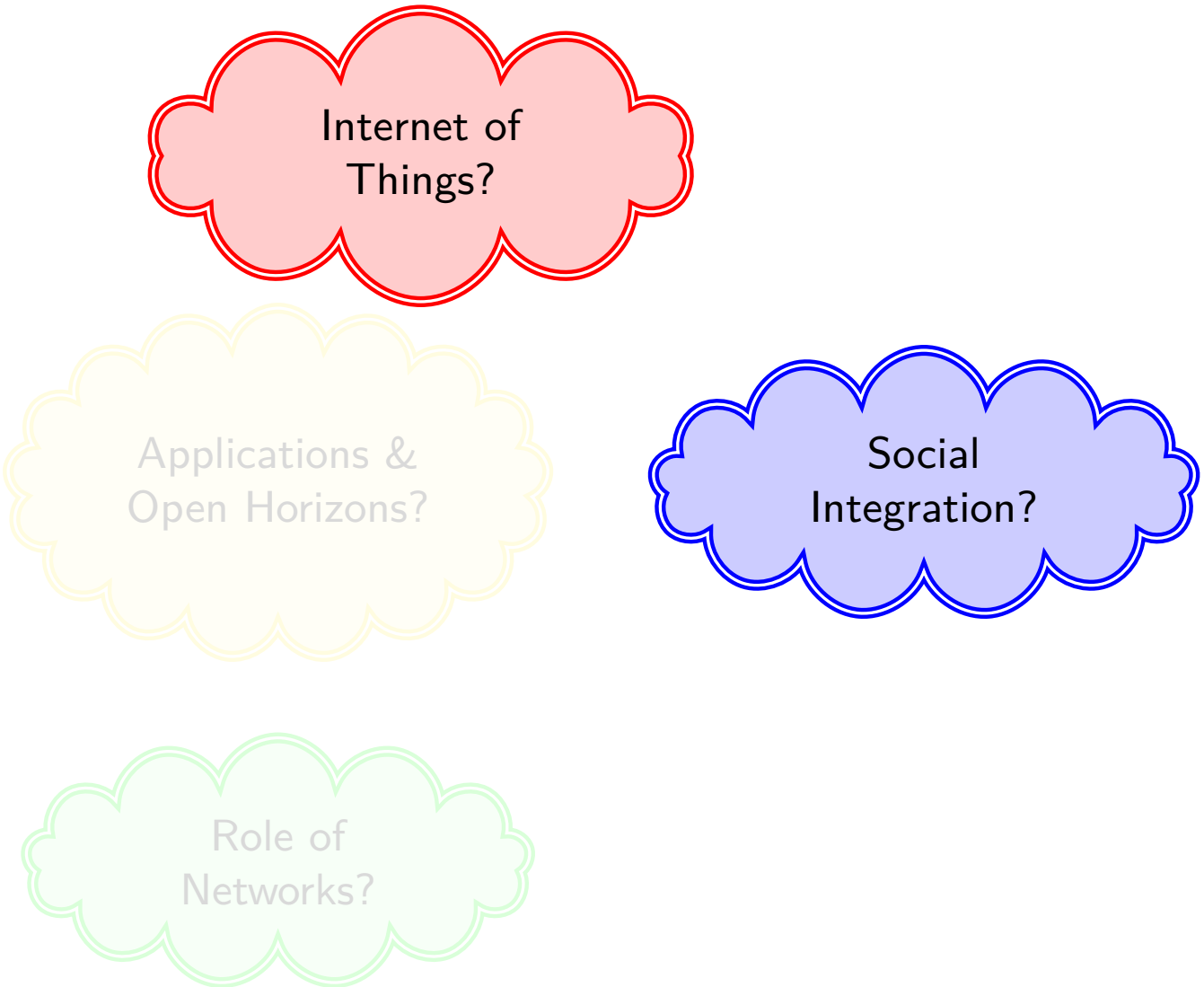

Towards Secure CPSs
Network Perturbations & Time-Delays
Efficient Coupling of Time-Scales
Applications
SS Operation Problems
Stability Control
SDP Formulations
Dynamic State Estimation
Observers
CKF
Tolerant to Attacks, UIs
Comparative Study
Robust Risk Mitigation
State Estimation
MILP
Fault Identification
Attacks & UI Estimation

