CREDC

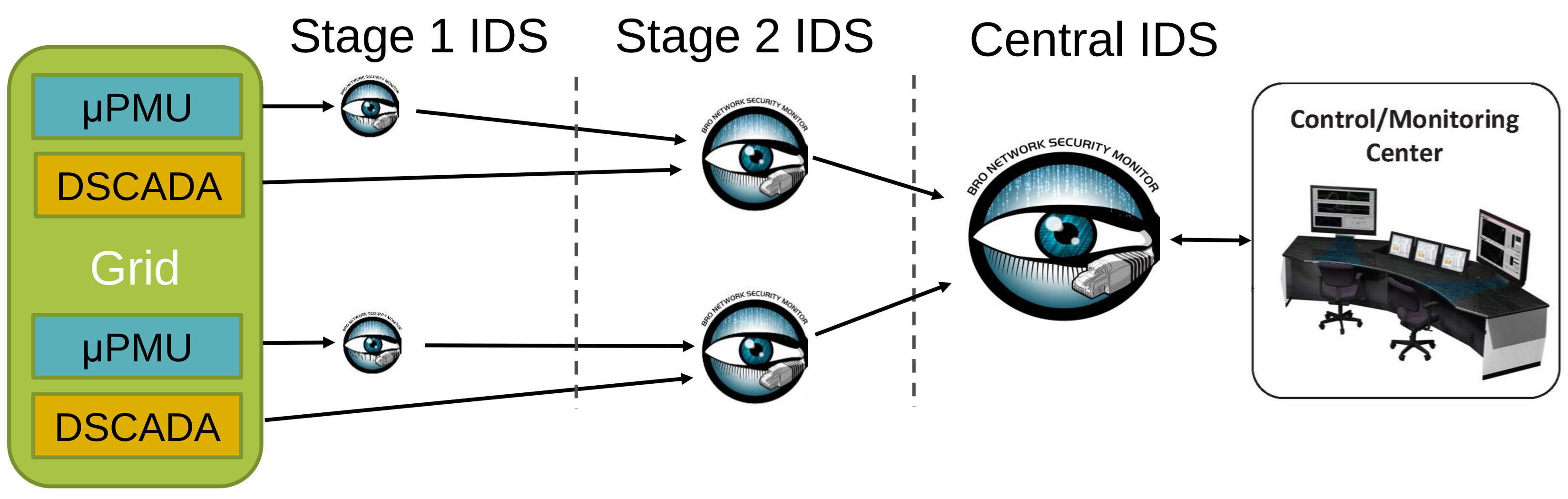
Supporting Security with Advanced Multimodal Grid Data Analytics

Micro Synchrophasor-Based Intrusion Detection in Automated Distribution Systems

M. Jamei, A. Scaglione, E. Stewart, S. Peisert, C. McParland, C. Roberts, and A. McEachern

GOALS

- Combine high-resolution µPMU data & sniffed DSCADA for intrusion detection.

