Vulnerability of Synchrophasor-based WAMPAC Applications' to **Time Synchronization Spoofing**

Dr. Luigi Vanfretti

RPI
ECSE, Troy, NY, USA
Web: ALSETLab.com
Email: vanfrl@rpi.edu
luigi.vanfretti@gmail.com

NASPI Work Group Meeting
Albuquerque, NM
April 24-26, 2018

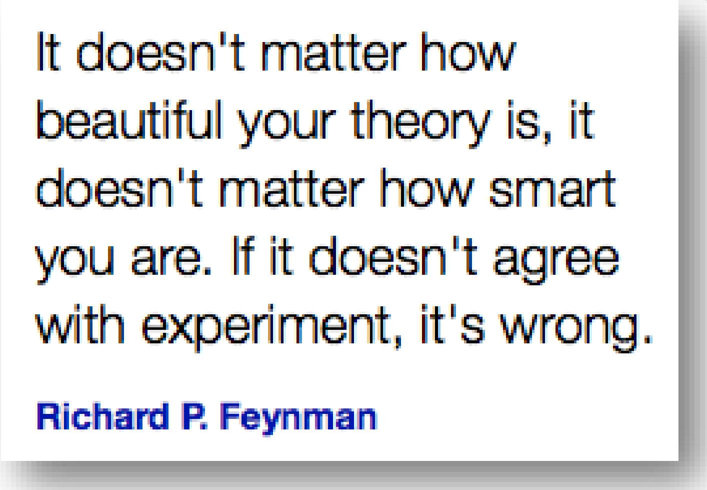
Outline and Main Messages

- **Motivation & Background**
  - What is the threat level?
  - Synchrophasor Technology Fundamentals
  - Vulnerability of WAMPAC Systems (Cyber-Physical Threats)

- **Experimental Methodology and Environment**
  - Methodology: How to lawfully attack (corrupt) GPS time?
  - Experimental set-up

- **Experiments**
  - Impact on PMU Computations
  - Impact of Time Synchronization Spoofing Attacks (TSSAs) on WAMPAC: Monitoring, Control and Protection
  - PMU behaviors under Time-Synch perturbations

- **Conclusions**
- Future Work



It doesn't matter how beautiful your theory is, it doesn't matter how smart you are. If it doesn't agree with experiment, it's wrong.

Richard P. Feynman

Main Messages

- Spoofing can affect PMUs and their applications.
- We need to understand and quantify their impact.
- To fully understand something, we need to reproduce it → do experiments!
- The presentation shows how to lawfully conduct experiments related to GPS spoofing, and to
- Experimentally characterizes the mechanisms that make jeopardize PMU applications and the grid.

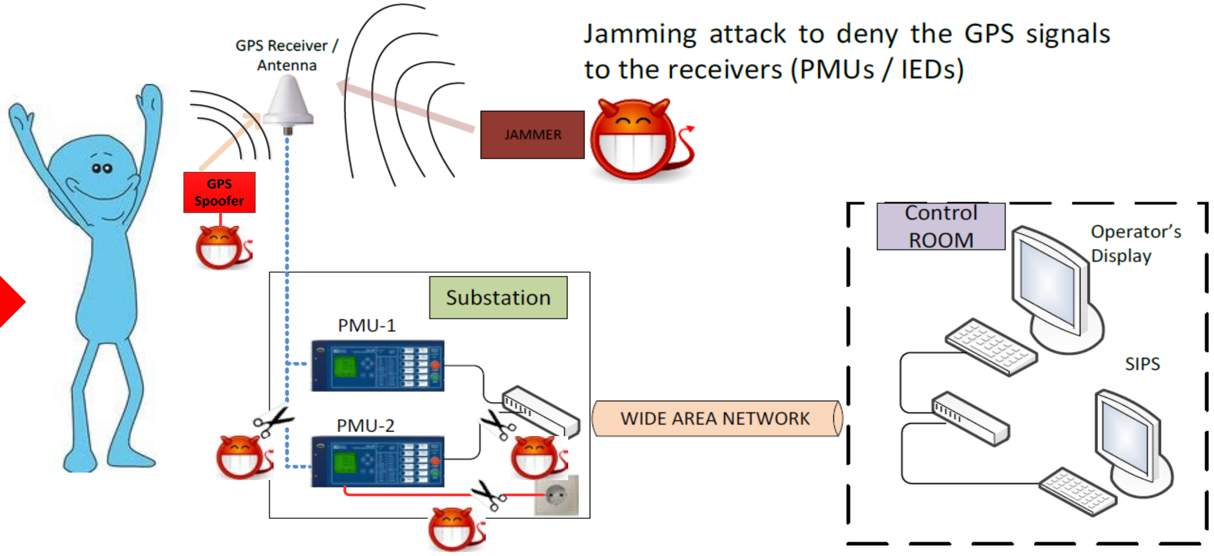
Pic: Megadeth

THE THREAT IS REAL!

Cyber-Physical *Security*
Vulnerabilities of PMU Applications due to GPS Spoofing

- Synchrophasor applications can be affected by:
  - Both physical and cyber attacks
- Cyber & physical attacks can be directed to critical systems used by PMUs:
  - Computer systems, communication systems,
  - *Timing systems (GPS)* → critical for computer and communication, can be "spoofed".

- GPS: The Global Positioning System, or GPS, is a satellite based navigation system developed by the United States Defense Department in the 1970's.
- It provides three items to users:
  - Position - Latitude, Longitude, and Height
  - Velocity - Velocity North, East, and Up
  - Time - in UTC (Universal Time Coordinated)
- ***GPS Time is the MASTER CLOCK!***

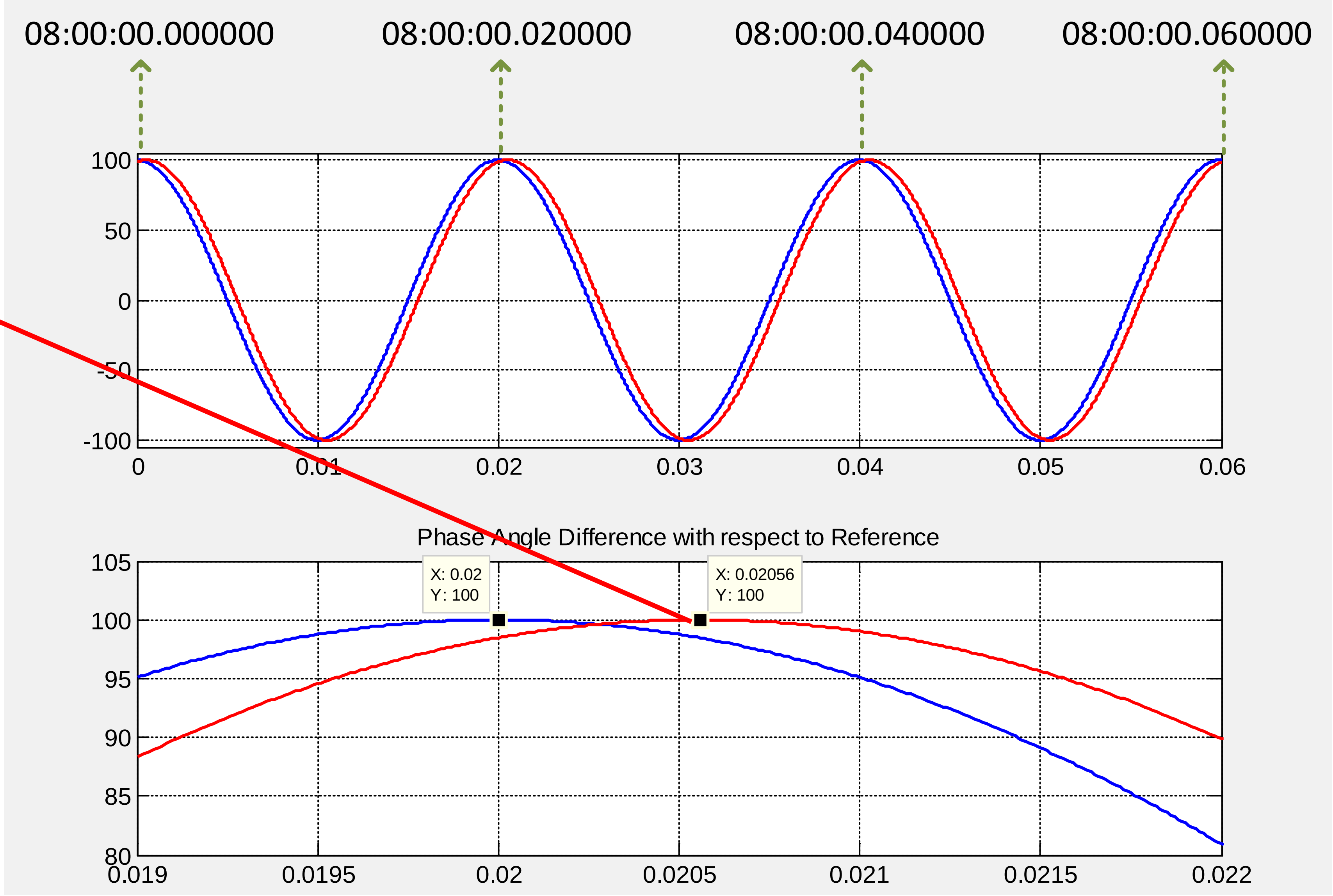

Jamming attack to deny the GPS signals to the receivers (PMUs / IEDs)

Time Synchronization and
SynchroPhasors Interdependency Fundamentals

- ***PMU Accuracy Requirement:*** IEEE C37.118.1-2011 specifies a Total Vector Error (TVE) limit of 1% i.e. 0.573^0 (degrees) or 31.8 μs at 50 Hz.
- Blue: reference (perfect)

- ***Interdependency:*** WAMPAC applications depend on the accuracy of the synchrophasors, and consequently on the precision input time signals.

- ***Vulnerability:*** The GPS system can be interfered both intentionally and/or cosmically.



CURENT

EXPERIMENTAL

METHODOLOGY AND ENVIRONMENT

Experimental Methodology (1/2) –

How to lawfully interfere with GPS? *i.e.* How to study the Time Synch. Signal attacks?

To interfere with Time Synchronization Systems

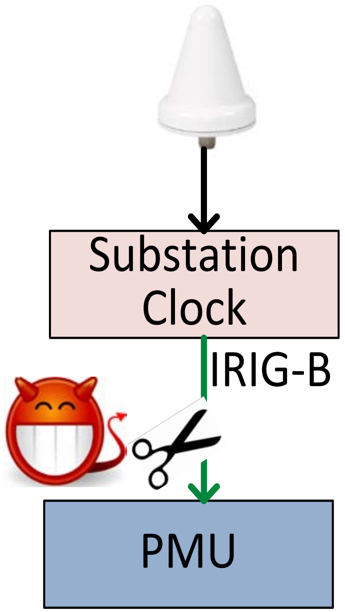
Make/Buy a GPS Jammer → NO

- Unlawful to intentionally interfere with GPS signal
- Impact on other technologies cellphone services, WIFI etc.

