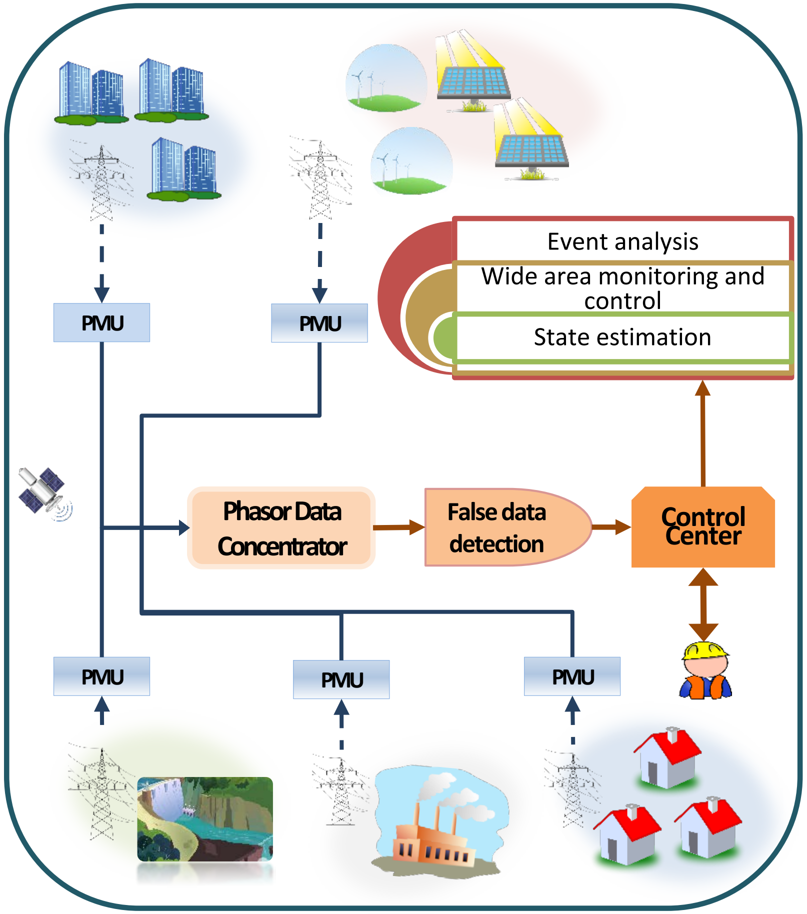
Securing Smart Power Grids under Data Measurement Cyber Threats

Challenges:

- Existing means for real-time power system monitoring and control, such as Phasor Measurement Units (PMU) are vulnerable to various types of cyber-attacks. However, the extent of the impact of cyber-attacks on power systems are unknown.
- Malicious PMU false data injections cannot be detected by existing bad data detection methodologies.
- The existing grid mitigation solutions do not take dependencies between the cyber and physical layers into consideration.

Solution:

- Estimate the impact severity of coordinated cyber-physical attacks on both the cyber and physical layers.
- Use efficient machine learning methodologies to detect anomalies in PMU data and identify vulnerable measurements.
- Develop a dynamic cascading failure model that is adaptive to real-time operating conditions and predicts impending failures following an attack.
- Develop effective mitigation strategies, e.g. controlled islanding against cyber attacks on PMUs.



NSF Grant No. 1600058.

Sara Eftekharnejad, PI, *Syracuse University*
Brian K. Johnson, James Alves-Foss,
University of Idaho

Scientific Impact:

- Quantification of the false data injection impacts in terms of causing cascading failures.
- Developing new anomaly detection techniques using PMU time-series data.
- Developing new methodologies to predict the failure probability of each power system component under real-time operating conditions.
- Developing possible countermeasures to mitigate successful cyber attacks on PMU measurements and prevent cascading blackouts.

Broader Impact:

- This work increases the reliability and resiliency of the power grids against cyber attacks, and leads to a more secure electricity delivery infrastructure.
- The results of this study has been integrated into courses at both institutions.
- The results of this project have been disseminated in multiple conferences and peer-reviewed journals.
- Broad participation of undergraduate students in research