



# State Estimation and Contingency Analysis of the Power Grid in a Cyber-Adversarial Environment

---

Robin Berthier<sup>1</sup>, Rakesh Bobba<sup>1</sup>, Matt Davis<sup>2</sup>,  
Kate Rogers<sup>2</sup>, and Saman Zonouz<sup>3</sup>

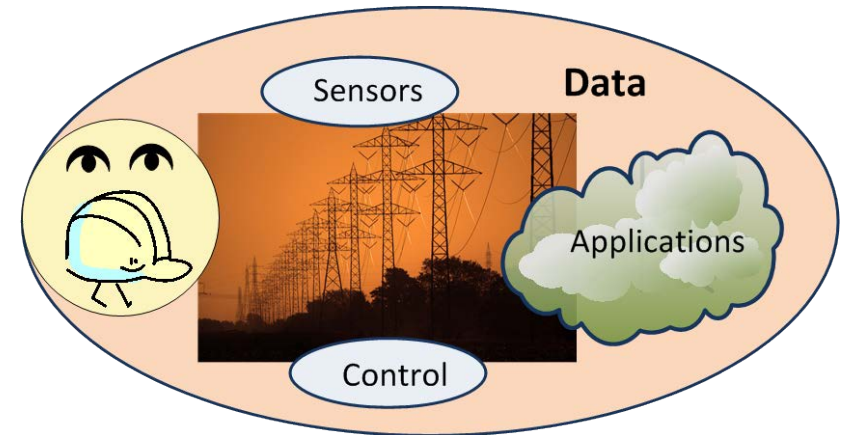
<sup>1</sup>Information Trust Institute  
University of Illinois at  
Urbana-Champaign  
Urbana, IL, USA  
*{rgb, rbobba}@illinois.edu*

<sup>2</sup>PowerWorld Corporation  
Champaign, IL, USA  
*{matt, kate}@powerworld.com*

<sup>3</sup>Department of Electrical  
and Computer Engineering  
University of Miami  
Miami, USA  
*s.zonouz@miami.edu*

# Motivation

- New technologies and new resources
- Extensive data integration
  - Sensory data
  - Control data
- Complex dependencies
- Stringent requirements



# Security vs. Dependability

- Dependability and fault tolerance
  - **Accidental** failures
  - *Second party is the (unintentional) nature*
    - *Future action set can (probabilistically) be predicted*
  - *Traditional probabilistic analysis/modeling*
  
- Security and intrusion tolerance
  - **Malicious** failures
  - *Second party are (intentional) attackers*
    - *If predicted, they can exploit the prior information to damage further*
  - New solutions are needed...

```
A problem has been detected and windows has been shut down to prevent damage to your computer.
DRIVER_IRQL_NOT_LESS_OR_EQUAL
If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:
Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.
If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use safe mode to remove or disable components, restart your computer. Press F8 to select Advanced startup options, and then select Safe Mode.
Technical information:
*** STOP: 0x000000D1 (0x0000000C,0x00000002,0x00000000,0xF86B5A89)
***
gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb
Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further assistance.
```

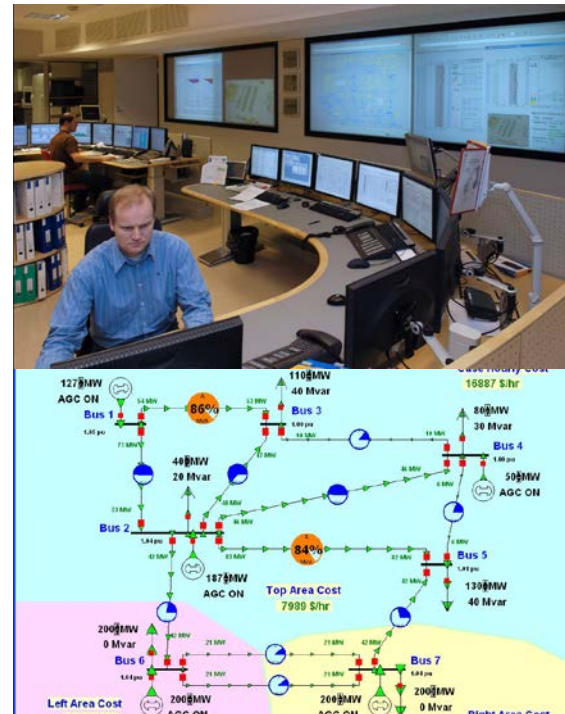


# Cyber-Physical System Security

- Systems in which cyber & physical systems are tightly integrated
  - Power systems
  - Process control networks
  - ...
- (Potentially) more catastrophic security incidents...



Targeting nuclear plants



Power Control Network



# Outline

---

- Power Grid Operation
  - Cyber-physical relationships
  - State estimation
- Cyber-Physical Threat Model
  - Step-1: Cyber network exploits
  - Step-2: Physical system-aware attacks
- Defense Solutions
  - Cyber network intrusion detection
  - System-aware detection and protection
    - Measurement protection and bad-data detection
  - System contingency analysis



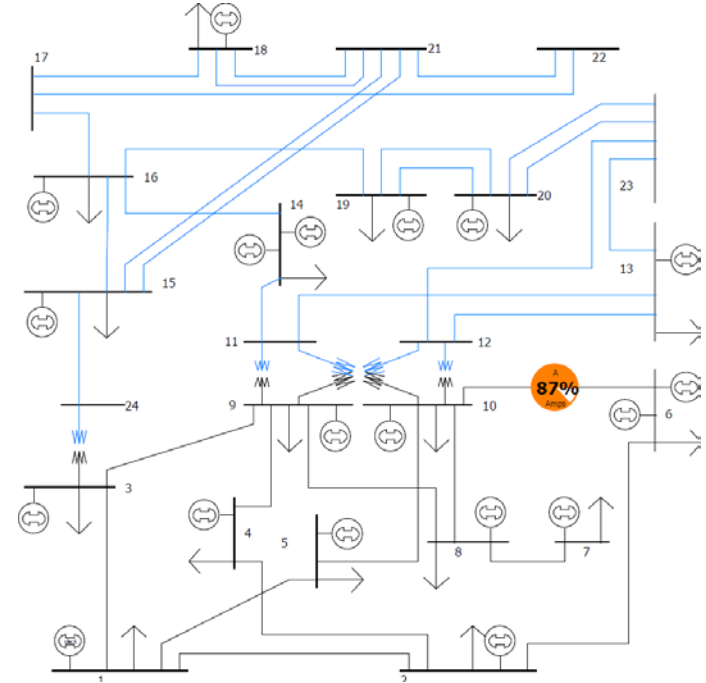
# Power Grid Operation

---

Cyber-physical relationships

# Power System Structure

- Major components:
  - Generators: produce electricity
  - Loads: consume electricity
  - Lines (T&D): transport energy from generators to loads
- Key Features
  - Absence of large-scale storage capabilities
  - Constraints: power balance, Kirchhoff's laws
  - Power flows through paths of “least resistance”
  - “Just-in-time” type manufacturing system





# Operation and Control

---

- *Economics* and *reliability* are the key drivers in power system operations and control
- Economics leads to large optimization problems for
  - Resource scheduling via unit commitment
  - Least-cost dispatch of available generation
- Reliability requirements typically entail no violations of physical limits and voltages and frequencies within prescribed bounds
  - Continuous monitoring
  - Hierarchical control architecture





