Cyber-Physical Intrusion Detection Incorporating μPMU Measurements in Automated Distribution Systems

Mahdi Jamei, Anna Scaglione

Arizona State University

Emma Stewart, Sean Peisert, Chuck McParland, Ciaran Roberts

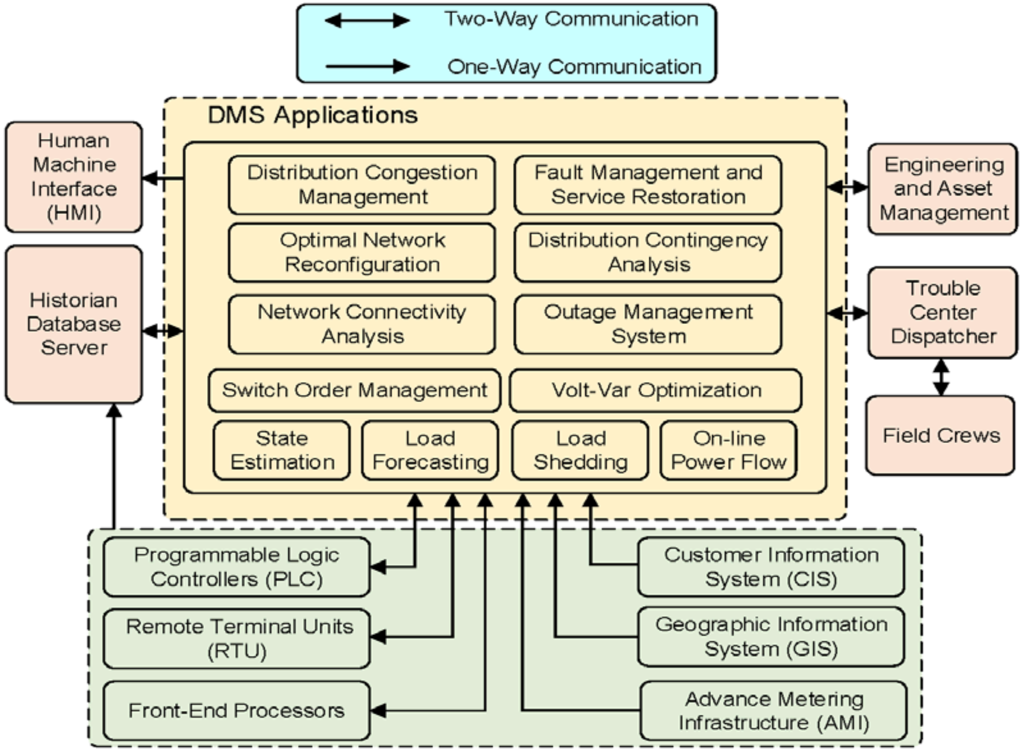
Lawrence Berkeley National Laboratory

Alex McEachern

Power Standards Lab

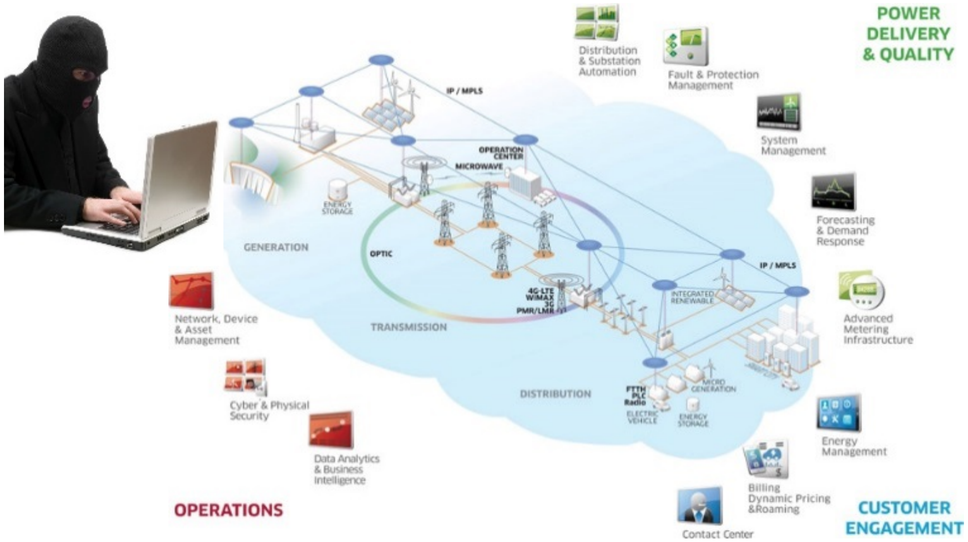
Cyber-Physical Distribution Grid

- Currently, there is some level of automation in distribution circuit, mostly at the medium voltage .
- Automation is moving towards forming Advanced Distribution Management System (ADMS).
- ADMS highly relies on cyber network for data exchange.



Motivation

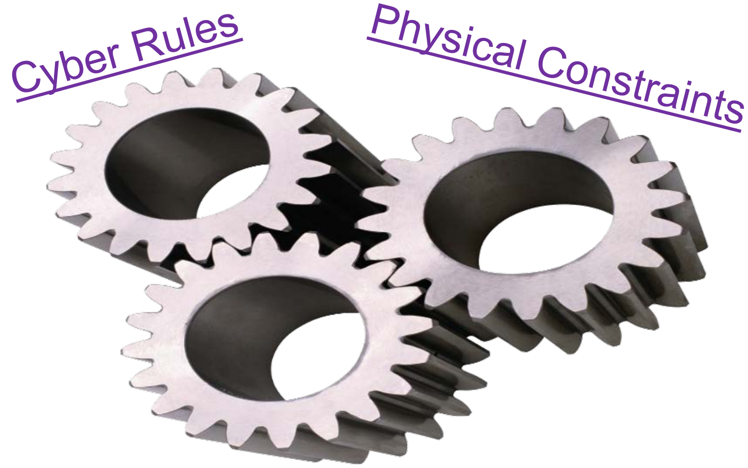
- Common protocols in ADMS (e.g. DNP 3.0, Modbus, ICCP,FTP,…) are not secure by design.
- Firewalls, authentication, cryptography, Intrusion Detection Systems (IDS) are insufficient for Cyber-Physical Systems (CPSs).
- Recent Ukraine power grid attack, Stuxnet malware, Maroochy Water Station wireless jamming attack, are just a few of the many examples.
- The inefficacy is mainly because of divergence from the knowledge of the physics of the system, and safe operation and limits.



Intrusion Detection System (IDS)

What is IDS? NIDS/LIDS inspects the sniffed communication packets to detect anomalies based on the defined security policies.

- Previous works including ours expanded the notion of NIDS leveraging the laws of physics governing the grid operation [1-4].

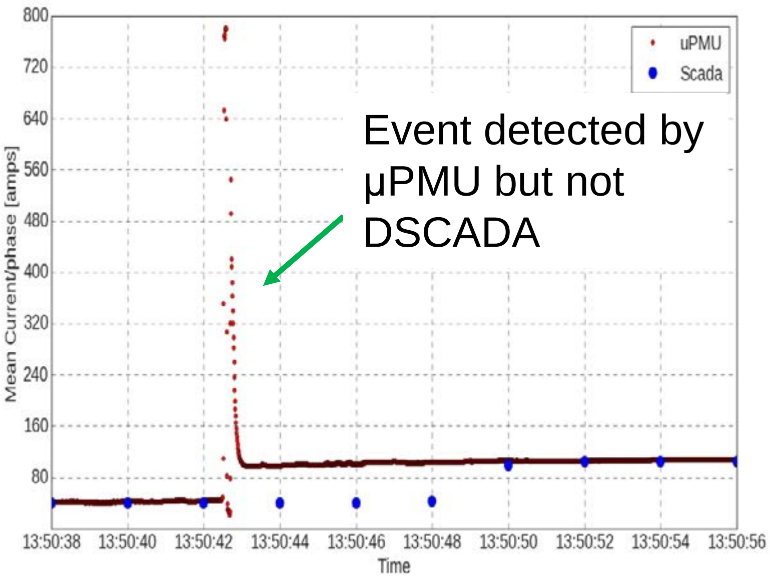


Hybrid-Control NIDS for CPS

- It still remains blind to sophisticated attacks, because:
  - –Physical state of the grid coming from SCADA are not updated at high rate.
  - –False data can be injected at the SCADA data source that misleads the NIDS.

Micro Synchrophasor Data: A Game Changer?

- Low-cost synchrophasor devices developed by our partners at PSL for distribution grid.
- Measuring voltage and current phasor with 120 Hz rate.
- Significantly more information vs event triggered DSCADA data.



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.

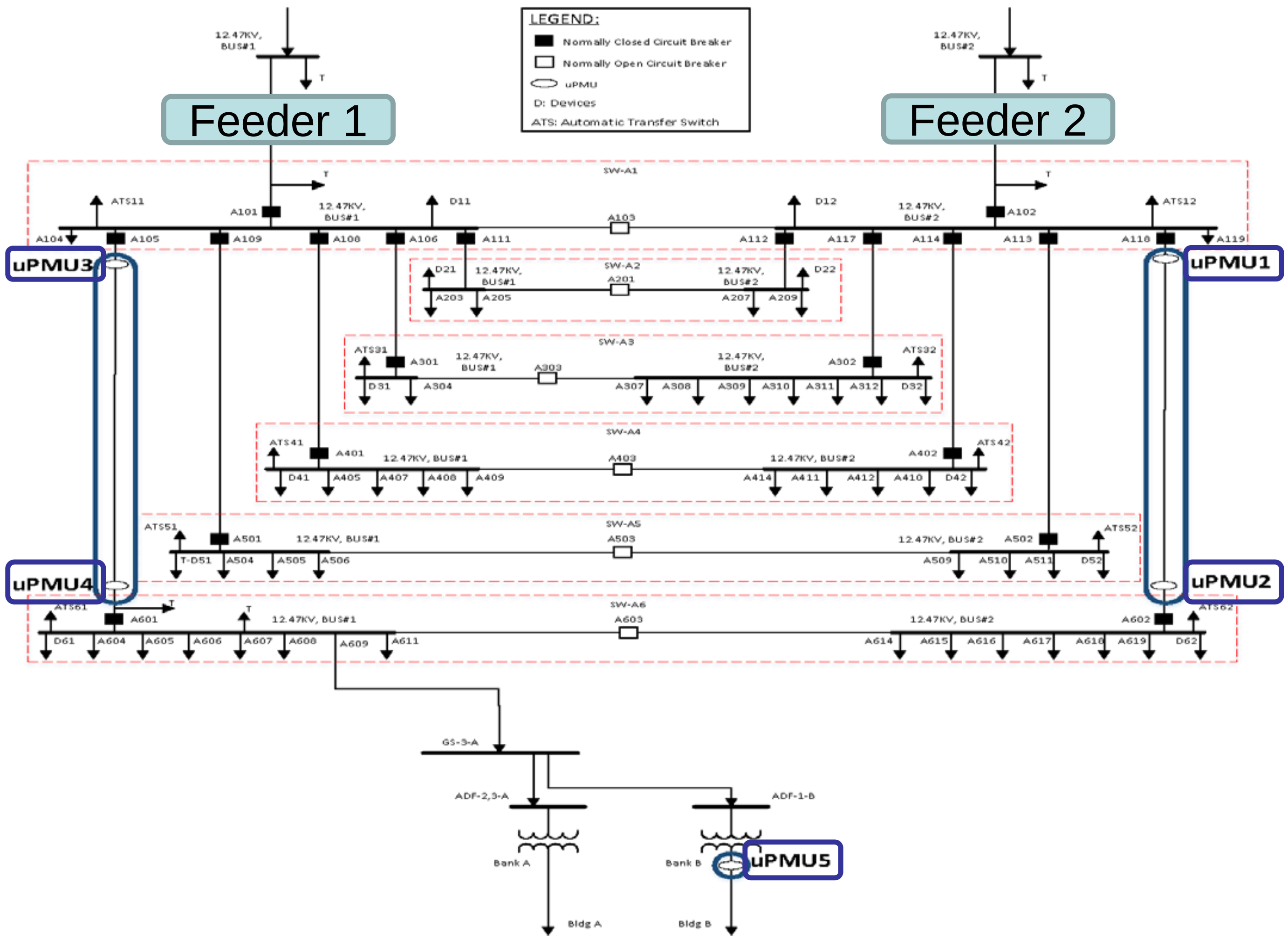
- Detected μPMU anomalies + knowledge of grid operation
  → grid security status hypotheses testing.

  - H0: Normal and Secure State
  - H1: Normal and Insecure State
  - H2: Abnormal and Secure State
  - H3: Abnormal and Insecure State

- Next, we showcase how different hypotheses are formulated through a real event.

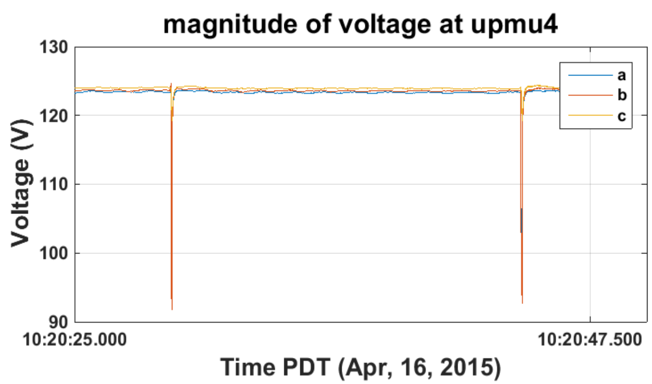
Analysis of a Real Anomaly through µPMU Data

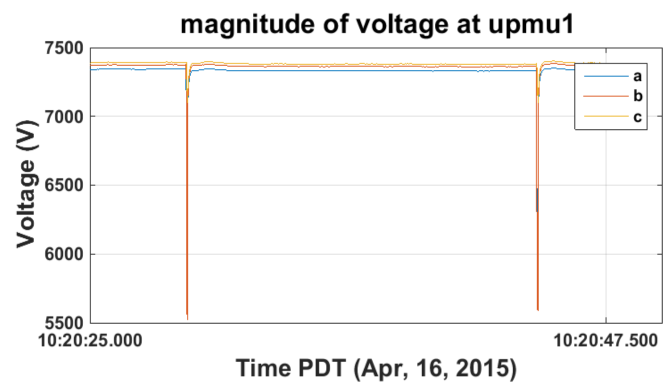
The spots where the µPMUs are installed in the substation

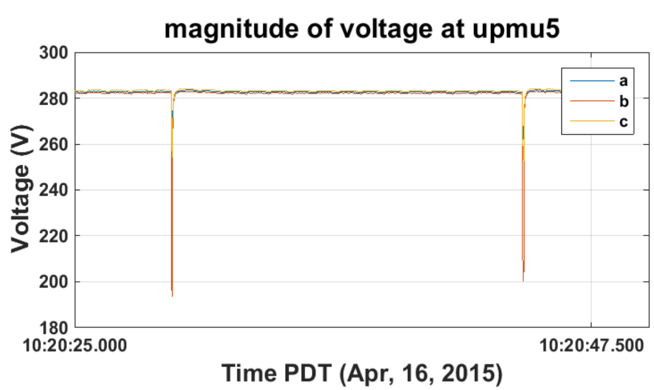


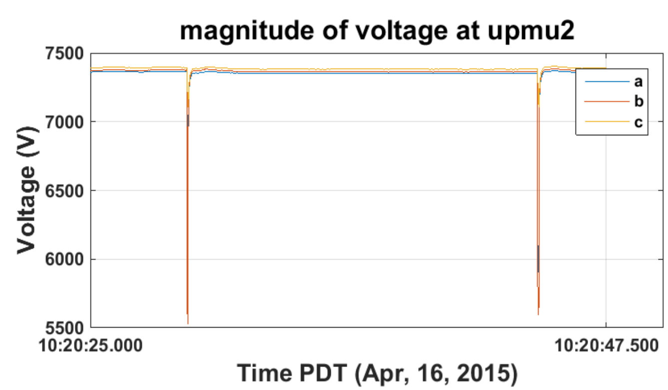
Anomaly Detection

- Two voltage sags were captured at LBNL 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.



