Smart Energy Grids and Cyber Security

André Teixeira
Department of Engineering Systems and Services
Faculty of Technology, Policy, and Management
TU Delft

Joint work with Kaveh Paridari (KTH), Henrik Sandberg (KTH), Karl H. Johansson (KTH),
Kin C. Sou (Chalmers), Iman Shames (U. Melbourne)

Motivation

- Northeast blackout Aug 14, 2003: 55 million people affected
- Software bug in energy management system stalled alarms in state estimator for over an hour
- Cyber-attacks against the power network control systems may result in similar consequences and pose a substantial threat

Is this a "real" concern?

Motivation

Getting quite real…

- First **known** hacker-caused outage
  - Dec 23rd, 2015
- Malware infected 3 regional operators in Ukraine
- Substations were disconnected, resulting in blackouts
- Malware "BlackEnergy" with "KillDisk" component

Ars Technica has arrived in Europe. **Check it out!**

RISK ASSESSMENT / SECURITY & HACKTIVISM

First known hacker-caused power outage signals troubling escalation

Highly destructive malware creates "destructive events" at 3 Ukrainian substations.

by **Dan Goodin** - Jan 4, 2016 9:36pm CET

Share Tweet Email 110

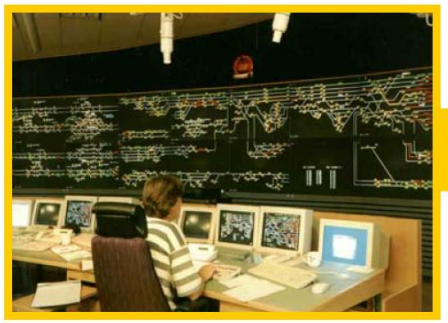
Krzysztof Lasoń

Highly destructive malware that infected at least three regional power authorities in Ukraine led to a power failure that left hundreds of thousands of homes without electricity last week, researchers said.

http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

From cybersecurity vulnerabilities to societal costs

Attack



SCADA system

Power network

Societal cost

Security issues

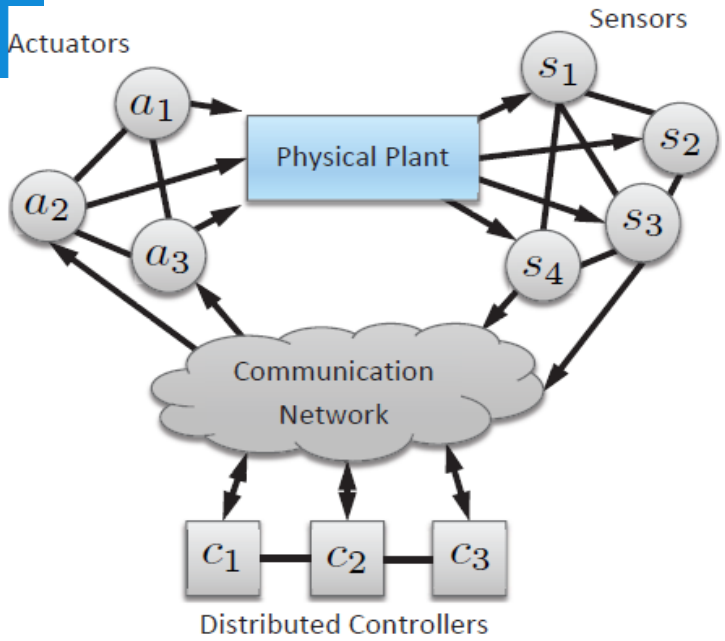
Power system: susceptible to operational errors and external attacks

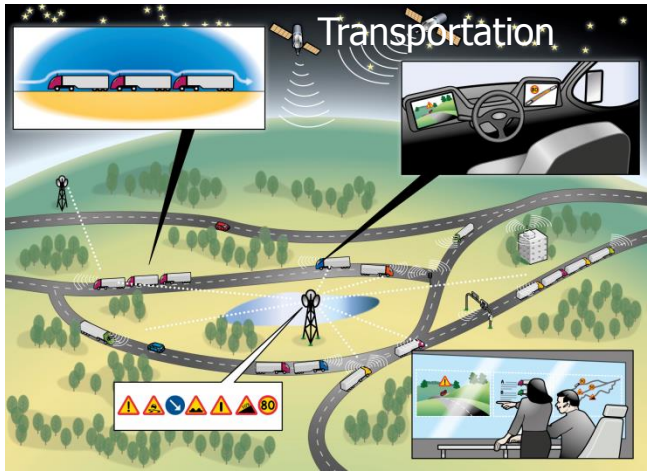
Smart grid technology makes the system even more vulnerable

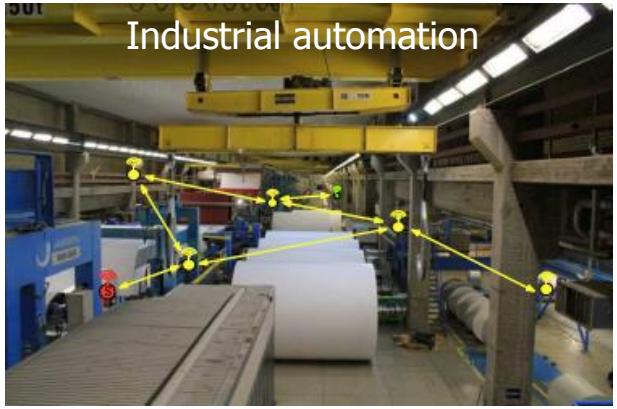
André Teixeira – Research Background

- 2009: Electrical engineer from the University of Porto, Portugal
- 2014: Ph.D. in Automatic Control at KTH Royal Institute of Technology, Stockholm, Sweden
  - "Cyber-Secure and Resilient Networked Control Systems".
  - **Networked Control System:** use digital data (exchanged through ICT infrastructures) to steer and monitor the behavior of physical processes
    - E.g.: autonomous cars, power plants, *power distribution systems*, *flood management systems…*
  - Cybersecurity concerns:
    - What if the **digital data is corrupted**/hacked? How can it be detected?
    - How does the **control algorithm react**? How is the **physical process affected**? How can it be **detected** and **mitigated**?
  - For more details: see my personal web page
- Oct. 2015: Assistant Prof. at TPM in the field of Cybersecurity of Critical Infrastructures

Networked Control Systems





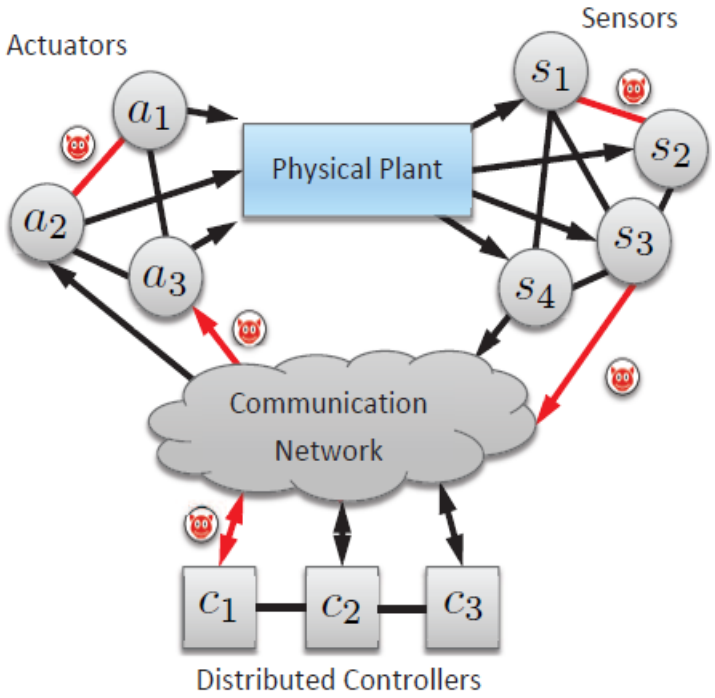


Cyber-Secure and Resilient Networked Control Systems

Networked control systems are to a growing extent based on **open communication and software technology**

- **E.g.: Legacy Energy Systems → Smart Energy Systems**

- Leads to **increased vulnerability** to cyber-threats with many potential points of attacks
- Cyber-attacks can have dramatic physical impact



- How to model adversaries and attacks?
- How to measure vulnerability?
- How to compute consequences?
- How to design protection and detection mechanisms?