Open Research Questions & Future Work

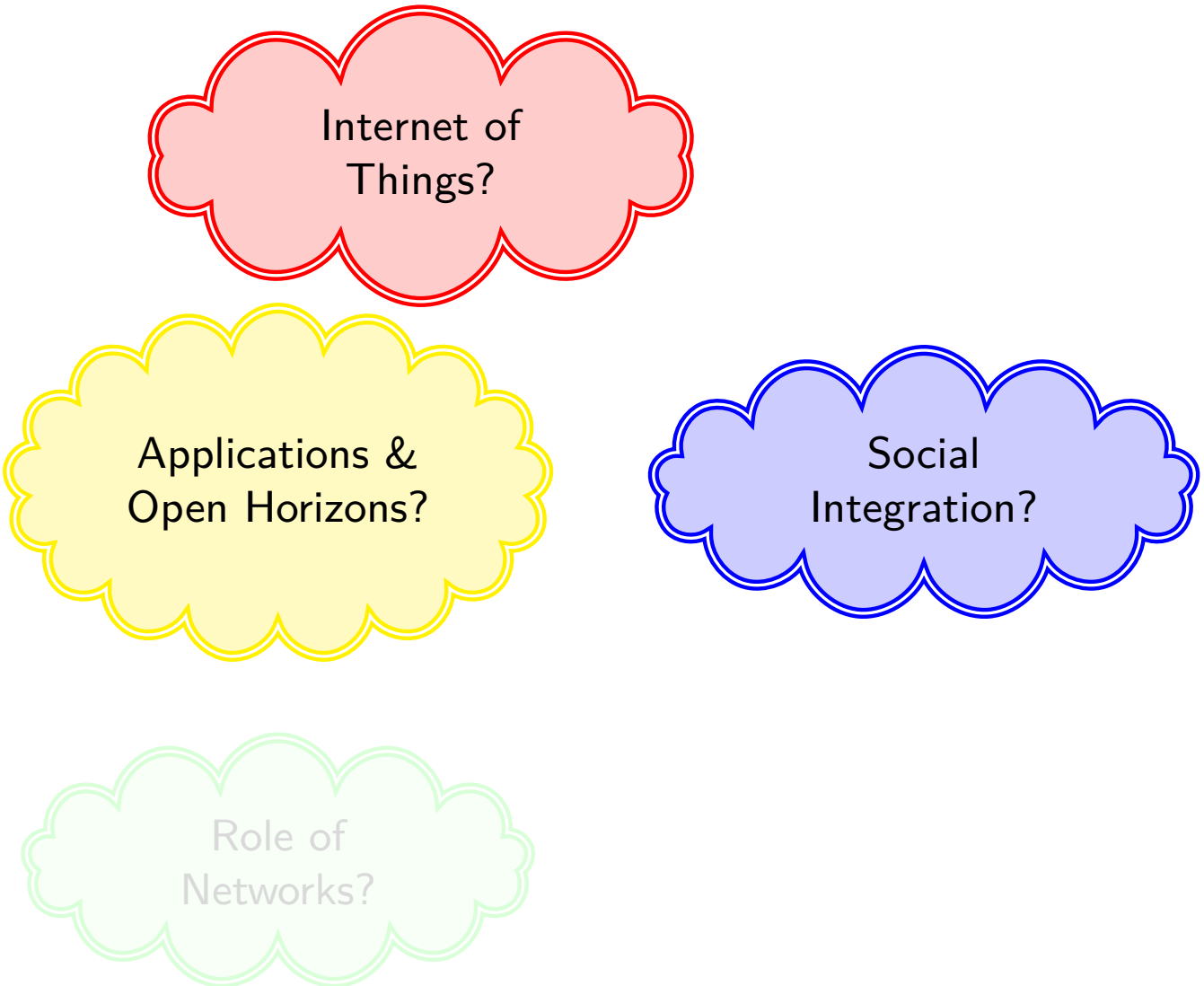
Open Research Questions & Future Work



