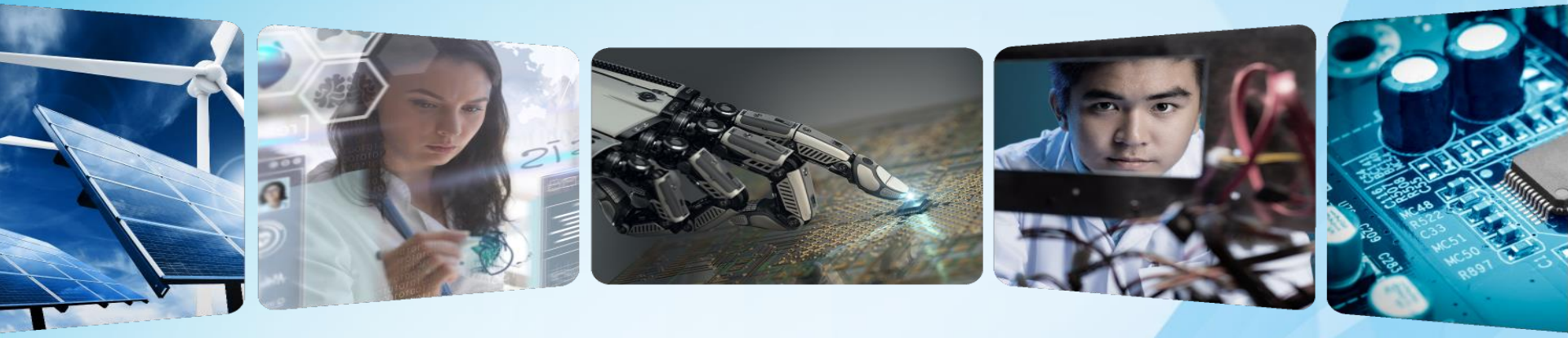
SAND2017-11940C



The Growing Need for Resilience in an Evolving Electric Grid

Charles Hanley

Sr. Manager, Grid Modernization and Resilient Infrastructures

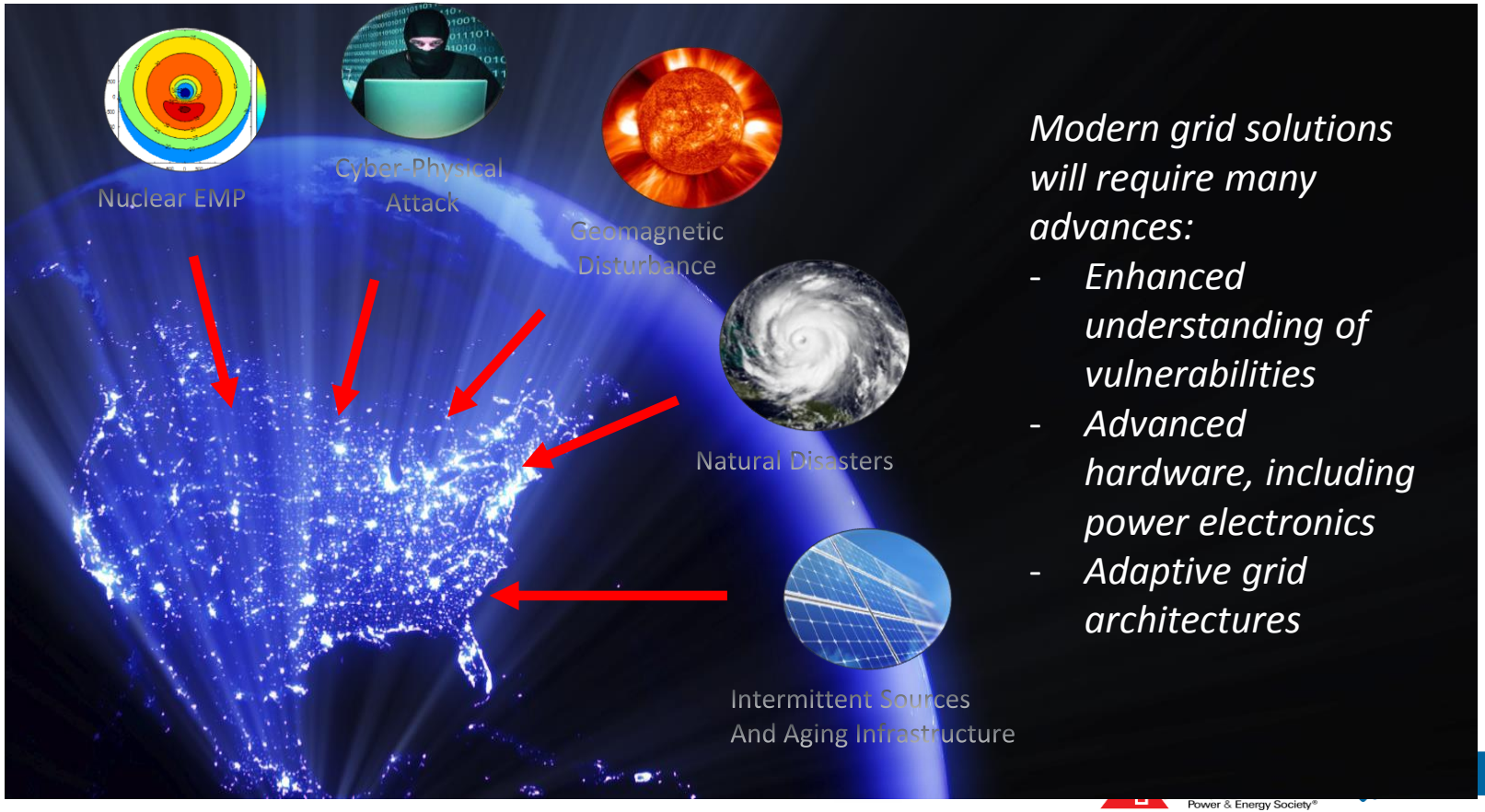
Sandia National Laboratories

eT&D Workshop; Aalborg, Denmark; 7 Nov. 2017

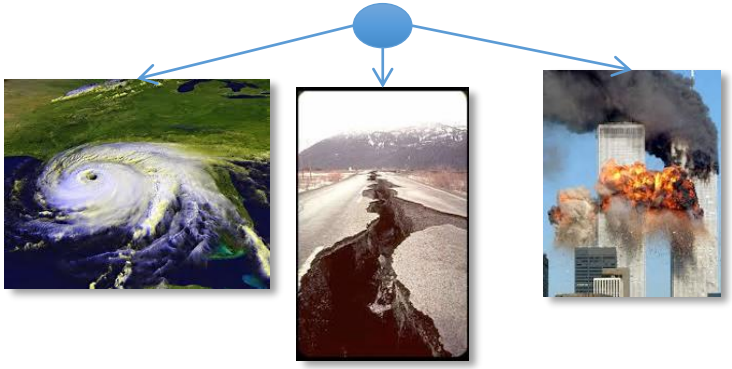
