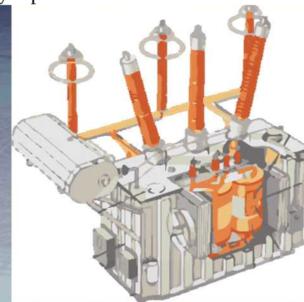
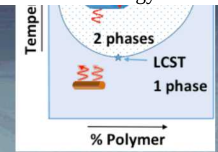
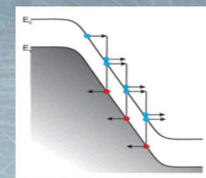





SAND2018-5698C

# Sandia's Research in Electric Grid Resilience: Emphasis on Grid Cyber Security

24 May, 2018

Presentation to the Emergency Management Issues Special Interest Group

Charles Hanley
Sr. Manager
Grid Modernization and Resilient Infrastructures

*Exceptional service in the national interest*

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

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.

# Outline of this Presentation

- National recognition of the need for resilience
- Brief introduction to Sandia's grid modernization work
- The development of resilience metrics
- Applying these metrics – several scenarios
- Deeper dive: cybersecurity for the grid

# External Drivers for a Modern Grid

*Our 21st Century needs a 21st Century grid to adapt to new threats, energy sources, and economic drivers.*

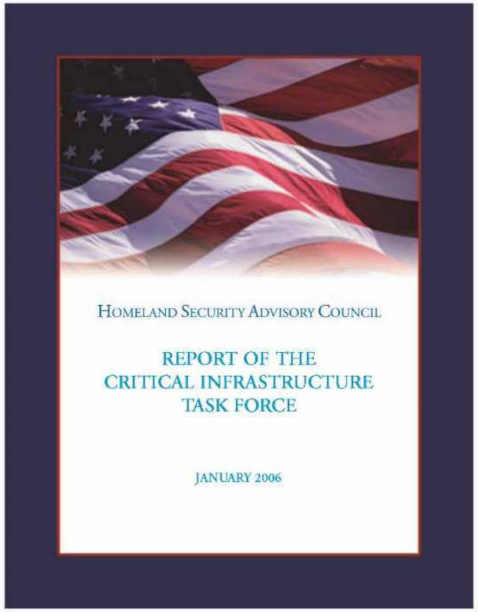




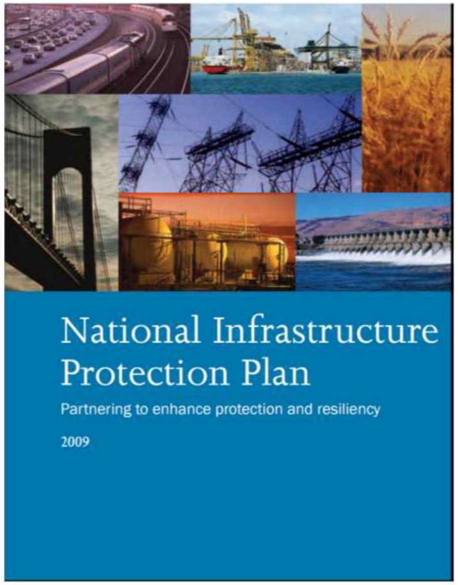


# Energy is Integral to National Security

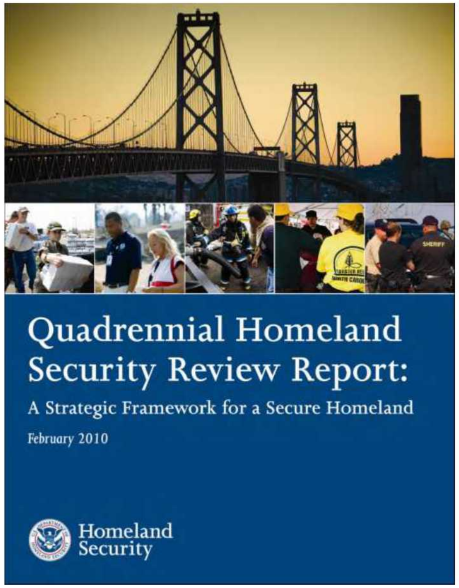
# Emergence of Resilience as National Security Priority