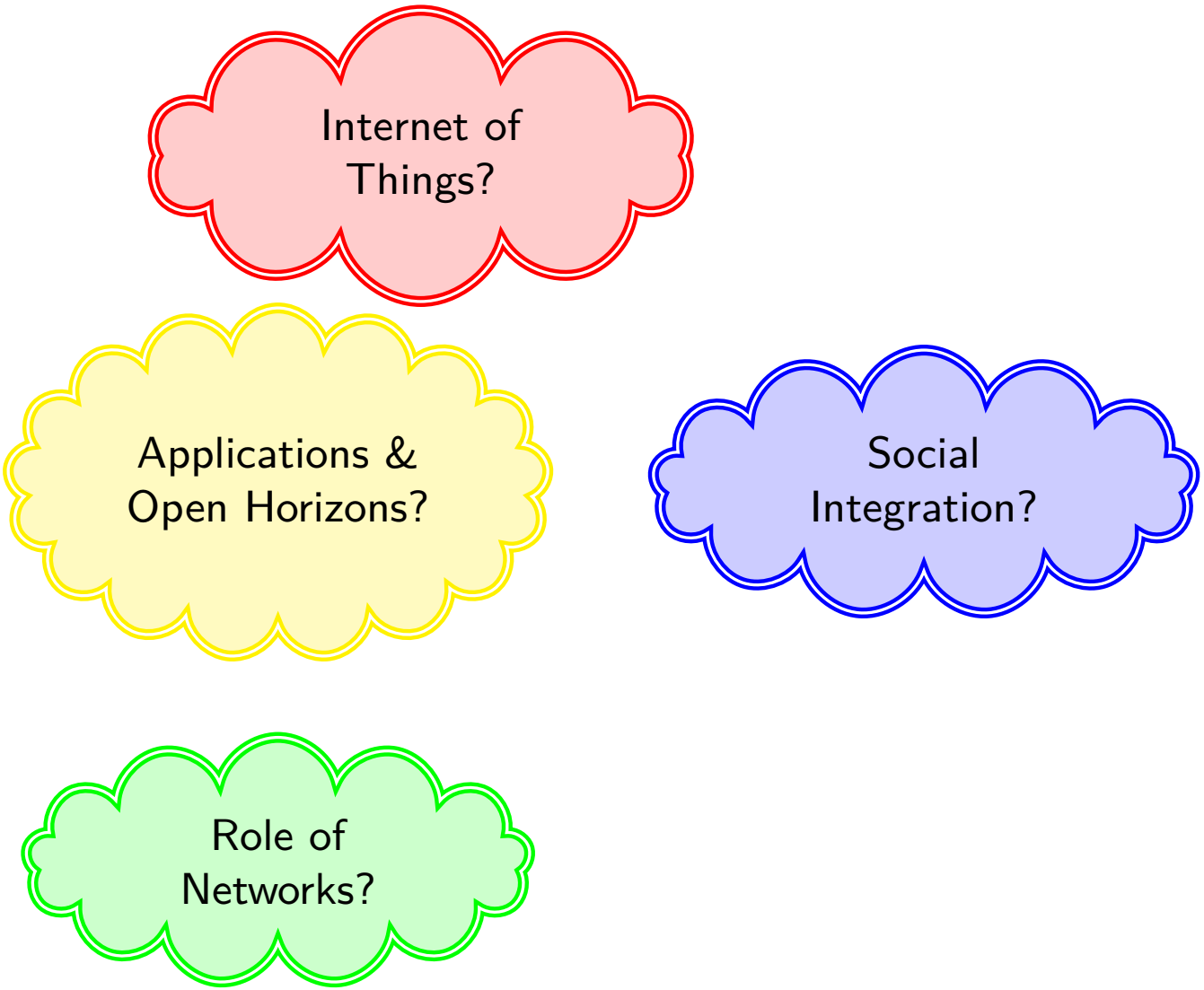
Open Research Questions & Future Work



Open Research Questions & Future Work