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

An “All Hazards” Approach to Grid Resilience

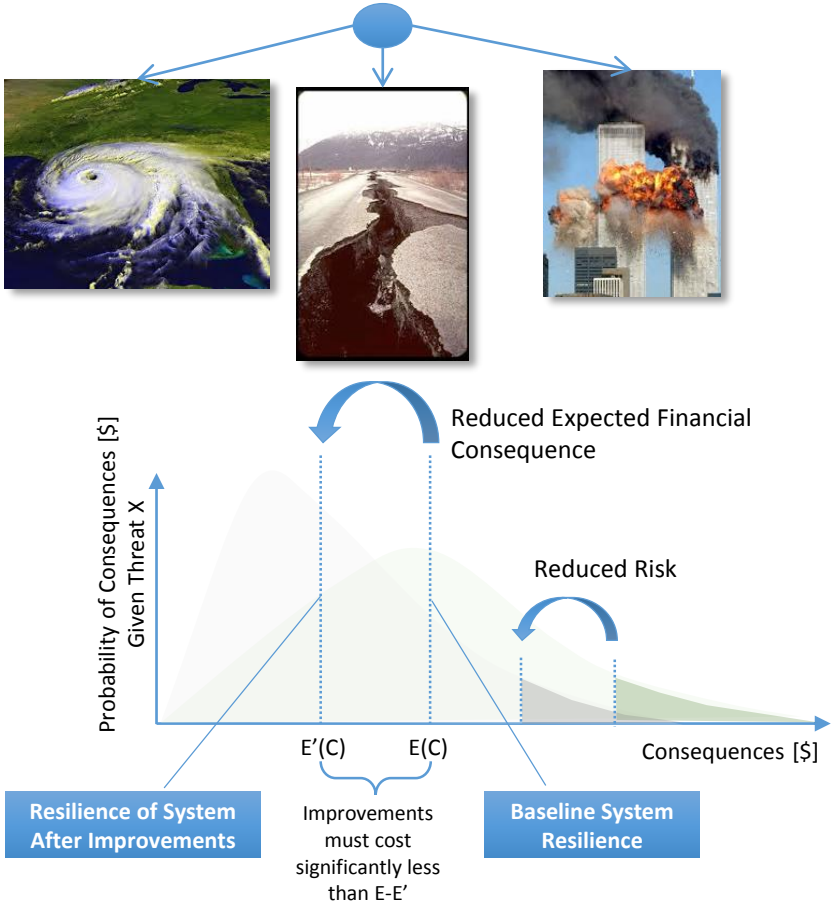
The U.S. electric grid is the root of our civilization, but it is aging, brittle, vulnerable to *numerous natural and man-made threats.*



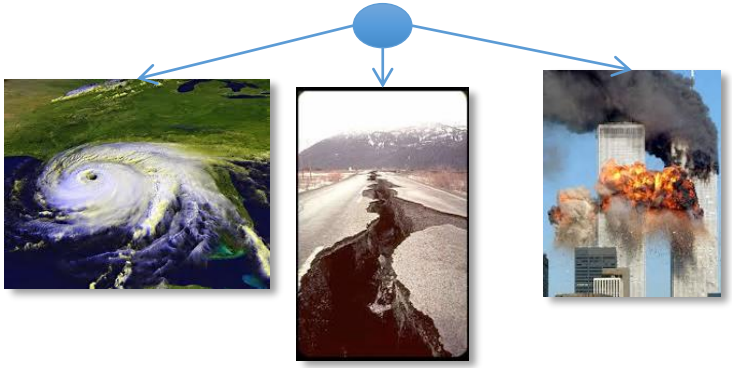
Resilience Analysis Approach is Threat-Based, Rigorous, and Quantifiable

