# Micro Synchrophasor-Based Intrusion Detection in Automated Distribution Systems: Towards Critical Infrastructure Security

Mahdi Jamei, Emma Stewart, Sean Peisert, Anna Scaglione
Chuck McParland, Ciaran Roberts, Alex McEachern

**Abstract**

Electric power distribution systems are undergoing many technological changes and concerns are surfacing on possible additional vulnerabilities. Resilient cyber-physical systems (CPSs) in general must leverage state measures and operational models that interlink the physical and the cyber assets that compose them, to assess the global state. In this paper we describe a viable process of abstraction to obtain this holistic system state exploration tool, through the analysis of data from Micro Phasor Measurement Units ($\mu$PMUs) combined with the monitoring of Distribution Supervisory Control and Data Acquisition (DSCADA) traffic, and using semantics to interpret these data that expresses the specific system physical and operational constraints in both cyber and physical realms.

**Index Terms**

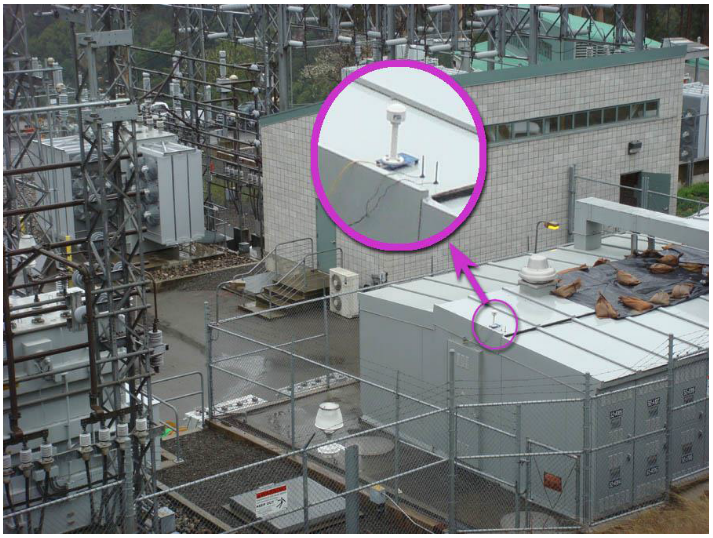
**Cyber Security, Distribution Grid, Intrusion Detection, Micro Phasor Measurement Unit ($\mu$PMU), Distribution Supervisory Control and Data Acquisition (DSCADA)**

## I. Introduction

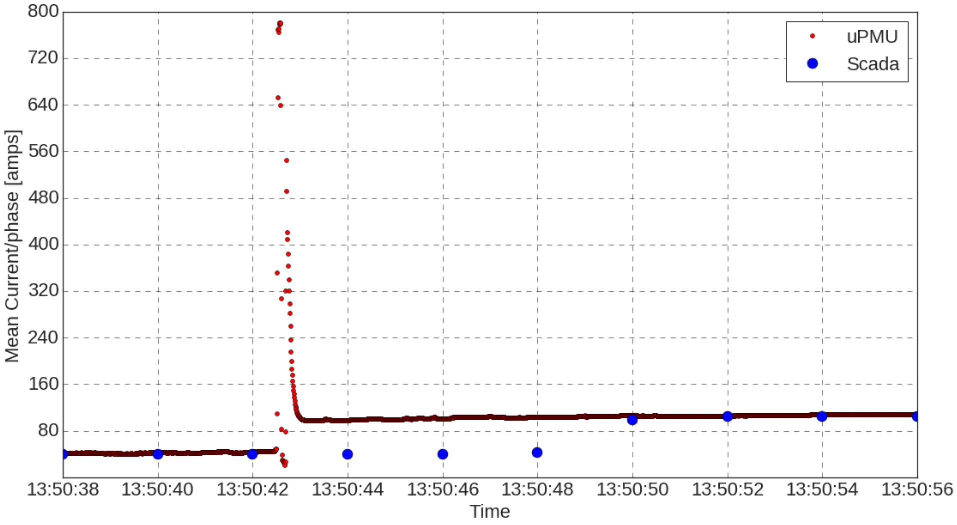
According to the U.S. Department of Homeland Security (DHS) reports, the sophistication and frequency of the attacks on the power grid are increasing [1]. For example, a recent report on the Ukraine attack [2] showed how a failure in the communication network security resulted in significant power outages. The Stuxnet malware or the sewage spill incident at the Maroochy Water Station, due to the wireless attack, are other examples showcasing how a misinformed control system can lead to catastrophic consequences.

Cyber security for energy delivery systems has, until now, focused primarily on the transmission grid and on securely transferring bits of information about the condition of power-grid elements (e.g., “Is this switch open or closed?”, “Which tap is selected on this transformer?”) and preventing unauthorized access to sensor and control packets. Once that access has been gained, there is little remediation action for the power grid, other than a communications blackout and manual fieldwork. The industry is seeking new approaches to this problem, also focusing on understanding security at the distribution level, in anticipation to a growth in automation.