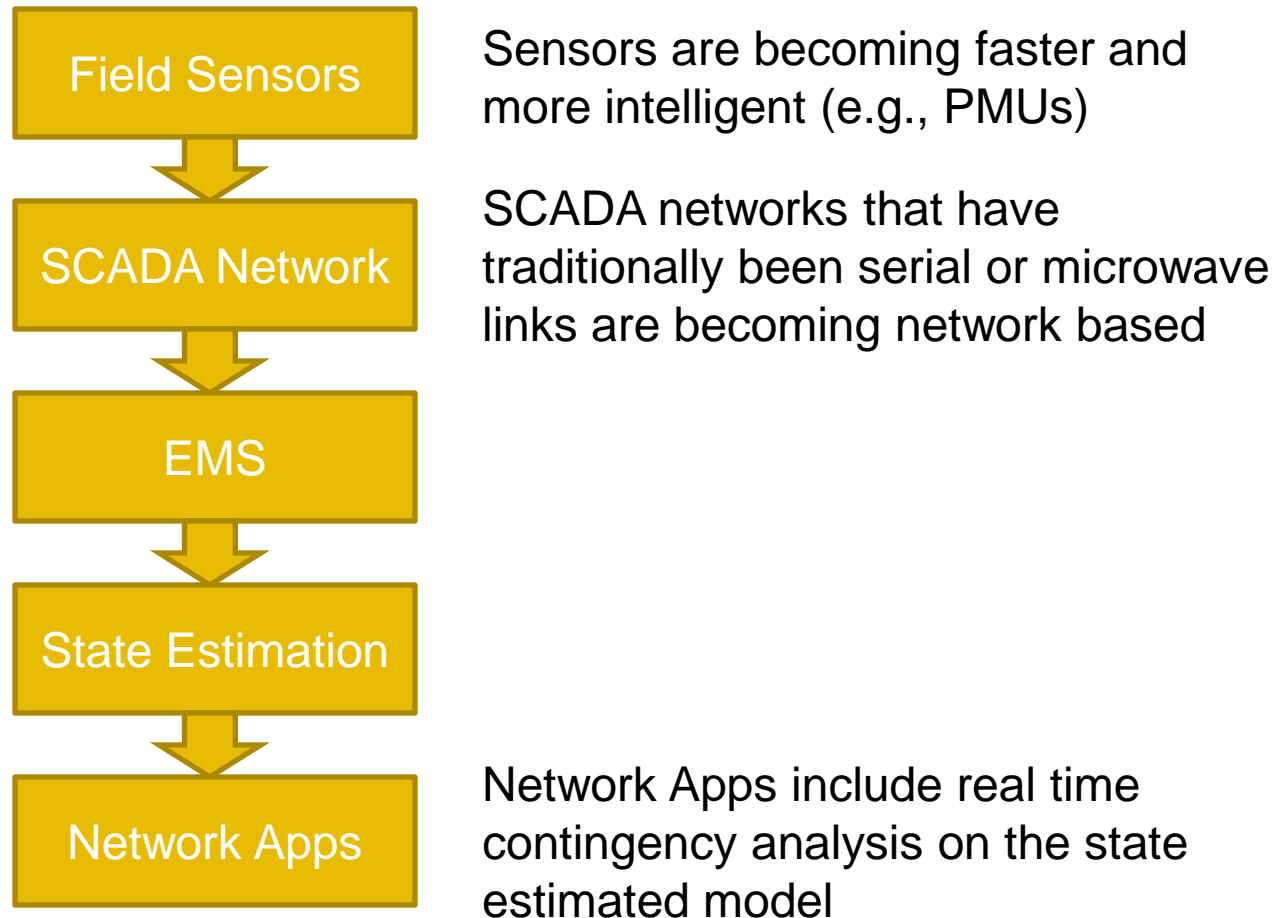
# Monitoring and Control

---

- Large and complex hardware-software systems are used for real-time operations and control
  - Energy management system (EMS)
  - Supervisory control and data acquisition (SCADA)
- Frequency is closely monitored and maintained around 60 Hz
  - Area control error (ACE) is measure for frequency excursions as well as deviations from scheduled interchanges – ideally, it should be *zero*
  - Automatic generation control (AGC) implements proportional-integral-derivative (PID) control to keep  $ACE = zero$

