GIAN short course

Cyber-Physical Security for the Smart Grid

Indian Institute of Technology, Bombay, India

Coordinator: Prof. R. K. Shyamasundar

Manimaran Govindarasu

Dept. of Electrical and Computer Engineering

Iowa State University

Email: gmani@iastate.edu

http://powercyber.ece.iastate.edu

March 5-16, 2018

Course Agenda

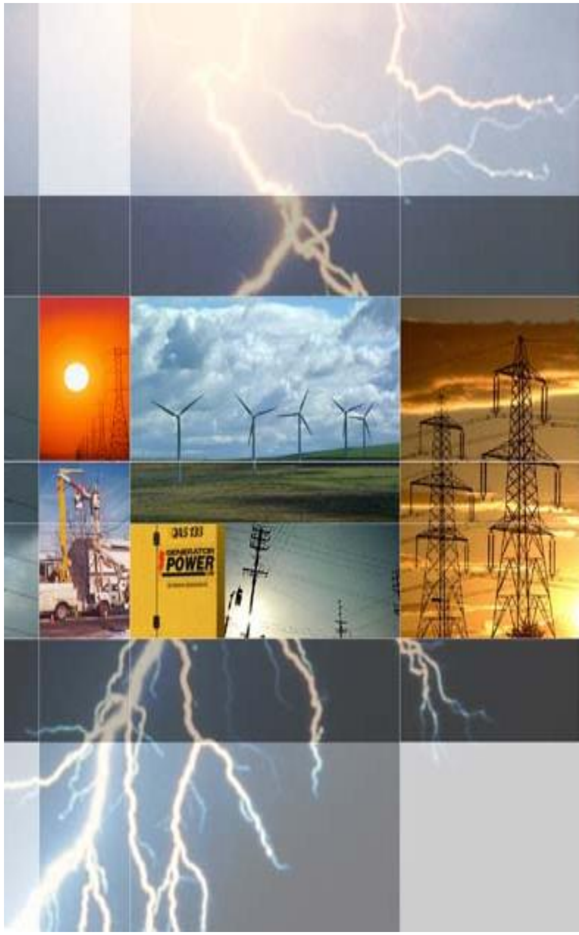
Day 01	• Module 1: Cyber Threats, Attacks, and Security concepts
Day 02	• Module 2: Risk Assessment and Mitigation & • Overview of Indian Power Grid
Day 03	• Module 3: Attack-resilient Wide-Monitoring, Protection, Control
Day 04	• Module 4: SCADA, Synchrophasor, and AMI Networks & Security
Day 05	• Module 5: Attack Surface Analysis and Reduction Techniques
Day 06	• Module 6: CPS Security Testbeds & Case Studies
Day 07	• Module 7: Cybersecurity Standards & Industry Best Practices
Day 08	• Module 8: Cybersecurity Tools & Vulnerability Disclosure
Day 09	• Module 9 : Review of materials, revisit case studies, assessments
Day 10	• Module 10: Research directions, education and training

Module 3: Cyber Security of Wide-Area Monitoring, Protection and Control (WAMPAC)

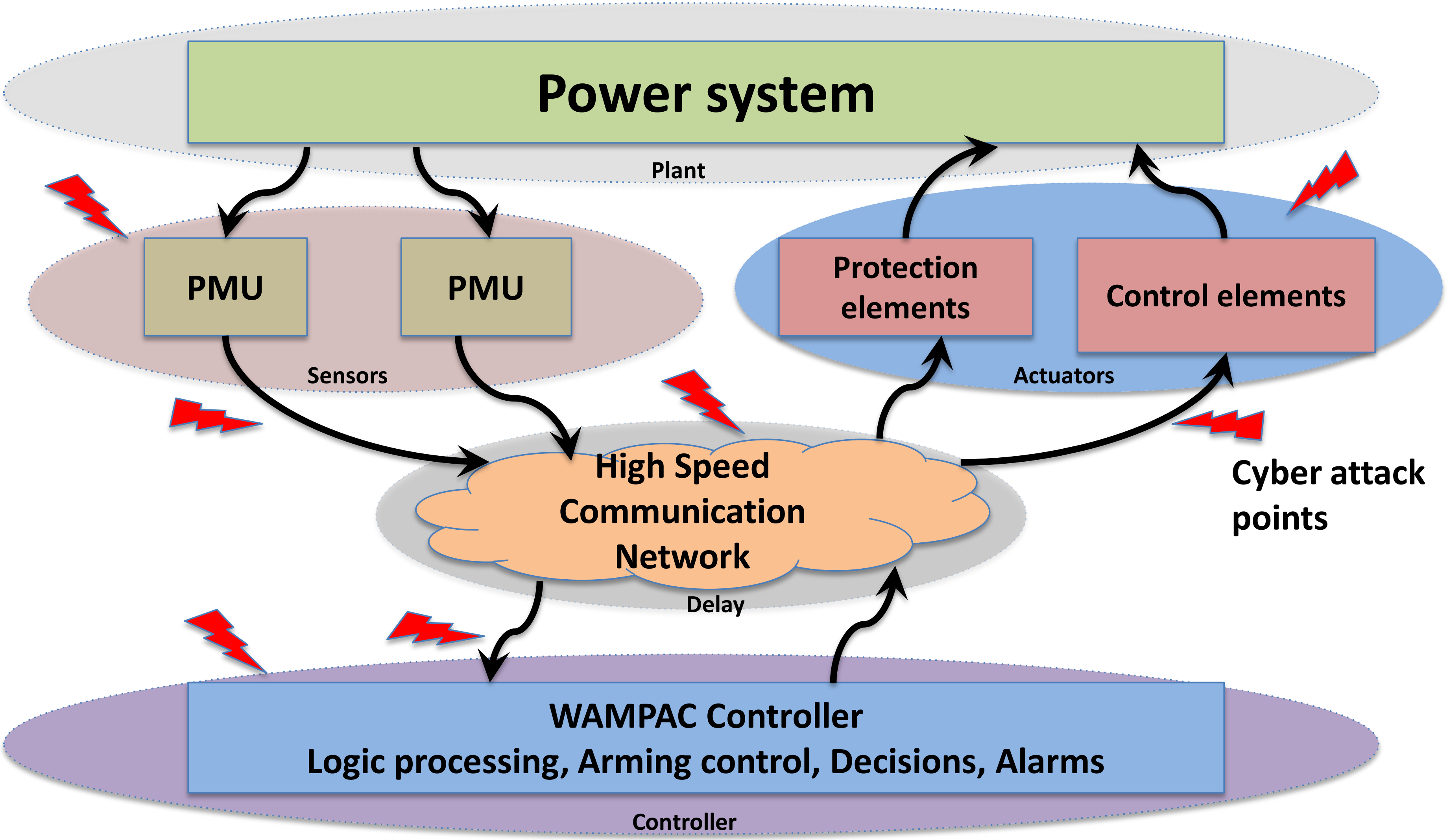
- Wide-Area Control
  Case study: Automatic Generation Control

- Wide-Area Protection
  Case study: Remedial Action Scheme

- Wide-Area Monitoring
  Case study: State Estimation

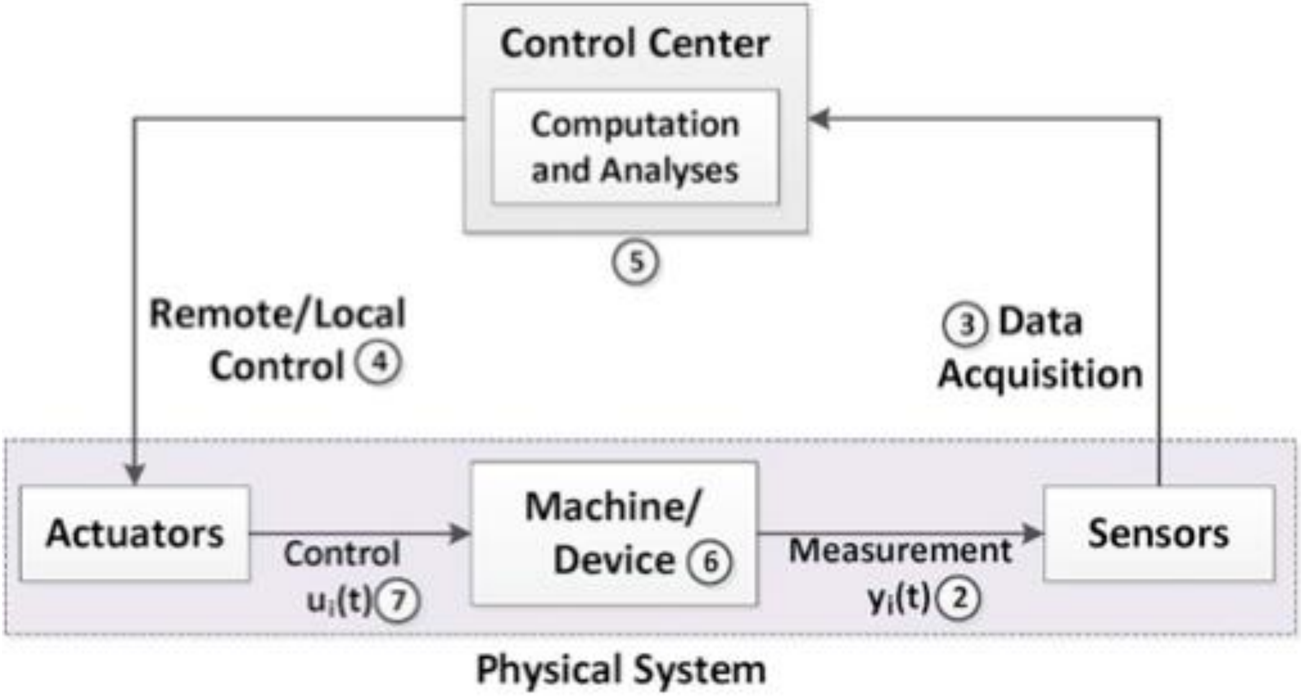


WAMPAC high-level architecture



Cyber attack points

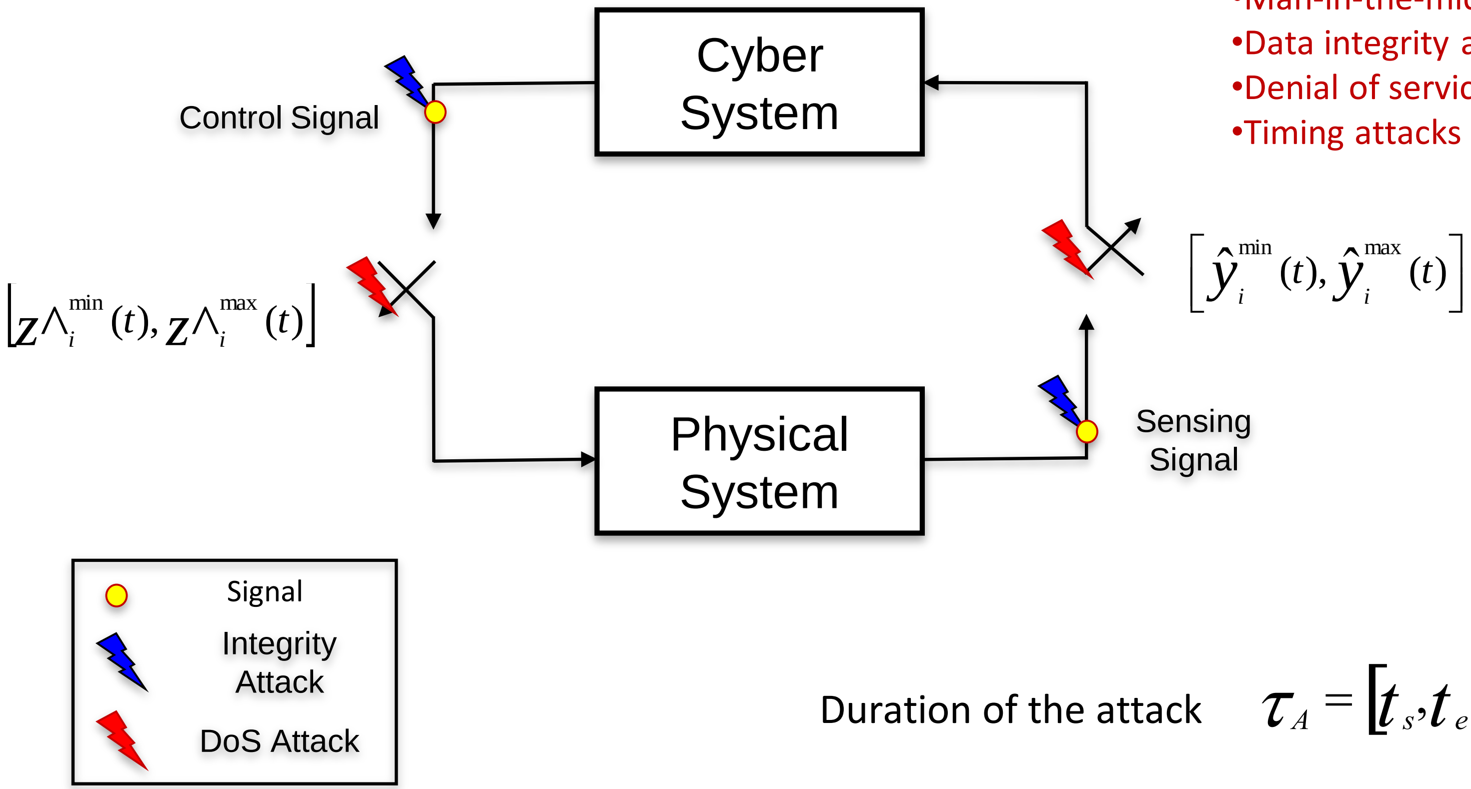
Typical Power System Control loop



S. Sridhar, A.Hahn and G. Manimaran – "Cyber–Physical System Security for the Electric Power Grid" – Proceedings of the IEEE, Jan 2012

Cyber-Physical Control – Attacks view

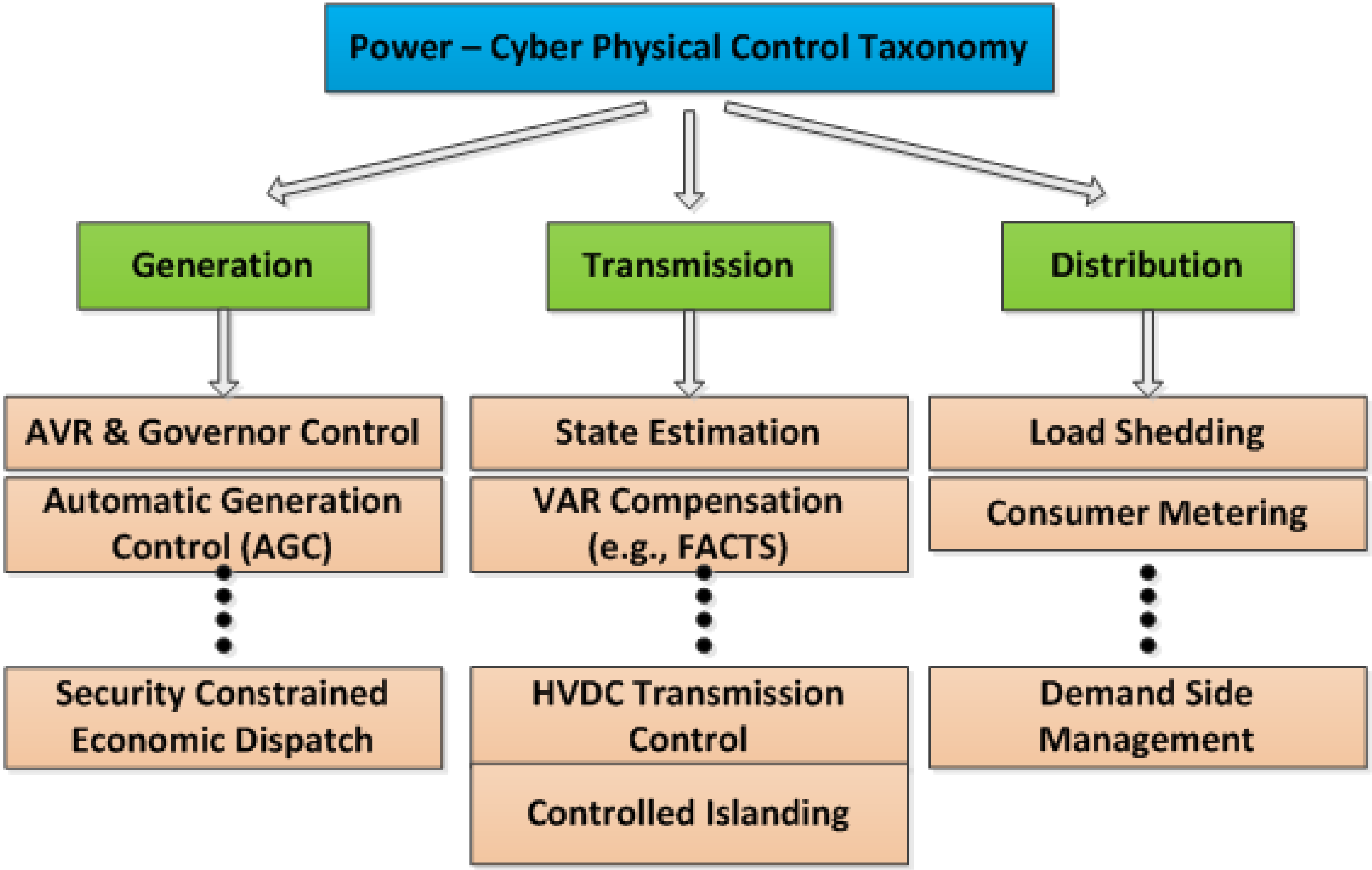
- Man-in-the-middle attacks
- Data integrity attacks
- Denial of service attacks
- Timing attacks …


Cyber System
Control Signal
$\hat{y}_i^{\min}(t), \hat{y}_i^{\max}(t)$
$\lfloor z\wedge_i^{\min}(t), z\wedge_i^{\max}(t)\rfloor$
Physical System
Sensing Signal
● Signal
Integrity Attack
DoS Attack

Duration of the attack $\tau_A = [t_s, t_e]$

Y. Huang, A. A. Cardenas, S. Sastry, “*Understanding the Physical and Economic Consequences of Attacks on Control Systems*”, Elsevier, International Journal of Critical Infrastructure Protection 2009.

Cyber-Physical Control Taxonomy


Power – Cyber Physical Control Taxonomy
Generation
Transmission
Distribution
AVR & Governor Control
Automatic Generation Control (AGC)
Security Constrained Economic Dispatch
State Estimation
VAR Compensation (e.g., FACTS)
HVDC Transmission Control
Controlled Islanding
Load Shedding
Consumer Metering
Demand Side Management

State Estimation in EMS

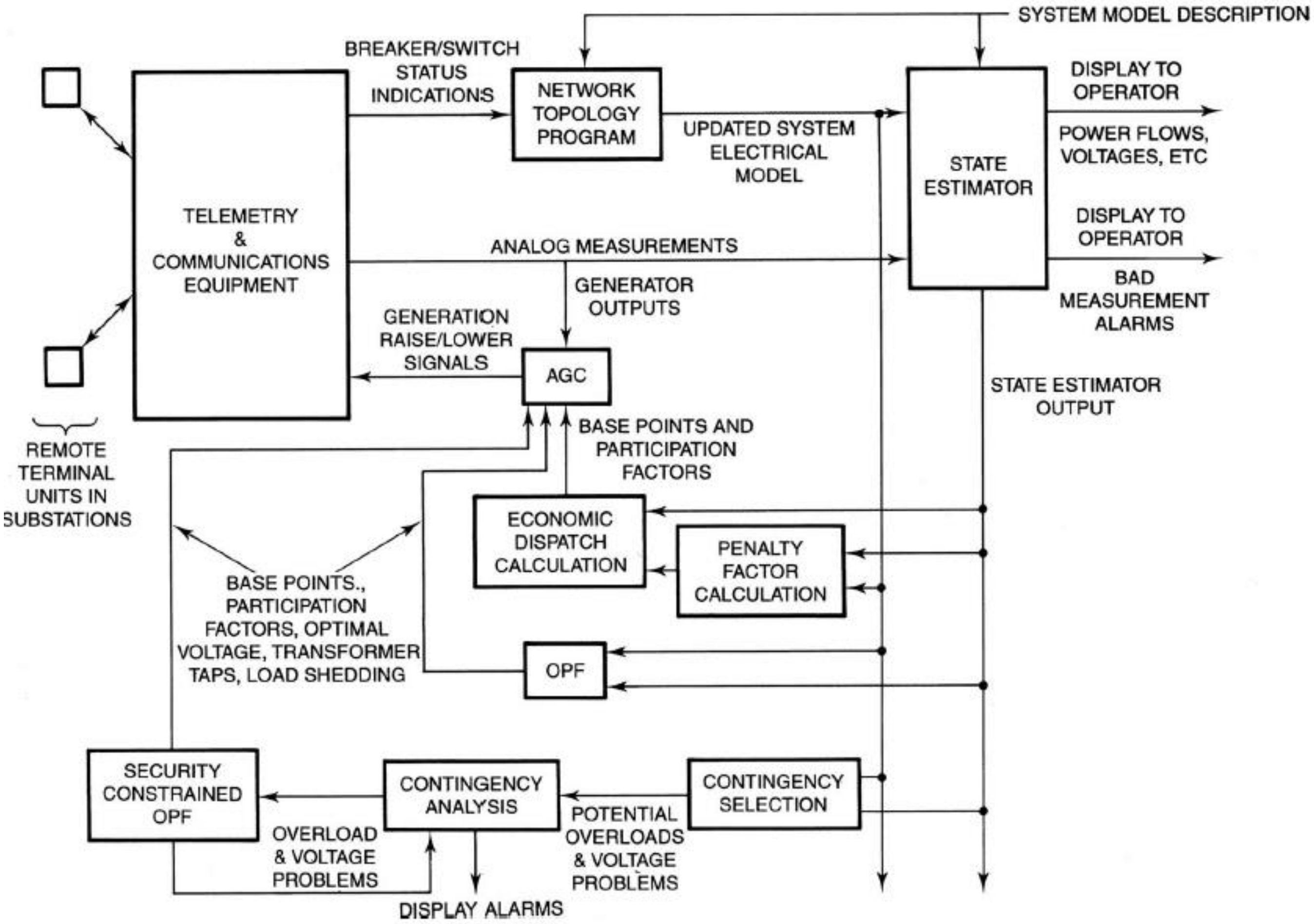

SYSTEM MODEL DESCRIPTION
BREAKER/SWITCH STATUS INDICATIONS
NETWORK TOPOLOGY PROGRAM
UPDATED SYSTEM ELECTRICAL MODEL
STATE ESTIMATOR
DISPLAY TO OPERATOR
POWER FLOWS, VOLTAGES, ETC
DISPLAY TO OPERATOR
BAD MEASUREMENT ALARMS
TELEMETRY & COMMUNICATIONS EQUIPMENT
ANALOG MEASUREMENTS
GENERATOR OUTPUTS
GENERATION RAISE/LOWER SIGNALS
AGC
STATE ESTIMATOR OUTPUT
BASE POINTS AND PARTICIPATION FACTORS
REMOTE TERMINAL UNITS IN SUBSTATIONS
ECONOMIC DISPATCH CALCULATION
PENALTY FACTOR CALCULATION
BASE POINTS., PARTICIPATION FACTORS, OPTIMAL VOLTAGE, TRANSFORMER TAPS, LOAD SHEDDING
OPF
SECURITY CONSTRAINED OPF
CONTINGENCY ANALYSIS
CONTINGENCY SELECTION
OVERLOAD & VOLTAGE PROBLEMS
POTENTIAL OVERLOADS & VOLTAGE PROBLEMS
DISPLAY ALARMS

FIGURE 9.20 Energy control center system security schematic.

Module 3: Attack-resilient Wide-Area Monitoring, Protection and Control

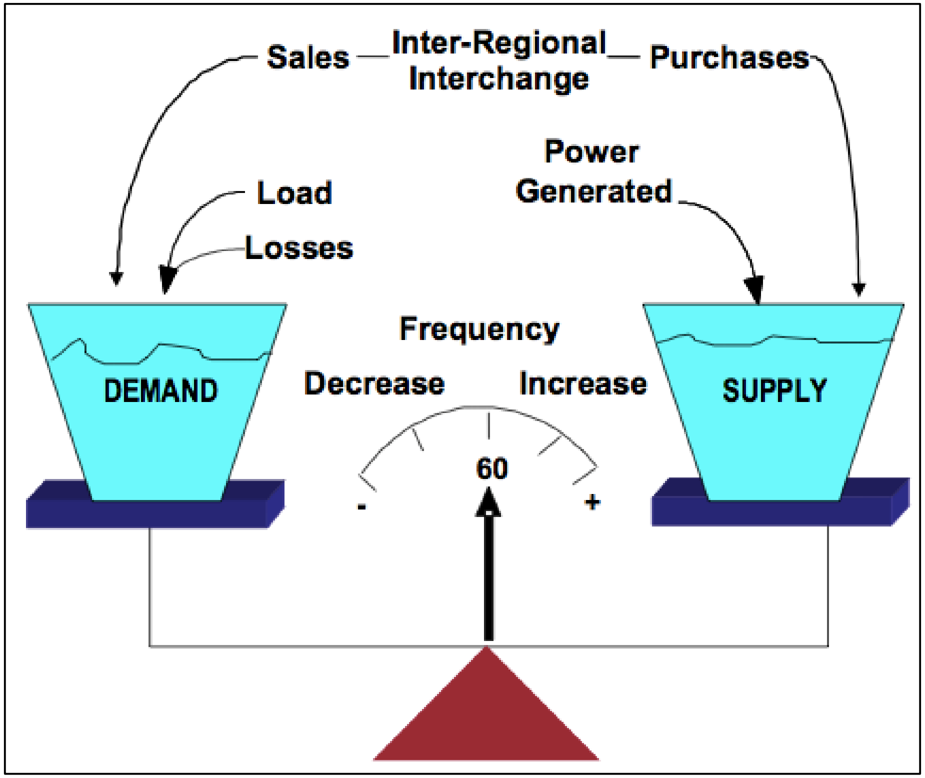
Case study: Automatic Generation Control (AGC)

Automatic Generation Control (AGC)

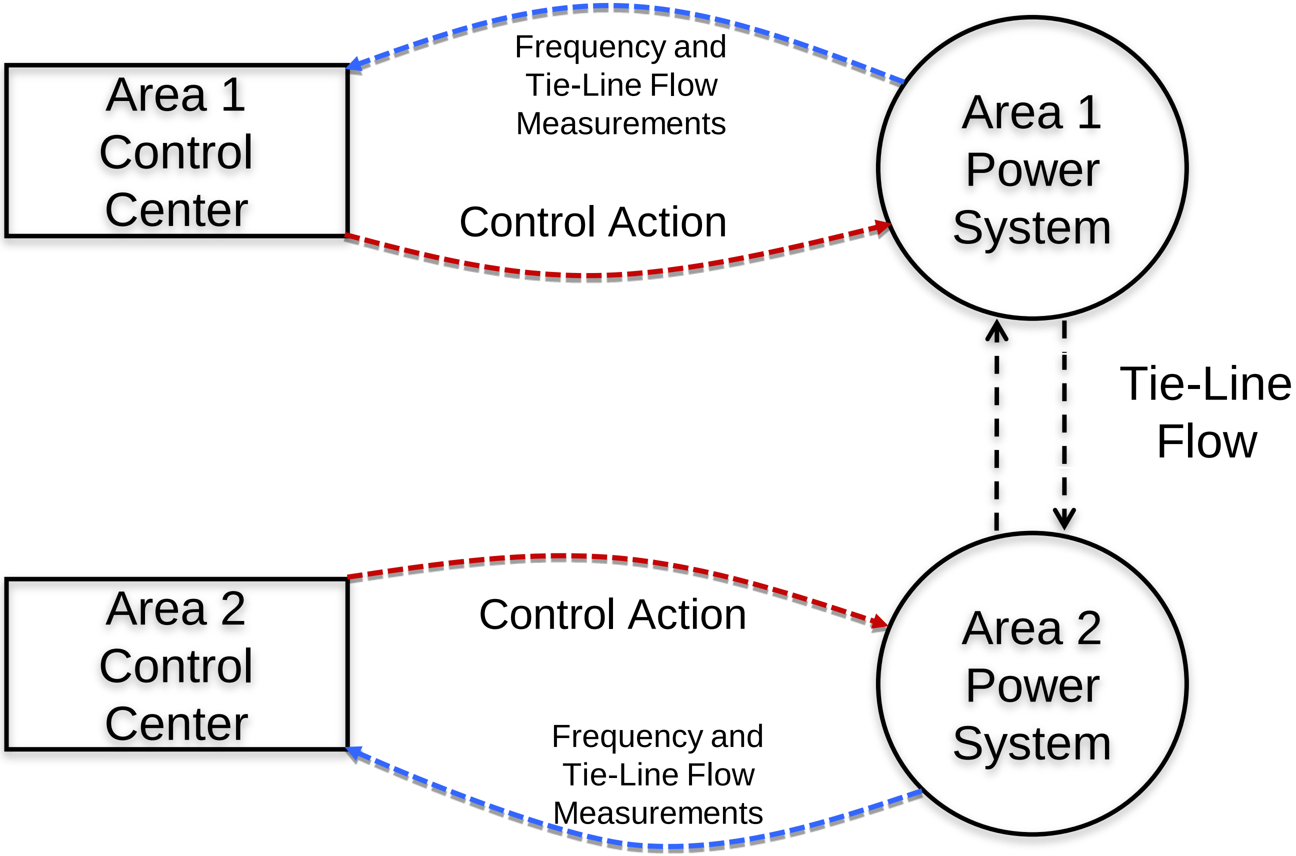
AGC Features

- Maintains frequency at 60 Hz
- Supply = Demand
- Maintain power exchange at scheduled value
- Ensures economic generation

[Figure from NERC Balancing and Frequency Control www.nerc.com]

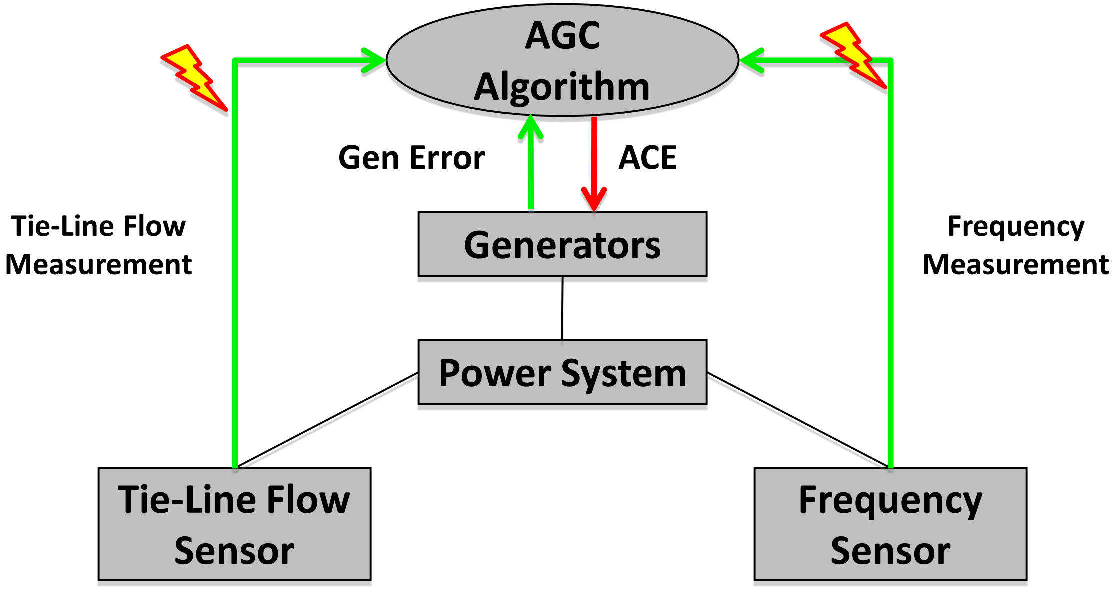


Automatic Generation Control (AGC)



Automatic Generation Control

Frequency Control



AGC Operation

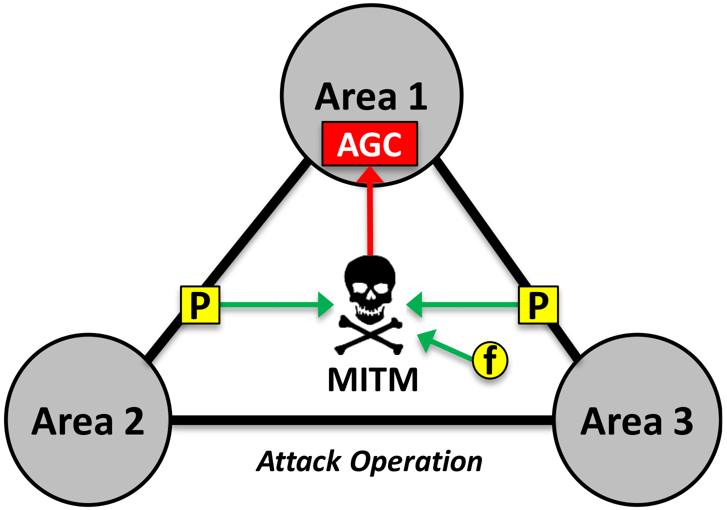
$$\text{ACE} = \mathbf{\Delta P_{net}} + \beta\ \mathbf{\Delta} \boldsymbol{f}$$

Attack: **Modify tie-line flow and frequency measurements**

Impact: **Abnormal operating frequency conditions**

Siddharth Sridhar and G. Manimaran – "Data Integrity Attacks and Impacts on SCADA Control System" – IEEE PES General Meeting, 2010

AGC – Example attack vectors



AGC Operation

ACE = **ΔP**$_{\mathbf{net}}$ + β **Δ*f***

- **Attack Models**

❖ *Scaling attacks* – Attacks that inject instantaneous change

$$P_{tie\_scaling}(t) = (1 + \lambda_{scaling}) * P_{sch}$$

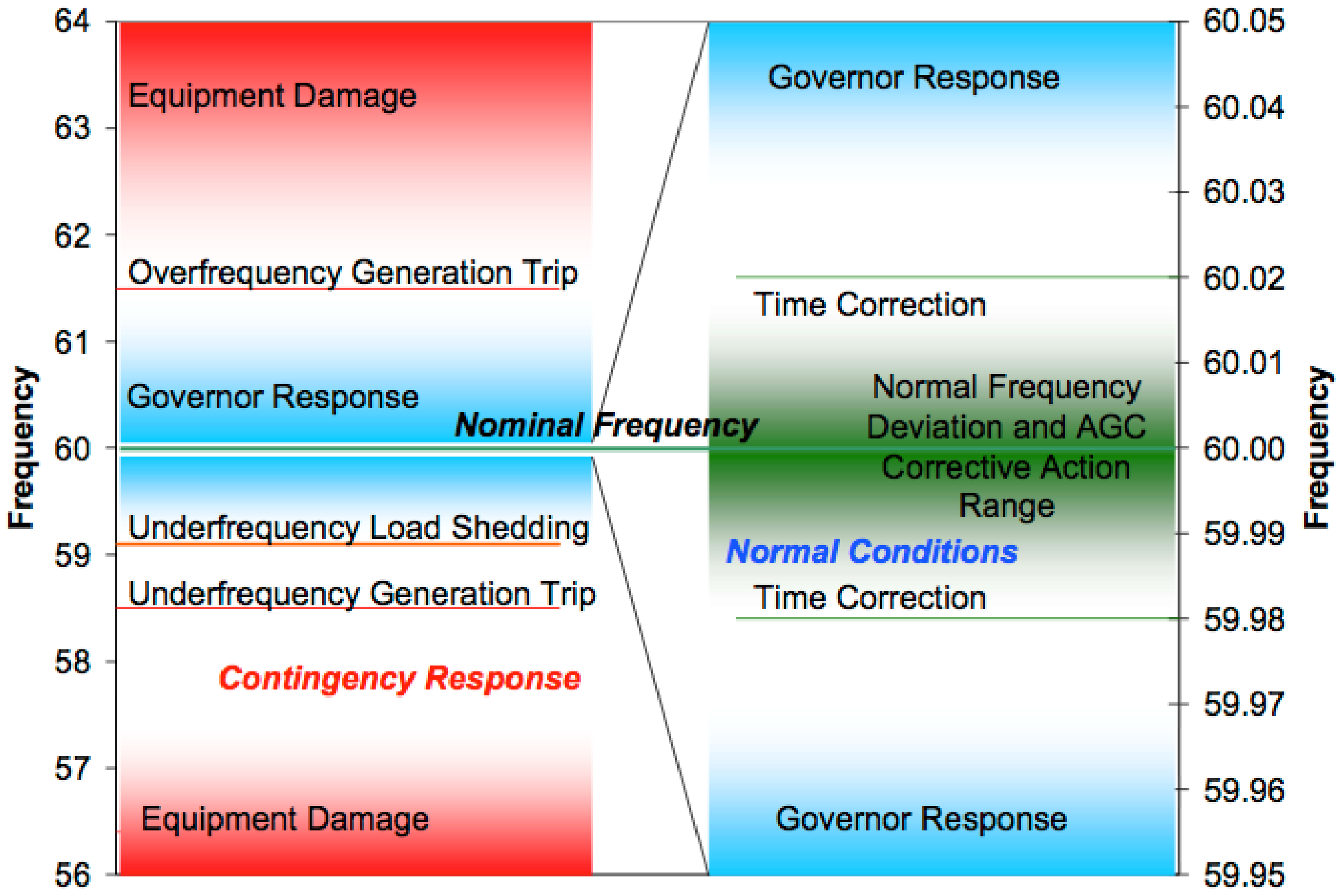
❖ *Ramp attacks* – Attacks that inject small changes over time

$$P_{tie\_ramp}(t) = P_{sch} + \lambda_{ramp} * t$$

❖ *Attack frequency: Value computed by the attacker*

$$f_{attack} = f_{act} - \frac{\Delta P_{tie\_attack}}{\sum(1/R + D)}$$

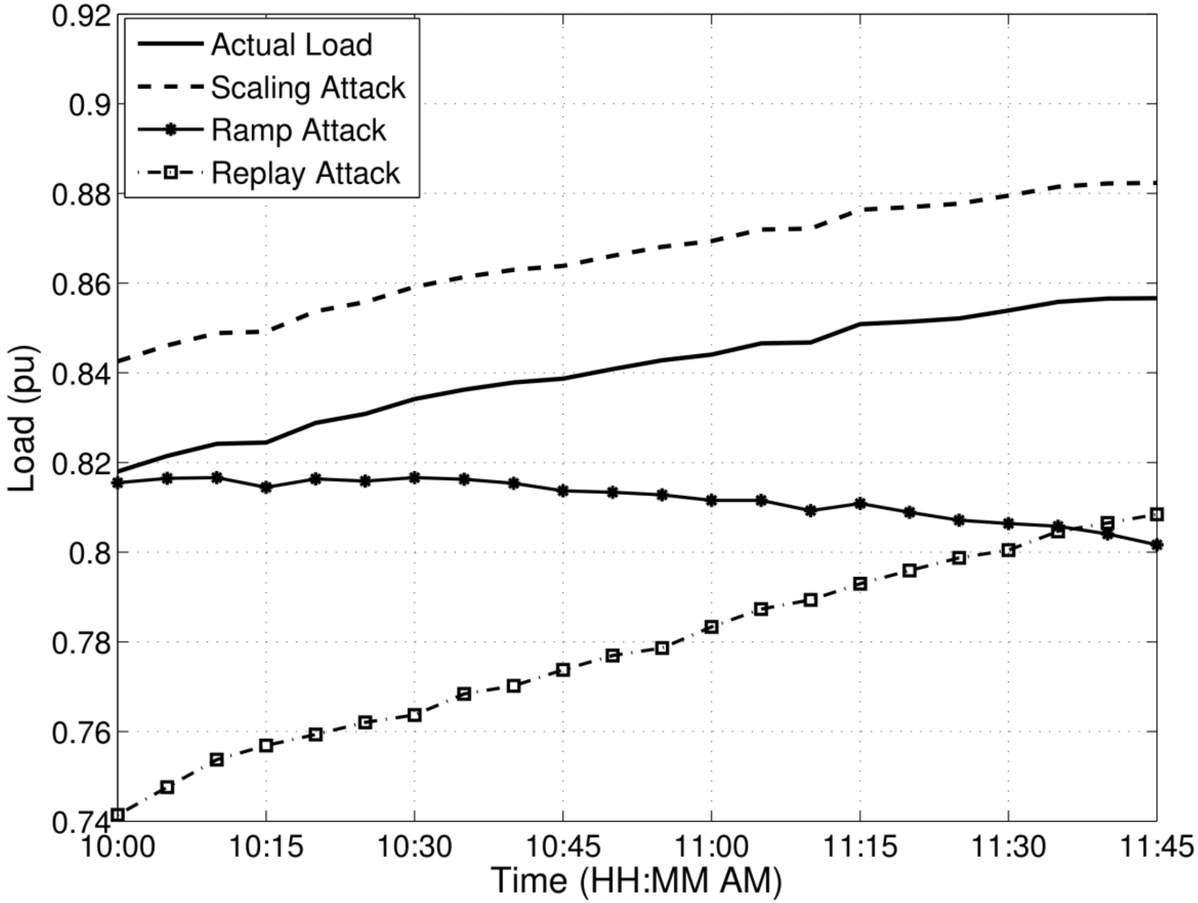
Impacts from Poor Frequency



Source: NERC (wwe.nerc.com) Figure from “Frequency Control Concerns in The North American Electric Power System”

AGC – attack impacts (sample result)

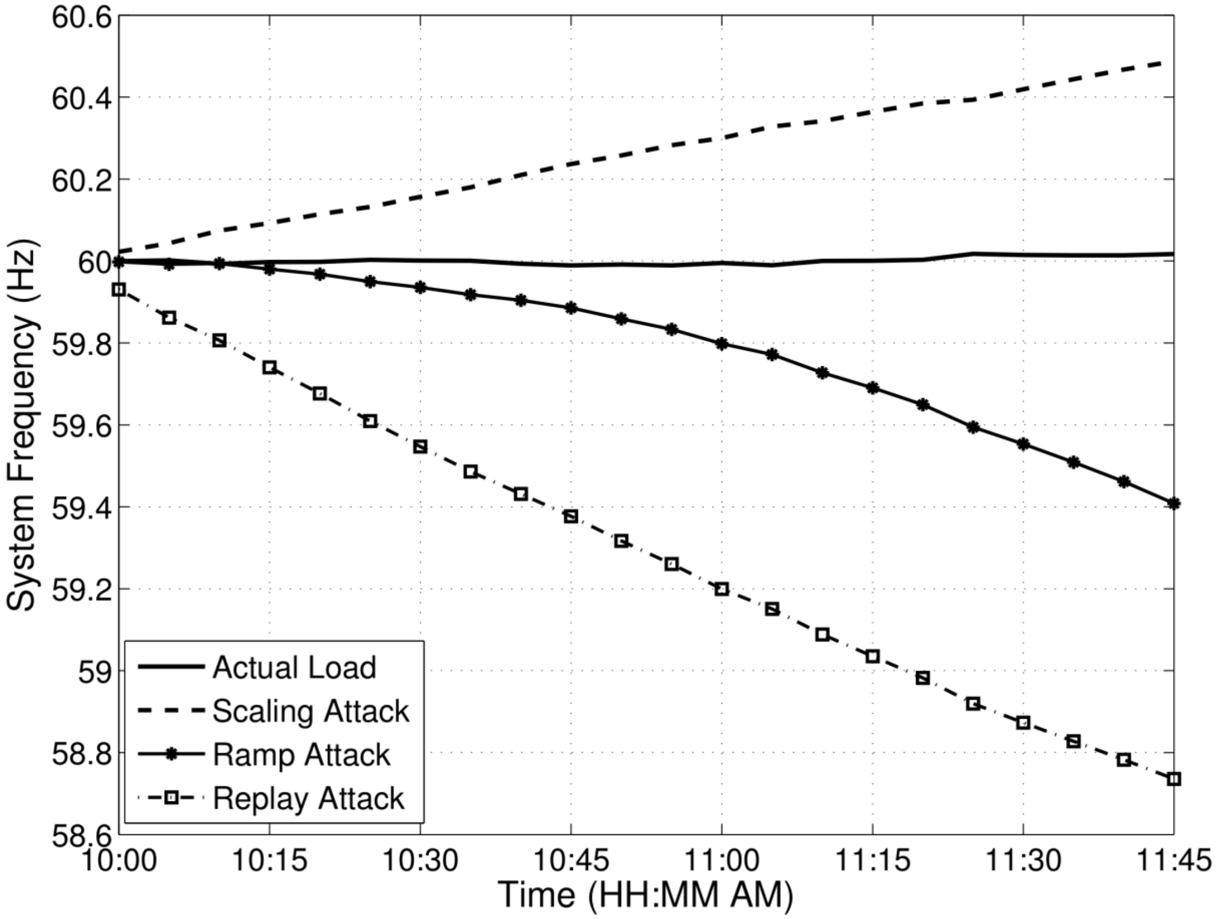
Attack Impact – Perceived Load at the Control Center



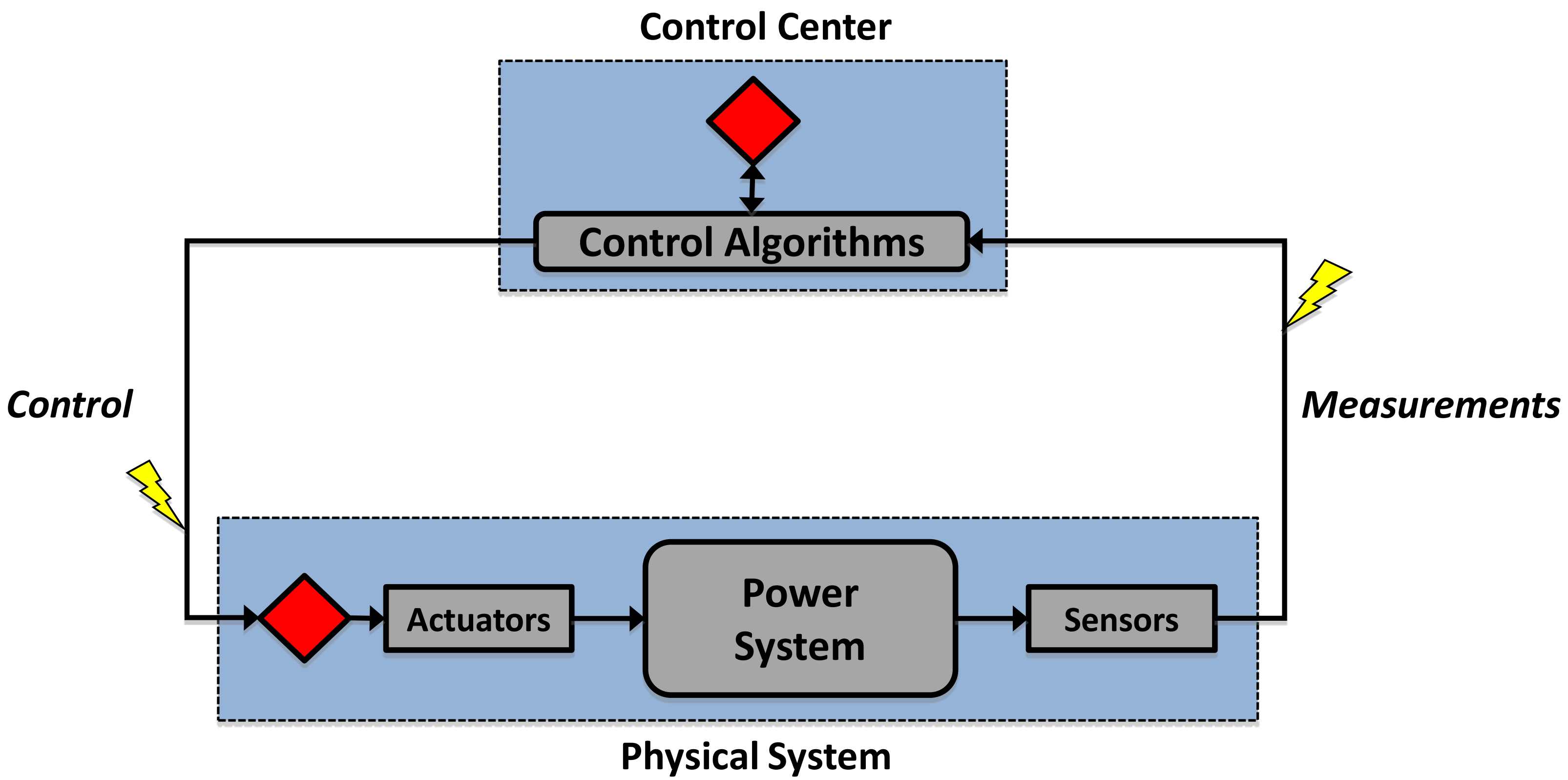
Siddharth Sridhar and G. Manimaran – "Data Integrity Attacks and Impacts on SCADA Control System" – IEEE PES General Meeting, 2010

AGC – attack impacts (sample result)

Attack Impact – Resulting System Frequency

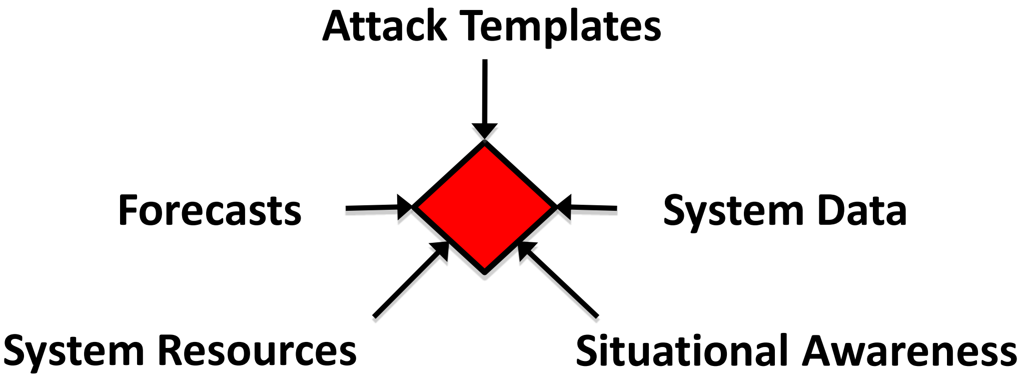


Attack Resilient Control (ARC)



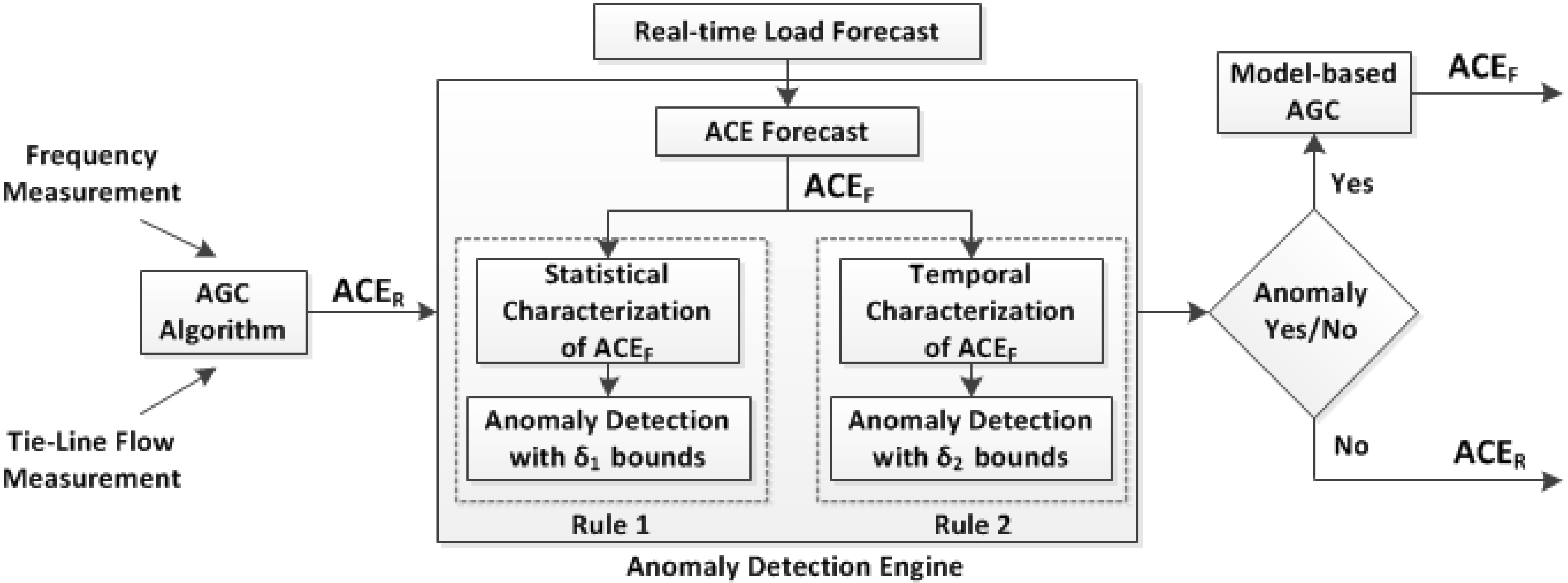
◆ → Intelligent Attack Detection and Mitigation Module

ARC – Intelligence Sources



- **Forecasts –** Load and wind forecasts
- **Situational Awareness –** System topology, geographic location, market operation
- **Attack Templates –** Attack vectors, signatures, potential impacts
- **System Data –** Machine data, control systems
- **System Resources –** Generation reserves, VAR reserves, available transmission capacity

Model-based Attack Detection and Mitigation for AGC


Real-time Load Forecast
ACE Forecast
ACE_F
Frequency Measurement
AGC Algorithm
ACE_R
Tie-Line Flow Measurement
Statistical Characterization of ACE_F
Anomaly Detection with δ_1 bounds
Rule 1
Temporal Characterization of ACE_F
Anomaly Detection with δ_2 bounds
Rule 2
Anomaly Detection Engine
Anomaly Yes/No
Yes
Model-based AGC
ACE_F
No
ACE_R

<u>Key</u>

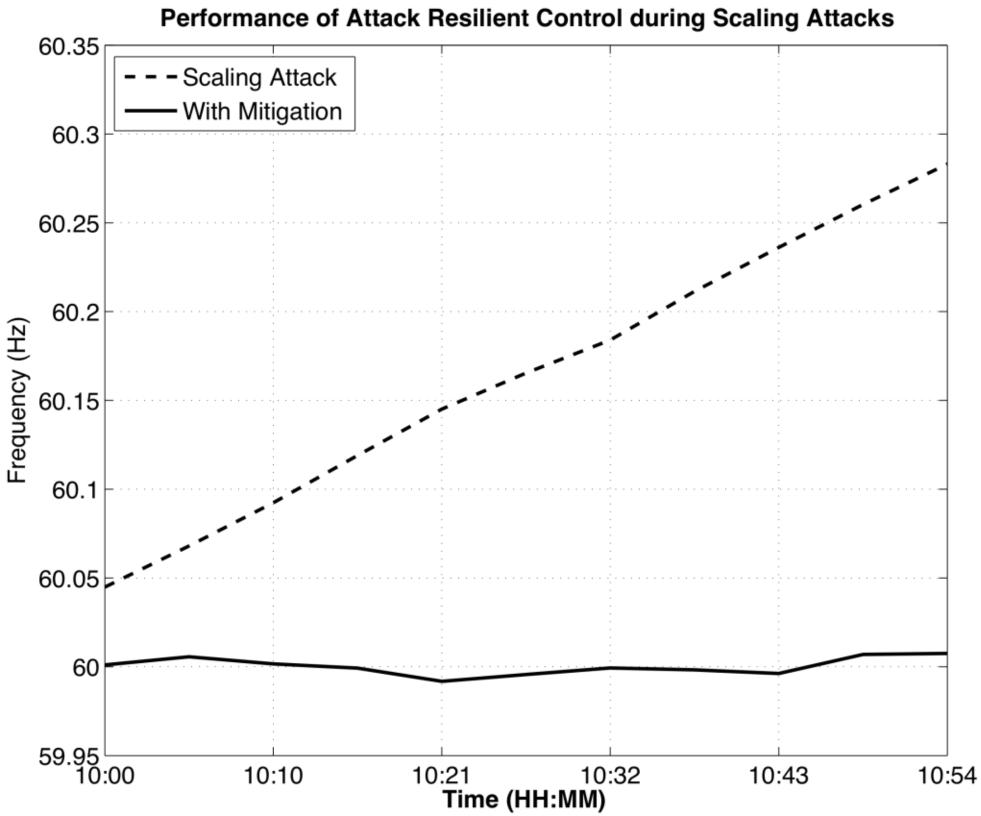
ACE_R – ACE obtained from real-time measurements

ACE_F – ACE obtained from forecast

S. Sridhar and M. Govindarasu, “Model-based attack detection and mitigation for automatic generation control”, IEEE Trans. on Smart Grid, vol. 5, no. 2, March 2014.

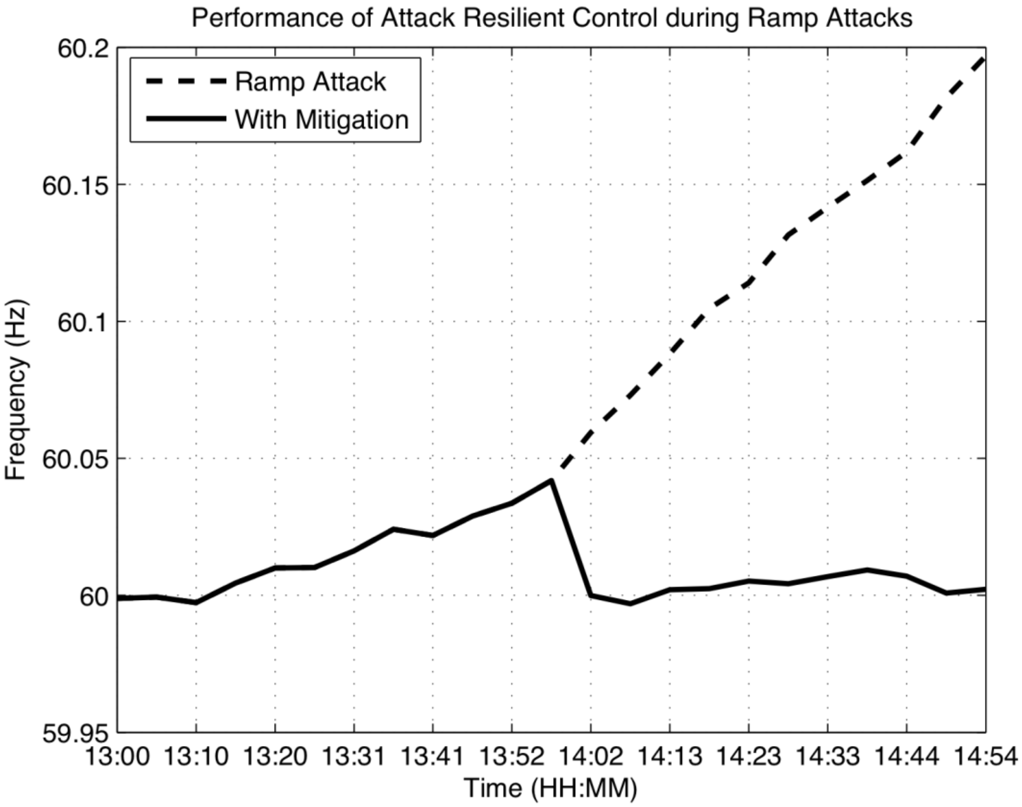
Attack Resilient Control for AGC

Result 1 – ARC during Scaling Attacks



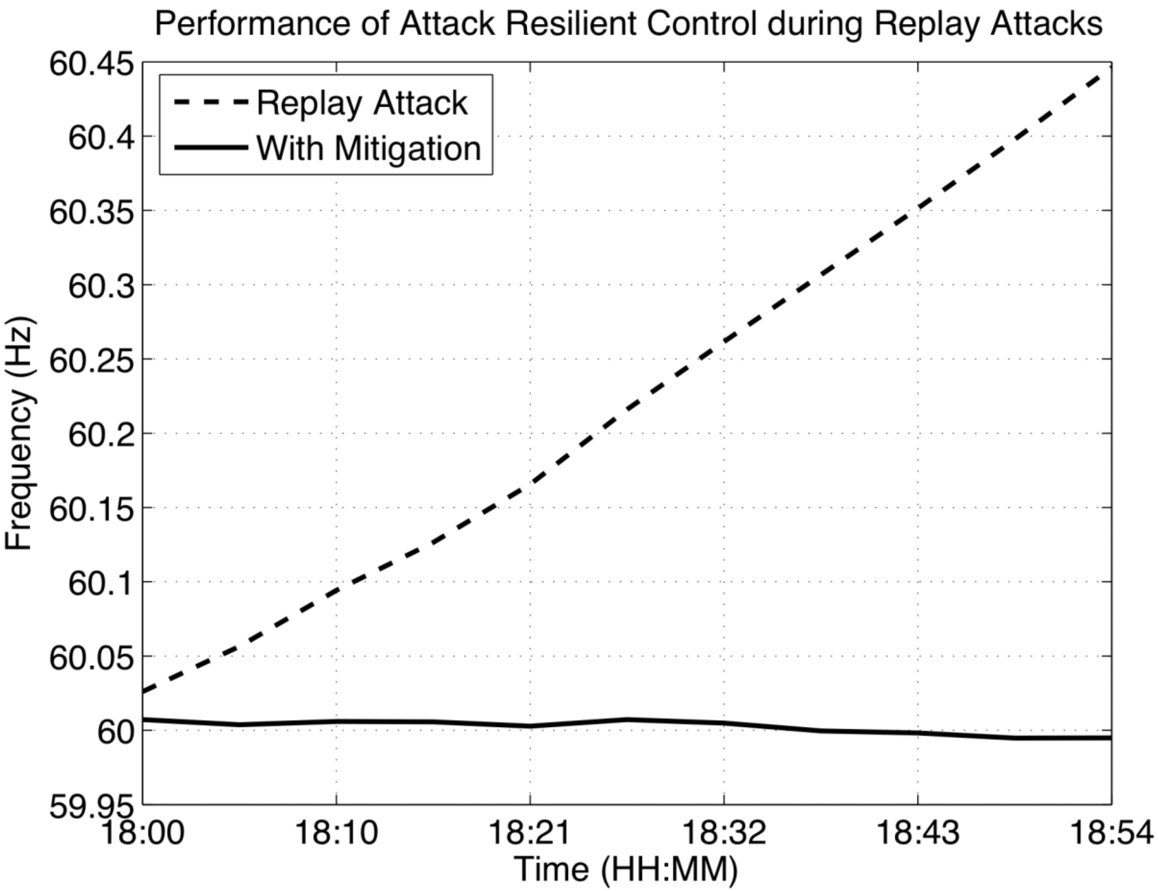
Attack Resilient Control for AGC

Result 2 – ARC during Ramp Attacks

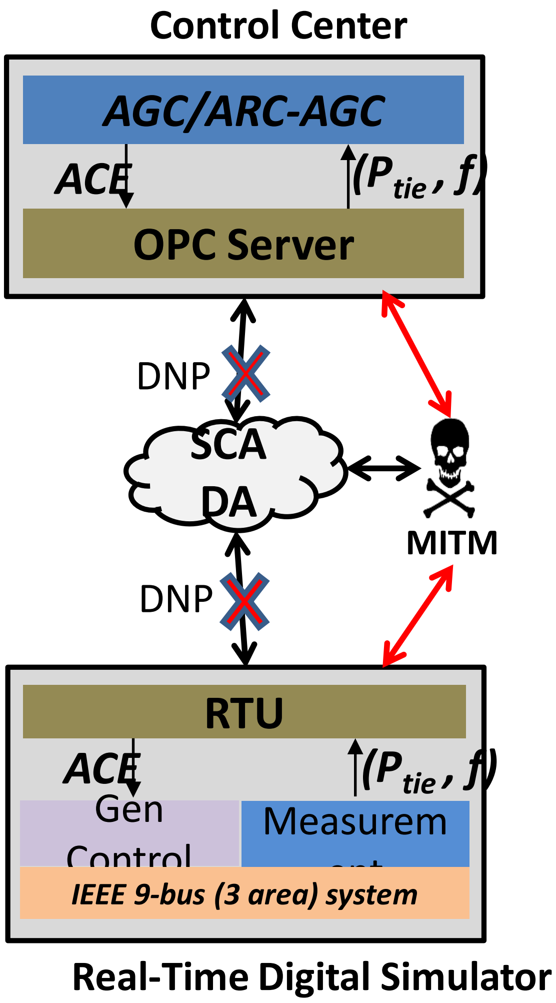


Attack Resilient Control for AGC

Result 3 – ARC during Replay Attacks



Testbed-based Attack-Defense Evaluation for AGC



- ❑ **Control Center**
  - OPC server to exchange measurements/control
  - AGC and ARC-AGC implemented using custom Python code.
- ❑ **SCADA/WAMS**
  - Measurements/control exchanged using DNP3 protocol
- ❑ **Real-Time Digital Simulator**
  - IEEE-9 bus system with 3 control areas modeled in RTDS
  - RTDS interfaced with Siemens RTU to send/receive measurements/control
- ❑ **Attack Execution Details**
  - Man-in-the-middle (MITM) attack performed using ARP spoofing
  - Attacker intercepts message exchange between control system and power system
  - Injects malicious frequency and tie-line flow measurements to AGC

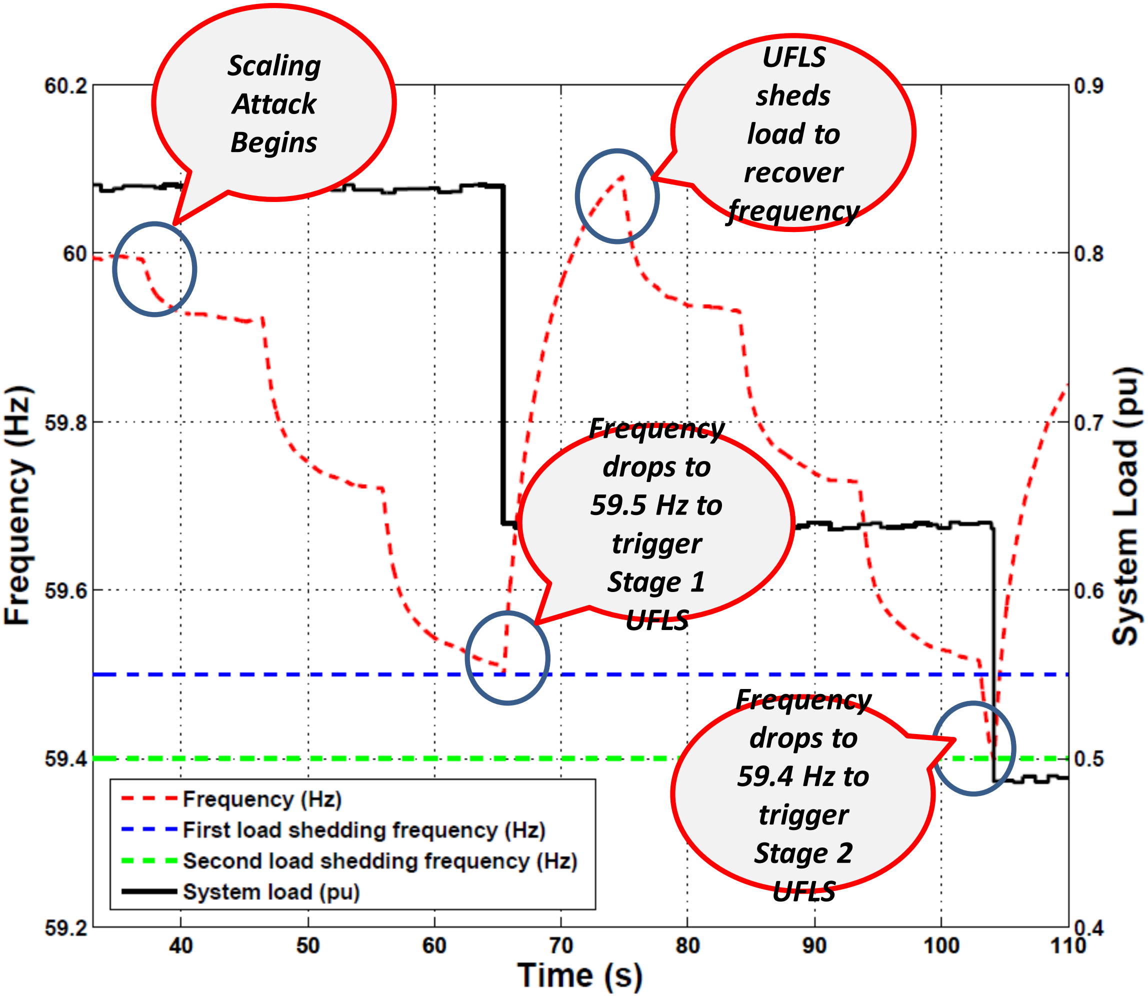
Attack Impact Study on AGC – scaling attack

Experimental setup

- AGC control commands dispatched once every 10 seconds
- Under-frequency load shedding thresholds at 59.5 Hz and 59.4 Hz.

Attack Details

- Scaling attack starts at ~35s
- First load shed occurs at ~65s
- Frequency recovers at ~75s
- Scaling attack continues
- Second load shed occurs at ~105s
- Scaling attack ramps frequency down much faster to shed load

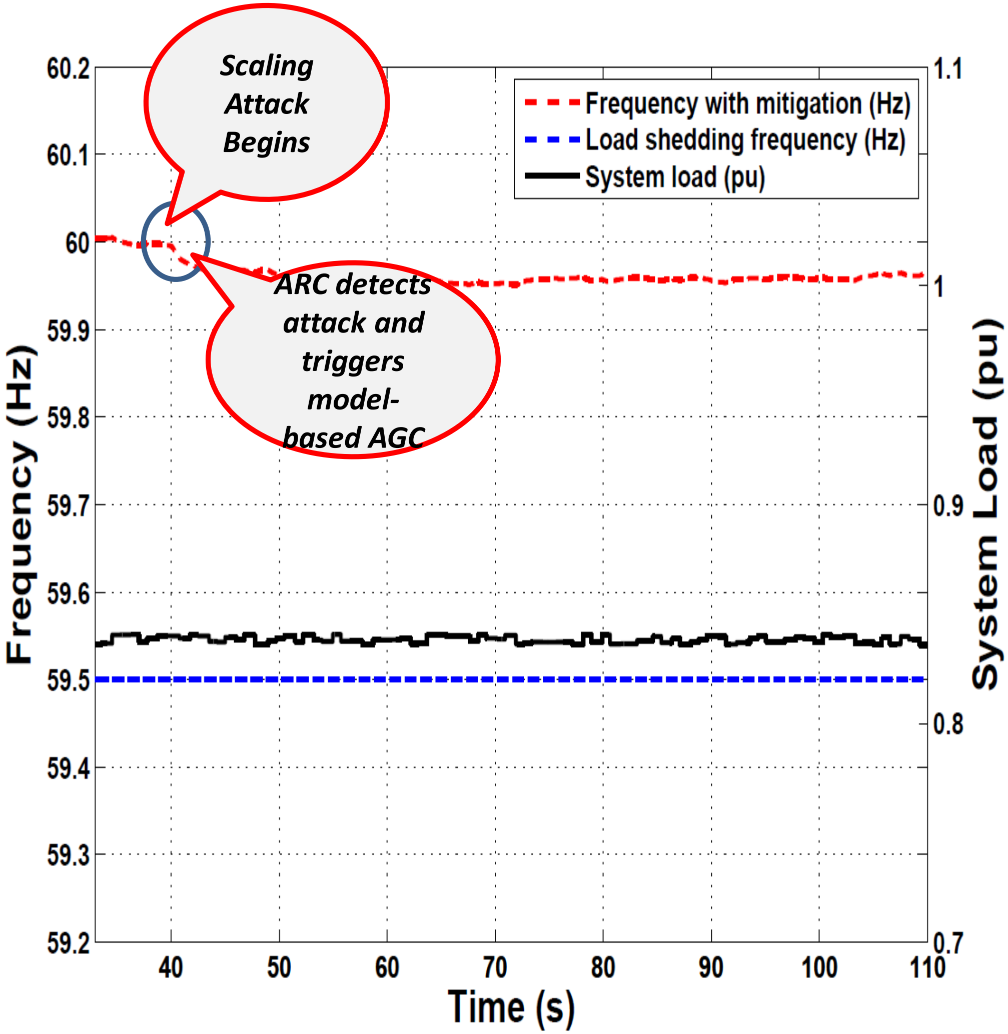


A. Ashok et. al, Testbed-based Evaluation of Attack Detection and Mitigation for AGC, Resilient Week , 2016

AGC with model-based mitigation

Attack-Defense Details

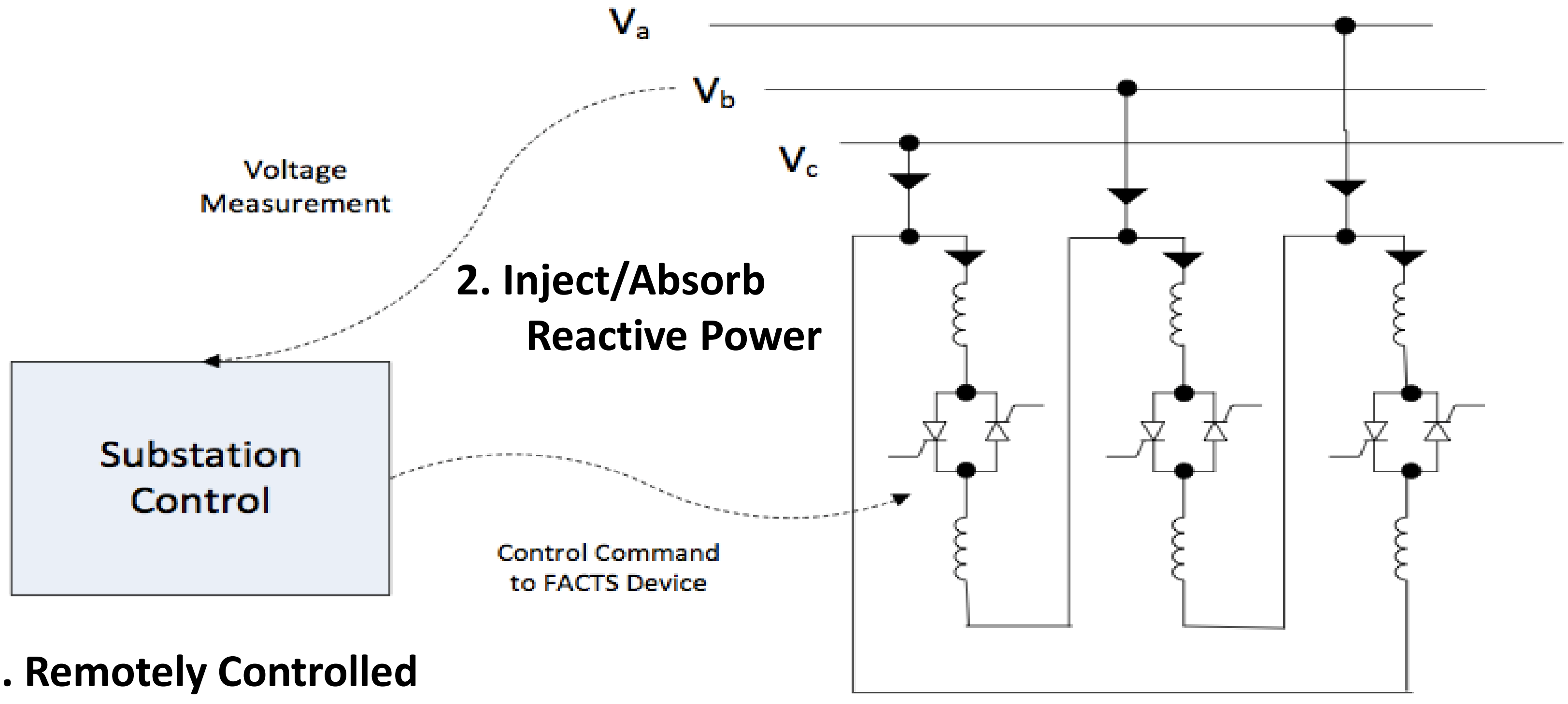
- Scaling attack begins at ~40 seconds
- Scaling attack detection is based on single comparison of ACE with min and max thresholds. Hence, detection is instantaneous.
- ARC detects scaling at ~40 seconds and triggers model-based mitigation.
- ARC prevents load shedding and restores frequency
- Mitigated system frequency is not ideal (closer to 60 Hz) as generator control dispatched using forecasts.



A. Ashok et. al, Testbed-based Evaluation of Attack Detection and Mitigation for AGC, Resilient Week , 2016

Voltage Control Loop - FACTS

1. Connected to Transmission Network



2. Inject/Absorb Reactive Power

3. Remotely Controlled

Three-Phase Thyristor Controlled Reactor

Voltage Control Loop - FACTS

- Attack Vectors (*)
  - Denial of Cooperative Operation
  - Desynchronization (time-based)
  - Data injection

- Data injection attack – Incorrect reactive power injection/absorption

- NERC voltage limit criteria violation

* Source – “Critical Infrastructure Protection”, Eric Goetx and Sujeet Shenoi, Springer 2009

Module 3: Attack-resilient Wide-Area Monitoring, Protection and Control (WAMPAC)

- Wide Area Protection
- Case Study: Remedial Action Scheme (RAS)

Classical Equipment Protection

What to protect?

❑ Generators,
❑ Transformers,
❑ Transmission lines,
❑ Buses,
❑ Capacitors, etc.

What are needed to protect?

❑ CT&PT,
❑ Relaying devices,
❑ Operating devices such as breakers.

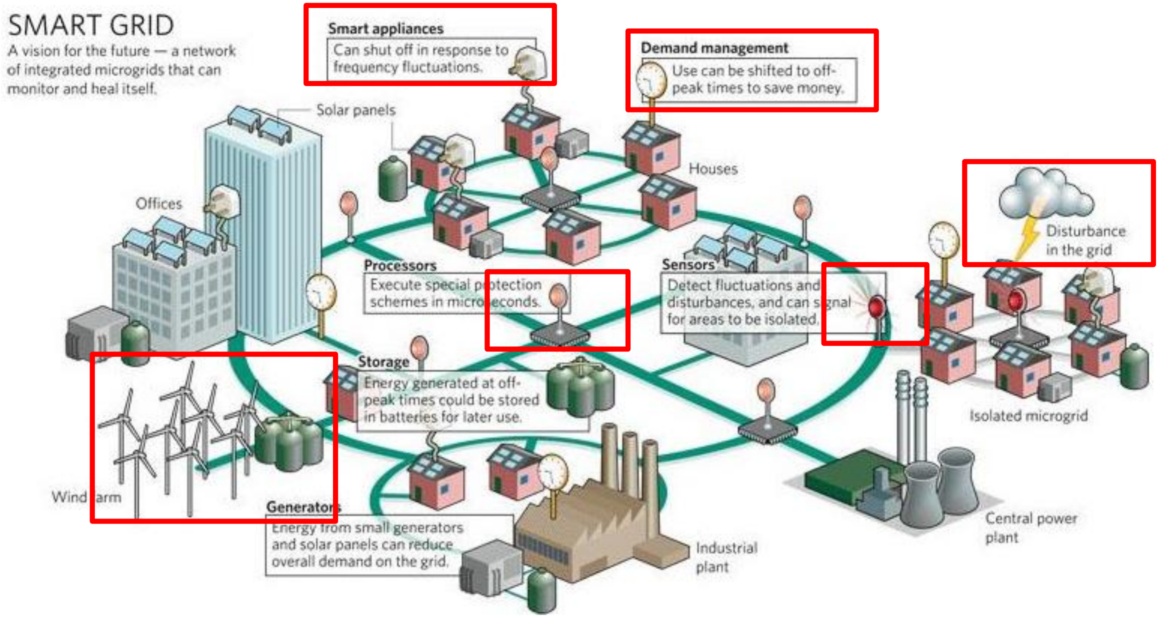
Features?

❑ Local function module,
❑ Data from 1 or 2 substations,
❑ Simple communication.

Power System Protection – importance of communication

“Protection algorithms and control strategy are now getting more and more relying on system-wide information. Therefore, **peer-to-peer communication between substations is in urgent need. ”**

“Meshed peer-to-peer network logical topology is more suitable for wide-area communication than star type.”



SMART GRID
A vision for the future — a network of integrated microgrids that can monitor and heal itself.
Smart appliances
Can shut off in response to frequency fluctuations.
Demand management
Use can be shifted to off-peak times to save money.
Solar panels
Houses
Offices
Disturbance in the grid
Processors
Execute special protection schemes in microseconds.
Sensors
Detect fluctuations and disturbances, and can signal for areas to be isolated.
Storage
Energy generated at off-peak times could be stored in batteries for later use.
Isolated microgrid
Wind farm
Generators
Energy from small generators and solar panels can reduce overall demand on the grid.
Industrial plant
Central power plant

[1] SPECIAL REPORT FOR SC B5 (Protection and Automation), CIGRE 2014

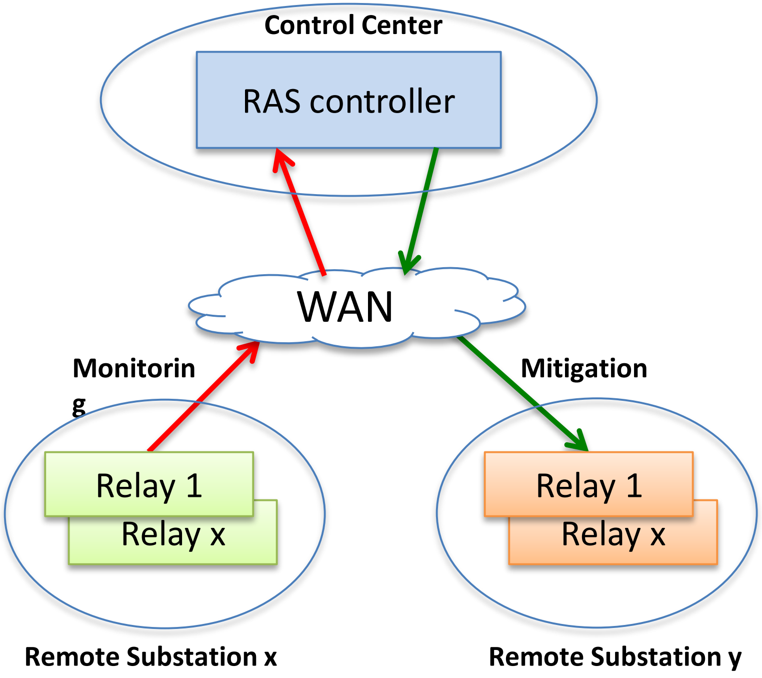
[2] http://www.powergenasia.com/conference/smartmeter.html

Wide-Area Protection

Remedial Action Schemes (RAS) – Automatic protection systems designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability.

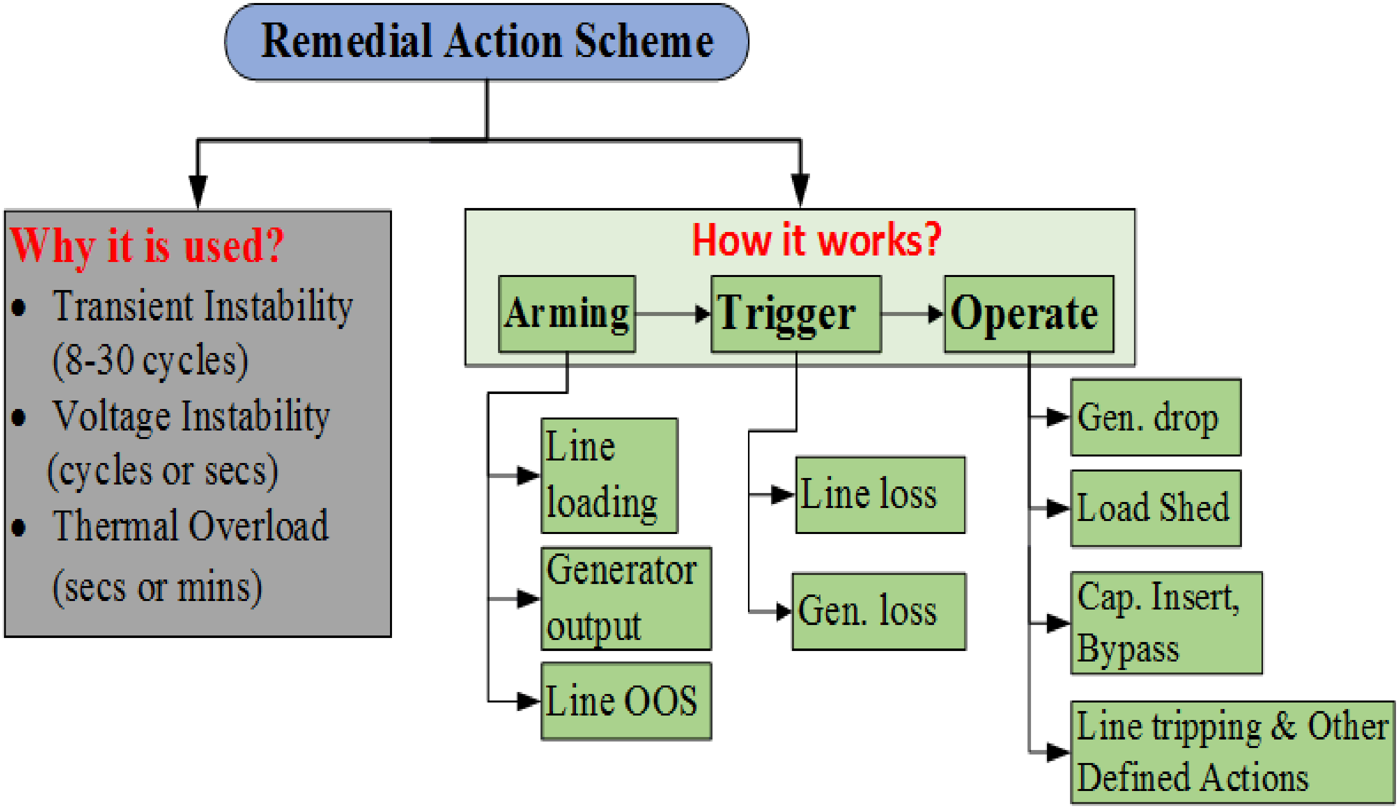
Some typical RAS corrective actions are :

- Changes in load (MW)
- Changes in generation (MW and MVAR)
- Changes in system configuration to maintain system stability, acceptable voltage or power flows



Source: V. Madani, D. Novosel, S. Horowitz, M. Adamiak, J. Amantegui, D. Karlsson, S. Imai, and A. Apostolov, "Ieee psrc report on global industry experiences with system integrity protection schemes (sips)," Power Delivery, IEEE Transactions on, vol. 25, pp. 2143 –2155, oct. 2010.

Wide-Area Protection



Remedial Action Scheme

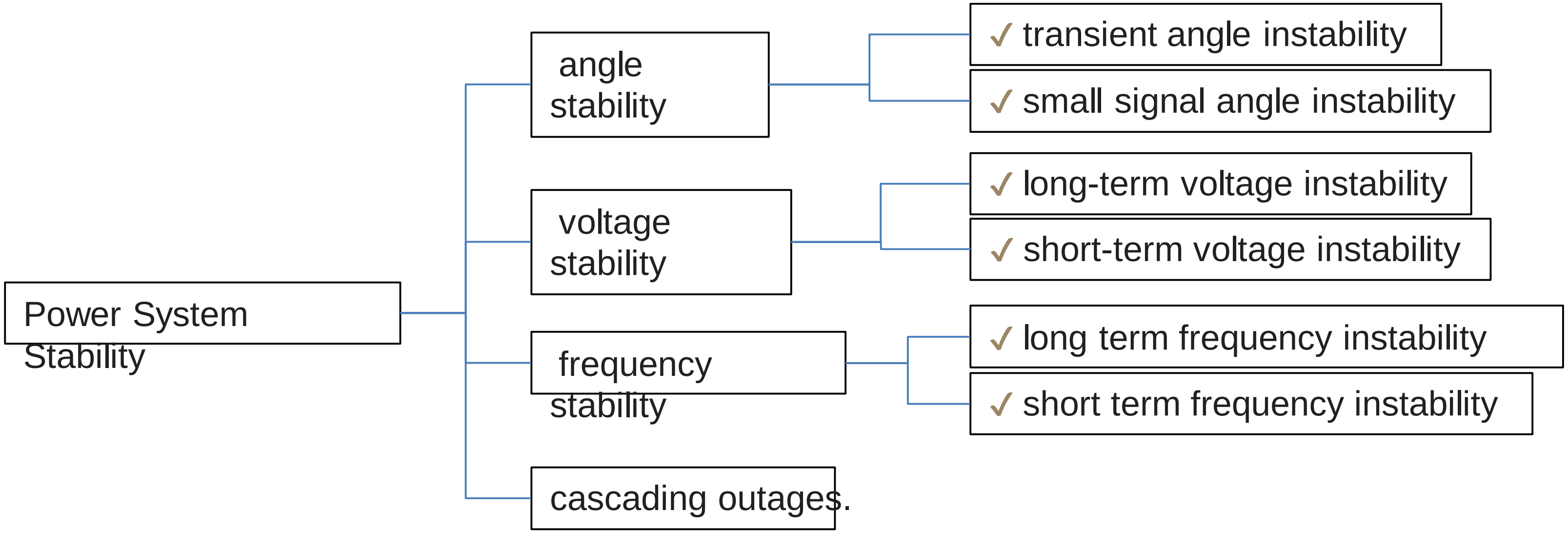
Why it is used?

- Transient Instability (8-30 cycles)
- Voltage Instability (cycles or secs)
- Thermal Overload (secs or mins)

Source: WECC RAS Design Guide, 2006

When would RAS be activated?

"… Such schemes are designed to maintain system stability, acceptable system voltages, acceptable power flows, or to address other reliability concerns. …"[1]


Power System Stability
angle stability
voltage stability
frequency stability
cascading outages.
✓ transient angle instability
✓ small signal angle instability
✓ long-term voltage instability
✓ short-term voltage instability
✓ long term frequency instability
✓ short term frequency instability

[1] http://www.nerc.com/pa/Stand/Prjct201005_2SpclPrtctnSstmPhs2/System_Protection_and_Control_Subcommittee_SPCS_20_SAMS-SPCS_SPS_Technic_02182014.pdf

Typical measurements

- ✓ Rotor angle (transient stability)
- ✓ Rotor speed (transient stability)
- ✓ Voltage magnitude (voltage stability)
- ✓ Frequency (frequency stability)
- ✓ Active power on transmission lines

Typical Remedial Actions

- ✓ Generator tripping (transient stability)
- ✓ Load shedding (transient/voltage/frequency stability)
- ✓ System separation (transient stability, cascading outage)
- ✓ Generation level control (transient/voltage stability)
- ✓ VAR compensation (voltage stability)

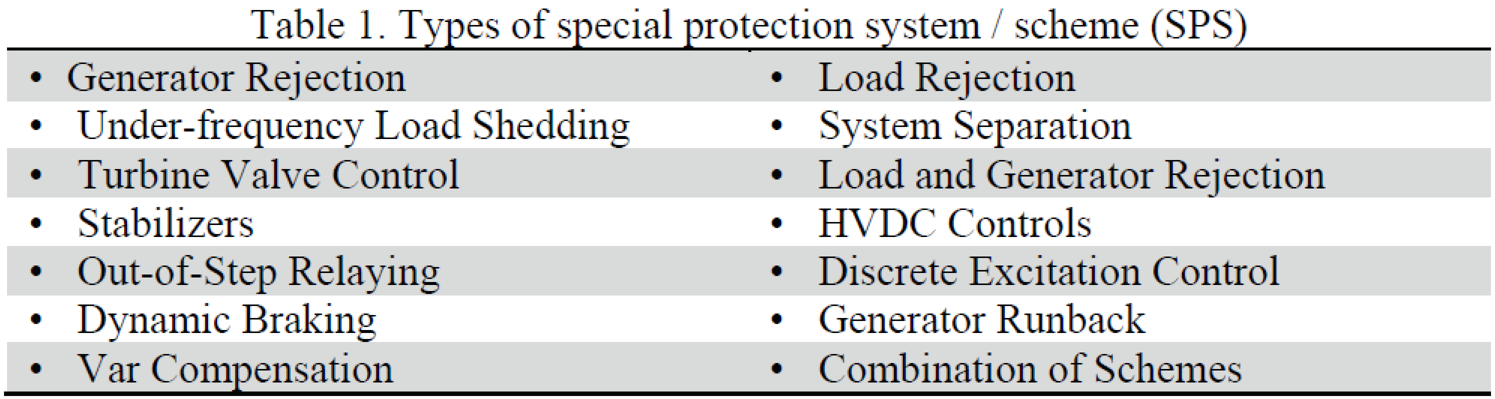
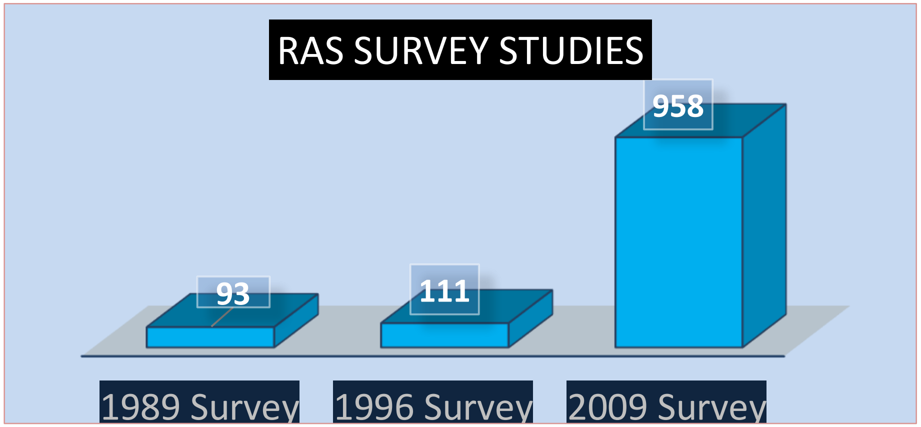


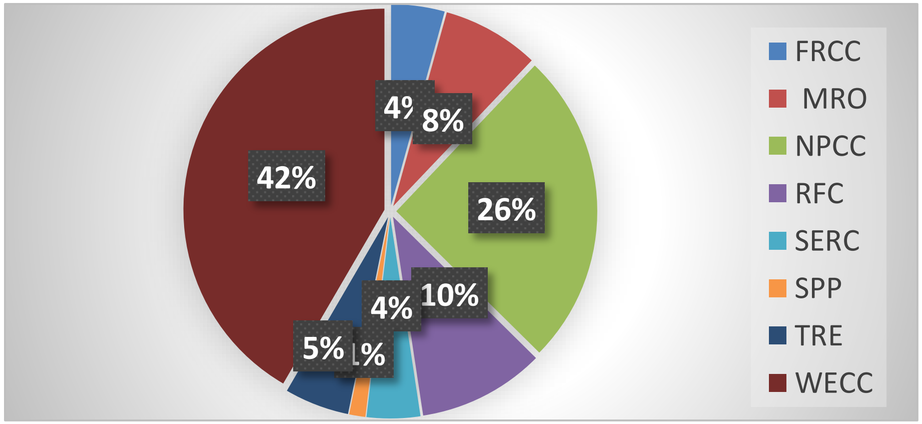
Table 1. Types of special protection system / scheme (SPS)

• Generator Rejection	• Load Rejection
• Under-frequency Load Shedding	• System Separation
• Turbine Valve Control	• Load and Generator Rejection
• Stabilizers	• HVDC Controls
• Out-of-Step Relaying	• Discrete Excitation Control
• Dynamic Braking	• Generator Runback
• Var Compensation	• Combination of Schemes

[1] S. Seo, et al. Development of Intelligent Generator Special Protection System (iG-SPS) to Improve Transient Stability in Dangjin Power Plants, CIGRE, B5-116, 2014.

