IOWA STATE UNIVERSITY

Autonomous Tools for Attack Surface Reduction

PI: Manimaran Govindarasu, Team: Iowa State University (Lead), Washington State University, Alstom Grid, Snohomish County Public Utility District, Pacific Northwest National Laboratory, Argonne National Laboratory

Motivation

- The electric grid's attack surface continues to grow with increased interconnectivity and automation encompassing the enterprise, control center, substations, and even beyond.
- Recent attack in Ukraine targeted critical distribution control center servers through SCADA VPN and also expanded its impact to target field devices at substations to create a regional blackout.
- Current energy delivery systems utilize static and monolithic architectures, configurations, and communications that make attacks against EDS systems more predictable.
- There is a lack of clear metrics and tools to assess the grid's continually expanding attack surface.
- There is also a need for automated approaches to reduce the attack surface at multiple layers including control center, substations and the wide-area SCADA communication networks.

Project Objectives

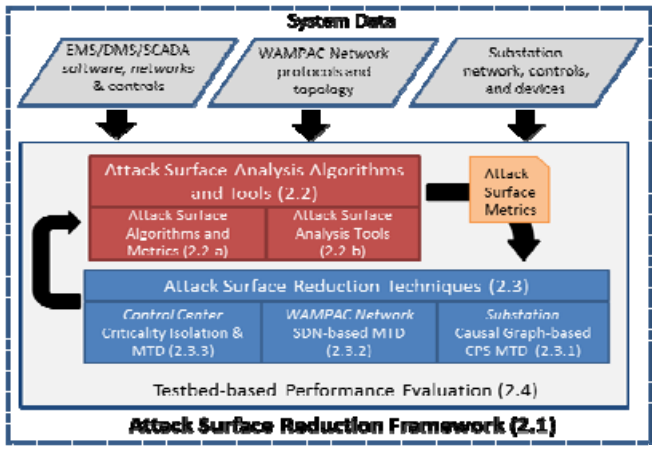
Phase I:

- Develop an integrated framework that continually assesses and autonomously reduces the attack surface for the power grid control environment.
- Develop attack surface analysis techniques, metrics, and tools that assesses the attack surface at multiple levels including the control center, substations, and the SCADA network.
- Develop attack surface reduction techniques and tools that dynamically reduce attack surface and hence increase attacker's cost without interfering in the critical functions of the system.
- Prototype, implement, and evaluate the techniques and tools on a realistic industrial CPS security testbed environment by leveraging the unique resources of the team.
- Develop a Commercialization plan to transition the developed tools into power system industry stakeholders for a broader adoption.

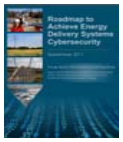
Phase II:

- Field demonstration, verification, and evaluation of the effectiveness of the attack surface analysis and reduction techniques on a realistic utility testbed environment.

