

Enhancing Power Grid Cybersecurity to Improve Critical Electric Infrastructure Resilience

Junjian Qi and Jianhui Wang

Energy Systems Division
Argonne National Laboratory

Funded by DOE OE Cybersecurity of Energy Delivery Systems (CEDDS)

August 18, 2016

Cyber Attacks Against Power Grid

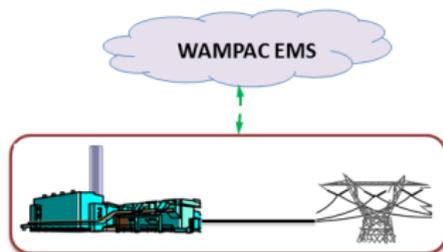
- ▶ Illegal entry into a Ukrainian electricity distribution company's computer and SCADA systems on December 23, 2015
- ▶ 11 110 kV and 23 35 kV substations disconnected for 3 hours
- ▶ 225,000 customers lose power across various areas



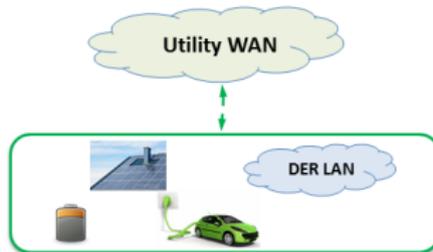
Source: Analysis of the Cyber Attack on the Ukrainian Power Grid, 2016.