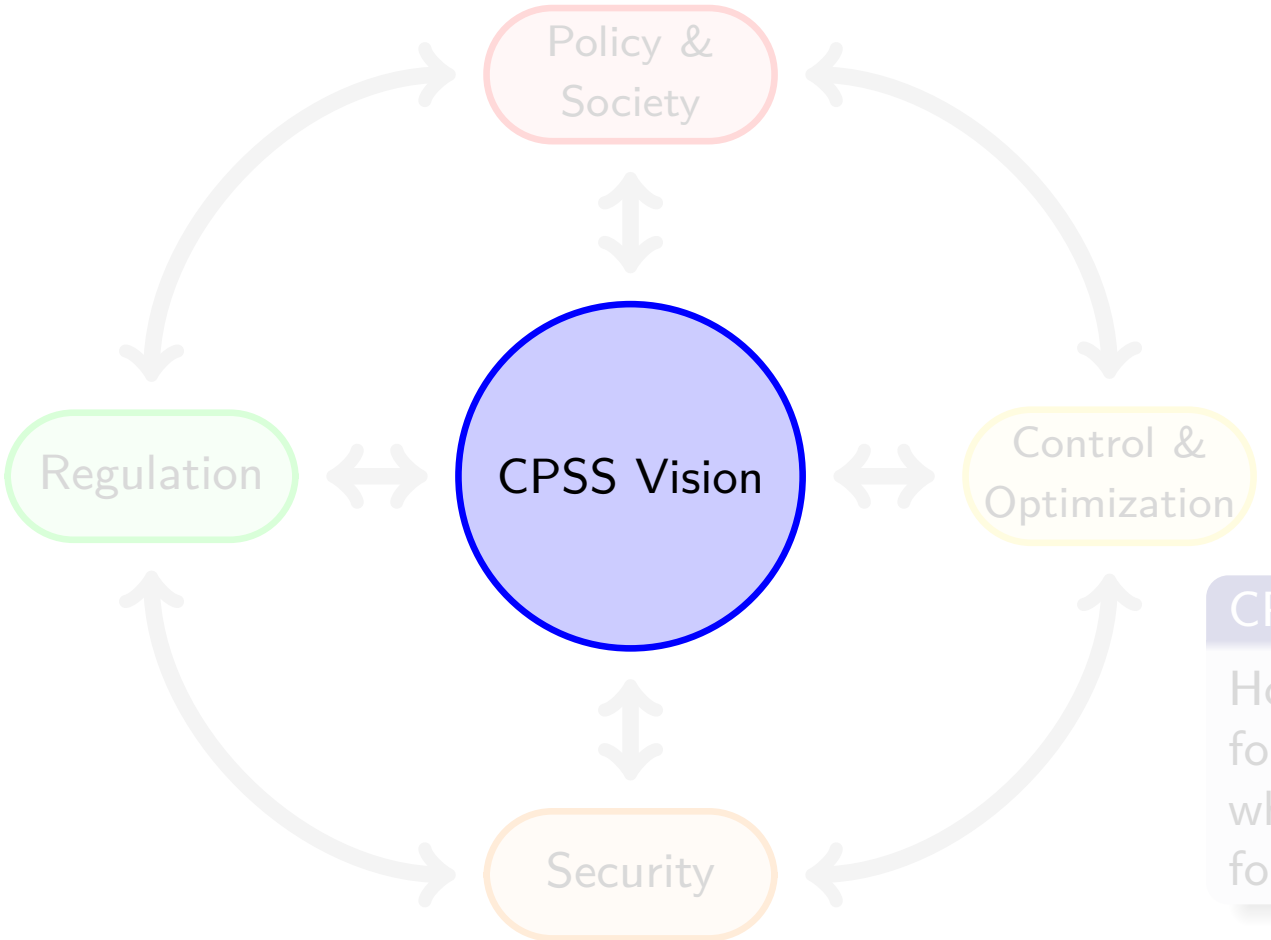
Open Research Questions & Future Work



Open Research Questions (2)