Due to the use of IRIG-B for time distribution, an alternative is to

Lawfully, generate/control/corrupt the IRIG-B signal distribution in a laboratory environment

- Develop IRIG-B signal generator



To characterize the impact on PMU Apps and the power grid

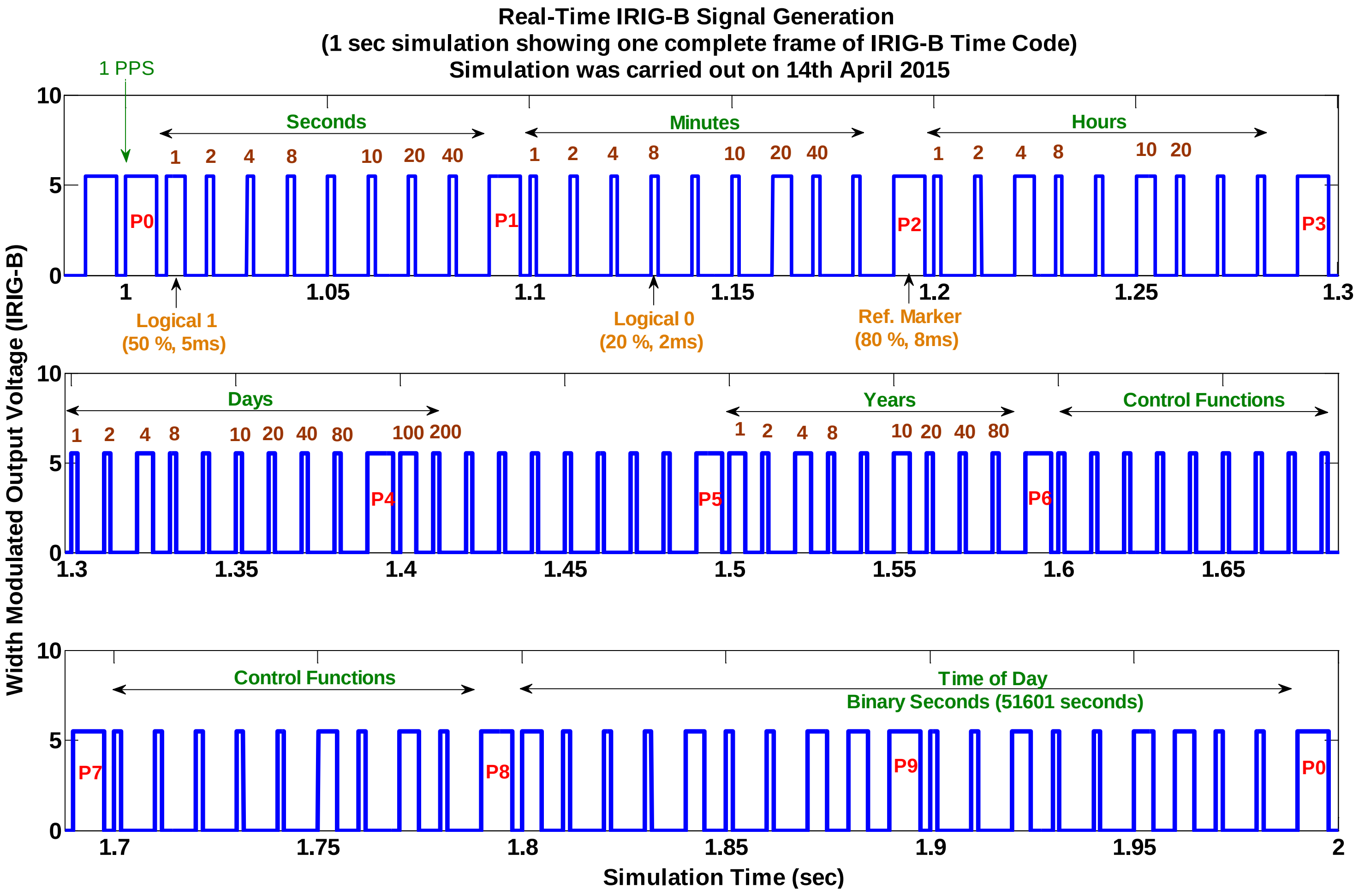
- Use Real-Time Hardware-in-the-Loop simulation
  - Simultaneously generate the voltage and current waveforms, AND the spoofed IRIG-B signal
- Put the RTS in the loop with **real** PMUs
- And the **prototype PMU data applications**: monitoring, control and protection

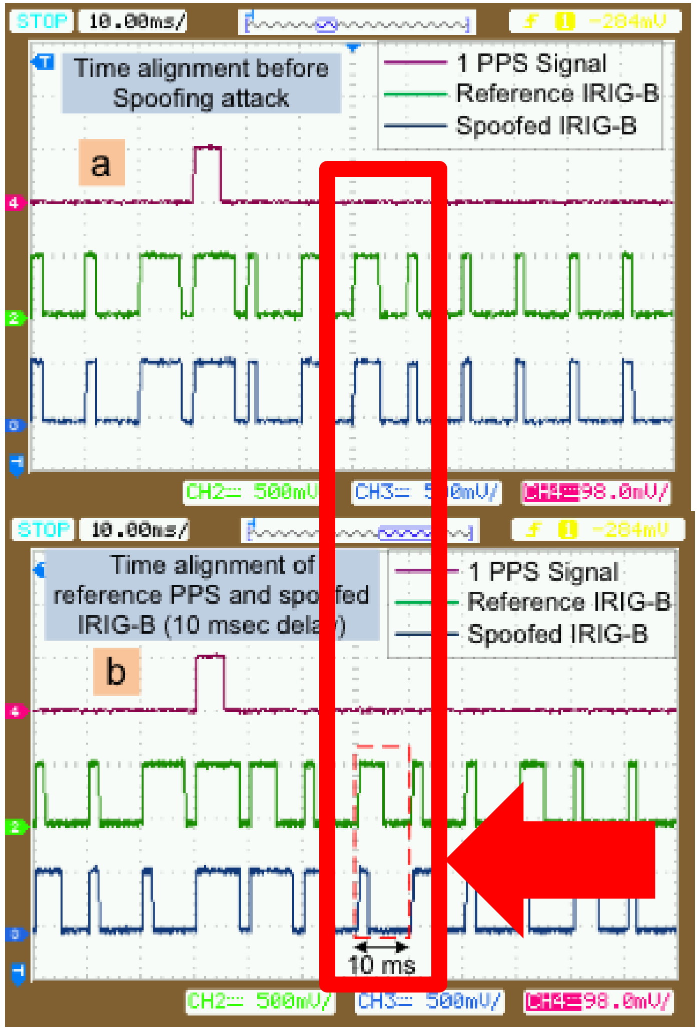
- ***Applications in this presentation:***
- Monitoring - Phase Angle Monitoring (PAM), Control - oscillation damping, Protection - anti-islanding protection

Experimental Methodology (2/2) –
IRIG-B Signal Generator for Real-Time Simulators

Get it on GitHub!

https://github.com/ALSETLab/IRIG-B_for_RT

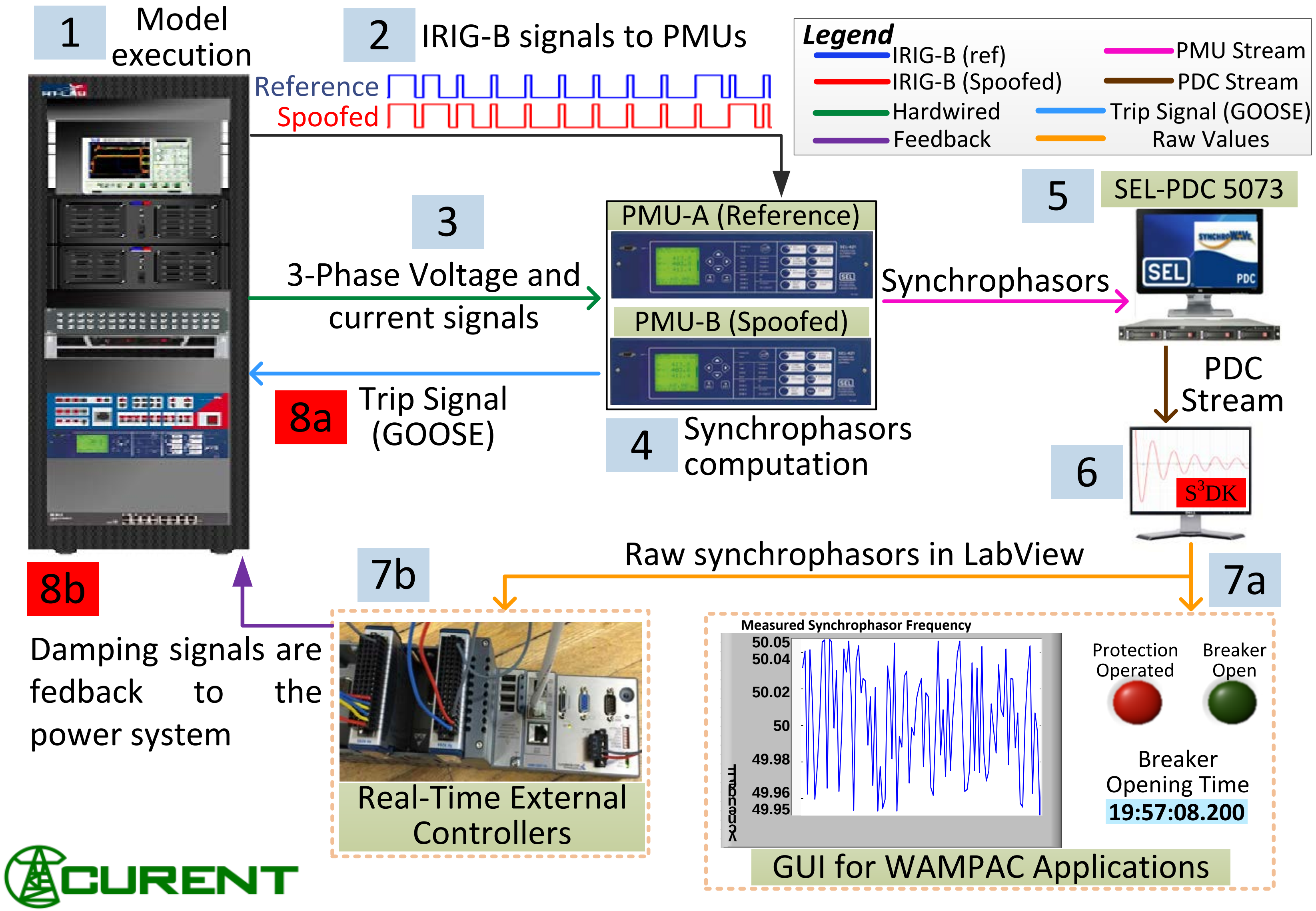

Real-Time IRIG-B Signal Generation
(1 sec simulation showing one complete frame of IRIG-B Time Code)
Simulation was carried out on 14th April 2015



- The TSSA is modeled through real-time IRIG-B signal generator, within the RT simulator.
- Possible to delay the time synchronization signals from microseconds to milliseconds.