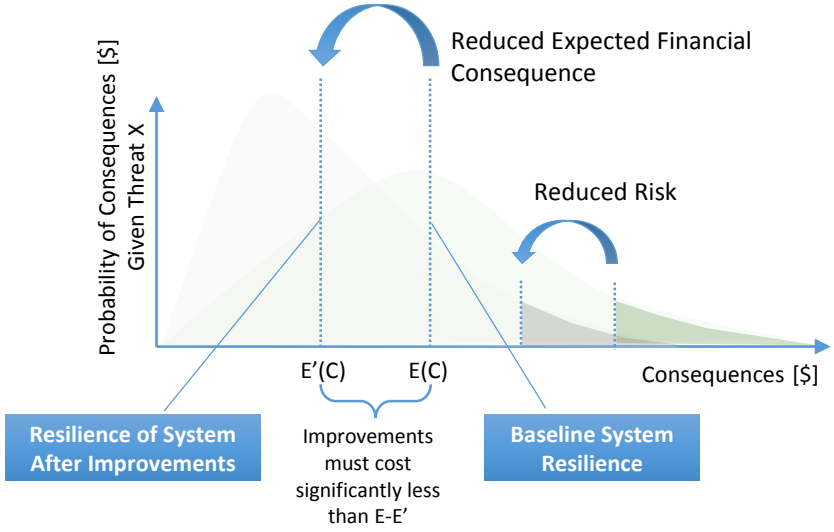


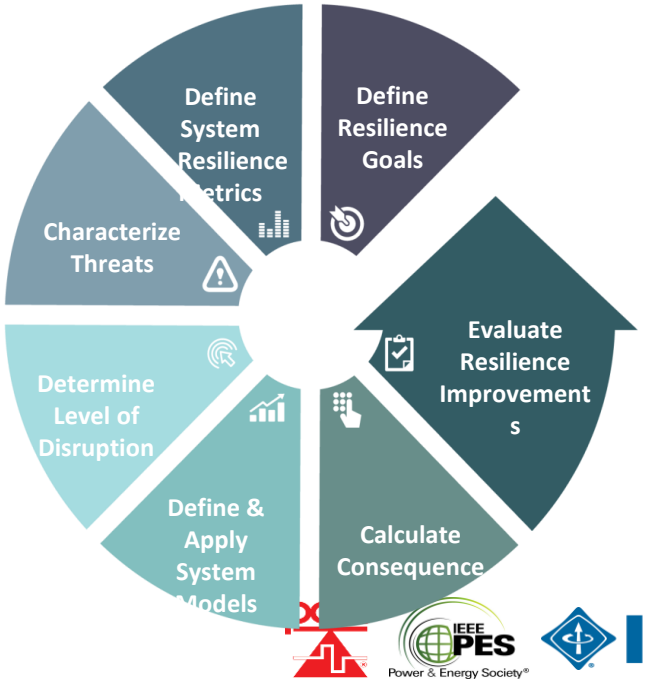
Resilience Analysis Approach is Threat-Based, Rigorous, and Quantifiable



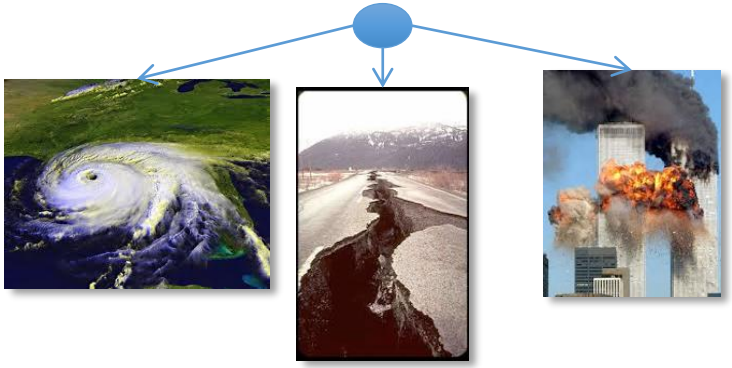
Resilience Analysis Approach is Threat-Based, Rigorous, and Quantifiable