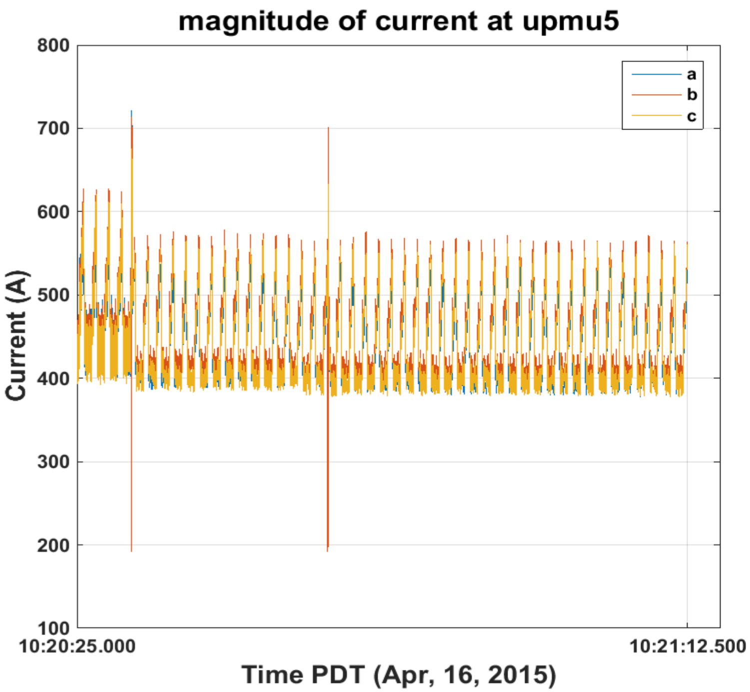


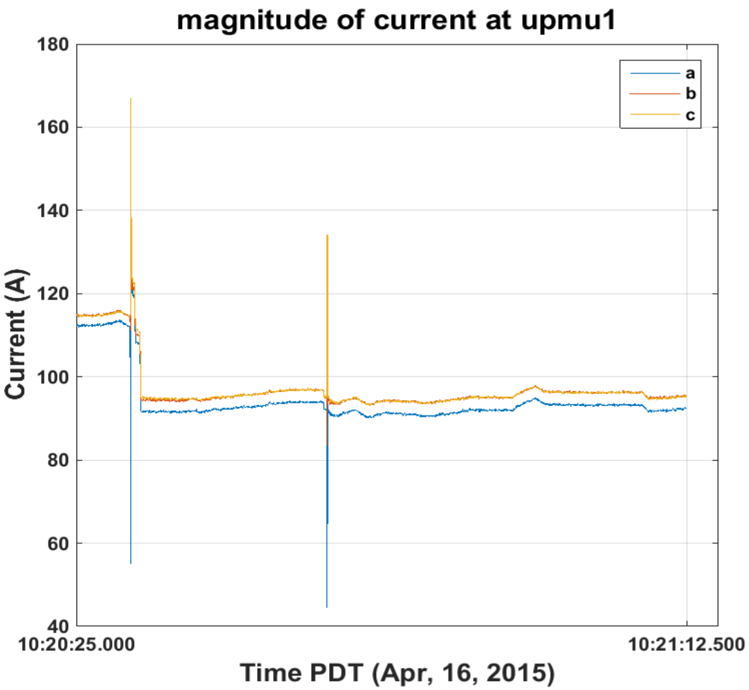




Anomaly Detection

- Two voltage sags were captured at LBNL 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.
- The corresponding current waveforms are also recorded:





Post-Detection Analysis

Observations

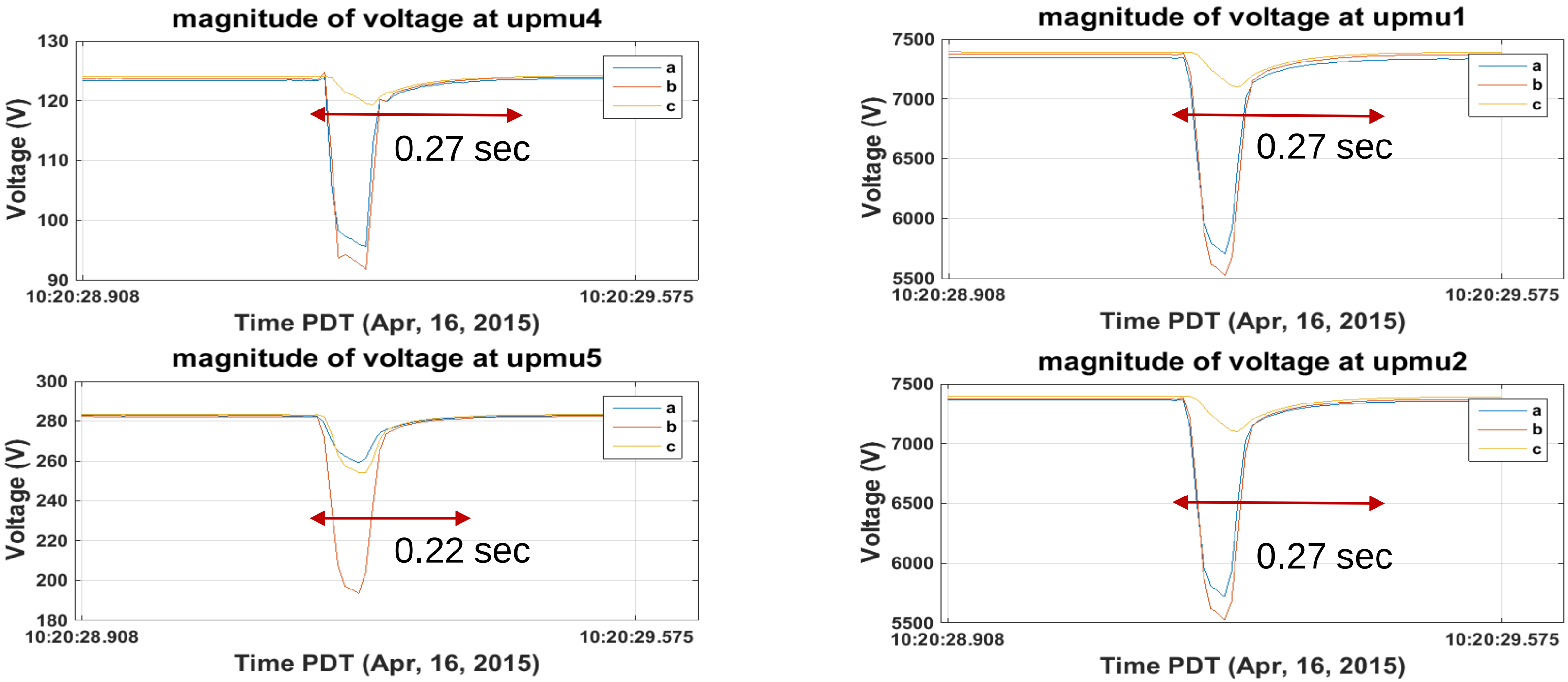
- The voltage reduction percentage (severity of voltage sag) is almost similar on the right side (µPMU 1) and left side (µPMU 4).

µPMU No. / Voltage reduction %	µPMU 1, 4	µPMU 5
Phase a	22 %	8.5 %
Phase b	25 %	45 %
Phase c	3.94 %	10.37 %

Post-Detection Analysis

<u>Observations</u>

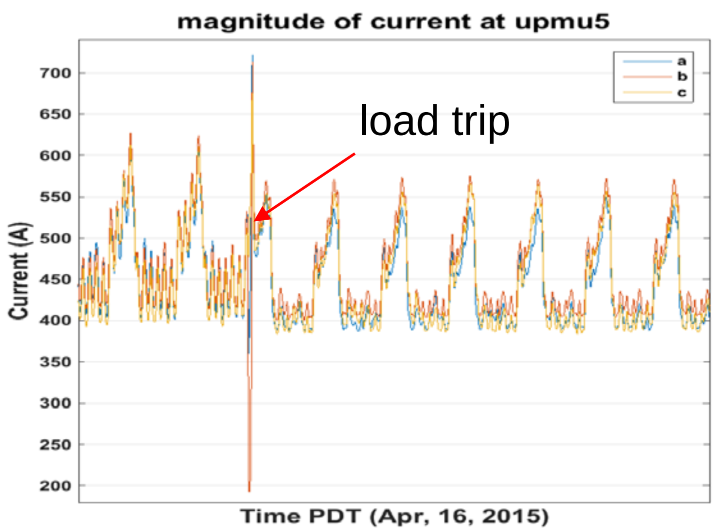
- The voltage reduction percentage (severity of voltage sag) is almost similar on the right side (µPMU 1) and left side (µPMU 4).
- The start time of voltage sag is the same in all the µPMUs.
- The voltage sag lasts for a duration of 0.22 - 0.27 sec.

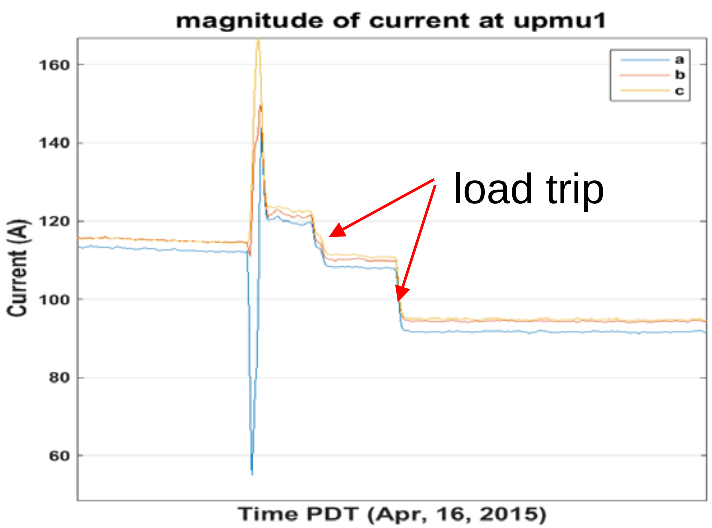


Post-Detection Analysis

Observations

- The voltage reduction percentage (severity of voltage sag) is almost similar on the right side (µPMU 1) and left side (µPMU 4).
- The start time of voltage sag is the same in all the µPMUs.
- The voltage sag lasts for a duration of 0.22 - 0.27 sec.
- Some of the load protection switches tripped including the one for a non-linear load in the Bank B.

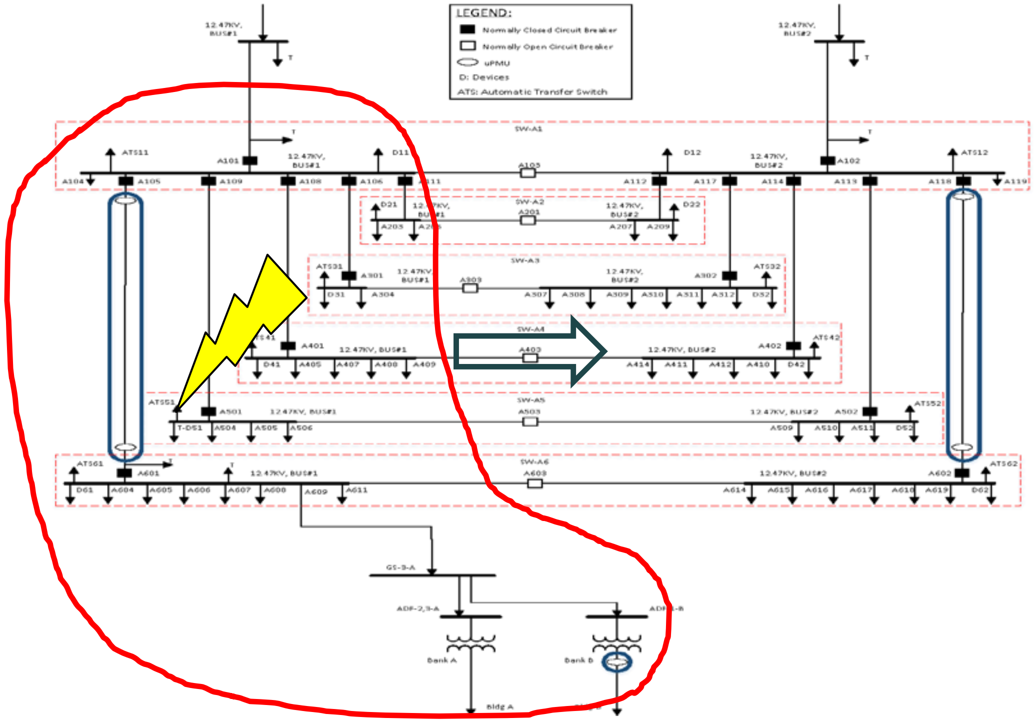




Post-Detection Analysis (cntd.)

Hypotheses Formulation & Testing:

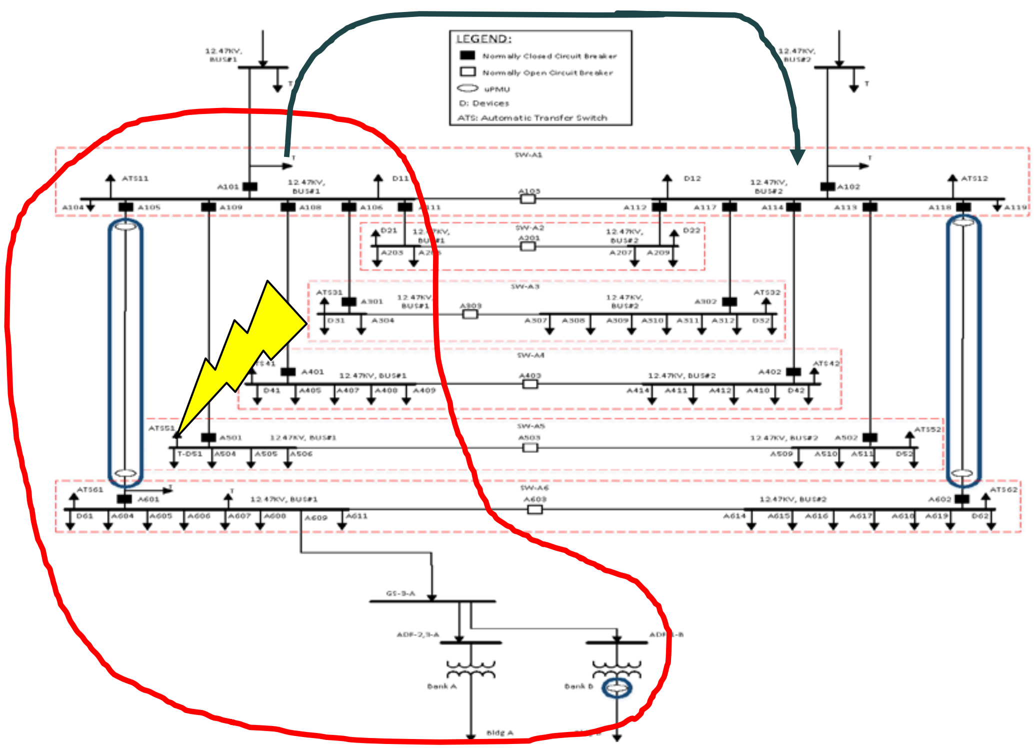
- Fault at one of the two feeders and spreading to the other one through the closed Normally Open (N.O.) breakers?
- N.O. breakers are activated either after fault clearance for energy restoration, or before fault clearance by attacker. So, sag either does not transfer, or transfers with delay.



Post-Detection Analysis (cntd.)

Hypotheses Formulation & Testing:

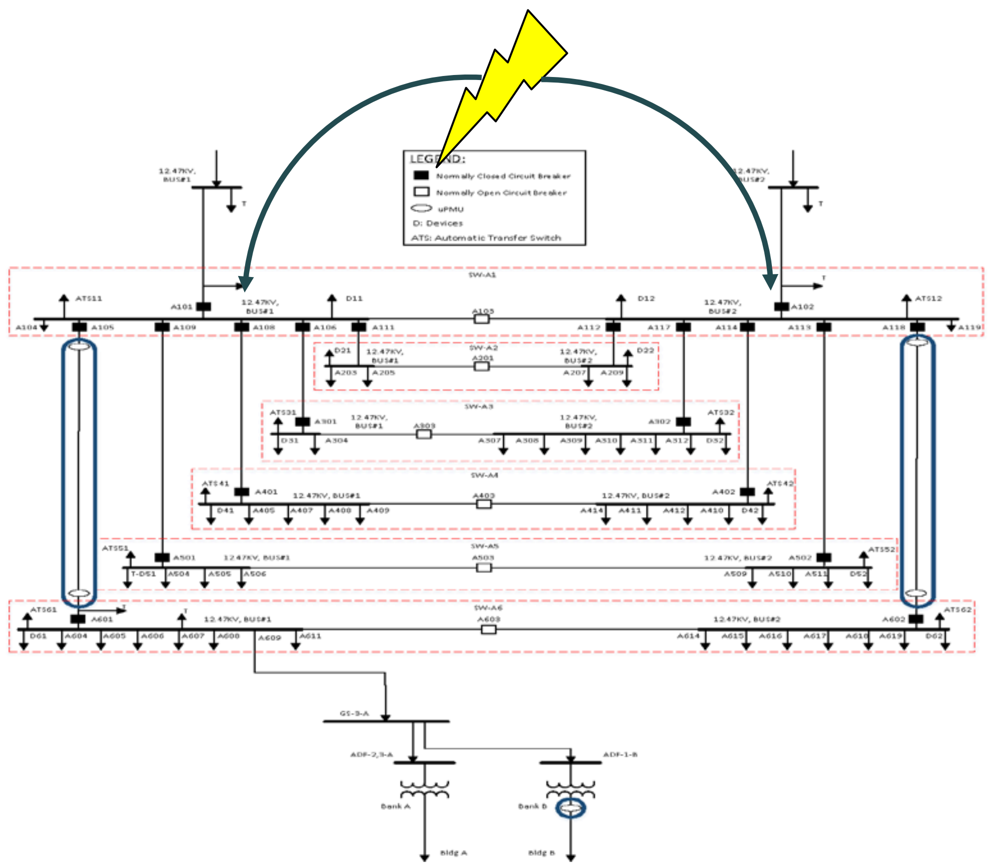
- Fault at one of the two feeders and spreading to the other one through subtransmission?
- Only plausible if the transmission grid is not stiff with respect to transients compared to the distribution feeders.