Power Grid Cybersecurity—An Overview

Bulk Power System



Distributed Energy Resources



Cloud Computing

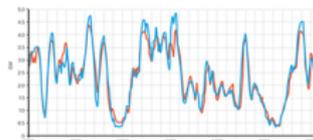
Security-Constrained
Economic Dispatch

Security-Constrained
Unit Commitment

⋮

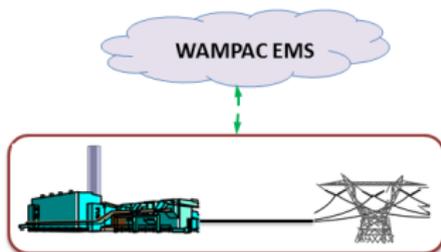


Forecasting Data

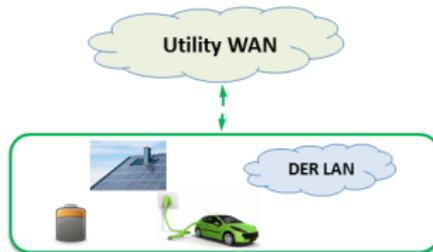


Power Grid Cybersecurity—An Overview

Bulk Power System



Distributed Energy Resources



Cloud Computing

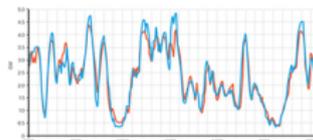
Security-Constrained
Economic Dispatch

Security-Constrained
Unit Commitment

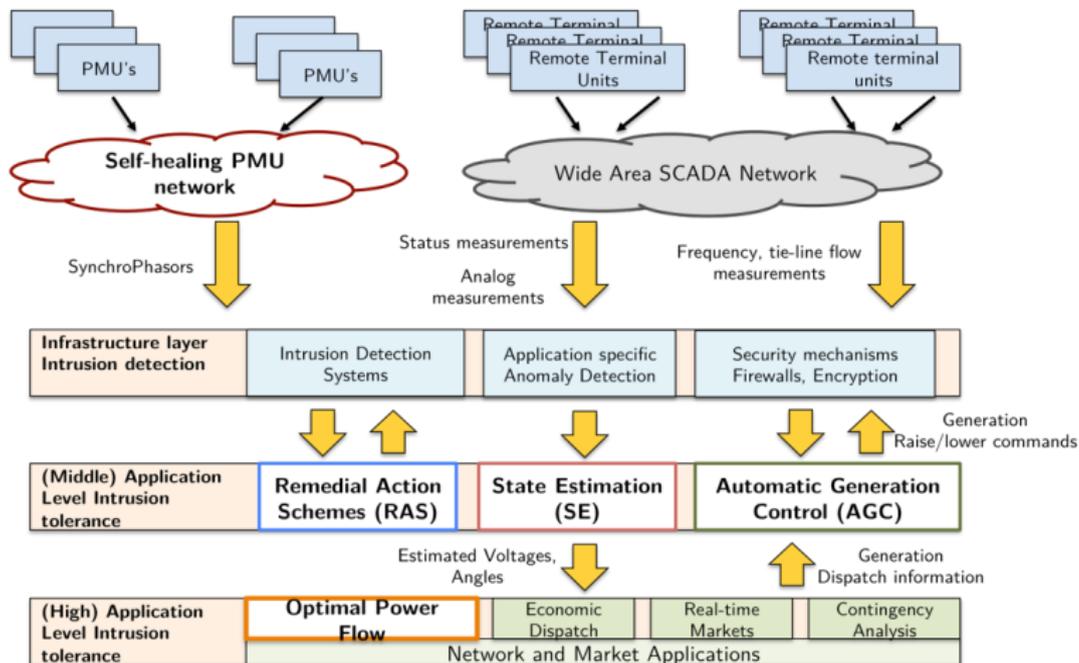
⋮



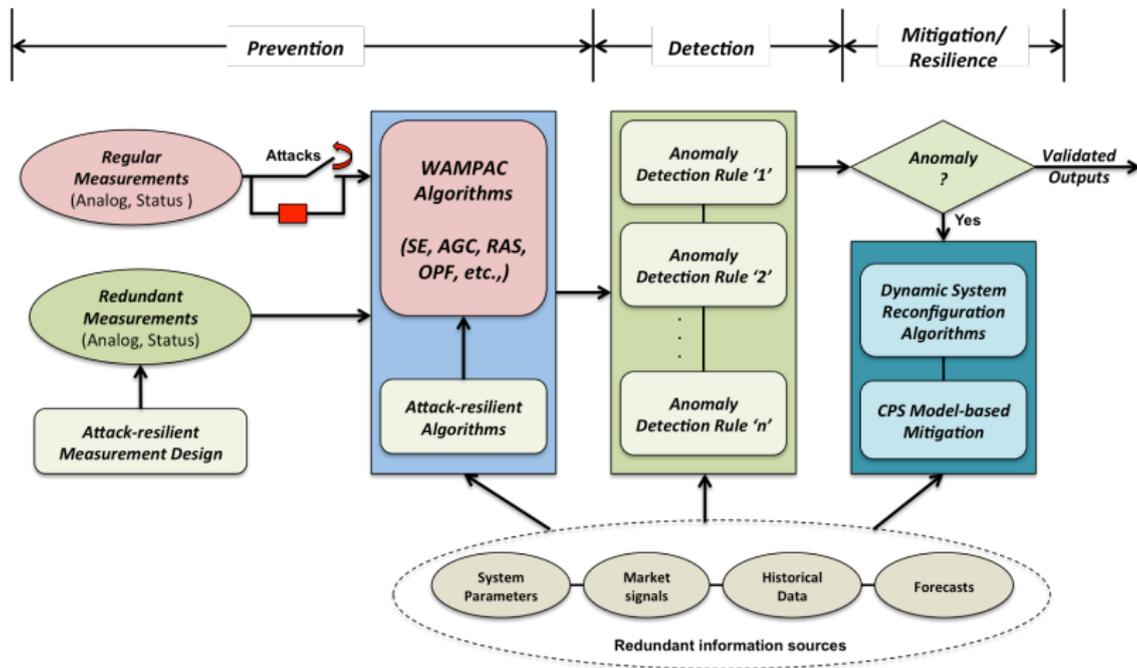
Forecasting Data



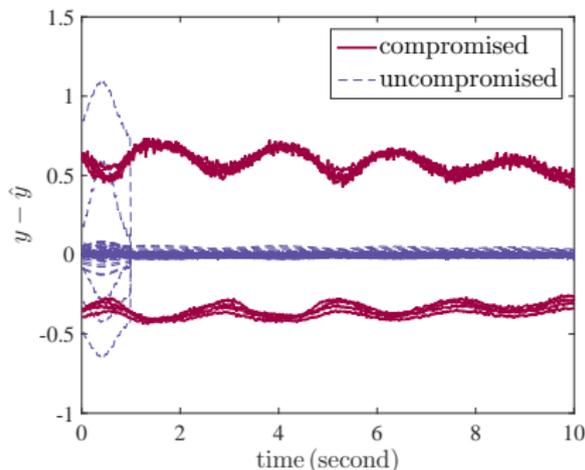
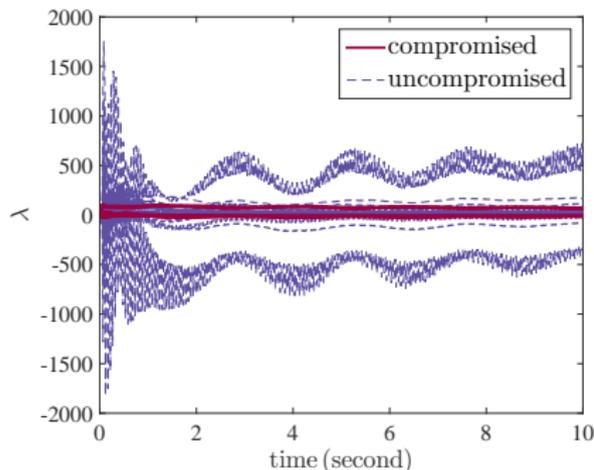
Bulk Power System Cybersecurity