While transmission grids states have been tightly monitored and their behavior at the physical level is reasonably well understood, the operators have been largely blind towards the real time condition of the distribution grid. Hence, in tandem with the effort of gaining situational awareness on the security of the system there is a growing need and interest in the deployment of sensors, like the Micro Phasor Measurement Units ($\mu$PMUs) that can capture the state at the distribution level [3]. These devices, recently developed by PSL [4], address both the technical and economic barriers limiting the deployment of conventional PMUs, which are aimed at the transmission grid, for the distribution level [5]. Fig. 1a shows a sample $\mu$PMU device installed in the partner utility grid. These devices sample at a rate of 120 samples/sec the three phase voltage and current phasors. In comparison to Distribution Supervisory Control and Data Acquisition (DSCADA) that samples power flow and power injections every 3-5 minutes, $\mu$PMU provides significantly more information, and often nuances which are missed in DSCADA data, as illustrated in the example in Fig. 1b. In this example, the magnitude of the current measured by the



(a)



(b)

Fig. 1: (a) $\mu$PMU Instrument from Power Sensors Ltd, (b) Measurement Comparison of $\mu$PMU and DSCADA

DSCADA meter is missing an overcurrent event that $\mu$PMU could capture. This information may prove critical in identifying cyber-attacks (see example in Section IV).

The goal of this paper is to describe a first comprehensive team effort in developing a security architecture leveraging $\mu$PMUs to directly measure at many points, in real time, the actual physical state of the distribution network. Our architecture interprets data in both cyber and physical domains and provides an independent, integrated picture of the distribution grid's state.

The significant advantages of this new approach are: (1) it is robust due to its distributed nature; (2) it can be used both to verify existing cyber-security systems and to detect potential cyber-attacks; (3) it can be inexpensively deployed at existing utilities.

### *A. Tightening Security in Advanced Distribution Management Systems*

Modernized distribution grids will rely heavily on an ensemble of remote and automatic control hardware and software typically referred to as Advanced Distribution Management Systems (ADMS). An underpinning of the activity described in this paper is to design a security framework in anticipation of the impending move towards ADMS. ADMS limits the need for direct human intervention, and when working properly, its functionalities enhance the reliability and safety of the system. While ADMSs are developed with careful consideration for safe physical operation, a number of their features make them uniquely vulnerable to cyber-attacks [6]. In ADMS, a DSCADA network is responsible to collect the information from field devices (e.g. switches, meters ...), and send back the according control commands. The presence of such network opens up a large attack surface. What makes the case even more challenging is that ADMS is an integrated network, so failures in one section could cascade into a large and widespread series of events.

In particular, communication that lacks end-to-end security can permit difficult-to-detect interference between sub-systems that could cause them to function in ways that threaten the safety and reliability of the power grid. Additionally, unlike modern computer systems that are upgraded every three to six years, many of the cyber-physical systems (CPSs), such as electric power system equipped with ADMS are amalgam of decades-old and very new components, operating side by side often with inconsistent operating controls, algorithms and guidelines.

To ensure that ADMS operates and fails in well-understood and controlled ways, one needs to tightly monitor the parts most exposed to an attack. The level of monitoring in CPSs is often a compromise between two competing design mandates: least function (design systems as simple as possible to perform their grid management functions); and robust monitoring (incorporate high-fidelity system status indicators to enable detection of and response to cyber-security events). Our framework leans towards the second predicament through the integration of $\mu$PMUs information in the security architecture, which provides a clear image of the physical trail left by cyber-physical-attacks.

## II. Present Security Remedies

The first steps in adding security in operational environments are typically to deploy firewalls and device-level authentication. Encryption is often also added to enhance confidentiality and integrity of the message content. Another common security mechanism on computer networks is intrusion detection, in which network traffic is monitored and analyzed to detect activities that either fit into a "known bad" category or deviate in a statistically significant way from "normal." The Tofino Security Appliance, the Digital Bond Quickdraw SCADA intrusion detection system, the Radiflow Secure Gateway, the Bro Security Framework [7] are all examples of network intrusion detection systems (IDSs) that can be applied to control systems.

Numerous examples have shown that all of these methods leave significant gaps in security and safety [8]. It has been recognized that one of the reasons for this is that most of these security methods are divorced from the knowledge of the physics of the system, its safe operations and limits, and its current physical operating point. This gap was recognized early on by e.g. [9]. Some of our own previous work for monitoring SCADA traffic expanded the notion of intrusion detection by leveraging the laws of physics governing the grid and imposing them as security constraints [10], [11]. Nonetheless, these methods also remain blind to more sophisticated attacks. One reason is that the data coming from SCADA systems are not updated with high frequency, so events causing many changes in a short period of time can be missed. In addition, attackers can inject false data at the device level, thus evading detection by the IDS.