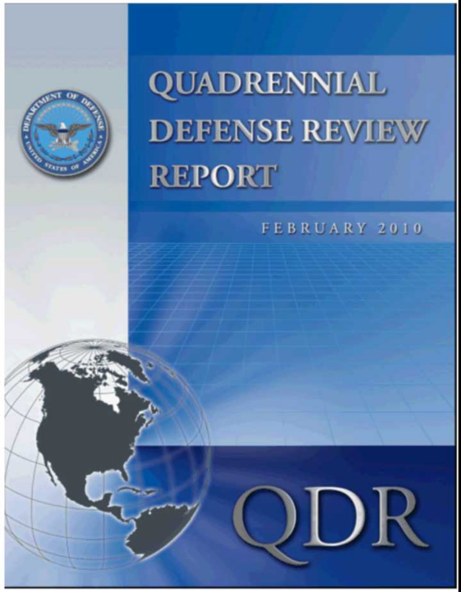

2006: a call for resilience




2009: resilience elevated to same level of importance as protection

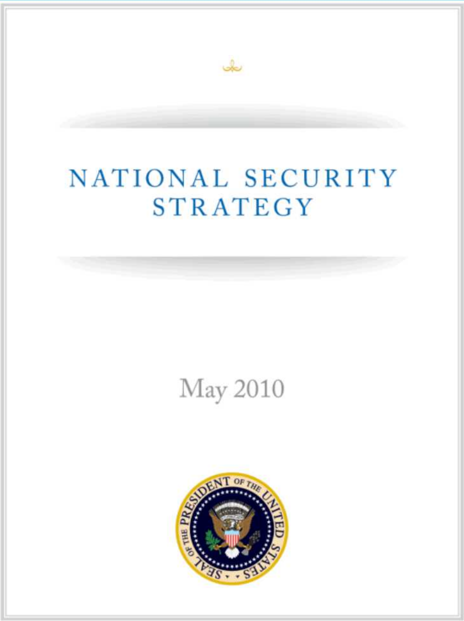



2010: Mission 5- "ensuring resilience to disasters"

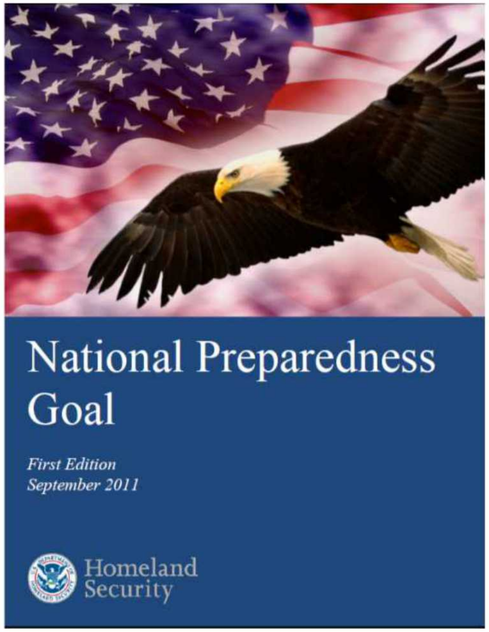



2010: "Increase the resiliency of U.S. forward posture and base infrastructure"

# Emergence of Resilience as National Security Priority (2)

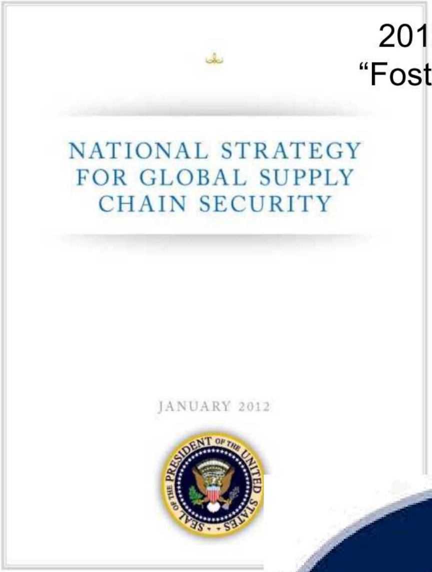



2010: advance US interests by "Strengthen[ing] Security & Resilience at Home"




2011: Definition of success- " a secure and resilient nation…"

Elements of preparedness include prevention, protection, mitigation, response, and recovery



