

# Smart Grids Cyber System

## Security: an Innovation

## Approach

---

Arturo Bretas

Department of Electrical and Computer Engineering

# Outline

---

- ▶ Introduction
- ▶ State Estimation
- ▶ Smart Grids Cyber-Security
- ▶ Result
- ▶ Conclusions

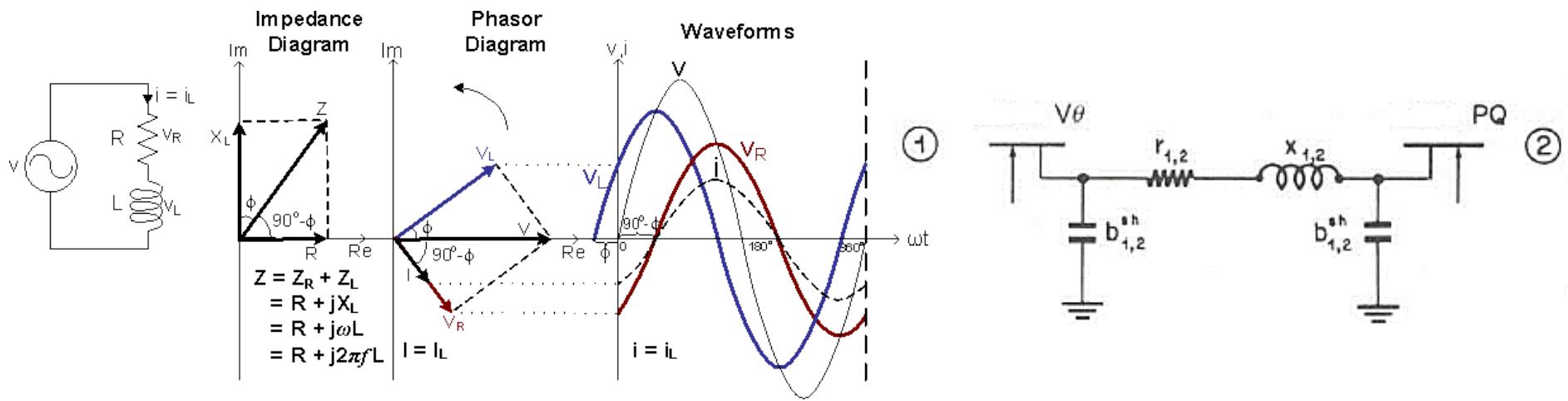
# Introduction

---

- ▶ Modern Power Systems:
- ▶ Energy monitoring systems
- ▶ Supervisory Control and Data Acquisition (SCADA) systems
- ▶ Phasor Measurement Units (PMUs)
- ▶ Smart Grids
  - ▶ Smart meters
  - ▶ Huge amount of data in real time
- ▶ Number of measurements > number of states
  - ▶ Voltage magnitude and angle
  - ▶ Inconsistent measurements

# Introduction

- State of a system
  - Smallest set of variables necessary to calculate any other variable
  - For power systems: voltage angle and magnitude