Post-Detection Analysis (cntd.)

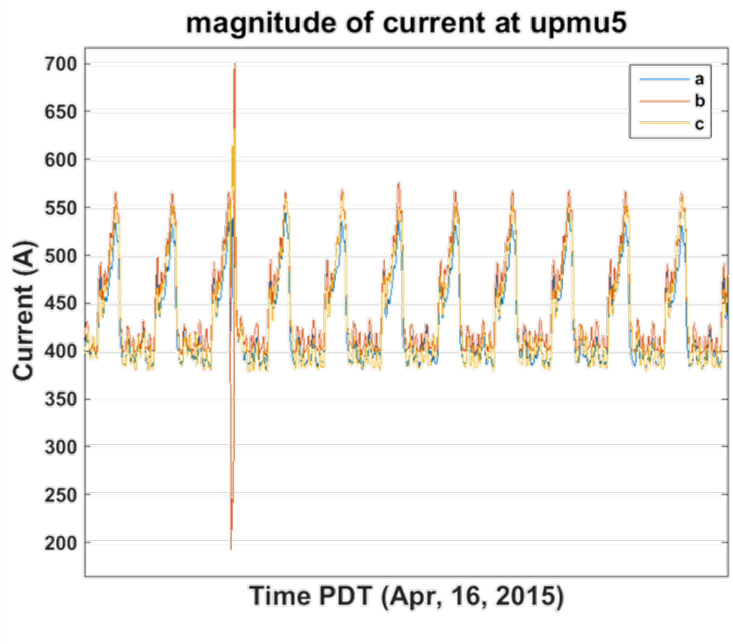
Hypotheses Formulation & Testing:

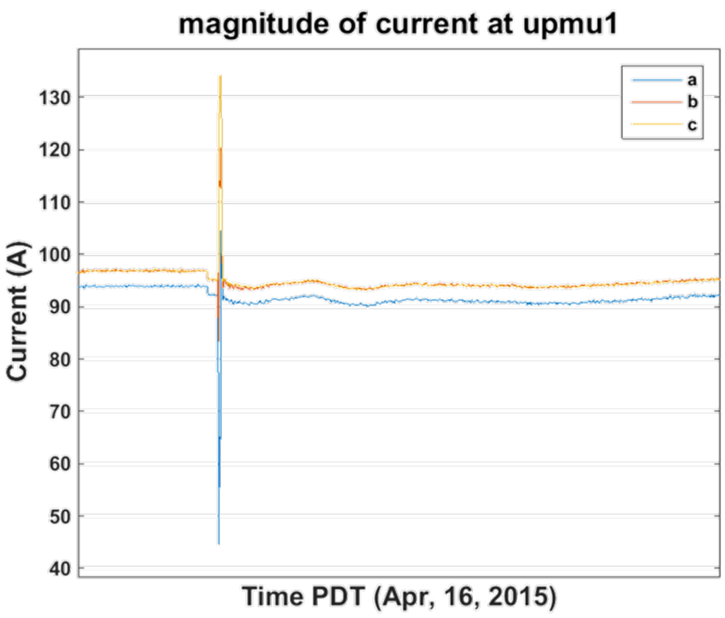
- Remote transmission level fault?
- ✓ voltage sags seen concurrently with the same severity in both feeders.



Second sag

- The second sag is most probably a recloser sag.
- However, since sensitive loads to this sag are already tripped, we do not see change of current before and after sag.





Three Phase Degree of Unbalance

- The data are projected as follows:

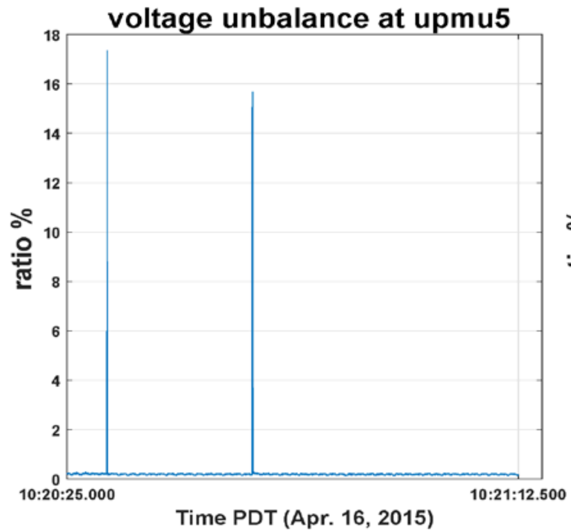
$$\vec{P} = (1, e^{-j2\pi/3}, e^{-j4\pi/3})^T$$

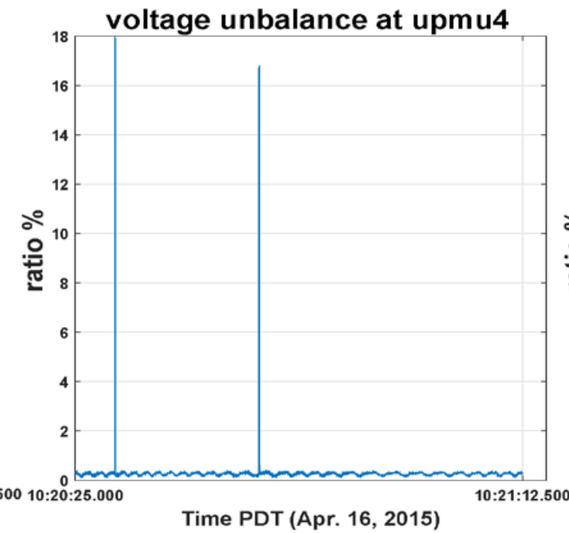
$\vec{X}[k]$: Three phase voltage/current phasor at time k

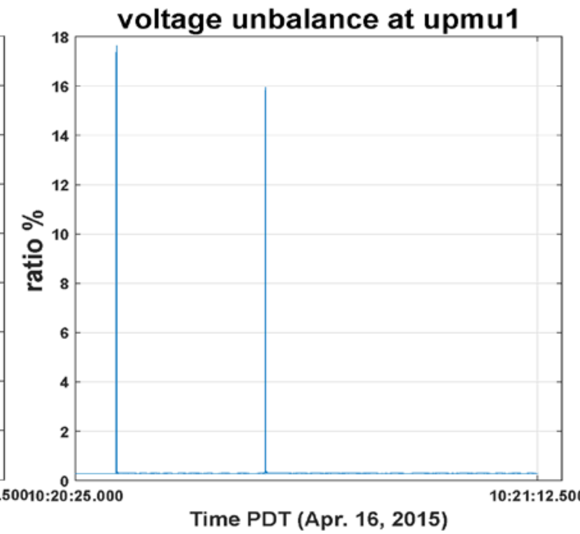
$$\vec{X}[k] = a_1[k]\vec{P} + a_2[k]\vec{e}_2 + a_3[k]\vec{e}_3$$

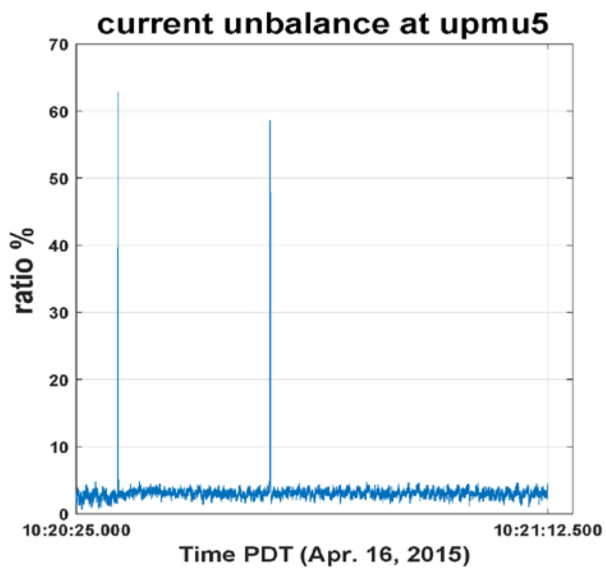
$$U[k] = \frac{\sqrt{a_2^2[k] + a_3^2[k]}}{|a_1[k]|} \times 100 \quad \text{Unbalanced Ratio}$$

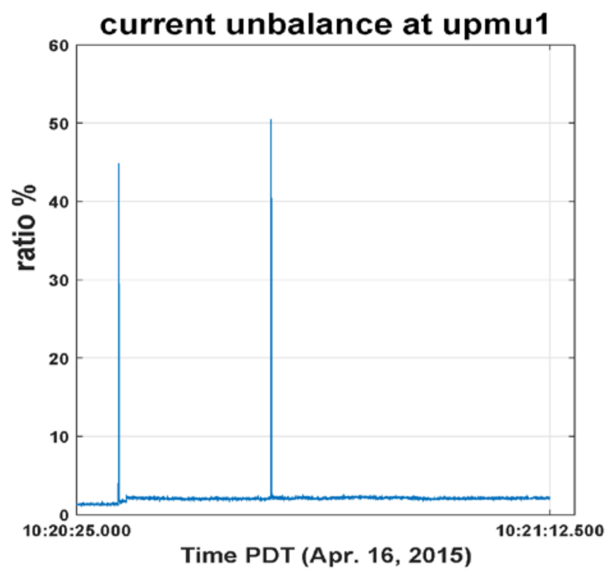
Three Phase Degree of Unbalance











Three Phase Degree of Unbalance

- The data are projected as follows:

$$\vec{P} = (1, e^{-j2\pi/3}, e^{-j4\pi/3})^T$$

$\vec{X}[k]$: Three phase voltage/current phasor at time k

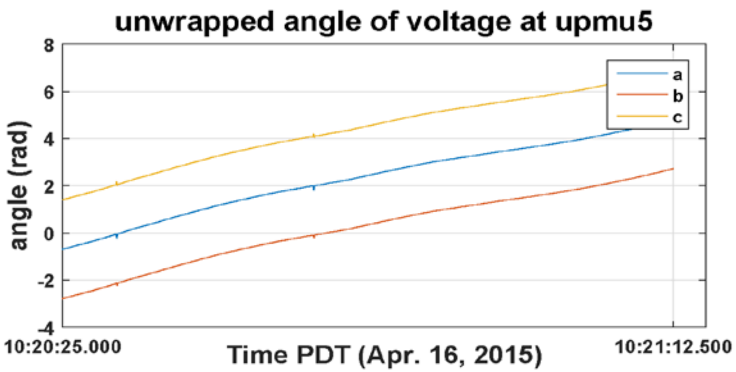
$$\vec{X}[k] = a_1[k]\vec{P} + a_2[k]\vec{e}_2 + a_3[k]\vec{e}_3$$

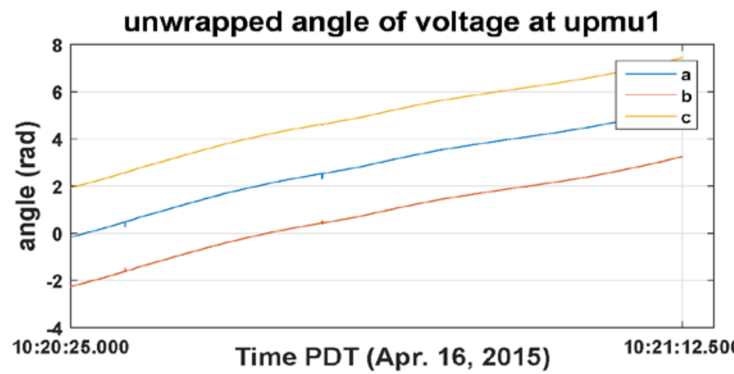
$$U[k] = \frac{\sqrt{a_2^2[k] + a_3^2[k]}}{|a_1[k]|} \times 100 \quad \text{Unbalanced Ratio}$$

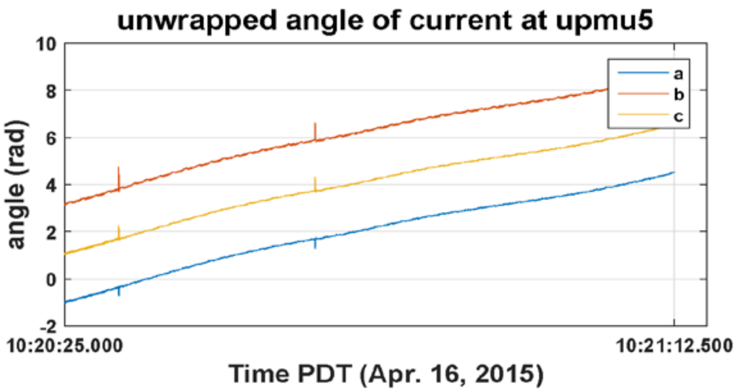
- The system unbalanced degree peaks at the voltage sags.
- Current waveform faces higher degree of unbalanced during voltage sags.
- Appropriate signature of the anomaly in the system.

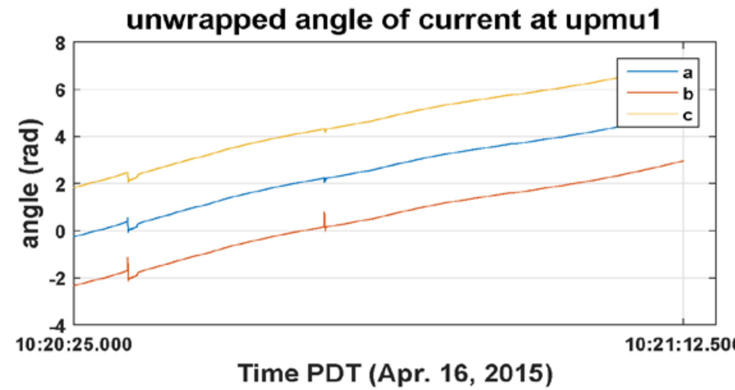
Unwrapped Phasor Angle $d_i[k]$

- The voltage phase angle is less indicative than the magnitude of voltage data for the anomaly.
- The changes in the current phase angle reveal the anomaly, and point to the fact that some phases being more affected.





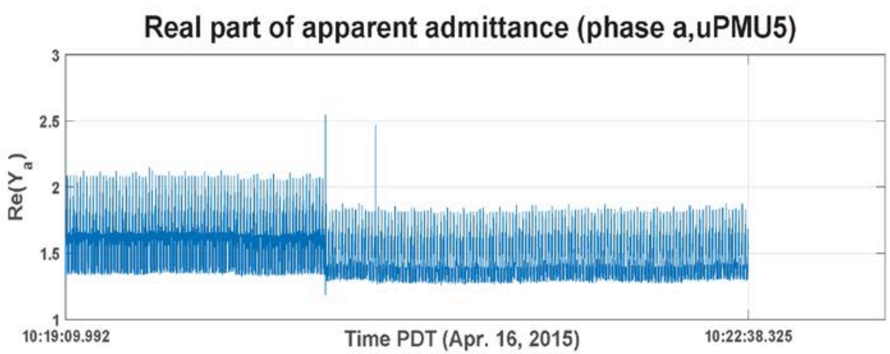


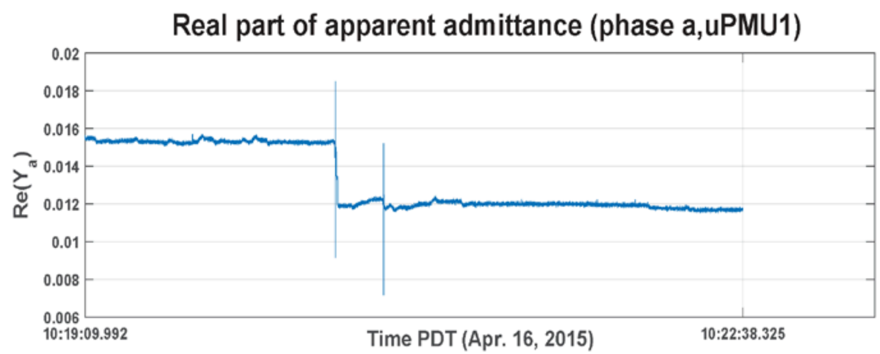


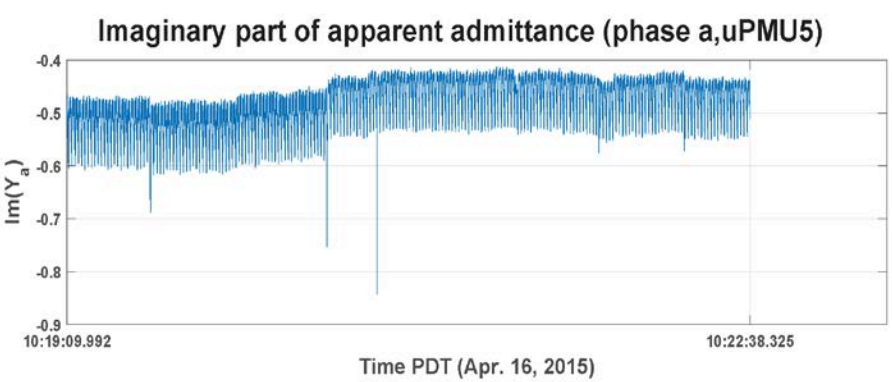
Apparent Admittance

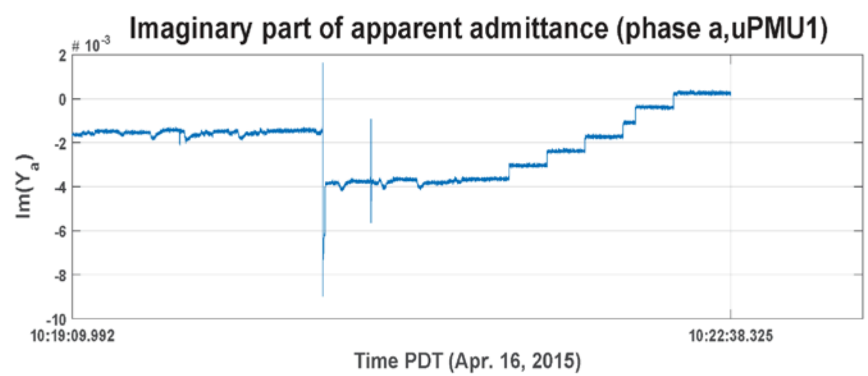
The apparent admittance measured by each µPMU is:

$$Y_i[k] = \frac{I_i[k]}{V_i[k]} \qquad i = a,b,c$$







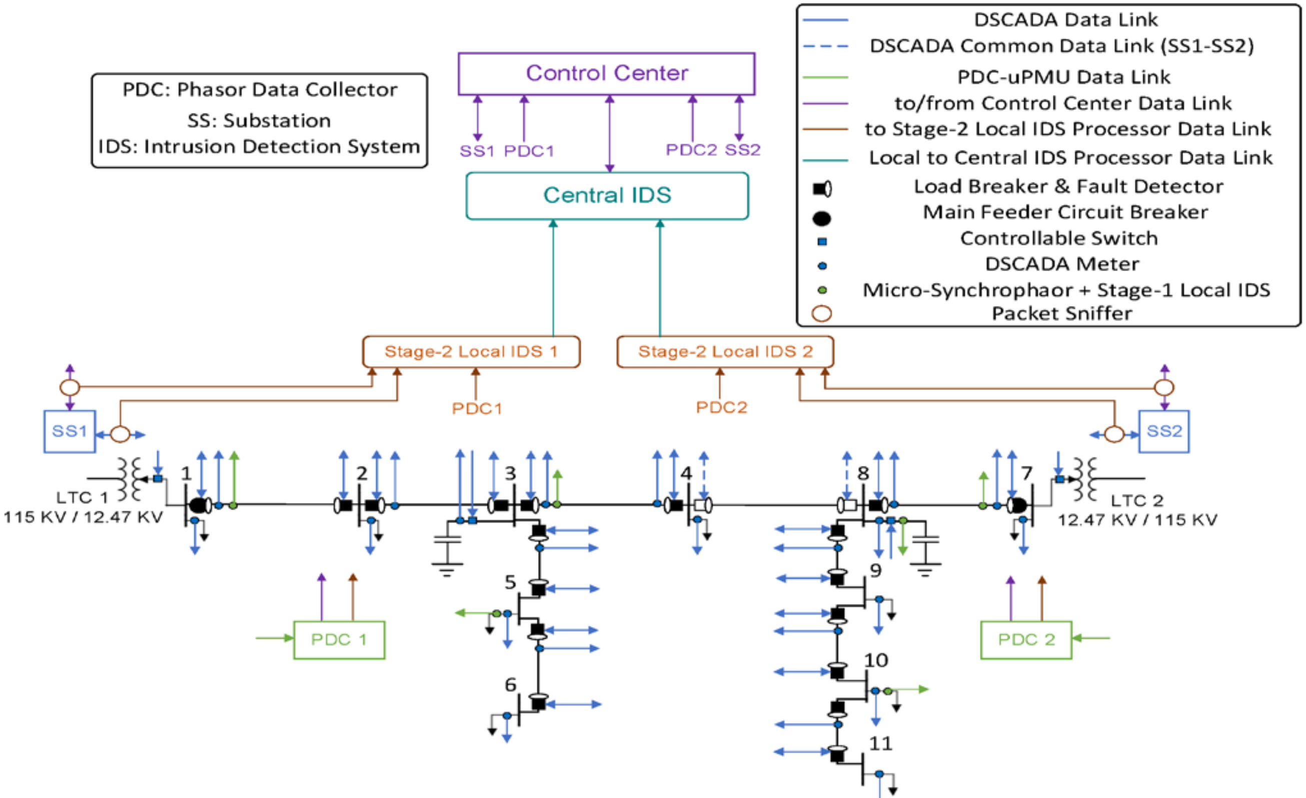


Lessons Learned

- Proof of μPMU ability in capturing grid anomalies.
- Ability to reason about different grid behaviors, which was not possible using just DSCADA data.
- Further verification about the cause of the event requires the DSCADA data to be checked (e.g. the status of the switches during the event).
- Some signatures are more indicative compared to others depending on the type of event.

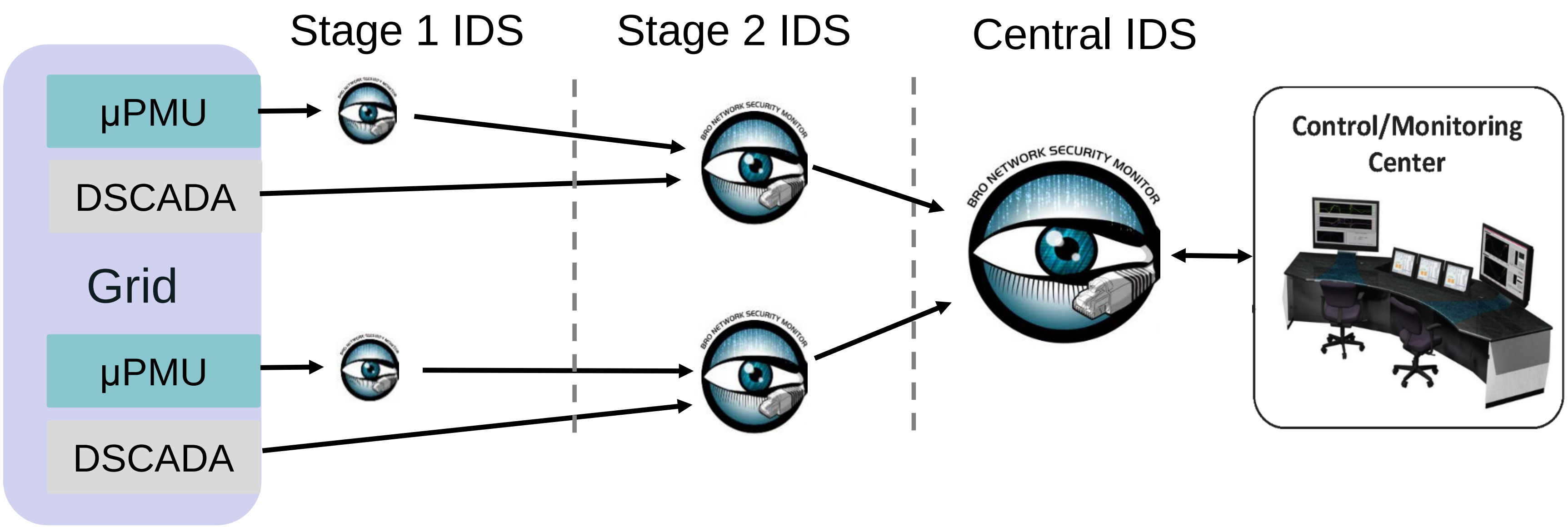
All-Embracing IDS Framework

- The goal is to combine high resolution μPMU data & sniffed DSCADA for Intrusion Detection.
- We envision the following framework:



Security Rules

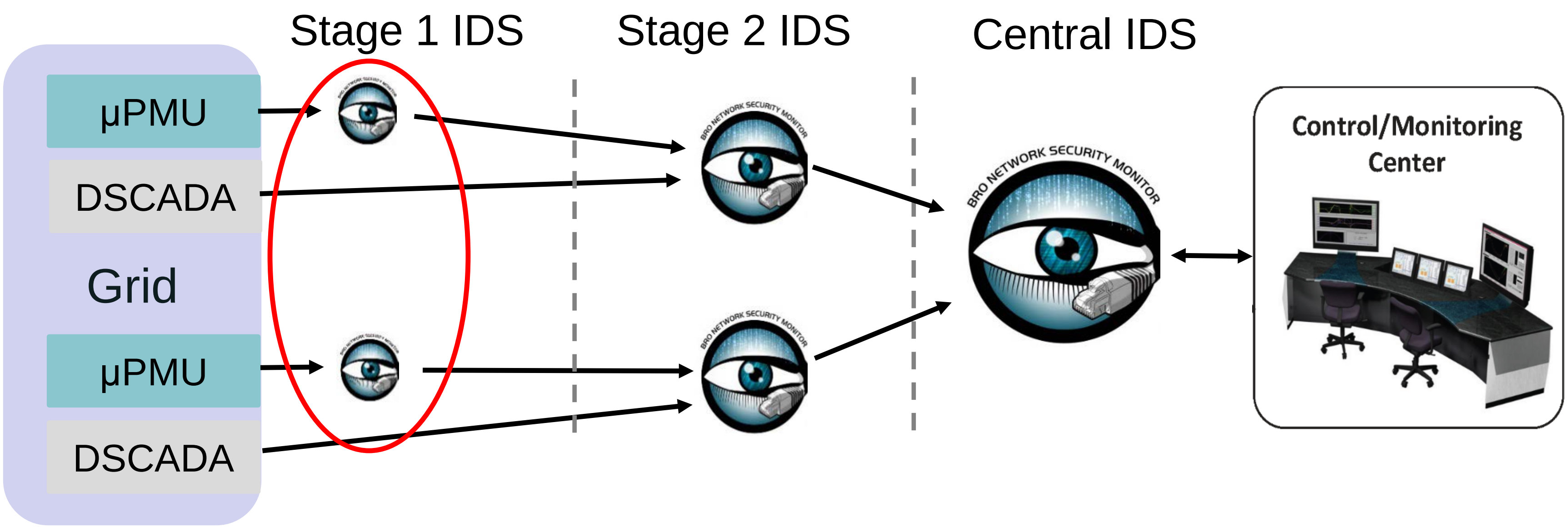
- The security policies are translated to mechanisms under our hierarchical BRO framework.



Security Rules

•The security policies are translated to mechanisms under our hierarchical BRO framework.

What happens at Stage 1 IDS (next to each μPMU)?



Security Rules

- The security policies are translated to mechanisms under our hierarchical BRO framework.

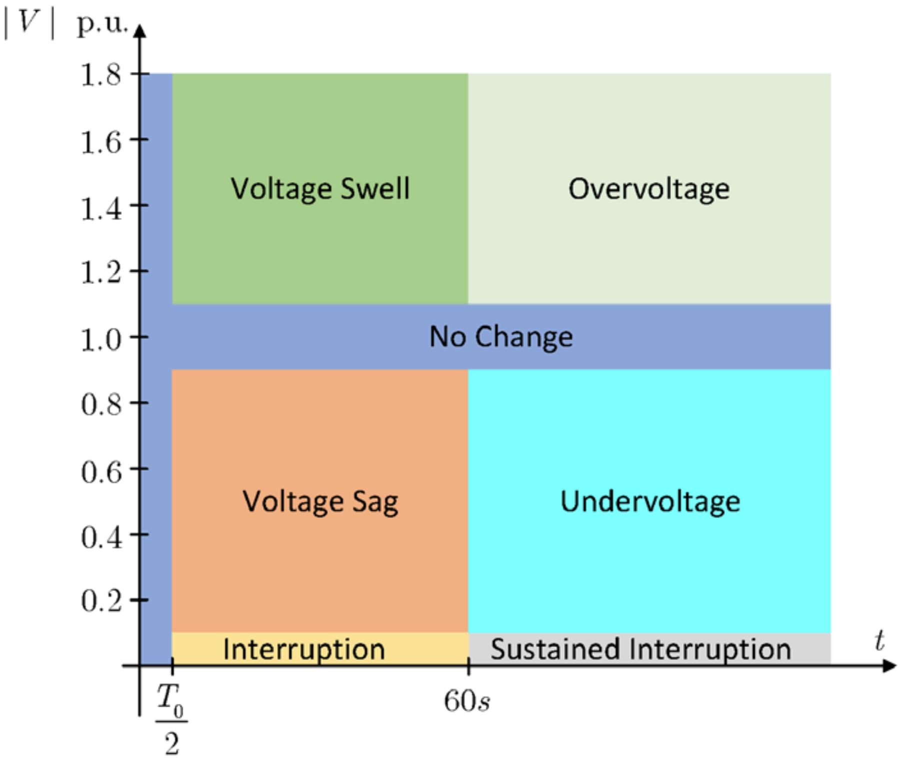
What happens at Stage 1 IDS (next to each μPMU)?

✓Detect anomalies in the voltage phasor magnitude *(static rules).*

✓Detect anomalies in current phasor magnitude, active, and reactive power, degree of balanced, and apparent admittance *(dynamic rules).*

✓Pre-processing data for stage-2 local IDS (e.g. anomaly start time, end time, behavior,…).

Stage1 Rules



VOLTAGE MAGNITUDE ANOMALIES

anomaly	signature [1]
(a_1) voltage sag	$0.1 \le \lvert V\rvert \le 0.9,\ T_0/2 \le t \le 60s$
(a_2) voltage swell	$1.1 \le \lvert V\rvert \le 1.8,\ T_0/2 \le t \le 60s$
(a_3) interruption	$\lvert V\rvert < 0.1,\ T_0/2 \le t \le 60s$
(a_4) sustained interruption	$\lvert V\rvert < 0.1,\ t > 60s$
(a_5) undervoltage	$0.1 \le \lvert V\rvert \le 0.9,\ t > 60s$
(a_6) overvoltage	$1.1 \le \lvert V\rvert \le 1.8,\ t > 60s$

$$\vec{P} = (1, e^{-j2\pi/3}, e^{-j4\pi/3})^T$$

$\vec{X}[k]$: Three phase voltage/ current phasor at time k

$$\vec{X}[k] = a_1[k]\vec{P} + a_2[k]\vec{e}_2 + a_3[k]\vec{e}_3$$

$$U[k] = \frac{\sqrt{a_2^2[k] + a_3^2[k]}}{|a_1[k]|} \times 100 \quad \text{Unbalanced Ratio}$$

$U[k] > \text{limit}[k]$ Anomaly

$U[k] \le \text{limit}[k]$ Normal

Stage1 Rules (fast change detection[5])

$$X_i[k] = |I_i[k]| \,/\, P_i[k] \,/\, Q_i[k] \,/\, d_i[k] \,/\, \mathrm{Re}\{Y_i[k]\} \,/\, \mathrm{Im}\{Y_i[k]\} \qquad i = a,b,c$$

$$X_i[k] = \mu_i[k] + w_i[k] \qquad \begin{cases} \mu_i[k] \text{ process mean at time k} \\ w_i[k]: \ \mathrm{N}(0,\sigma_i[k]) \text{ process noise at time k} \end{cases}$$

- For each process, we look for fast changes in the mean :

  H_0 : no change is detected

  H_1 : change is detected → What is the time of change?

$$f_{X_i|\mathrm{H}_0}[k] = \prod_{n=0}^{k} f_{X_i}(x_i[n];\mu_{i,0})$$

$$f_{X_i|\mathrm{H}_1}[k,k_c] = \prod_{n=0}^{k_c-1} f_{X_i}(x_i[n];\mu_{i,0}) \prod_{n=k_c}^{k} f_{X_i}(x_i[n];\mu_{i,1})$$

$\mu_{i,0}$: mean before change, $\mu_{i,1}$: mean after change, k_c : time of change

$$L_{X_i}[k,k_c] = \ln\left(\frac{f_{X_i|\mathrm{H}_1}[k,k_c]}{f_{X_i|\mathrm{H}_0}[k]}\right) \Rightarrow G_{X_i}[k] = \max_{1 \le k_c \le k} L_{X_i}[k,k_c]$$

$$\text{if } G_{X_i}[k] > \alpha \quad \text{decide } \mathrm{H}_1 \Rightarrow \hat{k}_c = \arg\max_{1 \le k_c \le k} L_{X_i}[k,k_c]$$

Stage1 Rules (fast change detection[5])

$$X_i[k] = |I_i[k]| \,/\, P_i[k] \,/\, Q_i[k] \,/\, d_i[k] \,/\, \mathrm{Re}\{Y_i[k]\} \,/\, \mathrm{Im}\{Y_i[k]\} \qquad i = a,b,c$$

$$X_i[k] = m_i[k] + w_i[k] \qquad \begin{cases} m_i[k] \text{ process mean at time k} \\ w_i[k] : \ \mathrm{N}\,(0, s_i[k]) \text{ process noise at time k} \end{cases}$$

- For each process, we look for fast changes in the mean :

  H_0 : no change is detected

  H_1 : change is detected → What is the time of change?