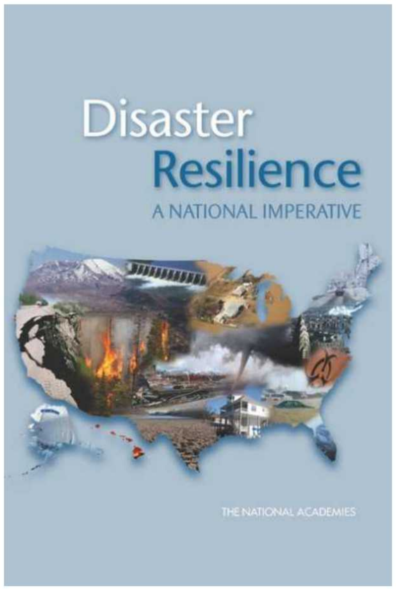

2012: Strategic goal 2 (of 2)- "Foster a resilient supply chain"

THE WHITE HOUSE
WASHINGTON

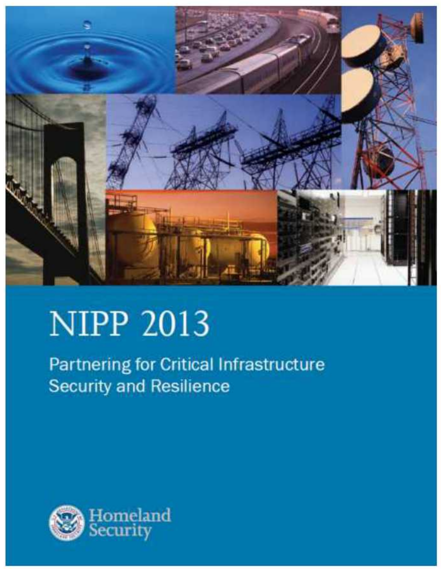
PPD-21 Critical Infrastructure Security & Resilience

2013: "advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure"

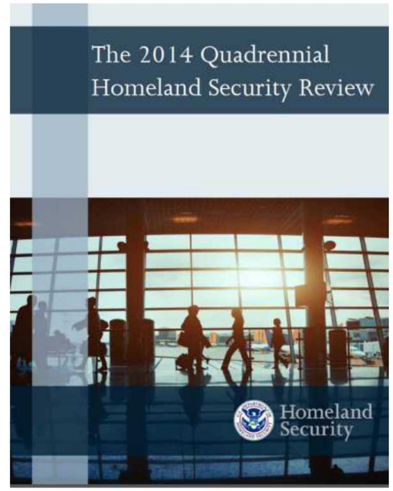
# Emergence of Resilience as National Security Priority (3)




2012: “recommendations about the necessary approaches to elevate national resilience to disasters in the United States”

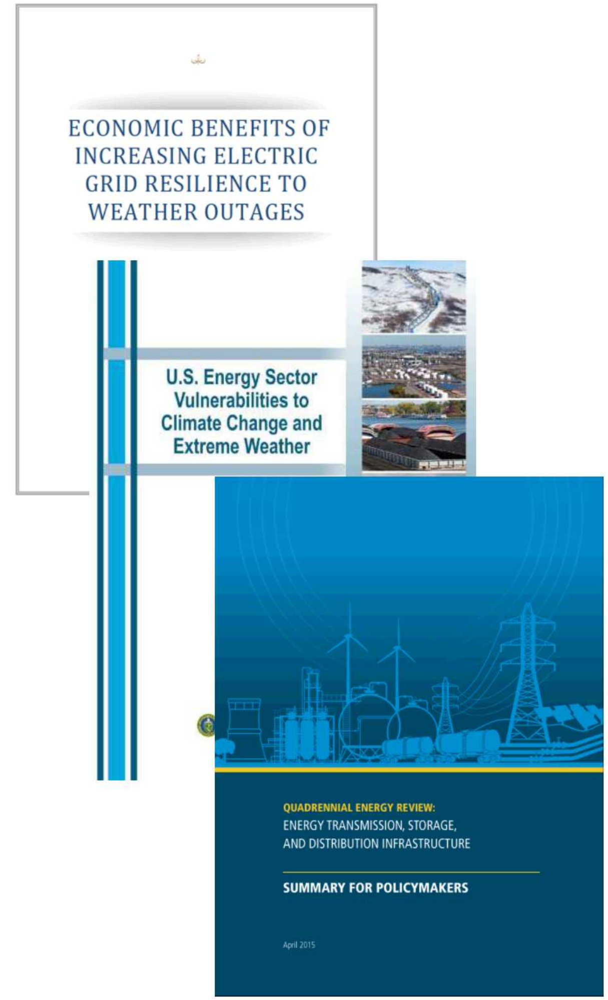



2013: Partnering for Critical Infrastructure Security and Resilience




2014: “a more focused, collaborative Departmental strategy, planning, and analytic capability”