Experimental Setup

Time Synch. Signal Spoofing



1 Model execution

2 IRIG-B signals to PMUs

Legend

- IRIG-B (ref)
- IRIG-B (Spoofed)
- Hardwired
- Feedback
- PMU Stream
- PDC Stream
- Trip Signal (GOOSE)
- Raw Values

3 3-Phase Voltage and current signals

PMU-A (Reference)

PMU-B (Spoofed)

4 Synchrophasors computation

Synchrophasors

5 SEL-PDC 5073

PDC Stream

6

8a Trip Signal (GOOSE)

8b

Damping signals are fedback to the power system

7b

Raw synchrophasors in LabView

7a

Real-Time External Controllers

Protection Operated

Breaker Open

Breaker Opening Time

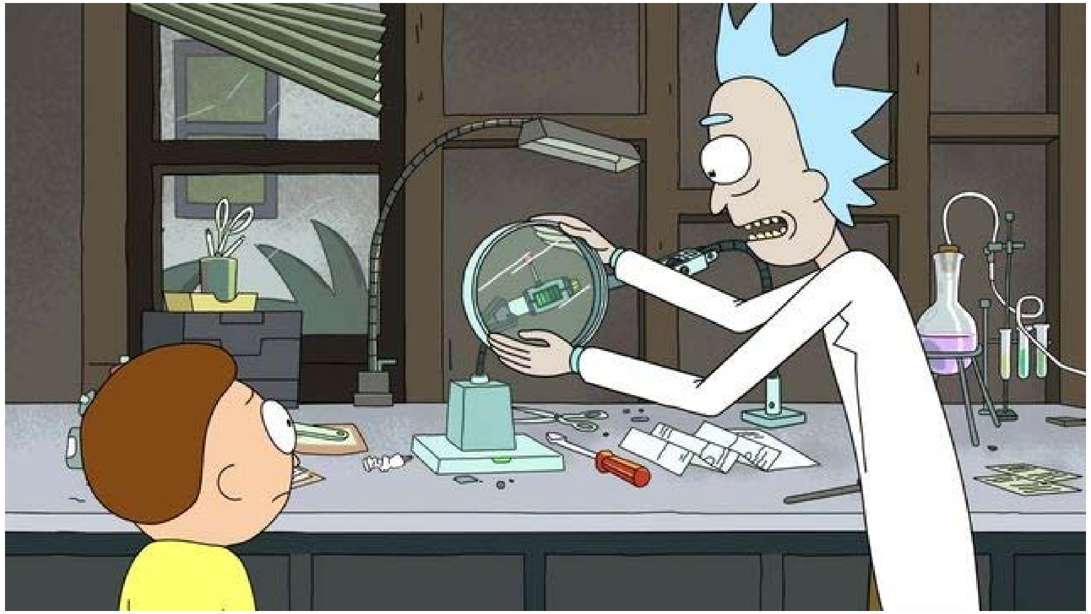
19:57:08.200

GUI for WAMPAC Applications

- IRIG-B generator and power system model executed in RTS
- PMU-A = reference PMU continuously receiving authentic (Reference) IRIG-B signals from the RTS.
- PMU-B = test PMU receives Spoofed IRIG-B signals from the RTS at a given point in time
- **Two case studies for all experiments** (but only selected results in this presentation):

Case A: "Rick"
Time Sync Signal Loss

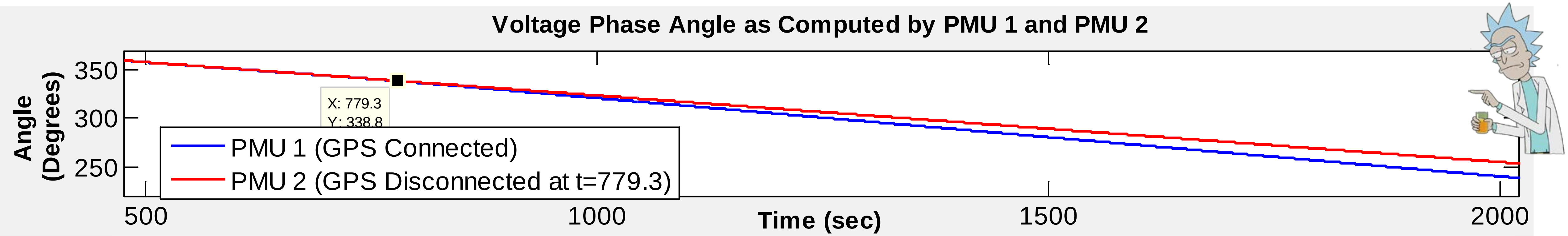
Case B: "Morty"
Time Sync Signal Spoofing



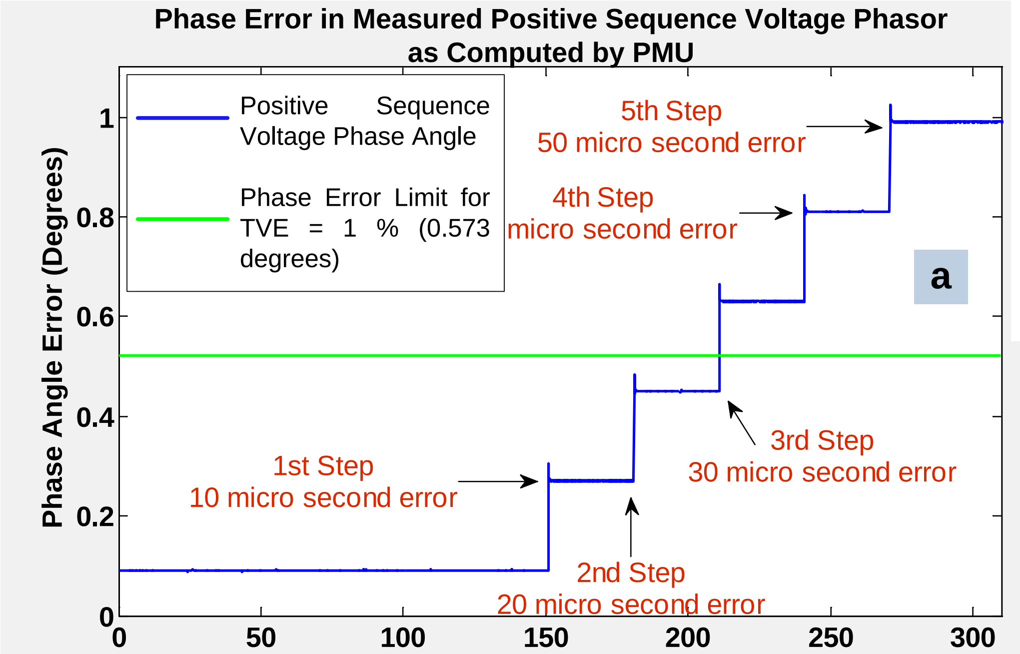
EXPERIMENTS

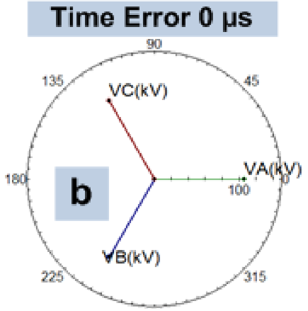
IMPACT ON PMU COMPUTATIONS AND APPS

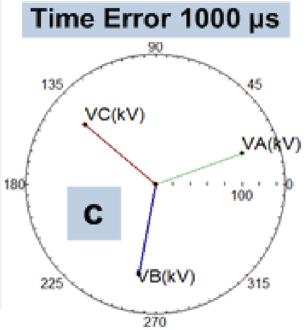
Experiment(s) 1: Impact on *Synchrophasor Computation*



As GPS time synchronization **signal to PMU 2 is lost**, its error in voltage phase angle computation increases.