Research Tasks

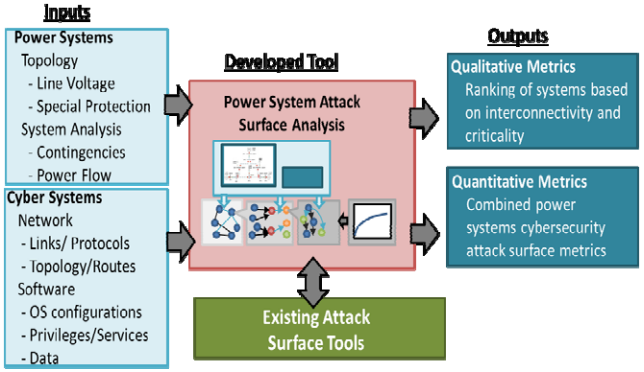


Alignment with DOE Roadmap



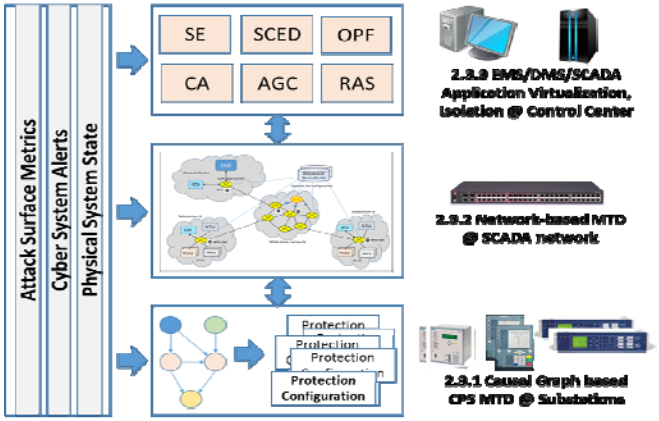
Addresses Energy Sector roadmap milestones		
2. Assess and Monitor Risk	**3. Develop and Implement New Protective Measures to Reduce Risk**	**4. Manage Incidents**
2.1 – Terms and measures for baselining security posture. 2.3 – Tools for real-time monitoring and risk assessment.	3.1 – Capabilities to evaluate robustness and survivability of platforms, systems, networks. 3.4 – Self-configuring energy delivery system network architectures. 3.5 – Capabilities to continue operation during attacks available built-in or as upgrades.	4.7 – Capabilities for automated response to cyber incidents, and best practices.

Attack Surface Analysis Metrics and Tools



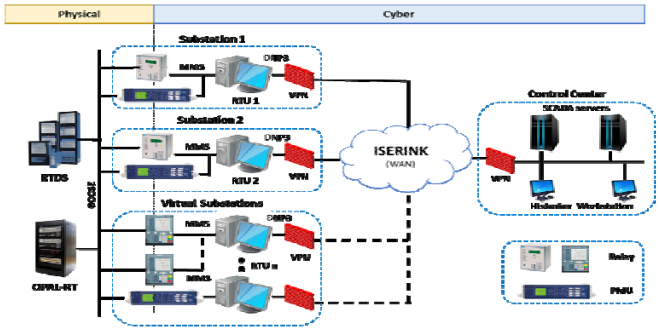
Attack Surface Reduction Algorithms

Attack Surface Reduction @ Multiple levels

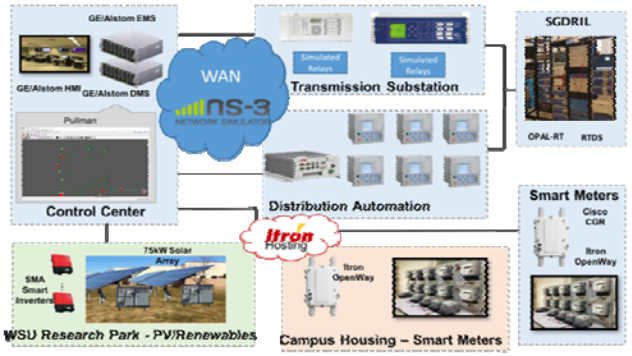


Testbed-based Implementation & Evaluation

Iowa State PowerCyber Testbed



Washington State Smart City Testbed



Commercialization & Demonstration

- ISU will work with Alstom, SnoPUD and other partners to develop a commercialization plan in the last quarter of Year 2 in the project.
- Year 3 includes field-testing and demonstration of capabilities with major involvements from our industry partners ALSTOM and SnoPUD.
- Alstom will co-lead the effort to integrate the attack surface analysis and reduction tools into their SCADA/EMS tool chain.
- SnoPUD will co-lead the effort to deploy the attack surface reduction tools into their Test and Live SCADA environment, and utilize them for testing.

Acknowledgements: This research project is funded by the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability's Cybersecurity of Energy Delivery Systems (CEDS) program through award # DE-OE0000830. Project Manager: James Briones, NETL, Program Manager: Dr. Carol Hawk, DOE.
For additional information about the project, please contact Dr. Manimaran Govindarasu (Email: gmani@iastate.edu).