2014 QDR has increased emphasis on resilience of space systems and supporting infrastructure




2013-2015: increased emphasis by DOE on resilience of the grid and energy infrastructure

# DOE Grid Modernization Initiative

- The Grid Modernization Initiative (GMI) works across the U.S. Department of Energy (DOE) to create the modern grid of the future. A modern grid must have:
  - Greater **RESILIENCE** to hazards of all types
  - Improved **RELIABILITY** for everyday operations
  - Enhanced **SECURITY** from an increasing and evolving number of threats
  - Additional **AFFORDABILITY** to maintain our economic prosperity
  - Superior **FLEXIBILITY** to respond to the variability and uncertainty of conditions at one or more timescales, including a range of energy futures
  - Increased **SUSTAINABILITY** through energy-efficient and renewable resources.

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

DOE Office of Electricity Delivery and Energy Reliability

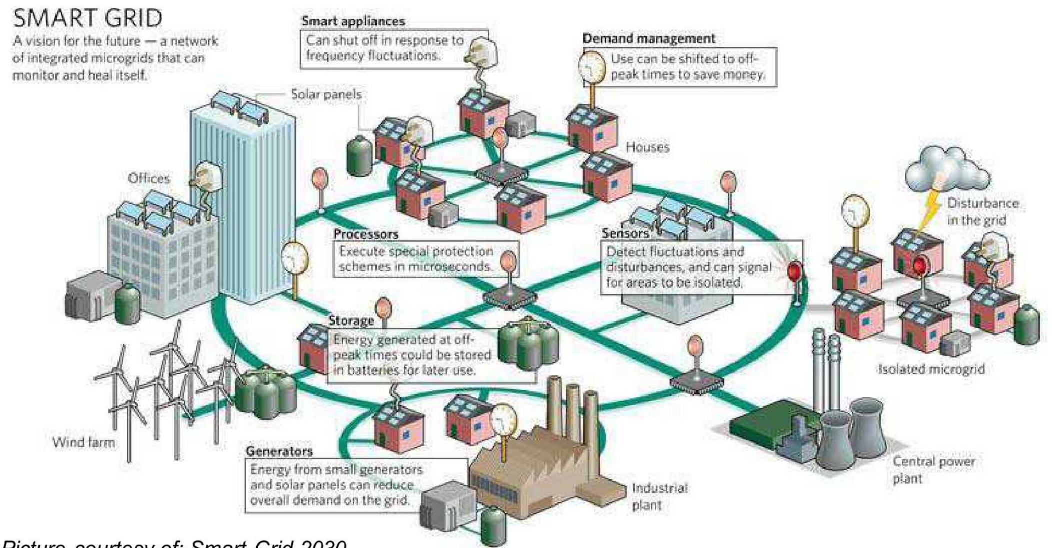
DOE Office of Energy Efficiency and Renewable Energy

DOE Office of Energy Policy and Systems Analysis

Grid Modernization Laboratory Consortium (GMLC)

# Sandia's Future Grid Vision

- *A world of interdependent and variable distributed systems that are optimized at multiple scales – including transmission – to maximize local resources in providing secure, resilient, and clean energy to all users at all times.*



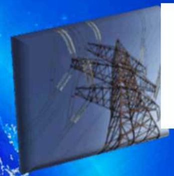

*Picture courtesy of: Smart Grid 2030*

*Our capabilities support this vision:*

- DER and renewable energy integration
- Power electronics and controls
- Secure and scalable microgrids
- Advanced grid analytics/complex systems
- Infrastructure interdependencies
- Cyber and physical security
- Embedded sensors, information processing, and secure manufacturing
- Energy storage systems