Enhancing Bulk Power System Cybersecurity



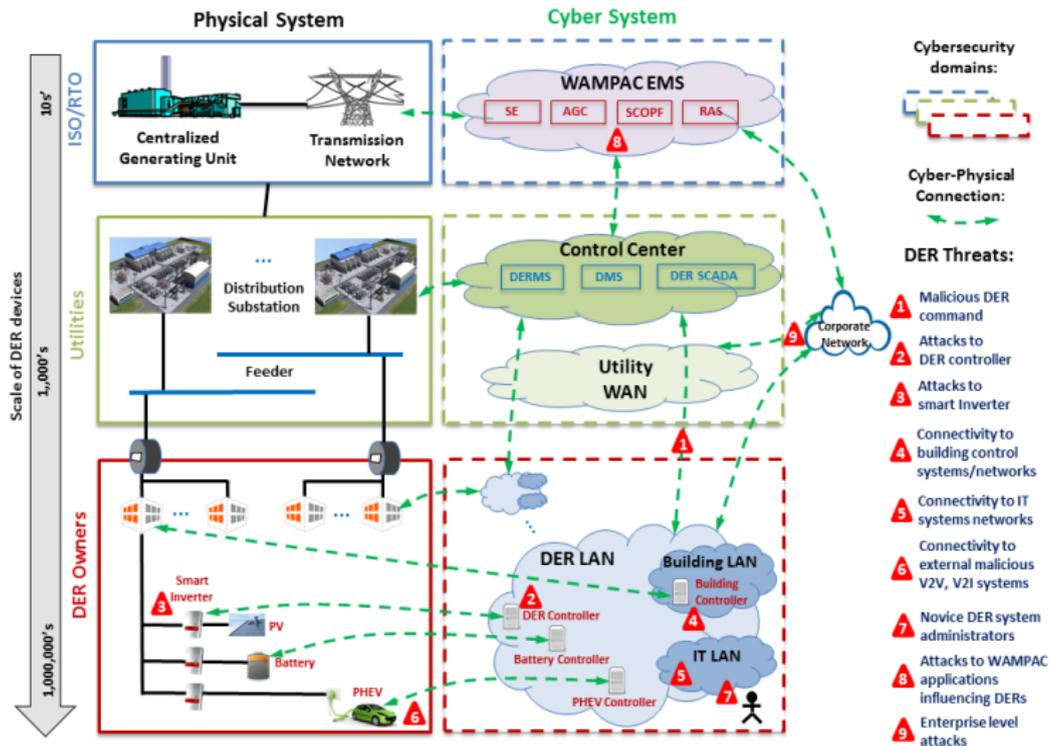
Enhancing Bulk Power System Cybersecurity—An Example for Dynamic State Estimation



