Leveraging Physics for Security: Micro-PMUs

Anna Scaglione, Arizona State University

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

Contents

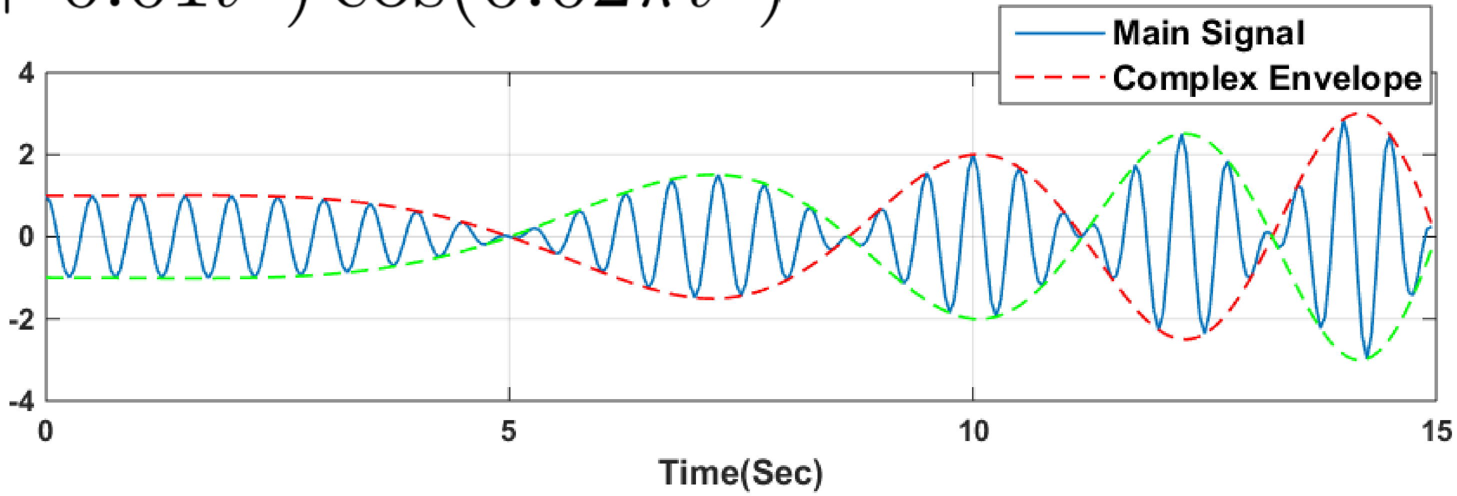
Example 1

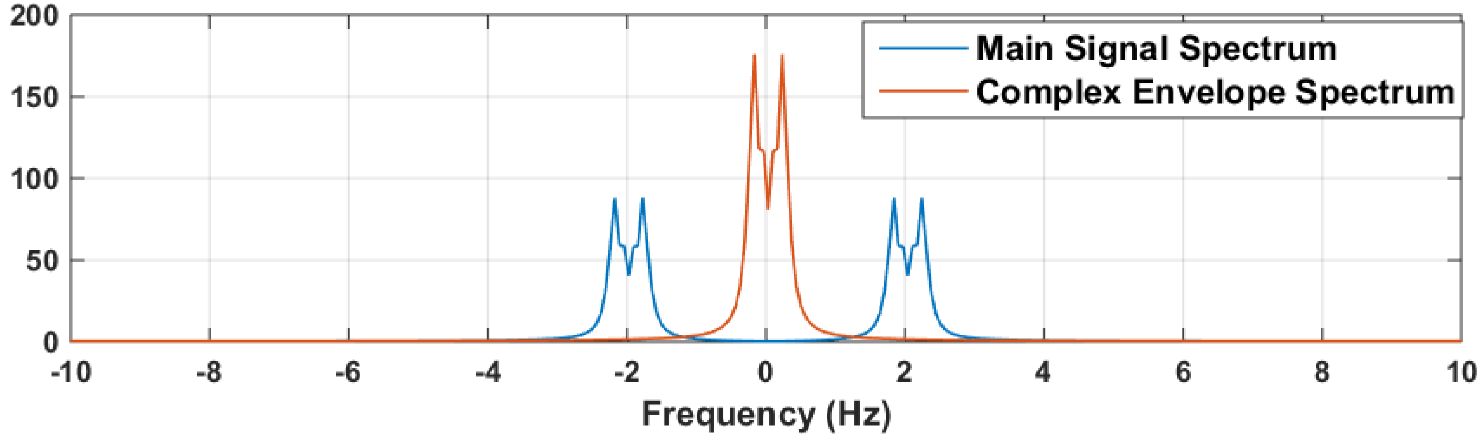
Real signal (e.g. AC voltage, AC current)

$$s(t) = (1 + 0.01t^2)\cos(0.02\pi t^2)\cos(4\pi t)$$

Phasor signal

$$\tilde{s}(t) = (1 + 0.01t^2)\cos(0.02\pi t^2)$$





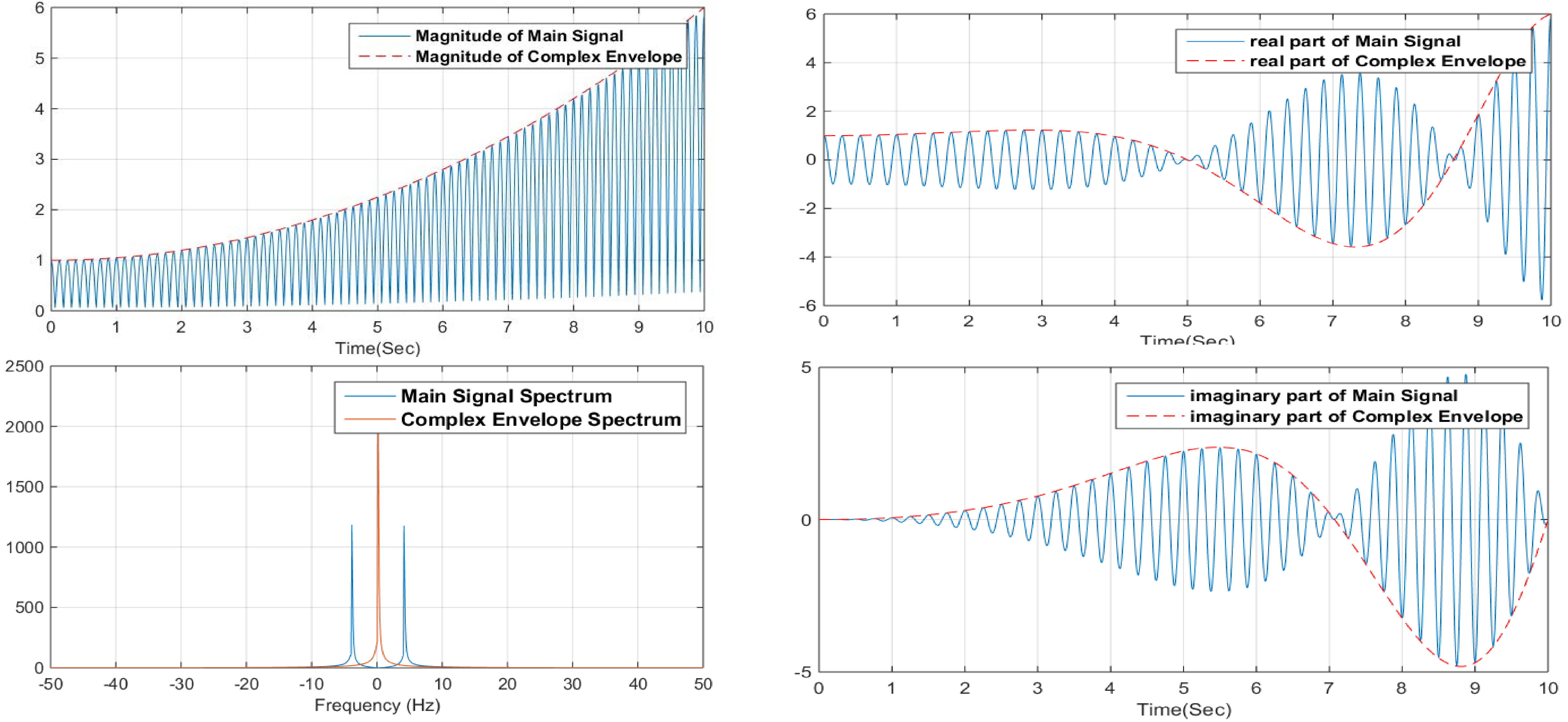
Example 2

Complex signal

$$s(t) = (1 + 0.05t^2)e^{j0.1\pi t^2}\cos(8\pi t)$$

Phasor signal

$$\tilde{s}(t) = (1 + 0.05t^2)e^{j0.1\pi t^2}$$



Phasor (Complex Envelope)