## III. Micro Synchrophasor Data: A Game Changer?

We believe deploying $\mu$PMUs can significantly increase the detection and classification capabilities of distribution operators. Many of the cyber-attacks aiming to cause changes in the physical layer leave footprints or anomalies in the $\mu$PMU measurements, such as voltage sags and swells, change of power flow direction, and electric current events. Our basic idea is utilizing the $\mu$PMU measurements to correlate the observed state of the system and the set of detected events through $\mu$PMU to form building blocks for the estimation of the grid security status. The knowledge about the system topology and operation

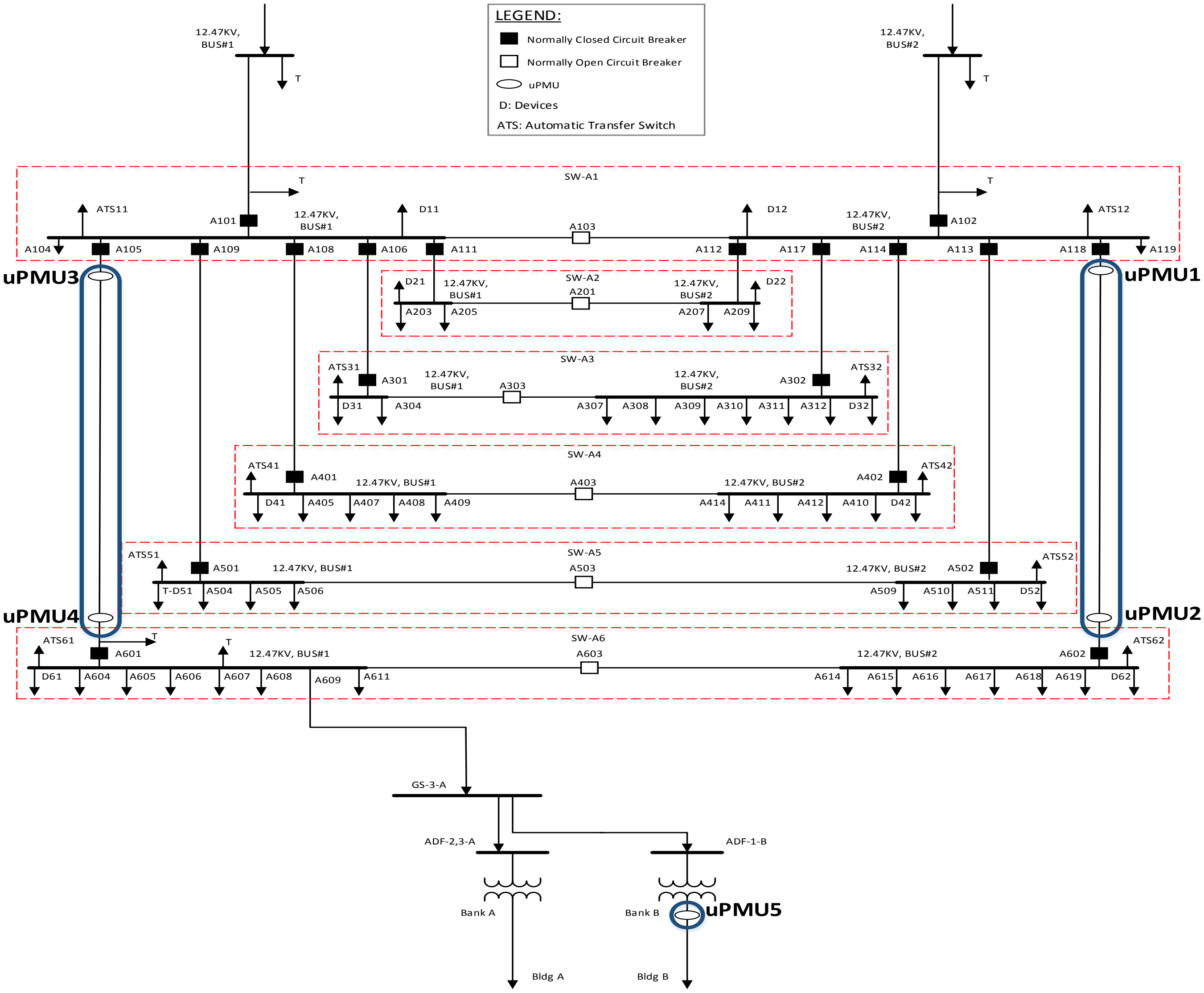
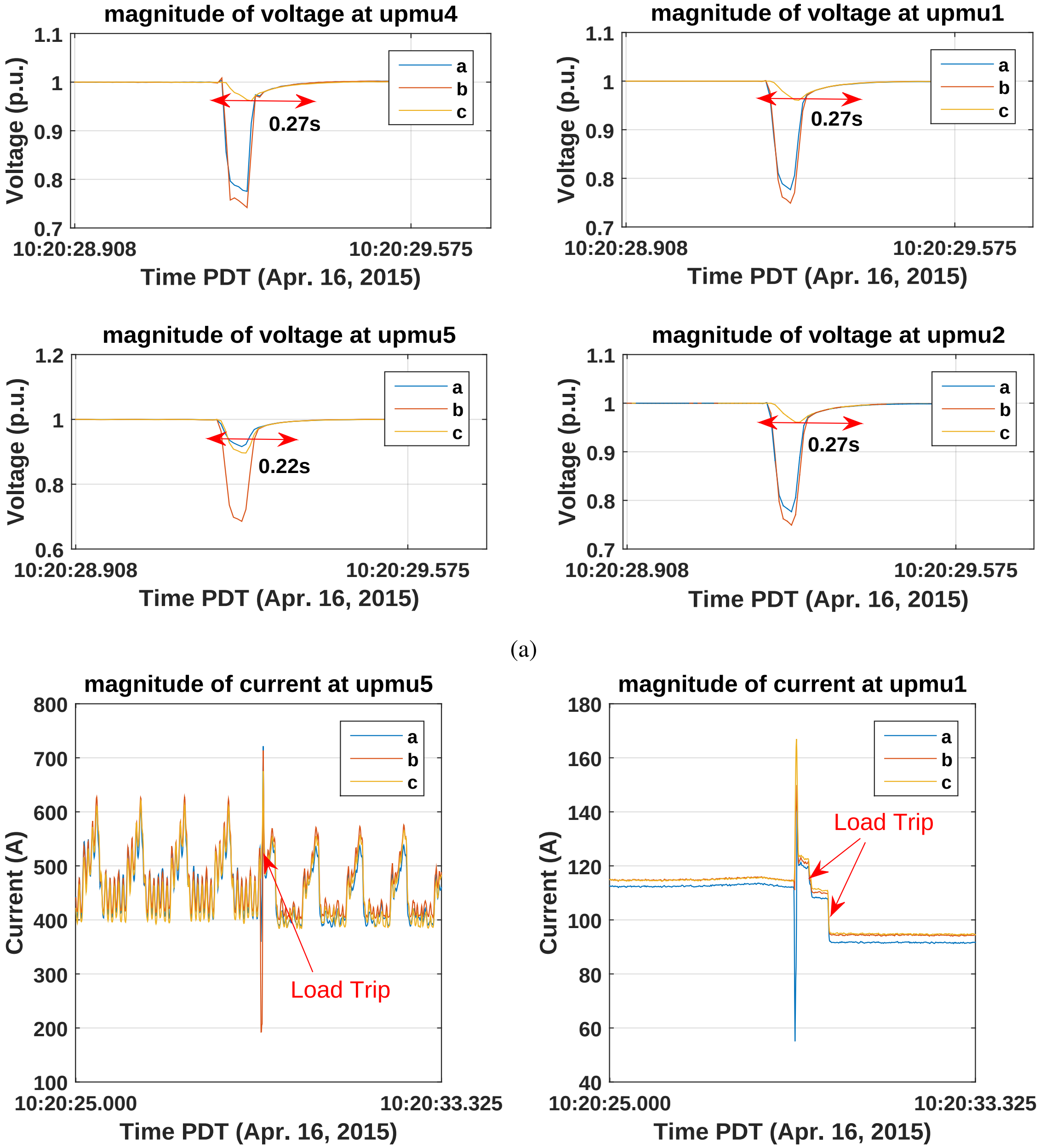