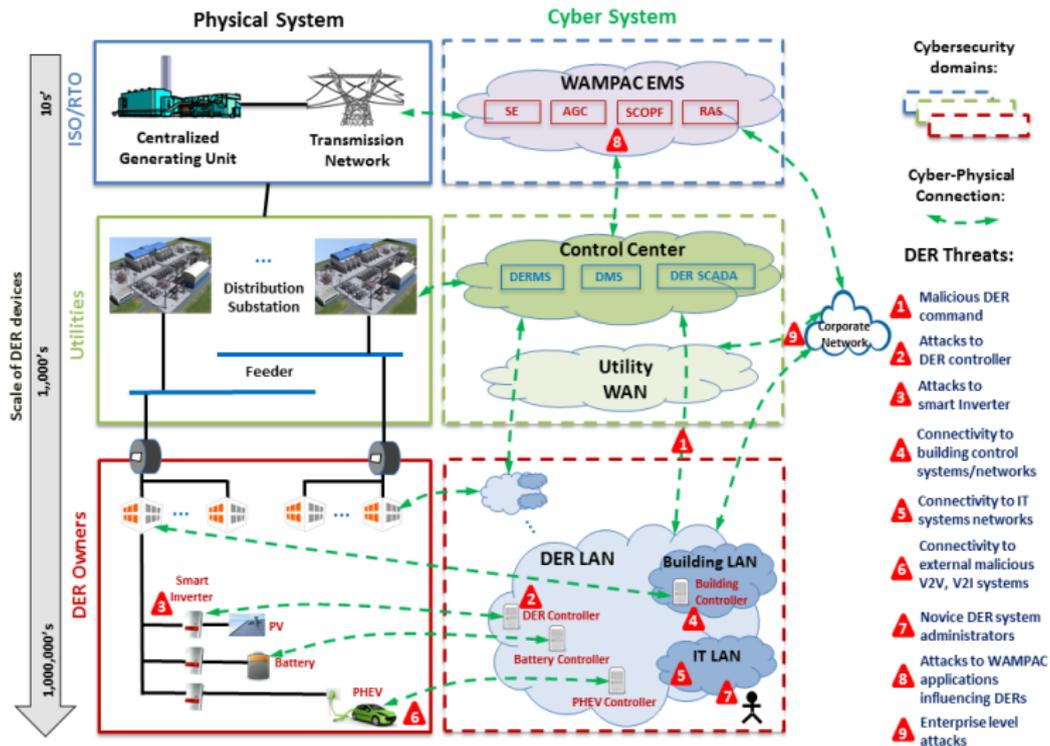
- [1] J. Qi, A. F. Taha, and J. Wang, "Comparing Kalman Filters and Observers for Dynamic State Estimation with Model Uncertainty and Malicious Cyber Attacks," *arXiv preprint arXiv:1605.01030*, 2016 (submitted to *IEEE Trans. Power Systems*).
- [2] A. F. Taha, J. Qi, J. Wang, and J. H. Panchal, "Risk Mitigation for Dynamic State Estimation Against Cyber Attacks and Unknown Inputs," *IEEE Trans. Smart Grid*, in press. DOI: 10.1109/TSG.2016.2570546



Emerging Distributed Energy Resources (DER) Architecture and Threats



Emerging Distributed Energy Resources (DER) Architecture and Threats



Challenges of DER Cybersecurity

Compared with AMI, DER cybersecurity has additional challenges:

- ▶ Divided administration

- ▶ Increased cyber-physical interdependencies

- ▶ Greater impact to grid

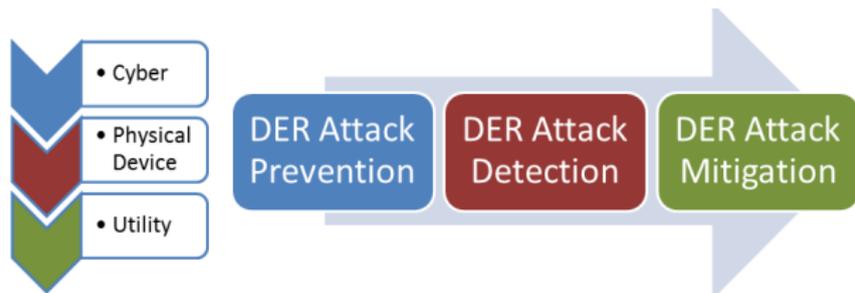
- ▶ Cryptography & key exchange

- ▶ Privacy

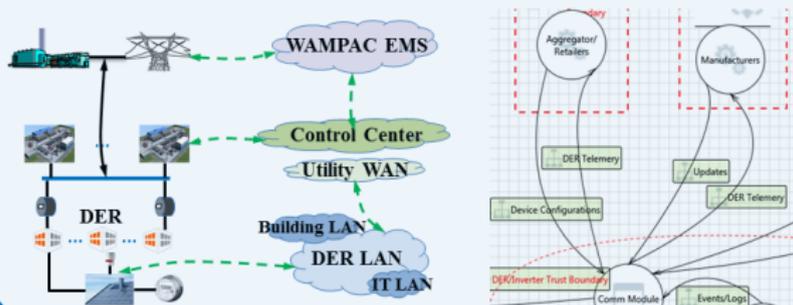
- ▶ More control functions



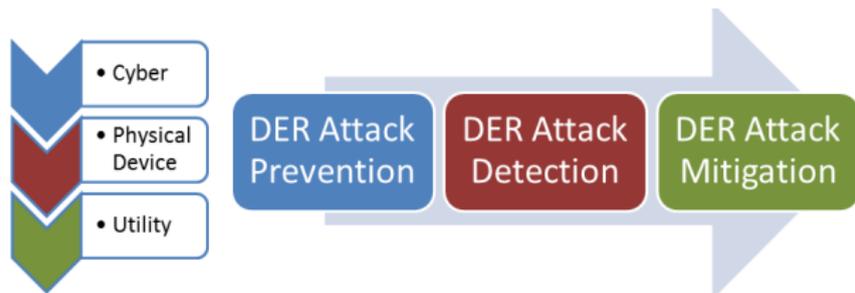
DER Cybersecurity Framework



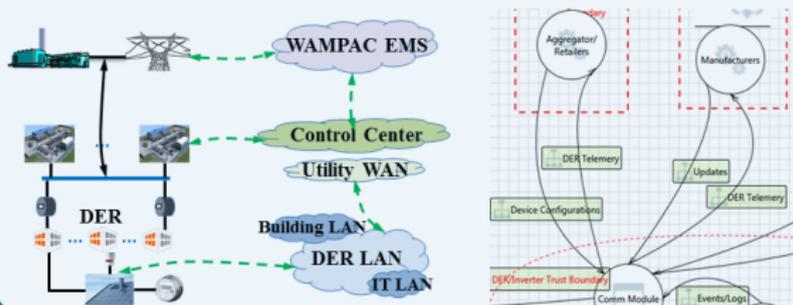
Cyber-Physical-Threat Modeling and Attack Impact Evaluation



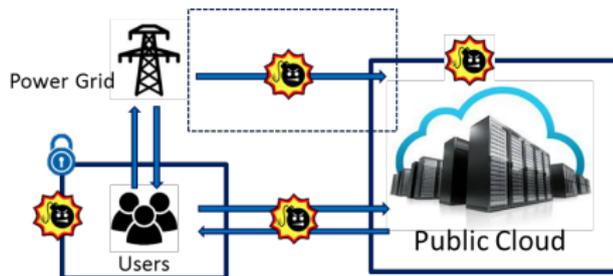
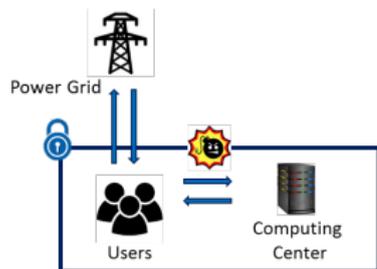
DER Cybersecurity Framework



Cyber-Physical-Threat Modeling and Attack Impact Evaluation



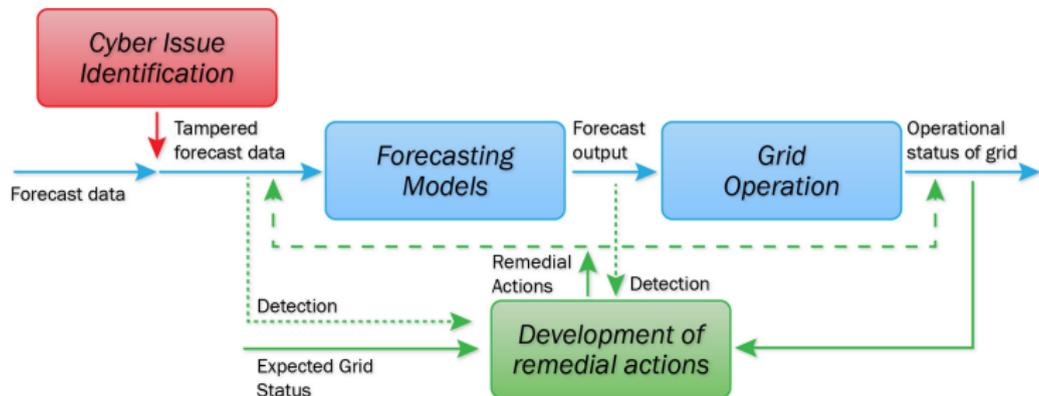
Cybersecurity of Cloud Computing and Outsourcing



- ▶ Infrastructure Security
- ▶ Data Privacy
confidentiality and integrity of **data** and **results**
- ▶ Time Criticality



Cybersecurity of Forecasting Data



A project led by Brookhaven National Laboratory

- ▶ Determine the potential impact of cybersecurity issues involving maligned forecasting data on the performance of energy delivery systems
- ▶ Develop detection and mitigation methods

Conclusion

- ▶ Power grid can be vulnerable to cyber attacks
- ▶ Power grid cybersecurity should be greatly enhanced
 - ▶ Bulk power system
 - ▶ DER
 - ▶ Cloud computing
 - ▶ Forecasting data

THANK YOU!