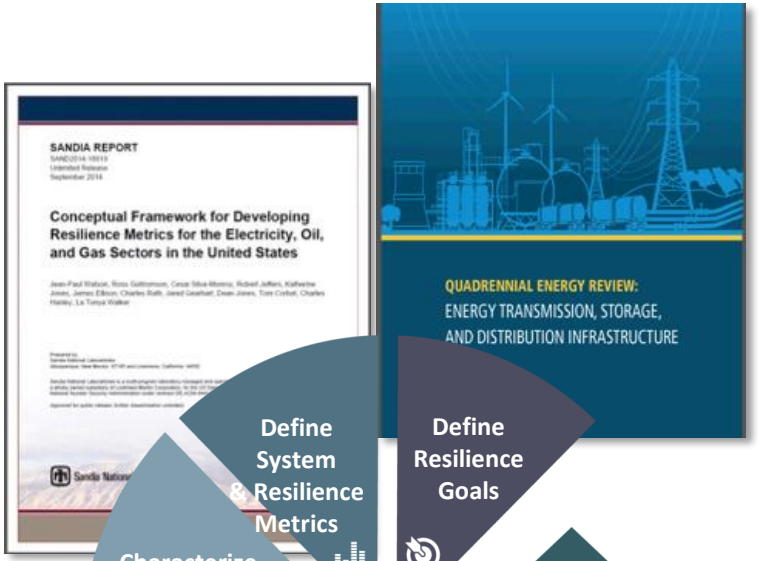


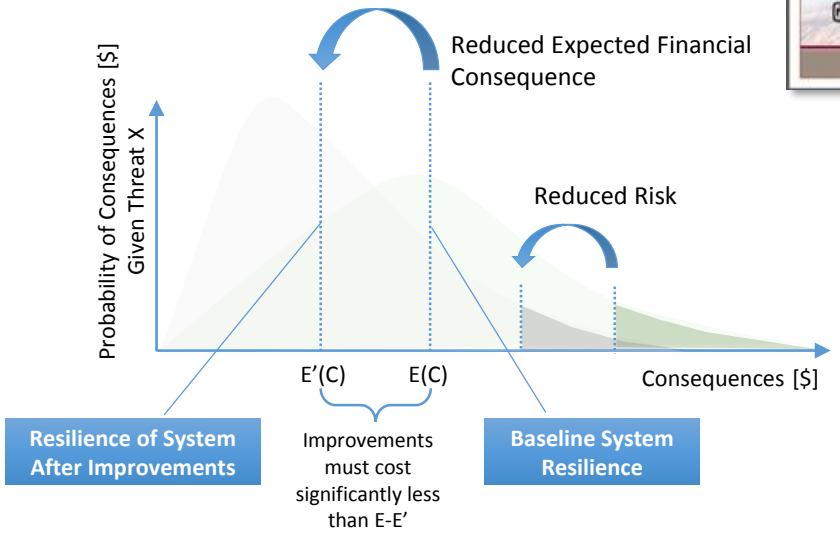


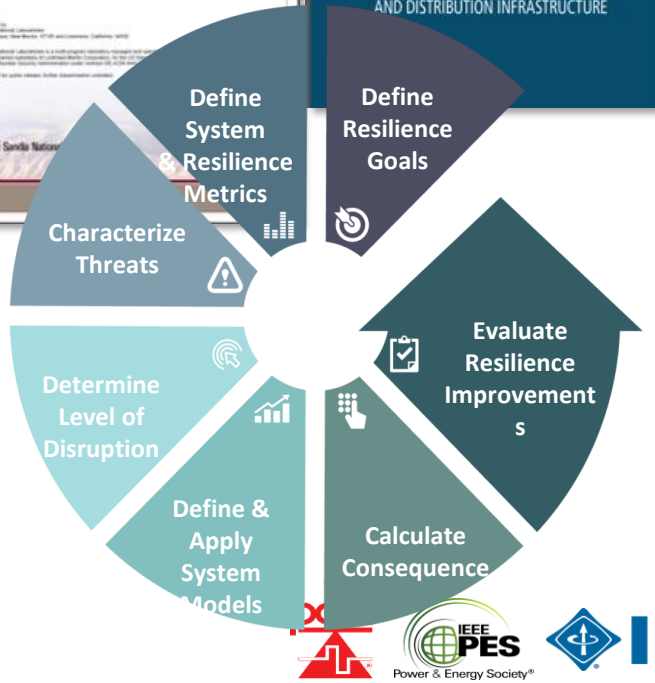


Resilience Analysis Approach is Threat-Based, Rigorous, and Quantifiable









Sandia's Industrial Control System Security Research

Provide decision makers with actionable information

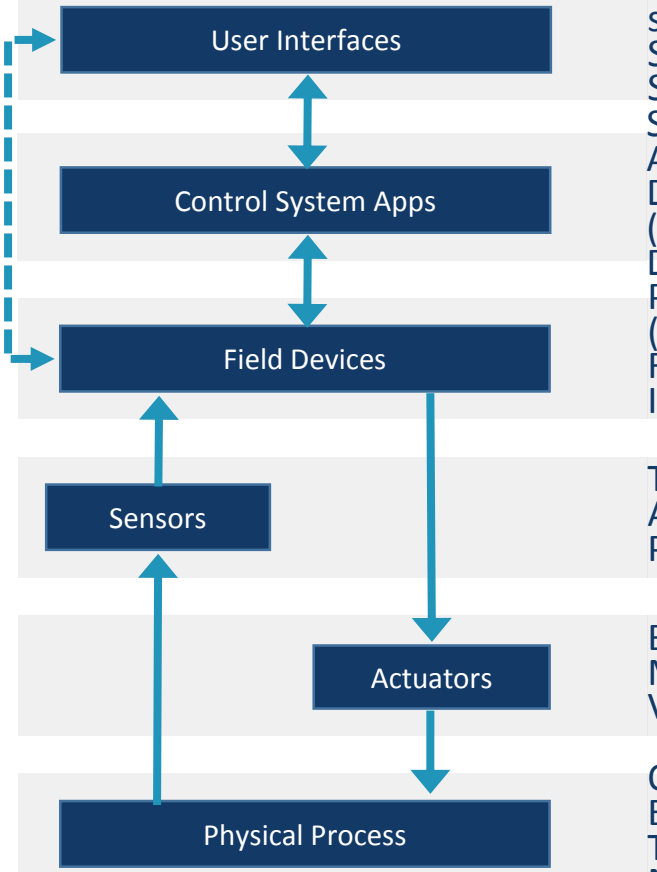
- Red Team Assessments
- Field Device Analysis
  - PLC monitoring and forensics
  - PLC firmware forensics
  - ICS network detection for ICS traffic
- Emulytics/SCEPTRE
- Exercise/Test Bed support