- Complex envelope: baseband representation of the band-pass signals.
  - In Theory:

analytic signal — complex envelope

$$s(t) \xrightarrow{1} s^+(t) = \frac{1}{2}s(t) + \frac{j}{2\pi t} \star s(t) \xrightarrow{2} \tilde{s}(t) = \sqrt{2}s^+(t)e^{-j2\pi f_0 t}.$$

shift and scale

$s(t)$ is bandpass

  - In practice:

W: frequency support of the signal — f_0: signal center frequency

Assume that $\frac{W}{2} \leq f_0$

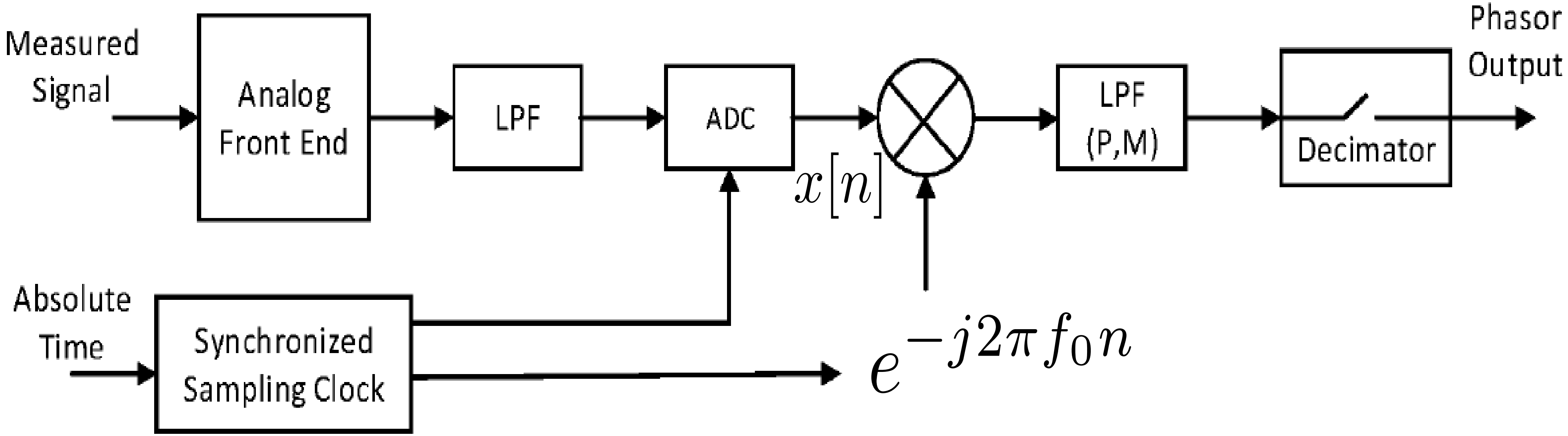
$$s(t) \xrightarrow{1} \tilde{s}(t) = \sqrt{2}(s(t)e^{-j2\pi f_0 t}) \star h(t)$$

$h(t)$: low-pass filter

Note : $\tilde{s}(t)$ is band-limited $\rightarrow$ can be sampled at $2f_0$ Hz.

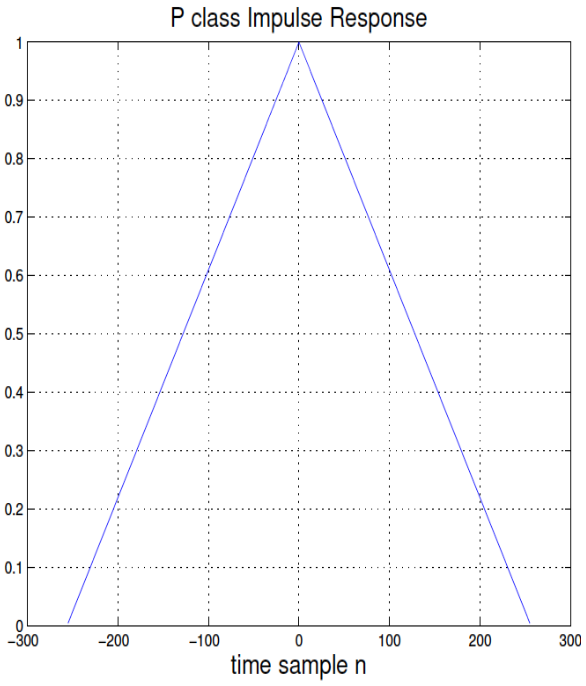
Micro-Phasor Measurement Units (µPMUs)

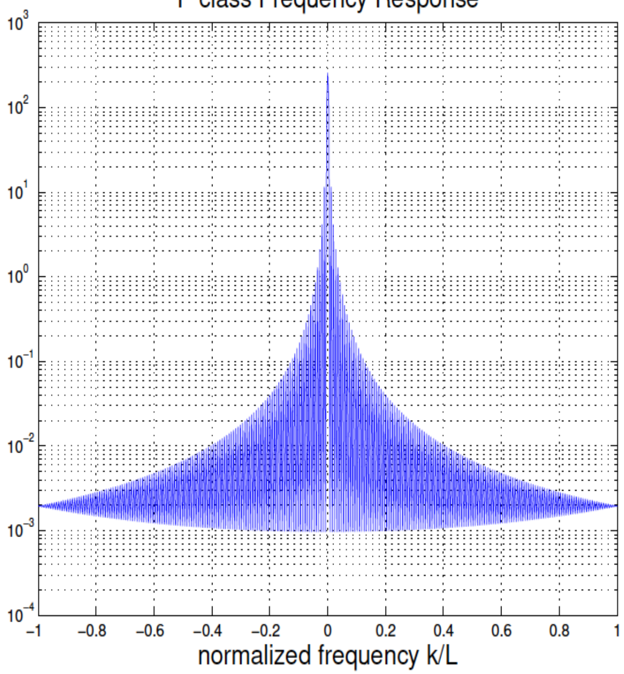
- Voltage and current in power system are (band-limited) bandpass signals.
- µPMUs are low-cost and small synchrophasor devices that sample voltage and current with 512*60 Hz rate and extract the complex envelope with 120 Hz.