# Power System Operations

Data flow in power system operations



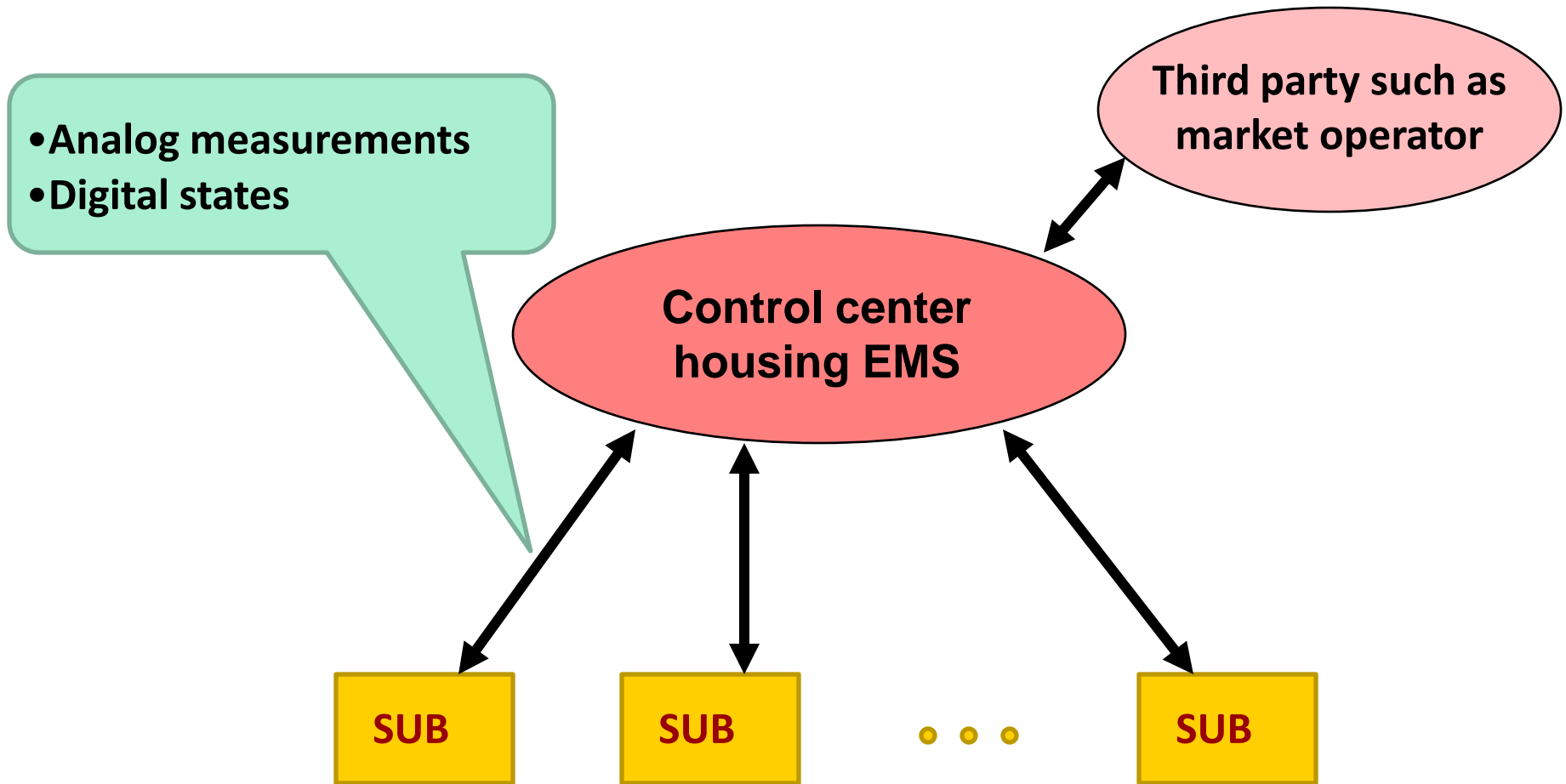


# Power Grid Operation

---

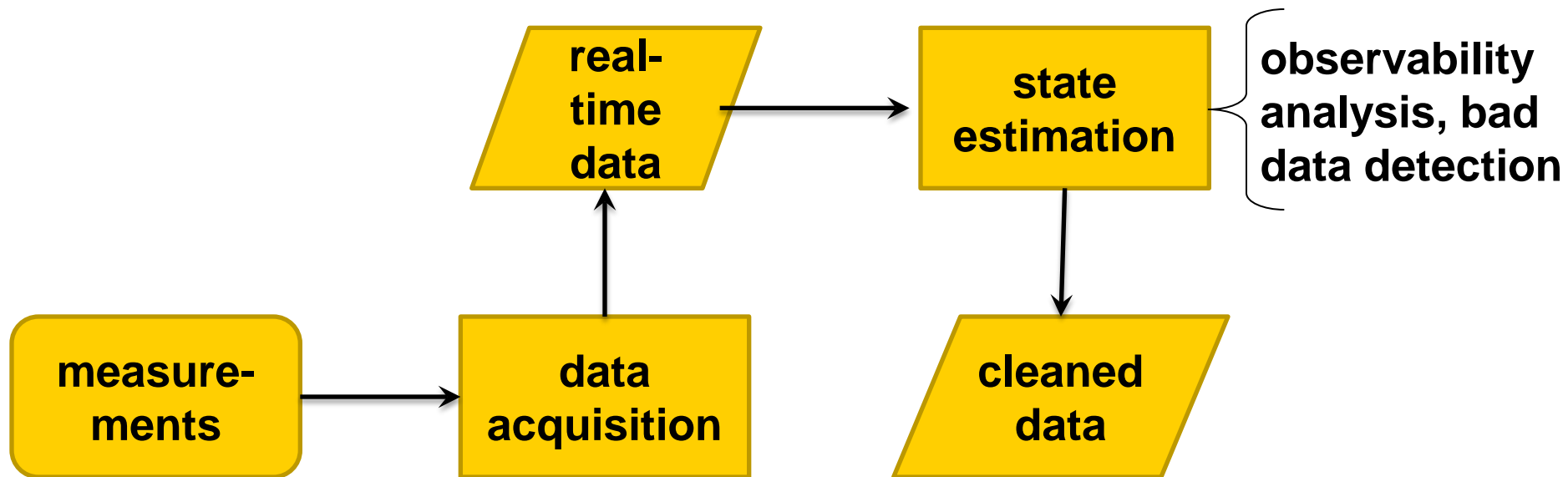
State Estimation

# Power Grid Observability



# State Estimation

- Key process in power system operation and control
- Problem statement: given certain measurements, find the *states* (voltages and angles) of the system





# State Estimation

- The power flow is the central tool of power system planners and operators

Inputs:

System topology  
Generation output  
Load values

Outputs:

Voltage magnitude and angle  
Line flows

$$P_{ij} = V_i^2[-G_{ij}] + V_i V_j [G_{ij} \cos(\theta_i - \theta_j) + B_{ij} \sin(\theta_i - \theta_j)]$$

$$Q_{ij} = V_i^2[-G_{ij}] + V_i V_j [G_{ij} \sin(\theta_i - \theta_j) + B_{ij} \cos(\theta_i - \theta_j)]$$

- Fundamentally, the power flow enforces the conservation of power at every Kirchoff's voltage law node in the system