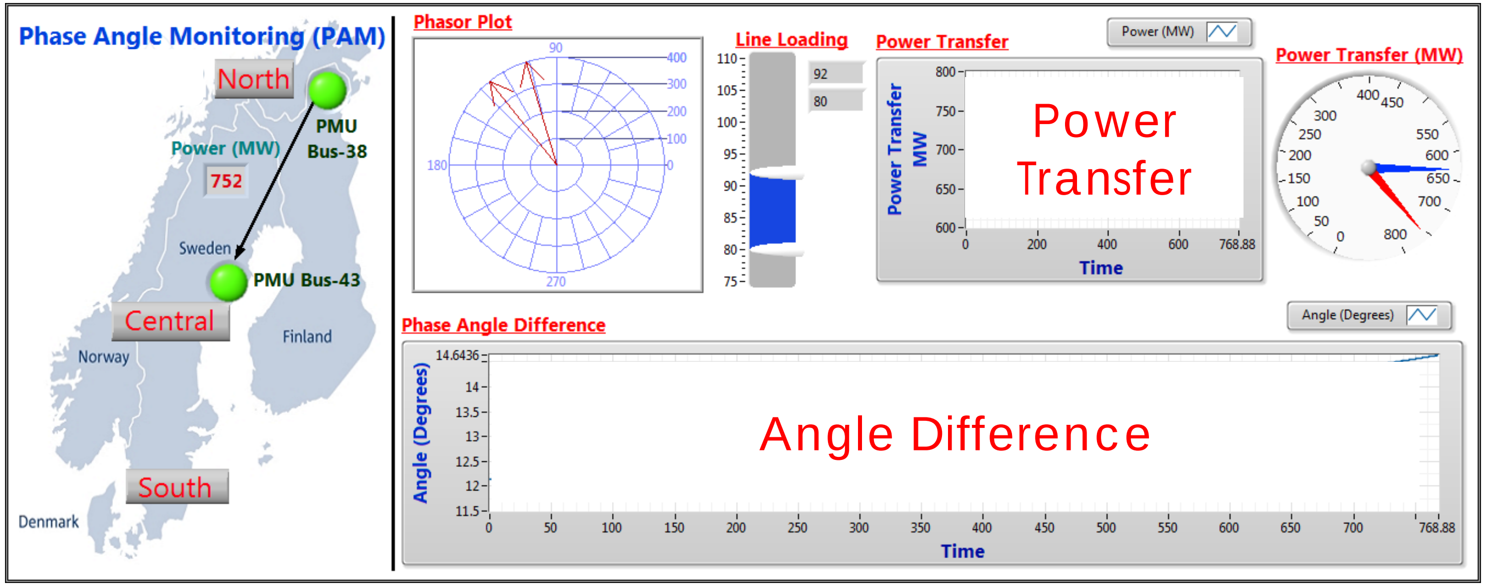


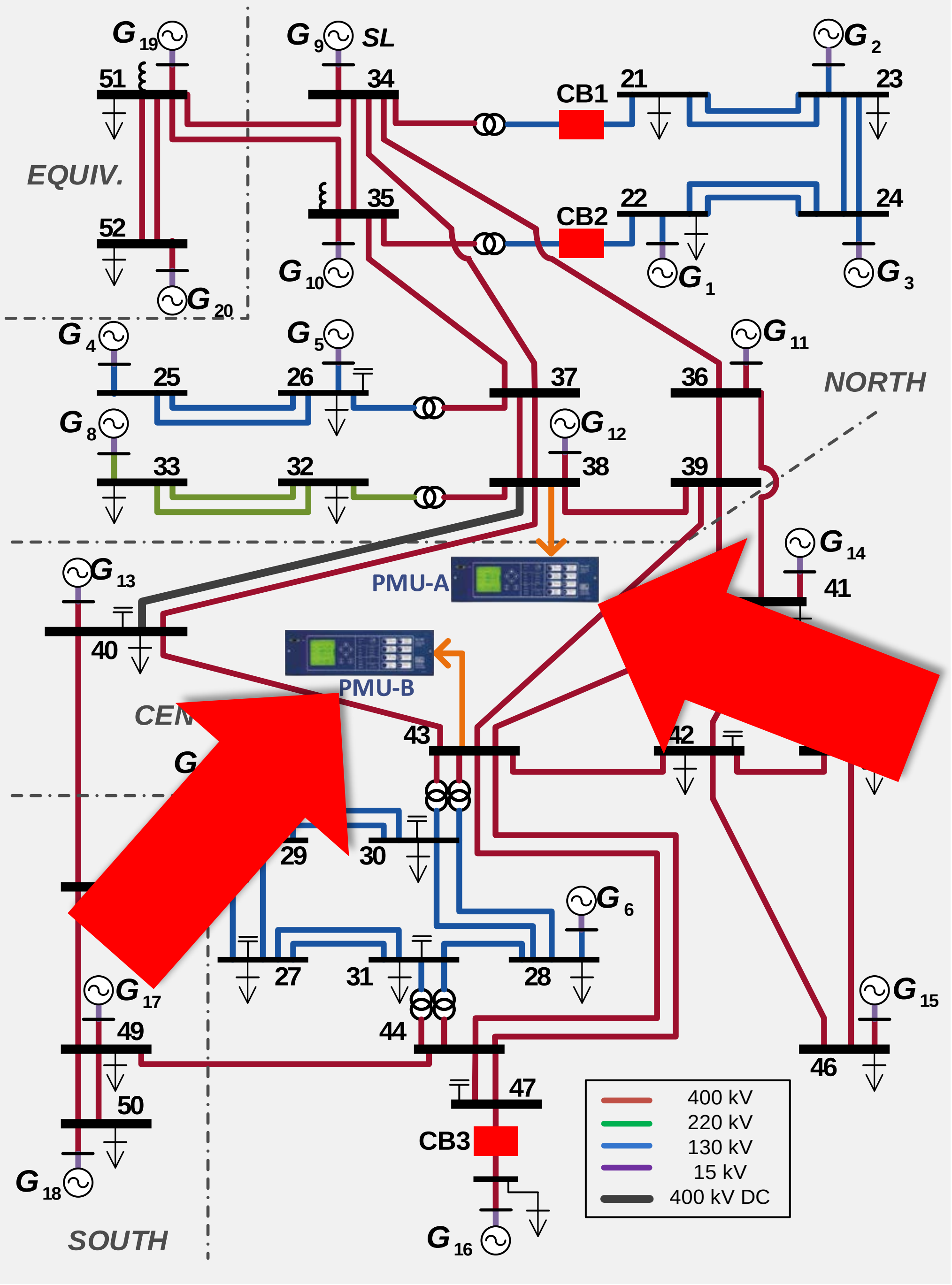
- TSSA results in an error in voltage phase angle computation beyond 0.573^0 mark as soon as the time error increases beyond 30 µs, thus breaching the maximum allowable TVE limit.
- The actual synchrophasors as computed by the PMU before and after time spoofing by 1000 µs, thus resulting in a phase angle error of about 18^0

App. 1:

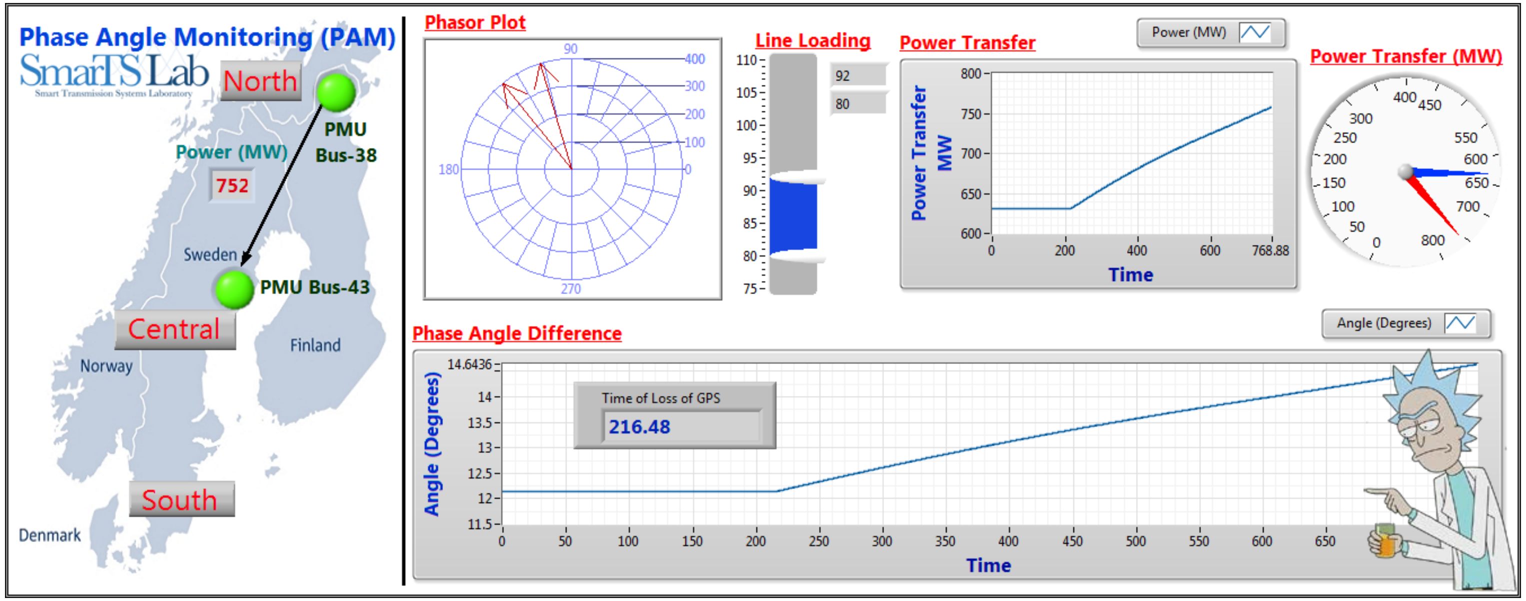
Phase Angle Monitoring Application

- The impact of Time Synchronization Signal Loss and TSSA on Phase Angle Monitoring is analyzed on a variant of the Nordic-32 power system model.
- PMU-A and PMU-B are receiving three phase voltages and currents from Bus-38 and Bus-43, respectively which allow monitoring a major corridor between the North and the Central part of the network.
- At a given point in time, the time synchronization signal input to PMU-B is disconnected or spoofed
- Prototype PAM App:





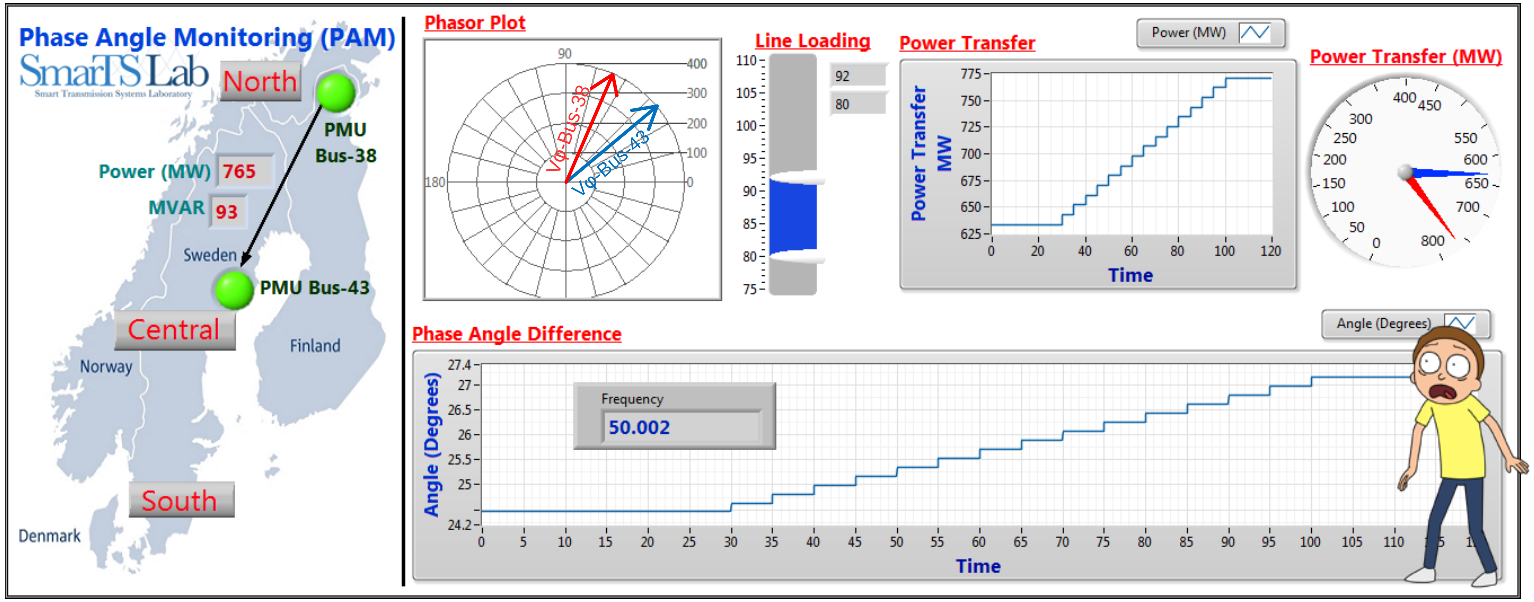
Experiment(s) 2: Impact on *Phase Angle Monitoring App.*



Power (MW) 752

Line Loading 92, 80

Time of Loss of GPS 216.48



Power (MW) 765

MVAR 93

Line Loading 92, 80

Frequency 50.002

Signal loss case:

- 550 s after the disconnection the signal to PMU2
- Erroneous increase in line loading from 80% to 92 %
- Corrupt reading: from 625 MW to 752 MW

TSSA case:

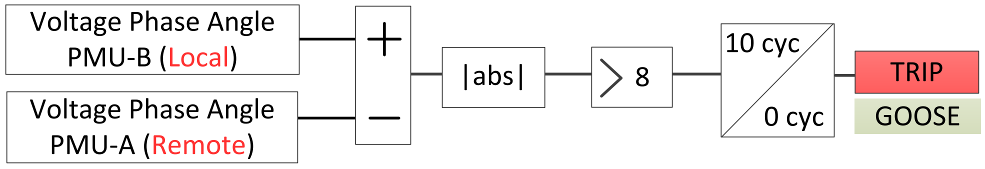
- From t = 30 s, the TSSA is launched on PMU-B (connected at Bus-43).
- Attack using steps of 10 μs at precisely every 5 seconds.
- Within a span of 70 s:
  - Erroneous increase in line loading of 12 %
  - An increase in power transfer from 630 MW to 765 MW

By end of TSSA, at t = 100 s, phase error = 2.69^0 due to a time synchronization error of 150 μs.