Design resilient systems to withstand cyber-attacks

- Research next generation security solutions
- Protect, Detect, React, Restore
- Partner with industry to "push" solutions to market

Mission: Reduce the risk of critical infrastructure disruptions due to cyber attacks on control systems.

Control System Architecture: Susceptibility At All Levels



- Human-Machine Interface (HMI) software
- Status displays
- Switches and dials

- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control Systems (EMS/DCS)
- Data Historians

- Programmable Logic Controllers (PLC)
- Remote Telemetry Units (RTU)
- Intelligent Electronic Devices

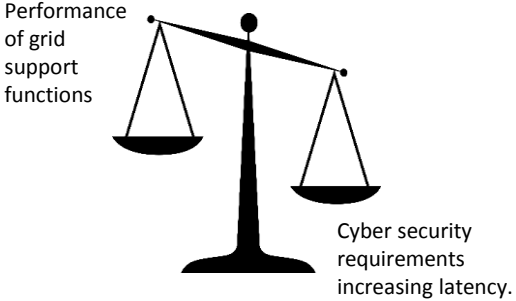
- Thermocouples
- Accelerometers
- Photoresistors

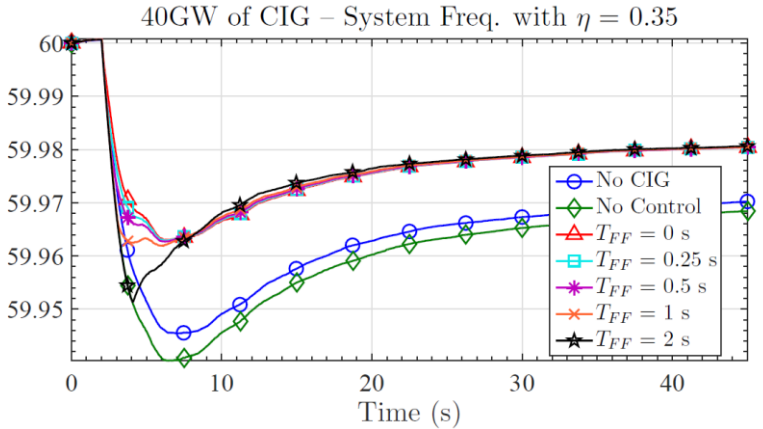
- Breakers/Switches
- Motors
- Valves

- Oil & Gas Refining
- Electrical Distribution and Transmission
- Manufacturing

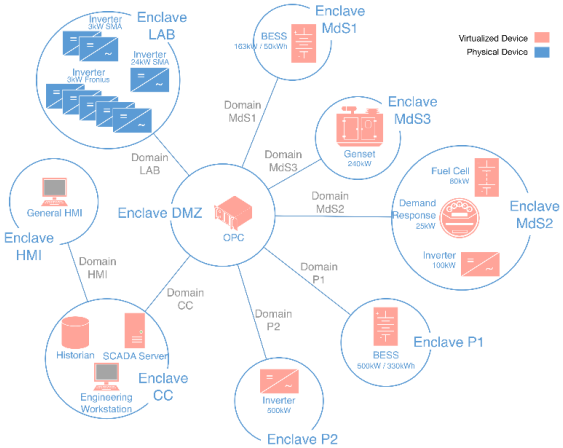
Situational Awareness and Mitigation Issue: System Performance vs Latency/Security

- DER will soon provide many grid-support capabilities (dispatchable power, contingency reserves, etc.) – in some cases via communications from grid operators, utilities, aggregators – through the public internet.
- The effectiveness of the function can be highly dependent on the speed of the communication.
- Sandia is studying the balance between implementing the highest degree of cyber security without eroding the performance of the distributed control system.





Influence of Communications Enabled – Fast Acting Imbalance Reserve (CE–FAIR) delay on N-1 nadir in western North American Power System (wNAPS).