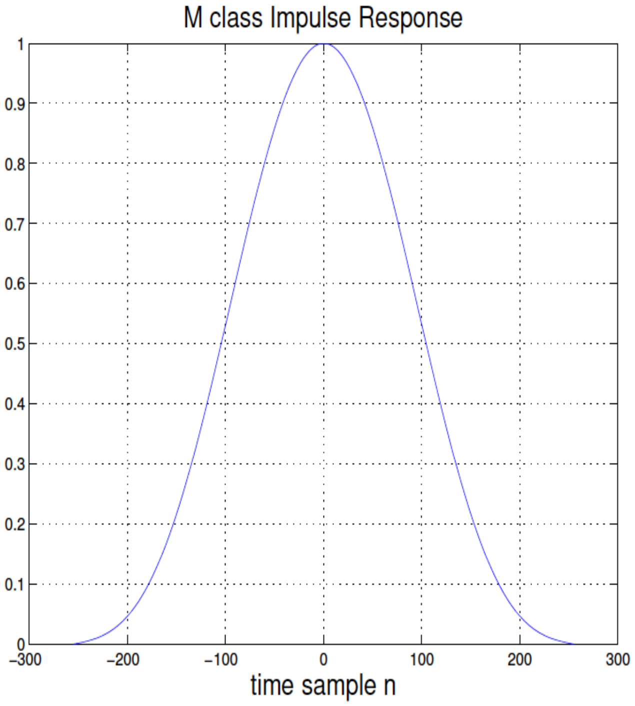


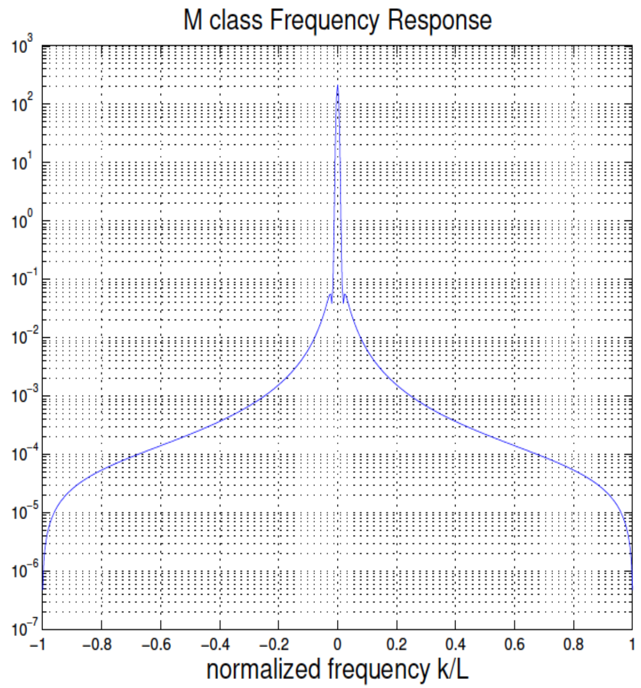
$$\mu\text{PMU output: } \mathbf{v}[k] \in \mathbb{C}^{3\times 1}, \quad \mathbf{i}[k] \in \mathbb{C}^{3\times 1}$$

- IEEE C.37 standard filters: P class and M class.
- P class and M class differ because they have two different responses for the Low Pass Filter (LPF). P has high side-lobes → more sensitive to noise but also to transients.









- µPMUs have proprietary filters to handle the different distribution grid environment as opposed to the transmission

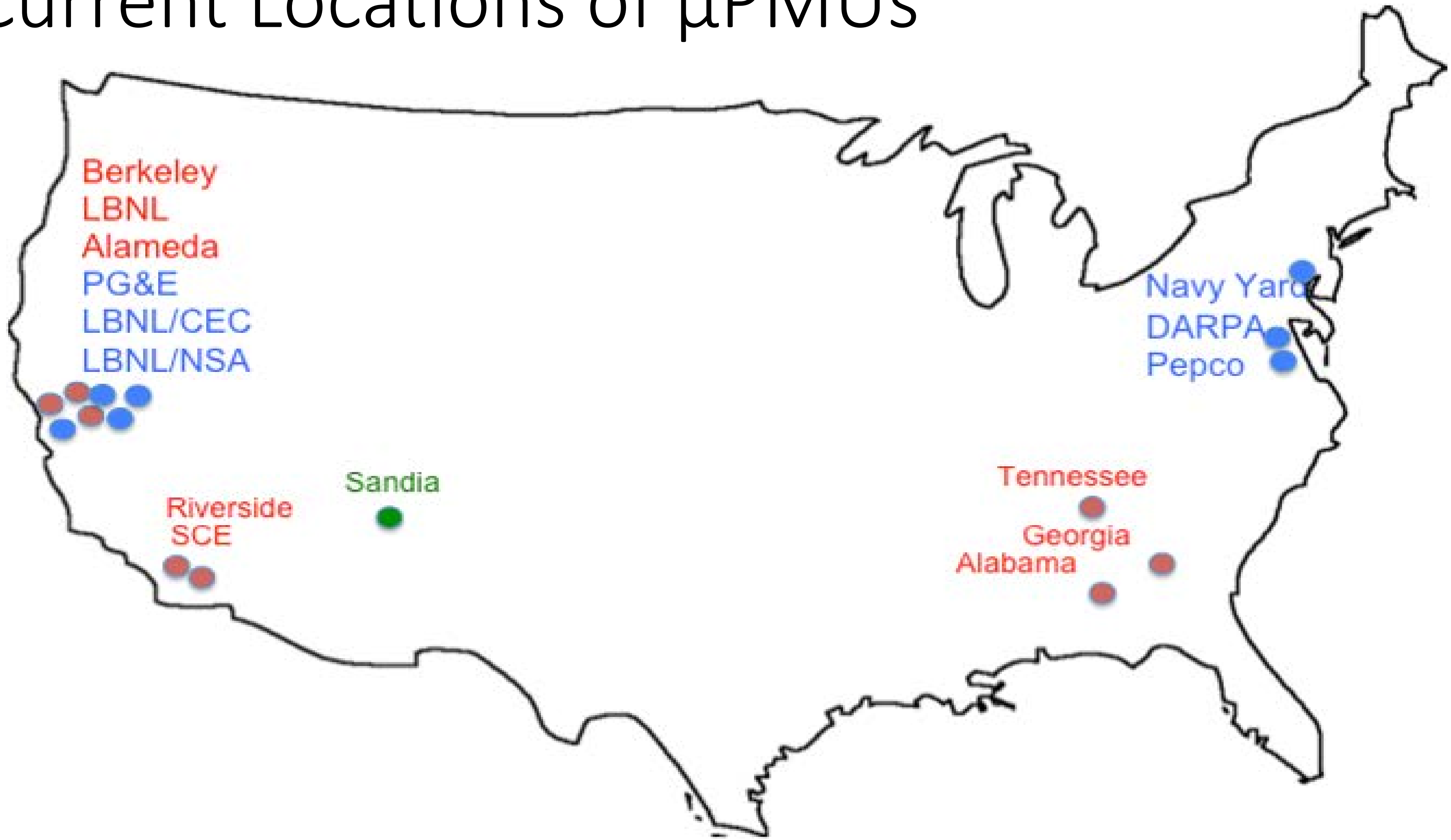
0.002° resolution, 0.0002% magnitude, 0.01% Total Vector Error (TVE)!

Micro-Phasor Measurement Units (Cntd.)