# Sandia's Grid Modernization Program Approach

Crosscut Initiatives



Transmission Planning & Operations

Renewable Energy & Distributed Systems Integration

Energy Storage

Defense Energy

Cyber and Physical Security

Grid Resilience

Microgrids

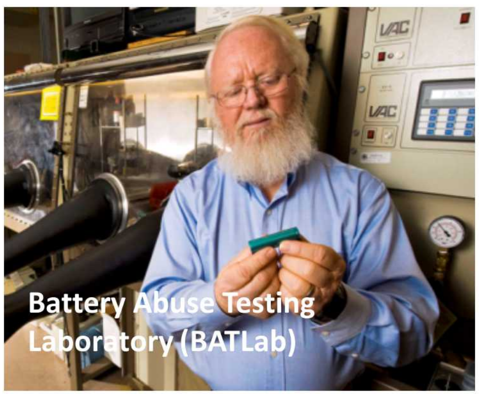
Grid Modernization Laboratory Consortium

Laboratory Directed Research & Development

# Sandia Labs & Facilities for Grid Mod Work



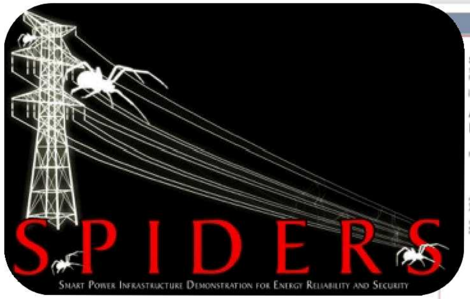




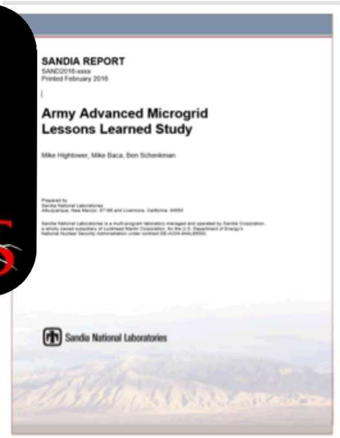

National Solar Thermal Test Facility




# Our Microgrid Work Began with Energy Assurance for Military Missions

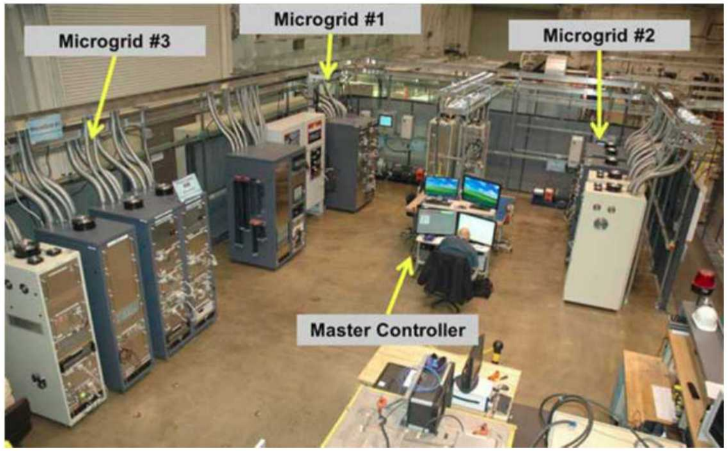



2015 JCTD TEAM OF THE YEAR AWARD


SANDIA REPORT

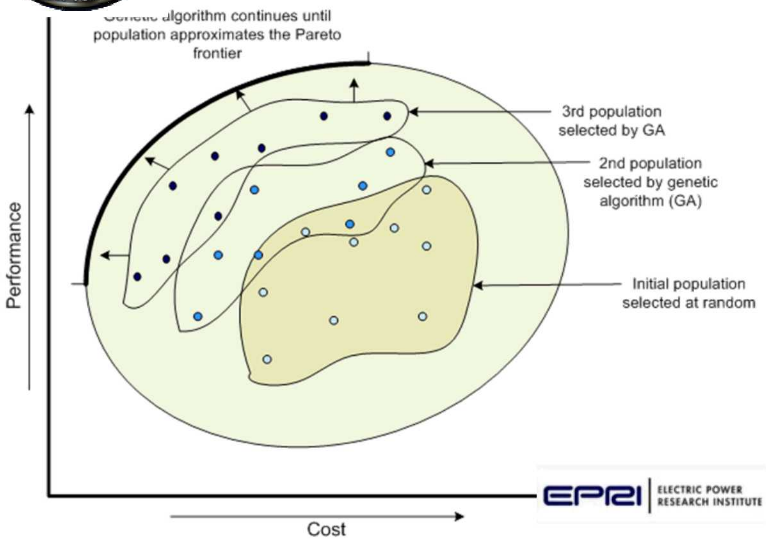
Army Advanced Microgrid Lessons Learned Study