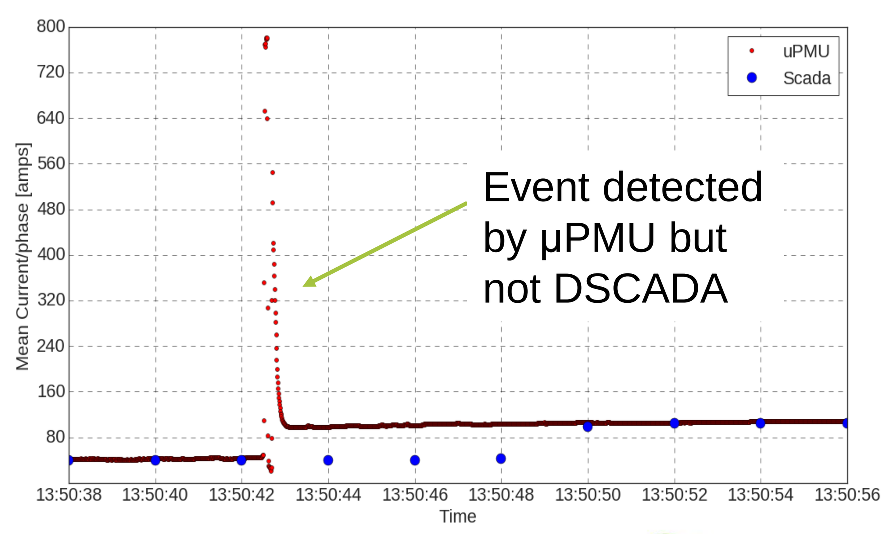


CURRENT SECURITY CHALLENGES

- Firewalls, authentication, cryptographic algorithms, intrusion detection systems (IDS)… are insufficient.
- Solutions are divorced from the knowledge of the physics of the system, safe operations and limits, and its current physical operating point.
- Extended IDS notion in previous work that checks the compliance of sniffed SCADA data with cyber-physical rules can be blind to some sophisticated attacks.

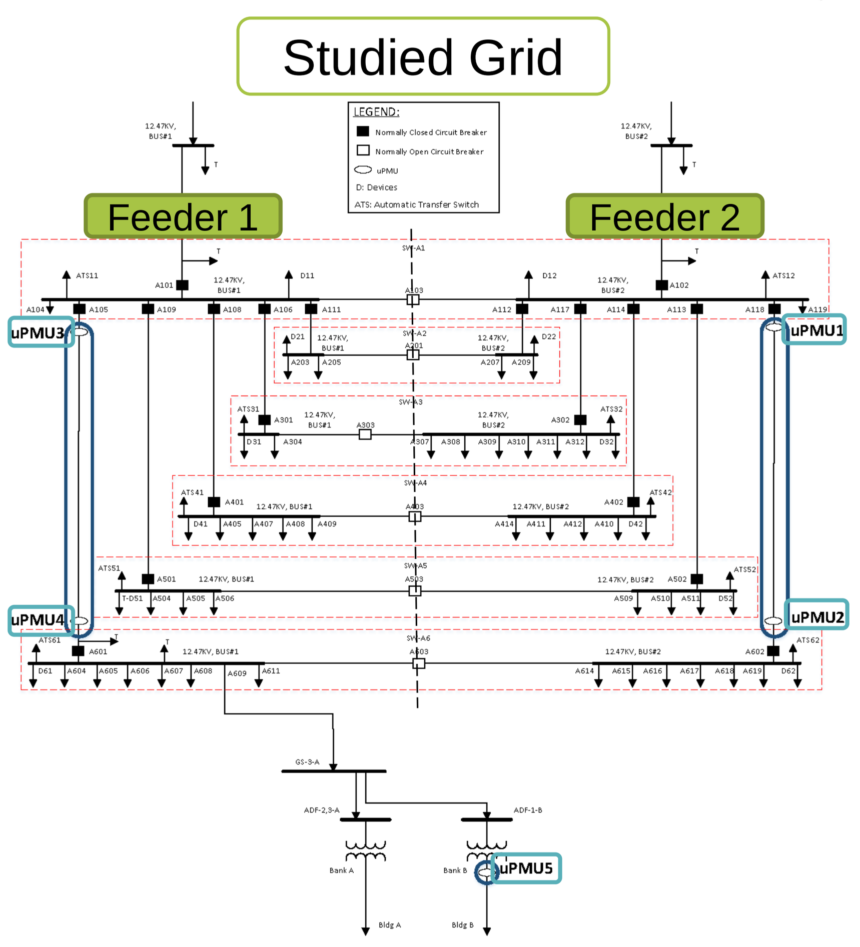
MICRO-PMU DATA (A GAME CHANGER)

- Situational awareness through µPMU devices.
- Significantly more information vs. event-triggered DSCADA data.



- Many cyber-attacks leave footprints in the µPMU data.
- Detected µPMU anomalies + knowledge of grid operation → security status hypotheses testing.