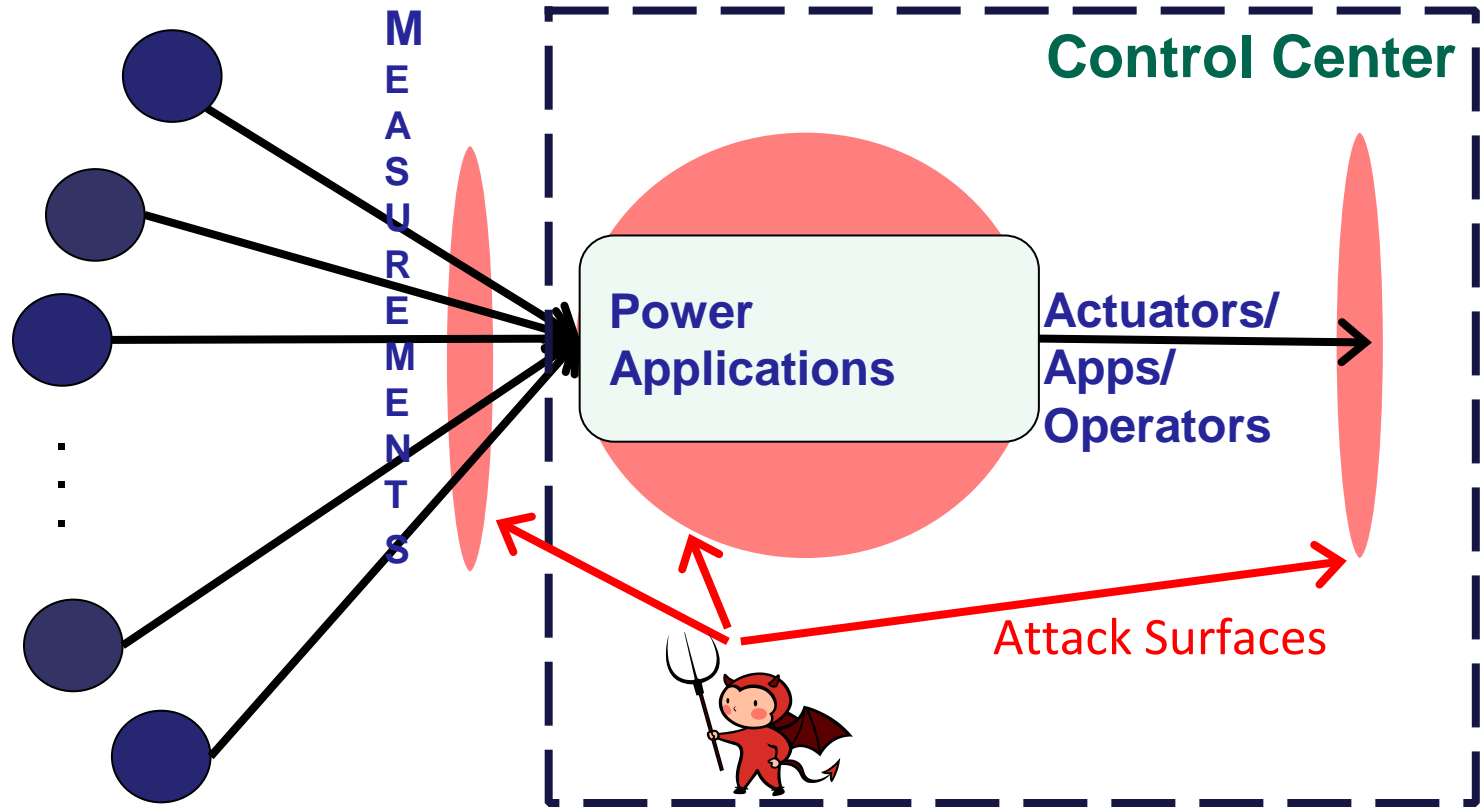
# Cyber-Physical Threat Model

---

Step-1: Cyber network exploits

Step-2: Physical system-aware attacks

# Cyber-Physical Threat





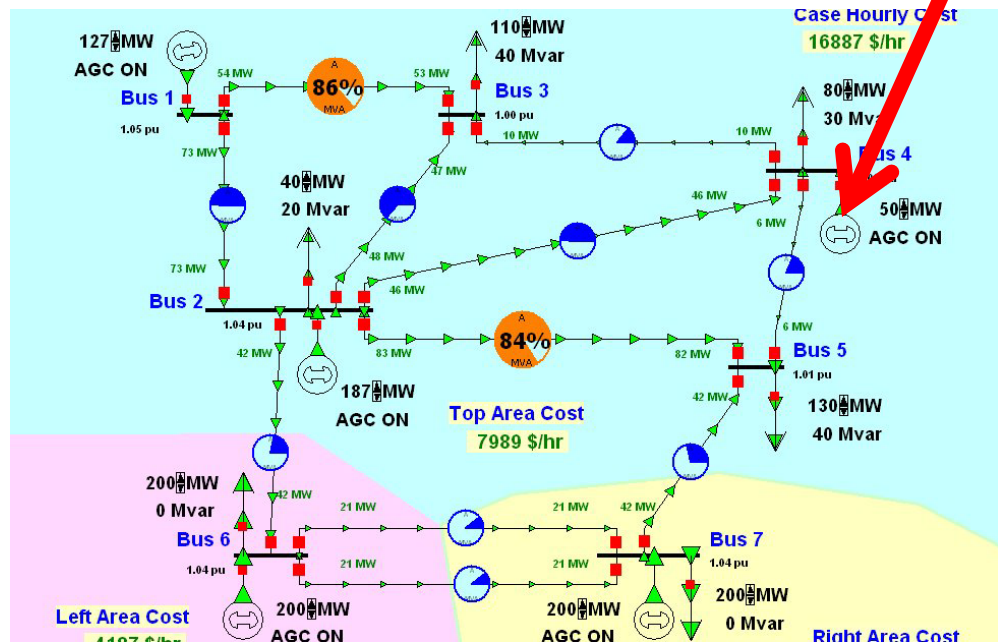
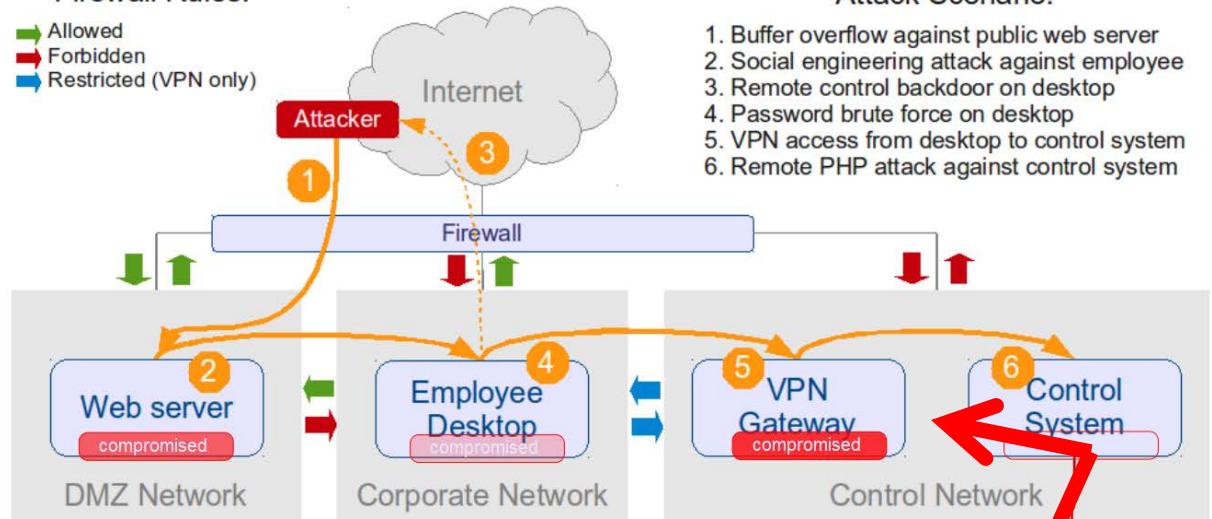
# Network Exploits

## Firewall Rules:

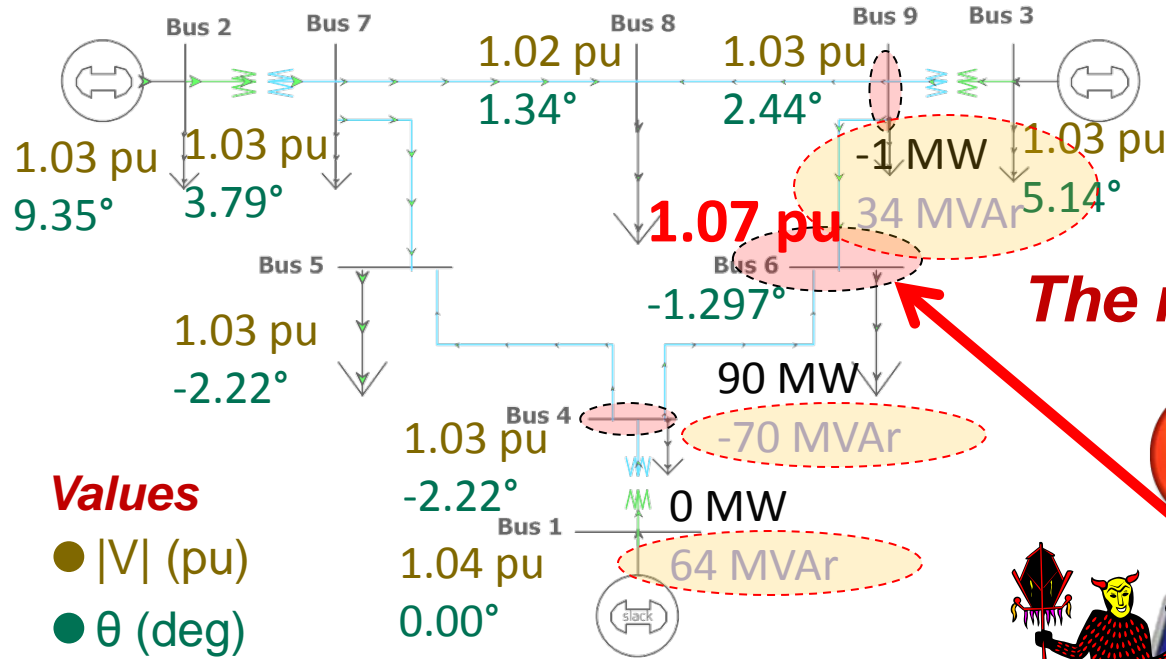
- ▶ Allowed
- ▶ Forbidden
- ▶ Restricted (VPN only)

## Attack Scenario:

1. Buffer overflow against public web server
2. Social engineering attack against employee
3. Remote control backdoor on desktop
4. Password brute force on desktop
5. VPN access from desktop to control system
6. Remote PHP attack against control system



# False Data Injection on State Estimation



## Values

- |V| (pu)
- θ (deg)
- P load (MW)
- Q load (MVar)

**Attack design:**  
Specifically chosen to satisfy the AC power flow solution equations

All states at non-malicious buses are preserved!





# Defense Solutions

---

Cyber Network Intrusion Detection

# Intrusion Detection Techniques

Legitimate Actions/Protocol Specification

Malicious Actions

## Anomaly-based

- + detect unknown attacks
- + high scalability
- no root cause
- high false positive rate

## Signature-based

- + low false positive rate
- + attack root cause
- require frequent update
- limited to known attacks

## Specification-based

- + detect unknown attacks
- + high accuracy
- poor scalability
- high development cost



# Specification-based Intrusion Detection

---

## ■ Opportunities:

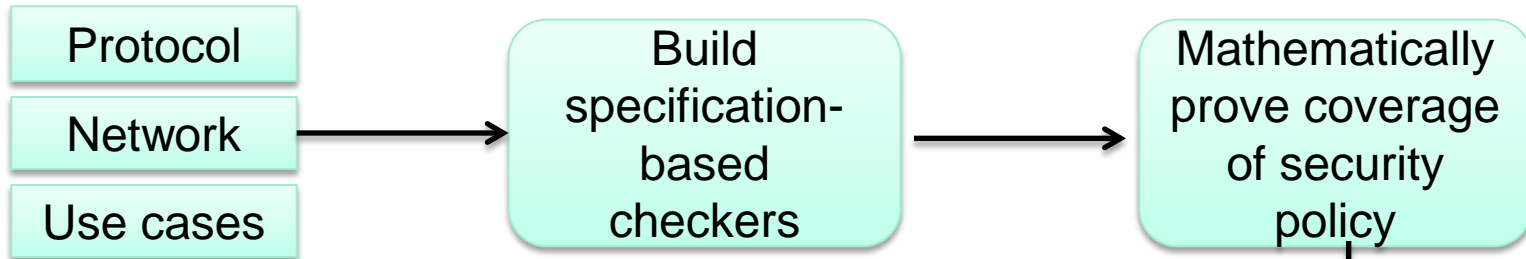
- Leverage tight control over communication protocols and system behavior
- Specification-based:
  - Little requirements about existing attacks
  - Ability to detect unknown attacks
  - No frequent update required
- Enable the use of mathematical proof (formal methods)