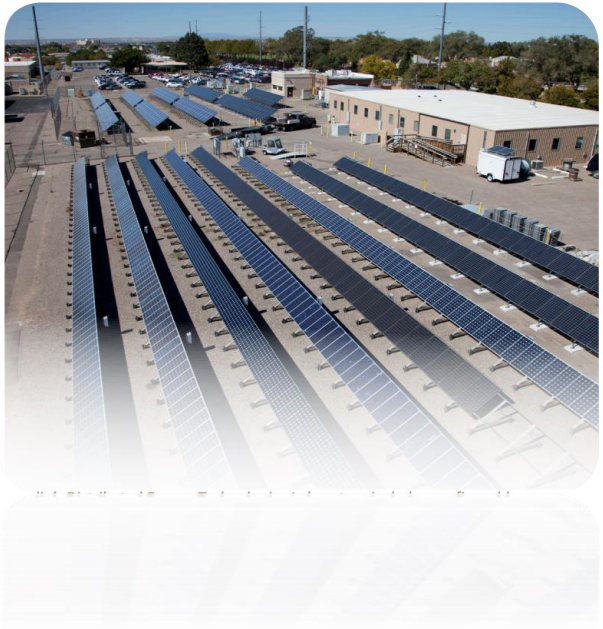


Cyber Reference Architecture which enclaves DER devices to minimize common-mode vulnerabilities.

F. Wilches-Bernal, R. Concepcion, J. Neely, R. Byrne, and A. Ellis, "Communication Enabled Fast Acting Imbalance Reserve (CE-FAIR)," submitted to IEEE Power Engineering Letters.

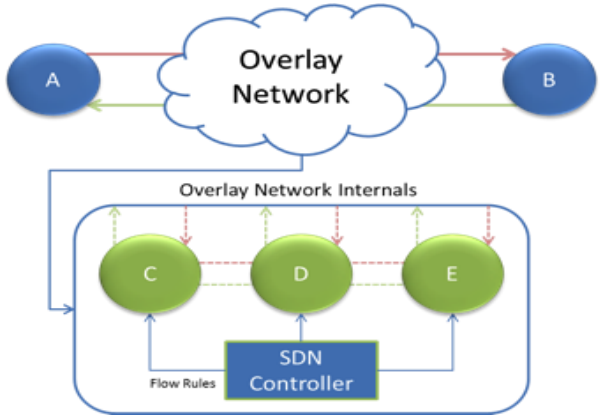
Threat Detection and Response with Data Analytics

- Goals: Develop machine learning to distinguish cyber threats from physical threats within a control system environment
- Progress: Integrated SEL-3620 (Ethernet Security Gateway) into Sandia's Distributed Energy Technologies Laboratory (DETL)
- Currently Implementing NESCOR scenarios within DETL environment
  - WAMPAC.11 – Compromised communication between substations
  - DER.6 - Compromised DER sequence of commands cause power outage
  - DER.16 – DER SCADA system issues invalid command
- Next steps: Configure and complete NESCOR scenario implementation
  - Analyze machine learning features and classification of cyber/physical events



Artificial Diversity and Defense Security (ADDSec)

- Moving Target Defense (MTD) cybersecurity for the energy sector
  - Change the energy delivery control system moment-by-moment to help prevent reconnaissance
  - Proactively disrupt and detect adversary at initial phases of attack planning
- Solution can be retrofitted into existing legacy/modern
- Partner SEL is developing compatible ADDSec commercial product for energy delivery control systems
  - Successful interoperability testing performed
    - April 12, 2017 within Virtual Power Plant environment (DETL will be integrated in July)
    - May 3, 2017 at SEL site
- SNL-led research team has upcoming demonstration at DoD Fort Belvoir microgrid site
  - Targeted for week of July 24, 2017 for initial tests/demonstration