RAS Deployments Survey (NERC Regions)

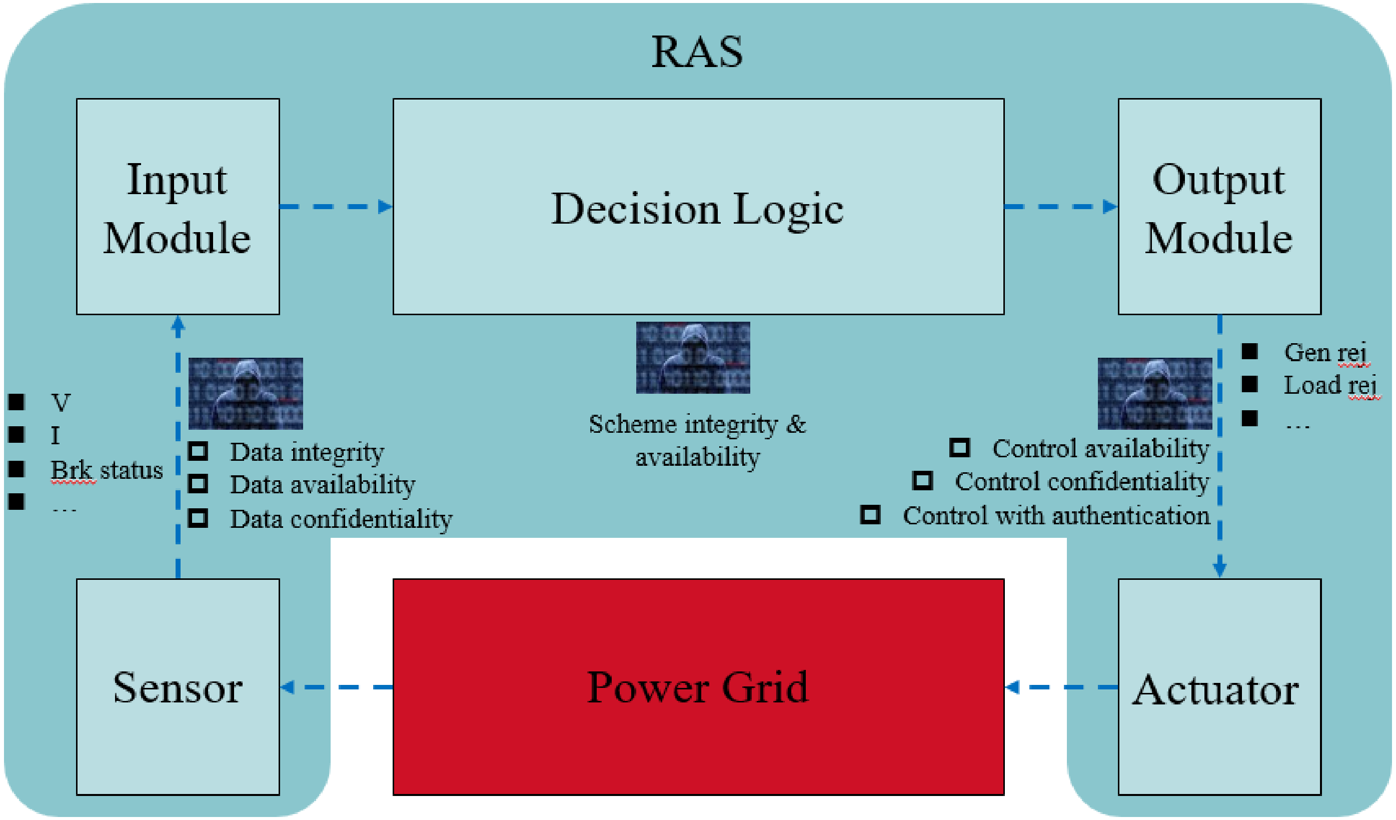




Total RASs by Region (NERC 2012)

Industry	Types of RAS
Southern California Edison, (2013)	Generation tripping, Load tripping, Combination
Idaho Power Company, (2010)	Generation tripping, Bypass/insert Capacitors
Bonneville Power Administration, (2009)	Generation/load tripping, Bypass/Insert Capacitors, others
BC Hydro, (2006)	Generation/line/load tripping, Bypass/insert Capacitors, others

Cyber Security Concerns in protection systems



RAS

Input Module

Decision Logic

Output Module

- V
- I
- Brk status
- …

□ Data integrity
□ Data availability
□ Data confidentiality

Scheme integrity & availability

- Gen rej
- Load rej
- …

□ Control availability
□ Control confidentiality
□ Control with authentication

Sensor

Power Grid

Actuator

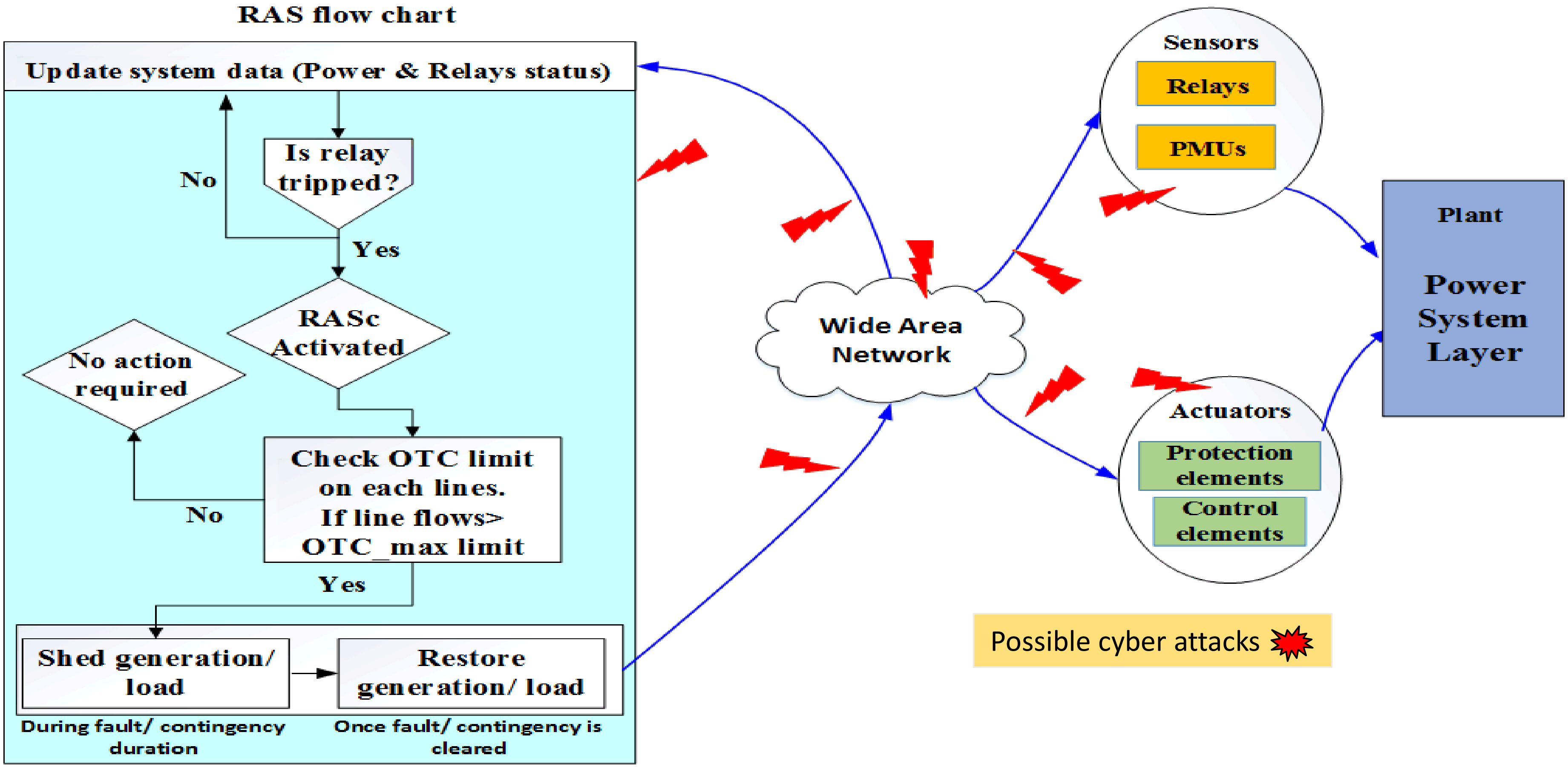
How vulnerable RAS for cyber attacks?

Protection pattern is ***centralization***. Typically, only one centralized controller can send out the control commands. If it is compromised, the function gets lost!

- **Attack targets:** Sensors, controllers, actuators, measurements

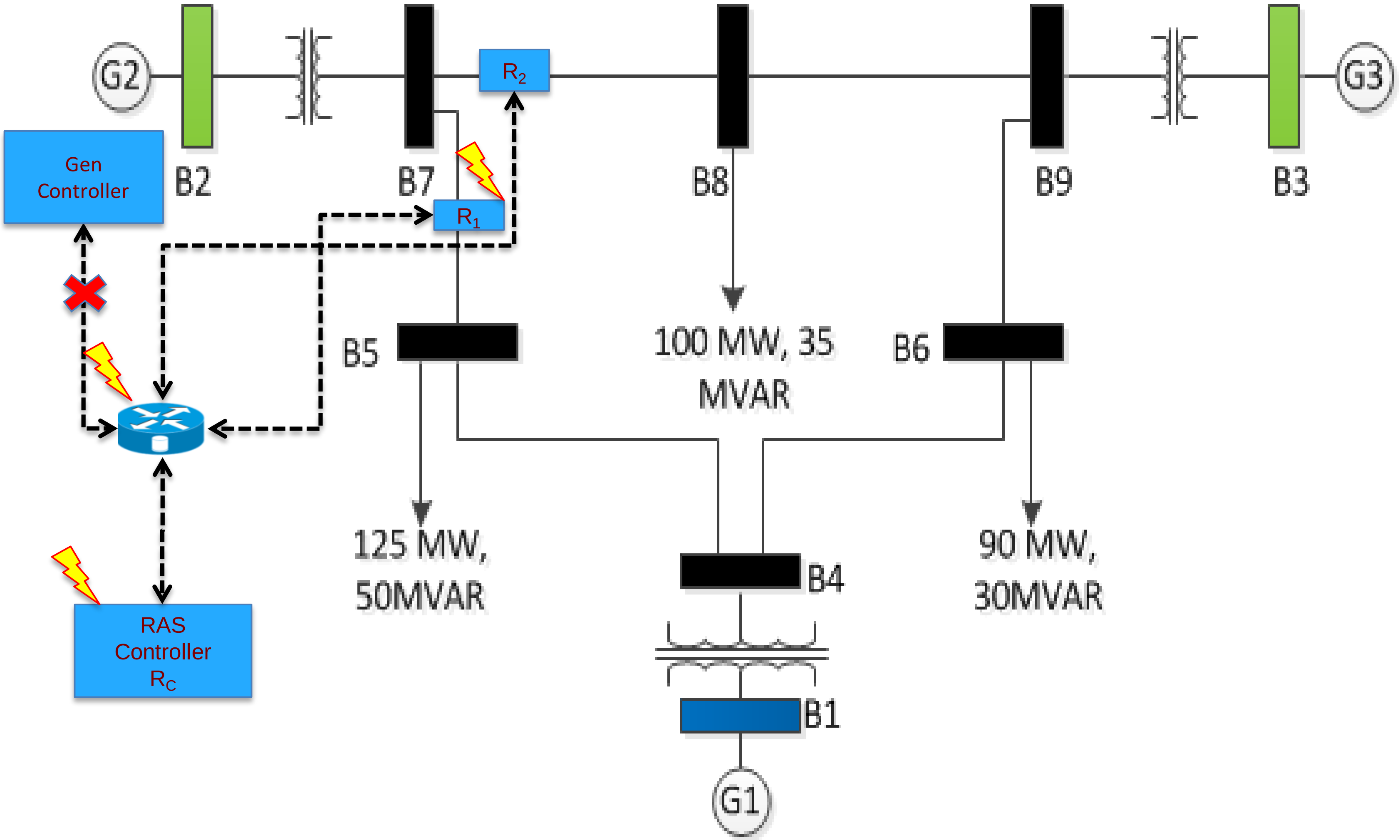
- False data injection – wrong decision
- Replay attack – wrong action
- DoS on controller – control unavailable
- Coordinated attacks
- ….

Wide-Area Protection – Attack Surface



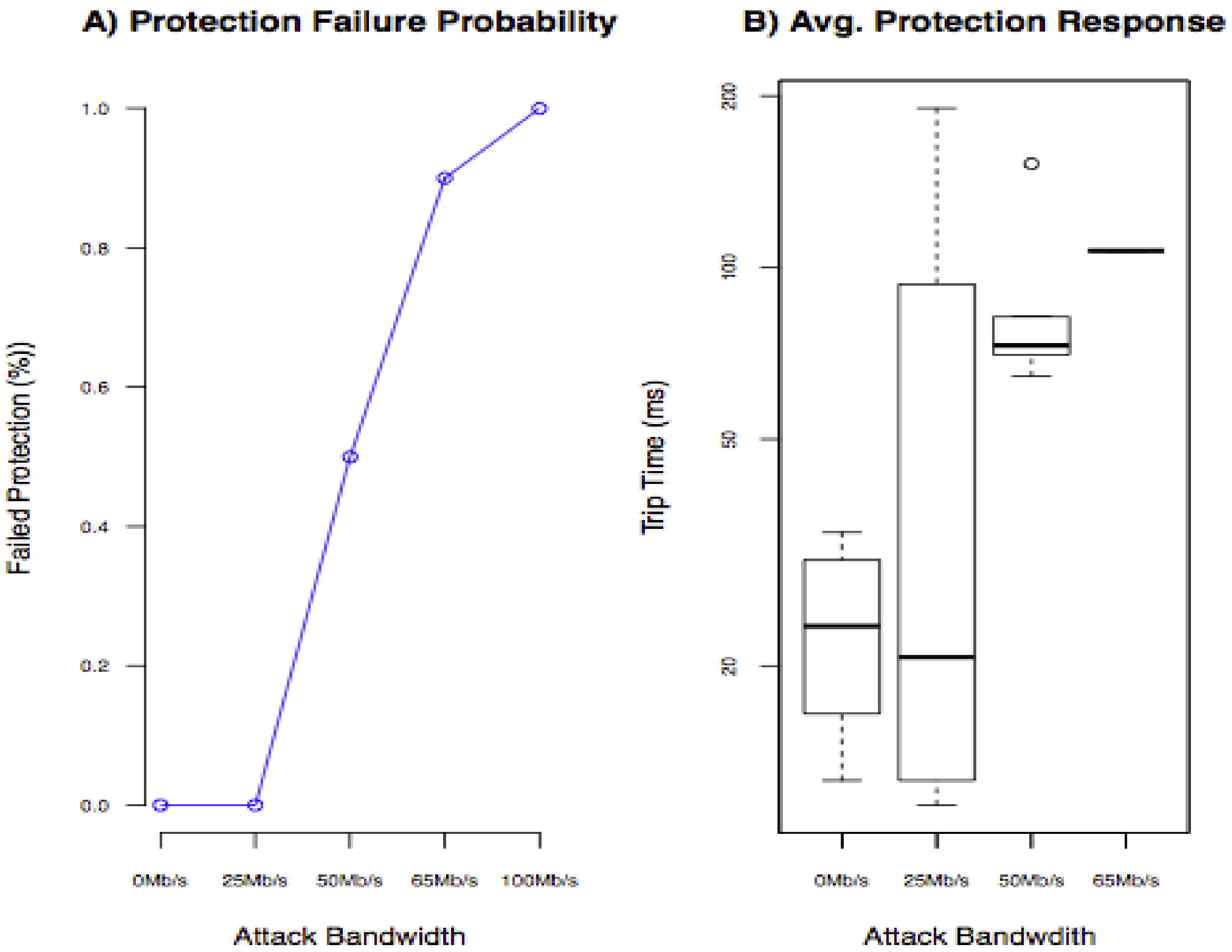
Possible cyber attacks

Case Study: Coordinated attack on RAS (WECC 9-bus)



A. Ashok, A. Hahn, S. Siddharth, and M. Govindarasu, “Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid, IEEE Trans. on Smart Grid, June 2013

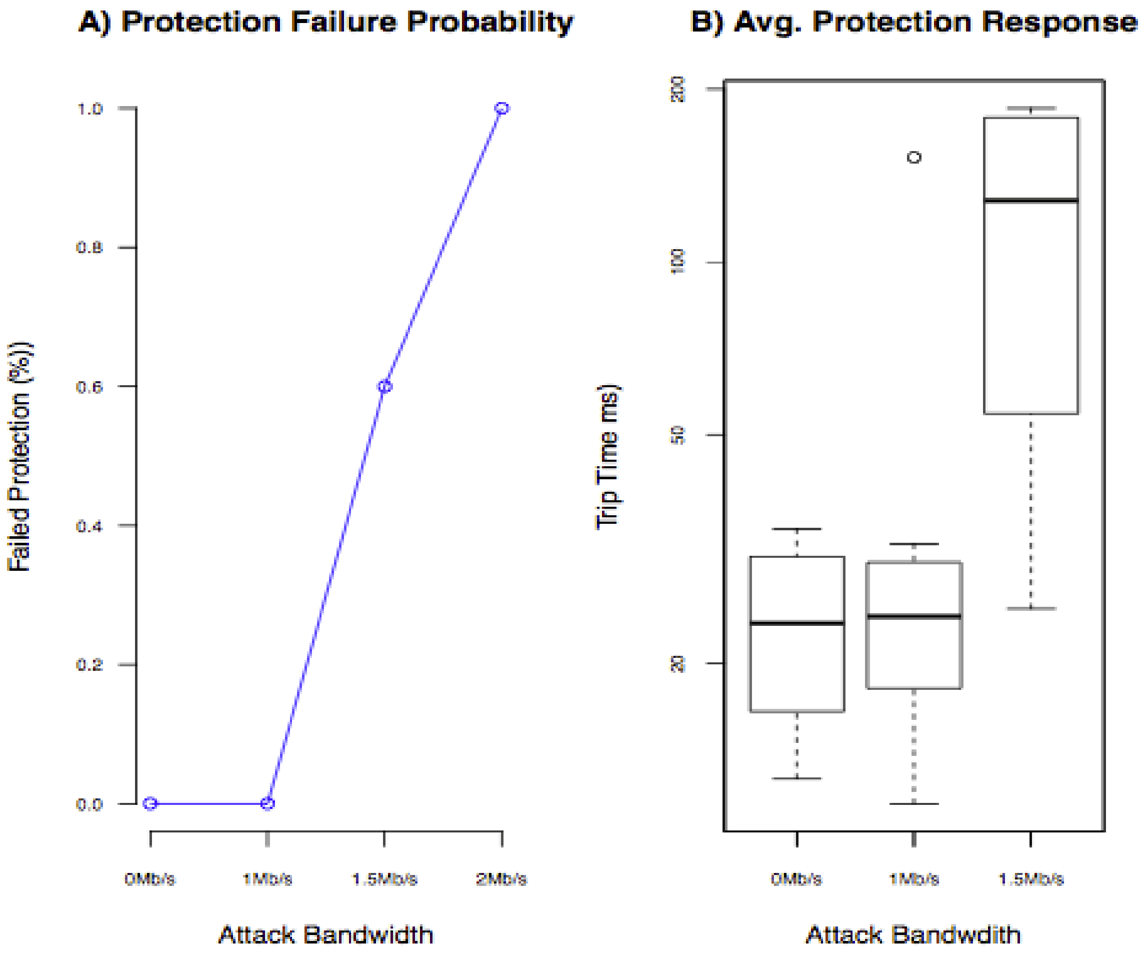
DoS on network router in RAS – protection failiure



