Jianhui Wang

Argonne National Laboratory

Cybersecurity for Renewables, Distributed Energy Resources, and Smart Inverters

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

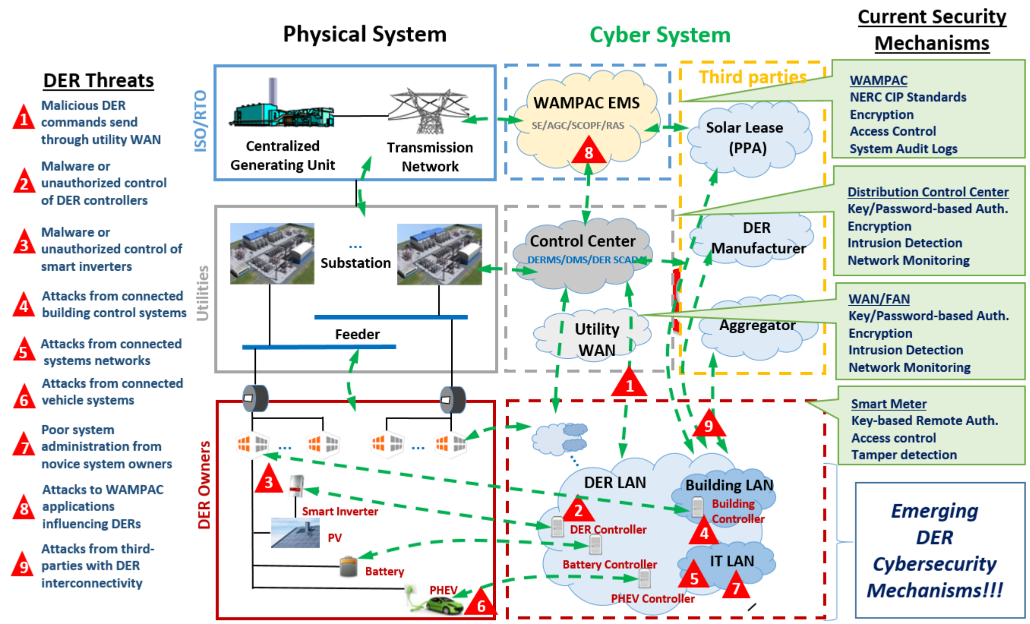
Summary

Objective

- Develop an attack-resilient architecture and layered cyber-physical solution portfolio to protect the integrated DER and power grid
- Enhanced cybersecurity at cyber, physical device, and utility layers of the power system

Schedule

- April 2016 – March 2019
- Technical Report on DER Cybersecurity Framework finished on Oct. 20, 2016



Performer:	Argonne National Laboratory
Partners:	Washington State University, EPRI
Federal Cost:	$1,800,000
Cost Share:	N/A
Total Value of Award:	$1,800,000
Funds Expended to Date:	10%

Advancing the State of the Art (SOA)

- Most existing research only focuses on the cybersecurity issues of smart meters which cannot meet the need for DER cybersecurity
- Advancing the State of the Art
  - This project will address the unique challenges of DER integration
  - We will identify the most important attack scenarios against DER from a system-level perspective
  - We will develop attack prevention, detection, and response measures specifically designed for DER integration at cyber, physical device, and utility layers, bridging IT and OT
- Feasibility of our approach
  - A team with capabilities on cybersecurity, communication, smart inverters, power system resilience, and testbed validation
  - A detailed research plan and several clearly defined and achievable milestones

Advancing the State of the Art (SOA)

- How end uses will benefit
  - Utilities and third parities: Enable trusted system architectures, reliable access control model, and secure communication (cyber layer); Targeted protection and real-time intrusion detection (utility layer)
  - Smart inverter vendors: Enhance cybersecurity of smart inverters and develop energy buffers (physical device layer)
- Respect operational requirements of energy delivery systems
  - The developed techniques will obey the operational requirements without harming the grid reliability and stability
- Advance the cybersecurity of energy delivery systems
  - Power grid is quickly integrating distributed energy resources which will significantly change the grid architecture
  - Enhancing the cybersecurity of DER integration is key to maintaining a high level of security of future smart grid

Progress to Date

The industry advisory board (IAB) was established on August 3, 2016 including the following members:

- Marc A. Child, Great River Energy, Chair of NERC’s CIPC
- Mark Oens, SnoPUD
- Frances M. Cleveland, Xanthus Consulting International
- Dmitry Ishchenko, ABB
- Dong Wei, Siemens
- Qiang (John) Fu, Eaton