Sandia National Laboratories

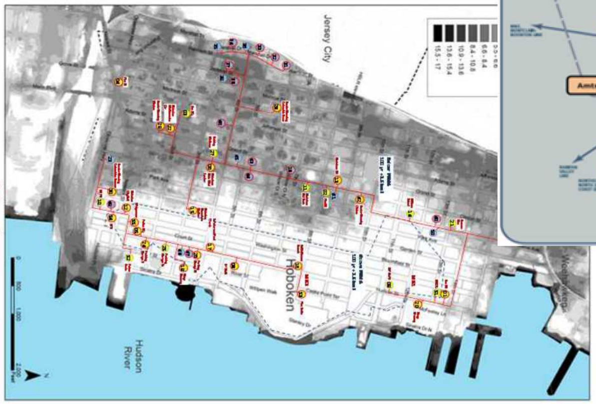


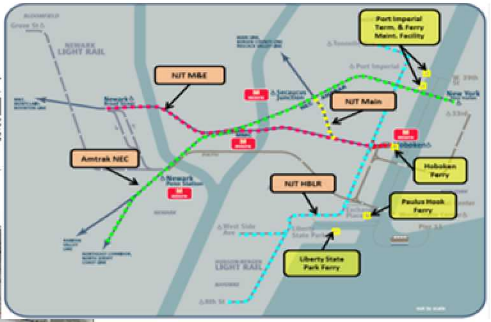

SECURE, SCALABLE MICROGRID GRAND CHALLENGE LDRD

SANDIA'S MICROGRID DESIGN TOOKIT




HOBOKEN NJ




NJ TRANSIT

# Defining Resilience

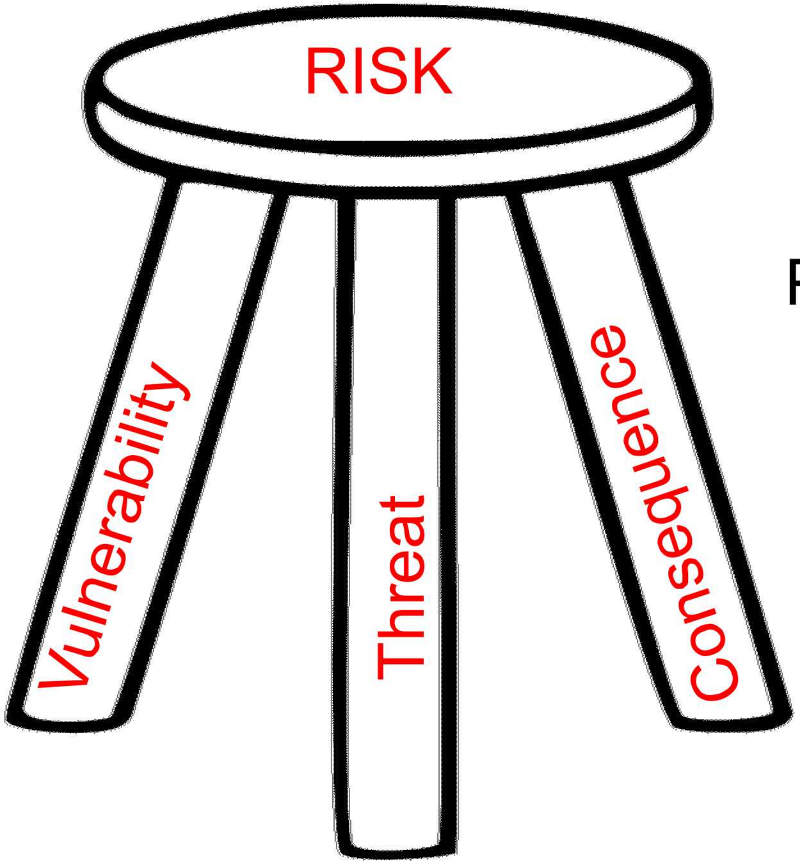
***"The term 'resilience' means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." -Resilience definition from PPD-21***

Sandia adds two words: "system" and "measure."