Real-Data Analysis:



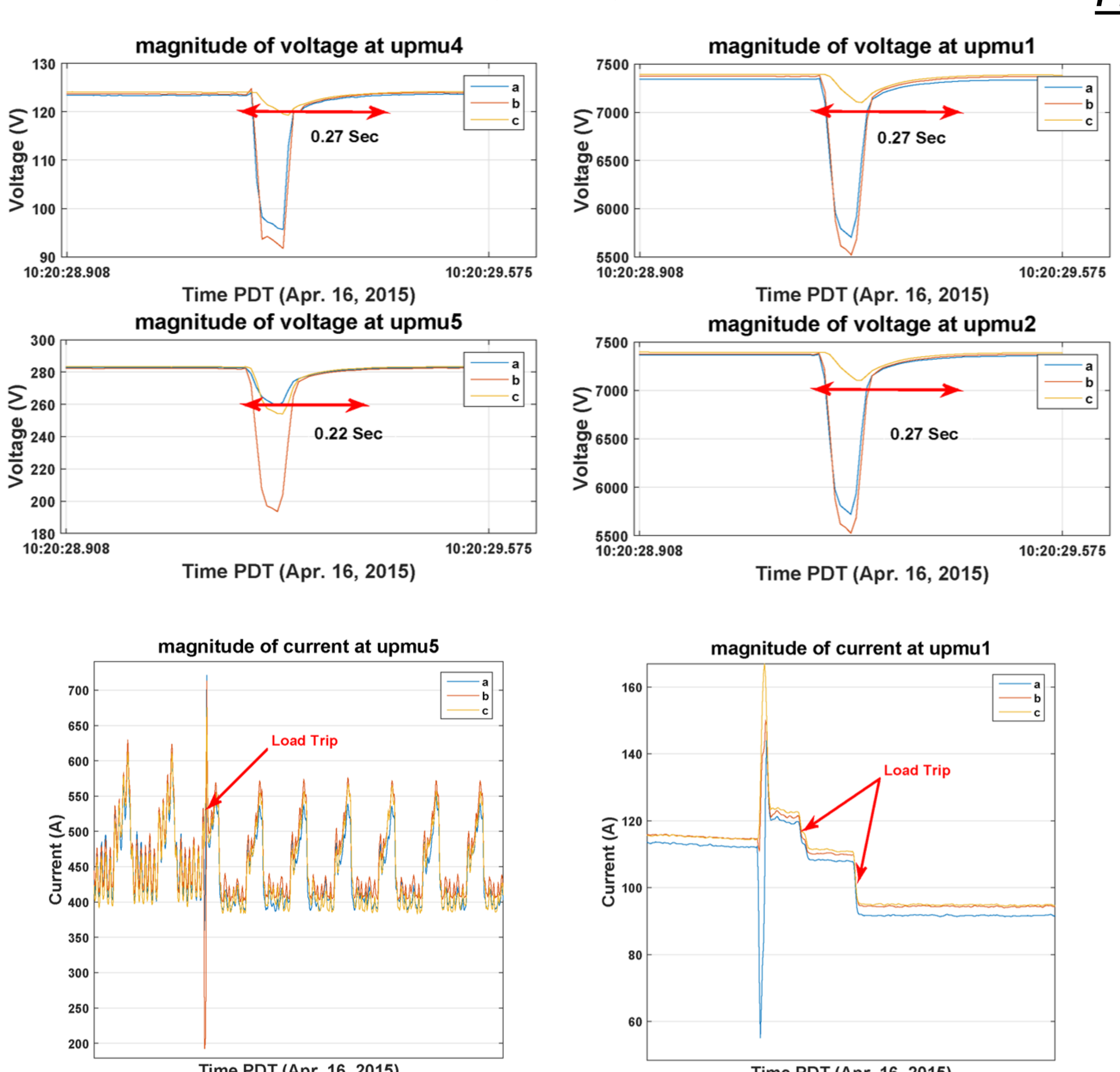
Example:

❖ Voltage sags detected.

What caused the event?

Key Observations:

1. Both Feeders are impacted.
2. Severity is the same at all µPMUs.
3. Duration and start time are almost the same at all µPMUs.



Hypotheses Formulation:

1. Fault at one of the two feeders and spreading to the other one through the closed Normally Open (N.O.) breakers?
2. Fault at one of the two feeders and spreading to the other one through substation?
3. Remote transmission-level fault?