App. 2:

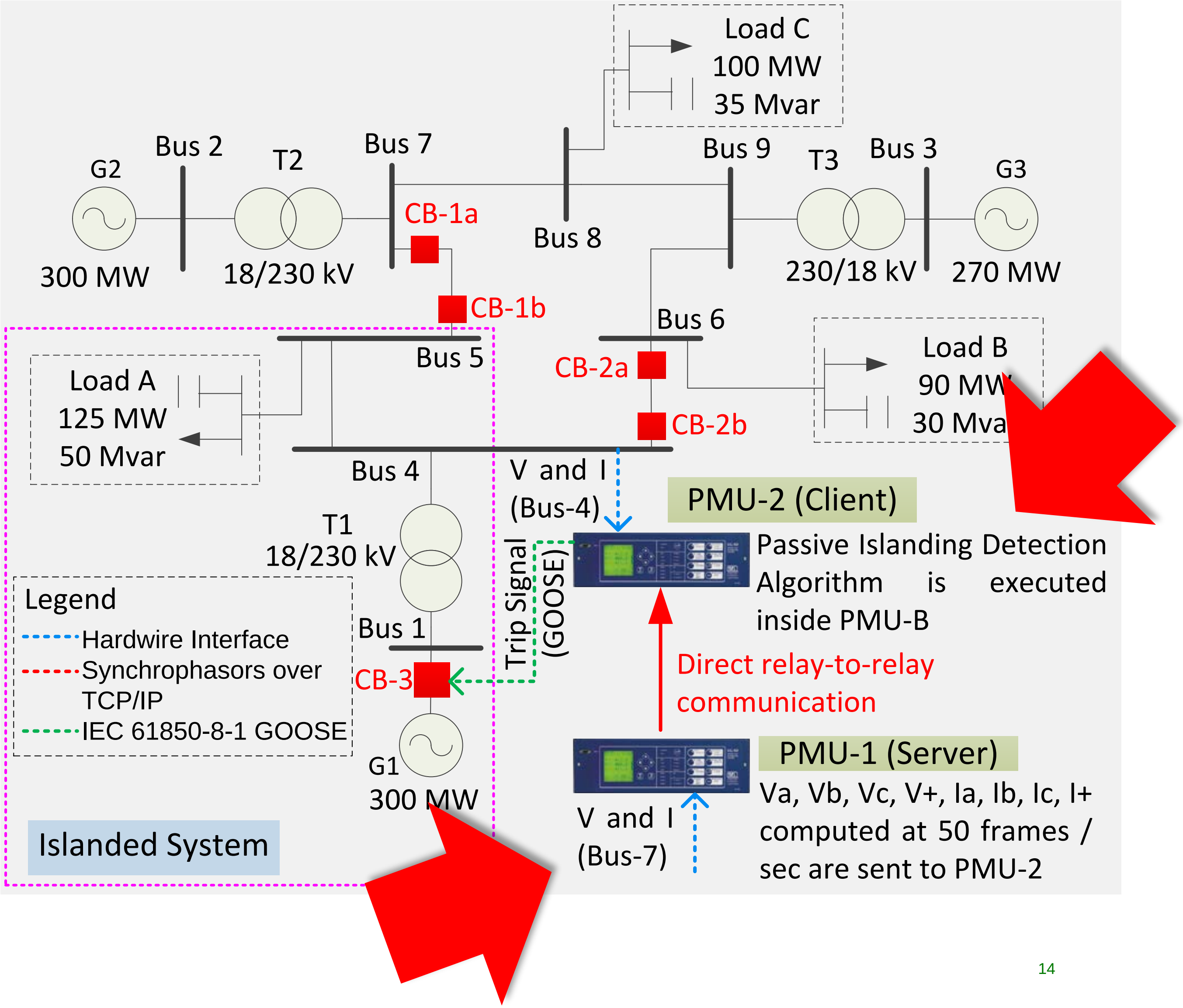
Synchrophasor-based Passive Anti-Islanding Protection

- Synchrophasor-based scheme and implementation:



```
PMV53 := V1YPMA % Storing Local Positive sequence synchrophasor voltage angle in user defined analog
PMV54 := RTCAP01 % Storing remote Positive sequence synchrophasor voltage angle in user defined analog
PMV55 := 8.00000 % Store threshold value of 8 degrees in user defined analog
PSV01 := abs (PMV53 - PMV54) > PMV55 % SET if measured synchrophasor synchrophasor voltage phase angle difference is greater than 8 degrees
PCT01IN := PSV01 % Input for conditioning timer. Timer tracks PSV01
PCT01PU := 10.000000 % Pickup is set to 10 cycles i.e. When PSV changes state from 0 to 1, the timer picks it up only if state of PSV01 stays 1 for 10 cycles
PCT01Q : Timer output SET to 1 when time exceeds 10 cycles after PSV01 is set
```

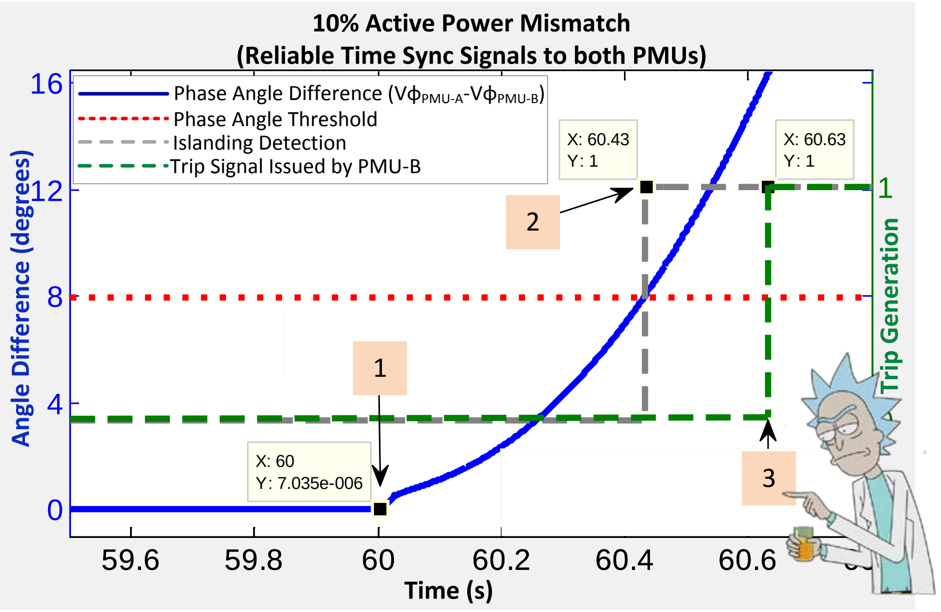
- **Experiment:**
  - If CB-1a, CB-1b and CB-2a, CB-2b are opened simultaneously, this results in an islanding condition with G1 supplying electric power to Load A at Bus 5.
  - Once the breakers are opened and the island is formed, G1 needs to be disconnected from the isolated network within 2 seconds as specified by IEEE Std. 1547-2008

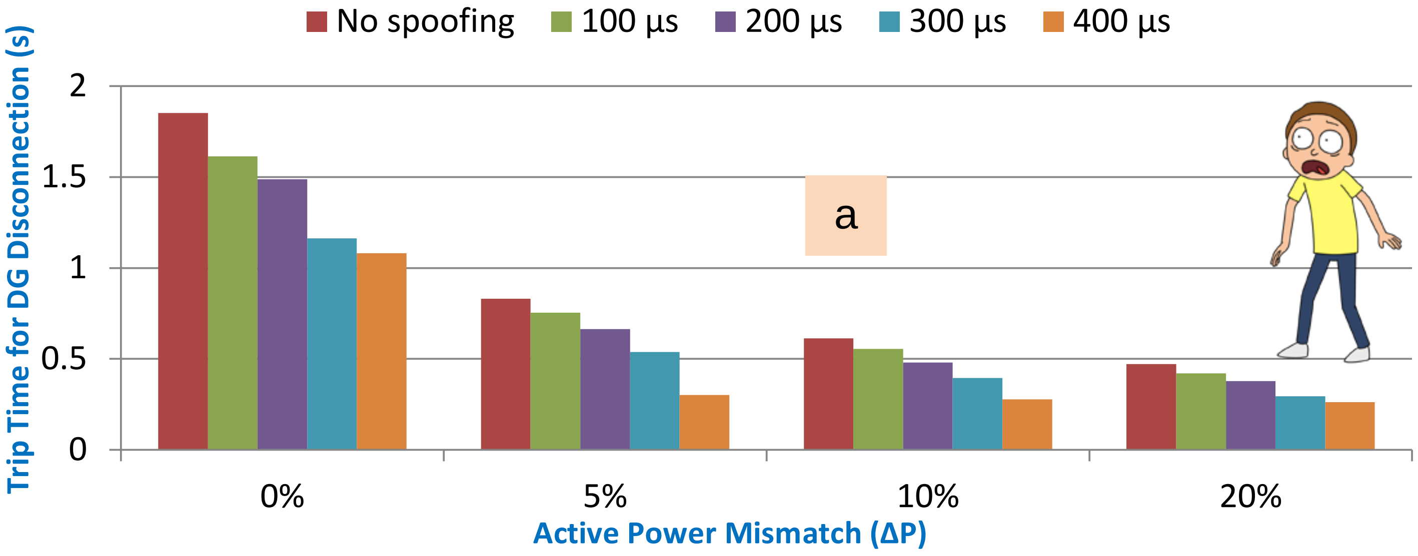


Experiment(s) 3: Impact on *PMU-based Passive Anti-Islanding Protection*

Signal Loss Case:

- At 60 s, island is formed by opening CBs.
- The phase angle difference (blue trace) goes beyond 8^0 at 60.43 s (grey trace).
- Timer elapses 10 cycles, the PMU-B issues a trip command to disconnect the DG from the isolated island (green trace).
- This increases by 1.022 s for 20 % active power mismatch and 0.62 s for 30 % active power mismatch.