"Without some numerical basis for assessing resilience, it would be impossible to monitor changes or show that community resilience has improved. At present, no consistent basis for such measurement exists…"

*-Disaster Resilience: A National Imperative, National Academy of Sciences*

# Resilience: A Risk-Based Approach




Probability of Consequences =

f(vulnerability, threat)

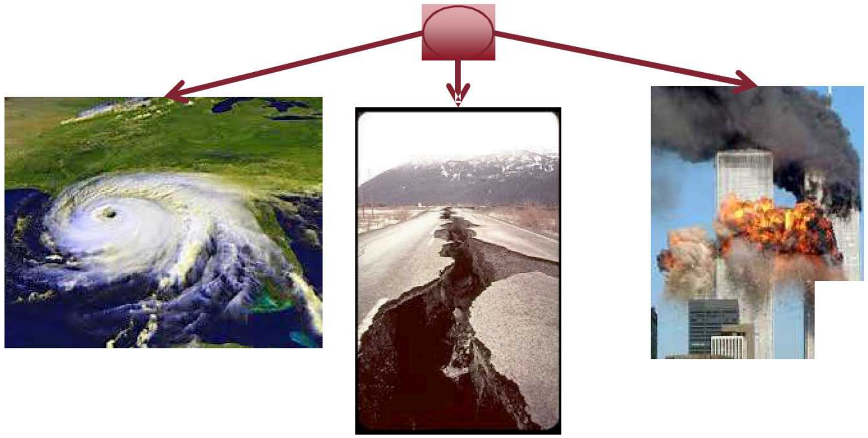
# Resilience versus Reliability

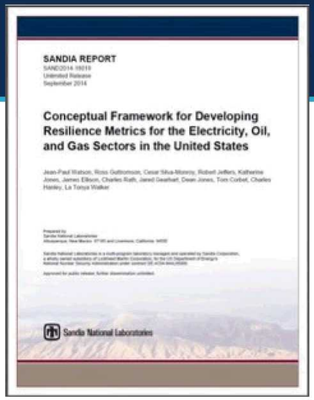
## Differentiating reliability and resilience is important

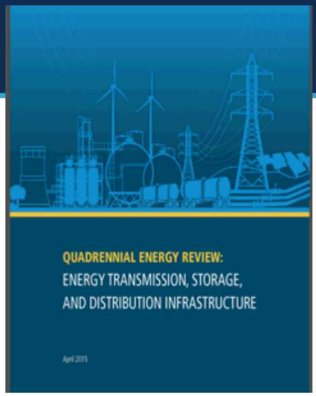
- Reliability is compulsory
- Reliability is related to rate recovery
- Adoption of resilience metrics will be easier if reliability definitions remain as-is

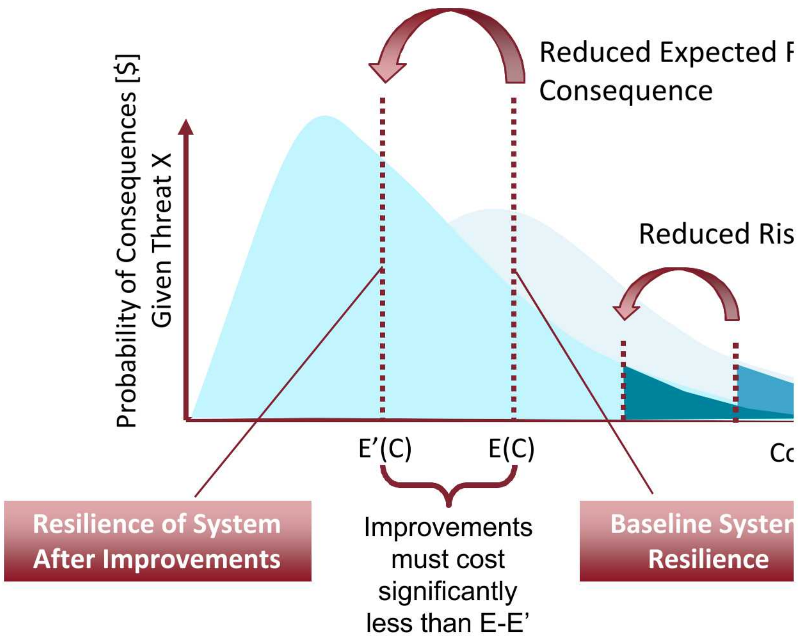
| **Reliability** | **Resilience** |
|---|---|
| High Probability, Low Consequence<br>(SAIDI/SAIFI exclude storm data) | Low Probability, High Consequence |
| Not risk based | Risk Based, includes:<br>Threat (you are resilient to something)<br>System Vulnerability (~reliability)<br>Consequence (beyond the system) |
| Operationally, You are reliable, or you are not [0 1]. Confidence is unspecified | Resilience is a continuum, confidence is specified |
| Focus is on the measuring impact to the system | Focus is on measuring impact to humans |