## ■ Challenges:

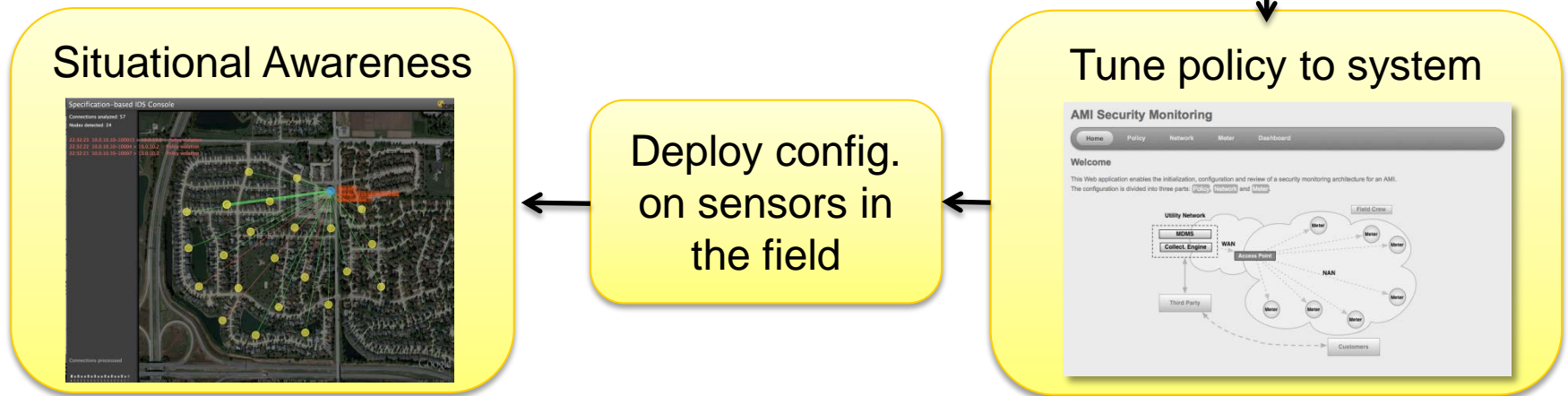
- Scalability: stateful protocol analysis is resource intensive
- Development costs: every protocol/application has to be specified

# Solution Overview\*

*Offline development process:*



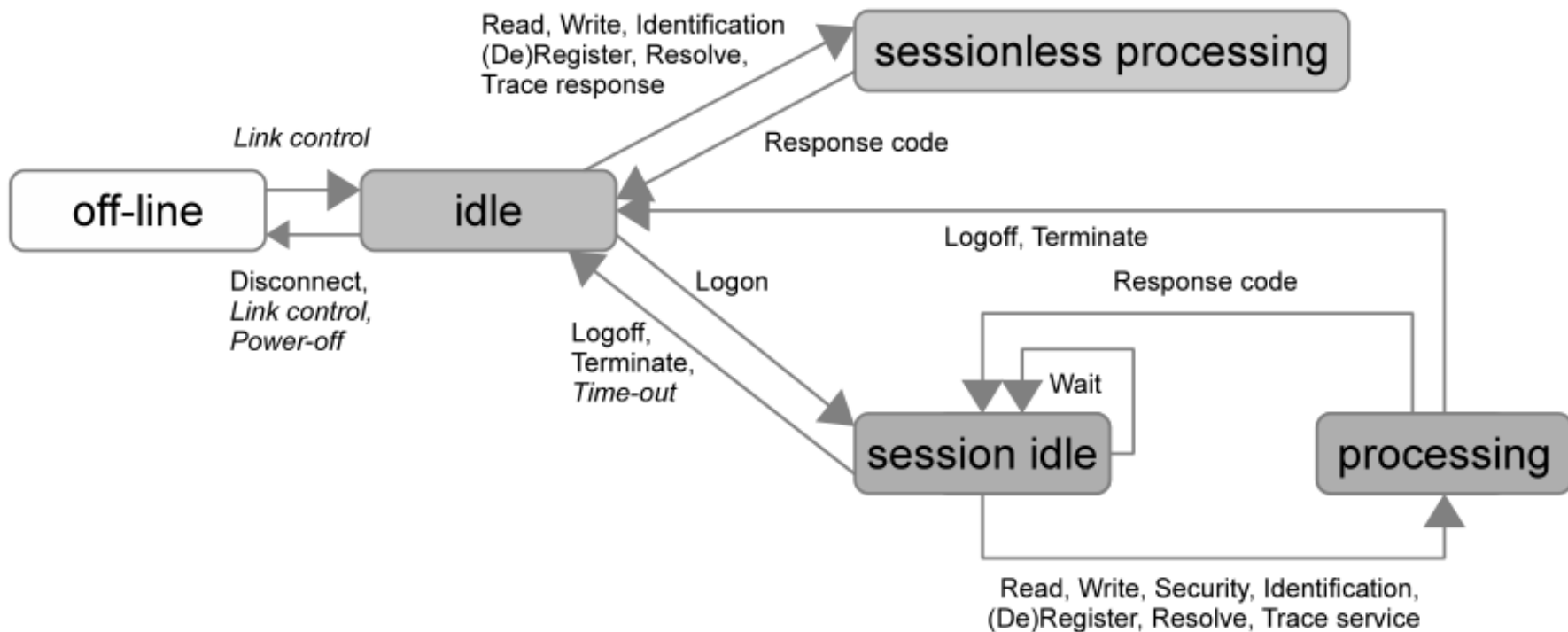
*Online operation process:*



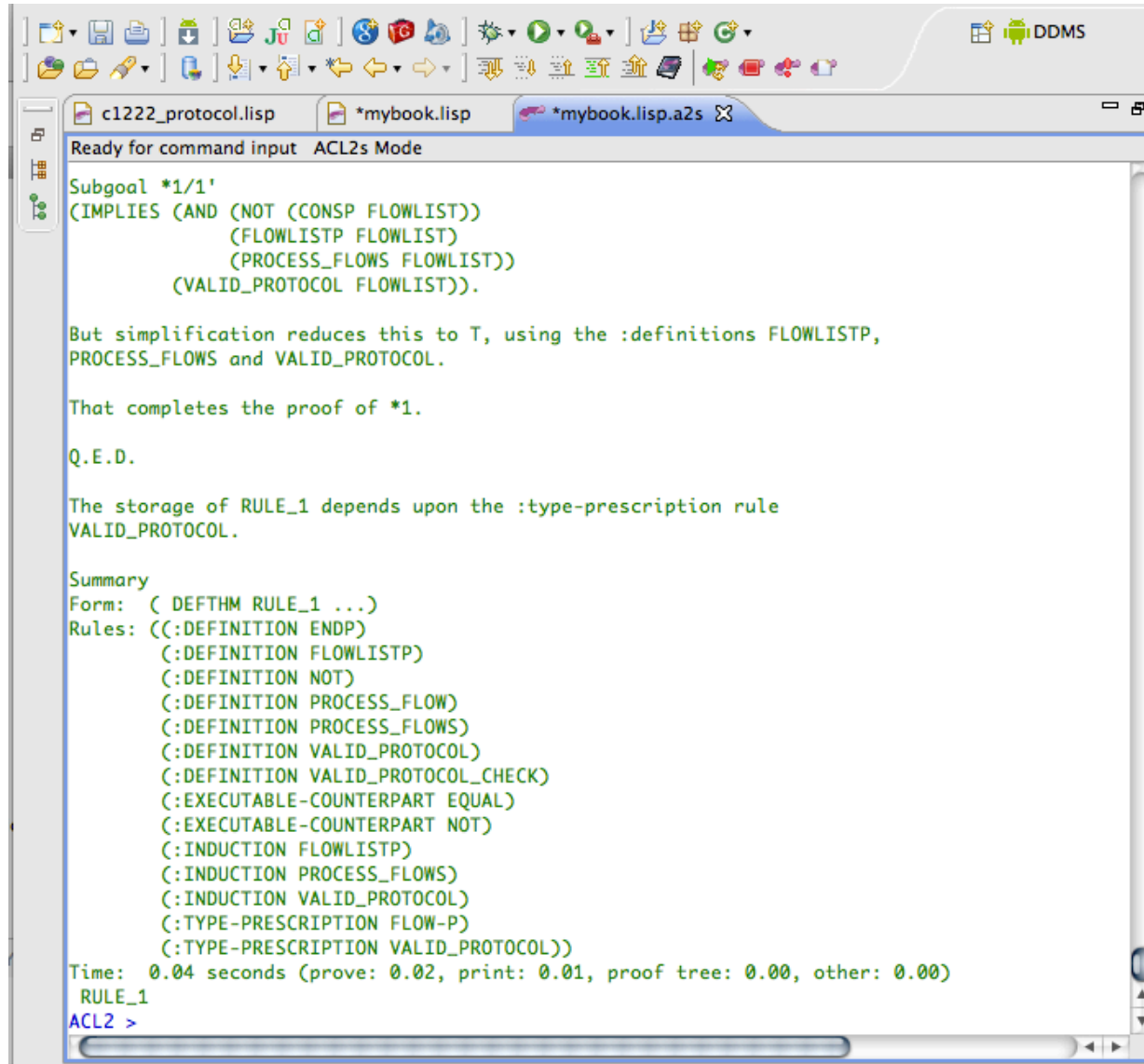
\*Robin Berthier, William Sanders: Specification-Based Intrusion Detection for Advanced Metering Infrastructures. PRDC 2011: 184-193