10% Active Power Mismatch
(Reliable Time Sync Signals to both PMUs)

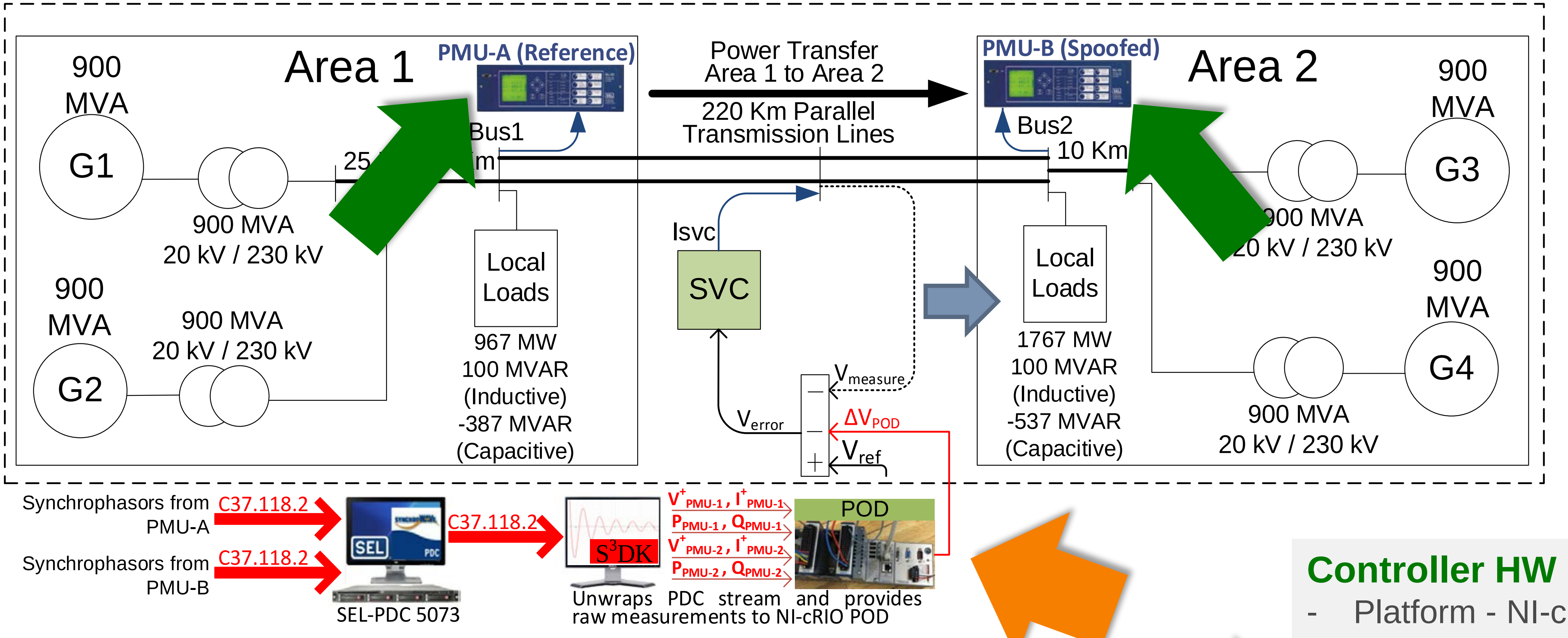


Spoofing case:

- As the TSSA is increased beyond 448.48 µs, the phase angle difference computed by PMU-B goes above 8^0 and the anti-islanding protection scheme initiates false tripping instantly.
- The operation time reduces with an increase in active power mismatch between generator G1 and Load-A for all cases i.e. with and without TSSA.

App. 3:

Wide-Area Phasor-Based Damping Control (WAPOD)



This WAPOD deployed in National Instrument's cRIO embedded control platform:

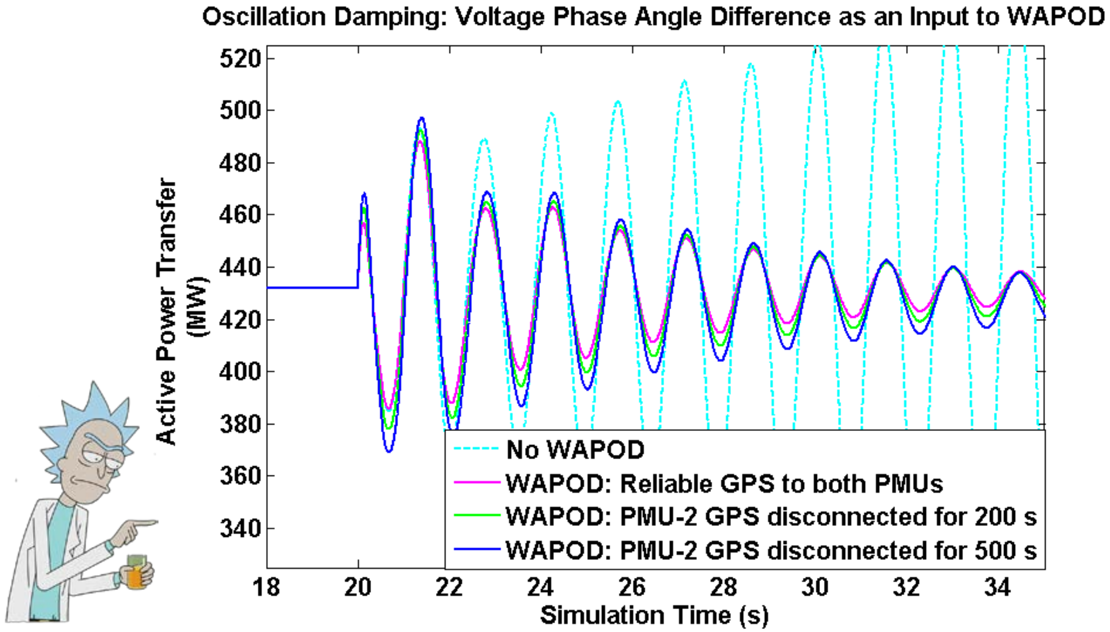
- Receives local and/or remote synchrophasors as inputs,
- Control Algorithm Implemented in the controller's FPGA:
  - Separates the controller input signal into average and oscillatory content
  - Oscillatory content of the signal is phase shifted to create the damping signal
- This damping signal is provided as a supplementary control signal to the Static VAR Compensator (SVC)

Controller HW Specs:

- Platform - NI-cRIO 9081 (1.06 GHz, 16 GB)
- Output - analog output module NI-9264 (25 kS/s per channel)

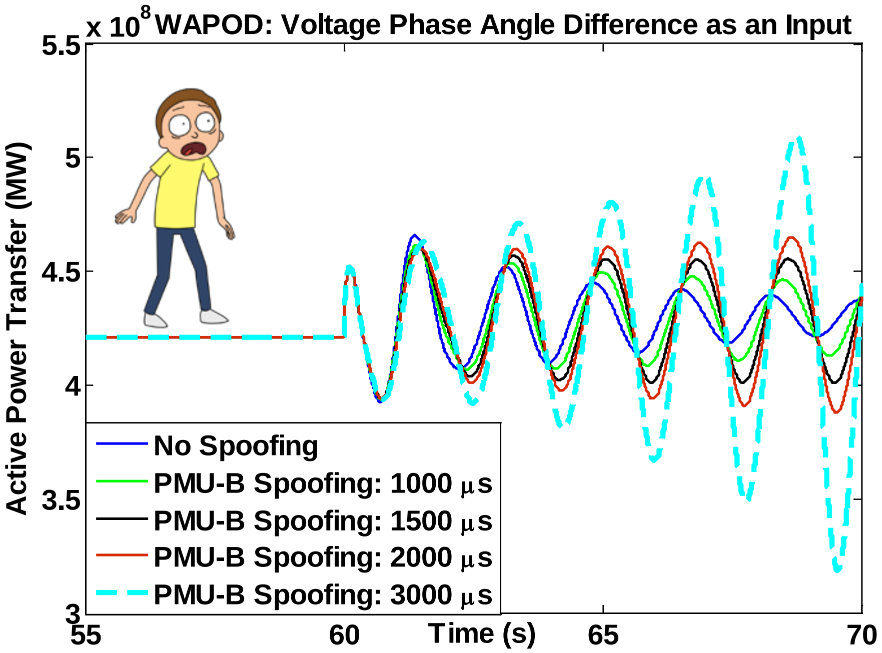
Experiment(s) 4: Impact on *PMU-based Passive Anti-Islanding Protection*

Signal Loss



- With the WAPOD disabled, the 0.64 Hz inter-area oscillation is not damped.
- WAPOD’s performance degrades as the GPS disconnection time for PMU-2 increases

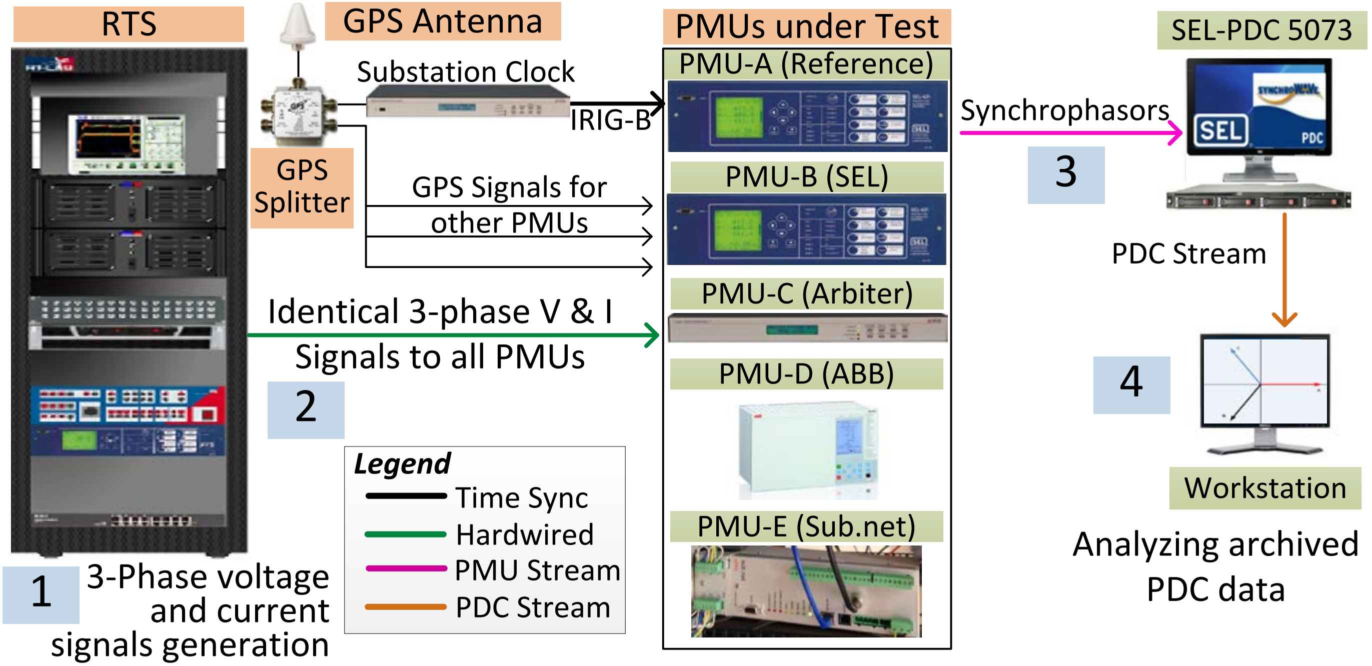
Spoofing Attack



- As the time synchronization error in PMU-B increases, its error in phase angle computation escalates.
- As the TSSA increases beyond 1500 μs, the WAPOD introduces a negative damping.