Fig. 2: Partner Utility Distribution Grid One-Line Diagram

provides the rules to check the compliance of the events seen in the $\mu$PMU measurements and in the network traffic, with the normal behavior of the system, with some level of certainty.

While ADMS and in particular DSCADA have potential existing security flaws due to the use of traditional and outdated security measured, $\mu$PMUs, as a new measurement device, are designed having modernized and advanced security practices in mind. As the first step, they are placed on a separate network from DSCADA, and are designed to be read-only devices, and to communicate over secure protocols. However, even if some of the $\mu$PMUs are compromised, since they only provide measurements (in spite of DSCADA, which also controls the devices and switches), many of the bad data detection techniques (e.g. [12]) can be used to remove the false data unless the number of compromised devices is large enough that data injection attack is lost in the noise. In this regard, the optimally-placed $\mu$PMUs can not only detect the bad data injection in DSCADA meters but also can be used to identify the bad data injection attack on a subset of $\mu$PMUs.

To illustrate the use of $\mu$PMU data in event detection and classification, we offer next an example based on the real data. Specifically, on April-16-2015 a power quality event was captured by the $\mu$PMUs installed at the partner utility grid shown in Fig. 2. The $\mu$PMUs data showed that a voltage sag occurred, impacting all the $\mu$PMUs placed on two separate feeders. The voltage and current phasor profiles during



(a)

(b)

Fig. 3: (a) Captured Voltage Sag by $\mu$PMUs, (b) Captured Current Phasor during Voltage Sag by $\mu$PMUs

the event can be seen in Fig. 3a, 3b, respectively. Different hypotheses can be formulated about what caused the voltage sag to happen, for example a local or remote transmission or distribution level fault, with a possible protection operation ensuing. Given the brevity of the event, it is extremely unlikely that DSCADA data would have captured the sags. But the enormous potential benefit of $\mu$PMU data in assessing security threats is best illustrated by the ability they offered to identify the likely source of the problem.

From Fig. 3a, 3b it is apparent that the severity of voltage sag is similar for the $\mu$PMUs on both circuits at the same voltage level. In addition, all the $\mu$PMUs captured the voltage sag simultaneously.