# Formal Verification of C12.22 protocol

- Validation through state machine:



# Formal Verification (cont.)



The screenshot shows the ACL2 theorem prover interface. The window title is "Ready for command input ACL2s Mode". The current subgoal is labeled "Subgoal \*1/1'". The goal expression is:

```
(IMPLIES (AND (NOT (CONSP FLOWLIST))
              (FLOWLISTP FLOWLIST)
              (PROCESS_FLOWS FLOWLIST))
         (VALID_PROTOCOL FLOWLIST)).
```

The output shows that the goal has been proven true (T) using the definitions FLOWLISTP, PROCESS\_FLOWS, and VALID\_PROTOCOL. The proof is completed, and the user is prompted with "Q.E.D.". A summary of the rules used in the proof is provided, including definitions for FLOWLIST, PROCESS\_FLOWS, and VALID\_PROTOCOL, and induction rules for FLOWLIST and PROCESS\_FLOWS. The time taken for the proof is 0.04 seconds.

```
Form: ( DEFTHM RULE_1 ...)
Rules: (:DEFINITION ENDP)
       (:DEFINITION FLOWLISTP)
       (:DEFINITION NOT)
       (:DEFINITION PROCESS_FLOW)
       (:DEFINITION PROCESS_FLOWS)
       (:DEFINITION VALID_PROTOCOL)
       (:DEFINITION VALID_PROTOCOL_CHECK)
       (:EXECUTABLE-COUNTERPART EQUAL)
       (:EXECUTABLE-COUNTERPART NOT)
       (:INDUCTION FLOWLISTP)
       (:INDUCTION PROCESS_FLOWS)
       (:INDUCTION VALID_PROTOCOL)
       (:TYPE-PRESCRIPTION FLOW-P)
       (:TYPE-PRESCRIPTION VALID_PROTOCOL))
Time: 0.04 seconds (prove: 0.02, print: 0.01, proof tree: 0.00, other: 0.00)
RULE_1
ACL2 >
```





# Attack Detection

- Violations at the network level

<i>Type</i>	<i>Feature</i>	<i>Extracted automatically</i>
Access	Origin/Dest.	From CE to meter
Data	Protocol	C12.22 over TCP/IP
Temporal	Frequency	1-2 per 1000 meters per day
Resource	Session size	< 100 bytes

- Violations at the application level

<i>Type</i>	<i>Feature</i>	<i>Extracted automatically</i>
Access	C12.19 tables	Table 0 (read), Table 3 (write)
Data	C12.19 values	Table 3, data: 0x01, offset: 0x00
Temporal	Session duration	< 1 minute
Resource	Services used	Logon, Full read, Partial write, Logoff



# Defense Solutions (cont.)

---

System-aware detection and protection

Power-System Measurement Protection  
and Bad-data Detection



# Current Bad Data Detection Solutions: Residual-Based Approaches

---

- Need to account for possibility of bad data
  - **Bad data** definition from (\*): “measurements that are grossly in error”
  - Bad data can potentially result in incorrect power-state estimates
- Measurement residuals – typical bad data detection for state estimation
  - if  $\|\underline{\mathbf{z}} - \mathbf{H}\underline{\mathbf{x}}\| \leq \tau$  no bad measurements*
- Goal of residual approaches: detect corrupted power measurements

\* A. Monticelli, State estimation in electric power systems: a generalized approach. Kluwer Academic Publishers, 1999.

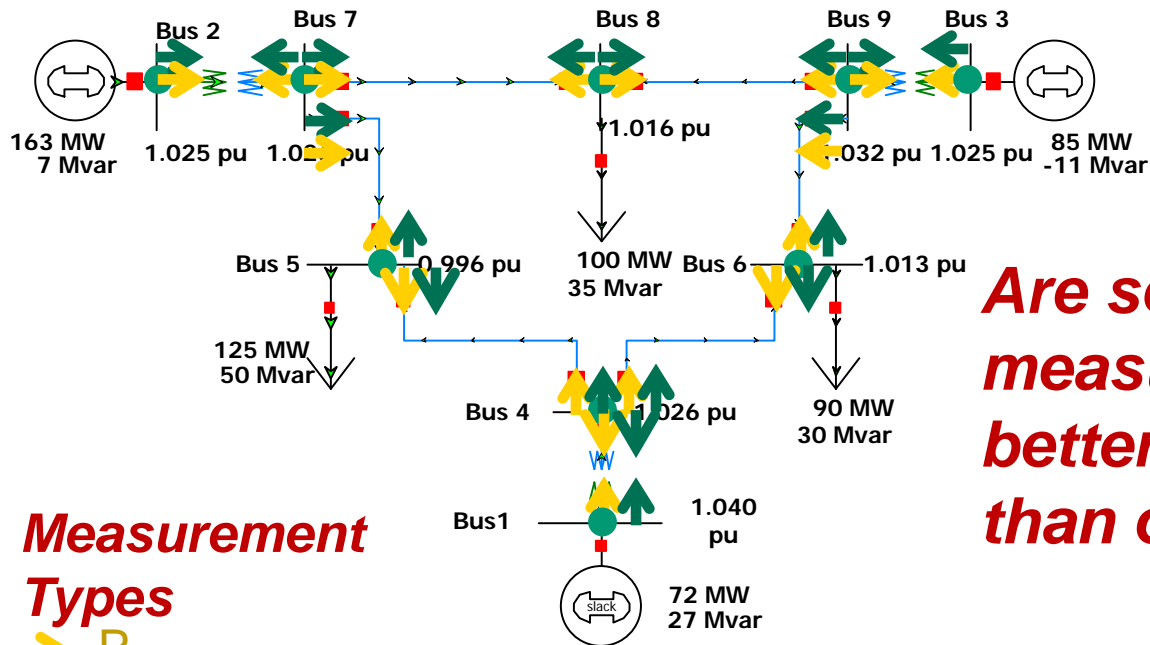


# Bad Data Detection: Residual -Based Approaches

---

- Coordinated attacks can work by creating “interacting bad-measurements” that satisfy the power flow solution equations, making them difficult or impossible to detect using conventional means
- ***Residual-based approaches may be fundamentally insufficient against coordinated security compromises***
- One obvious approach:
  - Protect all measurements from compromises