- Related to:
  - **Modeling frameworks**
  - **Risk Management**
  - **Anomaly detection**

Outline

- Motivation and Research Background
- **The Concept of Risk**
  - **Impact metrics for Energy Systems**
  - Likelihood Metrics for Energy Systems
- Scenarios and Risk metrics for Smart Grids
  - Scenario 1: False-Data injection on Transmission Grids
  - Scenario 2: Voltage control under adversarial actions
- Summary
- Future Challenges and Opportunities
- References

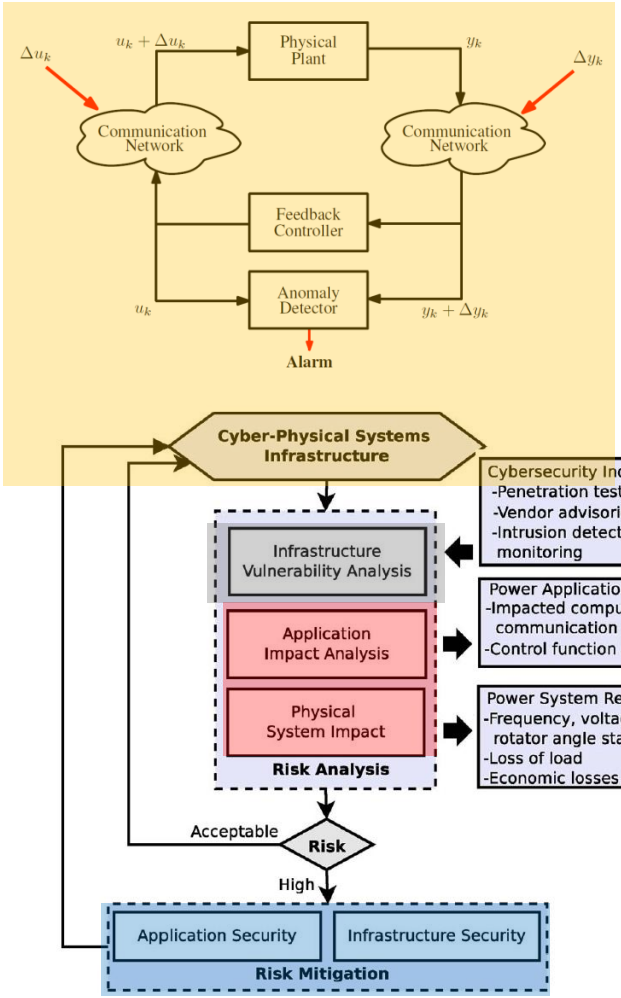
The Concept of Risk

- [Kaplan & Garrick, 1981] **Risk** is a set of tuples:
  - Attack **Scenario**
  - **Impact** of the attack
  - **Likelihood** of the attack

- How to model adversaries and attacks?
  - *Describe the system*
  - *Characterize the attack **scenario***

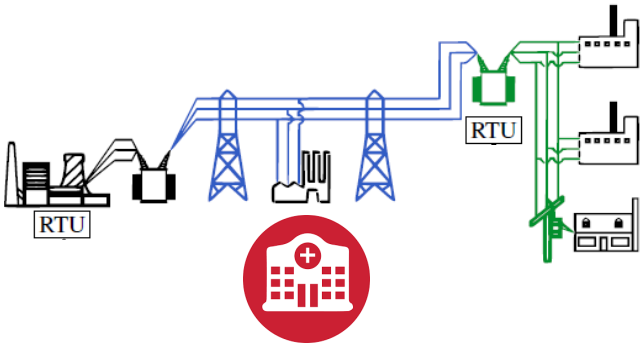
- How to measure vulnerability?
  - *Assess **likelihood** of attack (or a proxy)*
    - *Attack effort*
    - *Amount of resources (knowledge, corrupted channels)*

- How to compute consequences?
  - *Assess **impact** on performance objectives*
    - *Loss of performance*
    - *Loss of stability*
    - *Loss of desired properties*
    - *Violation of safety constraints*



[Sridhar *et al.*, Proc. IEEE, 2012]

Impact Metrics for Energy Systems



- **Operation Goals:**
- No blackouts (ideal)
- No blackouts in **critical loads**
- Efficiency
- Quality of power supply
  - Voltage @ 230V
  - Frequency @ 50Hz

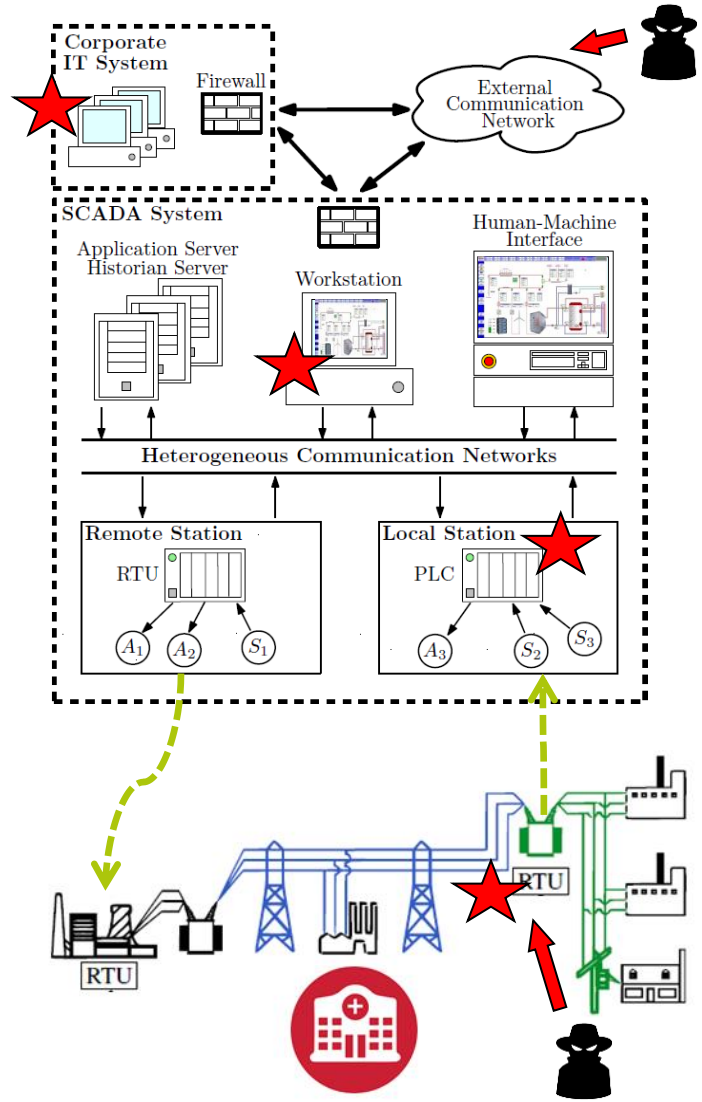
- **Impact Metrics:**
- Loss of load
- Loss of **critical load**
- Increase of costs
- Reduced quality of power supply
  - Maximum voltage variation
  - Maximum frequency variation
- Loss of stability / desired properties

Likelihood Metrics for Energy Systems

- Likelihood depends on ICT infrastructure

- **Successful attack:**
  - Successful initial infection
  - Sucessful dissemination of malware
  - **Sucessful infection of target devices**
  - **Sucessful control of target devices**

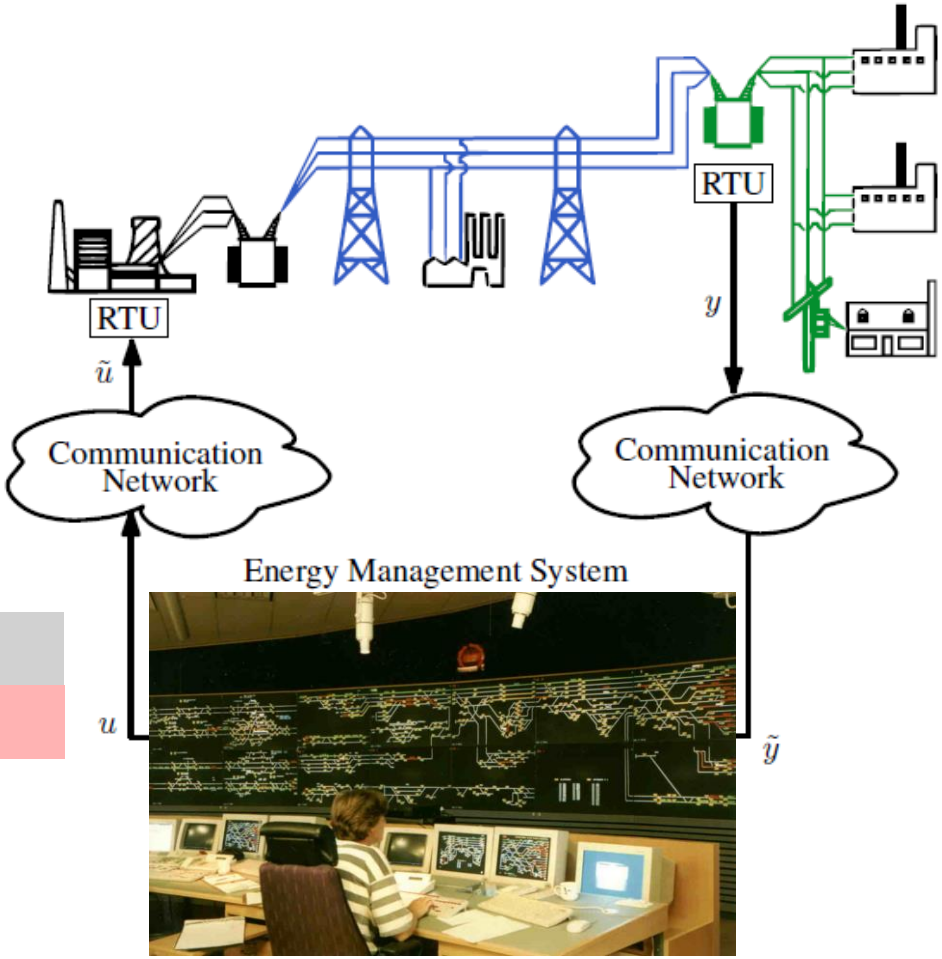
- **Likelihood metric:** probability of successful attack
  - Hard to compute – lack of historical data
  - Alternative: use proxy metrics that assess the attack effort
  - E.g.: number of infected target devices