A distribution level fault at one feeder causing the simultaneous transients that is transferred through sub-transmission to the other feeder is plausible only if the transmission grid is not stiff with respect to transients happening at the distribution feeders, which is usually not the case. Even if this is the case,

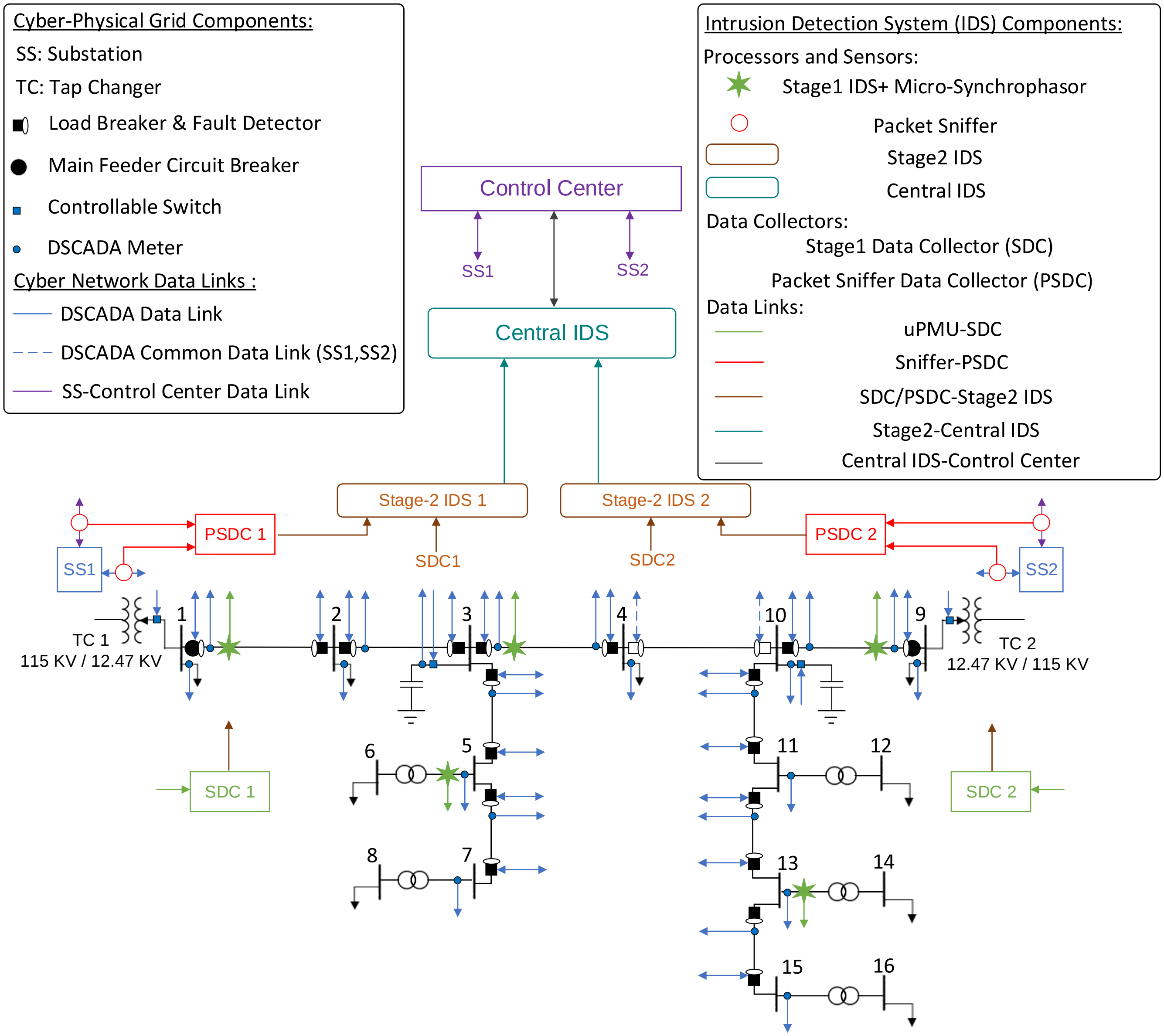


Fig. 4: The Hierarchical IDS Framework Includes: Stage-1 (Node Next to Each $\mu$PMU ($\star$)), Stage-2, and Central IDS.

the captured severity would be more significant on the feeder that the fault happened compared to the other that is not confirmed by the data. Another hypothesis is spreading of voltage sag through the closed Normally Open (N.O.) breakers to the other feeder. This is not corroborated by the data because the N.O. breaker between left and right side are secondary action, which means another breaker should first clear the fault and then this switch is closed to feed the healthy part of the grid. In that case, the sag is already over when the switch gets closed. Even if the attacker tries to close the switch before the fault clearance, the sag is transferred with a delay and different severity and shape to the other side. The transmission level event is the most plausible scenario, as it was visualized concurrently at all the two separate feeders, and is consistent with the $\mu$PMU data.