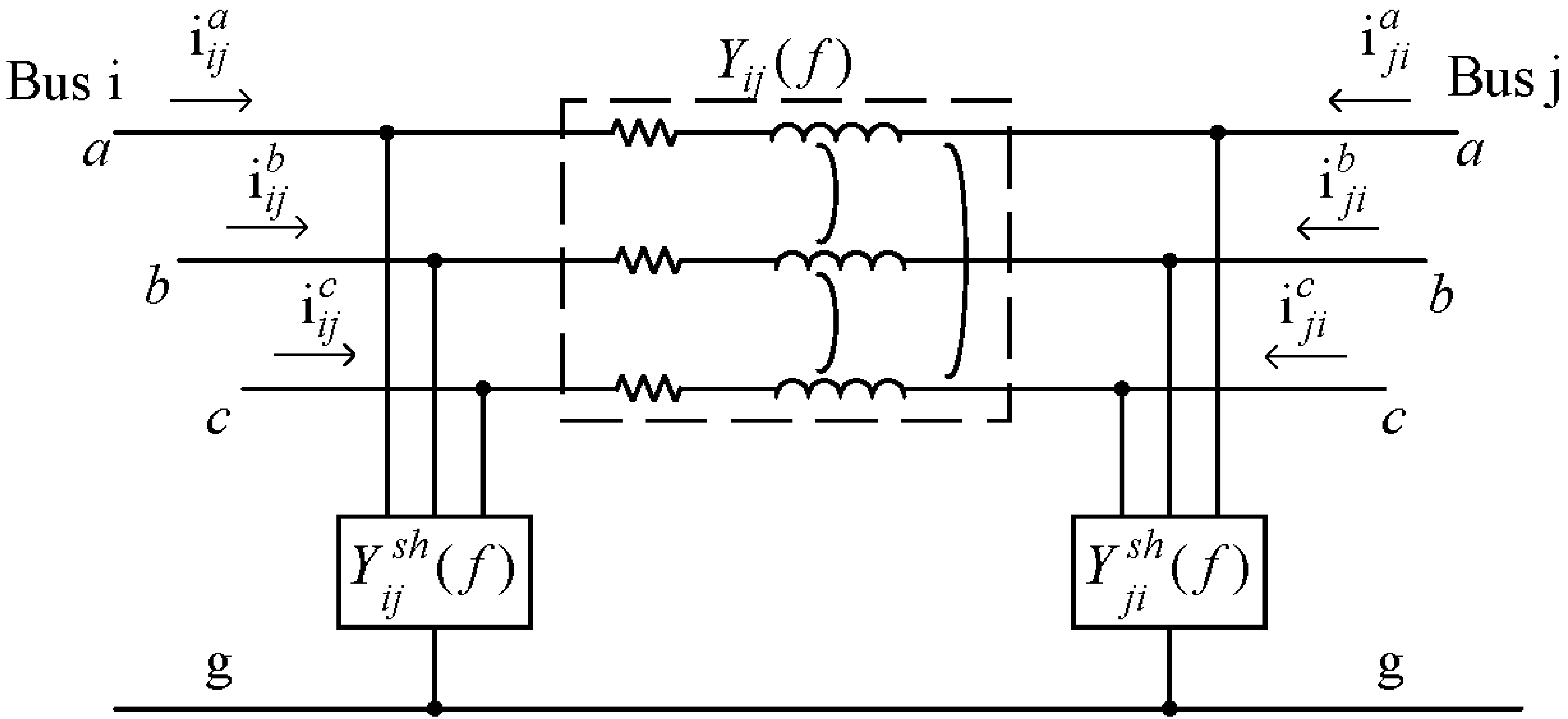
Installation at Grizzly Substation, Lawrence Berkeley National Lab, highlighting GPS and modem antennae.

- Sample Measurements: http://mobile.pqube3.com/ https://plot2.upmu.org/
- Designed for harsh distribution grid environment: http://PQube3.com/tough

Current Locations of μPMUs



Distribution Line Model



- Linear Time Invariant (LTI) system → Multi-Input Multi-Output (MIMO) representation also holds for the complex envelopes.

Distribution Line Model (cntd.)

$$\boldsymbol{i}_{ij}(f) = (\mathbf{y}^{sh}_{ij}(f) + \mathbf{y}_{ij}(f))\boldsymbol{v}_i(f) - \mathbf{y}_{ij}(f)\boldsymbol{v}_j(f)$$

$$\mathbf{i}_{ij}(t) = (\boldsymbol{y}^{sh}_{ij}(t) + \boldsymbol{y}_{ij}(t)) * \mathbf{v}_i(t) - \boldsymbol{y}_{ij}(t) * \mathbf{v}_j(t)$$

$\boldsymbol{y}^{sh}_{ij}(t)$: line shunt parameter impulse response $\quad$ $\boldsymbol{y}_{ij}(t)$: line series parameter impulse response

$$\mathbf{y}^{sh}_{ij}(f) \triangleq \boldsymbol{Y}^{sh}_{ij}(f + f_0),\ \mathbf{y}_{ij}(f) \triangleq \boldsymbol{Y}_{ij}(f + f_0)$$

$$\overline{\boldsymbol{Y}}_{ij}(f) \triangleq \boldsymbol{Y}^{sh}_{ij}(f) + \boldsymbol{Y}_{ij}(f)$$

$$\overline{\mathbf{y}}_{ij}(f) \triangleq \mathbf{y}^{sh}_{ij}(f) + \mathbf{y}_{ij}(f)$$

$$\overline{\boldsymbol{y}}_{ij}(t) \triangleq \boldsymbol{y}^{sh}_{ij}(t) + \boldsymbol{y}_{ij}(t)$$

$\Rightarrow$

$$\boldsymbol{i}_{ij}(f) = \overline{\mathbf{y}}_{ij}(f)\boldsymbol{v}_i(f) - \mathbf{y}_{ij}(f)\boldsymbol{v}_j(f)$$

$$\mathbf{i}_{ij}(t) = \overline{\boldsymbol{y}}_{ij}(t) * \mathbf{v}_i(t) - \boldsymbol{y}_{ij}(t) * \mathbf{v}_j(t)$$

In discrete time:

$$\mathbf{i}_{ij}[k] = \sum_{n=0}^{N-1} \overline{\boldsymbol{y}}_{ij}[n]\mathbf{v}_i[k-n] - \sum_{n=0}^{N-1} \boldsymbol{y}_{ij}[n]\mathbf{v}_j[k-n]$$

we assumed that $\boldsymbol{y}^{sh}_{ij}[n]$ and $\boldsymbol{y}_{ij}[n]$ are the samples respectively of $\boldsymbol{y}^{sh}_{ij}(t) \star h(t)$ and $\boldsymbol{y}_{ij}(t) \star h(t)$ and that they have finite support N, and are causal.

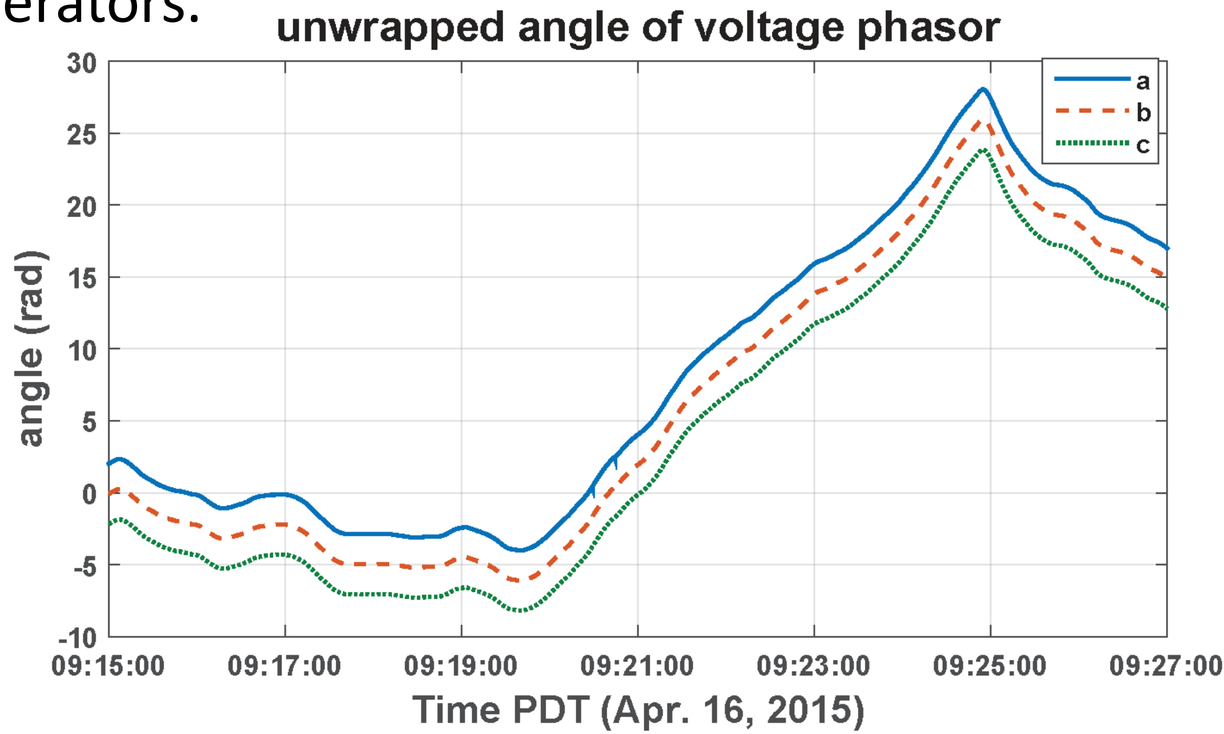
Line Model (Quasi steady-state)

- Steady-state never happens in reality [1]
  1. load-generation imbalances.
  2. active power demand interactions.
  3. large generators inertia.
  4. automatic speed controllers of the generators.