# System-Aware Measurement Protection



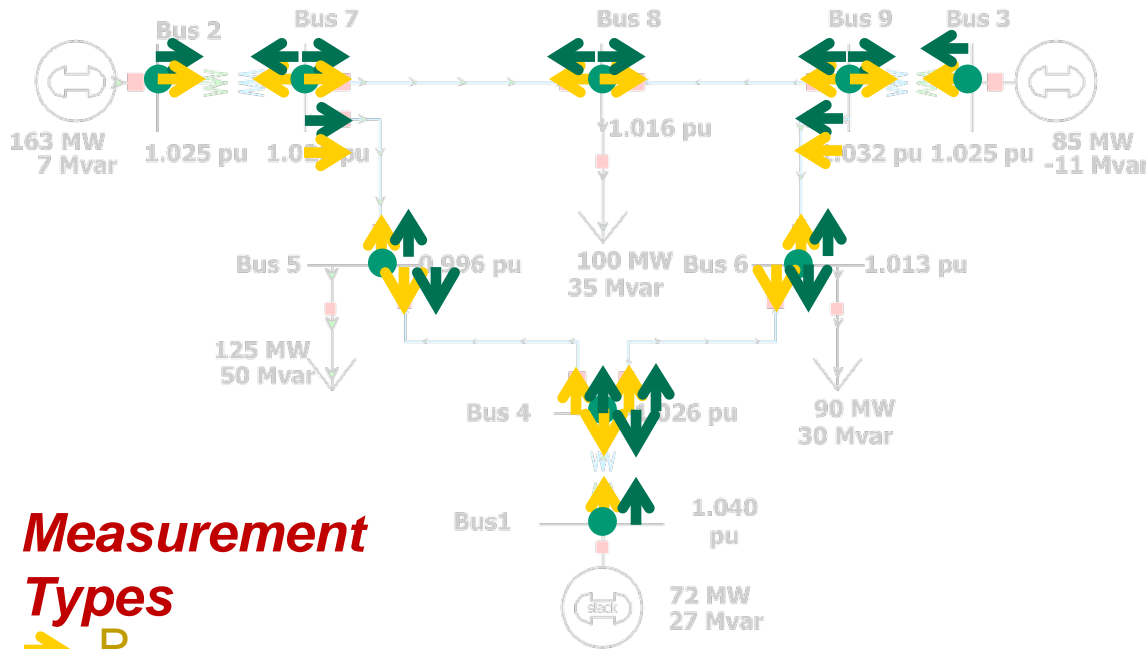
*Are some measurements better to protect than others?*

## Measurement

### Types

-   $P_{i,j}$
-   $Q_{i,j}$
-   $V_i$

# System-Aware Measurement Protection



Example: Basic Measurements

	i	j
$P_{ij}$	4	1
$P_{ij}$	2	7
$P_{ij}$	9	3
$P_{ij}$	5	4
$P_{ij}$	6	4
$P_{ij}$	7	5
$P_{ij}$	7	8
$P_{ij}$	8	9
$Q_{ij}$	4	1
$Q_{ij}$	8	9
$Q_{ij}$	7	2
$Q_{ij}$	3	9
$Q_{ij}$	4	5
$Q_{ij}$	4	6
$Q_{ij}$	5	7
$Q_{ij}$	8	7

## Measurement

### Types

→  $P_{i,j}$

→  $Q_{i,j}$

●  $V_i$

We show that no attacks are possible if  $H'_k$  has full rank

$$\begin{bmatrix} \mathbf{0} \\ \mathbf{a}_k \end{bmatrix} = \begin{bmatrix} \mathbf{H}'' & \mathbf{H}'_k \\ \mathbf{H}_k' & \mathbf{H}_{kk} \end{bmatrix} \begin{bmatrix} \mathbf{0} \\ \mathbf{c}_k \end{bmatrix}$$

$$\mathbf{0} = \mathbf{H}'_k \mathbf{c}_k$$

$$\mathbf{a}_k = \mathbf{H}_{kk} \mathbf{c}_k$$

Accomplished by protecting *basic measurements*



# Cost-Optimal Measurement Protection

- Protect a set of *Basic Measurements*<sup>\*</sup>
  - it is **necessary** but **not sufficient** to protect  $n$  measurements, to detect stealthy false data injection attacks
  - it is **necessary** and **sufficient** to protect a set of **basic measurements (BM)** to detect stealthy false data injection attacks
  - approaches to identify **BM** already exist and well-studied
  - choices are available – the set of **BM** is not unique
  - each verifiable state variable (e.g., PMU) reduces number of measurements to be protected by one
  - approach validated on the IEEE 9,14,30,118, and 300 bus test systems

<sup>\*</sup>R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, T. J. Overbye, “Detecting False Data Injection Attacks on DC State Estimation,” *First Workshop on Secure Control Systems (SCS 2010)*, April 2010.



# Defense Solutions (cont.)

---

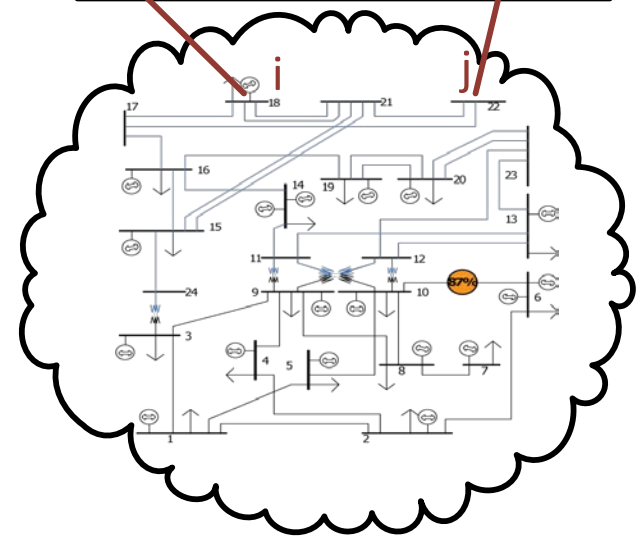
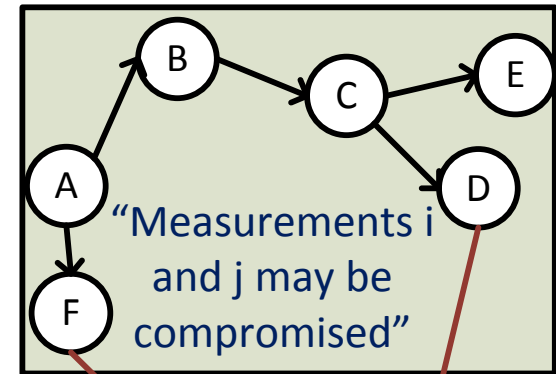
Integrated Cyber-Physical State Estimation



# Cyber-Physical State Estimation (CPSE)\*

- Co-utilize information from **cyber** and **power** network to (more precisely) determine the **state** of the **cyber-physical** system
- Use combined **information state** to provide a scalable approach to detecting bad data caused by a cyber event

Example



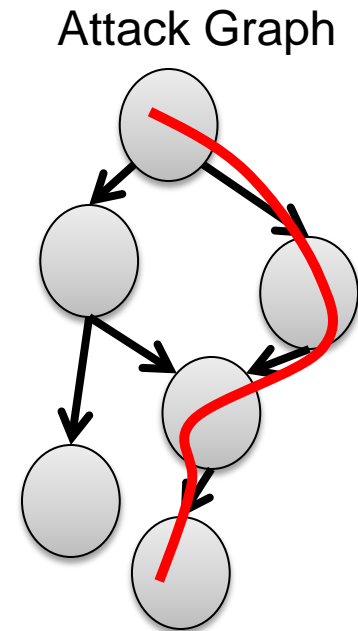
\*S. A. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, T. J. Overbye, “CPIDS: A Cyber-Physical Intrusion Detection System for Power-Grid Critical Infrastructures,” in review for *IEEE Transactions on Smart Grid*.

# Algorithm Step 1: Potentially-bad Data Identification

- From IDS reports, we (probabilistically) know attacker's current privileges  
→ From power network's topology, we know which measurements could/might have been modified by the adversary

- Example:

- network's topology
  - $i$ -th measurement (by  $PMU_i$ ): real power of the bus B2
- IDS alerts
  - $PMU_i$  is compromised  
→  $i$ -th measurement might have been corrupted!