PMU behaviors under Time-Synch perturbations:

Do all PMUs behave similarly?



RTS

1 3-Phase voltage and current signals generation

GPS Antenna

GPS Splitter

Substation Clock

IRIG-B

GPS Signals for other PMUs

Identical 3-phase V & I Signals to all PMUs

2

PMUs under Test

PMU-A (Reference)

PMU-B (SEL)

PMU-C (Arbiter)

PMU-D (ABB)

PMU-E (Sub.net)

Synchrophasors

3

SEL-PDC 5073

PDC Stream

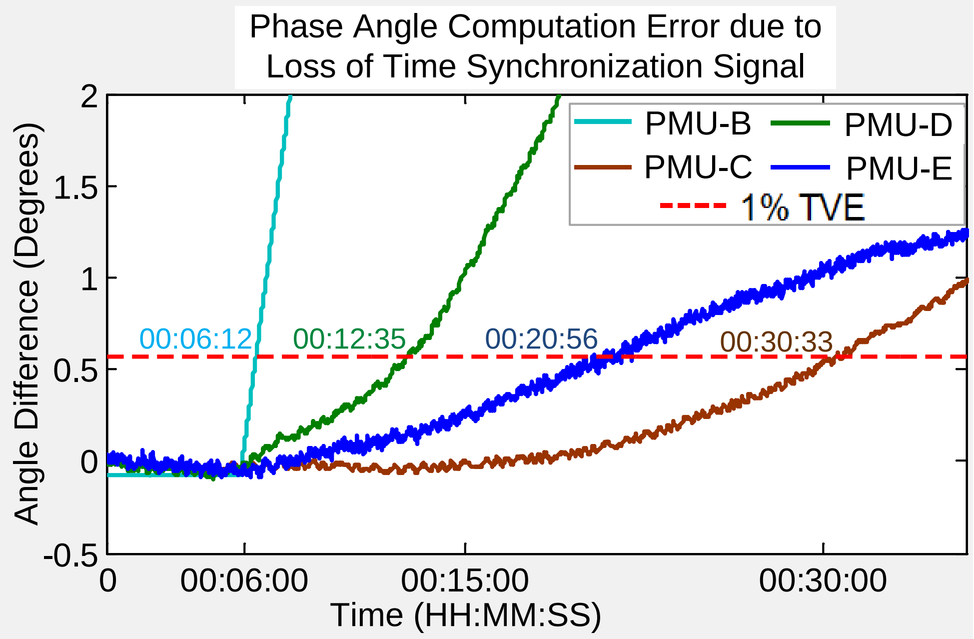
4

Workstation

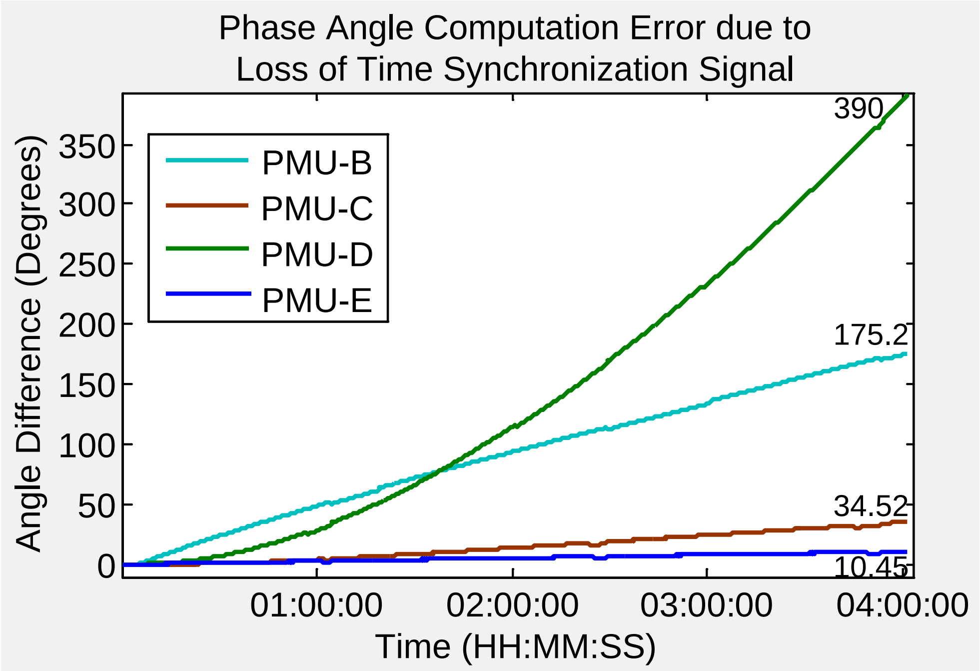
Analyzing archived PDC data

Legend

- Time Sync
- Hardwired
- PMU Stream
- PDC Stream



Phase Angle Computation Error due to Loss of Time Synchronization Signal

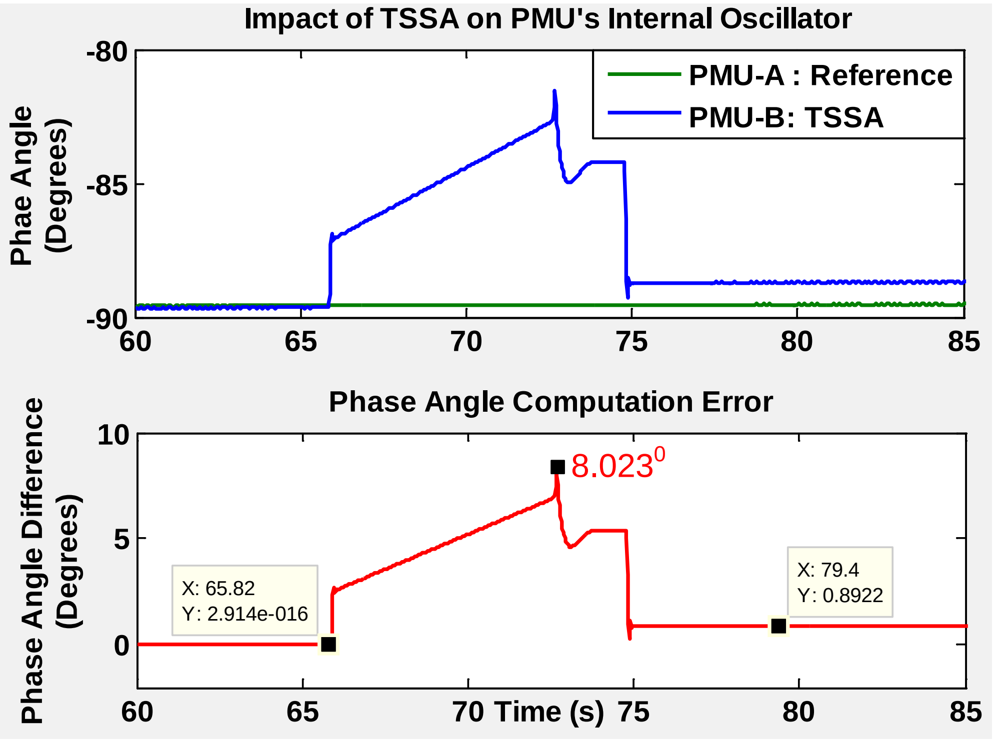


Phase Angle Computation Error due to Loss of Time Synchronization Signal

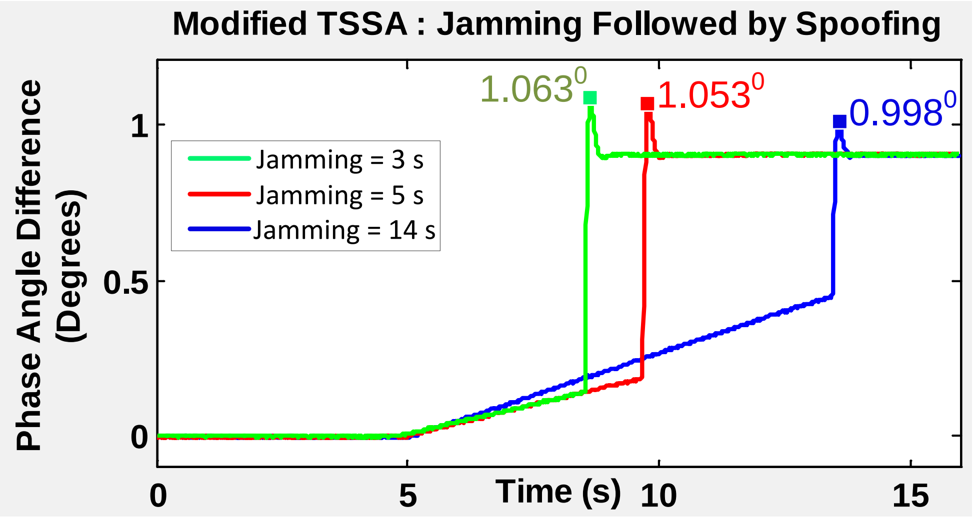
- At t = 00:05:40, the time signal to PMUs (B-E) was disconnected.
- All PMUs exceed 1 % TVE (0.573^0 or 31.8 µs) within 24 min of the loss of time-sync.
- For 4-hour experiment:
  - Max angle diff. error of 390^0 (21.64 ms), PMU-D, and
  - Min angle diff. error of 10.45^0 (0.58 ms), PMU-E.