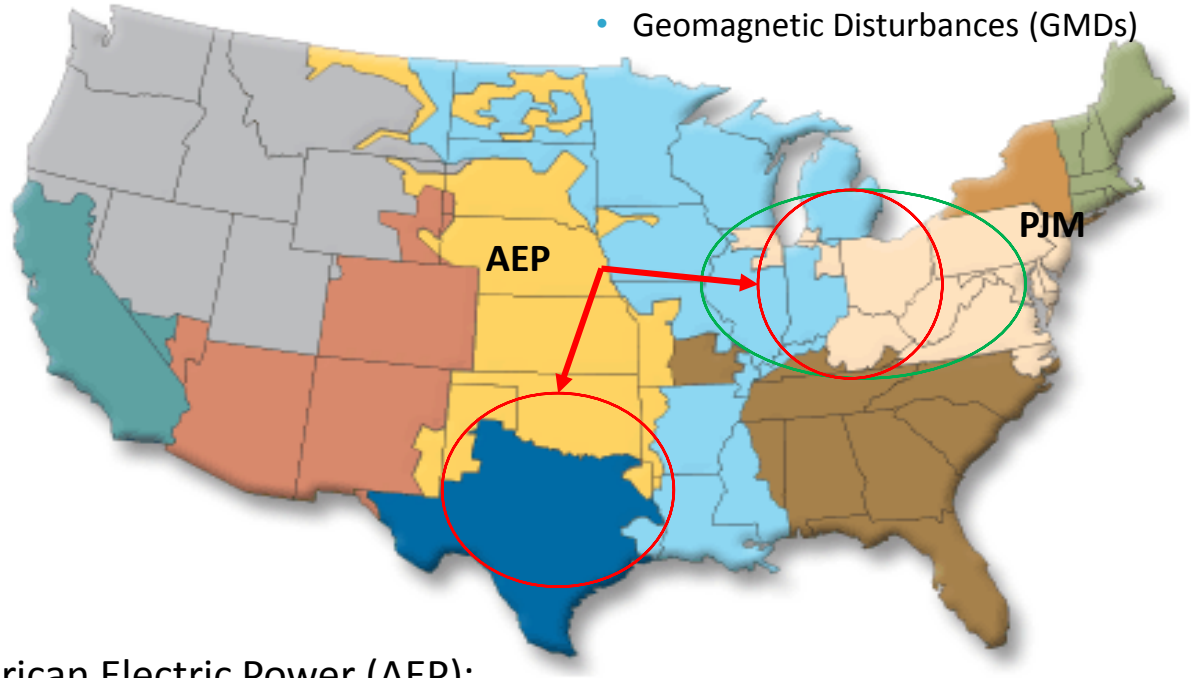


Sandia National Laboratories | Lawrence Livermore National Laboratory | Washington Gas Energy Systems | Chevron | GRIMM

SEL Schweitzer Engineering Laboratories | U.S. Department of Energy Electricity Delivery & Energy Reliability | pels | IEEE PES Power & Energy Society® | IEEE

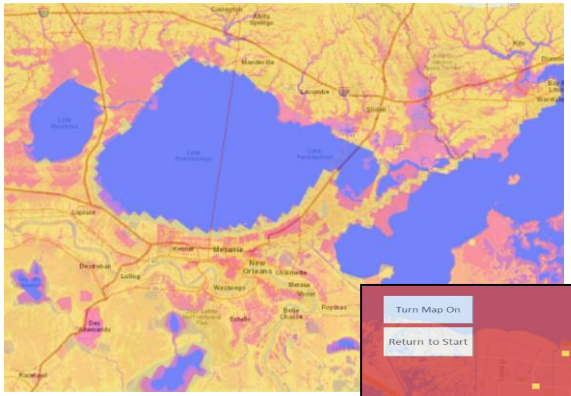
With Utility Partners: Resilience Metrics and Analytics for Decision-Making

- Pennsylvania-Jersey-Maryland (PJM) ISO:
  - Geomagnetic Disturbances (GMDs)



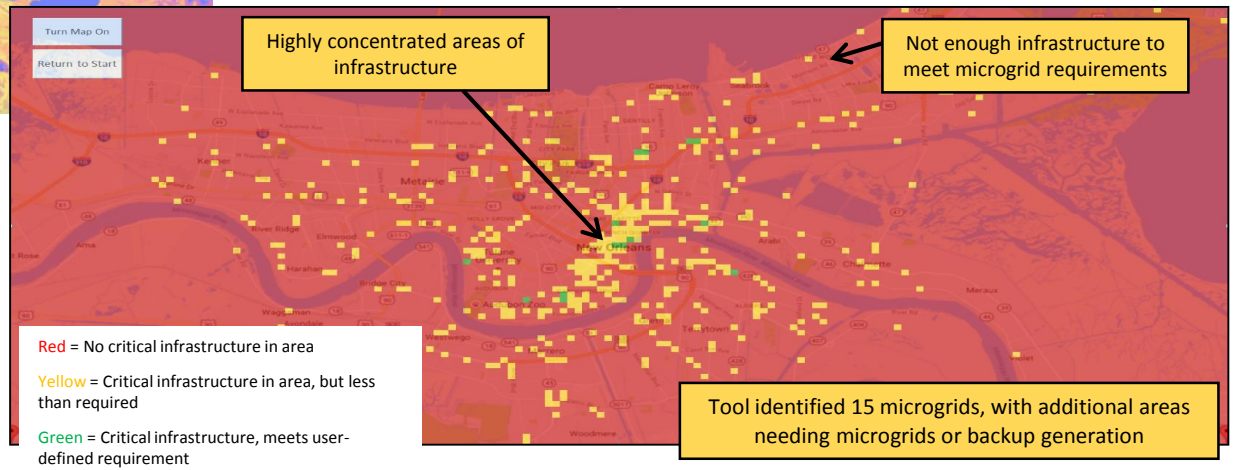
- American Electric Power (AEP):
  - Extreme weather (e.g., snow and ice storms)
  - Physical security threats (e.g., copper thieves and state actors)

Urban Resilience Case Study: New Orleans, LA



Results of Hurricane Inundation Modeling for New Orleans and surrounding regions

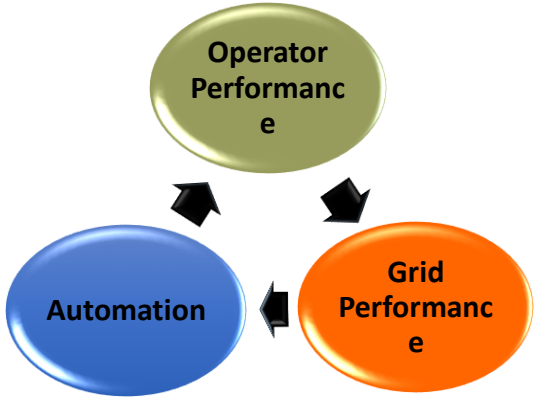
Area size of 1000 ft x 1000 ft | minimum of 4 buildings per microgrid