What is the effect on μPMU output??

$$\mathbf{v}_i[k] = \hat{\mathbf{v}}_i[k]e^{j\beta_k k}, \ \mathbf{i}_{ij}[k] = \hat{\mathbf{i}}_{ij}[k]e^{j\beta_k k}$$

β_k is the drift in the frequency.



1. Phadke, Arun G., and John Samuel Thorp. *Synchronized phasor measurements and their applications*. Springer Science & Business Media, 2008.

Line Model (Quasi steady-state cntd.)

Main assumption: $\hat{\mathbf{v}}_i[k-n] \approx \hat{\mathbf{v}}_i[k]$ and $\beta_{k-n} \approx \beta_k$ for $n = 0, \ldots, N-1$

$$\Rightarrow \quad \mathbf{i}_{ij}[k] \approx \left(\sum_{n=0}^{N-1} \overline{\boldsymbol{y}}_{ij}[n] e^{-j\beta_k n}\right) \mathbf{v}_i[k] - \left(\sum_{n=0}^{N-1} \boldsymbol{y}_{ij}[n] e^{-j\beta_k n}\right) \mathbf{v}_j[k]$$

$$\overline{\boldsymbol{Y}}_{ij}(f_0, \beta_k) \triangleq T\overline{\boldsymbol{Y}}_{ij}\left(f_0 + \frac{\beta_k}{2\pi T}\right) H\left(\frac{\beta_k}{2\pi T}\right),$$

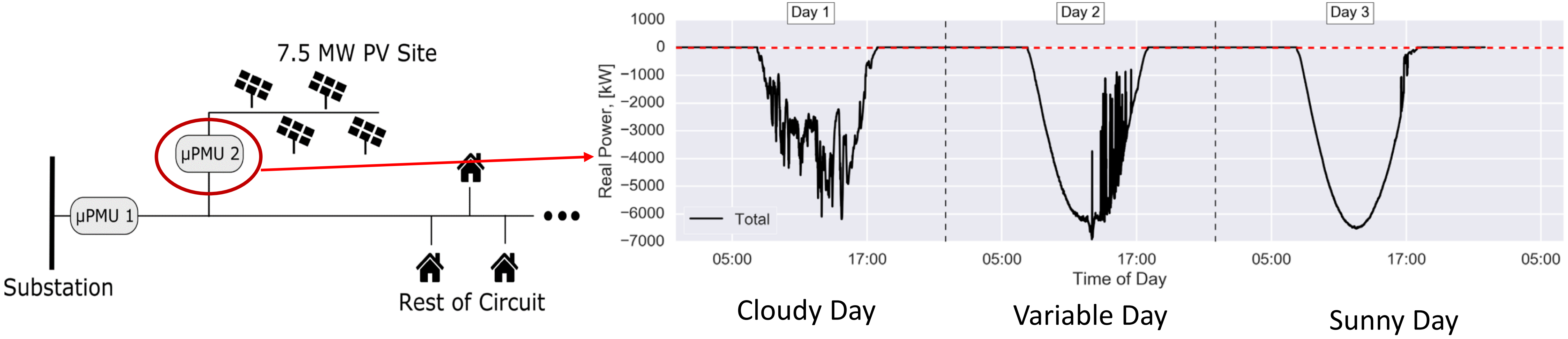
$$\boldsymbol{Y}_{ij}(f_0, \beta_k) \triangleq T\boldsymbol{Y}_{ij}\left(f_0 + \frac{\beta_k}{2\pi T}\right) H\left(\frac{\beta_k}{2\pi T}\right),$$

$$\Rightarrow \quad \mathbf{i}_{ij}[k] = \overline{\boldsymbol{Y}}_{ij}(f_0, \beta_k)\mathbf{v}_i[k] - \boldsymbol{Y}_{ij}(f_0, \beta_k)\mathbf{v}_j[k]$$

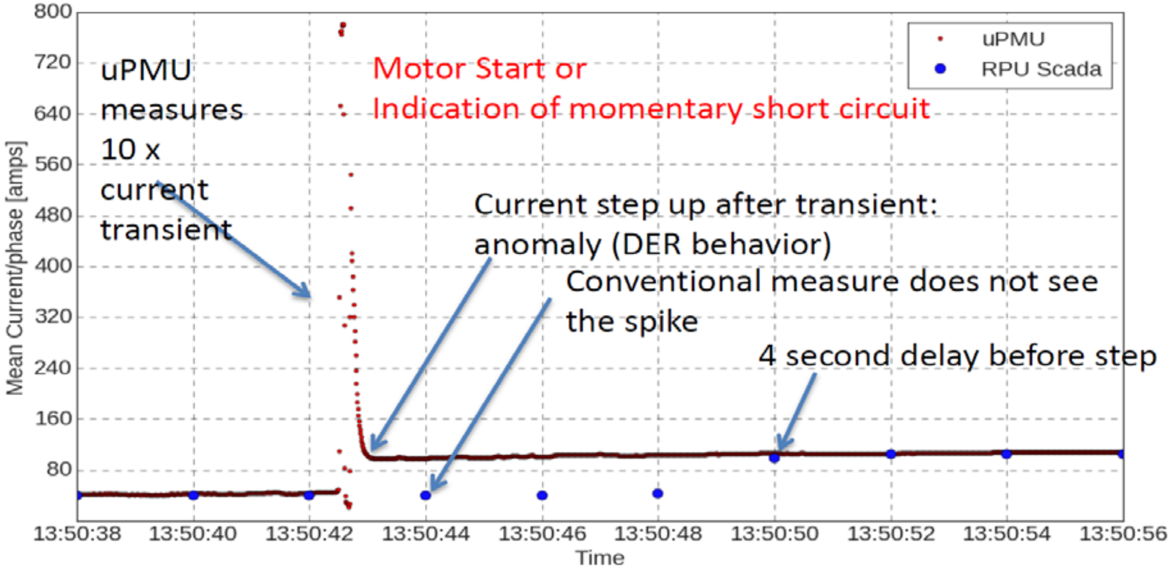
modulated admittance parameters.

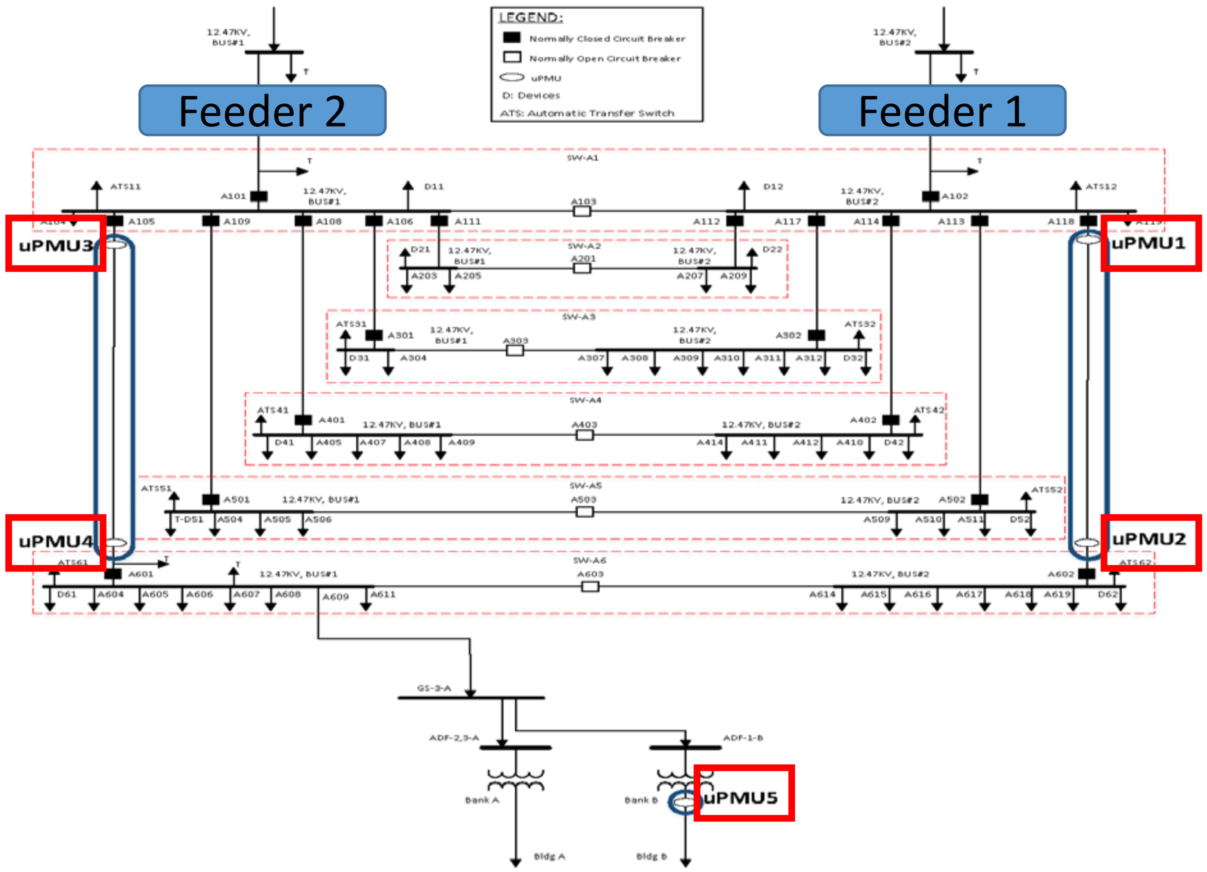
since $\frac{1}{T}\sum_{n=0}^{N-1} \boldsymbol{y}_{ij}[n] e^{-j2\pi f n T} = \boldsymbol{Y}_{ij}(f_0 + f) H(f)$ where $T = \frac{1}{120}$