Internal Clocks & Undetectable Attacks

- **When TSSA is launched instantly:**
  - the internal oscillator takes around 10 s to re-synchronize to the spoofed signal and during this period,
  - the phase angle computation error goes beyond 8^0.
- Such a TSSA is relatively easy to identify as the compromised PMU shows large phase angle deviations for a few seconds.



- Sophisticated/**Undetectable TSSA:**
- Jamming the authentic GPS signals for a given time window and increasing a fixed delay (steps)
  - Internal oscillator of the PMU will undergo smoother transitions to the spoofed signal and
  - Does not result in large phase angle deviations → harder to detect



Conclusions (1/2)

- Loss / Spoofing of time-synchronization signal results in corrupted power system monitoring results, delayed / faulty protection activation, and degradation of WAPOD controls.

- When the GPS signal is lost, the PMUs rely on their local oscillator to compute synchrophasors.
- *Each PMU has a different internal oscillator and therefore results in different phase angle computation error when its external time synchronization signal is lost.*

- When subjected to a TSSA instantly, the internal oscillator of the PMUs needs to resynchronize to the spoofed time synchronization signal which requires additional time.
  - *During this period, the PMUs report a large phase angle computation error, which can result in degradation & mal-operation of the associated monitoring, protection and control applications*

Conclusions (2/2)

To provide a quantitative metric for the TSSA's tolerance level of each application, it is necessary to consider:

- Threshold settings, e.g. phase angle difference to initiate a trip / control action.
  - These thresholds are system dependent and are unique for each application.
- Wide-Area Damping:
  - The change in system topology results in a shift in the mode's frequency and damping, requiring real-time (re)tuning while
  - Changes in time requires adaptive time-delay compensation,
  - Both not typically available in today's controls.
- The maximum tolerance for each application can be calculated using the demonstrated RT-HIL setup and the proposed TSSA methodology.
  - These tolerance levels are system and application dependent and therefore will be different for each case.
- ***Experimental methods and design tools for quantification are needed!***

Application	**Effect**	**Significance**
Phase Angle Monitoring	Misleading information resulting in false control actions either manually or automatic	Major
Anti-Islanding Protection	False activation of protection scheme leading to system separation	Major / Threshold dependent
Oscillation Damping Control	Controller's performance degradation that may result in negative damping injection into the system leading to loss of synchronism	Major / Controller and System dependent

Resources and Main References Related to this Talk

- *Main web:*
  - ALSETLab: http://ALSETLab.com
- *Github source code repositories:*
  - IRIG-B for Real-Time Simulators:
  - https://github.com/ALSETLab/IRIG-B_for_RT
  - Audur: Real-Time Wide-Area Controller
  - https://github.com/ALSETLab/Audur
  - S3DK Toolkit for PMU applications implementation:
  - https://github.com/ALSETLab/S3DK
  - Monitoring App:
  - https://github.com/ALSETLab/S3DK-SynchrophasorDisplay
  - STRONgrid Real-Time Data Mediator:
  - https://github.com/ALSETLab/S3DK-STRONGgrid

Time-Synchronization Spoofing and Jamming:

M. S. Almas, L. Vanfretti, R. S. Singh, and G. M. Jonsdottir, "***Vulnerability of Synchrophasor-based WAMPAC Applications' to Time Synchronization Spoofing***," in IEEE Transactions on Smart Grid , vol.PP, no.99, pp.1-1 doi: 10.1109/TSG.2017.2665461

M. S. Almas, and L. Vanfretti, "***Impact of Time-Synchronization Signal Loss on PMU-based WAMPAC Applications***", IEEE PES GM 2016, July 17-21, Boston, Massachusetts, USA.

R.S. Singh, H. Hooshyar and L. Vanfretti, "***Laboratory Test Set-Up for the Assessment of PMU Time Synchronization Requirements***," IEEE PowerTech 2015, The Netherlands, 2015.

Protection Application:

M. S. Almas and L. Vanfretti, "***RT-HIL Implementation of Hybrid Synchrophasor and GOOSE-based Passive Islanding Schemes***", IEEE Transactions on Power Delivery, Vol. 31, No. 3, pp. 1299-1309.

M.S. Almas, Luigi Vanfretti, **"A method exploiting direct communication between phasor measurement units for power system wide-area protection and control algorithms,"** MethodsX, Volume 4, 2017, Pages 346-359, ISSN 2215-0161.

Control Application:

G.M. Jonsdottir, M.S. Almas, M. Baudette, M.P. Palsson and L. Vanfretti, "RT-HIL Hardware Prototyping of Synchrophasor-and-Active-Load-Based Oscillation Damping Controllers," IEEE PES General Meeting 2016, Boston, MA, USA.

G.M. Jonsdottir, M.S. Almas, M. Baudette, L. Vanfretti, and M.P. Palsson, "RT-SIL Performance Analysis of Synchrophasor-and-Active Load-Based Power System Damping Controllers," IEEE PES GM 2015.

E. Rebello, L. Vanfretti, and M.S. Almas, "Experimental Framework for Testing Synchrophasor-Based Damping Control Systems," 2015 IEEE 15th International Conference on Environment and Electrical Engineering, June 10-13, 2015, Rome.

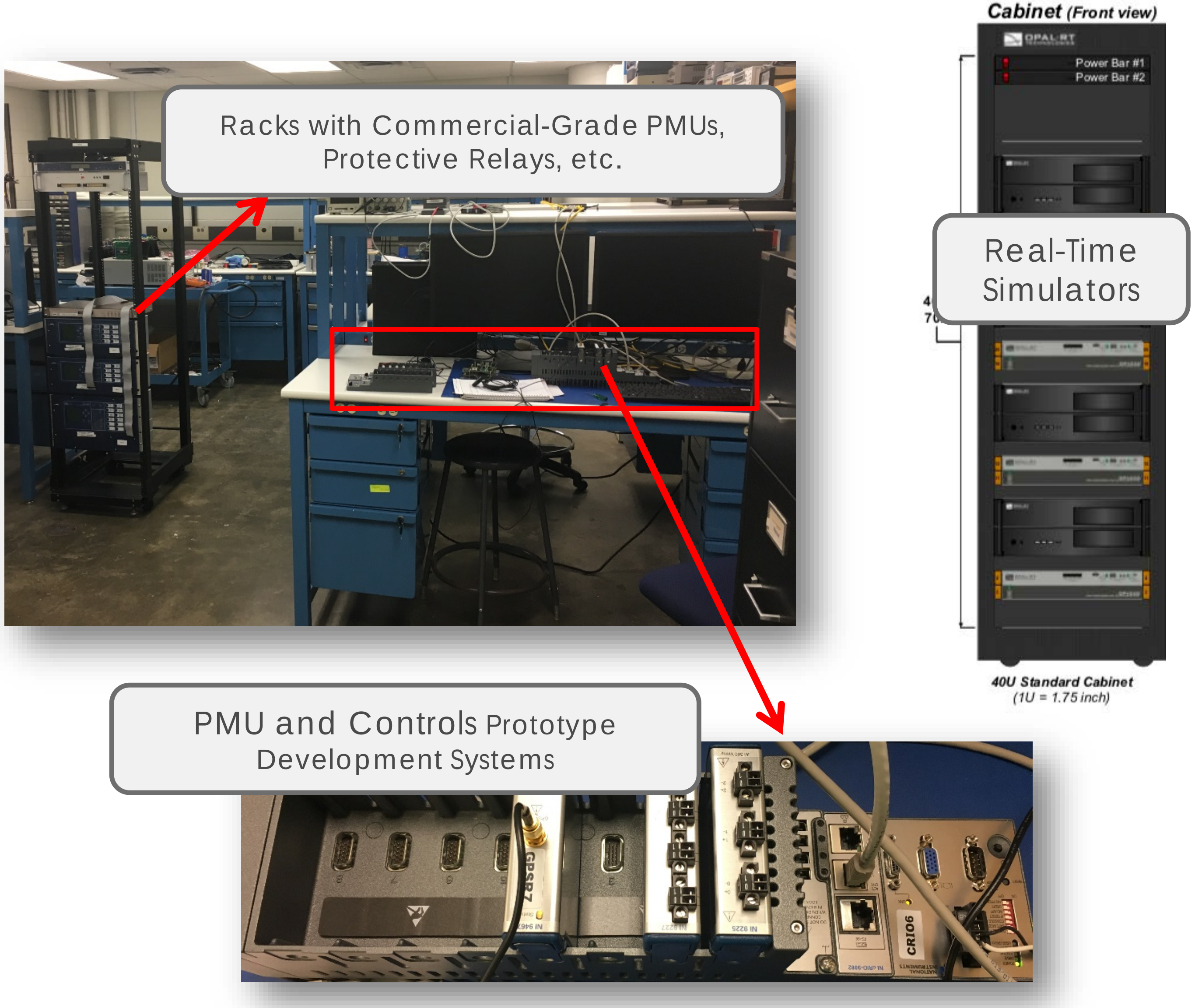
E. Rebello, L. Vanfretti and M.S. Almas, "Software Architecture Development and Implementation of a Synchrophasor-Based Real-Time Oscillation Damping Control System," IEEE PowerTech 2015, The Netherlands, 2015.

Monitoring Application:

M.S. Almas, M. Baudette, L. Vanfretti, S. Løvlund and J.O. Gjerde, "***Synchrophasor Network, Laboratory and Software Applications Developed in the STRONg2rid Project***", IEEE PES GM 2014, Washington DC, USA

Future Work

- We have now started to build a new real-time hardware-in-the-loop simulation lab at RPI for PMU R&D
- **ALSETLab** is being developed to solve real-world grid problems!
  - We want to work with you!
- Lab Development Status:
  - Laboratory space preparation
    - 6 work stations
  - Equipment being shipped.
  - Opal-RT Simulator in production.
  - In operation ~ Summer ’18.



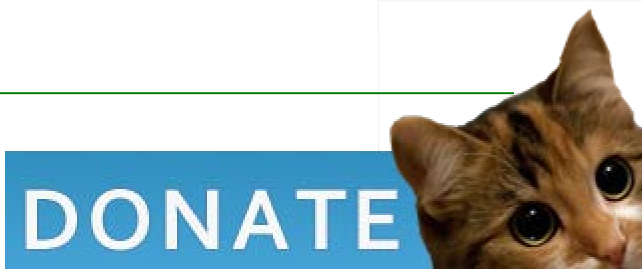
Racks with Commercial-Grade PMUs, Protective Relays, etc.

Real-Time Simulators

PMU and Controls Prototype Development Systems

ALSETLab

Needs your help!



Follow our donors example!

- *Platinum Contributors:*

Dominion Energy® — SEL SCHWEITZER ENGINEERING LABORATORIES

- Gold: GE Global Research
- Silver: N — GitHub