Development and Testing of Wide-Area Protection Applications

KTH ROYAL INSTITUTE OF TECHNOLOGY

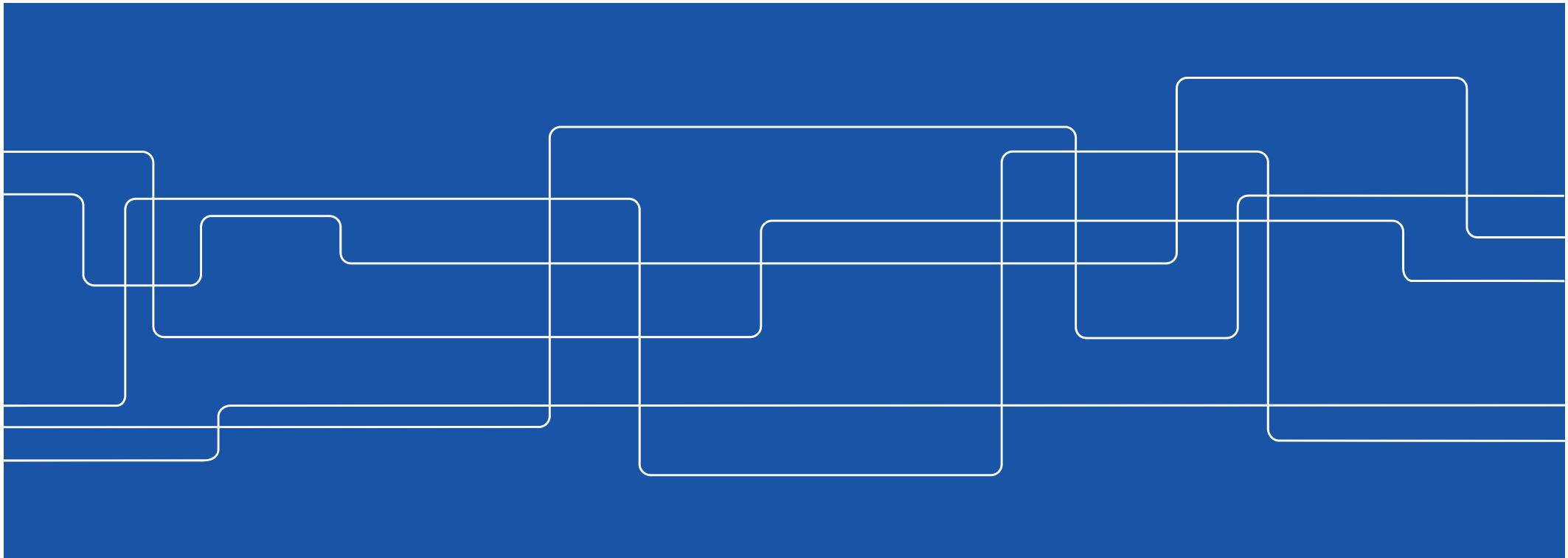
STRONg^{2}rid Project Results

Muhammad Shoaib Almas

PhD. Candidate

SmarTS-Lab Research Group

Department of Electric Power and Energy (EPE)



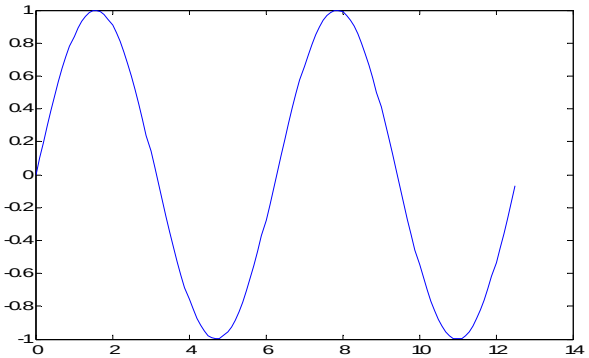
Outline

- PMUs: Smart Grid Enablers
- SmarTS-Lab
- Wide-Area Protection Applications
  - Anti-Islanding Protection
- Future focus
  - Vulnerabilities of WAMPAC Apps
- Conclusion

Enabler of the evolving Smart Grid

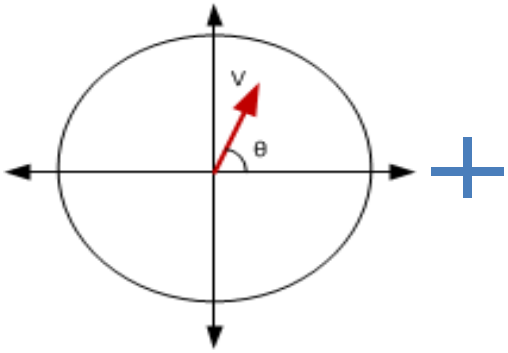
PHASOR MEASUREMENT UNITS (PMUs)

Synchrophasor Fundamentals

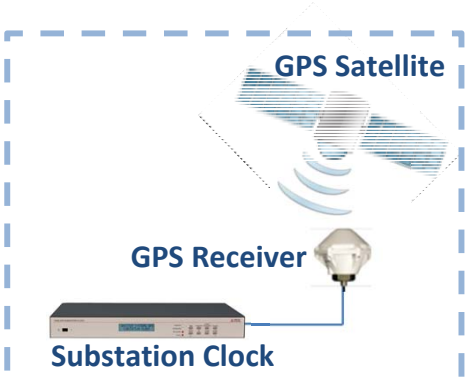


Sinusoidal waveform

Represented as

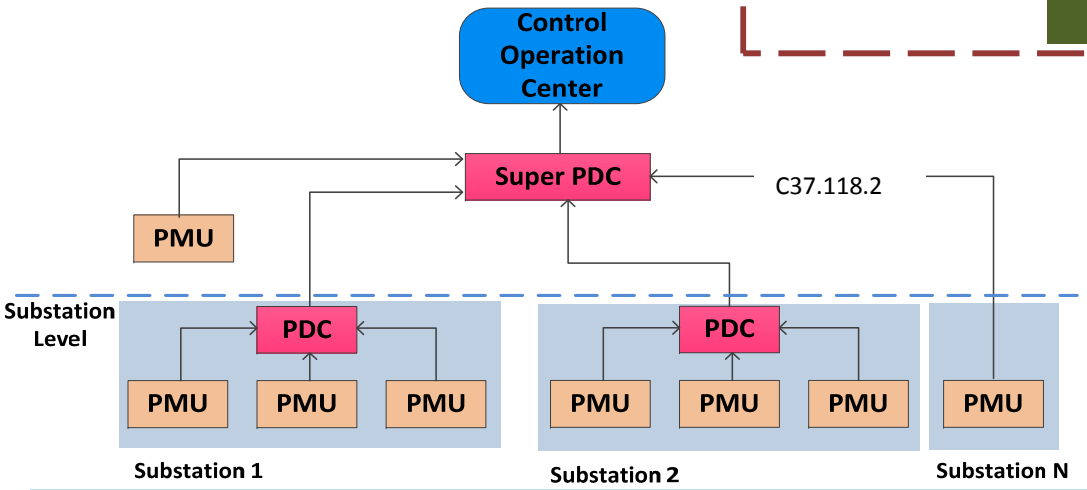


Phasors



Synchronized Time-Tag

Synchrophasors



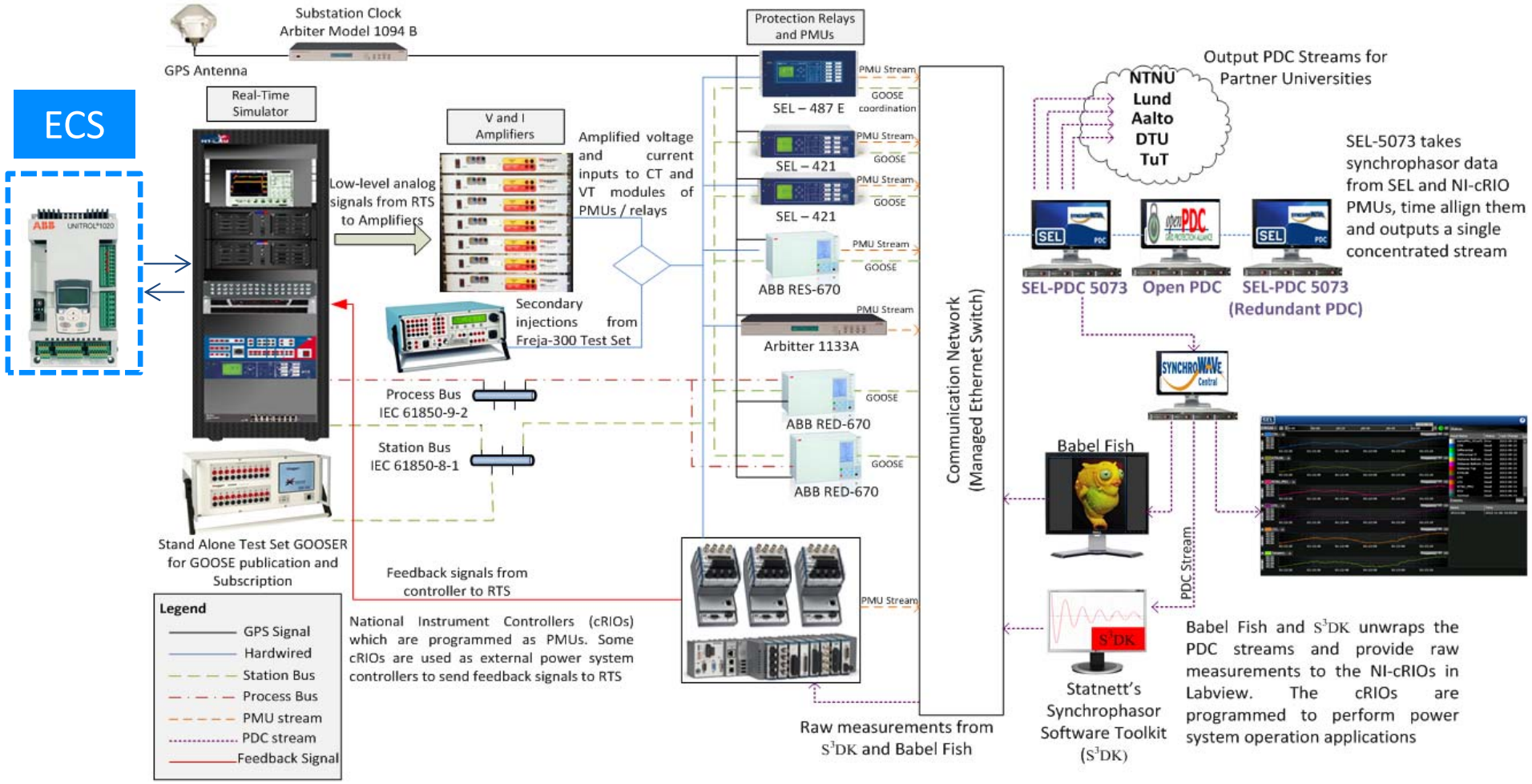
Typical Hierarchical Communication Layout of PMUs and PDCs

- Data rate upto 50 / 60 msgs per sec
- Numerous potential applications like islanding detection, state estimation, early warning systems, model validation, SIPS, RAS, etc

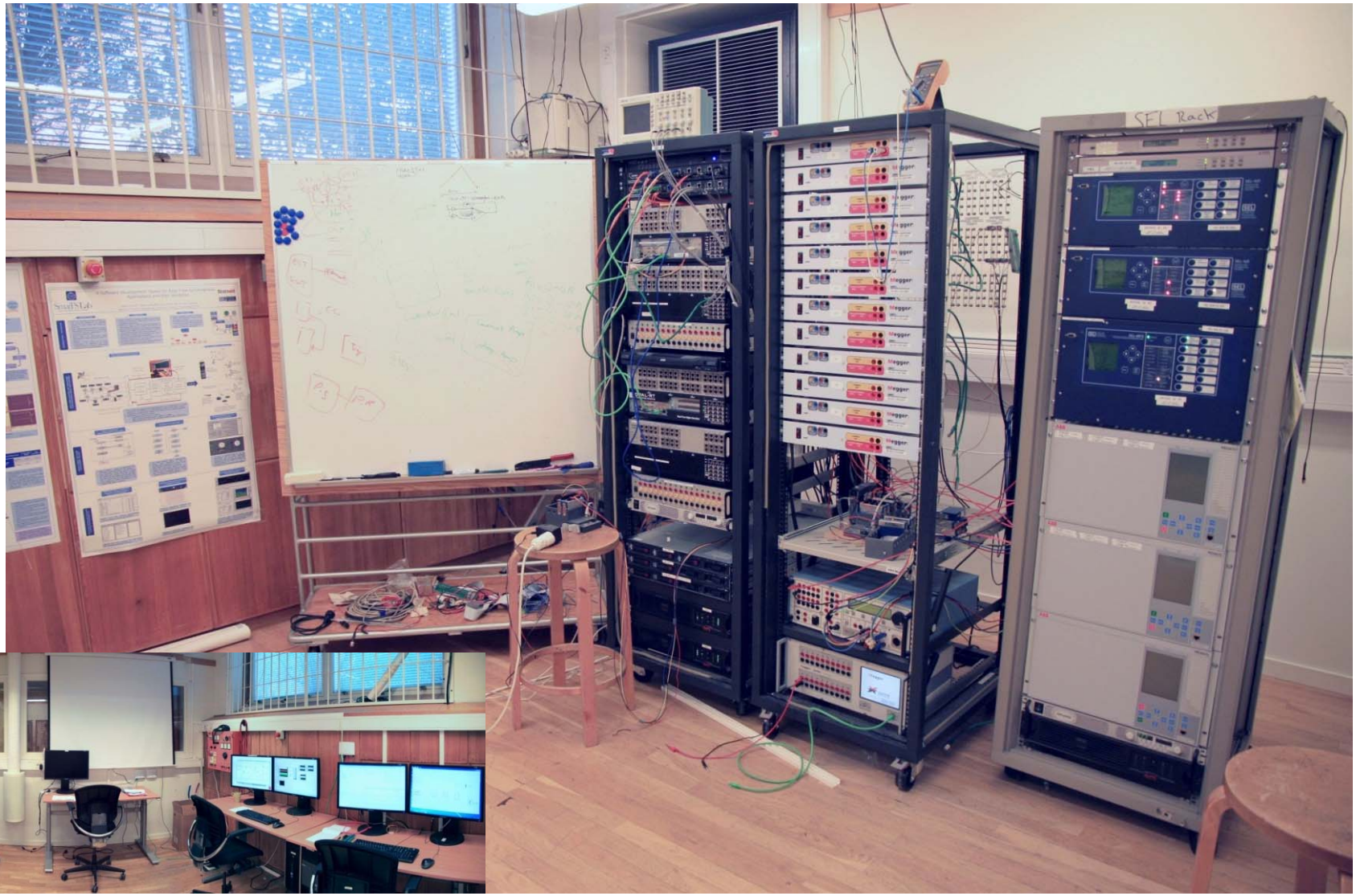
Platform for developing WAMPAC Applications

SMART TRANSMISSION SYSTEM LABORATORY (SmarTS-Lab)

SmarTS Lab Architecture



Our SmarTS Lab Architecture

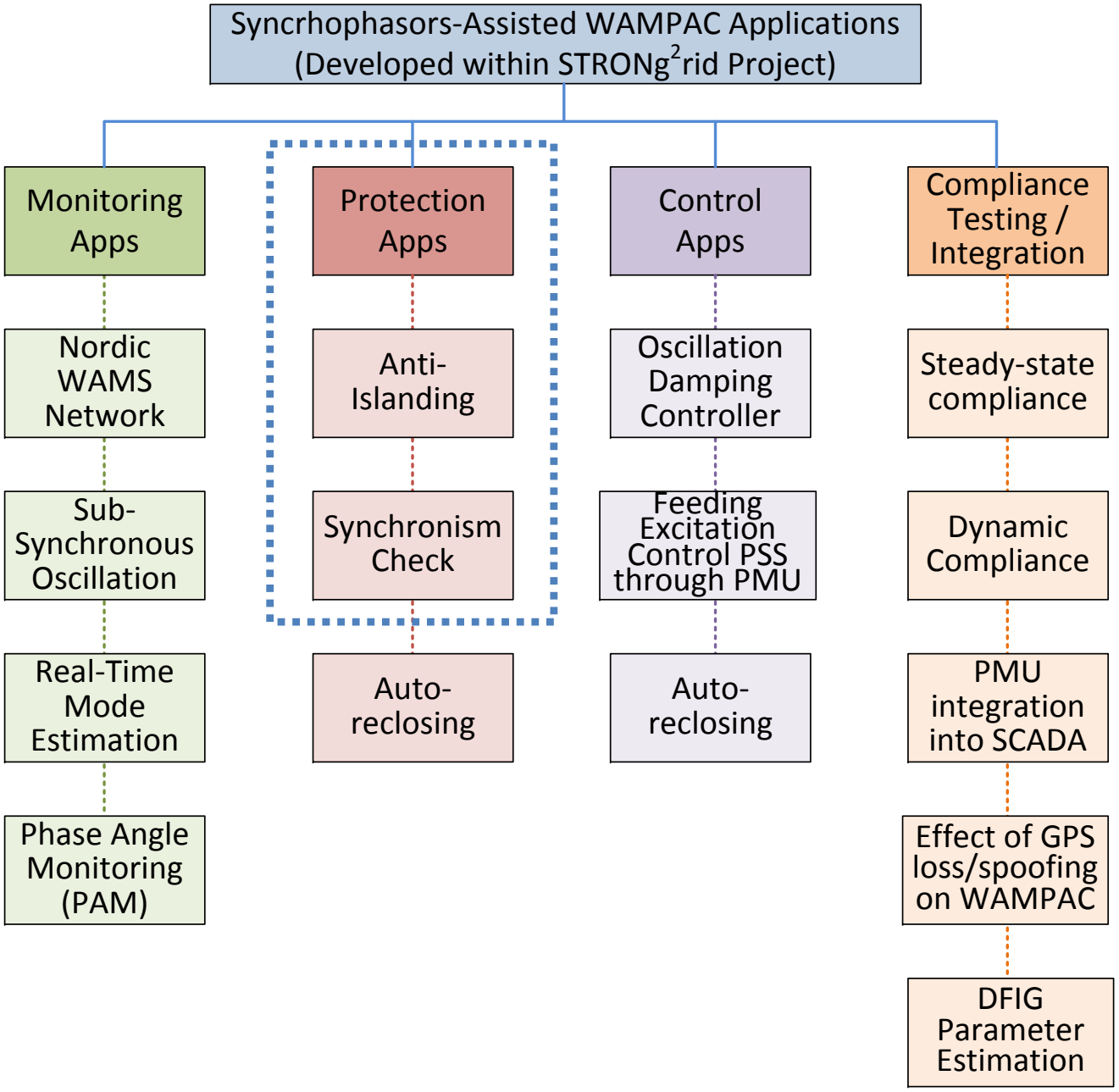


RT-HIL Design and Testing

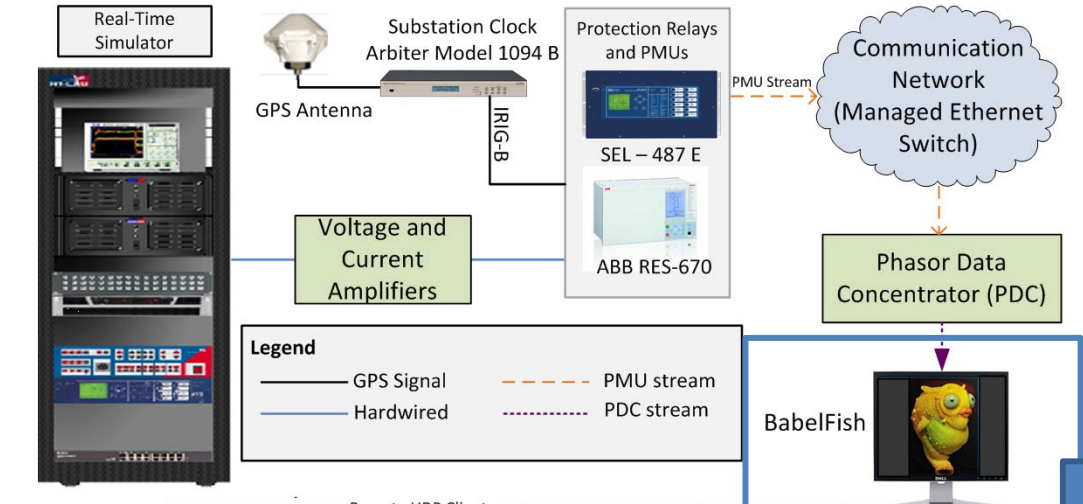
WAMPAC APPLICATIONS

Application developments

- Large number of PMU-assisted WAMPAC applications have been developed within the STRONg^{2}rid project.
- All these applications have been tested using Real-Time Hardware-in-the-loop (RT-HIL) facility at SmarTS-Lab



RT-HIL Setup : Minimum Requirement



Important piece of the puzzle

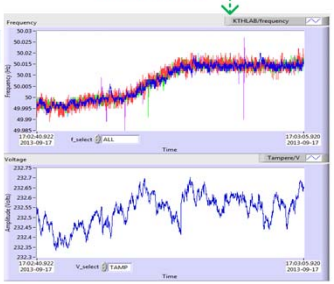
1

Remote UDP clients on different programming platform using user selected synchrophasor data from BF for further data manipulation

2

Selected synchrophasor data being received in National Instrument controllers using UDP for performing power system control applications

3

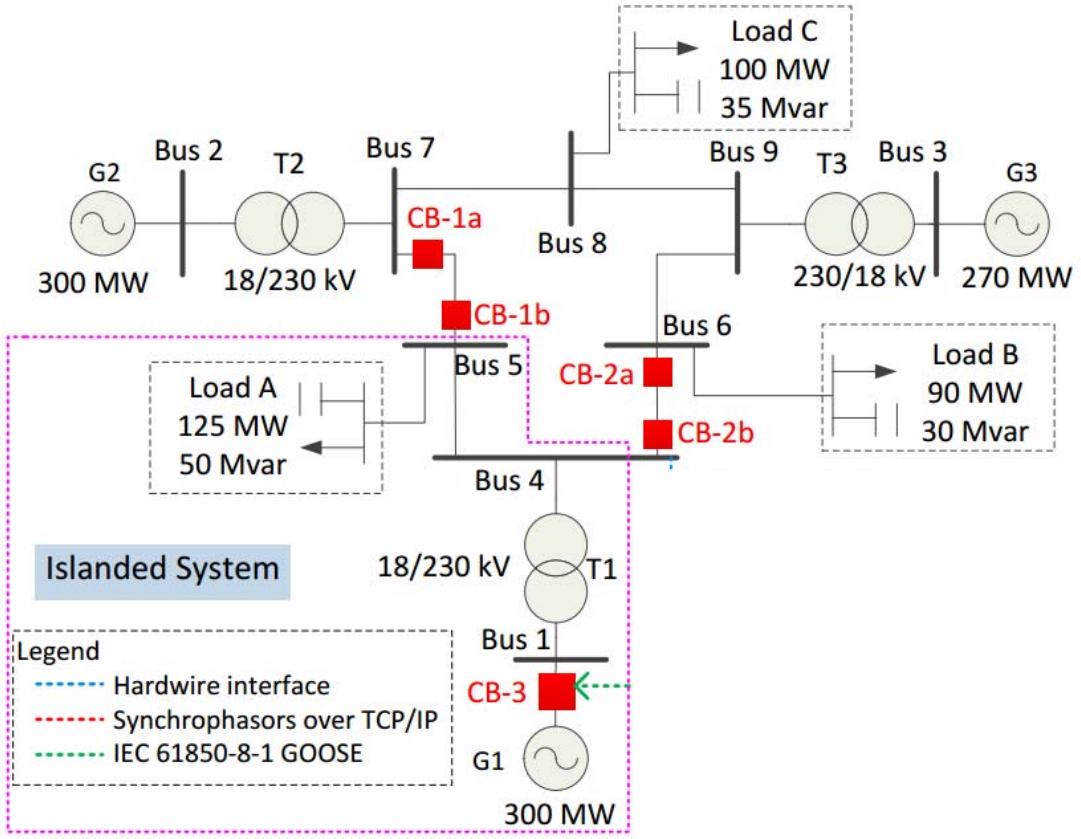


User selected synchrophasor data through BF being used in a power system monitoring application

WIDE AREA PROTECTION APPLICATIONS

- Anti-Islanding Protection

1. Anti-Islanding Protection
(Local and Wide Area Measurements)

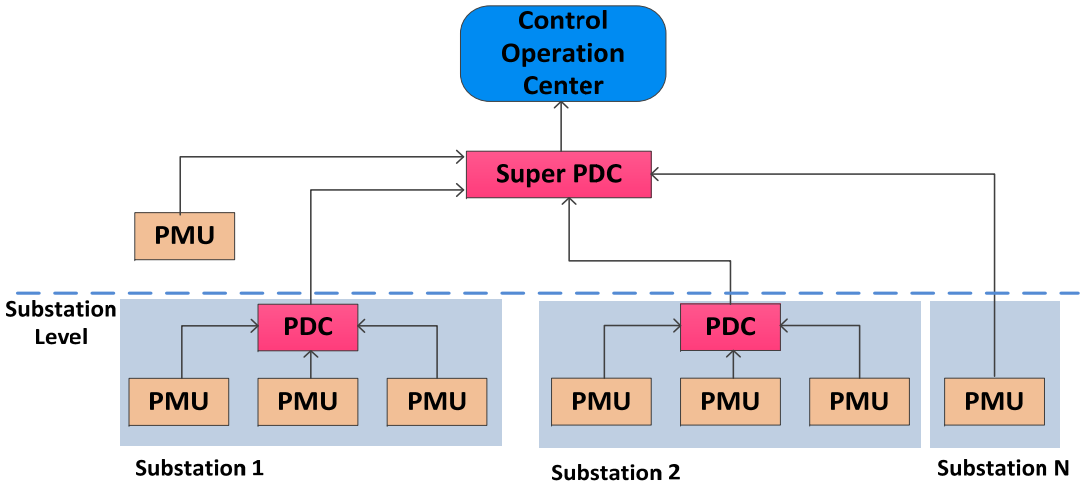


Simulink Model
IEEE 3 Machine, 9 bus System

- IEEE Std. 1547-2008 states that the DG must be disconnected from the isolated grid within **2 seconds** after an unintentional islanding event.
- This maximum delay of 2 seconds includes **islanding detection, trip signal generation, trip signal transfer and breaker opening** for the connected DG.

1. Anti-Islanding Protection
(Local and Wide Area Measurements)

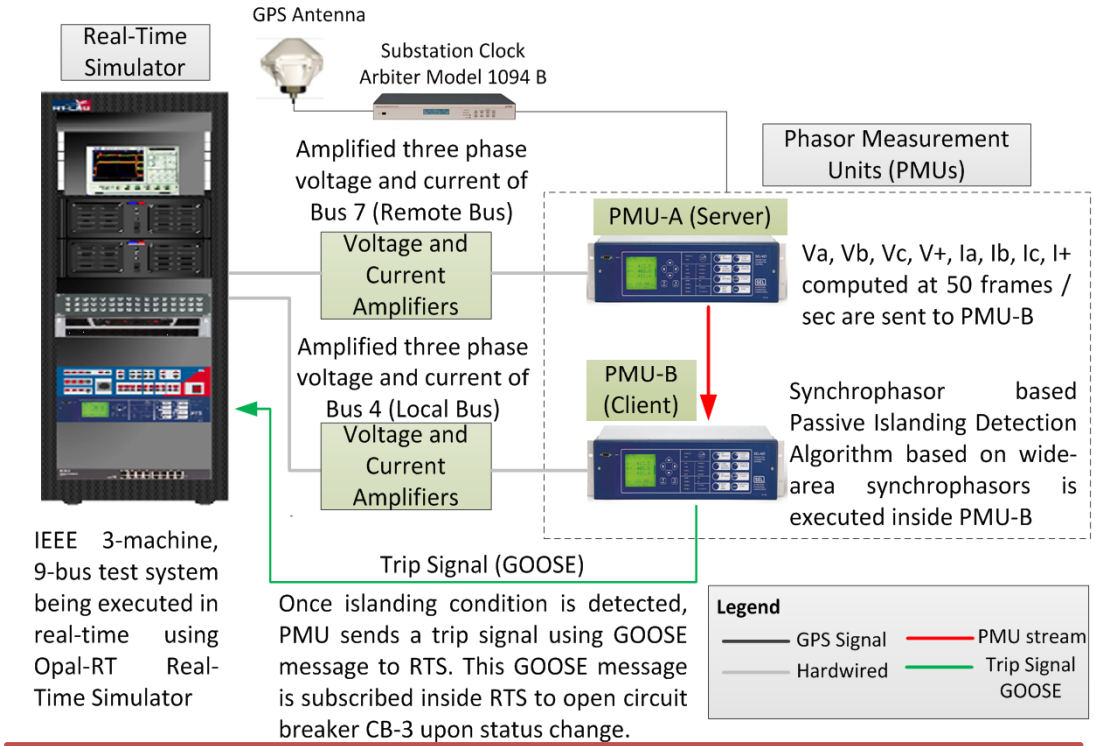
Latencies in PMU-based applications



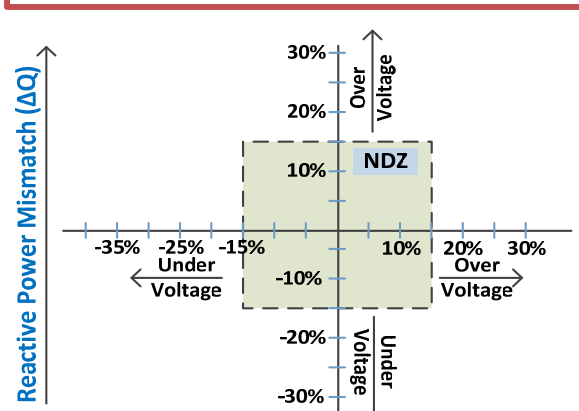
- PMU filtering delay
- Synchrophasor computation delay
- PMU Data Packaging Delay
- Link propogation delay
- Router delay
- PDC delay
- Feedback loop delay

Cause of Delay	Typical Range of Delay
Sampling Window	17 ms to 100 ms
Measurement Filtering	8 ms to 100 ms
PMU processing	0.005 ms to 30 ms
PDC processing Delay	**500 ms to 2 s**
Communication Distance	6 µs / km

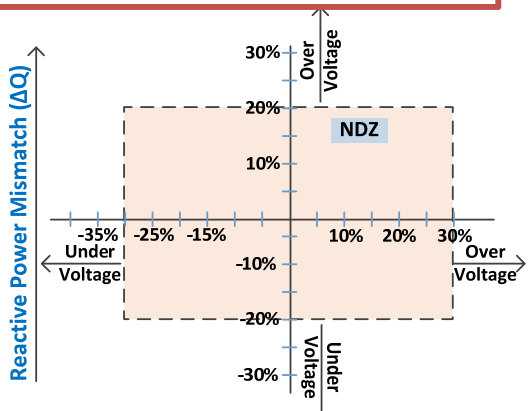
1. Anti-Islanding Protection
(Local and Wide Area Measurements)



NDZ for Local and Wide-area Synchrophasor-based anti-islanding



Wide-Area

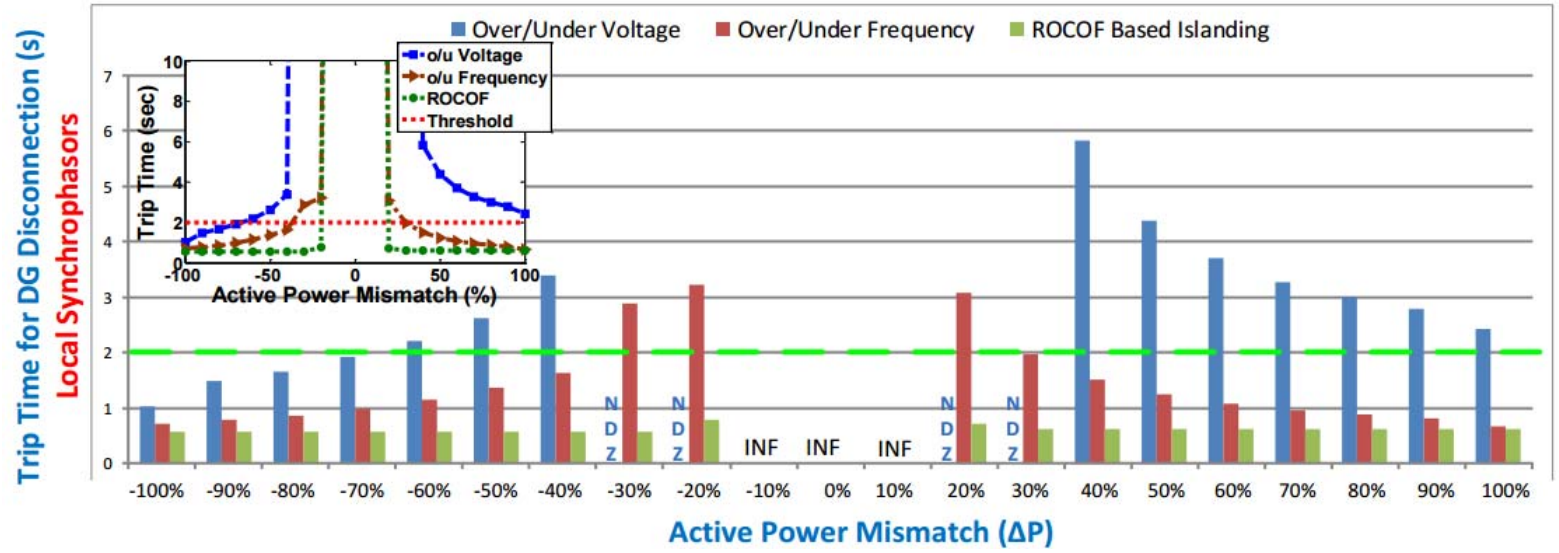


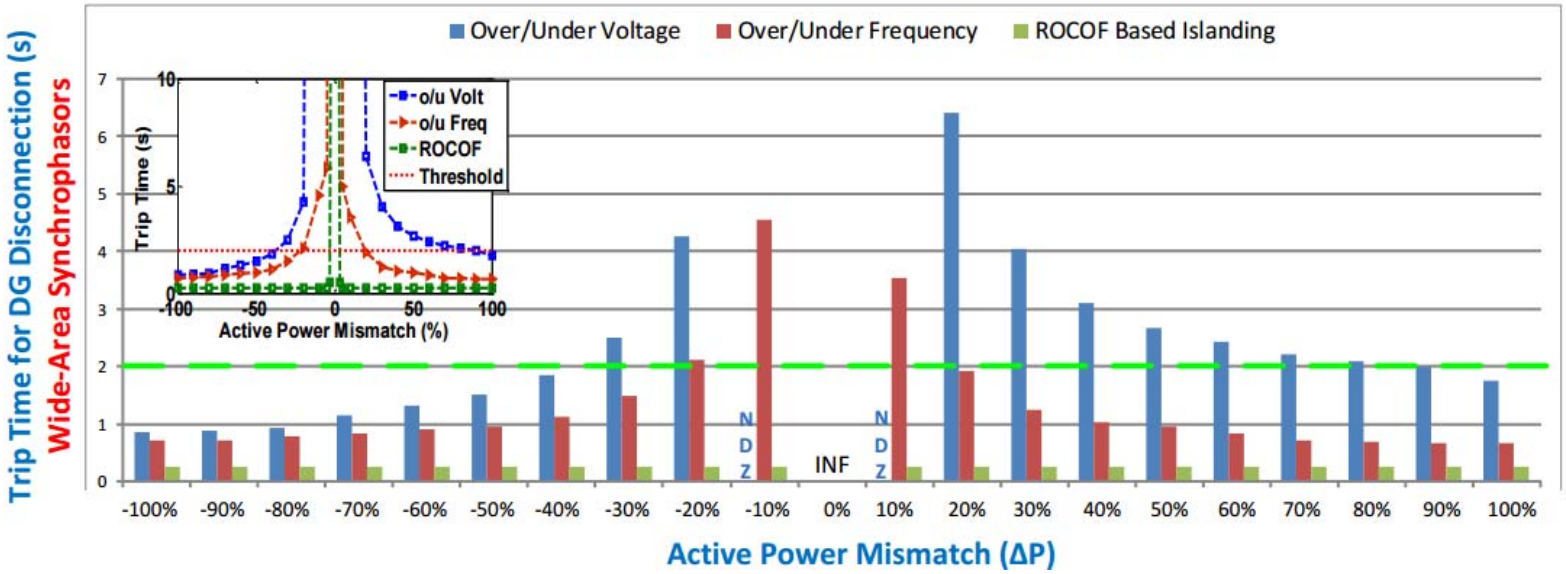
Local

- ROCOF-based schemes are effective for both active and reactive power mismatch, and result in faster operation.
- Wide-area schemes not only perform faster, but also have smaller NDZs

1. Anti-Islanding Protection
(Local and Wide Area Measurements)

If latencies are kept to a minimum, wide-area passive islanding detection schemes reduce the NDZ to half or two-third of the one using local synchrophasors.





Reference: M. S. Almas and L. Vanfretti, "RT-HIL Implementation of Hybrid Synchrophasor and GOOSE-based Passive Islanding Schemes", Accepted for publication in IEEE Transactions on Power Delivery, DOI: 10.1109/TPWRD.2015.2473669

Cybersecurity

VULNERABILITY OF PMU-BASED APPLICATIONS

Cybersecurity : Threats & Challenges

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine.

Official website of the Department of Homeland Security

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME | ABOUT | ICSJWG | INFORMATION PRODUCTS | TRAINING | FAQ

Control Systems
- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

Alert (IR-ALERT-H-16-056-01) More Alerts

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016

Print | Tweet | Send | Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

SUMMARY

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. In addition, there have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors. Public reports indicate that the BlackEnergy (BE) malware was discovered on the companies' computer networks, however it is important to note that the role of BE in this event remains unknown pending further technical analysis.

An interagency team comprised of representatives from the National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Computer Emergency Readiness Team (US-CERT), Department of Energy, Federal Bureau of Investigation, and the North American Electric Reliability Corporation traveled to Ukraine to collaborate and gain more insight. The Ukrainian government worked closely and openly with the U.S. team and shared information to help prevent future cyber-attacks.

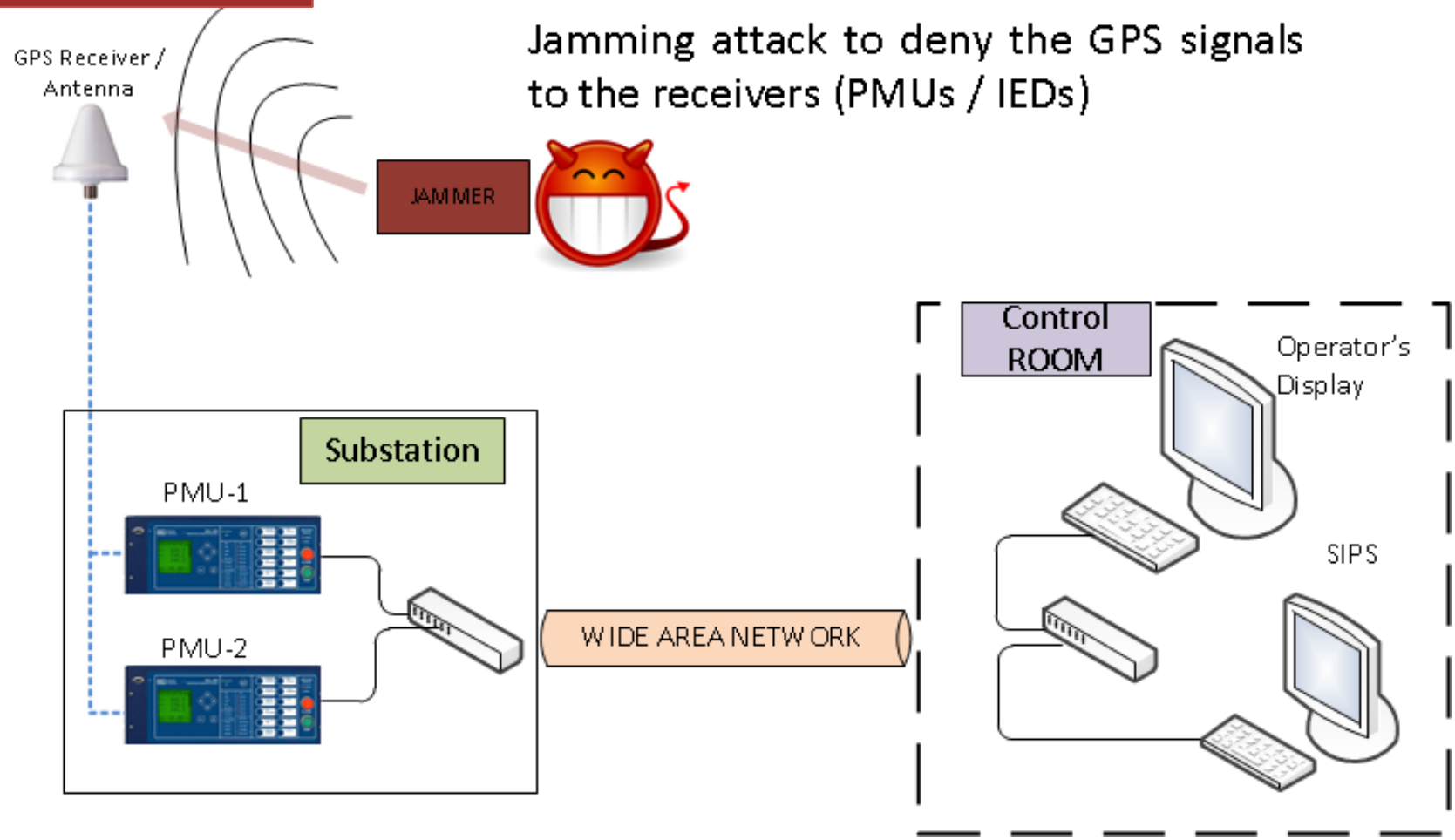
This report provides an account of the events that took place based on interviews with company personnel. This report is being shared for situational awareness and network defense purposes. ICS-CERT strongly encourages organizations across all sectors to review and employ the mitigation strategies listed below.

Additional information on this incident including technical indicators can be found in the TLP GREEN alert (IR-ALERT-H-16-043-01P and subsequent updates) that was released to the US-CERT secure portal. US critical infrastructure asset owners and operators can request access to this information by emailing ics-cert@hq.dhs.gov.

Reference: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

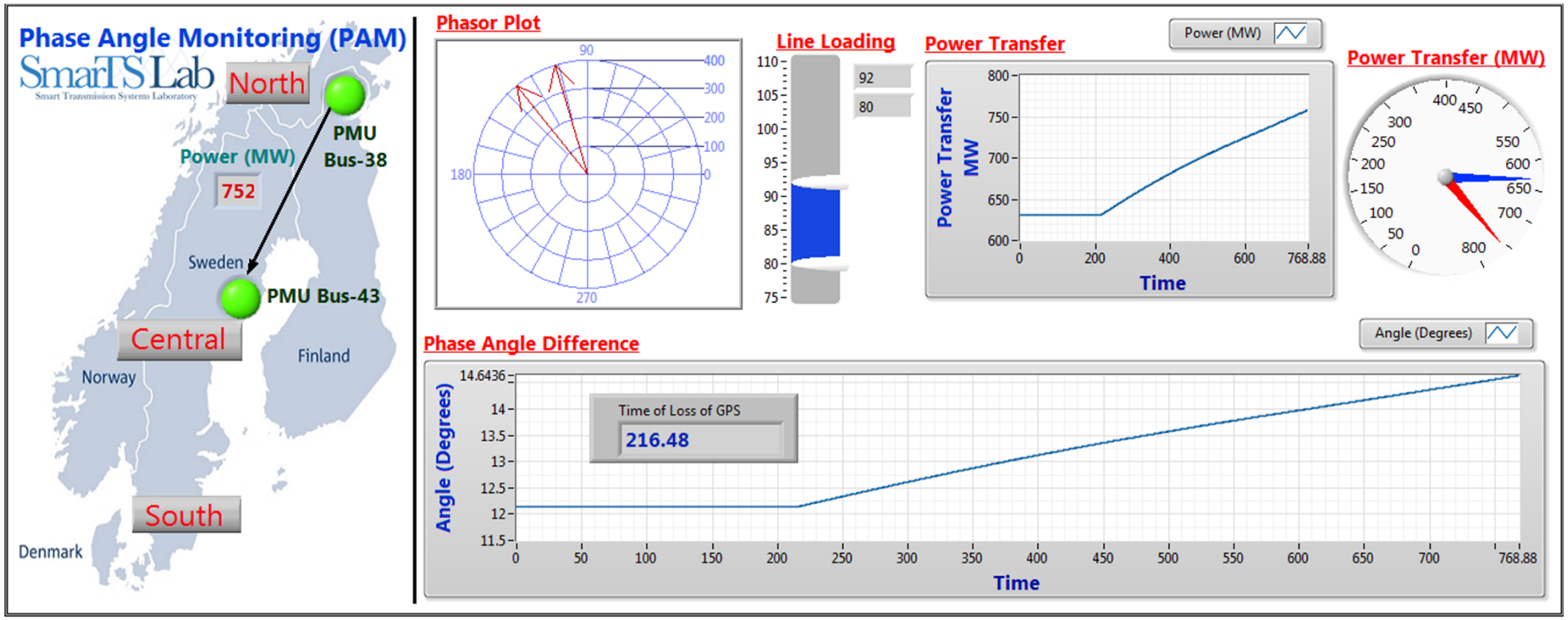
PMU Vulnerabilities

GPS Spoofing/Jamming



Impact of ~~Time-Synchronization Signal Loss~~ (Jamming) on WAMPAC Applications

Phase Angle Monitoring (PAM) application



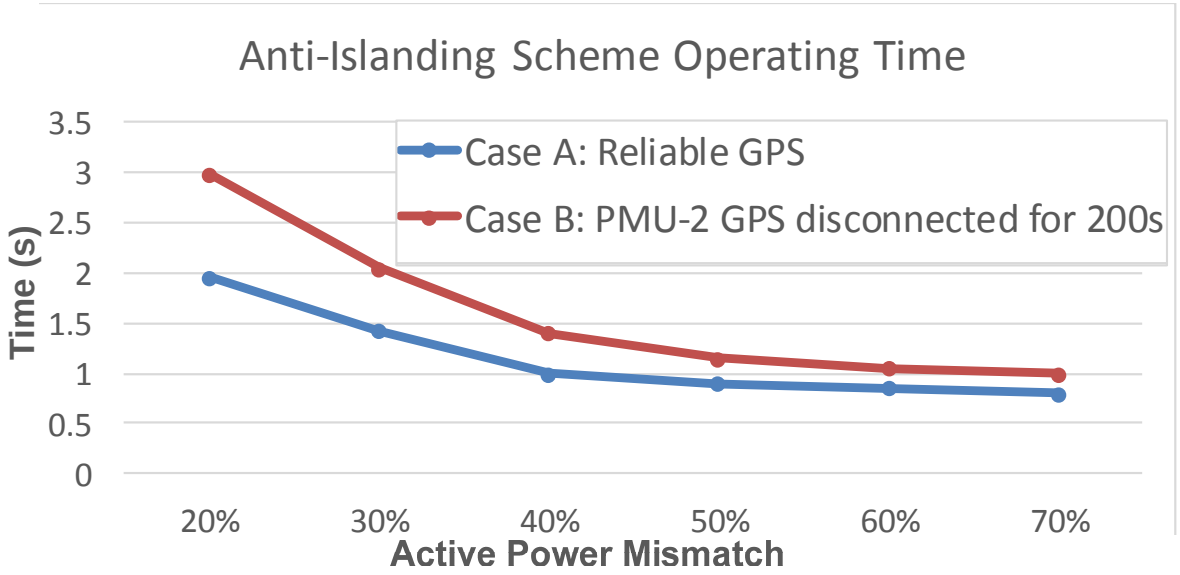
GPS Jamming resulted in

- Erroneous increase in line loading from 80% to 92 %
- Increase from 625 MW to 752 MW.
- Changes occurred within a span of 550 s once the jamming is launched

Impact of ~~Time-Synchronization Signal Loss~~ (Jamming) on WAMPAC Applications

Passive Anti-Islanding Protection

Due to jamming, the protection operation time has increased by 1.022 s for 20 % active power mismatch and 0.62 s for 30 % active power mismatch.



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

Conclusions/Recommendations

Conclusion

- Demonstrated the utilization of synchrophasor measurements for developing Wide-Area Protection Applications.
  - Wide area measurements can decrease the tripping time and reduce the Non Detection Zone (NDZ) for the scheme
- The test-bench demonstrated is useful for a myriad of applications in which simulation exercises in power system CAD software provides no realistic insight into the practical design and implementation challenges
- Real-Time QoS requirements (end-to-end delay) needs to be addressed for each type of WAMPAC applications
- A protocol parser is required to translate / unwrap legacy protocols into raw measurements.
- With more automation and dependence on IT infrastructure, cyber-security threats are a real concern.

Acknowledgements

- The work presented here is a result of the collaboration between iITC, KTH SmarTS Lab (Sweden), Statnett SF (Norway)
- This work has been financed by:
  - Statnett SF, the Norwegian transmission system operator, through its Smart Operation R&D program.
  - The Nordic Energy Research through the STRONg^{2}rid project.

Statnett norden Nordic Energy Research Sustainable Energy Systems 2050

- KTH SmarTS Lab: Luigi Vanfretti, M. Shoaib Almas, Maxime Baudette, Gudrun Jonsdottir, Eldrich Rebello

- Statnett SF: Stig Løvlund, Jan O. Gjerde, Luigi Vanfretti

Statnett

Thank you!

- Questions?
- http://www.kth.se/en/ees/omskolan/organisation/avdelningar/eps/research/smarttslab
- http://www.vanfretti.com
- luigiv@kth.se
- msalmas@kth.se

The scientific man does not aim at an immediate result. He does not expect that his advanced ideas will be readily taken up. His work is like that of the planter - for the future. His duty is to lay the foundation for those who are to come, and point the way. (*Nikola Tesla*)

SmarTS Lab
Smart Transmission Systems Laboratory