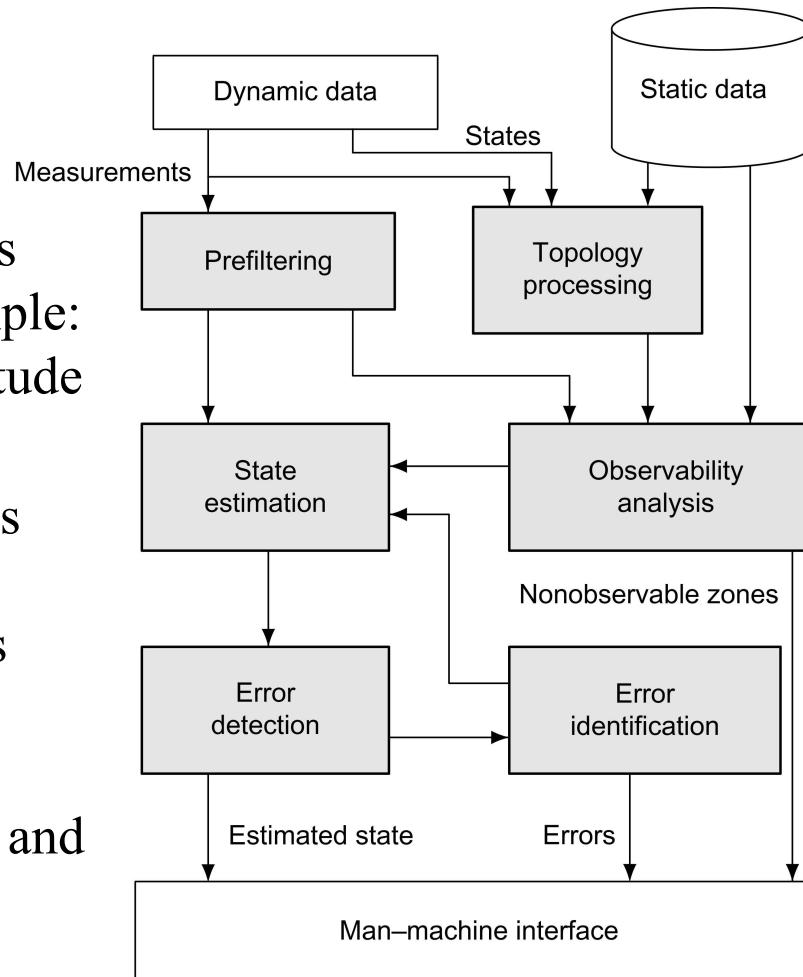
# State estimation

## ► Overview

**Pre filtering:** eliminates inconsistent data. Example: negative voltage magnitude

**State estimator:** obtains state. One method is Weighted Least Squares (WLS)

**Errors:** detect, identify and eliminate non-Gaussian errors



**Topology:** analyses electric network model. Example: switches (open or closed)

**Observability:** verifies if states can be obtained with available set of measurements

# State estimation

---

## ► WLS Algorithm:

► Initial state:  $\mathbf{V}=\mathbf{1}$ ,  $\boldsymbol{\theta}=\mathbf{0}$

► Update states:

$$\Delta \mathbf{x}^v = \left( \mathbf{H}(\mathbf{x}^v)^T \mathbf{W} \mathbf{H}(\mathbf{x}^v) \right)^{-1} \mathbf{H}(\mathbf{x}^v)^T \mathbf{W} [\mathbf{z} - \mathbf{h}(\mathbf{x}^v)]$$
$$\mathbf{x}^{v+1} = \mathbf{x}^v + \Delta \mathbf{x}^v$$