Cyber-Physical Social Systems (CPSS):

- Social & policy-decision making components in CPSs are often ignored
- $\Rightarrow$ Need to link physical, technology, & societal objectives [IEA, 2011]



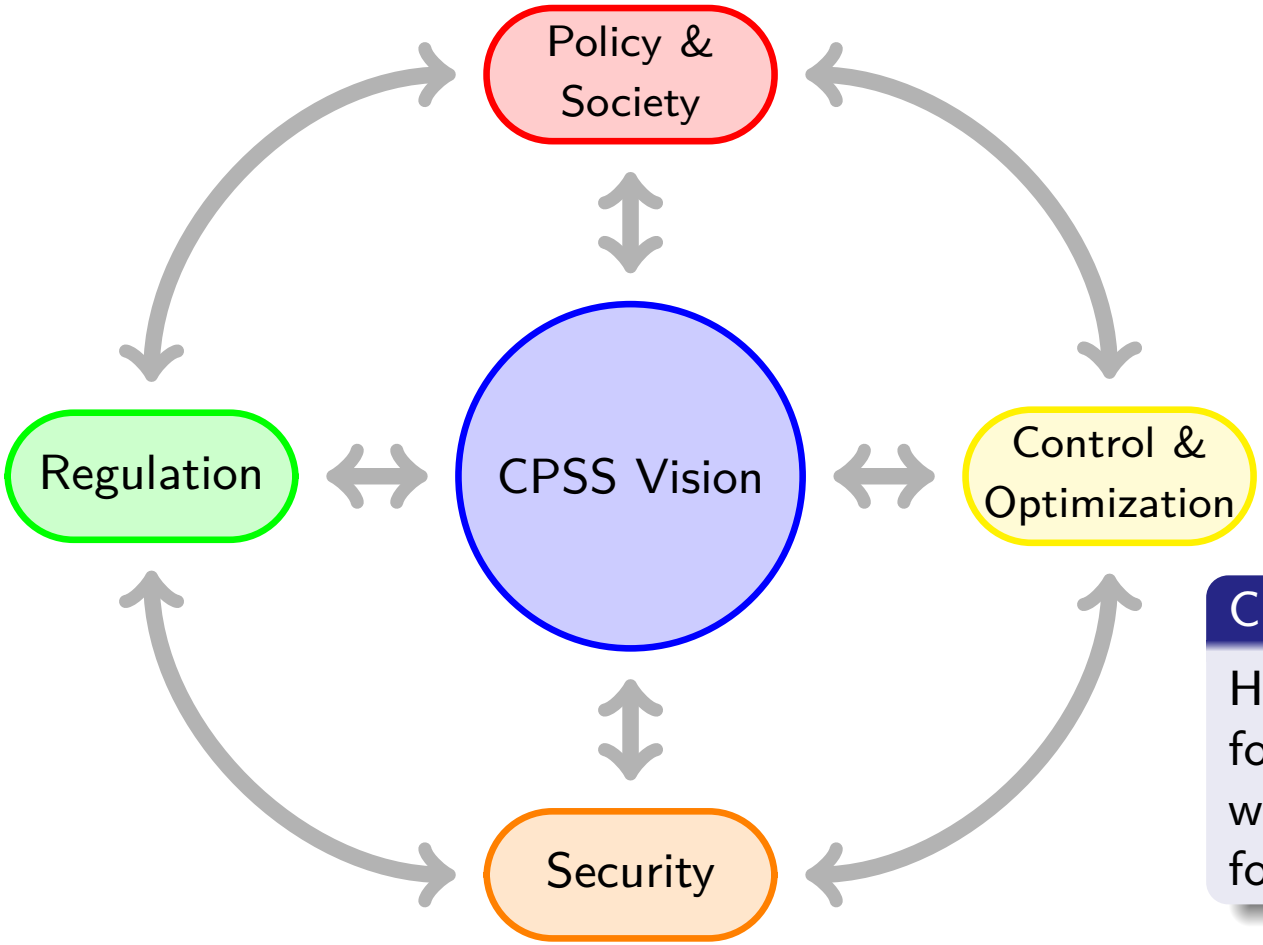
CPSS Research Question

How can we establish foundations for resilient CPSS while supporting policy design for economic incentives?