## IV. All-embracing IDS Framework: How to Utilize All the Resources?

The analysis of this event revealed the ability of the $\mu$PMUs to capture the footprints of a grid anomaly that led to physical impact. Based on this analysis we believe that this new rich source of data, combined with knowledge of the grid configuration and operations, allows to reason about different hypotheses and establish the likely cause of an event in a way that would not have been possible using DSCADA data or network traffic alone. In addition, it is worth mentioning that, depending on the type of events, some signatures would be more indicative than others of the situation. In the example we offered what the $\mu$PMU data cannot do is to clarify further what happened at transmission level, where we have neither observations nor detailed knowledge of the configuration and operations.

The abstraction of our $\mu$PMU-Based Intrusion Detection System ($\mu$PMU-IDS) architecture is shown in Fig. 4. In this figure, stage-1, stage-2, and central IDS form the three levels of IDS data processing, respectively. The correlation of the different data sources including the real-time $\mu$PMU measurements at multiple sites, and monitored DSCADA traffic are checked at different levels constantly to draw conclusions about the security state of the grid. In Section IV, we provide an example that illustrates how our data analytics differ from the standard network intrusion detection system.

The $\mu$PMU-IDS is designed to be scalable by partitioning the security rules hierarchically. The rules are established based on the physical constraints implied by the Physics of the grid in addition to the common cyber inspection in the computer networks security. The filters used in $\mu$PMU-IDS generalize and automate the process of hypothesis testing that we illustrated in the example we offered before, also utilize the DSCADA packets, and are based on encoding the semantics of the rules in a decision tree that can be inspected automatically by the $\mu$PMU-IDS components.

The $\mu$PMU-IDS is an incarnation of the Bro Network Security Monitor framework [13]. Functionally, the Bro Network Security Monitor is the "glue" that binds passive DSCADA system state observations, results leveraged from $\mu$PMU data archiving and analysis tools, and results obtained from circuit analysis activities. Output from the Bro framework will be in the form of predefined software events that can be customized to interact with commercial substation control systems.

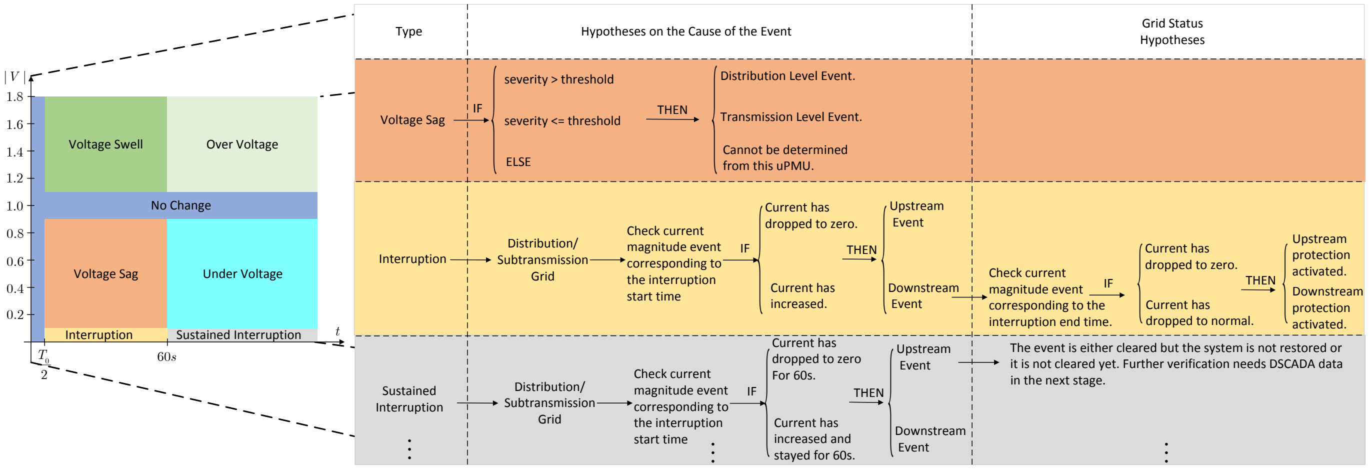
Interestingly, the $\mu$PMU-IDS rules pertaining the physical state emulate the behavior of an expert in the field looking at the logged data. Even without cyber security concerns this effort is important to address the *big data* issue, arising from the large amount of sensors and controllers placed on the grid, which would overwhelm the operators.

### *What Happens at Stage-1, Stage-2 and Central IDS Nodes?*

Each stage-1 IDS node that is located next to each $\mu$PMU (marked together with green star in Fig. 4) inspects for the signatures of anomalies in the phasor data streams of the corresponding $\mu$PMU. The rules inspect the anomalies in the voltage magnitude, estimated grid frequency, current magnitude, active and reactive power. In addition, the rules utilize the deviation from the steady-state Kirchhoff and Ohm's law as an indicator of transient behavior and possible changes in the physical parameters of the grid. The challenge is to use this model without full observability due to the limited number of $\mu$PMU devices. The radial structure suggests that placing $\mu$PMUs closer to the substation will increase the coverage, as transients happen in the sub-tree would be visible upstream. However, localizing the fault will become harder.