Outline

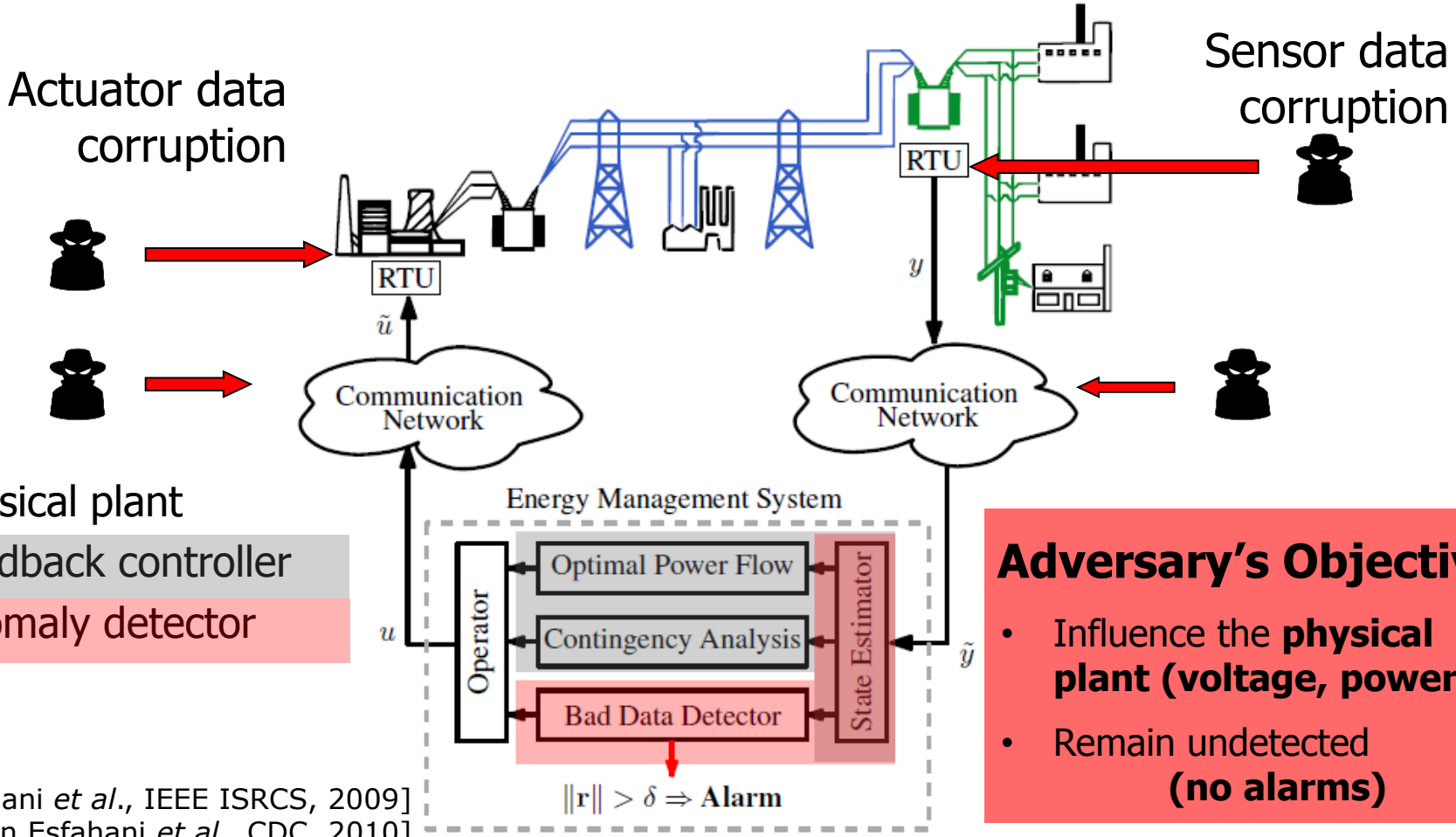
- Motivation and Research Background
- The Concept of Risk
  - Impact metrics for Energy Systems
  - Likelihood Metrics for Energy Systems
- **Scenarios and Risk metrics for Smart Energy Grids**
  - **Scenario 1: False-Data injection on Transmission Grids**
  - Scenario 2: Voltage control under adversarial actions
- Summary
- Future Challenges and Opportunities
- References

Control of Power Networks



- Physical plant
- Feedback controller
- Anomaly detector

Scenario: Closing the loop over corrupted data



- Physical plant
- Feedback controller
- Anomaly detector

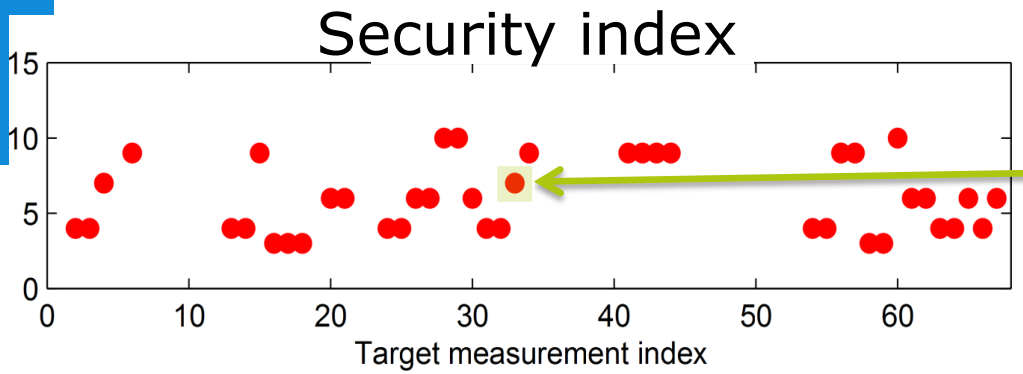
Adversary's Objective

- Influence the **physical plant (voltage, power)**
- Remain undetected **(no alarms)**

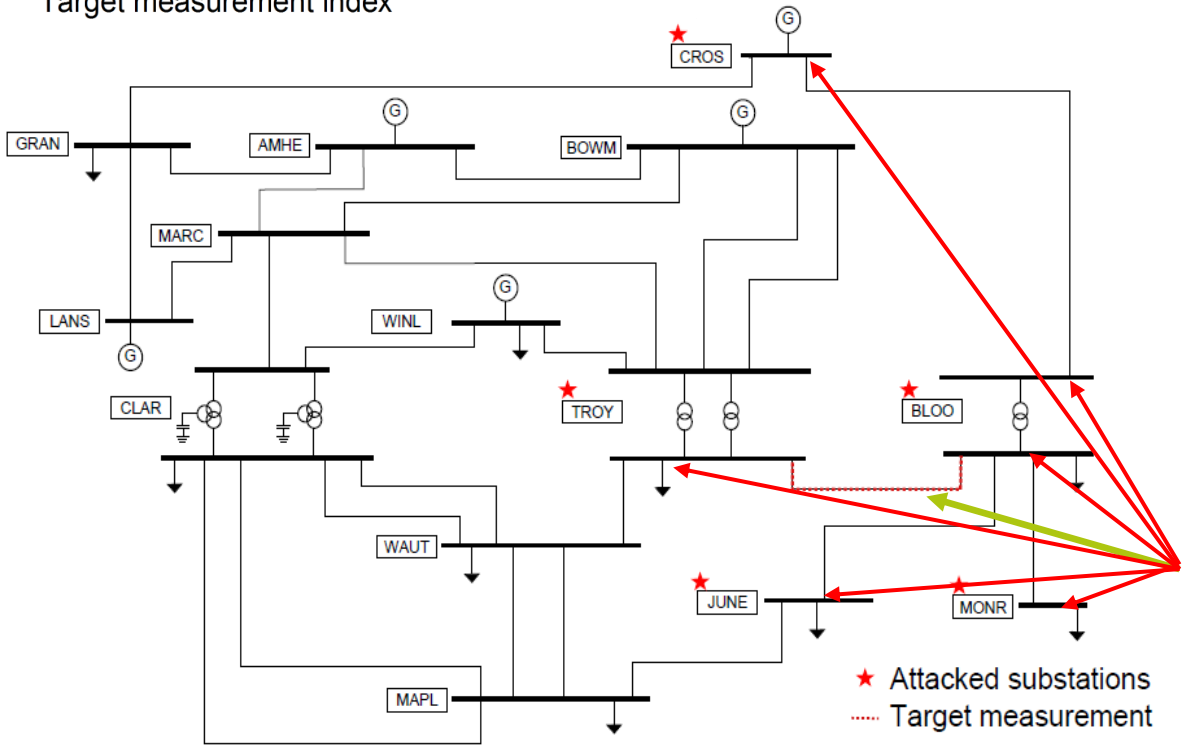
[Giani *et al.*, IEEE ISRCS, 2009]
[Mohajerin Esfahani *et al.*, CDC, 2010]

(Proxy for) **Likelihood**: Security Indices

- *How many measurements* must be corrupted to *remain undetected*?