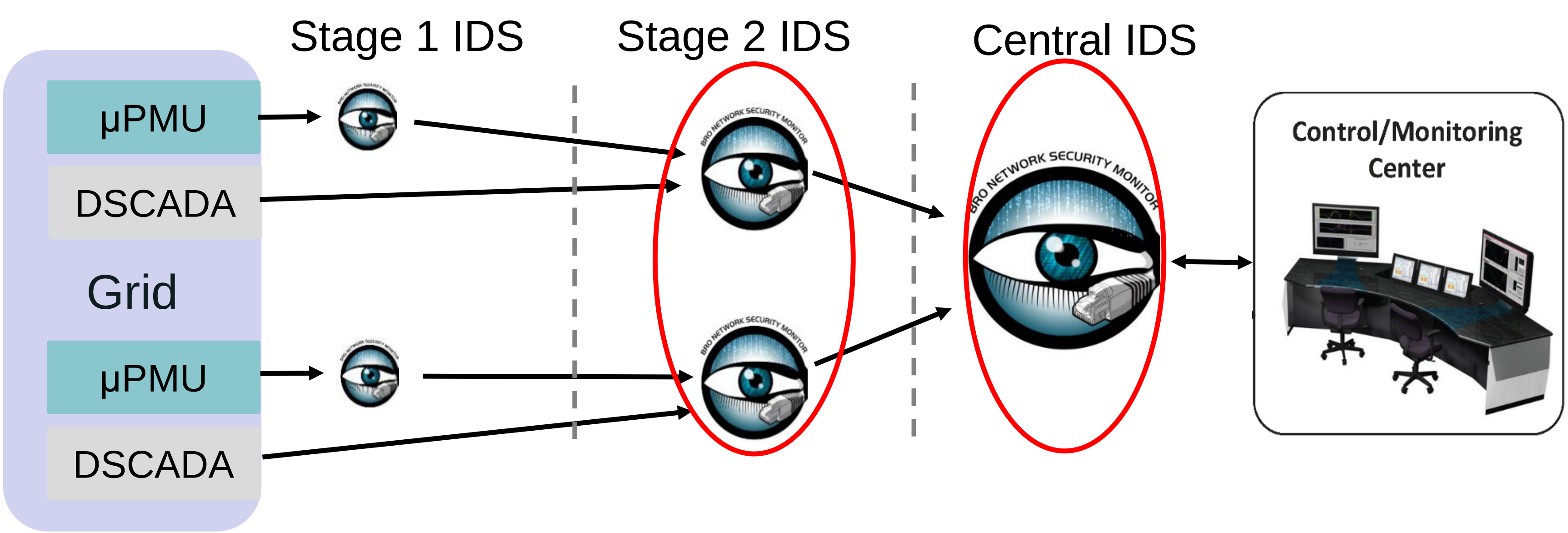
✓ The test is implemented recursively.

✓ Multiple changes are detected by resetting the algorithm after each change is found.

✓ We label anomalies by <u>surge</u>, <u>drop</u>, and <u>swing</u>.

Stage2 and Central IDS Rules

<u>What happens at Stage 2 and Central IDS?</u>



Stage2 and Central IDS Rules

What happens at Stage 2 and Central IDS?

❑ *Stage 2:*

✓Check the compliance of the reported event from stage 1 with the DSCADA traffic and other μPMUs.

✓Formulate and test additional hypotheses about the event cause with local grid picture.

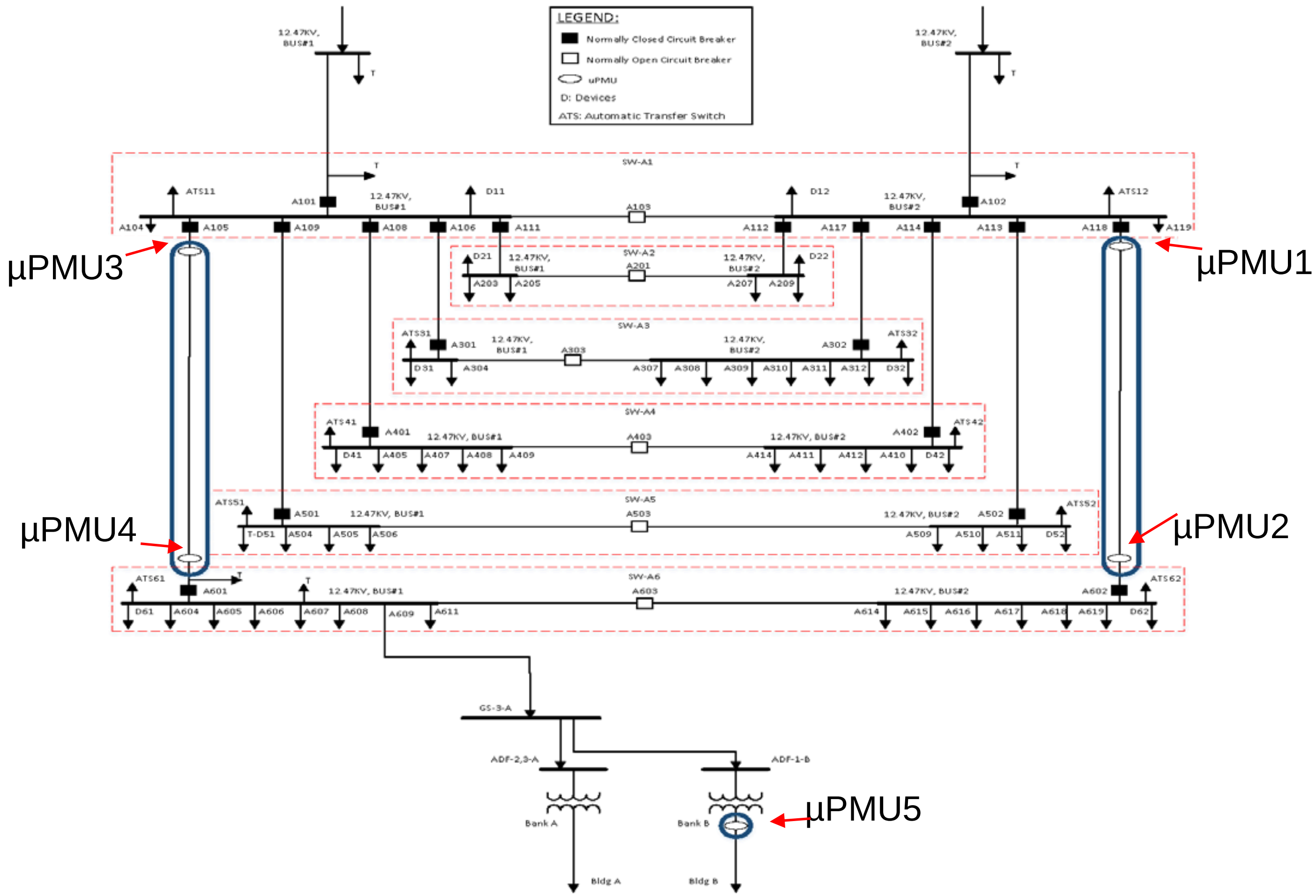
❑ *Central:*

✓Check the compliance of the reported event from stage 2 with the DSCADA traffic and other μPMUs.

✓Formulate and test final set of hypotheses about the event cause with full grid picture.

Examples of Stage2 and Central IDS

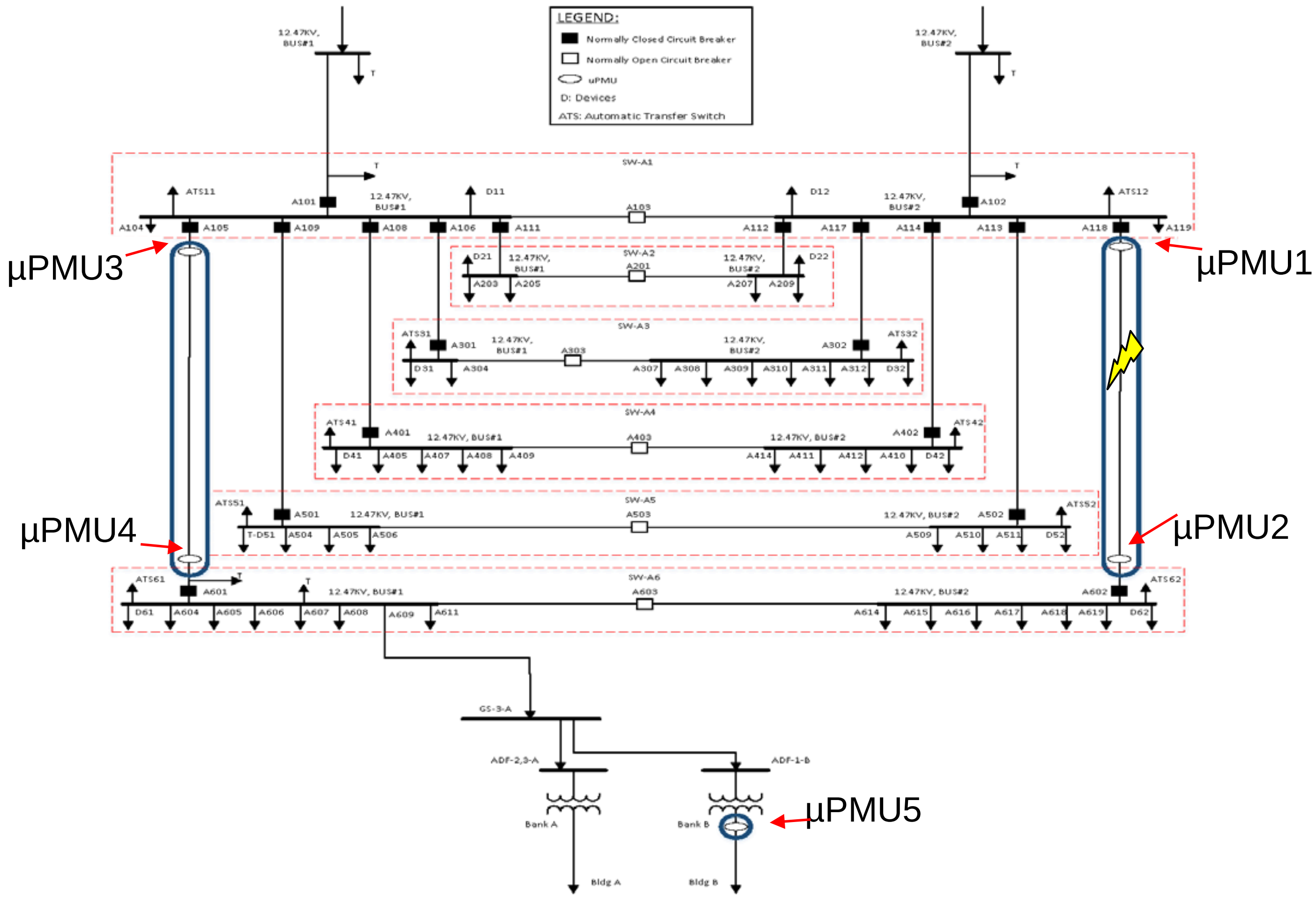
- Case1.



Examples of Stage2 and Central IDS

1. Fault occurs

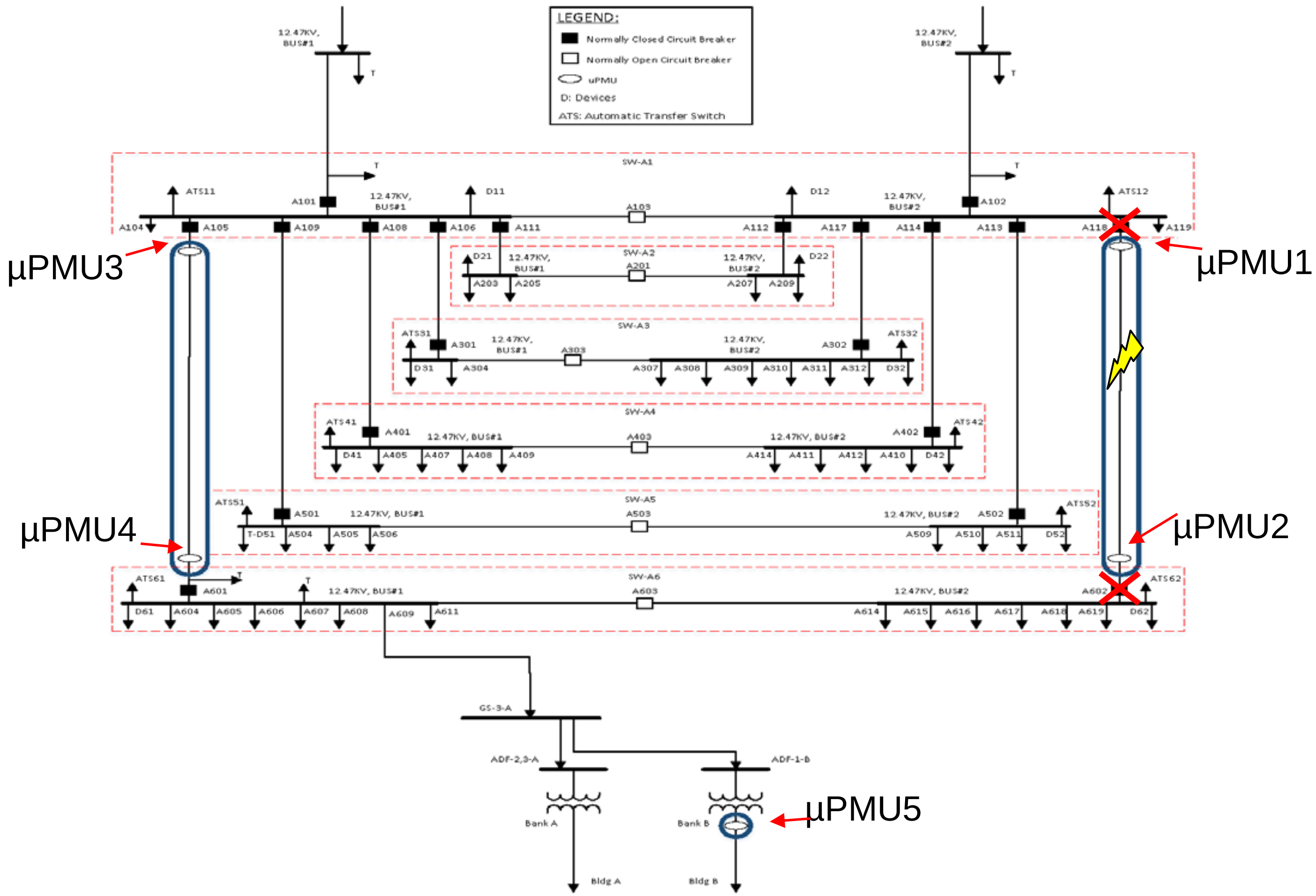
- Case1.



Examples of Stage2 and Central IDS

- Case1.