## Algorithm Step 2:

# Power State Estimation & Verification

- Throw the potentially-bad data away, and run a power state estimation using the remaining power measurements

$$P_{ij} = V_i^2[-G_{ij}] + V_i V_j [G_{ij} \cos(\theta_i - \theta_j) + B_{ij} \sin(\theta_i - \theta_j)]$$

$$Q_{ij} = V_i^2[-G_{ij}] + V_i V_j [G_{ij} \sin(\theta_i - \theta_j) + B_{ij} \cos(\theta_i - \theta_j)]$$

- Compute  $\|z - \mathbf{H}(\hat{\mathbf{x}})\|$ , and identify the corrupted measurements
  - based on how much they differ from their estimates



# CPSE Benefits

---

- Improved Bad-data Detection
  - Accuracy and Scalability
- Quick State Estimation Convergence
- Improved State Estimates



# Defense Solutions (cont.)

---

System Contingency Analysis



# Contingency Analysis (CA)

---

- Contingency analysis is a fundamental tool of power systems analysis
- Typically, a contingency analysis works with a power system model (power flow case) to determine potential problems
  - Full topology (node breaker) vs. planning models (bus branch)
- Answers the question: “*What happens when X goes out of service?*”

# Contingency Analysis Results

Contingency Analysis

Contingencies Options Results

Records Set Columns f(x) Options

Label	Skip	Processed	Solved	Post-CTG AUX	Islanded Load	Islanded Gen	QV Autoplot?	Violations	Max Branch %	Min Volt	Max Volt
2 L_000007Seven-000003FiveC1	NO	YES	YES	none			NO	1	149.4		
3 L_000002Two-000006SixC1	NO	YES	YES	none			NO	1	113.5		
4 L_000002Two-000003ThreeC1	NO	YES	YES	none			NO	1	103.8		
5 L_000002Two-000005FiveC1	NO	YES	YES	none			NO	0			
6 L_000003Three-000004FourC1	NO	YES	YES	none			NO				
7 L_000004Four-000005FiveC1	NO	YES	YES	none			NO				
8 L_000002Two-000004FourC1	NO	YES	YES	none			NO	0			
9 L_000006Six-000007SevenC1	NO	YES	YES	none			NO	0			
10 L_000006Six-000007SevenC2	NO	YES	YES	none			NO	0			

List of contingencies

Violation summary

Violations

Show related contingencies Combined Tables >

	Value	Limit	Percent	Area Name Assoc.	Nom kV Assoc.
1	406.19	271.94	149.37	Top-Top	138.0

Violations caused by contingency

Contingency Definition

Actions	
1	BRANCH 1 2 1 OPEN

What happens during contingency

Status Finished with 3 Violations and 0 Unsolveable Contingencies. Initial State Restored.  Refresh Displays After Each Contingency

Load Auto Insert Save Other > Start Run Close ? Help



# CA in Power System Operations

---

- State estimator runs every 2min or so
- After getting the state estimate real time contingency analysis (RTCA) runs on the estimated model
  - The list of contingencies must be picked carefully before being added to the RTCA contingency list
  - The RTCA list needs to include important contingencies, but it is time constrained





# CA Solution Methods

---

- There are several ways of solving the contingency analysis
  - Full AC power flow (Slowest, Most accurate)
  - DC power flow (Fast, no voltage/var information)
  - Linear sensitivities (Fast, less sensitive to topology)
- There is the traditional engineering tradeoff between accuracy and speed
- All solution methods are used in practice



# CA Solution Details

---

- Modeling a contingency accurately can be an intricate process
- The devil is in the details
- A few of the things that must be accounted for
  - Voltage controller and phase shifter response
  - AGC response
  - Special protection schemes / Breaker actions
  - Contingency modeling (full topology vs planning model)
- There is a lot that happens when a contingency is solved or even solving a power flow case

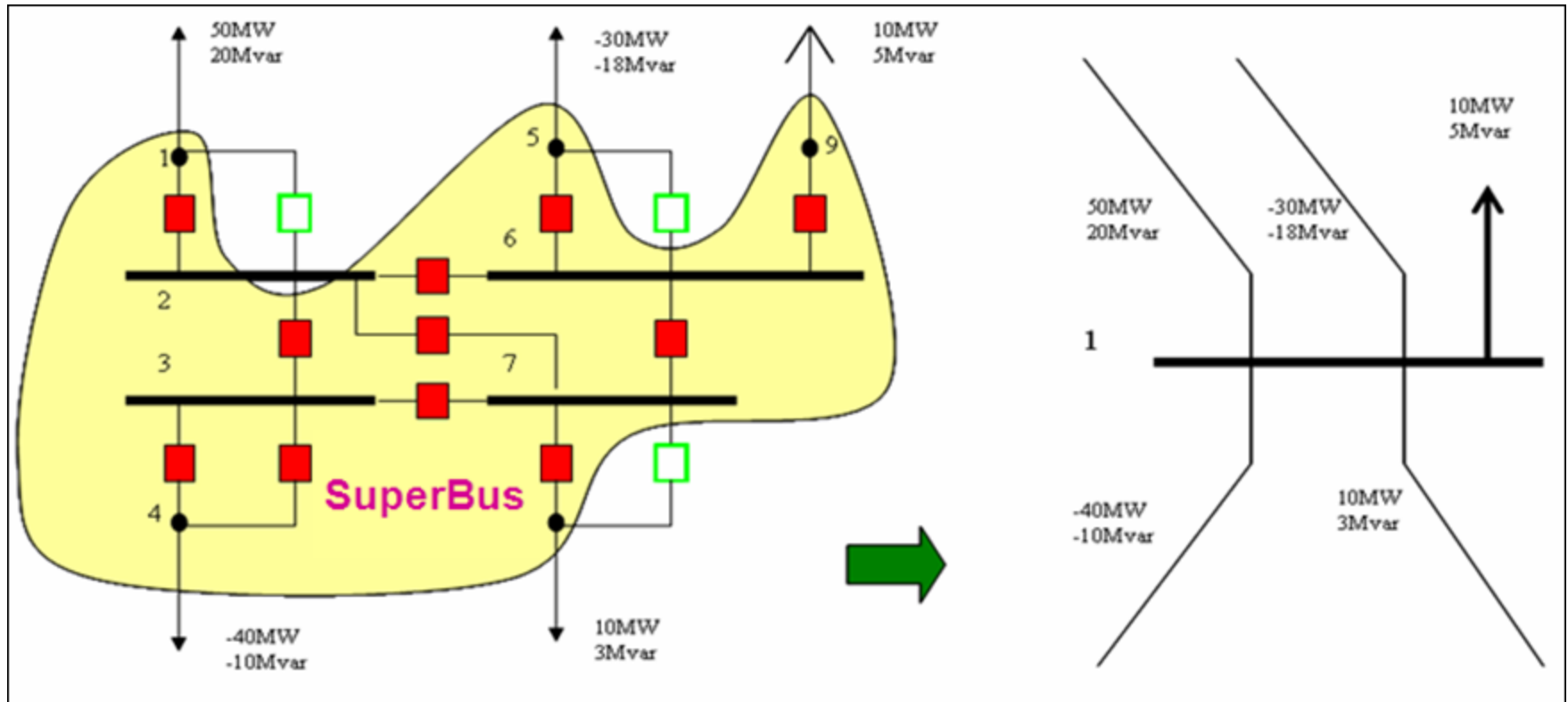
# EMS and Planning Models

## EMS Model

- Used for real-time operations
- Call this *Full-Topology* model
- Has node/breaker detail

## Planning Model

- Used for off-line analysis
- We call this *Consolidated* model





# Traditional Contingency Analysis (CA)

---

- The “N-1” criteria is used to operate the system so that there will be no violations when any one element is taken offline
- Future requirements are strengthening the security criteria (“N-1-1”) meaning many more contingencies need to be solved\*
  - Once multiple outages begin to be considered, the size of the contingency list can grow very large
  - For 1000 lines
    - N-1 means solving 1000 line outages
    - N-2 means solving 499500 line outages (1000 choose 2)



# Proposed System Contingency Analysis

---

- Question: “*What happens when X goes out of service?*”
  - X could be either a critical power component or cyber asset.
- Unlike traditional scenarios, cyber asset outages may be due to cyber adversaries
- Ongoing Research Topic!



# Conclusions

---

- Criticality of cyber-physical infrastructure security:
  - Complex relationship between cyber and physical components
  - Importance of accurate state estimation → target of interest for adversaries:
    - Step-1: Cyber network exploits
    - Step-2: Physical system-aware attacks
- Requirements for advanced defense solutions:
  - Specification-based network intrusion detection tailored for cyber-physical system characteristics
  - System-aware measurement protection and bad-data detection
  - System-wide contingency analysis
- Contingency analysis as potential solution for a unified cyber-physical state estimation



# Questions?

---

Robin Berthier

[rgb@illinois.edu](mailto:rgb@illinois.edu)

Saman Zonouz

[s.zonouz@miami.edu](mailto:s.zonouz@miami.edu)