In the left side of Fig. 5 we show as an example how specific rules on the voltage magnitude can convert the data into inferences on various possible hypotheses. On the left side of the figure the data are first classified depending on the deviation from the nominal voltage and event time duration values, both criteria are independent from the loading conditions. Therefore, they define static rules. In this sense, the frequency rules also fall into the static category. On the other hand, the criteria to check the anomalies in the current magnitude, active and reactive power, and governing algebraic equations should be adaptively updated, so we call them as dynamic rules. The way that some of these dynamic quantities lead to the selection of different hypotheses on some of the voltage events in the stage-1 IDS is shown in the right side of Fig. 5.

The chunks of data containing the event, along with the analysis in the first stage are then collected via Stage-1 Data Collectors (SDCs) and reported to the stage-2 nodes were the compliance of the event is also checked with the monitored DSCADA traffic, and with the data from other $\mu$PMUs that are forwarded



|V|
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
Voltage Swell
Over Voltage
No Change
Voltage Sag
Under Voltage
Interruption
Sustained Interruption
t
$\frac{T_0}{2}$
60s
Type
Hypotheses on the Cause of the Event
Grid Status Hypotheses
Voltage Sag
IF
severity > threshold
severity <= threshold
ELSE
THEN
Distribution Level Event.
Transmission Level Event.
Cannot be determined from this uPMU.
Interruption
Distribution/ Subtransmission Grid
Check current magnitude event corresponding to the interruption start time
IF
Current has dropped to zero.
Current has increased.
THEN
Upstream Event
Downstream Event
Check current magnitude event corresponding to the interruption end time.
IF
Current has dropped to zero.
Current has dropped to normal.
THEN
Upstream protection activated.
Downstream protection activated.
Sustained Interruption
Distribution/ Subtransmission Grid
Check current magnitude event corresponding to the interruption start time
IF
Current has dropped to zero For 60s.
Current has increased and stayed for 60s.
THEN
Upstream Event
Downstream Event
The event is either cleared but the system is not restored or it is not cleared yet. Further verification needs DSCADA data in the next stage.
⋮

Fig. 5: Decision Region and Hypotheses of the Voltage Magnitude Events in the First Stage of the Local IDS

to the same stage-2 IDS. DSCADA packets at stage-2 are received from Packet Sniffer Data Collectors (PSDCs) that are responsible for collecting and forwarding the sniffed packets via sniffers (marked as red circles in Fig. 4). This stage also has access to the partial topology of the grid, from which the data is collected. In addition to further verification of the proposed hypotheses at the first stage, another set of hypotheses are proposed and tested at the stage-2. For example, if the interruption is detected, the bidirectional fault detectors that should see the fault must be checked to unveil a possible spoofing attack. The duration of the interruption can also be compared with the protective load breaker time of operation to determine if the breaker has tripped on time. Having the local picture of the grid implies that the rule on the algebraic equations between the current and voltage to check if they hold can be extended to correlate the available $\mu$PMU measurements and drawing conclusion about the source of this change. All of these rules become multidimensional decision regions that allow to narrow down more precisely what happened.

The results of the stage-2 IDS processors along with the segments of data containing anomalies are sent to the central IDS for the final set of tests and analysis that require the full picture of the grid in terms of topology and information. The central IDS node collects data from one or more stage-2 IDSs in order to make a conclusion.

An example of an attack scenario is now outlined to demonstrate the hypotheses and process formulated in this work, and tested using the $\mu$PMUs and DSCADA packets. This example also clarifies how the DSCADA commands, along with the $\mu$PMU data are leveraged in the anomaly detection. In the test case shown in Fig. 4, a short circuit fault happens on the line connecting bus 5 to 7. In its normal operation, a protection algorithm in substation 1 will detect the fault and use the relay on bus-1 breaker to deenergize the left feeder, at which point the load breakers placed on line 5-7 will receive a command to isolate the fault and finally energy will be restored to the healthy part of the feeder, by closing the circuit breaker at bus 1. Assume that a knowledgeable attacker has gained access to the network and the IP address of the substation controller. For instance, in a first scenario, the attacker could stage a Man-in-the-Middle attack jamming the command of the controller to the relay intended to open the circuit breaker. A second possible scenario is that the attacker changes the firmware of the relay at bus 1 (as in the Ukraine attack case [2]) and prevent it from tripping. The stage-1 IDSs, monitoring for anomalies in the data from the $\mu$PMUs on the left feeder, will detect a transient and alert the stage-2 IDS 1 by sending the data through the SDC1 (see Fig. 4). The packets sniffed by network taps placed on the links that connect the substation to the relays operating the switches at bus 1 and line 5-7, are also sent to stage-2 IDS from the sniffers through the PSDC1. Depending on the location of the sniffers, the analysis of the packets could reveal the man-in-the-Middle attack, corroborating the anomaly detected from the $\mu$PMU. If not, the $\mu$PMU will still indicate that the fault is not cleared, in spite of the opening command having been issued, revealing an attack either to the relay in bus 1 firmware, like in the aforementioned second scenario, or the other possible attack mentioned as the first scenario that is launched after the sniffer. Notice that the latter would not be detectable from the packet analysis only. Finally, combining the results in the central level shows that no event is reported from feeder 2 in that period, which is expected from the conclusions in the stage-2 IDS.