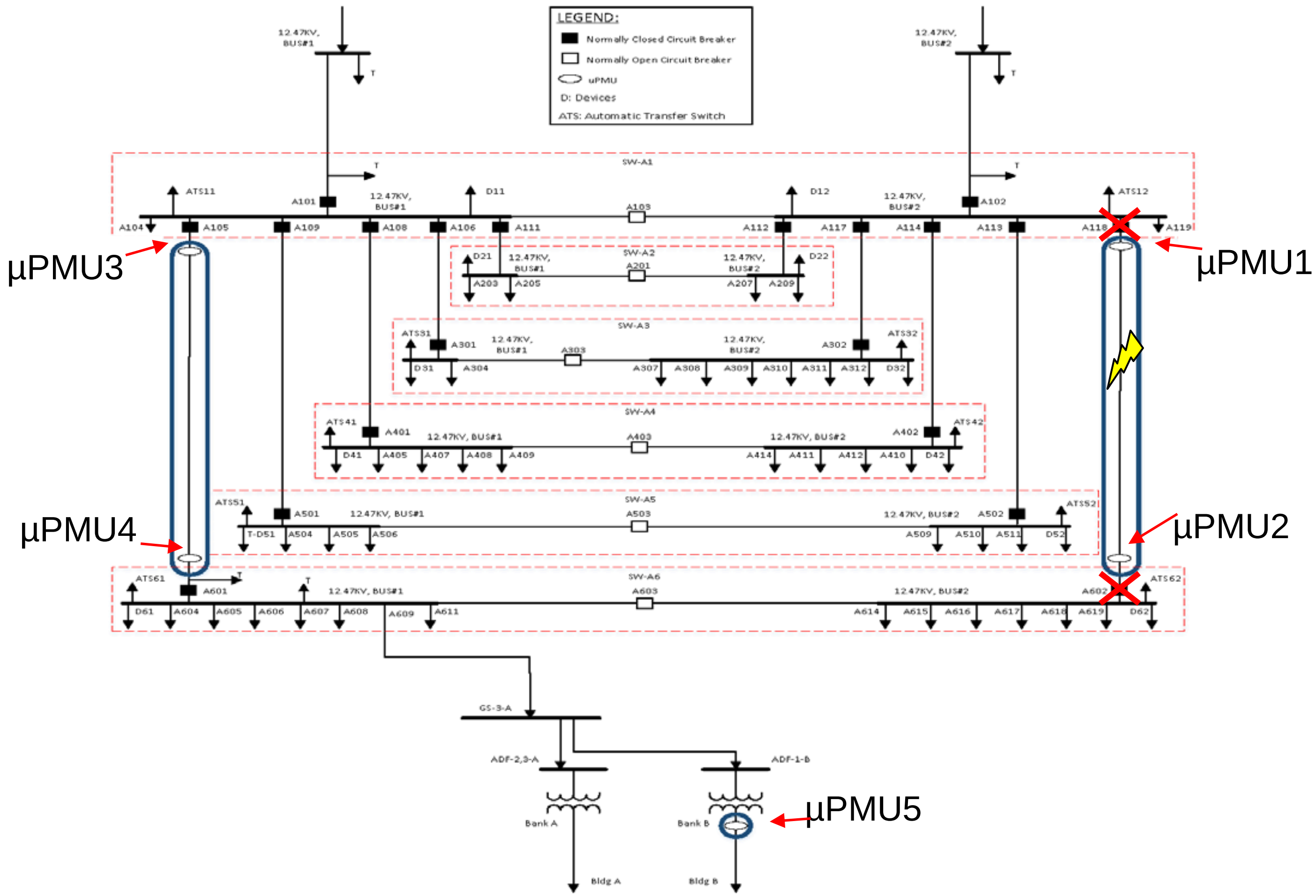
2. Attacker does not allow CB A113 and A502 to open by sending fake data to RTU



Examples of Stage2 and Central IDS

- Case1.

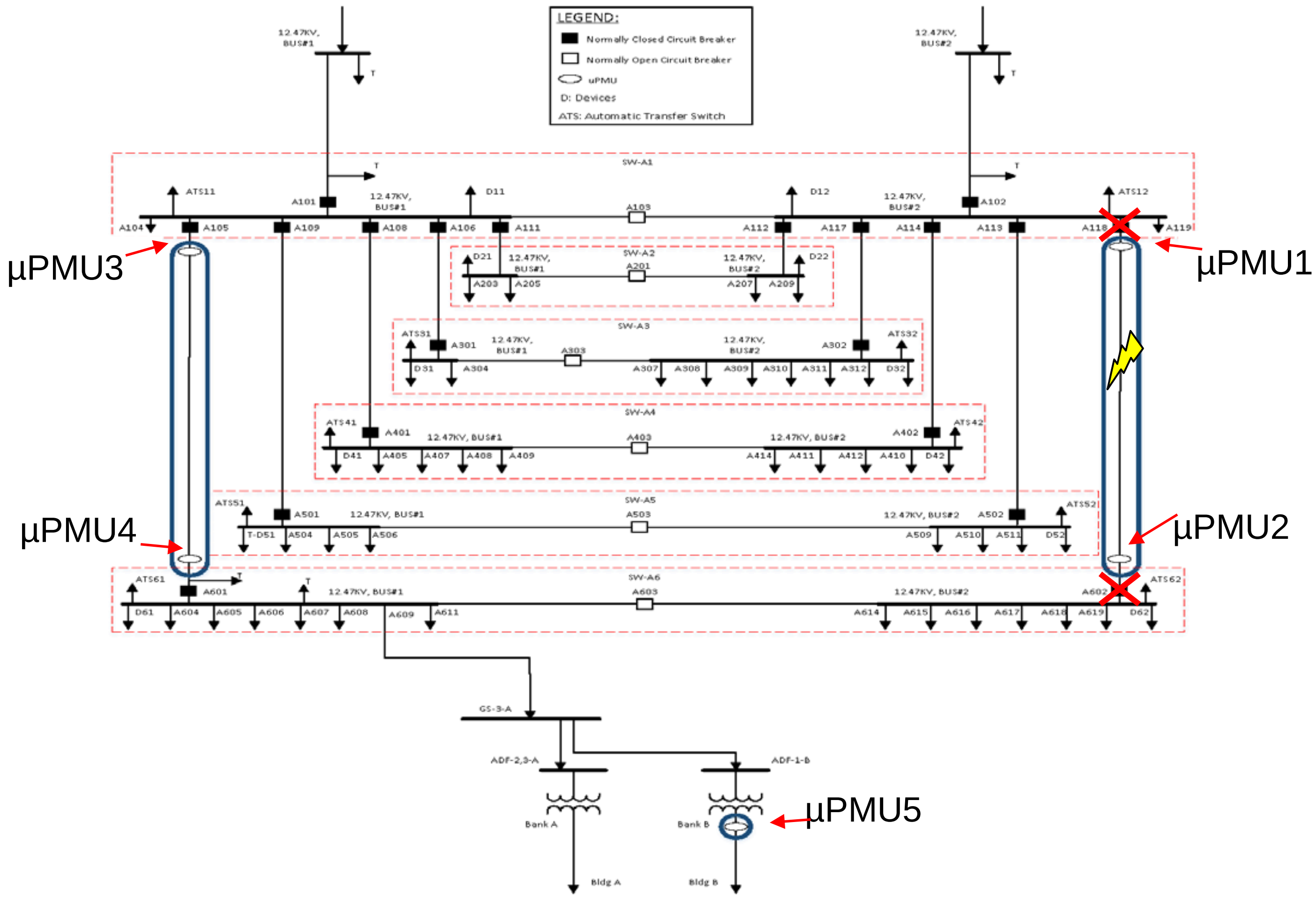
3. Voltage sag seen by µpmus is longer than the maximum allowed time



Examples of Stage2 and Central IDS

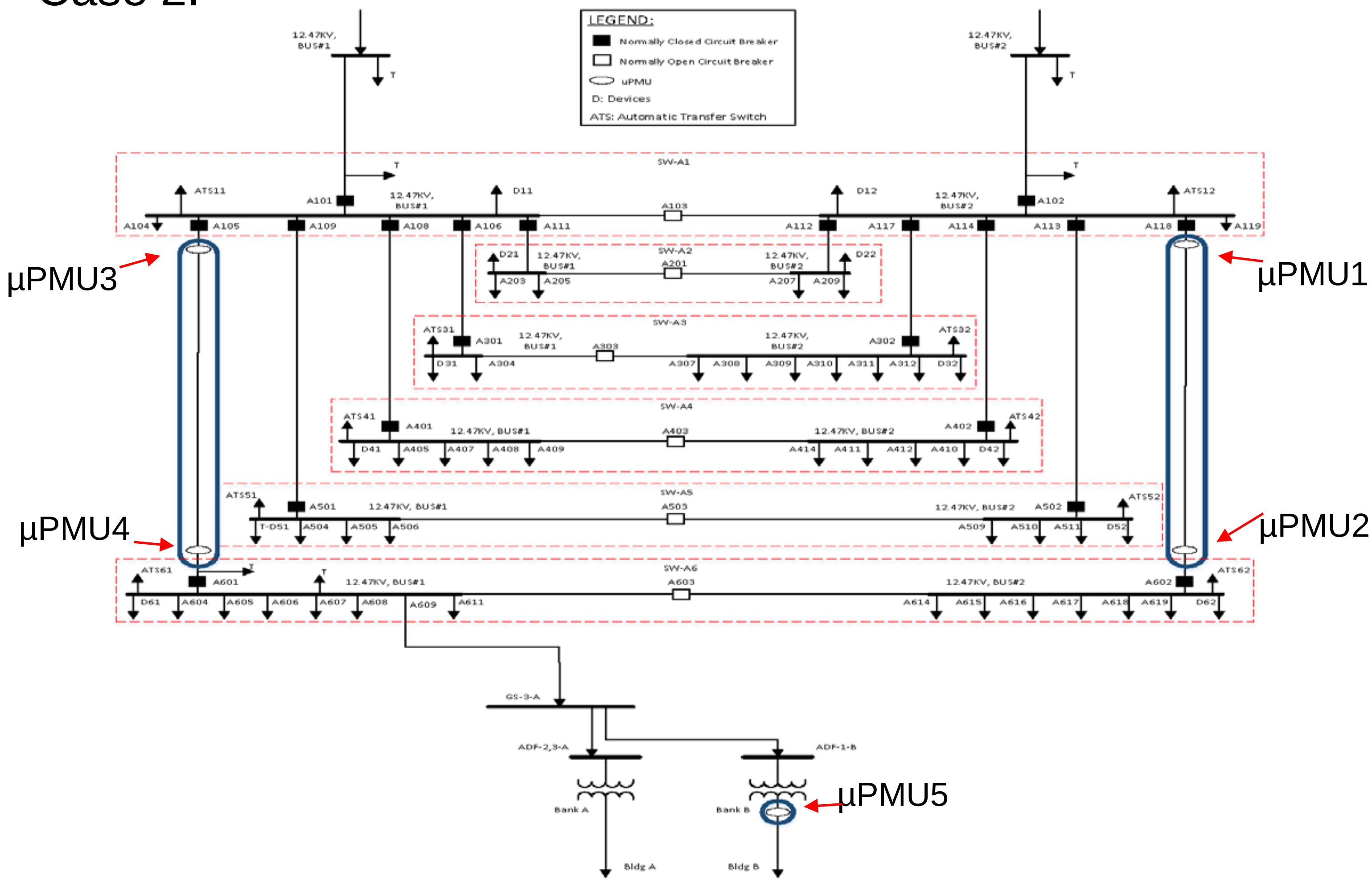
- Case1.

Anomaly Signature Found



Examples of Stage2 and Central IDS

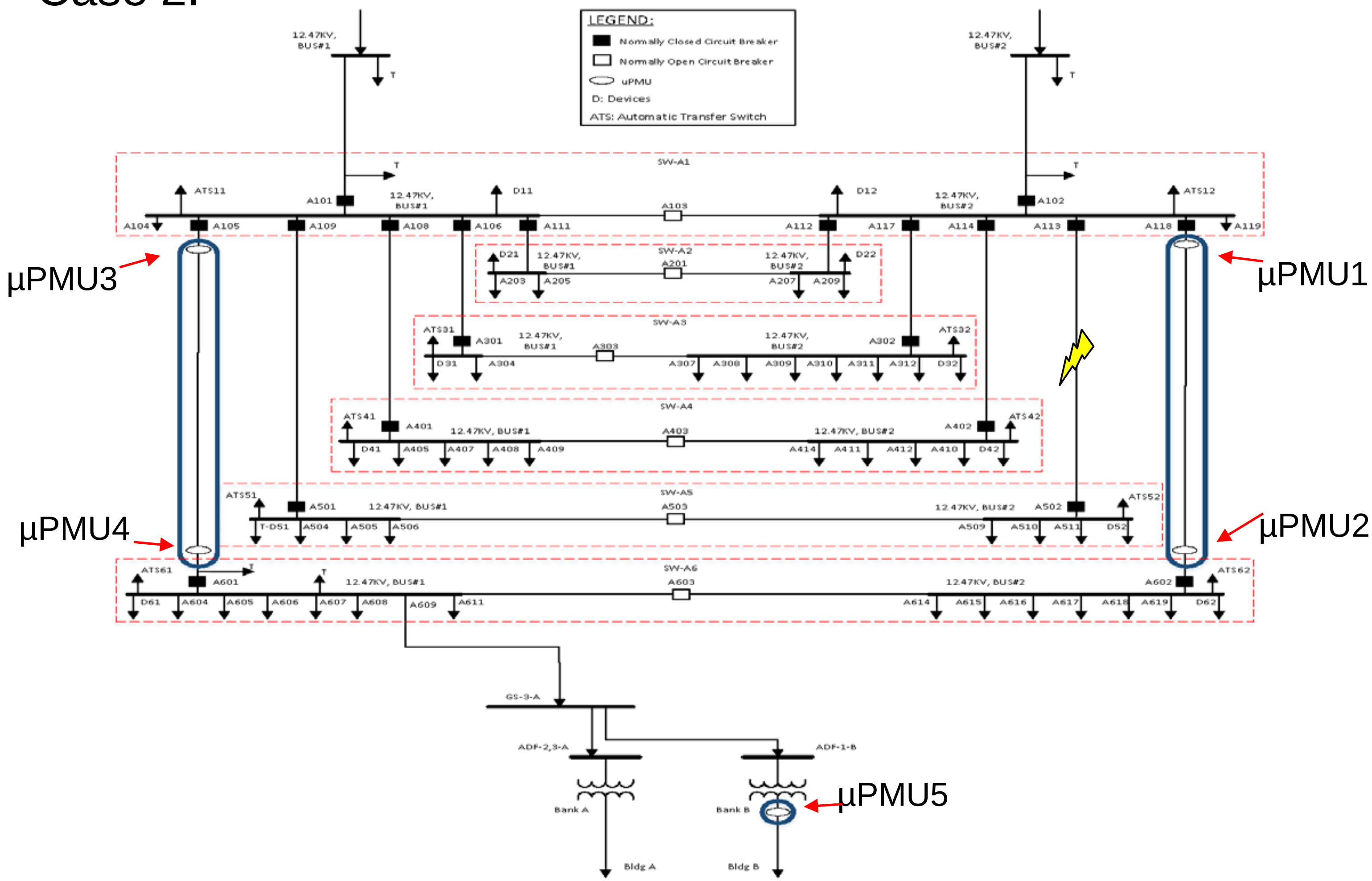
- Case 2.



Examples of Stage2 and Central IDS

1. Fault occurs

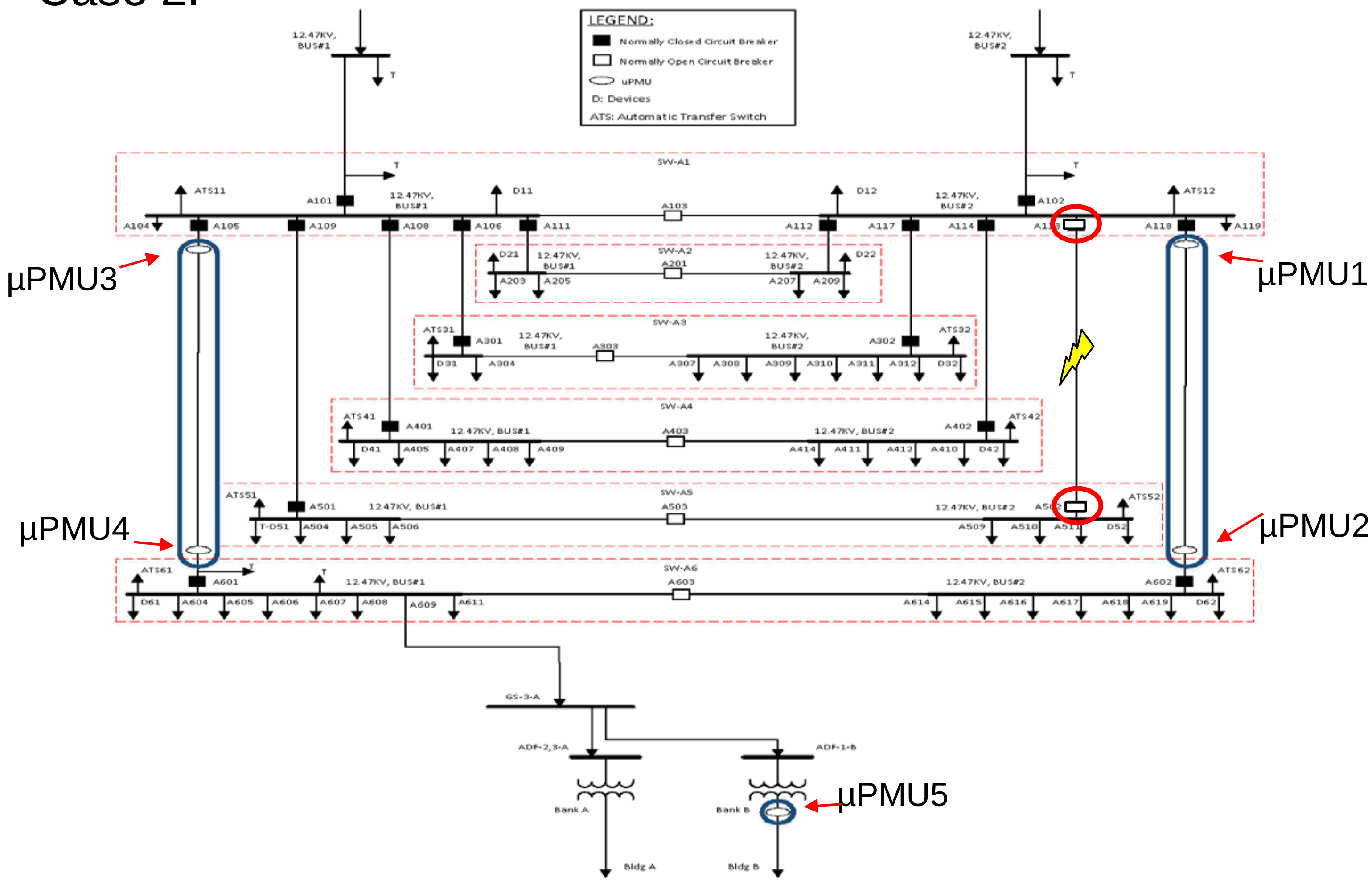
- Case 2.