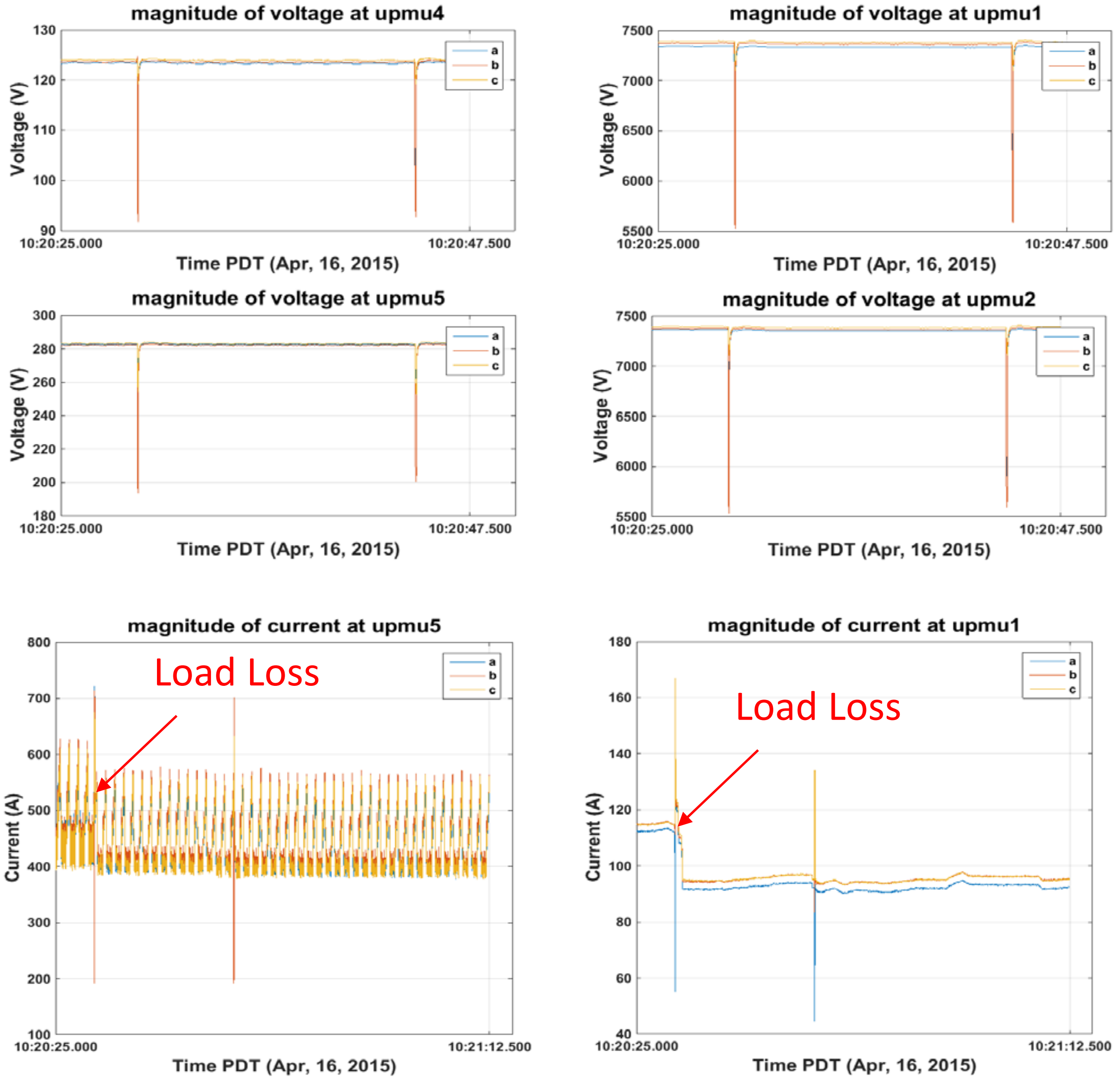
Situational Awareness



• Significantly more information vs event-triggered DSCADA.





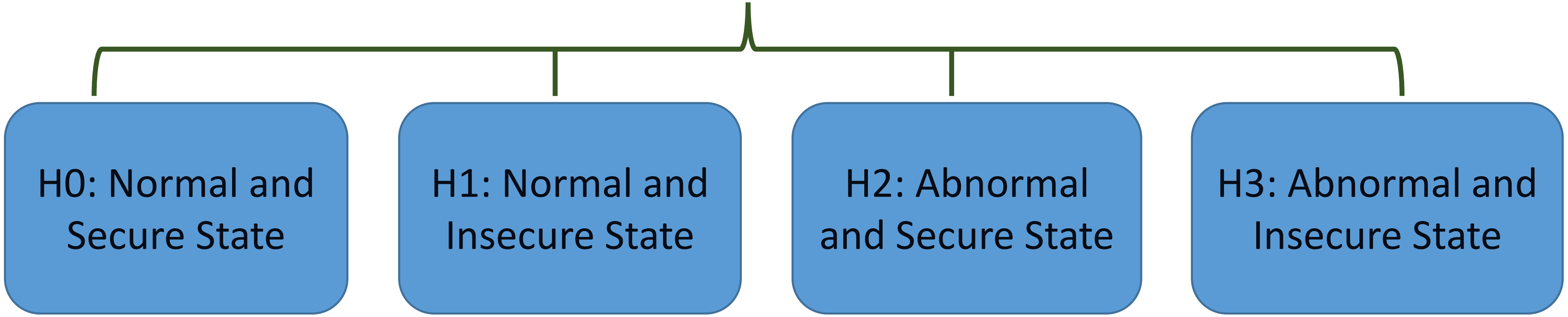


- Two voltage sags were captured on April. 16, 2015 between 10:20 AM – 10:21 AM PDT.
- The voltage sags can be seen in all the µPMUs → 2 separate distribution circuits impacted.
- It led to loss of some loads.

How to Utilize µPMU Data for Security?