## V. Conclusions

We believe that any security practice for CPSs that ignores the governing physical rules underlying the system under control will not be successful [10]. In this article, we have discussed how the knowledge about the distribution system topology and operation, along with the real-time physical measurements from $\mu$PMUs and monitored communication traffic—enables us to bind the "physical" and "cyber" world and to formulate and test a set of hypotheses regarding the security status of the distribution grid.

In future work, we will investigate the optimal placement of $\mu$PMUs and network monitors for maximum coverage for a given number of sensors.

## Acknowledgments

This research was supported in part by the Director, Office of Electricity Delivery and Energy Reliability, Cybersecurity for Energy Delivery Systems program, of the U.S. DoE, under contract DE-AC02-05CH11231. Any opinions, and findings expressed in this material are those of the authors and do not necessarily reflect those of the sponsors.

## References

[1] *Enabling Modernization of the Electric Power System.* U.S. Department of Energy, Quadrennial Technology Review 2015.

[2] cbc news Technology and Science, "cyberattack that crippled ukrainian power grid," http://www.cbc.ca/news/technology/ukraine-cyberattack-1.3398492.

[3] J. H. Eto, E. M. Stewart, T. Smith, M. Buckner, H. Kirkham, F. Tuffner, and D. Schoenwald, "Scoping study on research and priorities for distribution-system phasor measurement units," 2015.

[4] "PQube3 information," http://www.powersensorsltd.com/PQube3.php, accessed: 2016-01-15.

[5] A. von Meier, D. Culler, A. McEachern, and R. Arghandeh, "Micro-synchrophasors for distribution systems," in *Proc. IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, 2014, pp. 1–5.

[6] T. T. Tesfay, J.-P. Hubaux, J.-Y. Le Boudec, and P. Oechslin, "Cyber-secure communication architecture for active power distribution networks," in *Proceedings of the 29th Annual ACM Symposium on Applied Computing*. ACM, 2014, pp. 545–552.

[7] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Proc. SmartGridComm*. IEEE, 2010, pp. 350–355.

[8] J. Slay and M. Miller, *Lessons learned from the maroochy water breach.* Springer, 2008.

[9] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proc. 6th ACM Symposium on Information, Computer and Communications Security*, 2011, pp. 355–366.

[10] C. McParland, S. Peisert, and A. Scaglione, "Monitoring security of networked control systems: It's the physics," *Security & Privacy, IEEE*, vol. 12, no. 6, pp. 32–39, 2014.

[11] G. Koutsandria, R. Gentz, M. Jamei, A. Scaglione, S. Peisert, and C. McParland, "A real-time testbed environment for cyber-physical security on the power grid," in *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*. ACM, 2015, pp. 67–78.

[12] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 326–333, 2011.

[13] V. Paxson, "Bro: a system for detecting network intruders in real-time," *Computer networks*, vol. 31, no. 23, pp. 2435–2463, 1999.

**Mahdi Jamei** is a Ph.D. student of ECEE at ASU. He received his M.Sc. in ECE from Florida International University, 2014 and B.Sc. in EE from IUST, 2013. His main research area is in the cyber security of smart power grid. Contact him at mahdi.jamei@asu.edu.

**Emma Stewart** is a research scientist and deputy leader of Grid Integration at LBNL. Dr. Stewart develops methodologies for utilities to integrate data and also focuses on high penetration of distributed energy resources. She is a senior member of IEEE. Stewart completed her undergraduate degree in

Electrical and Mechanical Engineering from the University of Strathclyde in 2004 and a PhD in EE in 2009. Contact her at estewart@lbl.gov.

**Sean Peisert** is a staff scientist at LBNL, chief cybersecurity strategist at CENIC, and an associate adjunct professor at UC Davis. His research in computer security includes intrusion detection and vulnerability analysis. Peisert received a PhD in computer science from UC San Diego. He is a senior member of IEEE and the ACM. Contact him at sppeisert@lbl.gov.

**Anna Scaglione** is a professor of ECEE at ASU. Her expertise is in signal processing for communication systems, networks, and power system. Scaglione received a PhD in electrical engineering from the University of Rome La Sapienza. She is the recipient of the IEEE Donald G. Fink Award and is a Fellow of IEEE. Contact her at anna.scaglione@asu.edu.

**Chuck McParland** has been a staff computer scientist at LBNL since 1979, with a primary focus on developing and evaluating systems at the intersection of software and physical sensors and control systems. His recent focus has been smart grid and control system security. Contact him at cpmcparland@lbl.gov.

**Ciaran Roberts** is a scientific engineering associate at LBNL. Ciaran is a member of IEEE and received his MSc in Energy Systems Engineering in 2015 from University College Dublin. His work primarily focuses on power distribution engineering and the integration of distributed energy resources. Contact him at cmroberts@lbl.gov.

**Alex McEachern** is the President and CEO of PSL and the principal architect of the $\mu$PMU instrument described in this paper, is the chairman of the IEC power quality instruments standard working group. He is a Fellow of the IEEE. Contact him at Alex@PowerStandards.com.