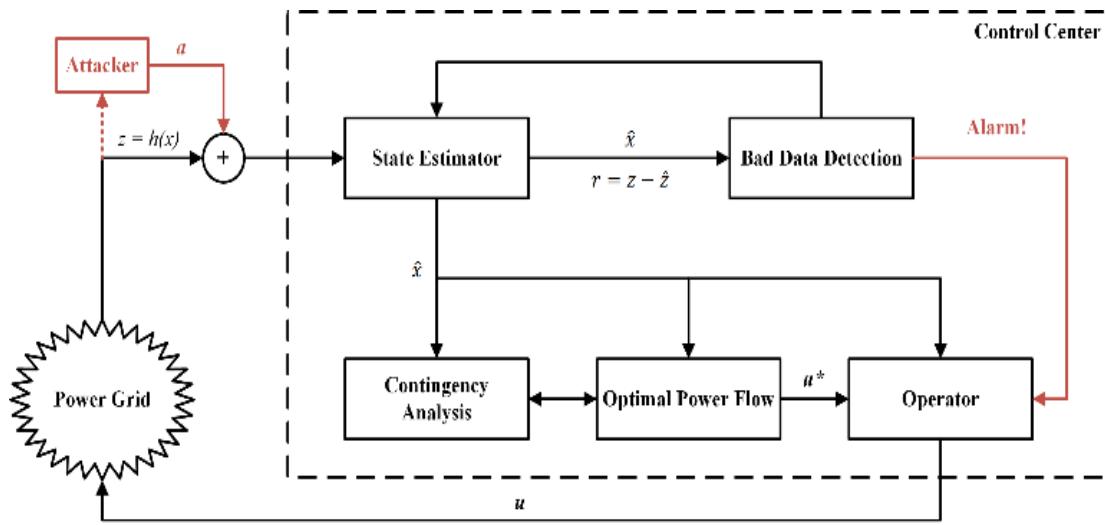
► Verify convergence criteria

$$\Delta \mathbf{x} \uparrow v \leq \xi$$

► Once it converges the residuals are calculated

$$\mathbf{r} = [\mathbf{z} - \mathbf{h}(\mathbf{x}^v)]$$

# Smart Grids Cyber-Security



# Error analysis

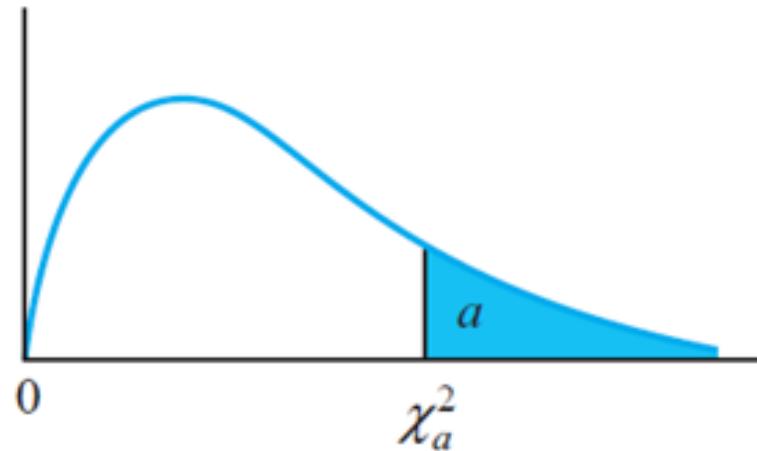
---

- Pre-filtering: identifies inconsistent measurement data
  - Negative voltage magnitude, load buses having positive power injection...
- Pre-filtering cannot detect more subtle errors
- WLS-SE uses post-processing to detect errors based on statistical properties of residuals
- Most used tests: chi-square and highest normalized error
- Given that errors have a Gaussian behavior, this analysis aims at finding errors that do not have those characteristics

# Error analysis

---

- The sum of the squares of a Gaussian distribution of independent random variables having zero mean and standard deviation equal to one follow the chi-square distribution



- The value of  $\chi_{\alpha/2}^2$  is defined by a significance level (probability) or by degree of freedom (independence)

# Error analysis

---

- Error detection:

$$J(\mathbf{x}) = [\mathbf{z} - \mathbf{h}(\mathbf{x})]^T \mathbf{W} [\mathbf{z} - \mathbf{h}(\mathbf{x})] = \sum_{i=1}^m \left( \frac{r_i}{\sigma_i} \right)^2 \quad \xrightarrow{\chi \downarrow \alpha \atop \gamma 2}$$

- Residuals and errors are related by

$$\mathbf{r} = \mathbf{z} - \mathbf{h}(\mathbf{x}) = \mathbf{S}\mathbf{e}$$

- $\mathbf{S}$  is the sensitivity matrix (not a diagonal matrix)

- Error identification:

- Using normalized error:

$$r_i^N = \frac{|z_i - h_i(\mathbf{x}^*)|}{\sqrt{\Omega_{ii}}} = \frac{|r_i|}{\sqrt{S_{ii} R_{ii}}}$$