Examples of Stage2 and Central IDS

2. CB A113 and A502 open

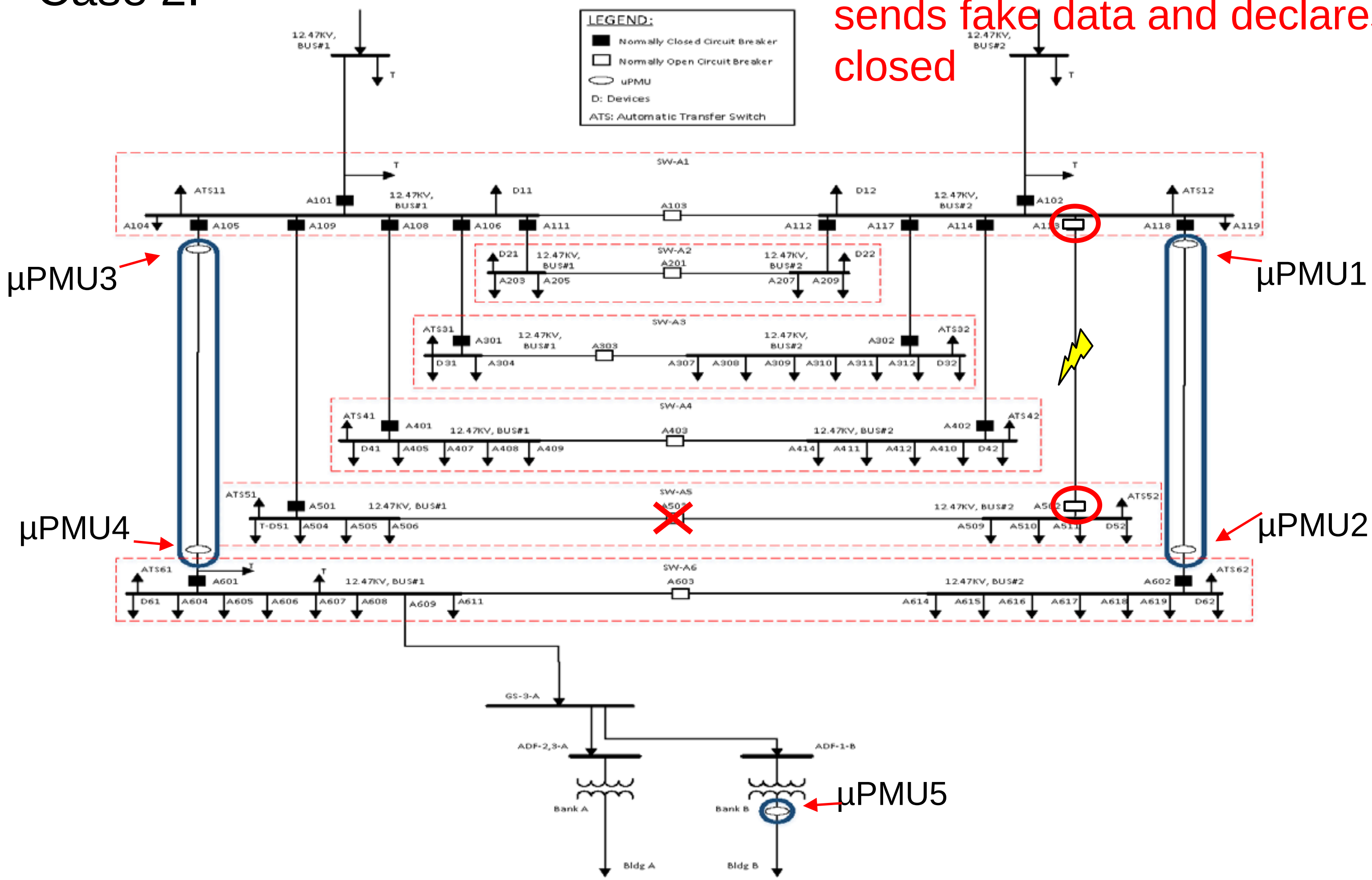
- Case 2.



Examples of Stage2 and Central IDS

3. Attacker prevents A 503 to close that is supposed to feed healthy part but sends fake data and declares that it is closed

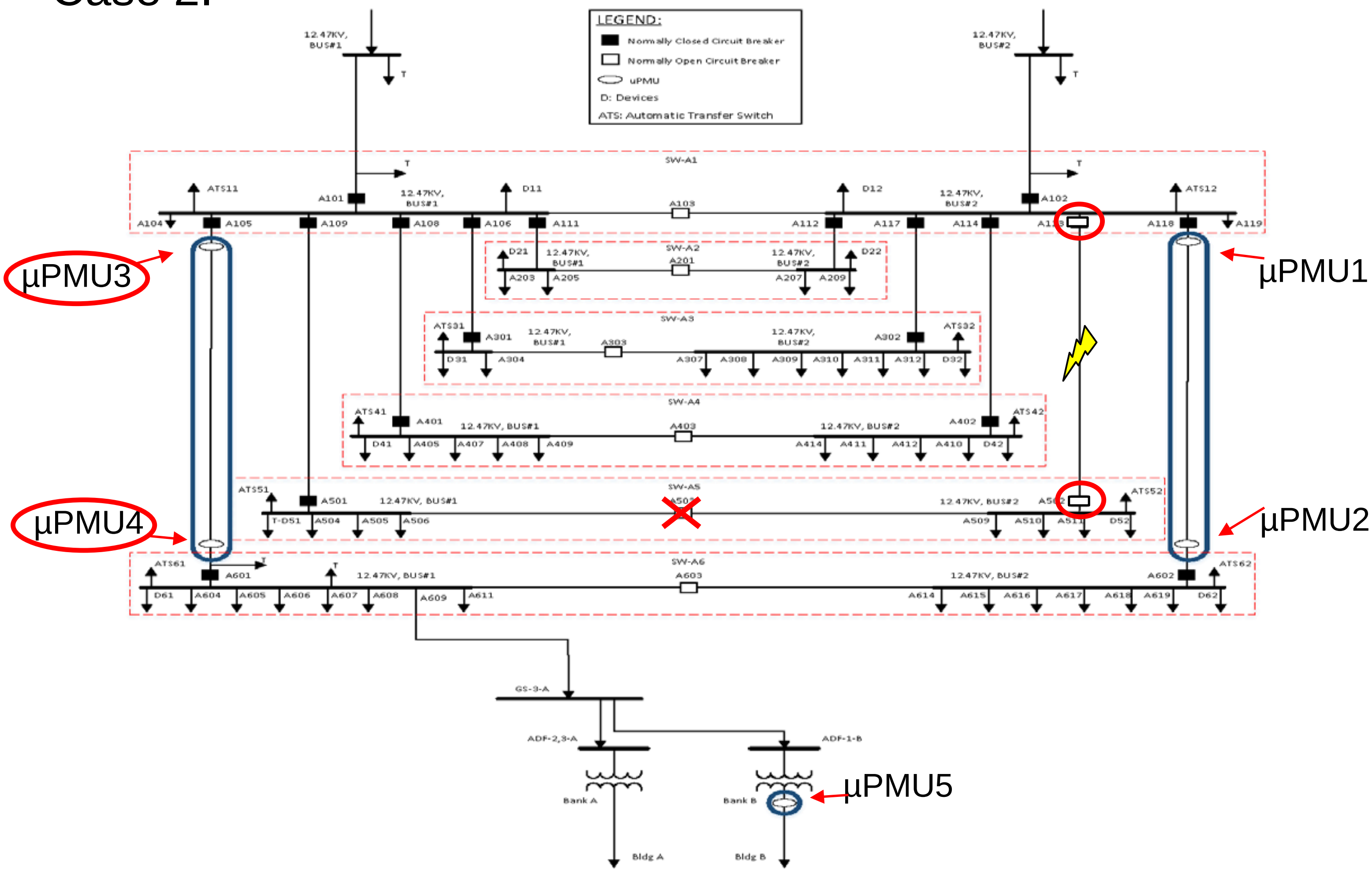
- Case 2.



Examples of Stage2 and Central IDS

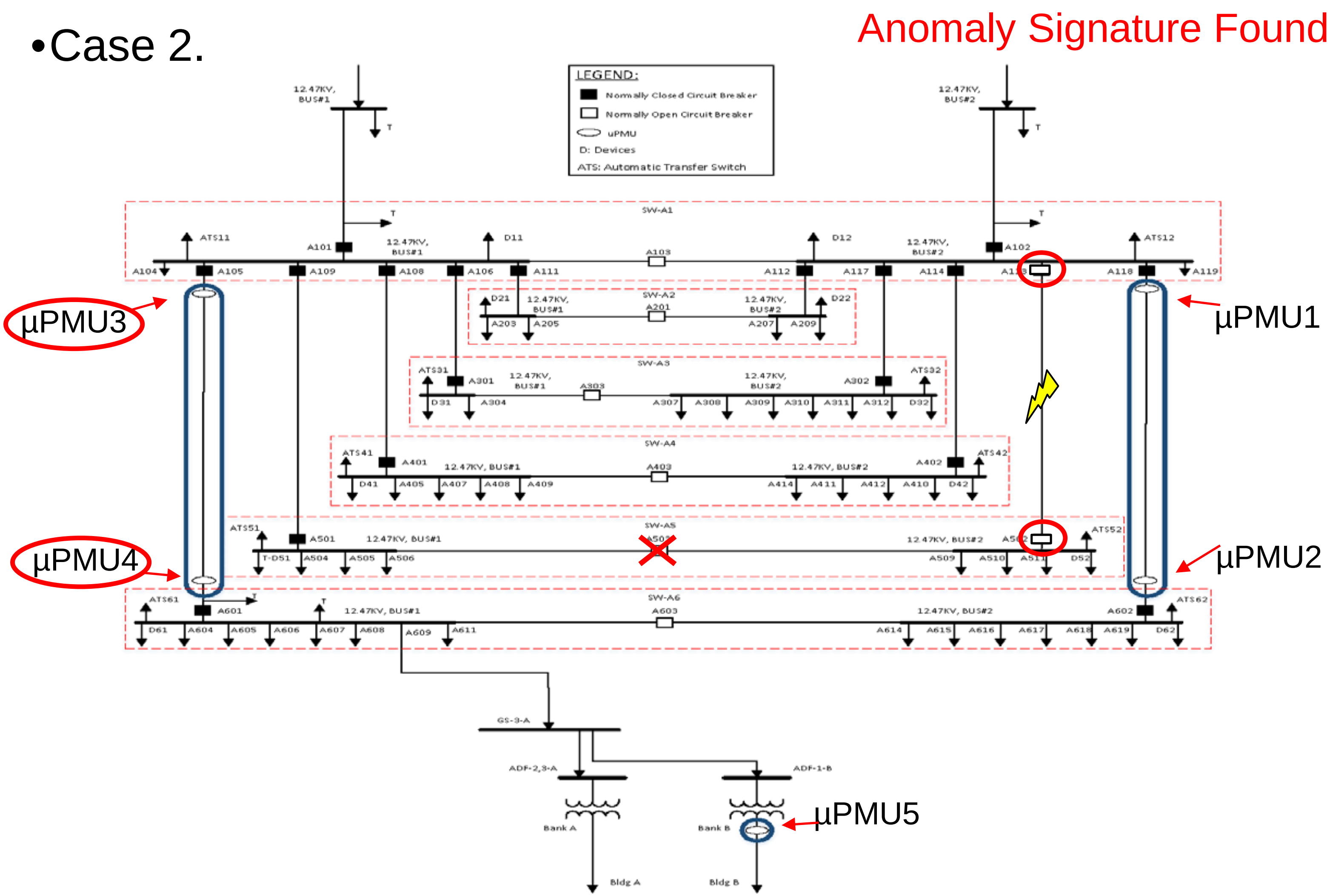
- Case 2.

4. µPMU3 and µPMU4 cannot see any expected switching sag



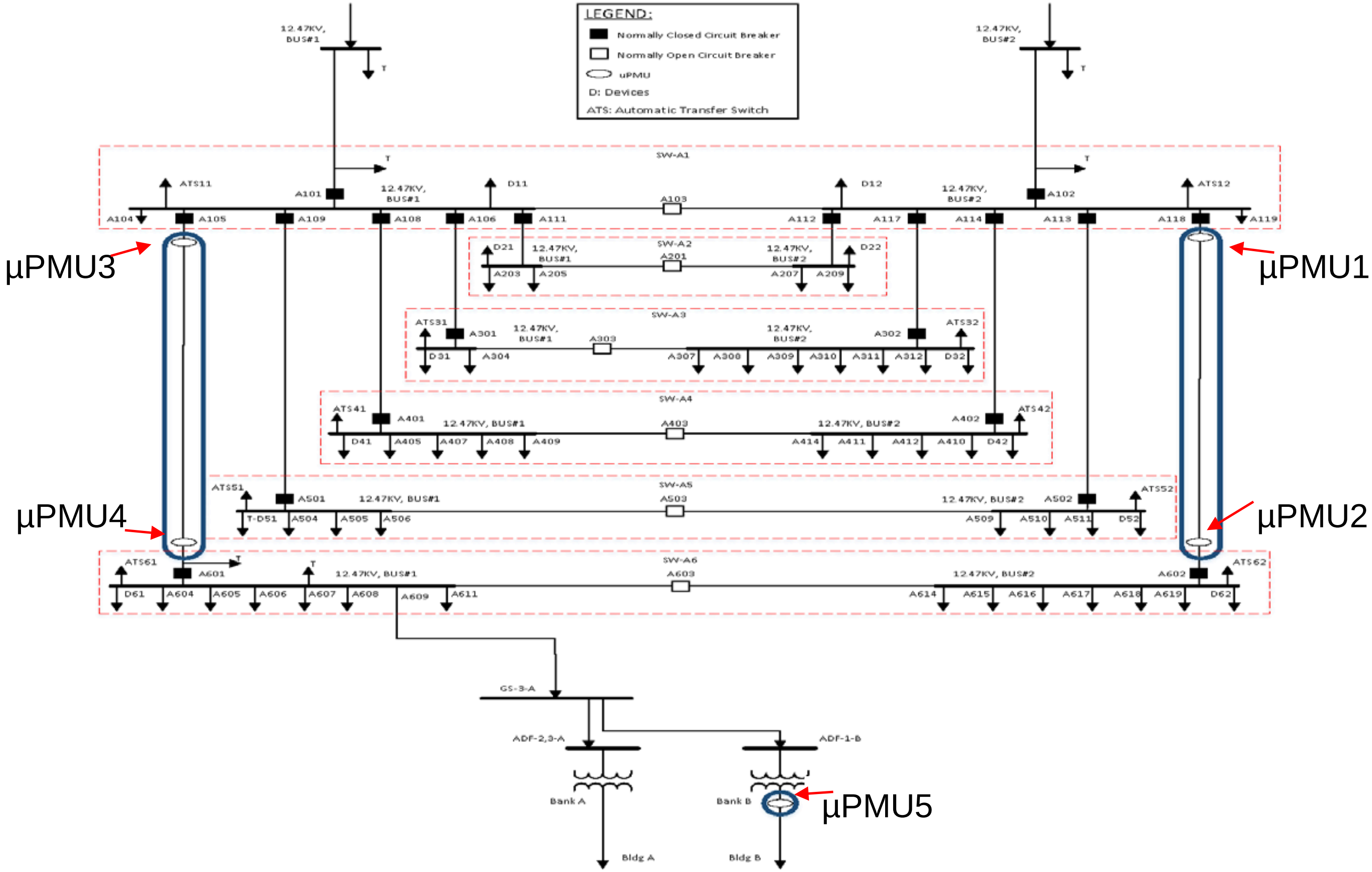
Examples of Stage2 and Central IDS

• Case 2.