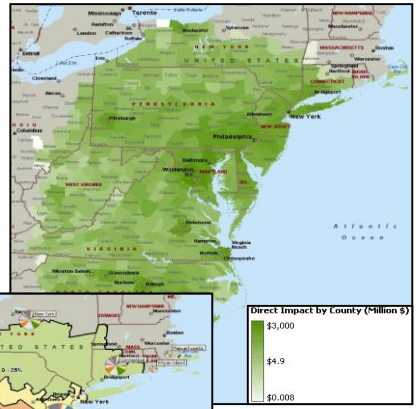
- Applying grid and infrastructure modeling to determine grid investments that will improve community resilience.
- **Resilience metric:** use microgrid designs to maximize the number of people with access to key services during flooding scenarios.

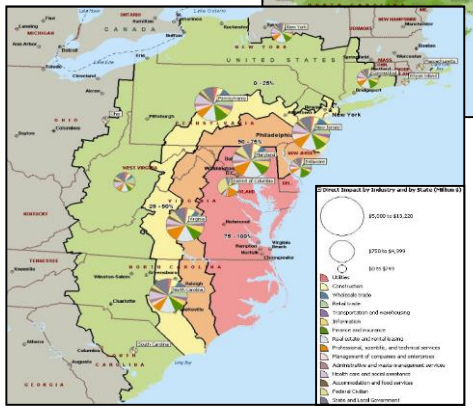
Additional Research Tools Are Being Used in Grid Resilience Analyses

- Cognitive Analysis – impacts of increased automation and data on performance
- Regional Economic Accounting Tool (REAcct)
  - GIS-Based
  - Fast studies on macro-econ impacts



Distribution of direct gross domestic product (GDP) reductions by county



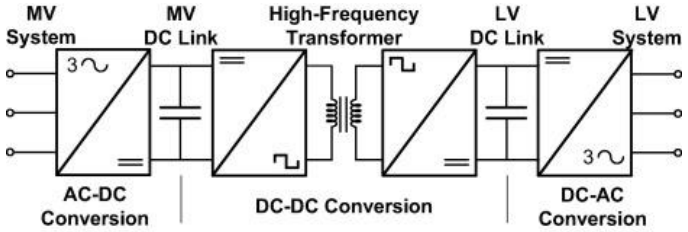


Distribution of economic impact by state and industry in the storm path

We are leveraging the broad set of capabilities in our DHS-sponsored *National Infrastructure Simulation and Analysis Center (NISAC)* for grid modernization

Power Electronics Advances are Crucial for Grid Resilience

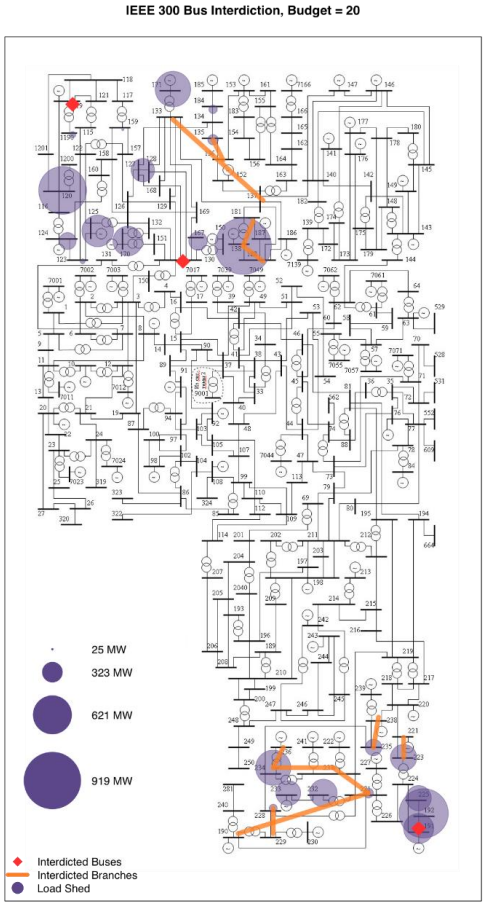
- EMP Resilient Power Electronics
- High Voltage Power Module Technologies
- Solid State Transformers
- Grid-Forming Inverters
- Hardware Enabled Secure BMS and ADMS Systems
- Rad-hard and Secure Power Flow Controllers
- Pervasive Current and Voltage Sensors across the Grid



Solid-state ac-dc-ac transformers promise isolation, decoupling, and resilience

Research areas include advanced materials, modular circuits, optical isolators, magnetics, advanced controls

Learnings from our Grid Resilience Work



Physical Interdiction Example on a 300 Bus System

- We've explored several individual threats
  - Moving to an integrated "all hazards" approach
  - Quantitative resilience is complex and data intensive!
- Highly dependent on stakeholder involvement
- Integrating new power electronics is critical
- Exciting new research is linking resilience to
  - Cybersecurity
  - Economic valuation
  - Inter-infrastructure dependencies
- We're currently working with DOE and utility partners to define and develop "resilience" as a grid service
  - Consortium partners welcome

IEEE