A) Protection Failure Probability

B) Avg. Protection Response

DoS on RAS Controller (Relay) – protection failure

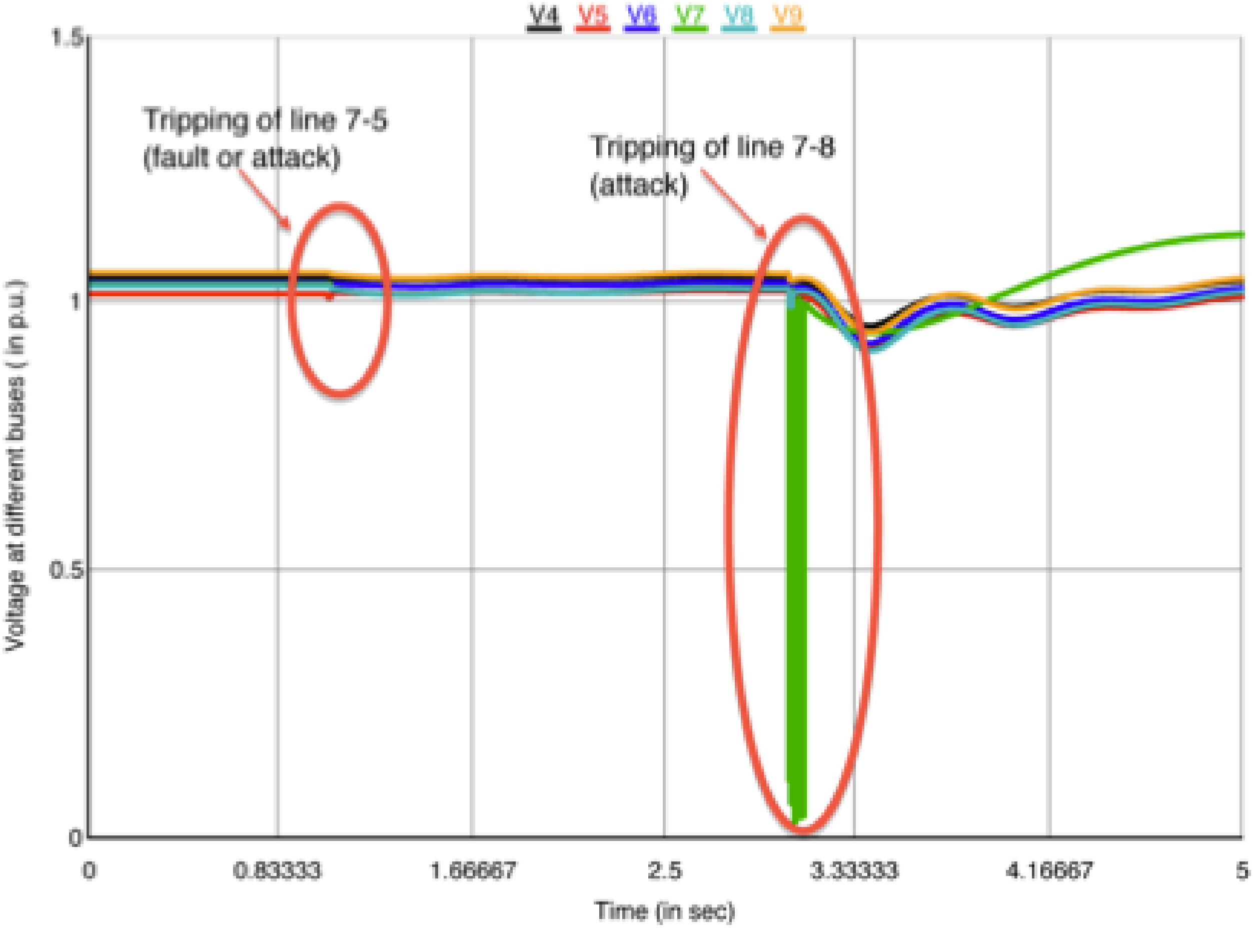


A) Protection Failure Probability

B) Avg. Protection Response

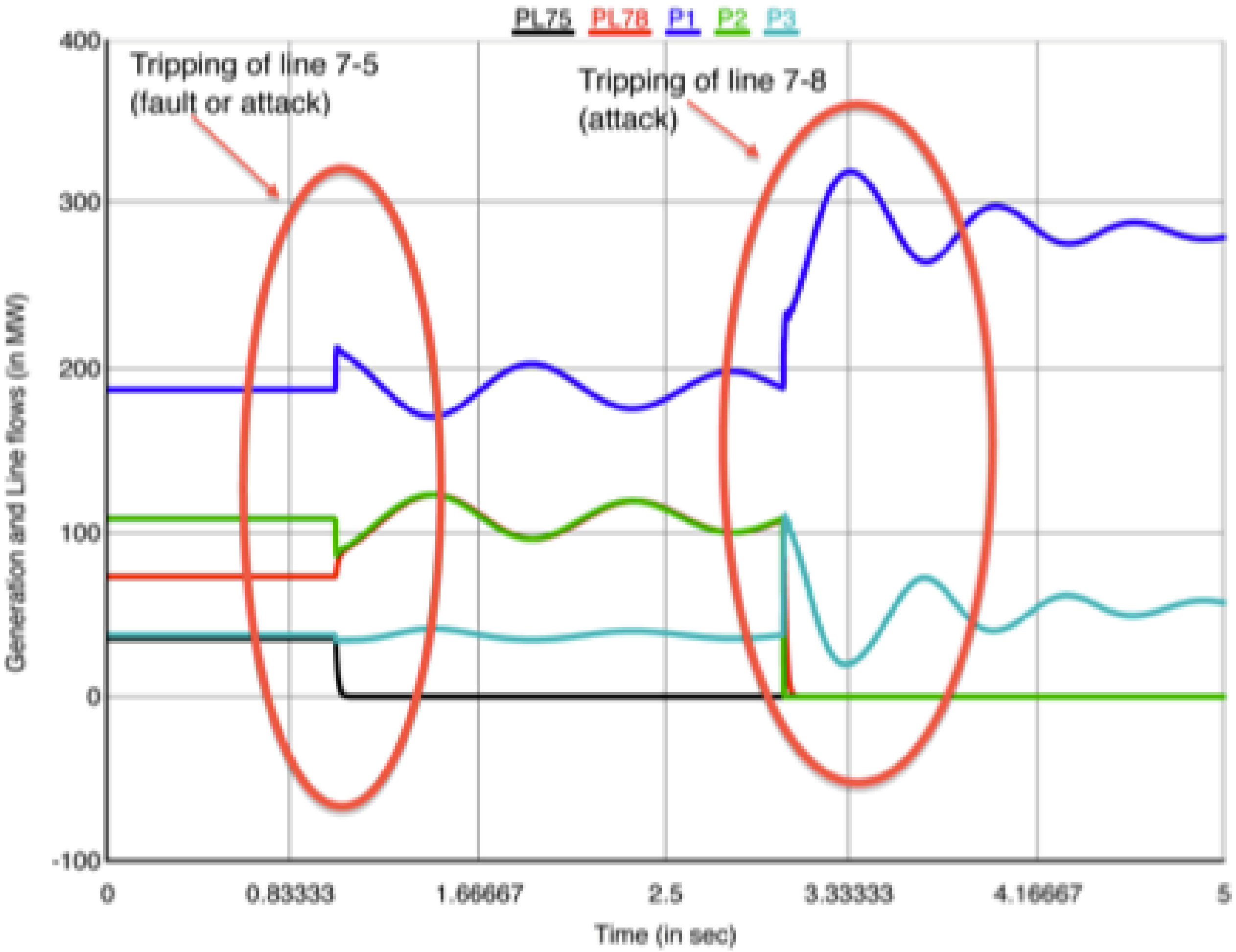
Power System Impacts

Impact on System Voltages



Power System Impacts

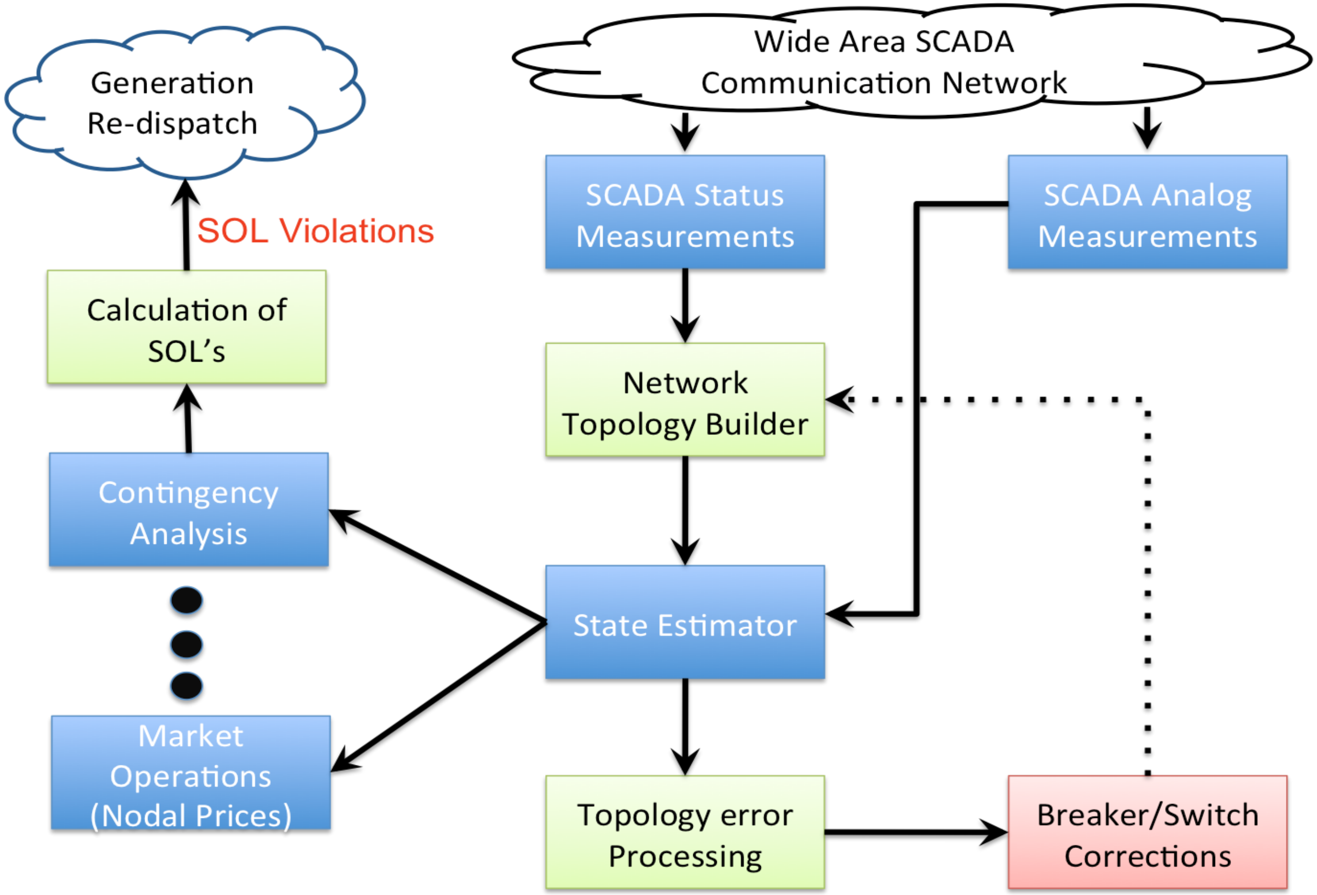
Impact on System Generation and Power flows



Module 3: Attack-resilient Wide-Area Monitoring, Protection and Control (WAMPAC)

Case study: State Estimation (Monitoring)

State Estimation Overview

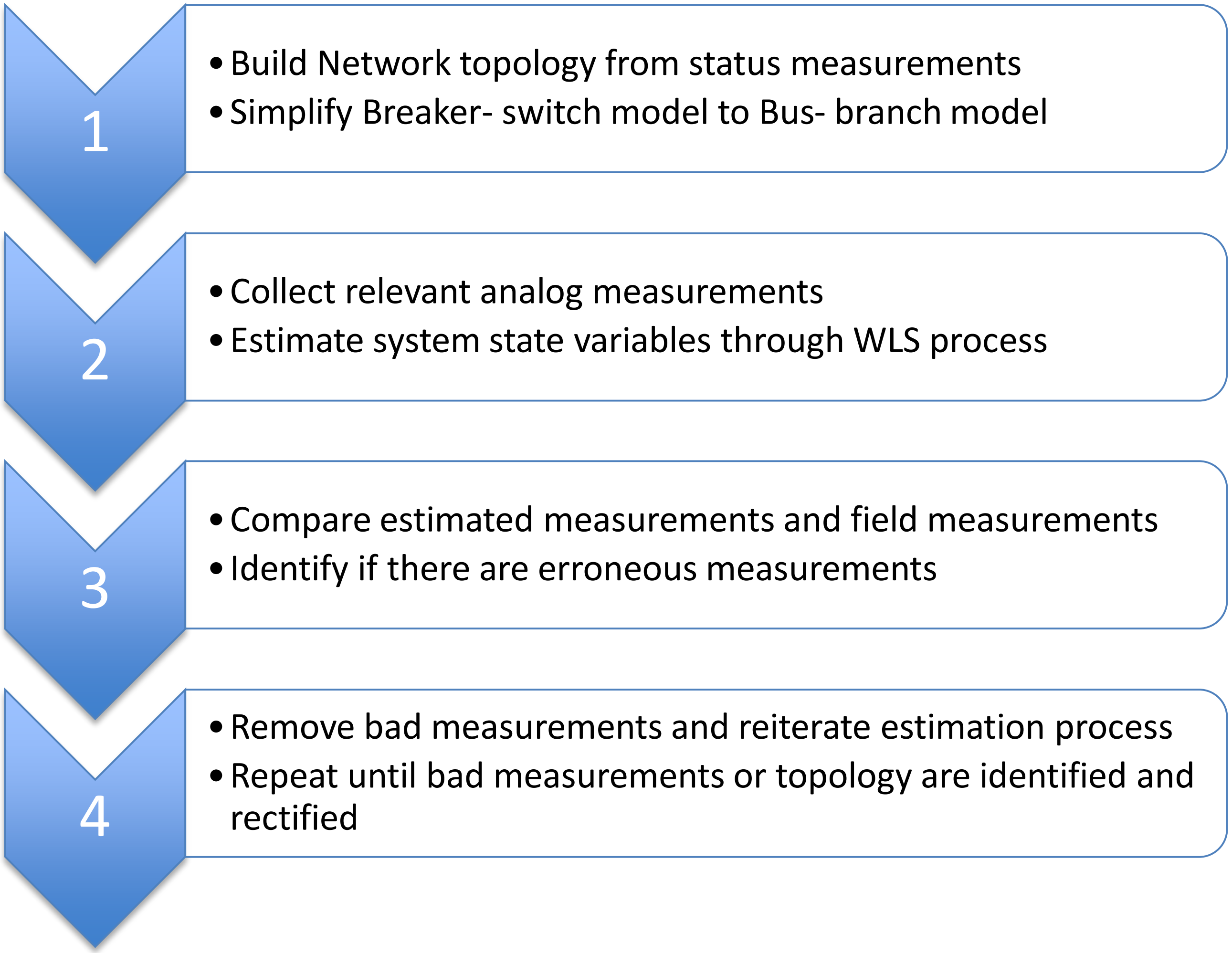

Generation Re-dispatch
SOL Violations
Calculation of SOL's
Contingency Analysis
Market Operations (Nodal Prices)
Wide Area SCADA Communication Network
SCADA Status Measurements
SCADA Analog Measurements
Network Topology Builder
State Estimator
Topology error Processing
Breaker/Switch Corrections

Input of State Estimation

- Analog Measurements
  - Real Power on transmission lines (P)
  - Reactive Power on transmission lines (Q)
  - Real and Reactive Power injection at buses (P_{inj}, Q_{inj})

- System State Variables
  - Voltages and phase angles at all buses (V_{mag} and V_{ang})

State Estimation : Detailed Process



1

- Build Network topology from status measurements
- Simplify Breaker- switch model to Bus- branch model

2

- Collect relevant analog measurements
- Estimate system state variables through WLS process

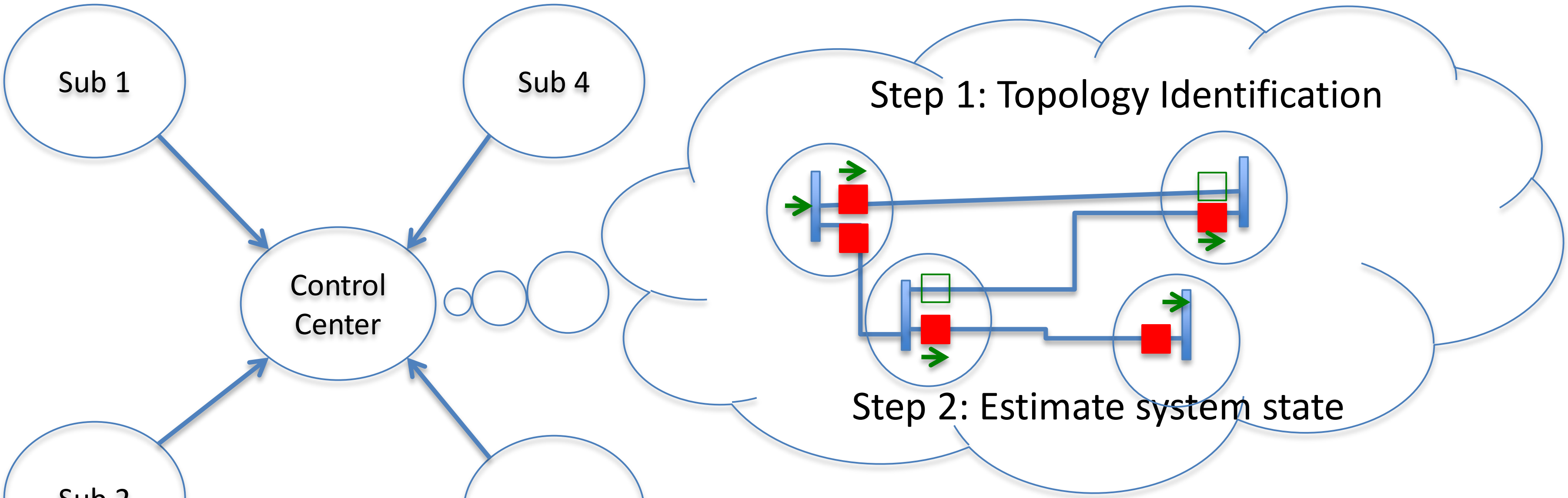
3

- Compare estimated measurements and field measurements
- Identify if there are erroneous measurements

4

- Remove bad measurements and reiterate estimation process
- Repeat until bad measurements or topology are identified and rectified

Obtain the Topology

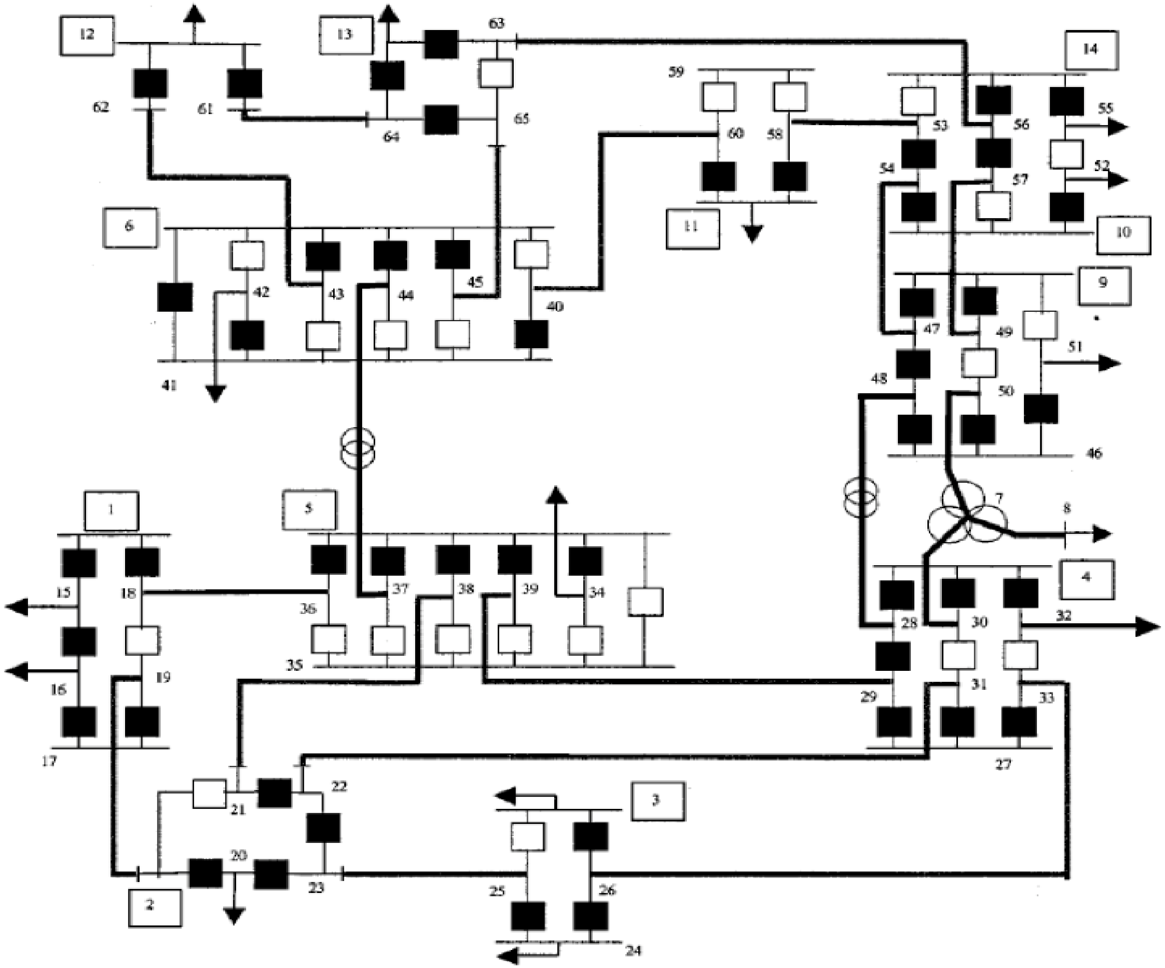

Sub 1
Sub 4
Control Center
Sub 2
Sub 3
Step 1: Topology Identification
Step 2: Estimate system state

‘n’ states in the system

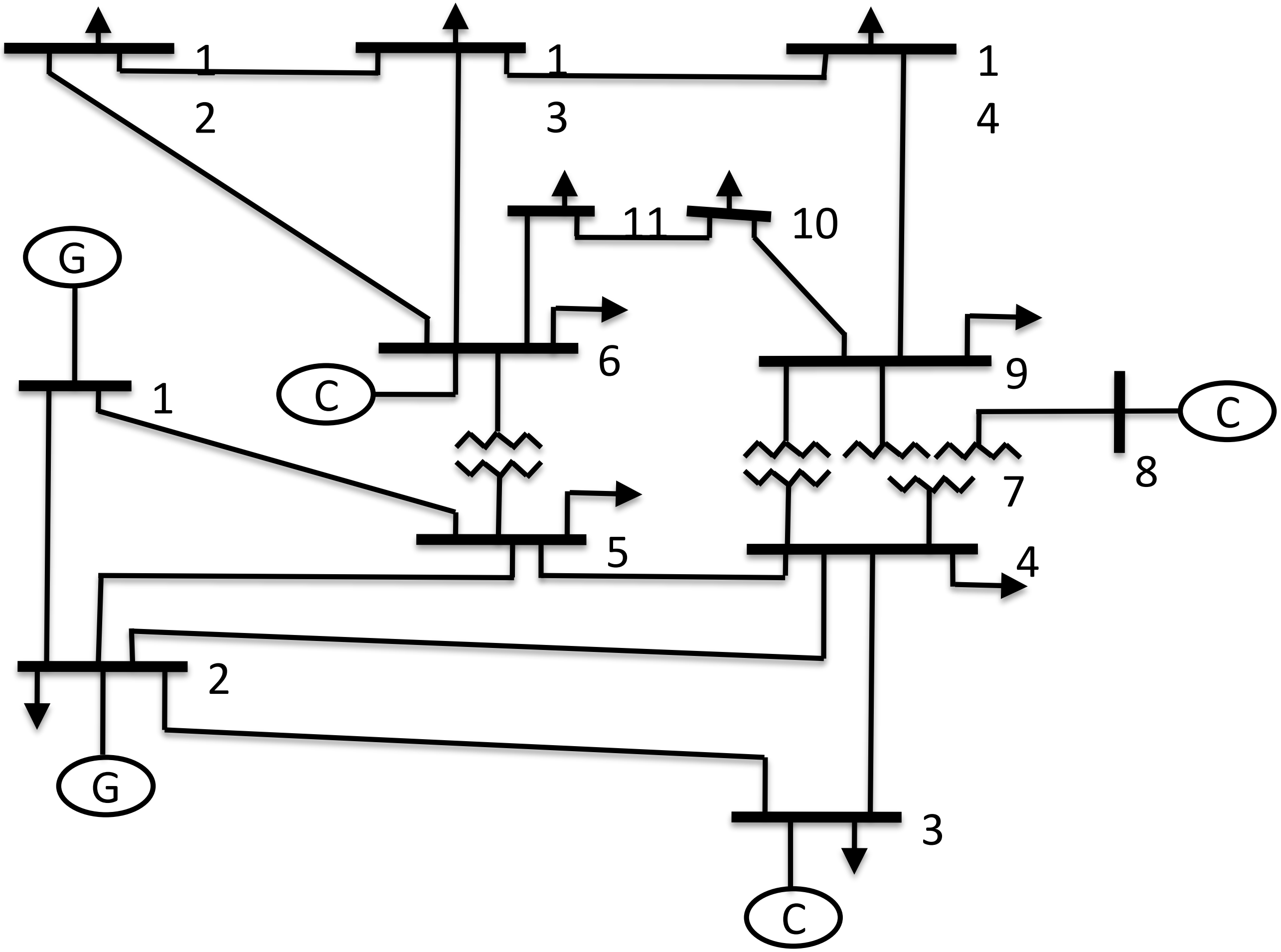
‘m’ measurements available in the system