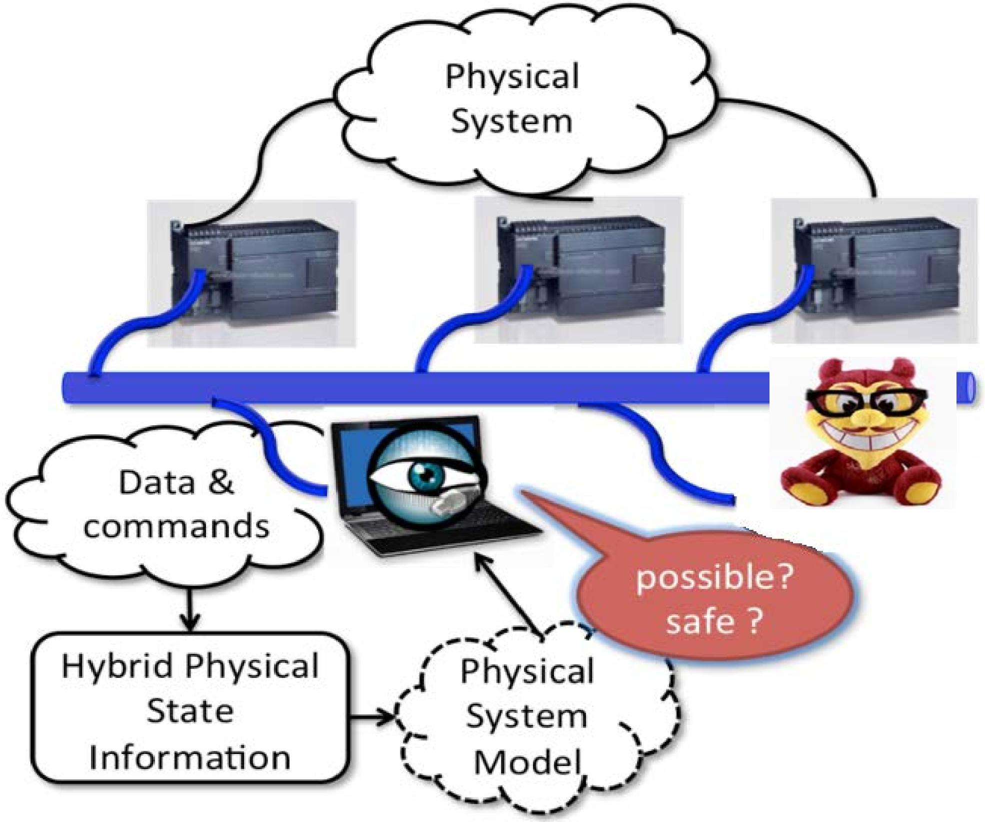
- Deployment of µPMUs significantly increases the detection and classification capabilities of distribution operators.
- Many cyber-attacks targeting the physical layer leave footprints in the µPMU data.
- Detected µPMU data anomalies + knowledge of grid operation

→ grid security status hypotheses testing.



How to leverage Physics?

- Collect real-time measured data from micro phasor measurement units (µPMUs) in the power distribution grid that reflect the physical condition of the system.
- Collect cyber network traffic to and from points in the distribution grid using Bro Intrusion Detection System.
- Using models of distribution grid state, analyze the distribution grid for unsafe operation.
- When anomalies are found, compare deviations from µPMUs with SCADA traffic to determine if cyber event is at cause.



Data Analysis

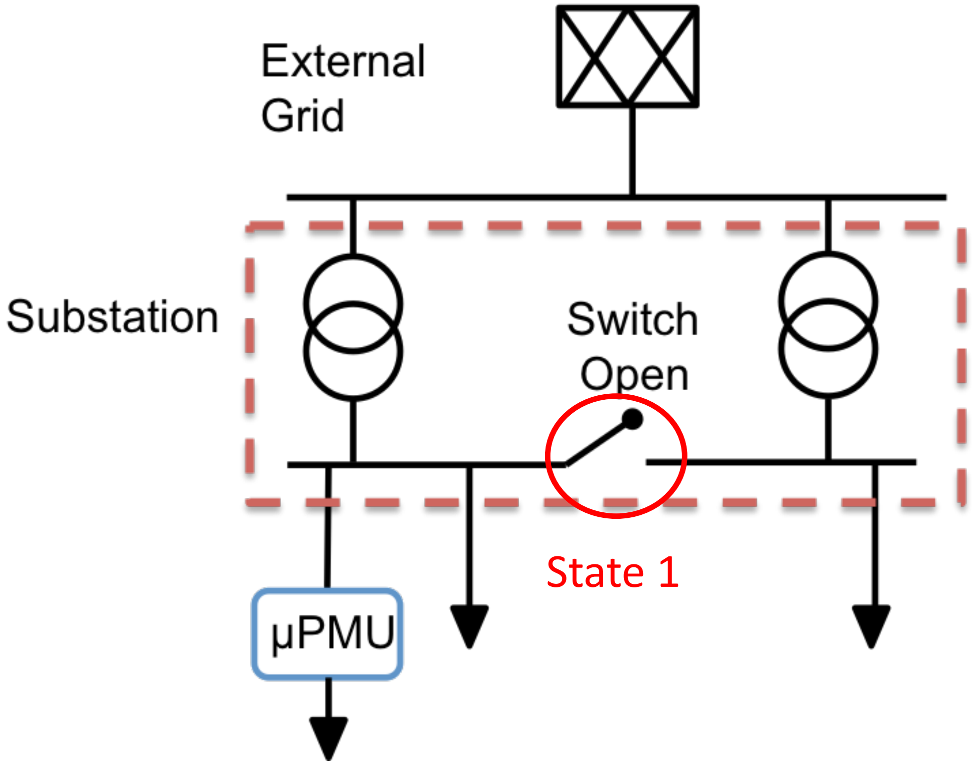
μPMU data functions of interest to be inspected for anomalies are:

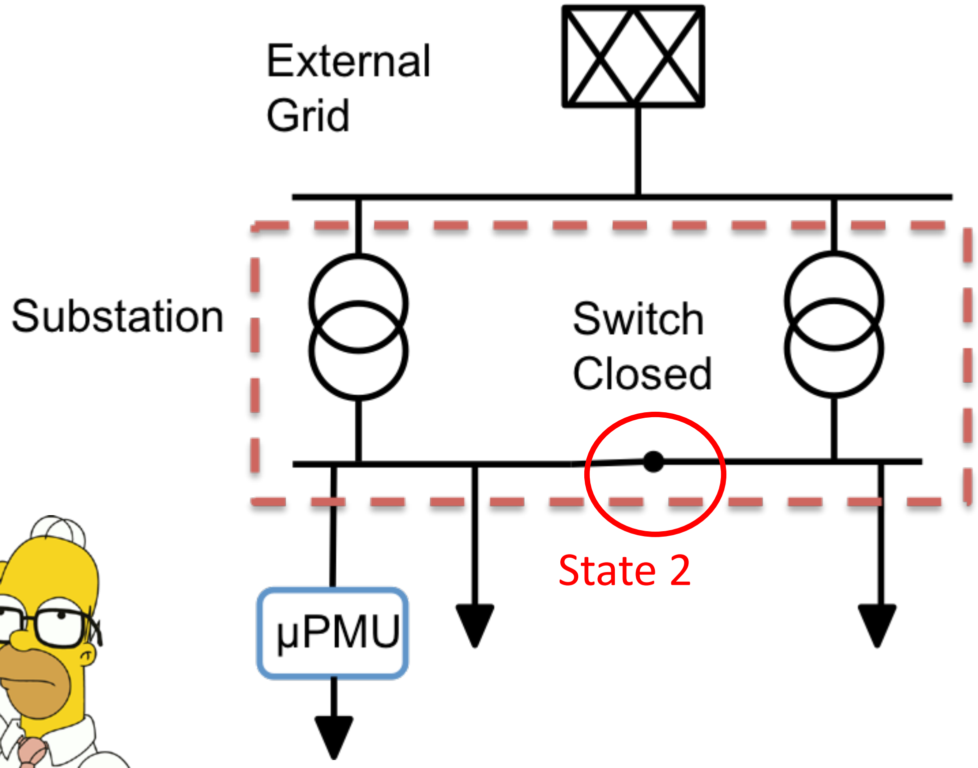
- ✓ Voltage magnitude
- ✓ Frequency
- ✓ Current magnitude
- ✓ Active power
- ✓ Reactive power
- ✓ Governing laws of Physics
  - → Validity of quasi steady-state regime using single or multiple μPMU data.
  - → Source impedance Thevenin changes.