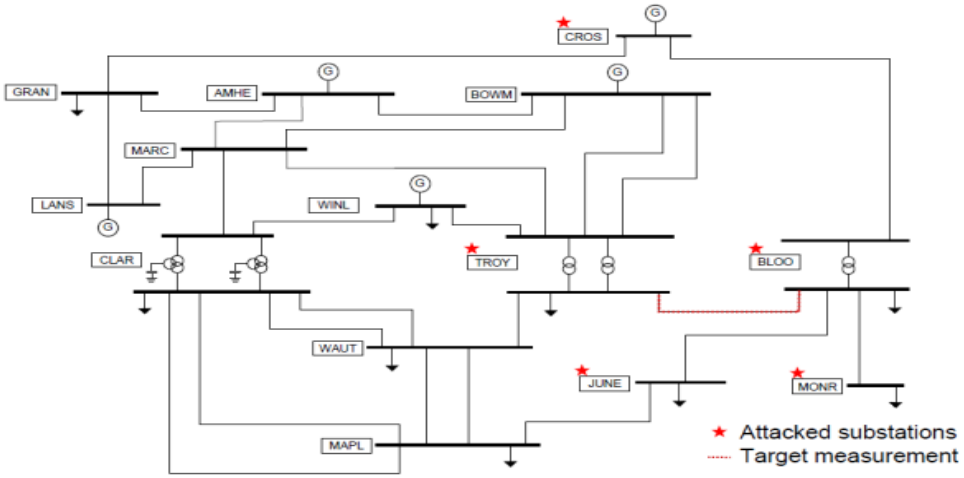


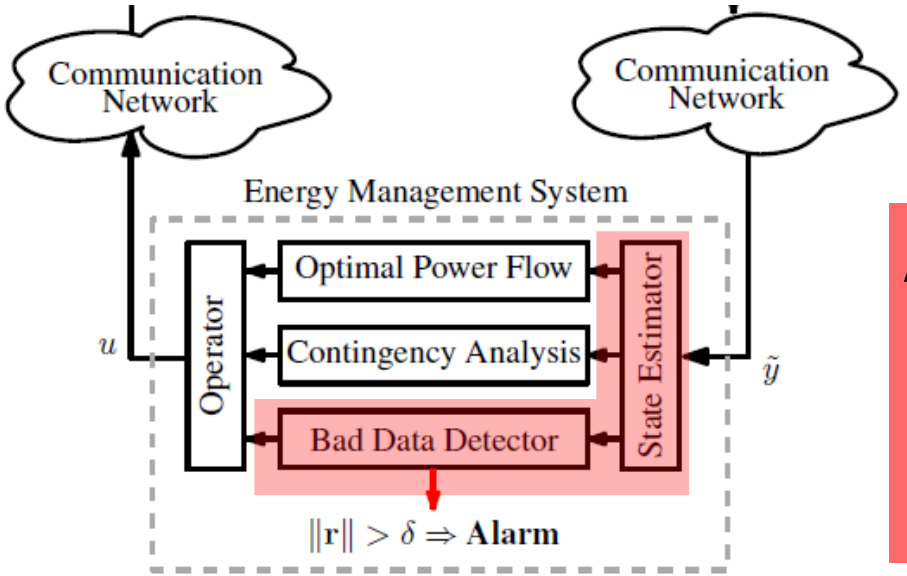
At least 7 measurements involved in a stealth attack against measurement 33



Attack 33
(7 measurements)

Experiments on SCADA/EMS Testbed





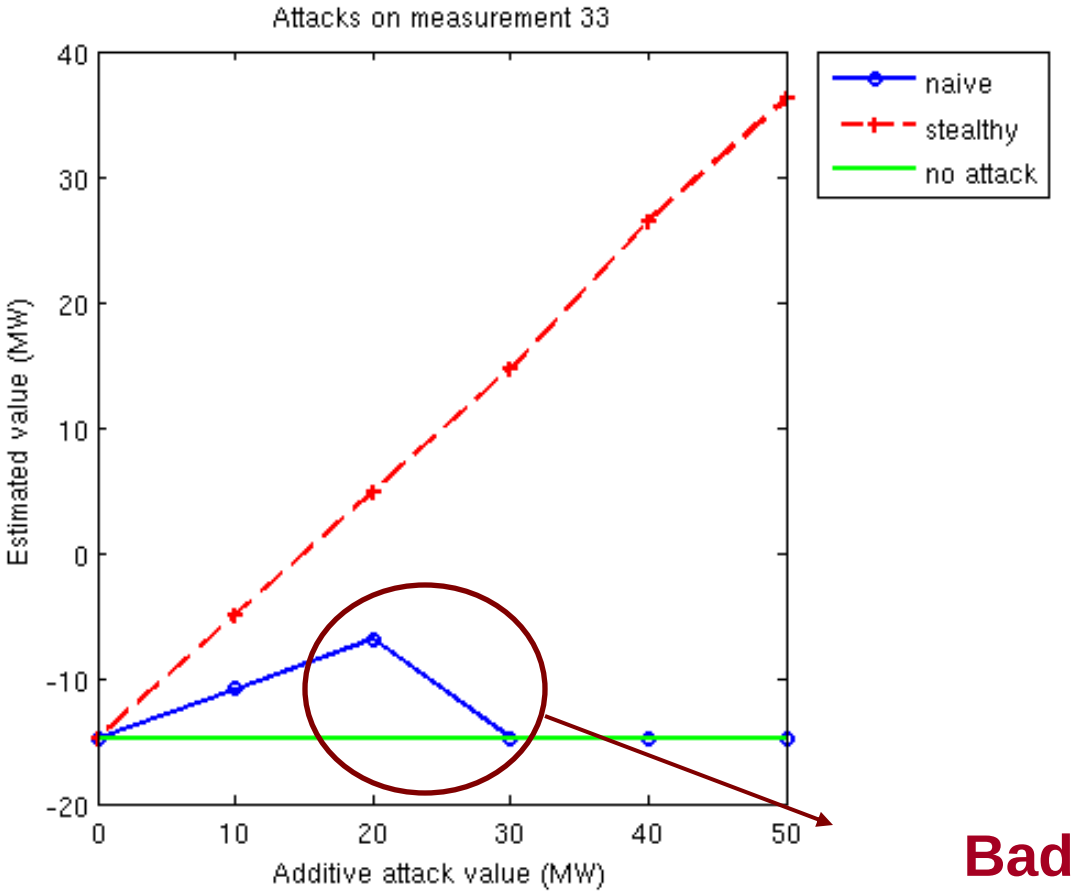
Sensor data corruption

Adversary's Objective

- Remain undetected **(no alarms)**

[Teixeira *et al.*, 2011]

Bad Data Detection Alarms

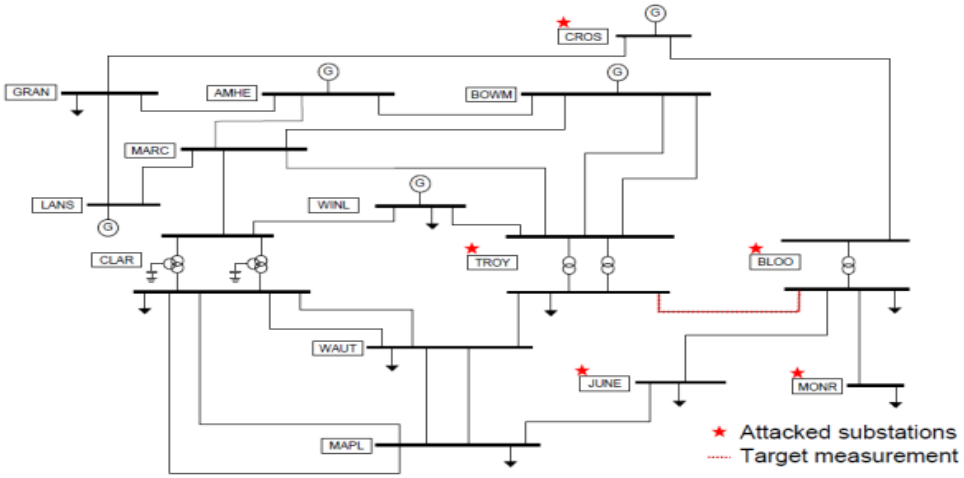


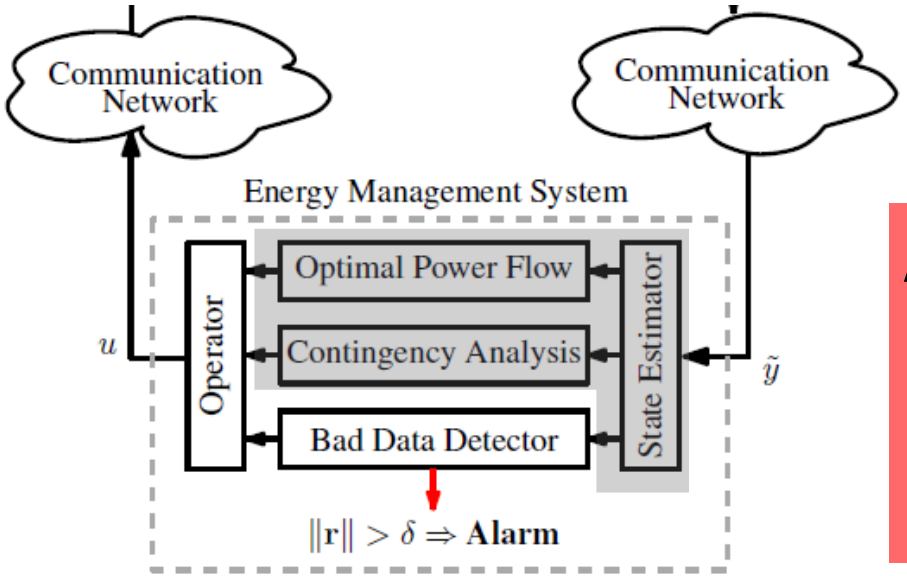
False value (MW)	Estimated value (MW)	# BDD Alarms
-14.8	-14.8	0
35.2	36.2	0
85.2	86.7	0
135.2	137.5	0
185.2	Non convergent	-

Bad Data Detected & Removed

- Attacks of 150 MW (55% of nominal value) pass undetected in a real system!

Experiments on SCADA/EMS Testbed





Sensor data corruption

Adversary's Objective

- Influence the **physical plant (voltage, power)**
- Remain undetected **(no alarms)**

[Teixeira *et al.*, 2011]

Contingency Alarms

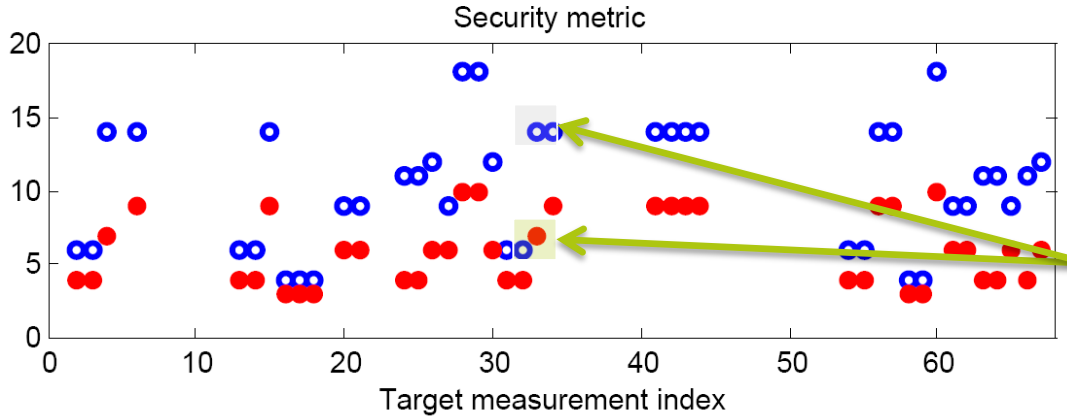
Target bias, a_{33}	False value (MW), z^a_{33}	Estimate (MW), $\hat{z}^a_{33}$	#BDD Alarms	#CA Alarms
0	-14.8	-14.8	0	2
50	35.2	36.2	0	2
100	85.2	86.7	0	10
150	135.2	137.5	0	27
200	185.2	-	-	-

- 25 new CA alarms and no BDD alarms!
- What is the reaction in the control room?
  - The human operator may think the system is in a seriously bad state, but in reality the system is in the same state as before the attack

Protection Strategies

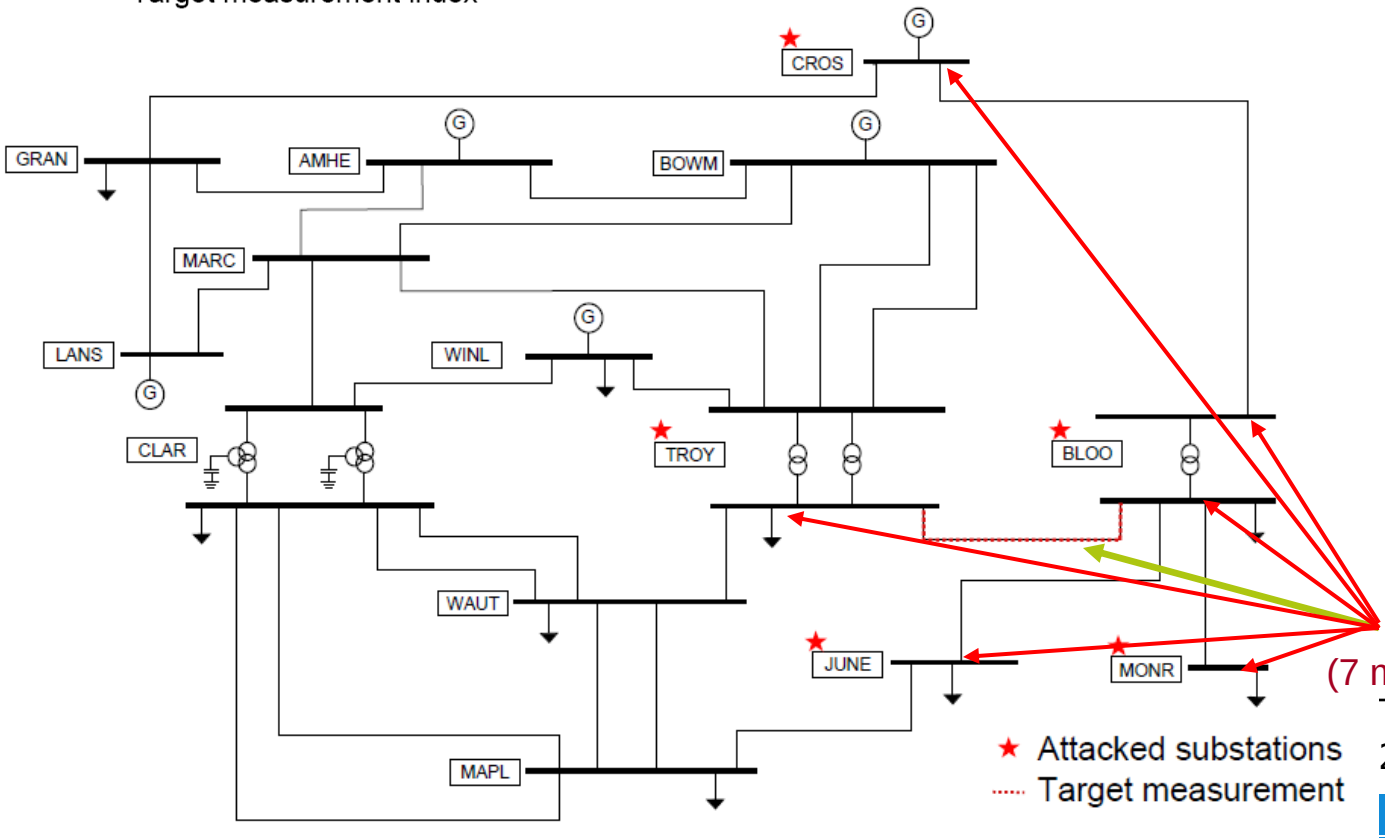
- Introduce encryption and re-route communication
  - Use security metric to identify critical measurements
  - Possibly weight metric based on expected impact, using optimal power flow [Vukovic *et al.*, 2012], [Teixeira *et al.*, 2012]
- Augment bad-data detection with cross-checking with historical data of operation [Kosut *et al.*, 2010]
- Improve available bad-data detection algorithms
  - Discover model mismatch between active/reactive power flow measurements [Sou *et al.*, 2012]

1. Use Metric to Assign Protection



• = Current measurement config.
o = Upgraded measurement config.