- $\mathbf{R} = \mathbf{W}^{-1}$

# Innovation Approach

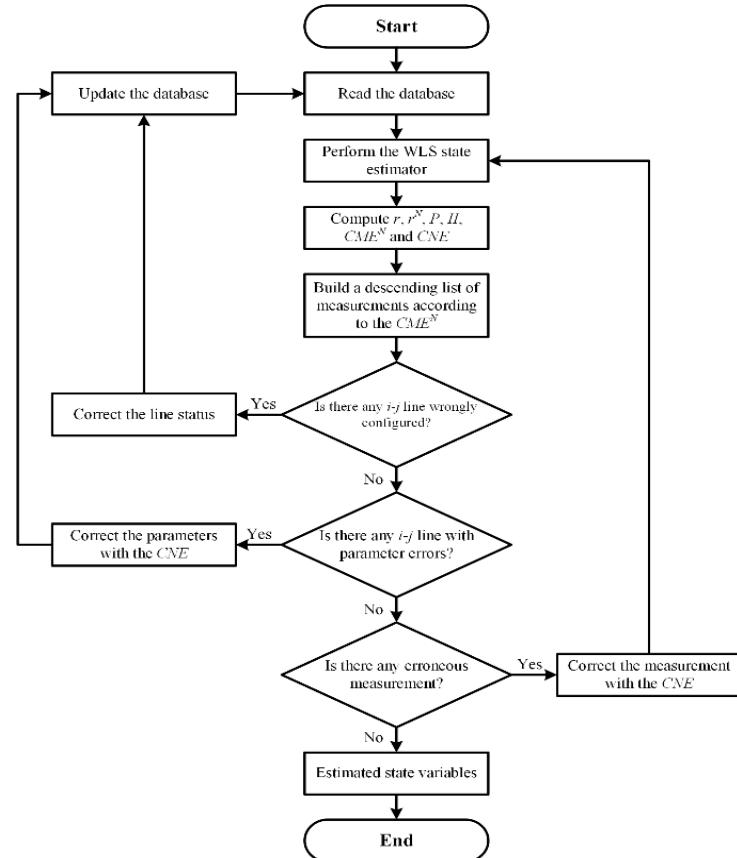
$$CME_{mi} = r_{mi} \sqrt{1 + \frac{1}{II_{mi}^2}}$$

$$II_{mi} = \sqrt{1 - K_{mi,mi}} / \sqrt{K_{mi,mi}}$$

$$J'(\hat{\mathbf{x}}) = (\mathbf{CME}) \mathbf{W} (\mathbf{CME})^T$$

$$J'(\hat{\mathbf{x}}) \geq \chi^2_{(nm,\alpha)}$$

$$CME_{mi}^N = |CME_{mi}| / \sigma_{mi}$$



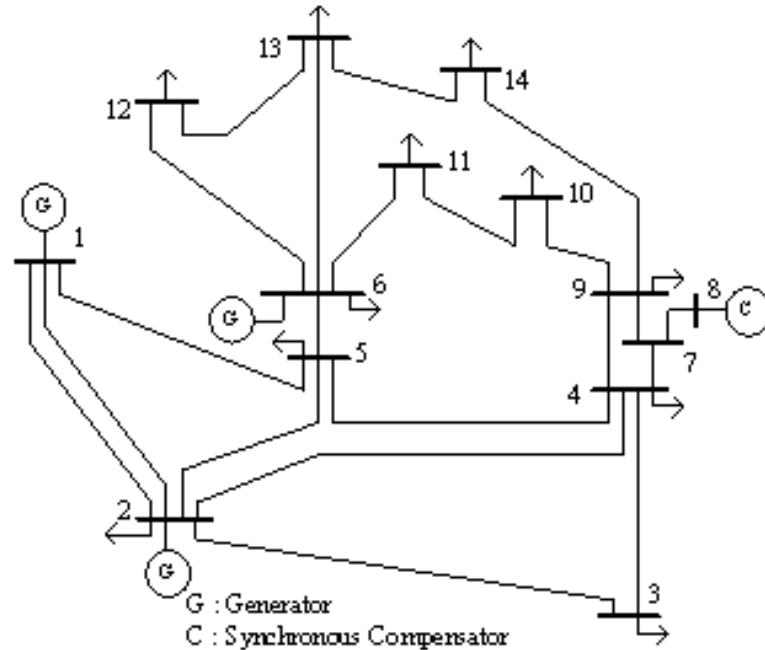
# Case Study

i) Attack Scenario I: Multiple measurements errors in the IEEE 14-bus test system

Gross error of magnitude  $0.1762pu$  (reactive power injection at bus 7);

Gross error of magnitude  $1.5689pu$  (active power injection at bus 2);

Gross error of magnitude  $-0.9420pu$  (active power injection at bus 3).



agent  $Q:08-07 =$

agent  $P:01-02 =$

agent  $P:03 =$

# Case Study

---

## Original Measurement

$$Q:08-07 = 0.1762$$

$$P:01-02 = 1.5689$$

$$P:03 = -0.9420$$

## Multiple Errors Processing

### Measurement with Error

$$(Q:08-07) + 9\sigma = 0.1963$$

$$(P:01-02) + 5\sigma = 1.6589$$

$$(P:03) + 4\sigma = -0.9021$$

## Processing Error Step 1

### Meas. with

|                         | II     | CME <sup>N</sup> | CNE     |
|-------------------------|--------|------------------|---------|
| <b>Q:08-07 = 0.1962</b> | 2.1884 | 9.3760           | 10.3085 |

**Corrected Measurement: Q:08-07 – CNE\* = 0.1760pu**

(Correction Error = 0.1135%)

## Processing Error Step 2

### Meas. with

|                         | II     | CME <sup>N</sup> | CNE    |
|-------------------------|--------|------------------|--------|
| <b>P:01-02 = 1.6466</b> | 4.6720 | 4.7656           | 4.8736 |

**Corrected Measurement: P:01-02 – CNE\* = 1.5663pu**

(Correction Error = 0.1657%)

## Processing Error Step 3

### Meas. with

**$\geq 3.0$**

|                       | II     | CME <sup>N</sup> | CNE    |
|-----------------------|--------|------------------|--------|
| <b>P:03 = -0.9033</b> | 2.4543 | 3.9560           | 4.2718 |

**Corrected Measurement: P:03 – CNE\*  $\sigma = -0.9418$ pu**

(Correction Error = 0.0212%)

# Case Study

---

*ii) Attack Scenario II: Simultaneous measurement error and parameter error in the IEEE 14-bus test system*

Gross error of magnitude  $-6\sigma$  added to measurement  $P:04-09 = 0.1609pu$  (active flow from bus 4 to bus 9);

Error of 6% added to the parameters of the line 06-12.

# Case Study

---

| CME <sup>N</sup> Descending List   |        |                  |          |
|--|--------|------------------|----------|
| Measurement  | II     | CME <sup>N</sup> | CNE      |
| P:04-09  | 2.9654 | -5.8800          | -6.2053  |
| Q:12   | 0.4989 | -5.8059          | -13.0046 |
| P:12-06  | 2.0719 | 4.7710           | 5.2976   |
| Q:12-06  | 1.9688 | 4.0204           | 4.5093   |
| Q:06-12  | 2.0766 | -3.9147          | -4.3450  |
| Q:13   | 0.9701 | -3.0646          | -4.4012  |
| Meas. with   | II     | CME <sup>N</sup> | CNE      |
| <b>P:04-09 = 0.1509</b>  | 2.9654 | -5.8800          | -6.2053  |
| <b>Corrected Measurement: P:04-09 – CNE* = 0.1602</b><br><b>(Correction Error = 0.4351%)</b> |        |                  |          |

# Case Study

---

## CME<sup>N</sup> Descending List

| Measurement | II     | CME <sup>N</sup> | CNE      |
|-------------|--------|------------------|----------|
| P:12-06     | 2.0691 | 5.4585           | 6.0626   |
| Q:12        | 0.4989 | -5.0717          | -11.3601 |
| Q:12-06     | 1.9688 | 4.2039           | 4.7151   |
| Q:06-12     | 2.0765 | -2.7853          | -3.0915  |
| Q:13        | 0.9701 | -2.6720          | -3.8375  |
| P:13-12     | 1.0450 | 1.9677           | 2.7235   |

## Parameters Correction

| Parameter | Database Value | Erroneous Value | Corrected Value | Correction Error |
|-----------|----------------|-----------------|-----------------|------------------|
|           | 1.5260         | 1.6175          | 1.5250          | 0.0655%          |
|           | -3.1760        | -3.3665         | -3.1741         | 0.0598%          |
|           | 0.0000         | 0.0000          | 0.0000          | 0.0000%          |

# Conclusions

---

- Innovation State Estimator: Extension/Enhancement of WLS;
- Initial Test Results are Encouraging;
- Capable to Detect, Identify and Correct Cyber-Attacks on Measurements and Parameters;
- Current Research on Topological Attacks and Physical Attacks.