Hypotheses Testing:

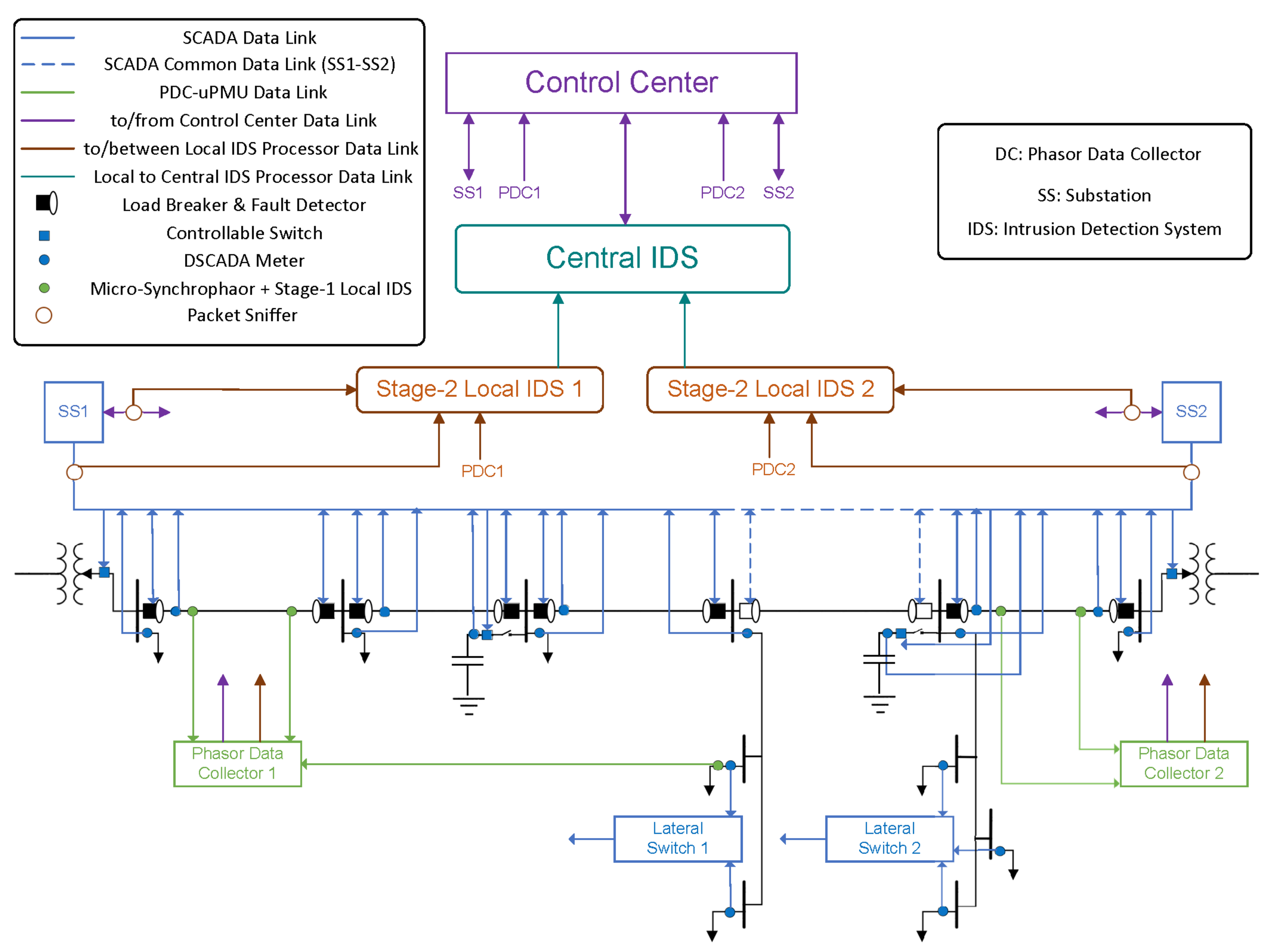
- *Hypothesis 1* ✗: N.O. breakers are activated either after fault clearance for energy restoration, or before fault clearance by attacker. Consequently, sag either does not transfer, or transfers with delay.
- *Hypothesis 2* ✗: Only plausible if the transmission grid is not stiff with respect to transients compared to the distribution feeders.
- *Hypothesis 3* ✓: *voltage sags seen* concurrently with the same severity in both feeders.