With few measurements protected, 14 measurements have to be involved in an undetectable attack! (instead of 7)



Attack 33
(7 measurements)

Summary Scenario 1

- Multiple interacting attacked measurements may be undetectable
- Security metric identifies measurements that are relatively "easy" to attack (locates weak spots)
- Experimental validation shows significant possible impact in control center (CA alarms)
- Protection strategies include encryption and re-routing of critical measurements

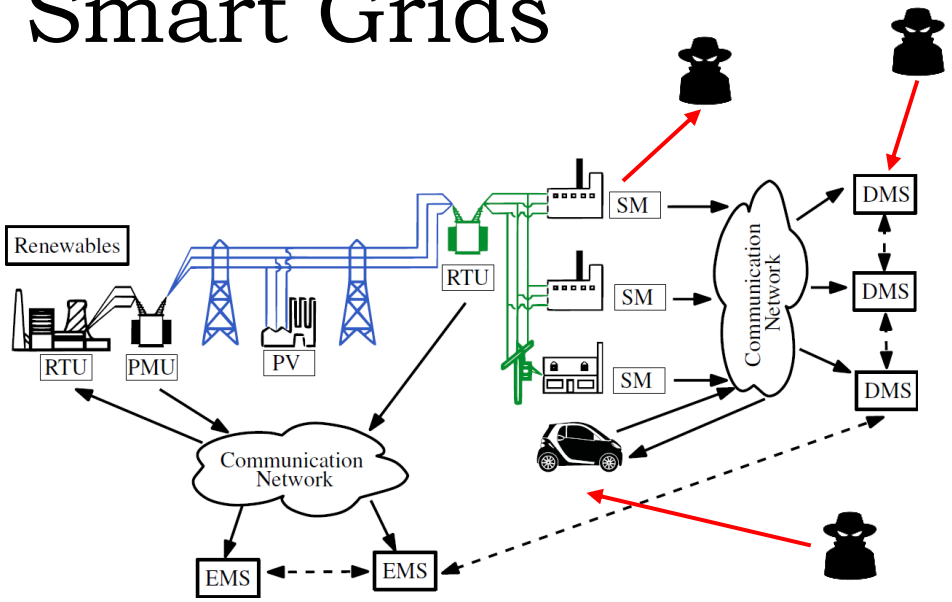
Outline

- Motivation and Research Background
- The Concept of Risk
  - Impact metrics for Energy Systems
  - Likelihood Metrics for Energy Systems
- Scenarios and Risk metrics for Smart Grids
  - Scenario 1: False-Data injection on Transmission Grids
  - **Scenario 2: Voltage control under adversarial actions**
- Summary
- Future Challenges and Opportunities
- References

Cyber Security of Smart Grids

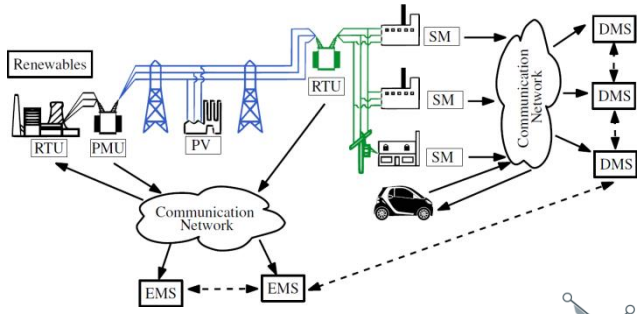
Smart Grids

- More smart devices and control loops
- Large increase in communication and data
- Leads to increasing vulnerability to cyber-physical threats with many potential points of attacks
- The Smart Grid is a cyber-physical system
  - **Power system** and **IT infrastructure** tightly coupled through SCADA and control systems
  - integrated with data analytics environments
  - Multiple stakeholders



SMART GRID PROTECTION AGAINST CYBER ATTACKS

Attack Scenarios for Smart Grids



References with Attack Scenarios

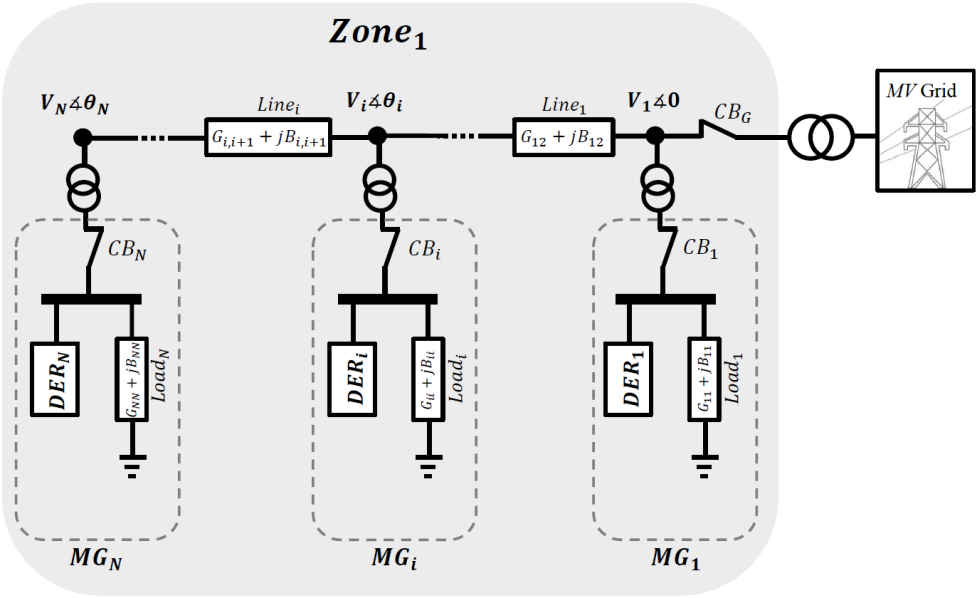
- "*Cyber Security for DER Systems*",
  NESCOR, Electric Power Research Institute, 2013

- "*The Future Of Smart Cities: Cyber-physical Infrastructure Risk*",
  Office of Cyber and Infrastructure Analysis, DHS, August 2015

- *"Electric Sector Failure Scenarios and Impact Analyses"*,
  NESCOR, Electric Power Research Institute, 2014
  - DER.15 Threat Agent Spoofs DER Data Monitored by DER SCADA Systems
  - DGM.6 Spoofed Substation Field Devices Influence Automated Responses

- Chosen scenarios: Voltage control under adversarial actions [Teixeira et al., ETFA, 2015]

Power System Model

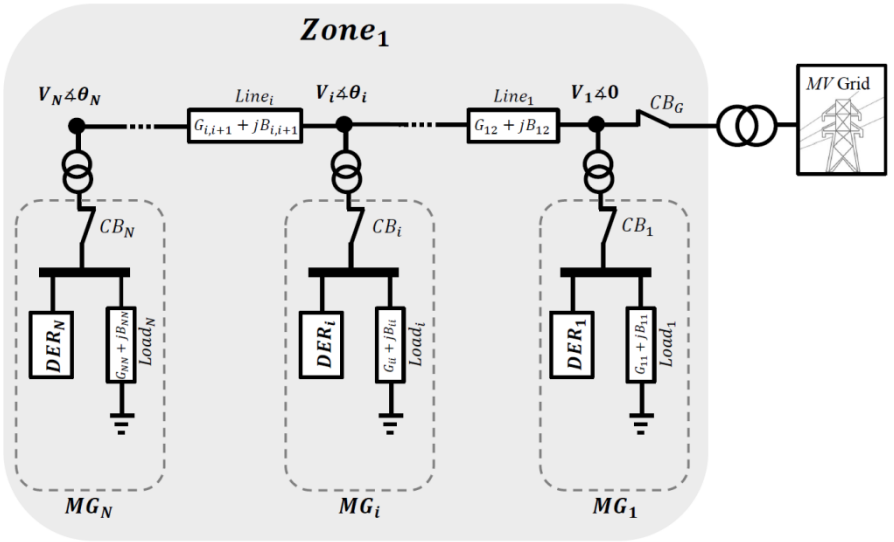


- **Interconnected microgrids**
- Model each microgrids as:
  - Lumped inverter-controlled Distributed Energy Resources (DERs)
  - Lumped loads
- Inductive lines, but with resistive losses

Power System Model

- States of each microgrid
  - Voltage level: V_i (pu)
  - Phase angle: θ_i (rad)
- Microgrid model

$$\tau_i \dot{V}_i(t) = u_{V_i}(t)$$
$$\tau_{\theta_i} \dot{\theta}_i(t) = u_{\theta_i}(t)$$



- Transmission Line: $Y_{ij} = G_{ij} + \mathrm{j}B_{ij}$

Homogeneous line ratio: $\rho = \dfrac{G_{ij}}{B_{ij}}$

- Power injections:

$$P_i = V_i^2 G_i - \sum_{j \in \mathcal{N}_i} V_i V_j \left(G_{ij} \cos(\theta_i - \theta_j) + B_{ij} \sin(\theta_i - \theta_j) \right),$$

$$Q_i = -V_i^2 B_i - \sum_{j \in \mathcal{N}_i} V_i V_j \left(G_{ij} \sin(\theta_i - \theta_j) - B_{ij} \cos(\theta_i - \theta_j) \right)$$

Power System Model: Voltage Dynamics

- Microgrid model: $\tau_i \dot{V}_i(t) = u_{V_i}(t)$

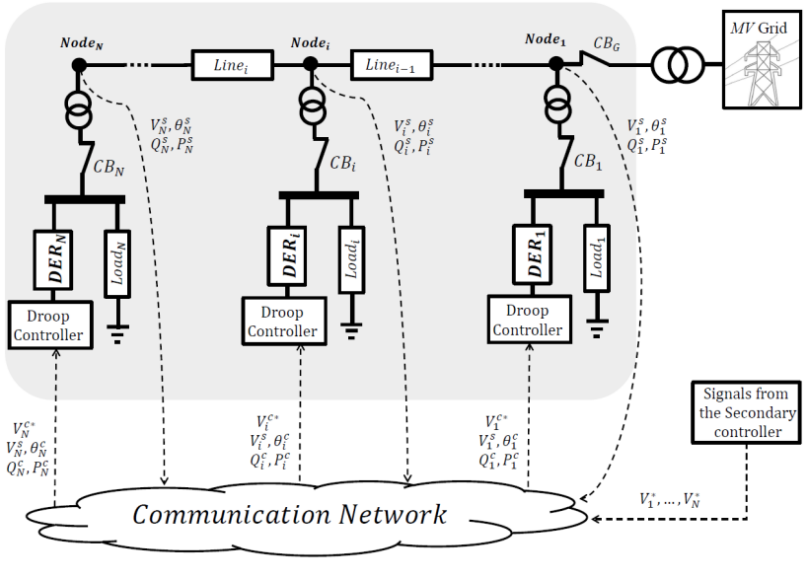
  Assume constant phase-angles

- Voltage droop controller:

$$u_{V_i}(t) = -\kappa_i V_i^c(t)\left(V_i^c(t) - V_i^{c\star}(t)\right) - Q_i^c(t)$$

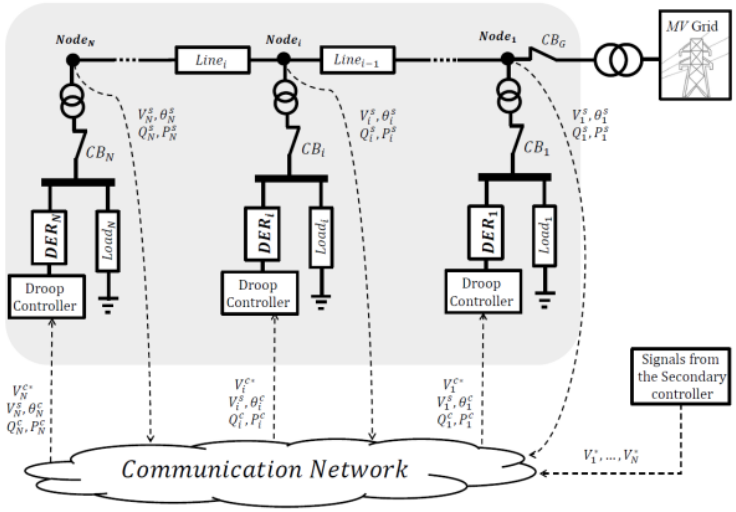
κ_i Controller gain
$V_i^{c\star}$ Received voltage reference
V_i^c Received voltage measurement
Q_i^c Received power injection measurement

[Simpson-Porco et. al, TAC, 2015]



- Under nominal operation: $\tau_i \dot{V}_i = -\kappa_i V_i\left(V_i - V_i^\star\right) - Q_i$

Voltage Dynamics

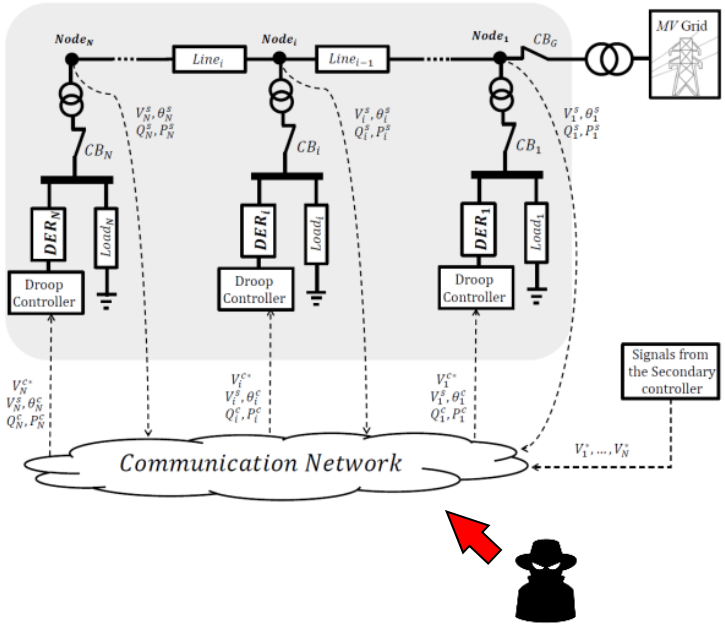


- Nominal operation: $\tau_i \dot{V}_i = -\kappa_i V_i \left(V_i - V_i^\star\right) - Q_i$

- Desired system properties
  - Stability - ensured for large control gains: $\kappa_i \geq \sum_{j \in \mathcal{N}_i} (\sqrt{\rho^2 + 1} - 1)|B_{ij}|$
  - Positivity - ensured for small phase-angle differences: $|\tan(\theta_i - \theta_j)| \leq \rho^{-1}$
    - Positivity ensures desirable properties, e.g.,
      - an **increase in reference** results in a **voltage increase** throughout the system

Risk of Adversarial Actions

- Attack Scenarios:
  - Voltage Reference Attack
  - Voltage Measurement Routing Attack
- Possible Impact Metrics:
  - Maximum Voltage Variation
  - Loss of Positivity
  - Loss of Stability
- Possible Likelihood Metrics:
  - Number of corrupted reference signals
  - Number to re-routed measurement signals
- Risk Assessment: mathematical analysis of attack scenarios
  - Study the impact metrics by analyzing models
  - Use results to guide simulation-based analysis

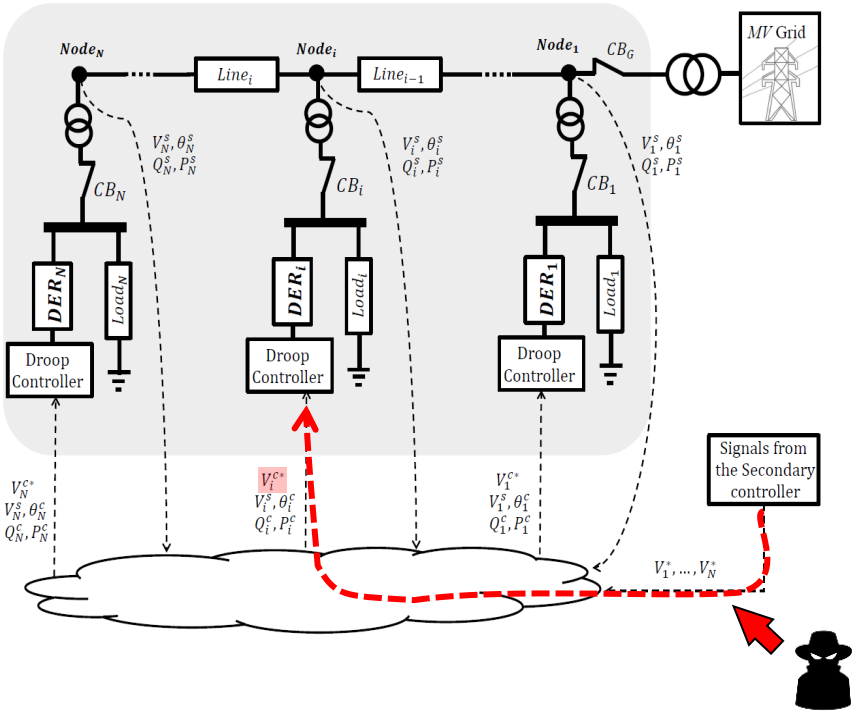


Voltage Reference Attack

- Demonstration reported in Kang et al. ”Investigating Cyber-Physical Attacks against IEC 61850 Photovoltaic Inverter Installations”, ETFA 2015
- Voltage reference of MG-i is compromised

$$u_{V_i}(t) = -\kappa_i V_i^c(t)\,(V_i^c(t) - u^a(t)) - Q_i^c(t)$$

- Theoretical results:
  - **Computation of maximum voltage increase**
  - **Increase in reference** leads to **increased voltages**
  - Voltage increase **decays with distance** to attacked microgrid (for line topologies)

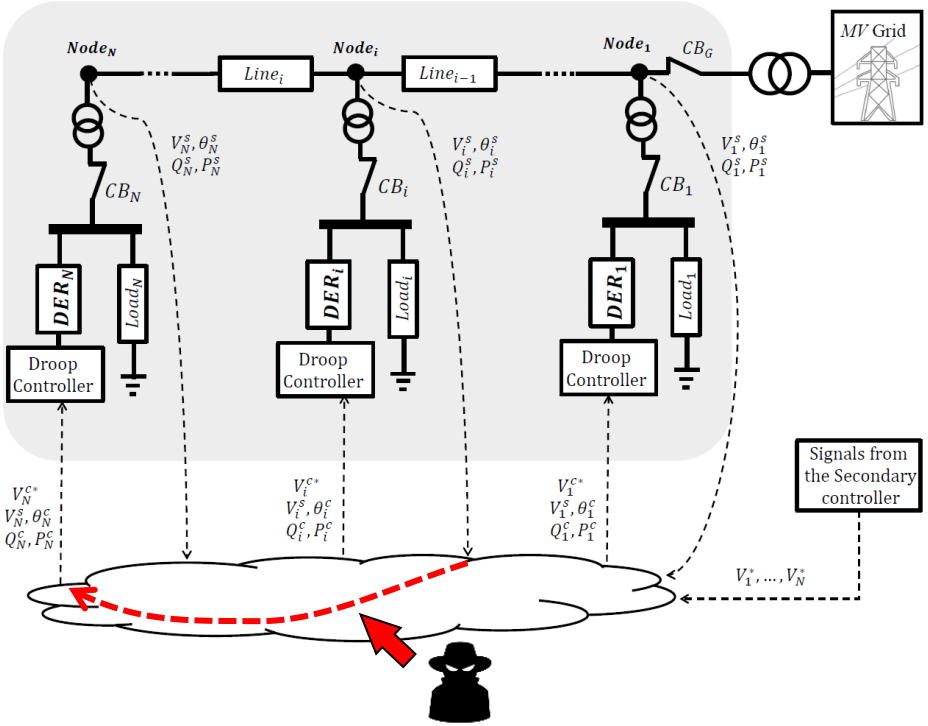


Voltage Measurement Routing Attack

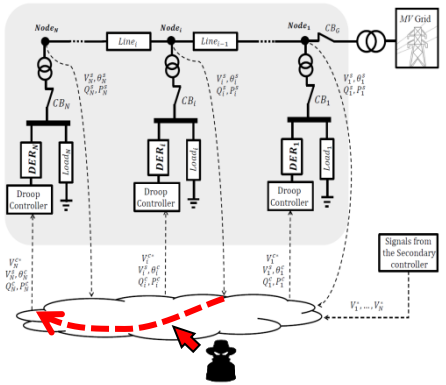
- Voltage measurement of one MG-j redirected to another MG-i

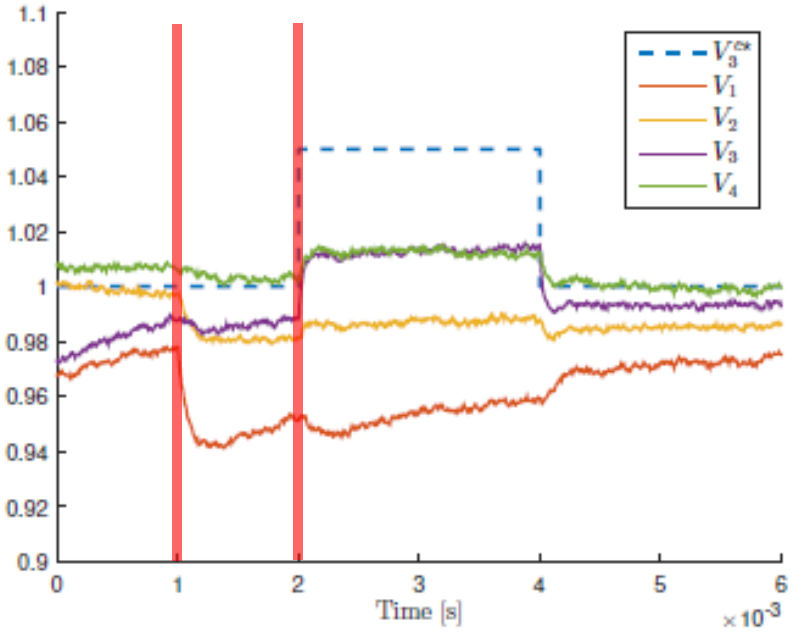
$$u_{V_i}(t) = -\kappa_i V_j^c(t)\left(V_j^c(t) - V_i^{c\star}(t)\right) - Q_i^c(t)$$

- Theoretical results:
  - **Loss of positivity**
  - **Equillibrium change** (depends on pre-attack voltage levels)
  - **Increase in reference** may lead to **decreased voltages**
  - **If** MG-i and MG-j **are not neighbors**, **stability may be lost** for high control gains!



Voltage Measurement Routing Attack: Numerical Results





- Measurement of MG4 redirected to MG1
- Reference of MG3 changed
- Voltage of MG1 **decreases** after attack and after reference change

Outline

- Motivation and Research Background
- The Concept of Risk
  - Impact metrics for Energy Systems
  - Likelihood Metrics for Energy Systems
- Scenarios and Risk metrics for Smart Grids
  - Scenario 1: False-Data injection on Transmission Grids
  - Scenario 2: Voltage control under adversarial actions
- **Summary**
- **Future Challenges and Opportunities**
- References

Summary

- The concept of Risk: {**Scenario** ; **Impact** ; **Likelihood**}
- The **Scenario** description if the basis for risk assessment
- **Impact** follows from the operational objectives
  - Desired properties (stability)
  - Safety margins
  - Efficiency and performance
- **Likelihood** relates to required resources/effort
  - May be hard to assess, use proxies instead
- Examples of Attack Scenarios:
  - False-data injection
  - Malicious re-routing of measurements

Future Challenges and Opportunities

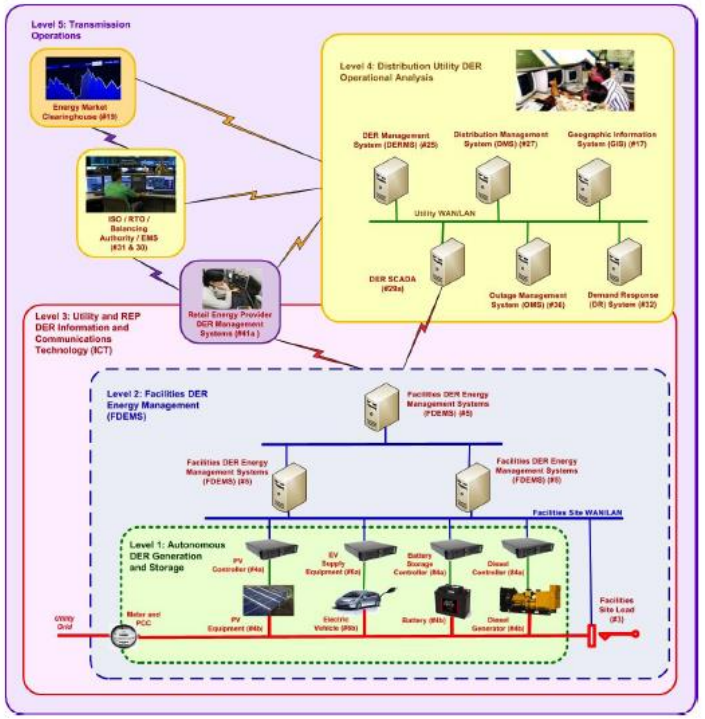
Tackling the diversity of Threat Scenarios for Smart Cities

- *"The Future Of Smart Cities: Cyber-physical Infrastructure Risk",* Office of Cyber and Infrastructure Analysis, DHS, August 2015
  - "Sample Vector 2: A malicious actor intercepts and manipulates **energy price data** in **demand response** systems to cause demand fluctuations and **potential outages**."
  - "Sample Vector 3: **Installation of new** cyber-physical **components** onto legacy components **leads to interoperability problems**, unintended consequences, and smart generation system disruptions."
  - Many other examples in different domains (transportation, water & waste management, energy…)

Future Challenges and Opportunities

Tackling the complexity of Smart Grids (and its security implications)

- *"Cyber Security for DER Systems",* NESCOR, 2013
  - Multiple entities / stakeholders across multiples layers
  - Who "pays the bill" of a cyber attack?
  - Who invests in cyber security and privacy?
  - What are the economics of cyber security and privacy?
- Could *cyber security* be a "show-stopper"?
- New EU data protection regulation
  - 2. Data **processors** will be held responsible for data protection



References

- A. Teixeira, H. Sandberg, G. Dán, and K. H. Johansson. *"Optimal Power Flow: Closing the Loop over Corrupted Data"*. In Proc. American Control Conference, Montreal, Canada, 2012
- A. Teixeira, K. Paridari, H. Sandberg, and K. H. Johansson. *"Voltage control for interconnected microgrids under adversarial actions"*. In Proc. 20th IEEE International Conference on Emerging Technologies and Factory Automation, Luxembourg, 2015

Extensions to generic dynamical systems

- A. Teixeira, H. Sandberg, and K. H. Johansson. *"Strategic Stealthy Attacks: the output-to-output l2-gain"*. In Proc. 54th IEEE Conference on Decision and Control, Osaka, Japan, 2015.
- A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. *"A Secure Control Framework for Resource-Limited Adversaries"*. Automatica, vol. 51, pp. 135-148, Jan. 2015.
- A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson. *"Secure Control Systems: A Quantitative Risk Management Approach"*. IEEE Control System Magazine, vol. 35, no. 1, pp. 24-25, Feb. 2015.

References (cont.)

- Stanley Kaplan, B. John Garrick "*On The Quantitative Definition of Risk"*, Risk Analysis, vol.1, no.1, 1981

- *"The Future Of Smart Cities: Cyber-physical Infrastructure Risk",* Office of Cyber and Infrastructure Analysis, DHS, August 2015
- *"Cyber Security for DER Systems",* NESCOR, 2013
- "Electric Sector Failure Scenarios and Impact Analyses", NESCOR, 2014