First IAB meeting held on August 10, 2016

Continued support through webinars and technical reviews

Progress to Date

Major Accomplishments

Milestone #1 (6 month ACA) Achieved

- Completion of design of DER cyber security framework that comprehensively covers cyber-physical-threat modeling, DER attack prevention, detection and mitigation across cyber, device, and utility levels
- Technical report detailing the developed DER cyber security framework
- Completion of design of attack-defense experiments to validate/evaluate the security and attack-resilient properties of the proposed framework
- Invited paper for IET Cyber-Physical Systems: Theory & Applications Inaugural Issue

Challenges to Success

Fasting-Moving DER Industry

- Team members and industry advisory board members from industry
- Closely track the industry development

Simulation Tools

- Leverage work in other GMLC and CEDS projects

Data Availability

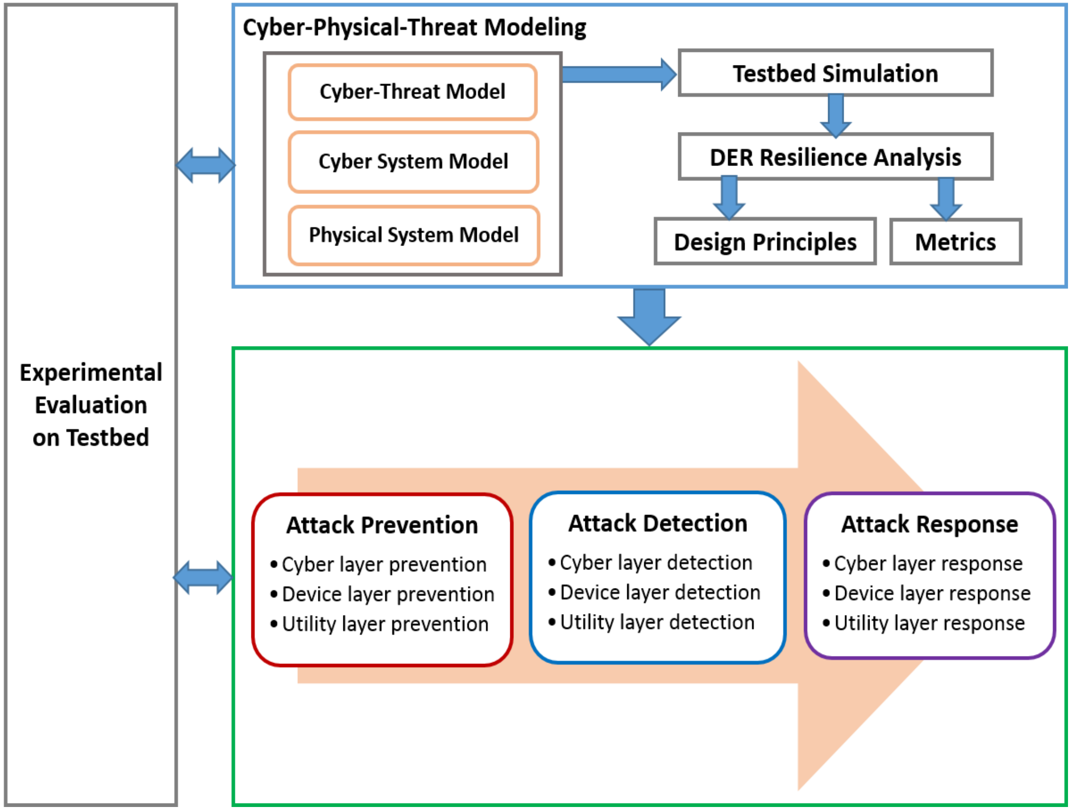
- Obtain data both from simulation and Smart City testbed at Washington State University

Analysis Methods

- Specially developed methods for DER integration

Collaboration/Technology Transfer

- Targeted end users for the technology or knowledge
  - Utilities and third parities: for the cyber layer and utility layer cybersecurity mechanisms
  - Smart inverter vendors: for physical device layer work on smart inverters and energy buffers
- Plans to gain industry acceptance
  - Developed methods will be tested on the Smart City Testbed at Washington State University
  - Promote the methods through the industry advisory board members from both utilities and vendors



Next Steps for this Project

Approach for the next year or to the end of project

Key Milestones to accomplish

- By the end of the first year: Complete the design of DER cyber threat modeling and resilience metrics
- By the end of the second year: Complete the design of DER attack prevention and detection techniques at cyber, physical device, and utility layers of the system
- By the end of the third year: Complete the design of DER attack response techniques at cyber, physical device, and utility layers of the system; complete extensive experimental evaluations on Smart City Testbed

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