Weighted Least Squares (WLS): Minimize the error of the measurements and the estimates subject to satisfying power system equations

Breaker- Switch Model: IEEE 14 bus model



Bus – Branch Model : IEEE 14 bus model



State Estimation Methodology

Under DC power flow model, the relation between states and measurements can be written as:

$$\boxed{z = Hx + e}$$

z is the vector of measurements

H is the measurement Jacobian matrix

x is the vector of states (phase angles)

e is the vector of measurement errors

$$\boxed{\hat{x} = \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} z}$$

$\hat{x}$ is the vector of estimated state variables

R is the measurement covariance matrix

$$\boxed{r = z - H\hat{x}}$$

r is the measurement residual

‘m’ measurements to estimate ‘n’ states

State Estimation Bad Data Detection

Weighted Least Squares (WLS) algorithm

Minimize the error of the measurements and the estimates subject to satisfying power flow equations

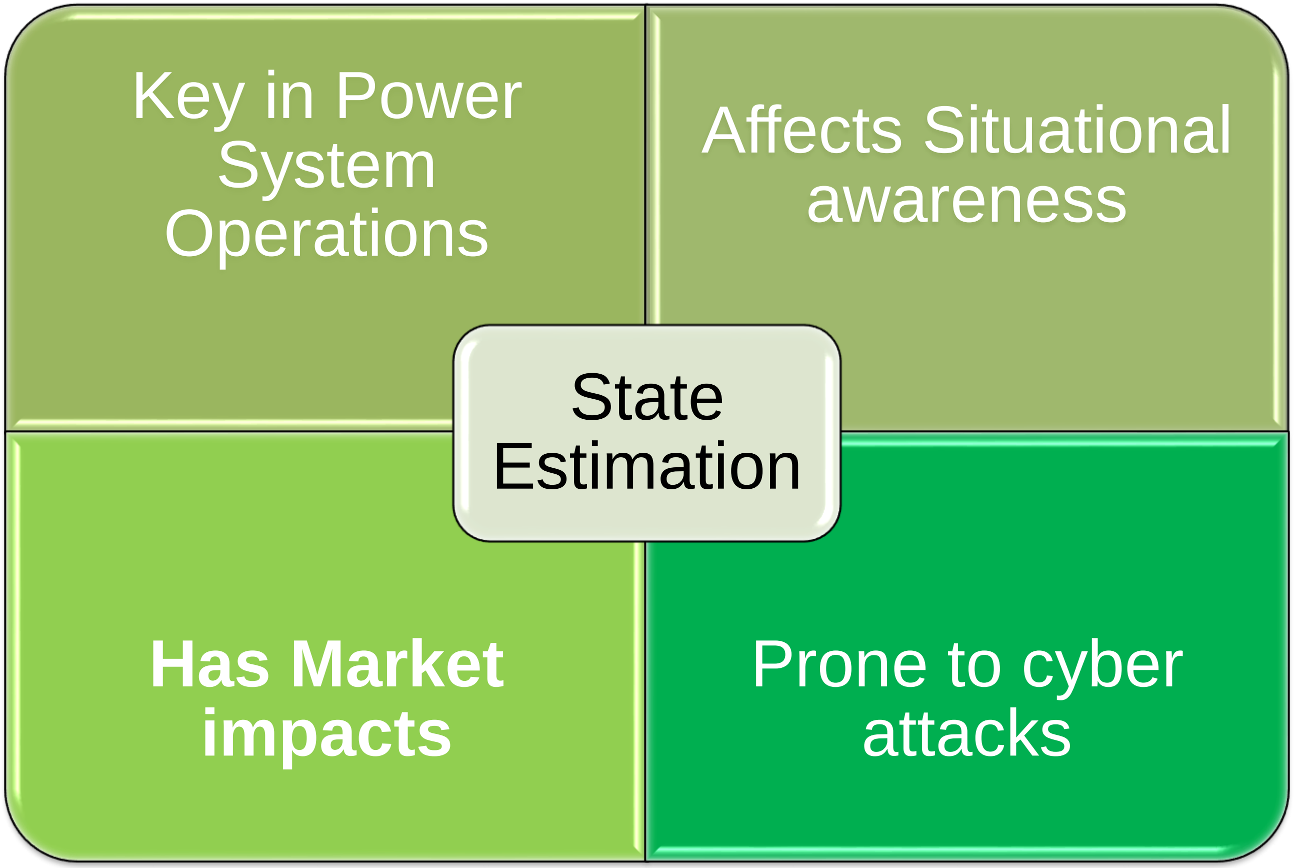
Bad Data Detection: Normalized residual test

$$\boxed{r = z - H\hat{x}}$$

Measurements considered bad if residuals do not meet this condition

$$\boxed{\left|z - H\hat{x}\right| R^{-1} \pounds\, t}$$

Cyber attacks on State Estimation



Key in Power System Operations

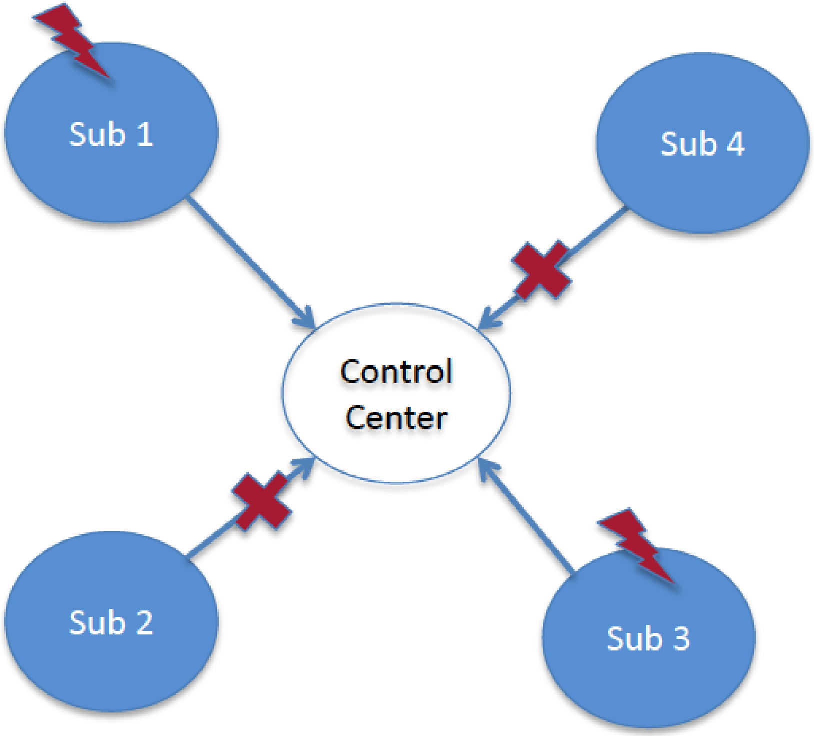
Affects Situational awareness

State Estimation

Has Market impacts

Prone to cyber attacks

Cyber attacks on State Estimation



Attack types

-Data Integrity attacks

-DoS attacks

Attack targets

-Analog measurements

-Status measurements

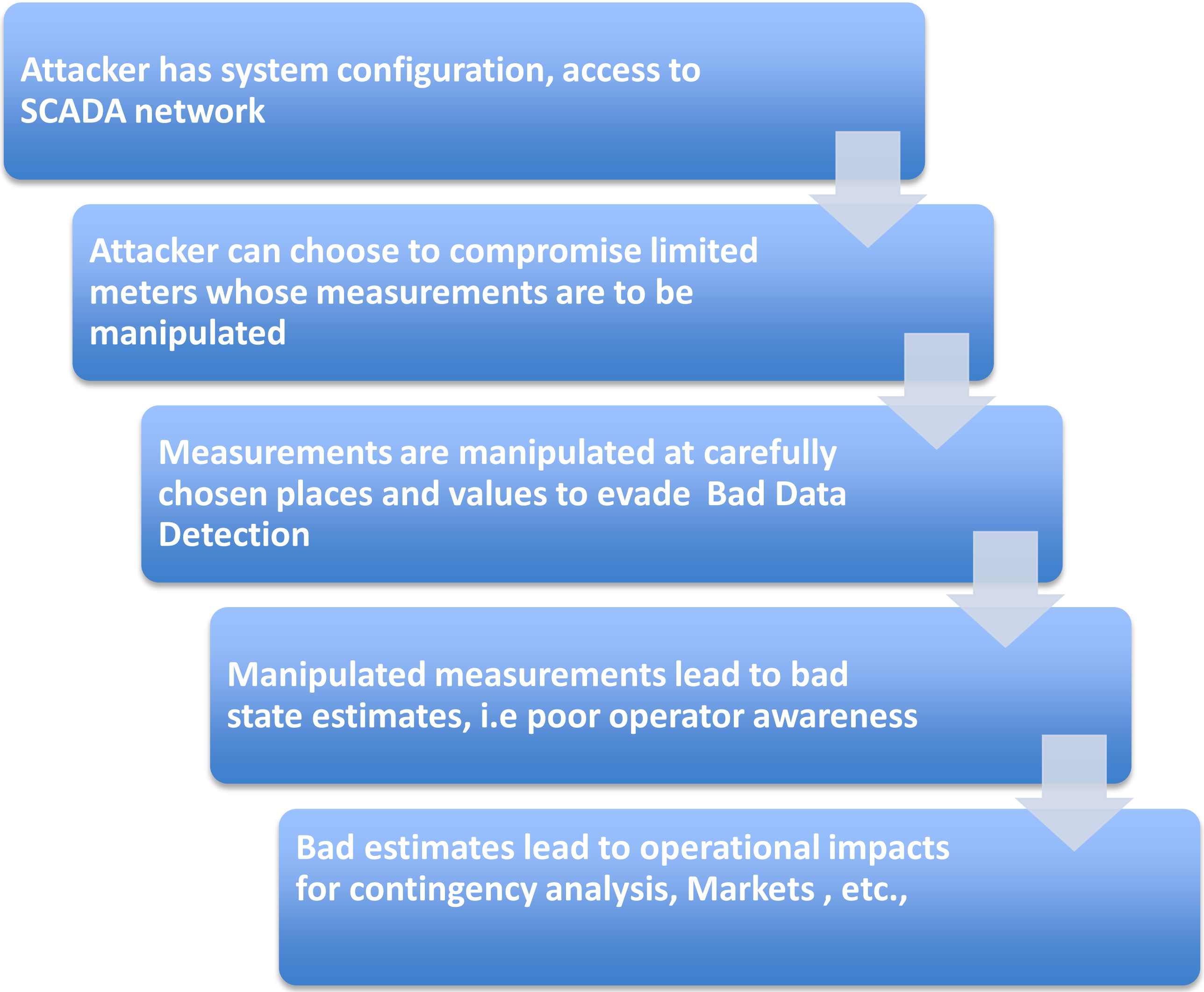
Creating Smart topology attacks

- **Naïve attack**: Manipulate the status of an arbitrary field device like relay/breaker to cause topology error
  - Detected by Bad Data Detection in State Estimator
- **Intelligent attack**: Manipulate the status of a field device corresponding to a critical measurement
  - Critical measurements impact system observability
  - Cause no change in measurement residuals

Types of Cyber attacks on State Estimation

- Attacks on Network Topology
  - Cause system operator to assume wrong network and therefore cause error in calculations
- Attacks on Network Measurements
  - Cause system operator to believe the system operating state in something else rather than reality, i.e no situational awareness

Attacks on Network Measurements



Attacker has system configuration, access to SCADA network

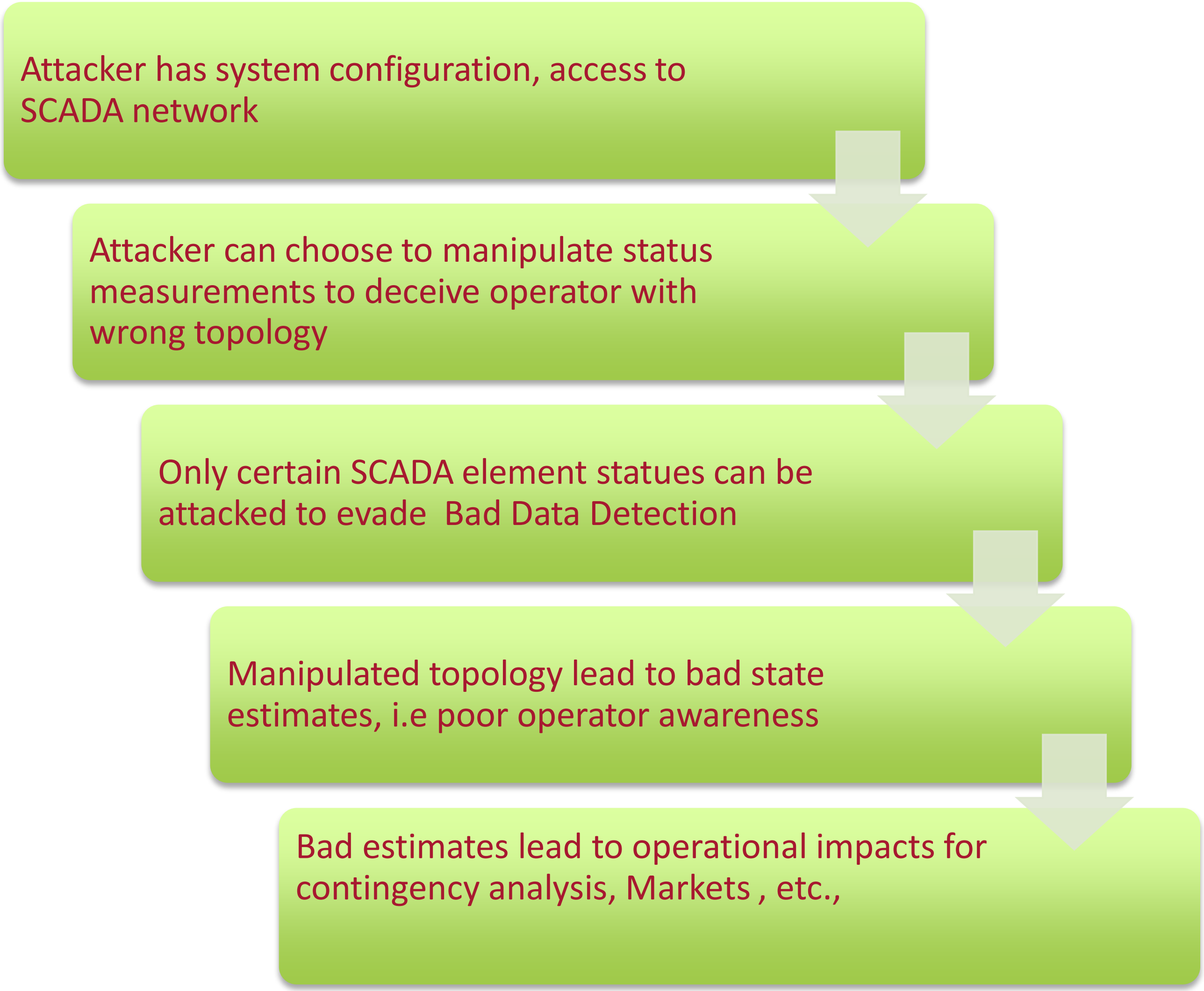
Attacker can choose to compromise limited meters whose measurements are to be manipulated

Measurements are manipulated at carefully chosen places and values to evade Bad Data Detection

Manipulated measurements lead to bad state estimates, i.e poor operator awareness

Bad estimates lead to operational impacts for contingency analysis, Markets , etc.,

Attacks on Network Topology



Attacker has system configuration, access to SCADA network

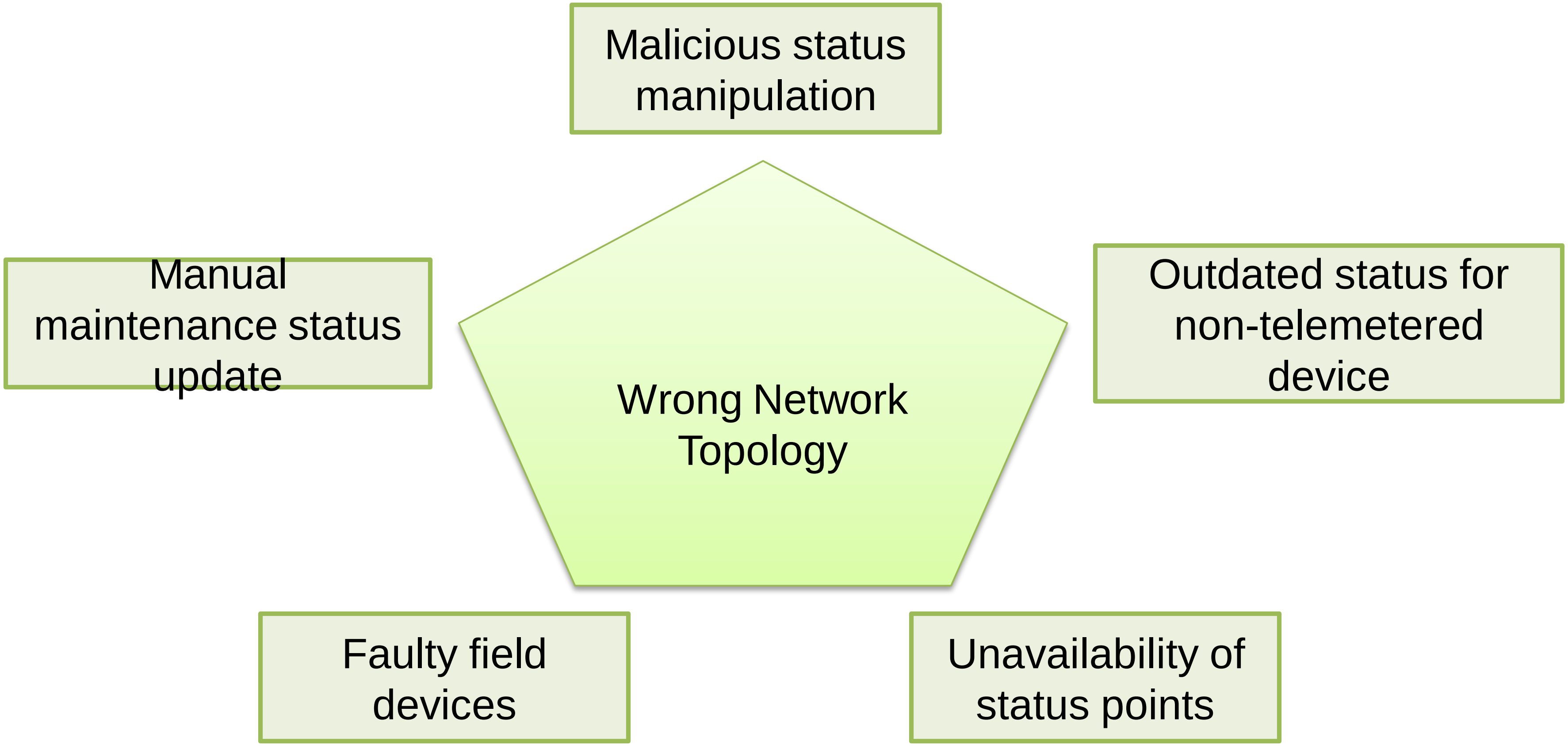
Attacker can choose to manipulate status measurements to deceive operator with wrong topology

Only certain SCADA element statues can be attacked to evade Bad Data Detection

Manipulated topology lead to bad state estimates, i.e poor operator awareness

Bad estimates lead to operational impacts for contingency analysis, Markets , etc.,

Causes of Wrong Network Topology



Malicious status manipulation

Manual maintenance status update

Wrong Network Topology

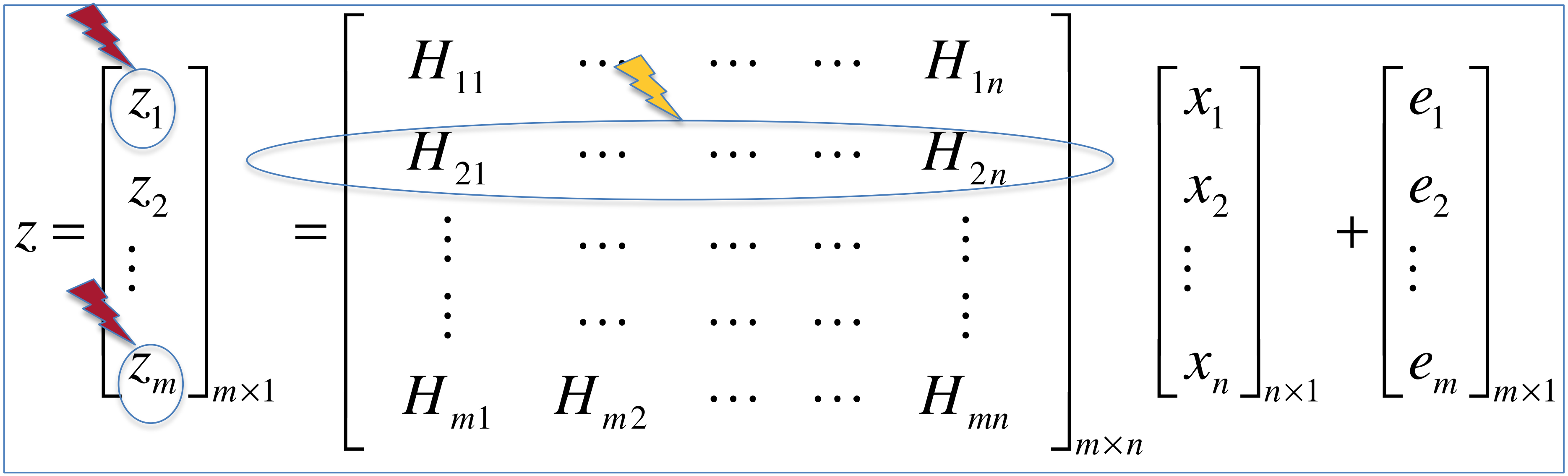
Outdated status for non-telemetered device

Faulty field devices

Unavailability of status points

Cyber Attacks on State Estimation

$$\boxed{z = Hx + e}$$



$$z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix}_{m\times 1} = \begin{bmatrix} H_{11} & \cdots & \cdots & \cdots & H_{1n} \\ H_{21} & \cdots & \cdots & \cdots & H_{2n} \\ \vdots & \cdots & \cdots & \cdots & \vdots \\ \vdots & \cdots & \cdots & \cdots & \vdots \\ H_{m1} & H_{m2} & \cdots & \cdots & H_{mn} \end{bmatrix}_{m\times n} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}_{n\times 1} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix}_{m\times 1}$$

⚡ Data integrity attacks on analog measurements

⚡ Data integrity attacks on status measurements

Attacker has measurement configuration, H

Cyber Attack Model (1)

Attack on analog measurements

$$\boxed{z = Hx + e} \qquad \boxed{z_a = z + a = H\hat{x}_{attack} + e}$$

For an attack to evade bad data detection

$$\boxed{\left| z_a - H\hat{x}_{attack} \right| R^{-1} = \left| z + a - H\left(\left(H^T R^{-1} H\right)^{-1} H^T R^{-1}(z + a)\right) \right| R^{-1}}$$

$$= \left| z - H\hat{x} + \left(a - H\left(H^T R^{-1} H\right)^{-1} H^T R^{-1} a\right) \right| R^{-1}$$

$$= \left| z - H\hat{x} \right| R^{-1} \pounds\, t, \quad if \quad a = Hc$$

c is any constant vector.

* Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in Proceedings of the 16th ACM conference on Computer and communications security, ser. CCS '09. New York, NY, USA

Cyber Attack Model (2)

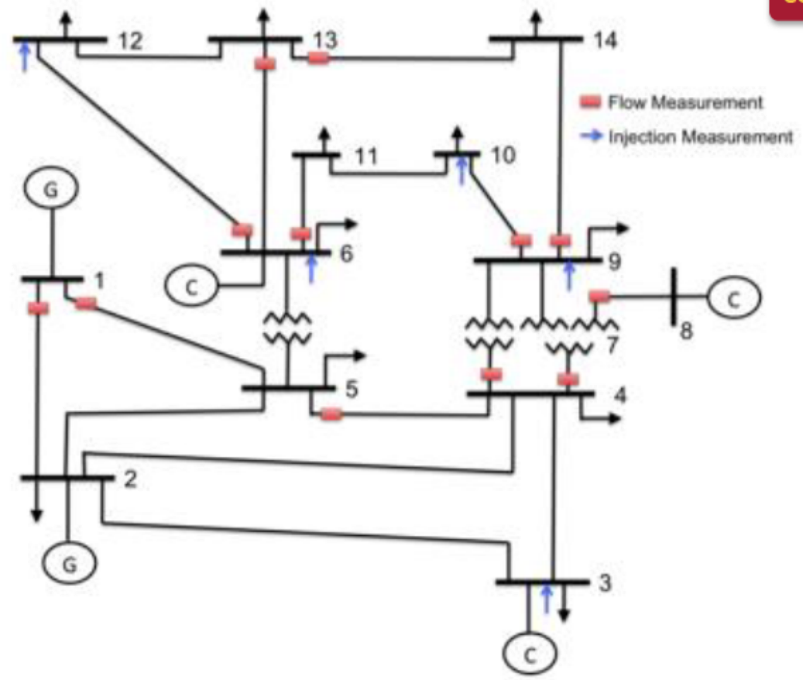
Attack on status measurements

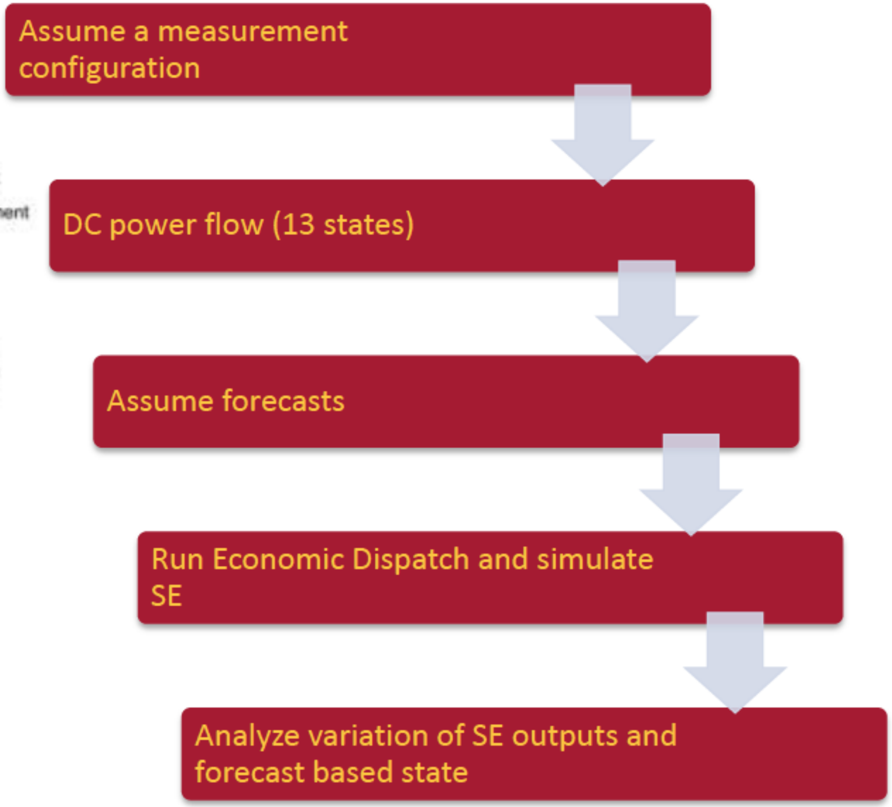
$$z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix}_{m\times 1} = \begin{bmatrix} H_{11} & \cdots & \cdots & \cdots & H_{1n} \\ H_{21} & \cdots & \cdots & \cdots & H_{2n} \\ \vdots & \cdots & \cdots & \cdots & \vdots \\ \vdots & \cdots & \cdots & \cdots & \vdots \\ H_{m1} & H_{m2} & \cdots & \cdots & H_{mn} \end{bmatrix}_{m\times n} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}_{n\times 1} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix}_{m\times 1}$$

If measurement z_2 is a ‘**critical measurement**’, a topology error will remove a row from H. Then, the state corresponding to a zero column in H becomes ‘**unobservable**’.

$$z = \begin{bmatrix} z_1 \\ z_3 \\ \vdots \\ z_m \end{bmatrix}_{(m-1)\times 1} = \begin{bmatrix} H_{11} & \cdots & \cdots & \cdots & H_{1n} \\ H_{31} & \cdots & \cdots & \cdots & H_{3n} \\ \vdots & \cdots & \cdots & \cdots & \vdots \\ \vdots & \cdots & \cdots & \cdots & \vdots \\ H_{m1} & H_{m2} & \cdots & \cdots & H_{mn} \end{bmatrix}_{(m-1)\times n} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}_{n\times 1} + \begin{bmatrix} e_1 \\ e_3 \\ \vdots \\ e_m \end{bmatrix}_{(m-1)\times 1}$$

Case Study: IEEE 14 bus system





Assume a measurement configuration

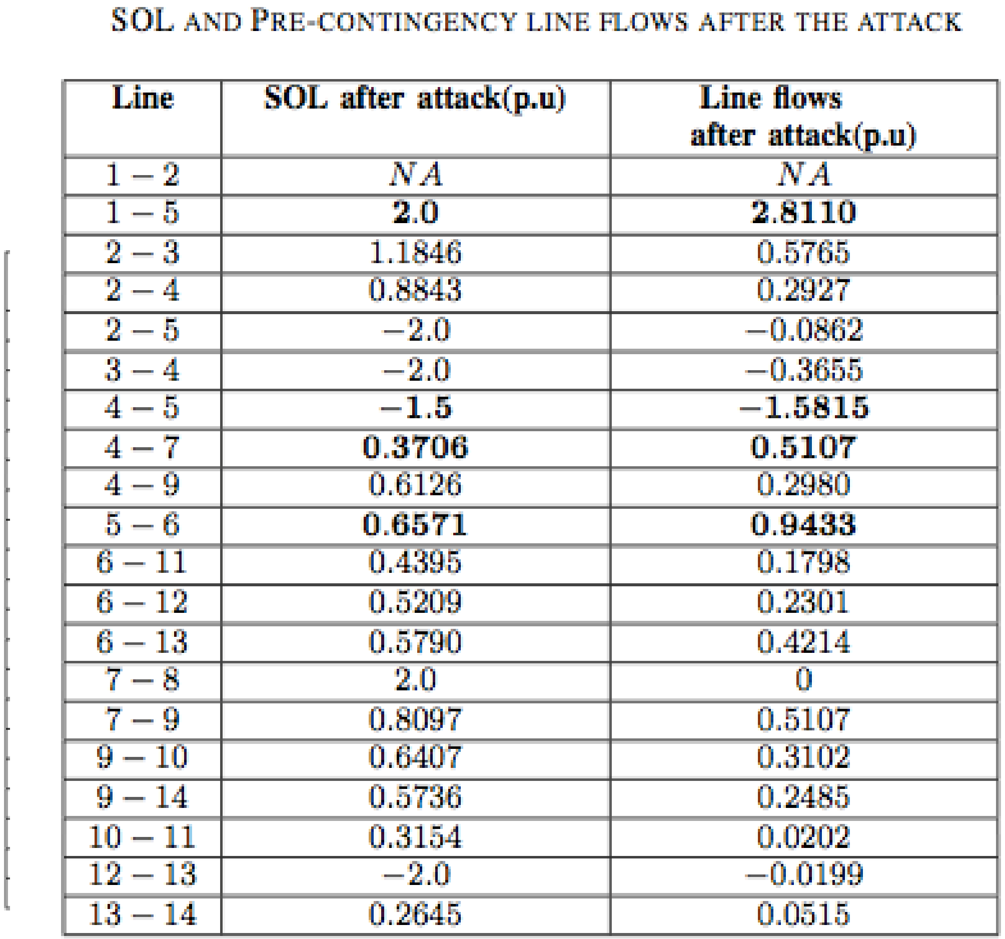
DC power flow (13 states)

Assume forecasts

Run Economic Dispatch and simulate SE

Analyze variation of SE outputs and forecast based state

Case Study: Results



SOL AND PRE-CONTINGENCY LINE FLOWS AFTER THE ATTACK

Line	SOL after attack(p.u)	Line flows after attack(p.u)
1 − 2	*NA*	*NA*
1 − 5	**2.0**	**2.8110**
2 − 3	1.1846	0.5765
2 − 4	0.8843	0.2927
2 − 5	−2.0	−0.0862
3 − 4	−2.0	−0.3655
4 − 5	**−1.5**	**−1.5815**
4 − 7	**0.3706**	**0.5107**
4 − 9	0.6126	0.2980
5 − 6	**0.6571**	**0.9433**
6 − 11	0.4395	0.1798
6 − 12	0.5209	0.2301
6 − 13	0.5790	0.4214
7 − 8	2.0	0
7 − 9	0.8097	0.5107
9 − 10	0.6407	0.3102
9 − 14	0.5736	0.2485
10 − 11	0.3154	0.0202
12 − 13	−2.0	−0.0199
13 − 14	0.2645	0.0515

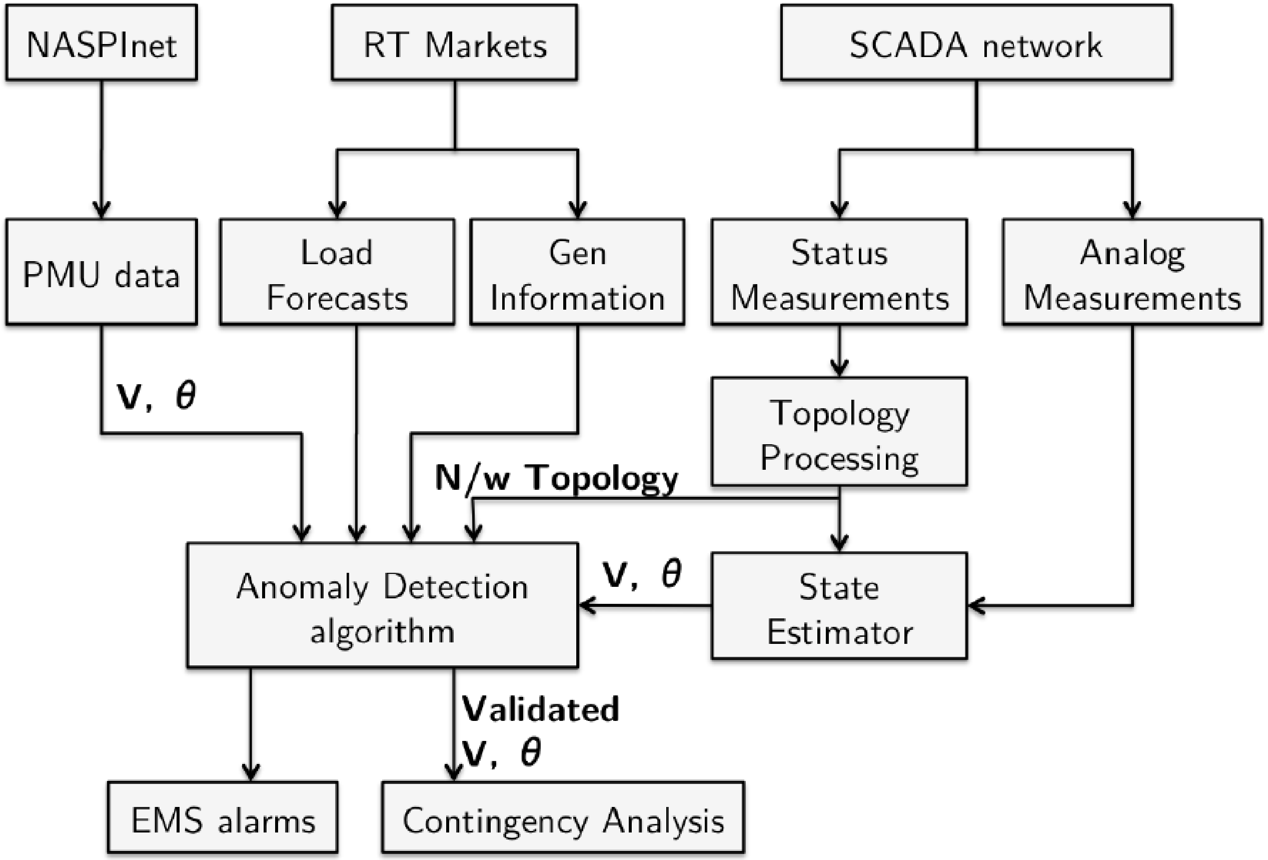
- Critical branches:1-2, 7-8.
- Attack scenario:
  - Remove branch 1-2
- Impacts:
  - One unobservable state
  - Several SOL violations
  - Unnecessary re-dispatch
  - Market Impacts

A. Ashok and G. Manimaran, "**Cyber attacks on power system state estimation through topology errors", IEE PES General Meeting, 2012**

Mitigation of cyber attacks on SE

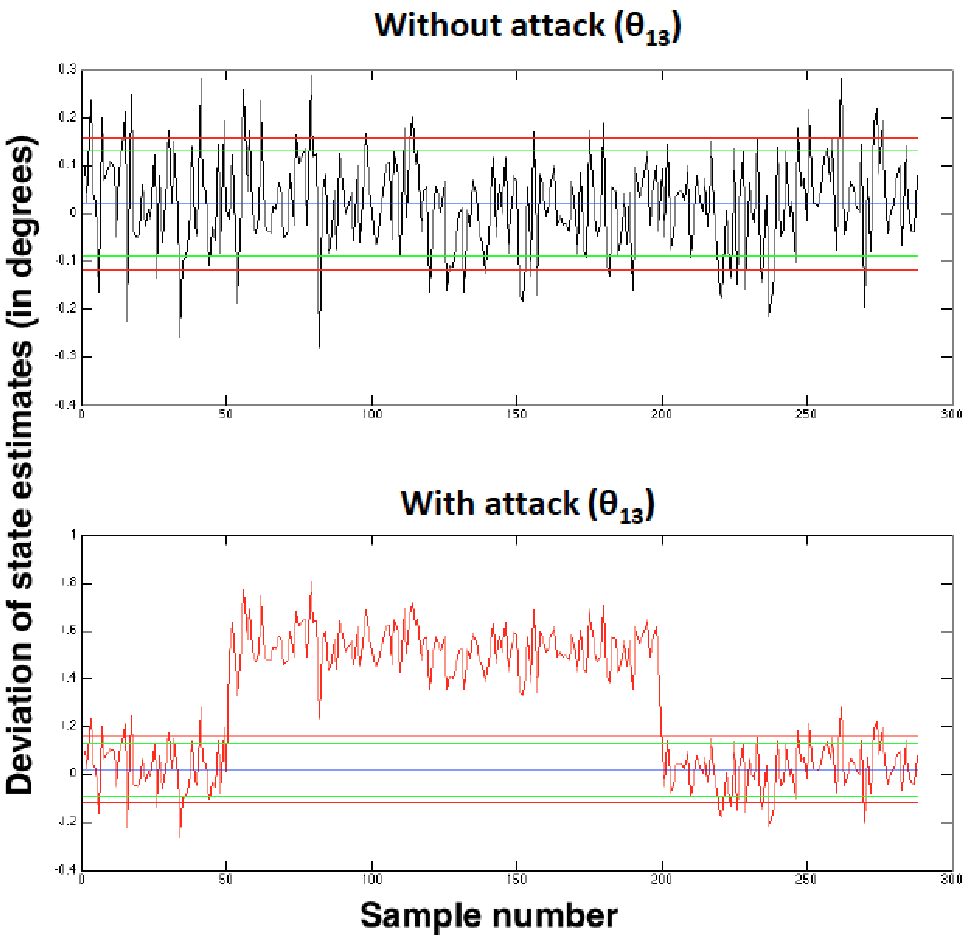
- Could be at infrastructure or application layers
  - Infrastructure: IDS, Anomaly detection, Encryption
  - Application: Intelligent SE algorithms
- Common mitigation: Deploy PMU’s at target locations to improve redundancy
- Assumption: PMU measurements are secure, accurate.

Mitigation of cyber attacks on SE



A. Ashok, M. Govindarasu, and A. Ajjarapu, "Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation," IEEE Trans. on Smart Grid, July 2016.

Detection of stealthy attacks

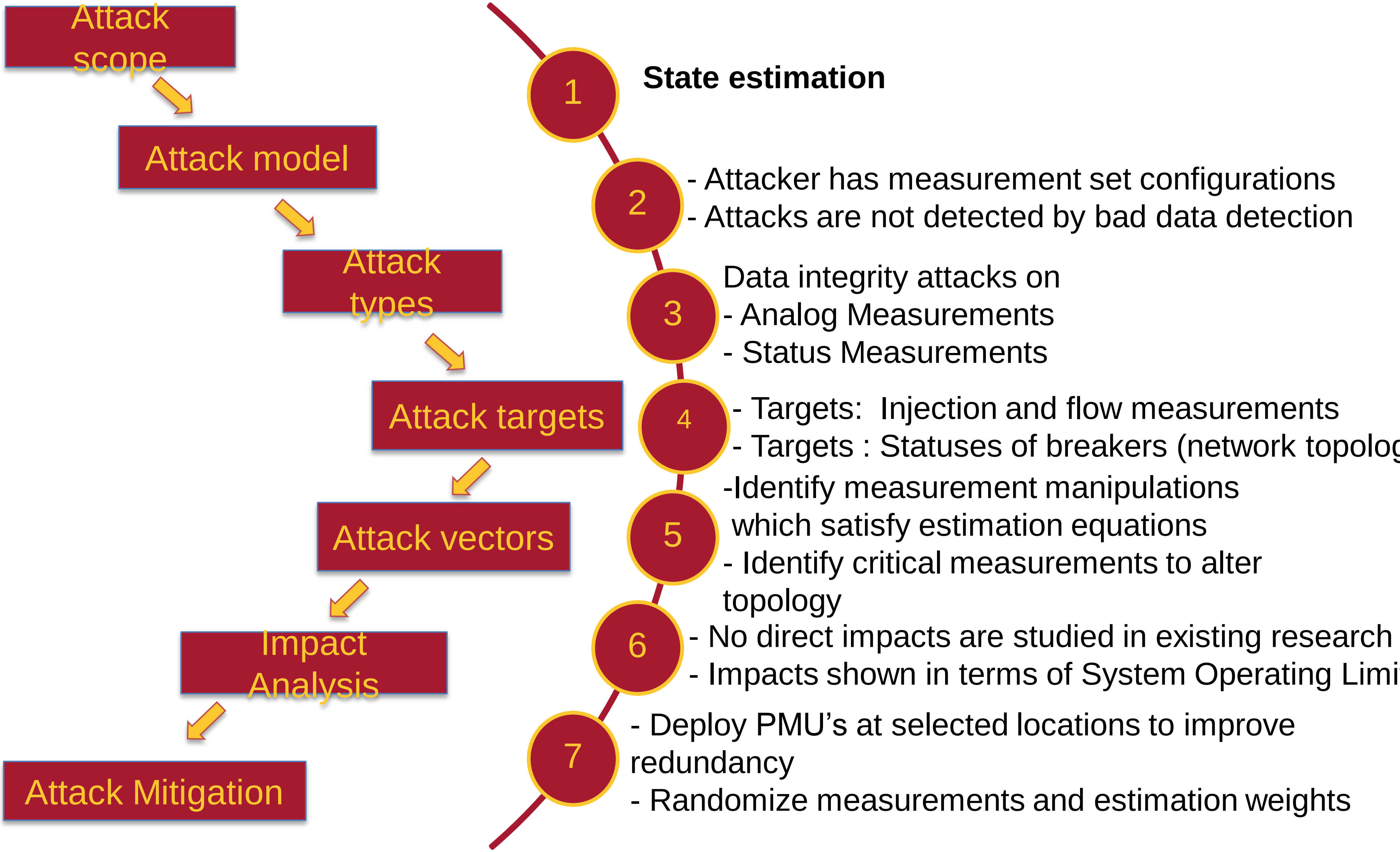


Without attack (θ_{13})

With attack (θ_{13})

Each sample corresponds to one 5 minute interval as per Real-Time Markets

Research Methodology



Attack scope

Attack model

Attack types

Attack targets

Attack vectors

Impact Analysis

Attack Mitigation

1 **State estimation**

2 - Attacker has measurement set configurations
- Attacks are not detected by bad data detection

3 Data integrity attacks on
- Analog Measurements
- Status Measurements

4 - Targets: Injection and flow measurements
- Targets : Statuses of breakers (network topolog

5 -Identify measurement manipulations which satisfy estimation equations
- Identify critical measurements to alter topology

6 - No direct impacts are studied in existing research
- Impacts shown in terms of System Operating Limi

7 - Deploy PMU's at selected locations to improve redundancy
- Randomize measurements and estimation weights

Summary

- Cyber-Physical Security of WAMPAC is critical for bulk power system reliability.

- Attack-resilient WAMPAC involves
  - Identifying vulnerabilities
  - Analyzing impacts
  - Developing cyber-physical counter measures

Conclusions

- Cybersecurity and attack-resiliency of WAMPAC is very critical to reliable and economic operation of bulk power system

- CPS mitigation measures leverage underlying physics of system operation and available trusted data sources
  - Automatic Generation Control (Control), Voltage Control …
  - State Estimation (Monitoring), Oscillation monitoring & damping control ...
  - Remedial Action Schemes (Protection) ….

- Attack-Resilient WAMPAC algorithms need to be integrated into EMS of the control center