Open Research Questions (2)

Cyber-Physical Social Systems (CPSS):

- Social & policy-decision making components in CPSs are often ignored
- $\Rightarrow$ Need to link physical, technology, & societal objectives [IEA, 2011]



CPSS Research Question

How can we establish foundations for resilient CPSS while supporting policy design for economic incentives?

Questions And Suggestions?

Thank You!

Please visit

engineering.utsa.edu/~taha

IFF you want to know more ☺

References I

(2011). Smart grids, technology roadmap. Tech. rep., International Energy Agency.

Arasaratnam, I., & Haykin, S. (2009). Cubature kalman filters. *Automatic Control, IEEE Transactions on*, *54*(6), 1254–1269.

Chow, J. H., & Cheung, K. W. (1992). A toolbox for power system dynamics and control engineering education and research. *Power Systems, IEEE Transactions on*, *7*(4), 1559–1564.

DHS (2015). http://www.dhs.gov/office-infrastructure-protection.

EPRI (2014). Electric sector failure scenarios and impact analyses. Tech. rep., Electric Power Research Institute (EPRI).

Gallup (2005). http://www.gallup.com/poll/17881/electricity-retains-power-greatest-invention.aspx.

Ghahremani, E., & Kamwa, I. (2011). Dynamic state estimation in power system by applying the extended kalman filter with unknown inputs to phasor measurements. *IEEE Trans. Power Syst.*, *26*(4), 2556–2566.

Ghahremani, E., & Kamwa, I. (2015). Local and wide-area pmu-based decentralized dynamic state estimation in multi-machine power systems. *Power Systems, IEEE Transactions on*, *PP*(99), 1–1.

Jeschke, S. (2013). Cyber-physical systems — history, present and future.
URL http://www.ima-zlw-ifu.rwth-aachen.de/fileadmin/user_upload/INSTITUTSCLUSTER/Publikation_Medien/Vortraege/download//CPS_27Feb2013.pdf

Kalsi, K. (2010). *Decentralized observer-based control of uncertain dynamic systems*. Ph.D. thesis, Purdue University.

Pasqualetti, F., Dörfler, F., & Bullo, F. (2011). Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, (pp. 2195–2201).

Siljak, D., Stipanovic, D., & Zecevic, A. (2002). Robust decentralized turbine/governor control using linear matrix inequalities. *Power Systems, IEEE Transactions on*, *17*(3), 715–722.

Singh, A., & Pal, B. (2014). Decentralized dynamic state estimation in power systems using unscented transformation. *Power Systems, IEEE Transactions on*, *29*(2), 794–804.

Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, *100*(1), 210–224.

Teixeira, A., Sandberg, H., & Johansson, K. (2010). Networked control systems under cyber attacks with applications to power networks. In *American Control Conference (ACC), 2010*, (pp. 3690–3696).

Tripathy, P., Srivastava, S., & Singh, S. (2010). A divide-by-difference-filter based algorithm for estimation of generator rotor angle utilizing synchrophasor measurements. *Instrumentation and Measurement, IEEE Transactions on*, *59*(6), 1562–1570.

Wang, S., Gao, W., & Meliopoulos, A. (2012). An alternative method for power system dynamic state estimation based on unscented transform. *IEEE Trans. Power Syst.*, *27*(2), 942–950.

Zhang, W., Su, H., Wang, H., & Han, Z. (2012). Full-order and reduced-order observers for one-sided lipschitz nonlinear systems using riccati equations. *Communications in Nonlinear Science and Numerical Simulation*, *17*(12), 4968 – 4977.
URL http://www.sciencedirect.com/science/article/pii/S1007570412002584