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).

ALL-EMBRACING IDS FRAMEWORK

- We envision the following framework:

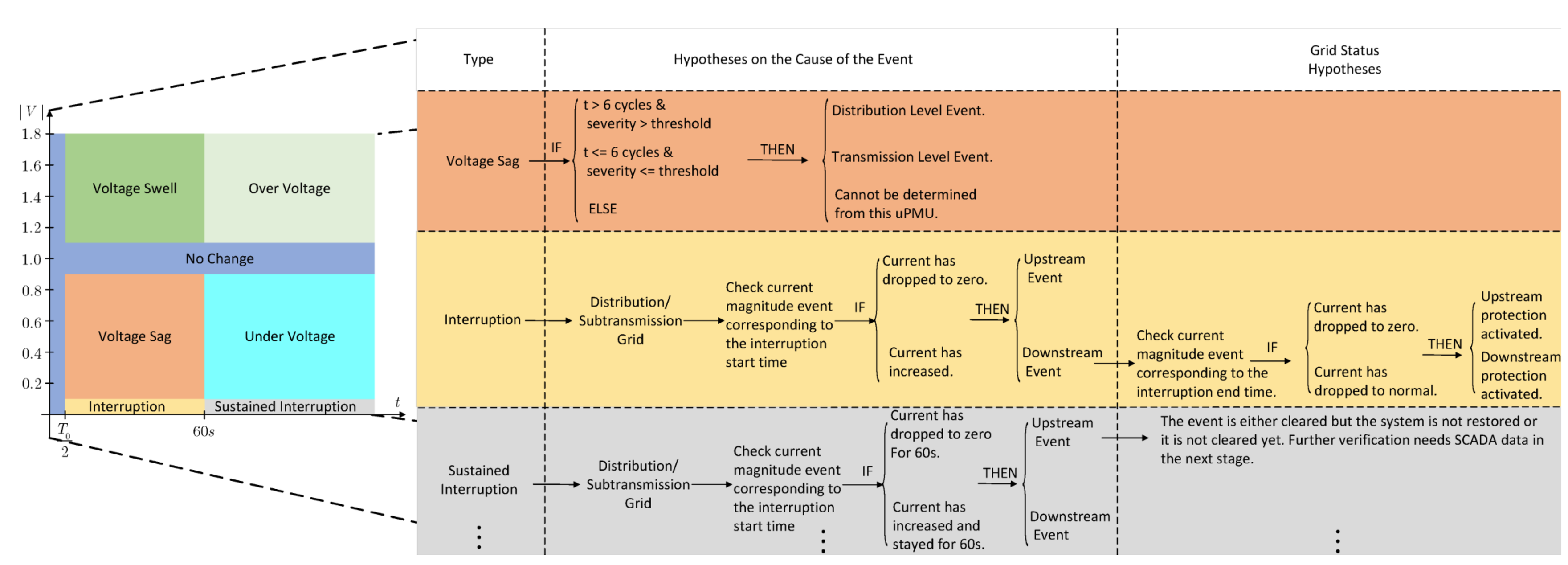


What happens at Stage 1 next to µPMU:

✓ Detect anomalies in the voltage phasor magnitude (static rules), and in current phasor magnitude and active and reactive power (dynamic rules).

✓ Formulate and test some hypotheses regarding the cause of detected anomalies.

✓ Pre-processing data for stage-2 local IDS.



What happens at Stage 2 (fuse a few µPMUs and DSCADA)?:

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

✓ Formulate & test additional hypotheses with local grid picture.

What happens at central IDS (fuse all µPMUs and DSCADA)?:

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

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

FUTURE EFFORTS

- Enriching stages and central rules to form a robust structure.
- Prioritize important vulnerabilities and simulate attack scenarios to validate the efficacy of the proposed architecture and rules.
- Real-world test and integration under BRO framework.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY