Jianhui Wang
Argonne National Laboratory

A Resilient Self-Healing Cyber Security Framework for Power Grid

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

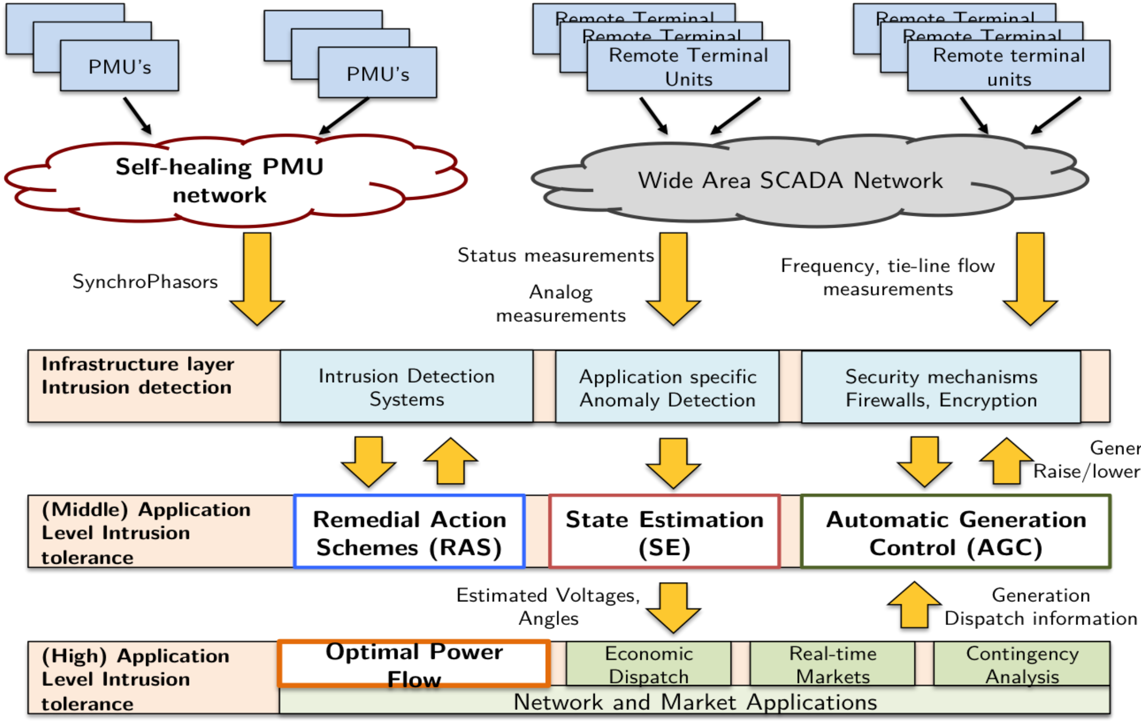
Summary

Objective

To develop an attack-resilient Wide-Area Monitoring, Protection, and Control (WAMPAC) framework, with associated computational algorithms and software tools, to prevent and mitigate cyber-attacks and achieve resilience of the bulk power system.

Schedule

- March 2015 – Feb 2017



PMU's

PMU's

Self-healing PMU network

Remote Terminal

Remote Terminal

Remote Terminal Units

Remote Terminal

Remote Terminal

Remote terminal units

Wide Area SCADA Network

SynchroPhasors

Status measurements

Analog measurements

Frequency, tie-line flow measurements

Infrastructure layer Intrusion detection

Intrusion Detection Systems

Application specific Anomaly Detection

Security mechanisms Firewalls, Encryption

Gener

Raise/lower

(Middle) Application Level Intrusion tolerance

Remedial Action Schemes (RAS)

State Estimation (SE)

Automatic Generation Control (AGC)

Estimated Voltages, Angles

Generation Dispatch information

(High) Application Level Intrusion tolerance

Optimal Power Flow

Economic Dispatch

Real-time Markets

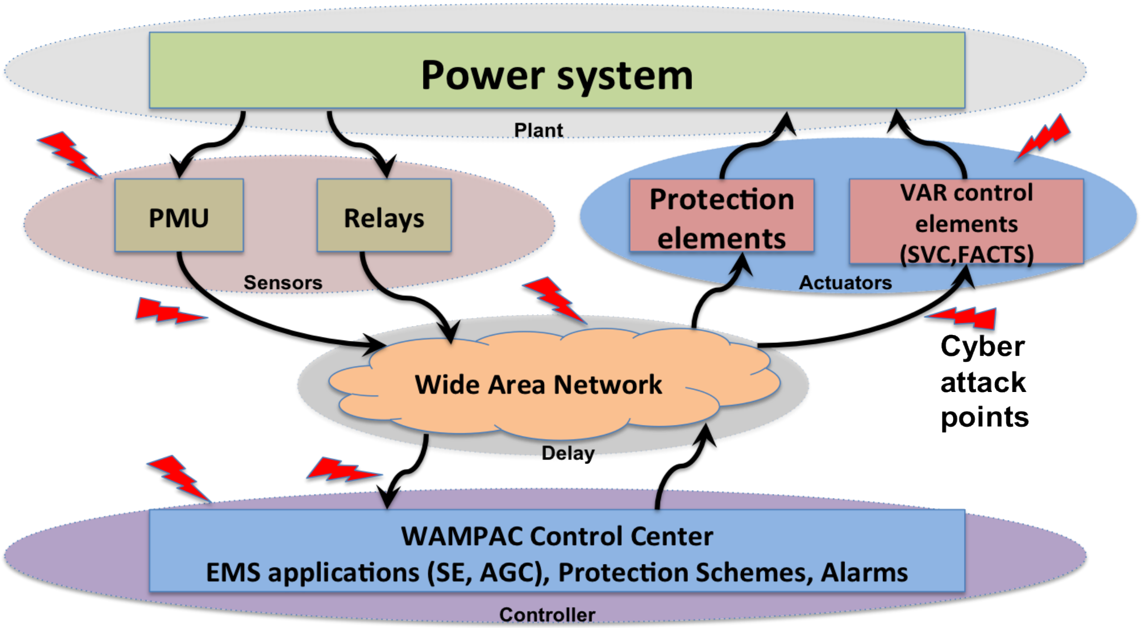
Contingency Analysis

Network and Market Applications

Performer:	**Argonne National Laboratory**
Partners:	**Pacific Northwest National Laboratory, Iowa State University, Illinois Institute of Technology**
Federal Cost:	**$2,000,000**
Cost Share:	**N/A**
Total Value of Award:	**$2,000,000**
Funds Expended to Date:	**80%**

Advancing the State of the Art (SOA)

- Most of the existing research only focuses on the intrusion detection at the network level and is not able to correlate network events with anomalies founded in the application layer.
- The goal of the proposed research is to develop an attack-resilient WAMPAC framework and associated algorithms to secure the bulk power system against cyber-attacks, including HILF malicious cyber events.
- In addition to the stated research objectives, design, implementation, and experimental validation of the algorithms are integral parts of the project.



Report on A Resilient Self-Healing Cyber Security Framework for Power Grid

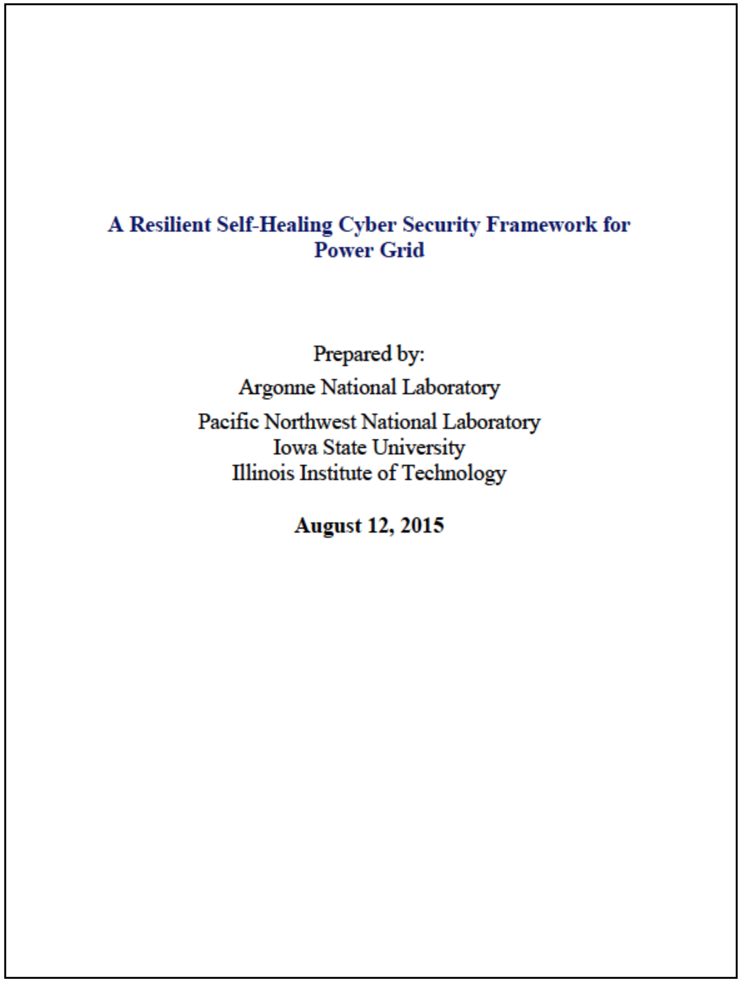
The industry advisory board (IAB) was established on May 9, 2015 including the following members:

- Jay Giri, GE/Alstom Grid
- Annabelle Lee, EPRI
- Scott Mix, NERC
- Melanie Seader, EEI
- Jianzhong Tong, PJM

Regular IAB meetings and webinars, technical review and advice, etc.

Some comments from IAB members:

- *"…an important initiative for the industry."*
- *"This is an excellent proposal with interesting ideas."*



A Resilient Self-Healing Cyber Security Framework for Power Grid

Prepared by:

Argonne National Laboratory

Pacific Northwest National Laboratory
Iowa State University
Illinois Institute of Technology

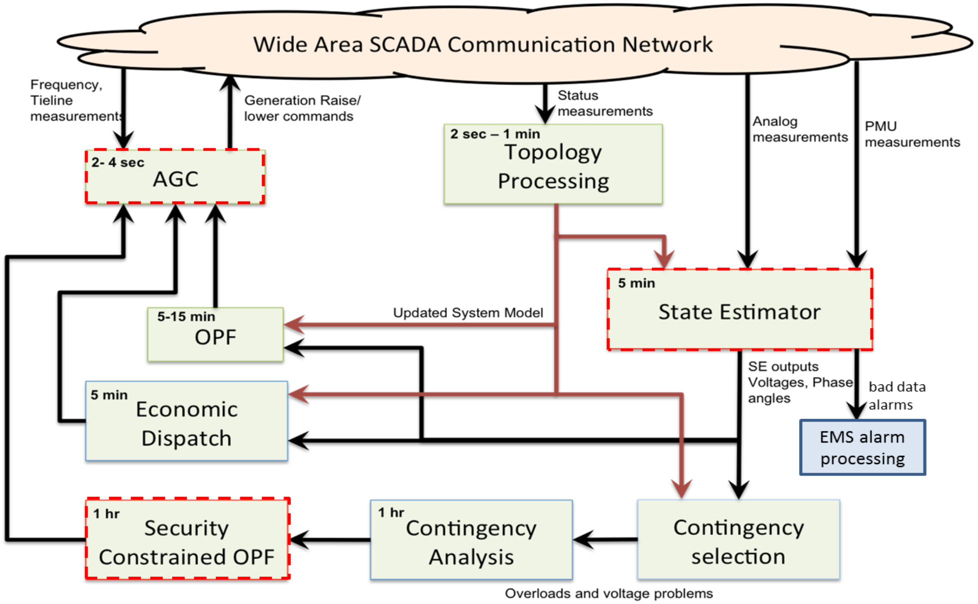
August 12, 2015

Progress to Date

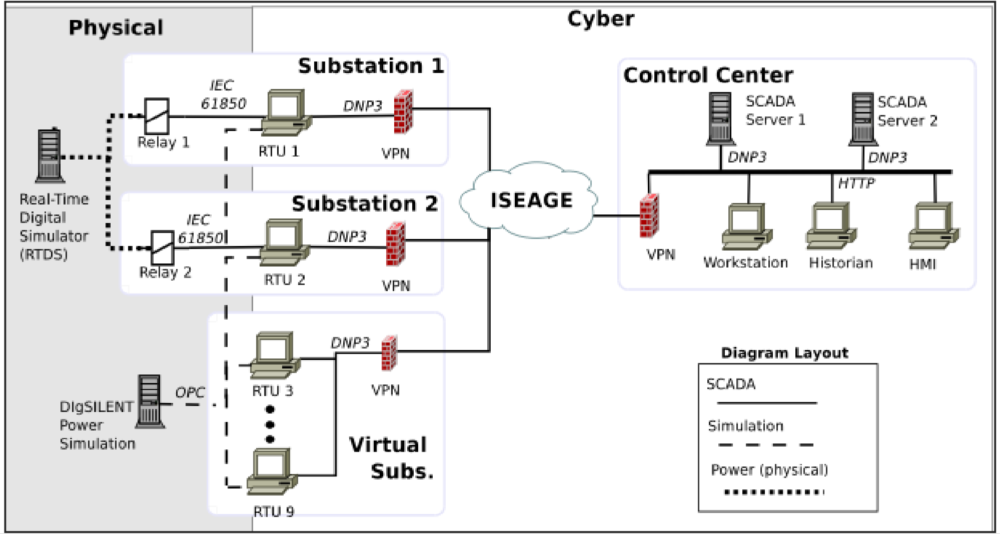
Major Tasks Accomplished

- Attack-resilient WAMPAC architecture
  - SDN-based self-healing PMU communication network
- Attack-resilient State Estimation
  - Extensive tests on PJM 15451-bus system show superior performance even in the case of multiple non-interacting bad data injection
- Attack-resilient AGC
  - Create a federated testbed environment using PowerNET (PNNL) and PowerCyber (ISU) for attack-defense experimentation on Wide-Area Control application (Automatic Generation Control).
- Attack-resilient Protection Scheme
  - Stealthy coordinated attack vectors on Remedial Action Scheme (RAS) and multi-agent based attack-resilient RAS
- Attack-resilient SCOPF
  - Tests on a 2869-bus PEGASE system

Fundamental WAMPAC Applications and Their Time Scales



Iowa State University PowerCyber Testbed for Smart Grid



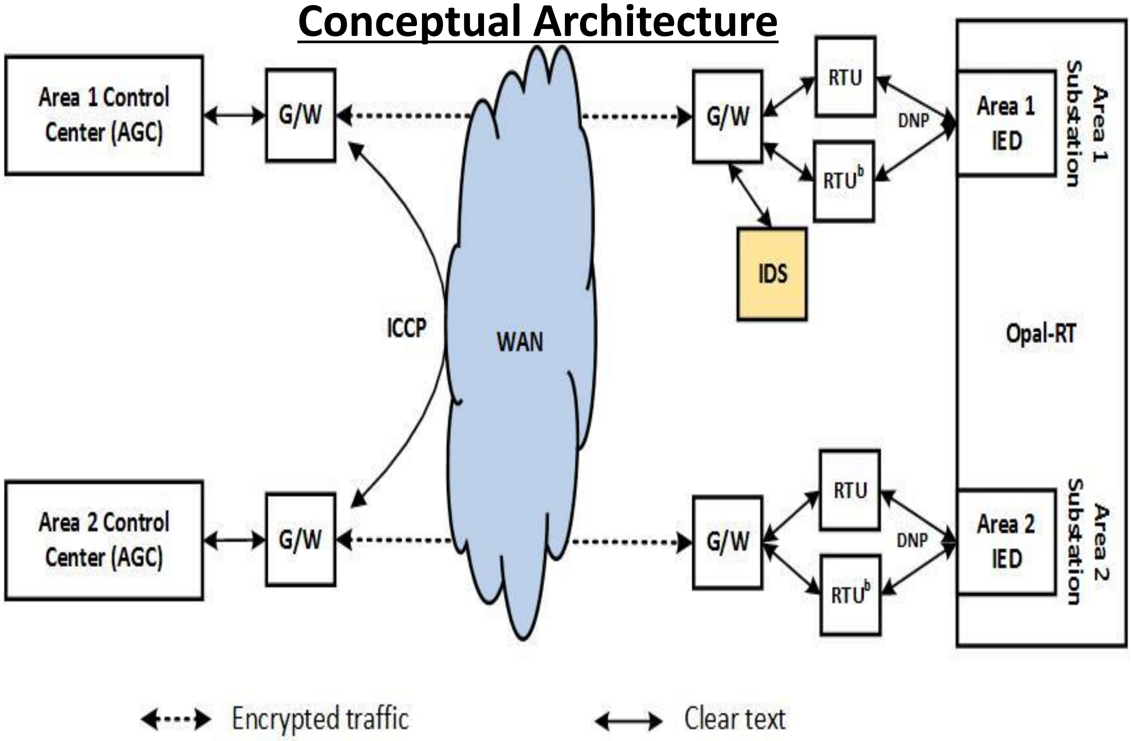
Progress to Date and Next Steps

Next Steps

- Continued development of the attack-resilient wide-area control research with new extensions being added for attack-resilient generator controls.

- Developing a federated capability for cyber-physical testing that uses PNNL's PowerNet and Iowa State University's CyberPower testbeds.
  - Proof of concept link was established between the two testbeds in Sept. 2016.

Conceptual Architecture



Experiment Details

- **Power system modeling – PowerNET**
  - IEEE 39-bus system implemented in OPAL-RT
  - Multiple areas – Control Centers, RTUs in PowerCyber
- **Cyber (SCADA) modeling – PowerCyber**
  - Substation RTU to Control Center using DNP3
  - Control Center interaction using ICCP
  - RTU <–> Control Center - encrypted channel through VPN
- **Attack scenarios**
  - Substation RTU host compromised
  - DoS attacks on substation network
  - Data integrity attacks inside substation network

Challenges to Success

Challenges:

- PMU deployment and applications
- Industry adoption and openness

Outreach and Collaboration

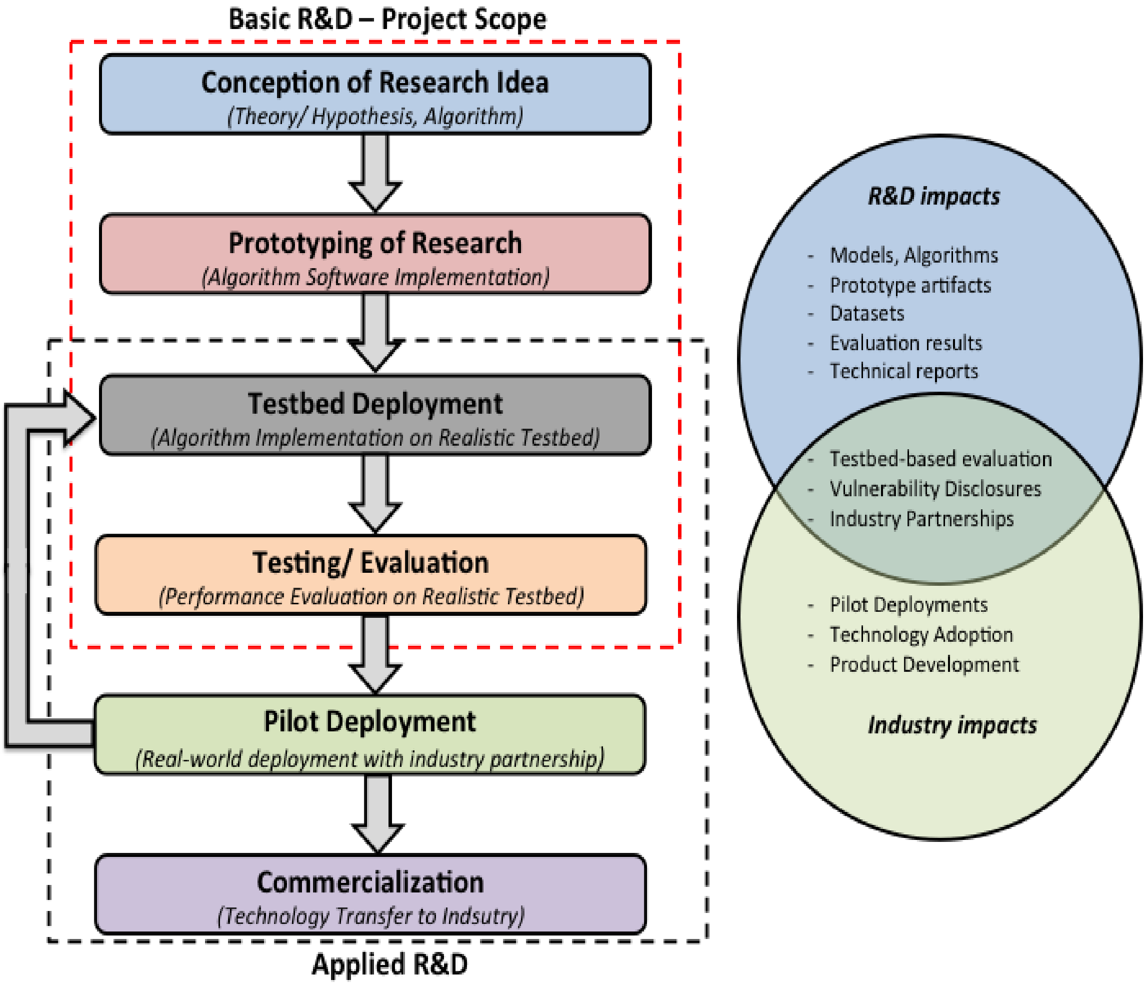
- Organize industry short courses on cyber security (e.g., NERC GridSecCon 2016 Cybersecurity training session)
- Organize/participate in panel sessions on cyber security in professional conferences
- Journal and conference publications
- Enhanced collaboration with industry:
  - ABB-led new CEDS industry call project on Cyber Attack Resilient HVDC System
  - ISU-led new CEDS industry call project on Autonomous Tools for Attack Surface Reduction

Publications

1) A. Taha, J. Qi, J. Wang, J. Panchal, Risk Mitigation for Dynamic State Estimation Against Cyber Attacks and Unknown Inputs, *IEEE Transactions on Smart Grid*, in press.
2) H. Lin, C. Chen, J. Wang, J. Qi, D. Jin, “Self-Healing Attack-Resilient PMU Network for Power System Operation”, *IEEE Transactions on Smart Grid*, in press, 2016
3) A. Ashok, Pengyuan Wang, M. Brown and M. Govindarasu, "Experimental evaluation of cyber attacks on Automatic Generation Control using a CPS Security Testbed," *Power & Energy Society General Meeting*, 2015 IEEE, Denver, CO, 2015, pp. 1-5.
4) A. Ashok, S. Sridhar, D. McKinnon, P. Wang and M. Govindarasu, “Testbed-based Performance Evaluation of Attack Resilient Control for AGC,” August 2016. **Best paper award at Resilience Week 2016.**
5) X. Liu, X. Liu, and Z. Li, “Cyber Risk Assessment of Transmission Lines in Smart Grids,” *Energies*, vol.8, no.12, pp.13796-13810, Dec. 2015
6) X. Liu and Z. Li, “Local Topology Attacks in Smart Grids,” *IEEE Transactions on Smart Grid*, in press.
7) X. Liu and Z. Li, “False Data Attacks against AC State Estimation with Incomplete Network Information,” *IEEE Transactions on Smart Grid*, in press.
8) X. Liu, Z. Li, and Zuyi Li, “Masking Transmission Line Outages via False Data Injection Attacks,” *IEEE Transactions on Information Forensics & Security*,in press.
9) Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, “Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems”, *IEEE Transactions on Smart Grid*, in press.
10) Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, “Analyzing Locally Coordinated Cyber-Physical Attacks for Undetectable Line Outages”, *IEEE Transactions on Smart Grid*, in press.
11) M. Govindarasu et al., Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control (WAMPAC) for Power Grid, *Proceedings of the IEEE,* under review.
12) P. Wang and M. Govindarasu, “Multi Intelligent Agent based Cyber Attack Resilient System Protection and Emergency Control”, *IEEE ISGT*, Sep. 2016.
13) V. K. Singh, A. Ozen, and M. Govindarasu, “Stealthy Cyber Attacks and Impact Analysis on Wide-Area Protection of Smart Grid”, NAPS, Sep. 2016.

Collaboration/Technology Transfer

- Electric power sector asset owner networks are the targeted use case for the tools.
- ANL project team has identified organizations that are currently involved and/or expected to be involved in the transition of the technology.
- ANL project team will continue to consult with IAB and reach out to the companies to gain their interest in adopting the tools under this project and enter into technology transfer negotiations.
- ANL project team will attend energy sector conferences, and workshops to demonstrate the tools developed under this project and its applicability and adoption by end-users.


Basic R&D – Project Scope
Conception of Research Idea
(Theory/ Hypothesis, Algorithm)
Prototyping of Research
(Algorithm Software Implementation)
Testbed Deployment
(Algorithm Implementation on Realistic Testbed)
Testing/ Evaluation
(Performance Evaluation on Realistic Testbed)
Pilot Deployment
(Real-world deployment with industry partnership)
Commercialization
(Technology Transfer to Indsutry)
Applied R&D
R&D impacts
- Models, Algorithms
- Prototype artifacts
- Datasets
- Evaluation results
- Technical reports
- Testbed-based evaluation
- Vulnerability Disclosures
- Industry Partnerships
- Pilot Deployments
- Technology Adoption
- Product Development
Industry impacts

Thank You!

Jianhui Wang   Ph.D.
Section Lead – Advanced Power Grid Modeling
Energy Systems Division
Argonne National Laboratory
9700 S. Cass Avenue, Bldg. 362
Argonne, IL 60439, USA
Jianhui.wang@anl.gov