Examples of Stage2 and Central IDS

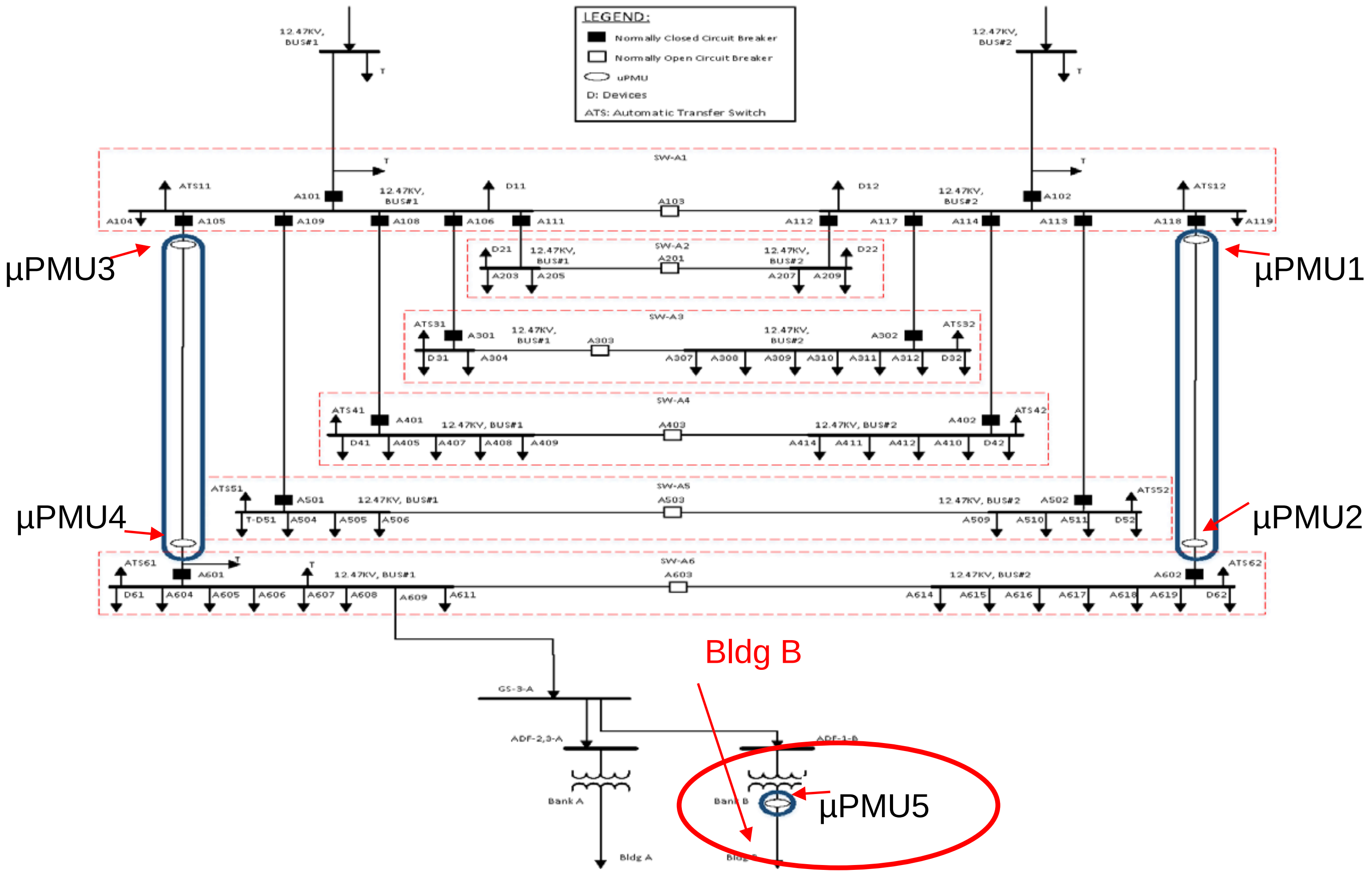
- Case 3.



Examples of Stage2 and Central IDS

- Case 3.

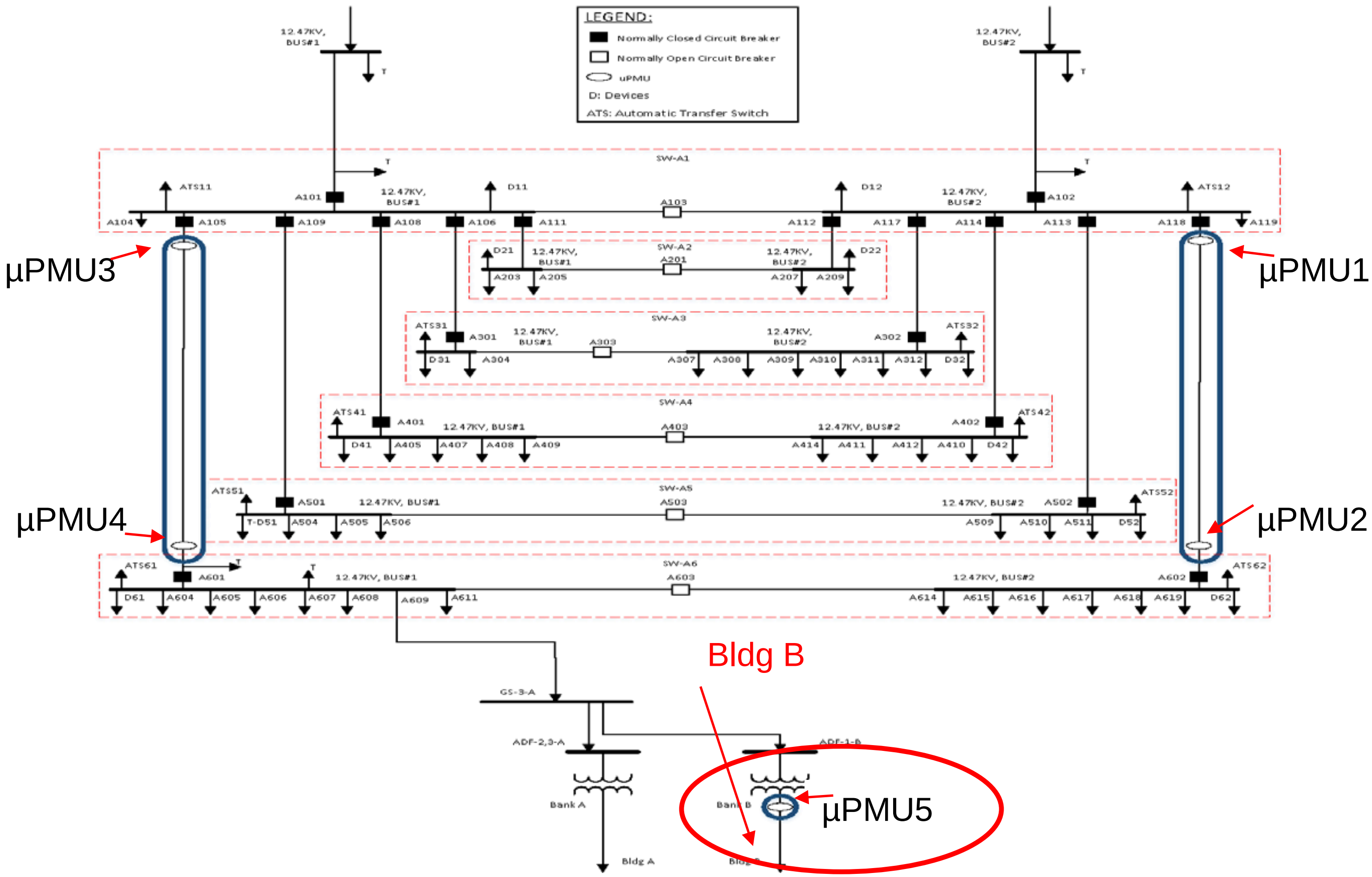
1. Voltage sag occurs and spreads to the sensitive loads at Bldg B



Examples of Stage2 and Central IDS

- Case 3.

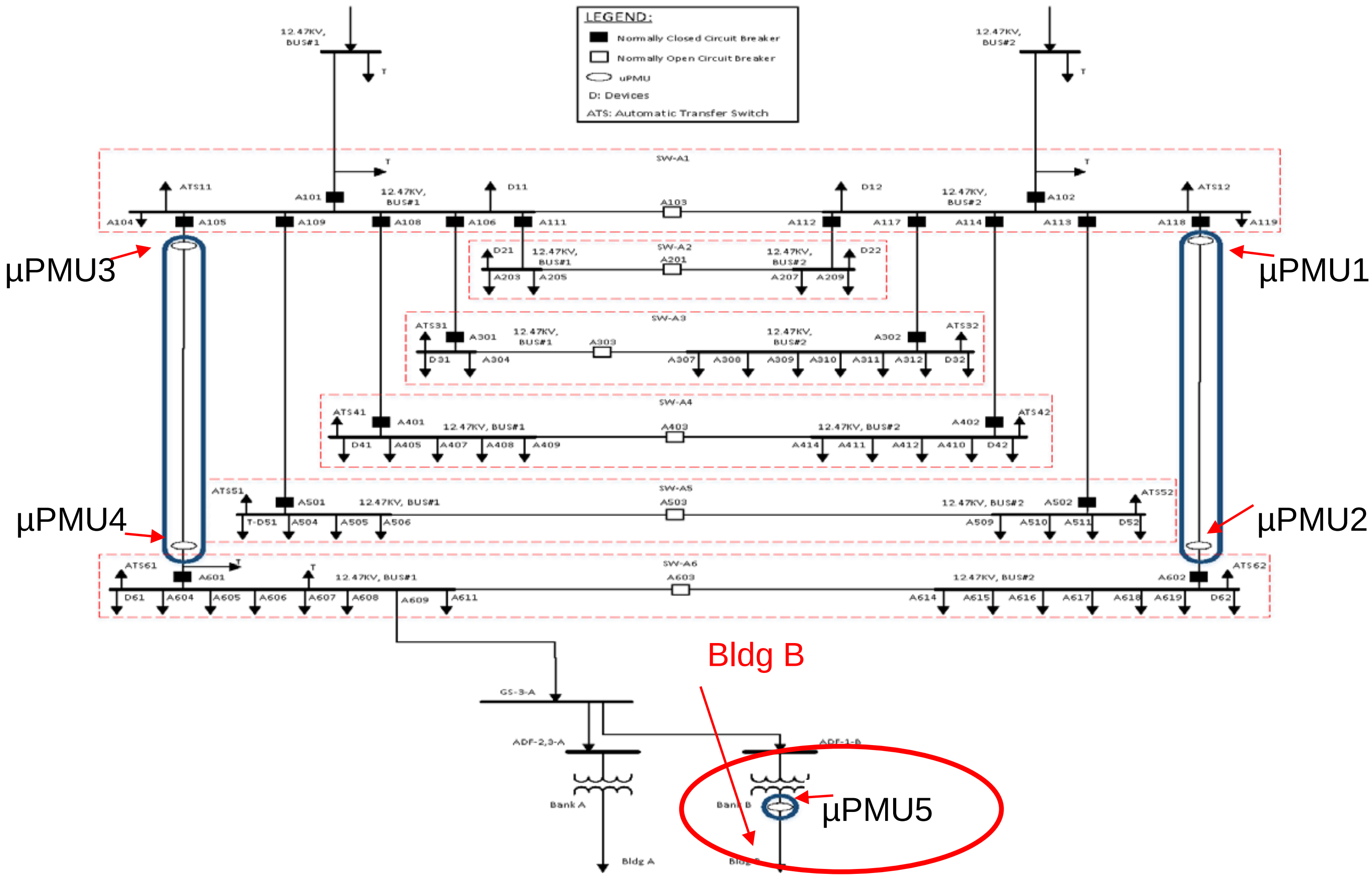
2. Attacker does not allow sensitive loads to trip but it sends fake status that they are tripped



Examples of Stage2 and Central IDS

3. µPMU5 and µPMU6 cannot see any load change due to trip

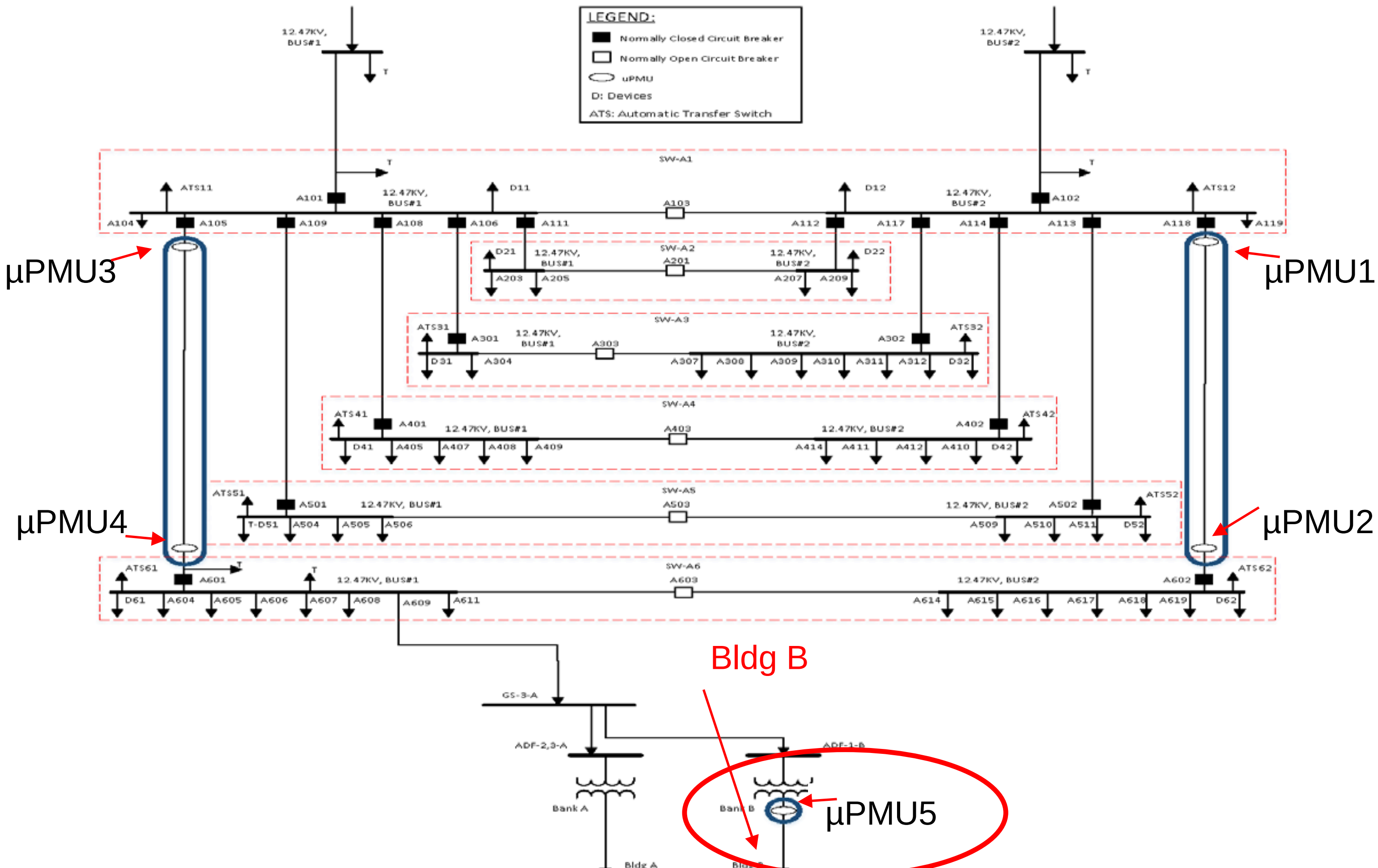
- Case 3.



Examples of Stage2 and Central IDS

Anomaly Signature Found

- Case 3.



Conclusions

We introduced a µPMU-based IDS framework:

✓It is highly robust due to being highly distributed, both in physical and communication terms.

✓It can be used both to verify existing cyber-security systems on the grid and to detect potential cyber-attacks.

✓It can be inexpensively and rapidly deployed at existing utility facilities.

✓It is scalable due to hierarchical defined policies, where the topology dependency decreases as we move downward in the tree.

✓It is fully automated process, and can relieve the pain of operators to analyze enormous amount of data.

Gaps and Future Efforts

1. Optimal μPMU placement in the distribution grid with IDS minimum false positive and negative objective .
2. Enriching the satge-2 and central rules for better utilization of the resources.
3. Efforts on decentralizing the central algorithms to distribute the computation requirements over the grid.
4. Testing and validating the efficacy of the rules for different cases and events through simulation.
5. Exporting a prototype architecture using BRO framework, as the initial effort for migration to the industry level.

References

1. Parvania, Masood, et al. "Hybrid Control Network Intrusion Detection Systems for Automated Power Distribution Systems." *Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on*. IEEE, 2014.
2. Koutsandria, Georgia, et al. "A hybrid network IDS for protective digital relays in the power transmission grid." *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*. IEEE, 2014.
3. Koutsandria, Georgia, et al. "A Real-Time Testbed Environment for Cyber-Physical Security on the Power Grid." *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*. ACM, 2015.
4. McParland, Chuck, Sean Peisert, and Anna Scaglione. "Monitoring Security of Networked Control Systems: It's the Physics." *Security & Privacy, IEEE* 12.6 (2014): 32-39.
5. Basseville, Michèle, and Igor V. Nikiforov. *Detection of abrupt changes: theory and application*. Vol. 104. Englewood Cliffs: Prentice Hall, 1993.

Thank you!