Example: Detecting Reconnaissance Attacks

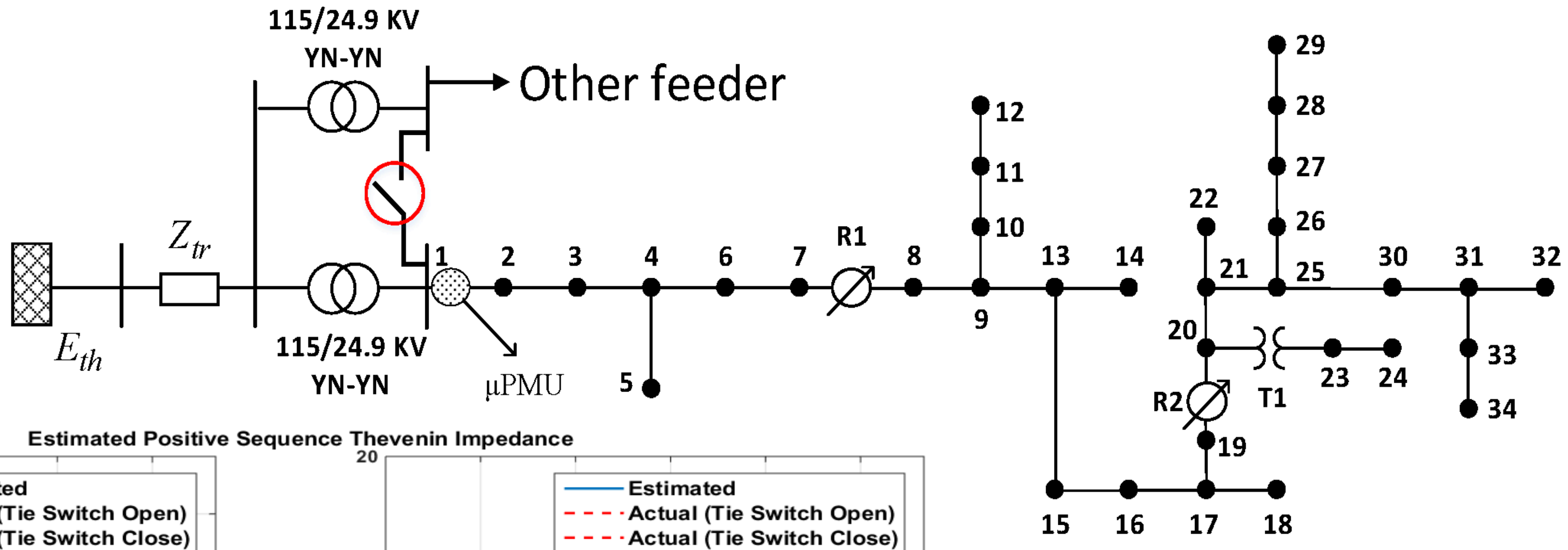
- Attackers are likely to test their ability to control devices/switches prior to attack
- Ukraine attack of December 23rd 2015
  - Attackers appeared to have gained access more than 6 months prior to attack[1]
  - Believed that they tested their capabilities prior to deployment.
- Can we detect these tests and inform operators?
  - Passively monitor and learn networks steady-state behavior
  - Once change has been detected notify operator
  - Operator confirms whether change was intentional or potential attack

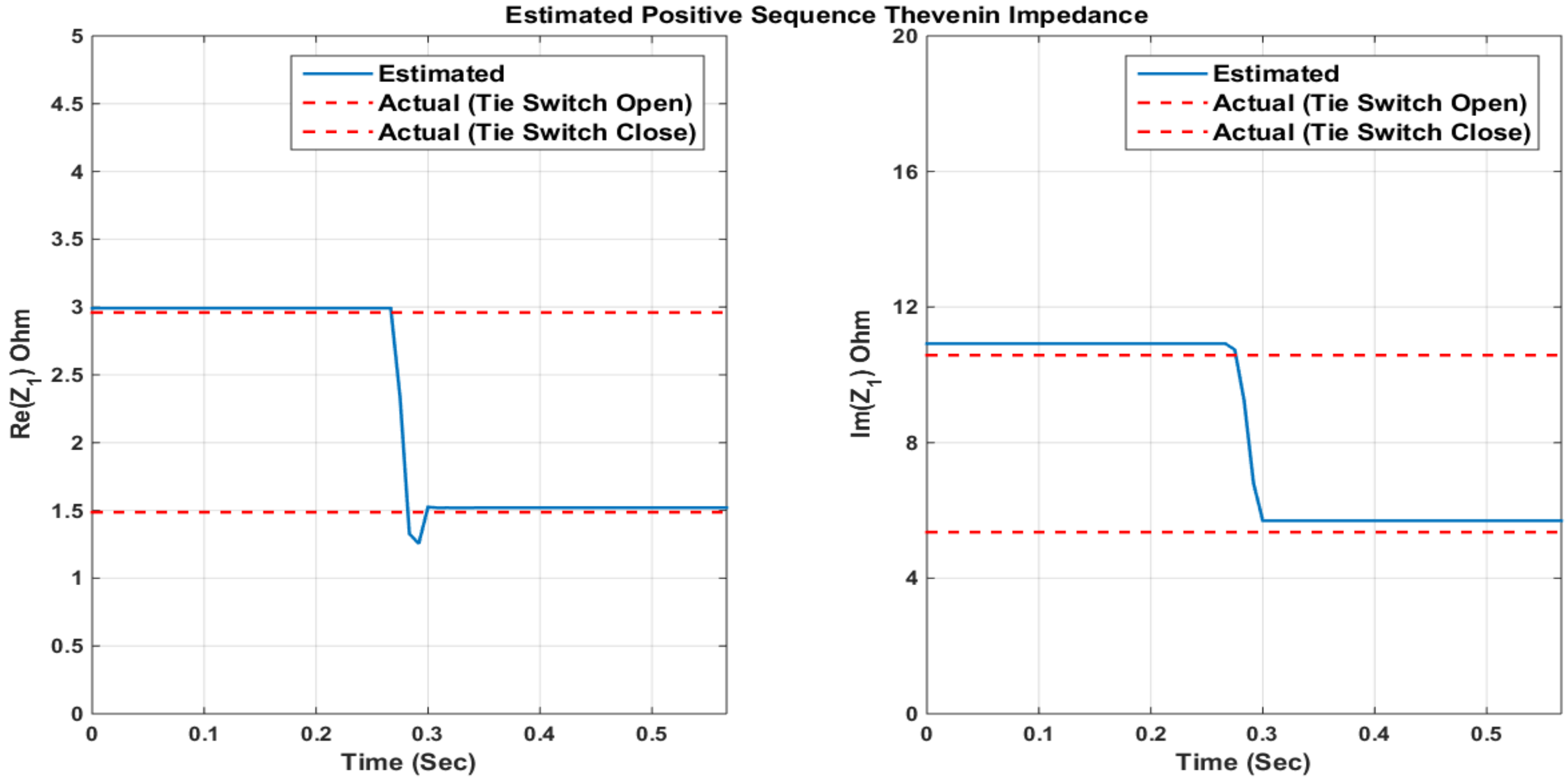
Use Case: Detecting Operation of Bus Tie Switch





- If we are sitting outside the substation can we detect a change of the bus-tie switch?
- Calculation of Thevenin Equivalent Impedance of grid as seen from μPMU can detect such a change - Inform operators of change in status of bus-tie switch.


115/24.9 KV
YN-YN
Other feeder
Z_{tr}
E_{th}
115/24.9 KV
YN-YN
μPMU
R1
R2
T1
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34


Estimated Positive Sequence Thevenin Impedance
Estimated
Actual (Tie Switch Open)
Actual (Tie Switch Close)
Re(Z1) Ohm
Time (Sec)
Estimated
Actual (Tie Switch Open)
Actual (Tie Switch Close)
Im(Z1) Ohm
Time (Sec)

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security