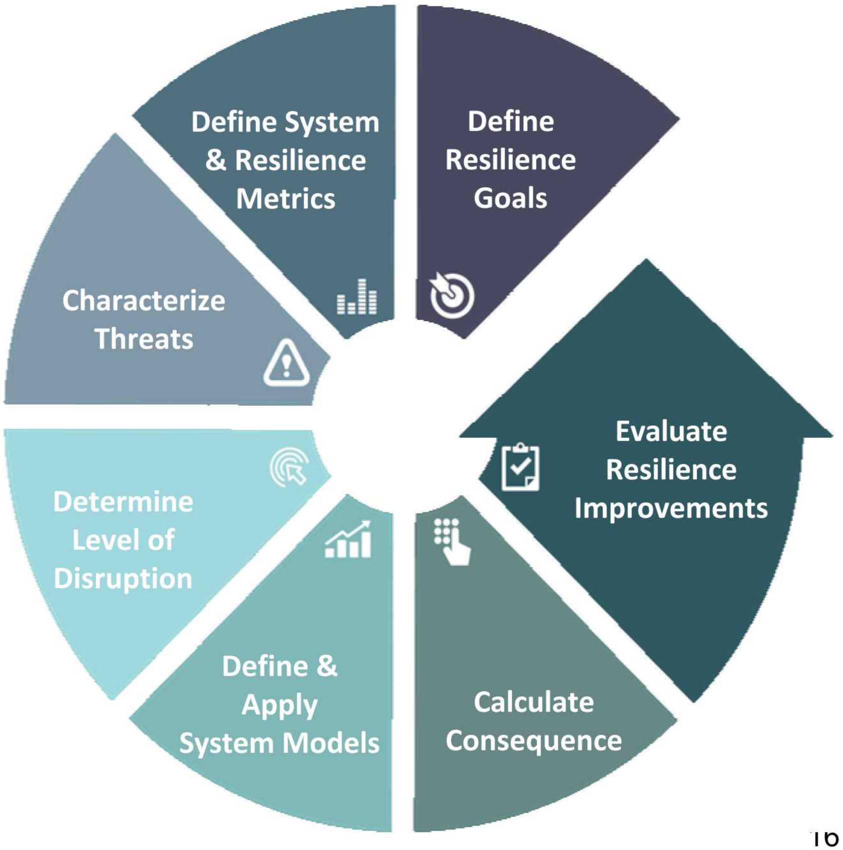
# Resilience Analysis Approach is Threat-Based, Rigorous, and Quantifiable



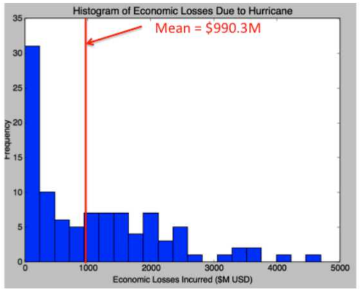


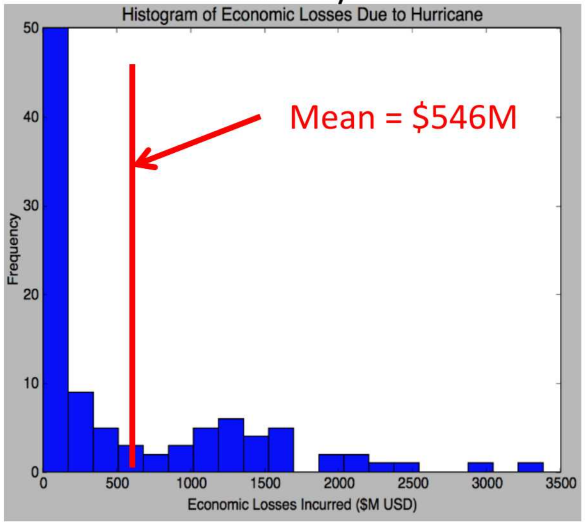
# Ex: How Should We Invest $100M for a resilient grid infrastructure?



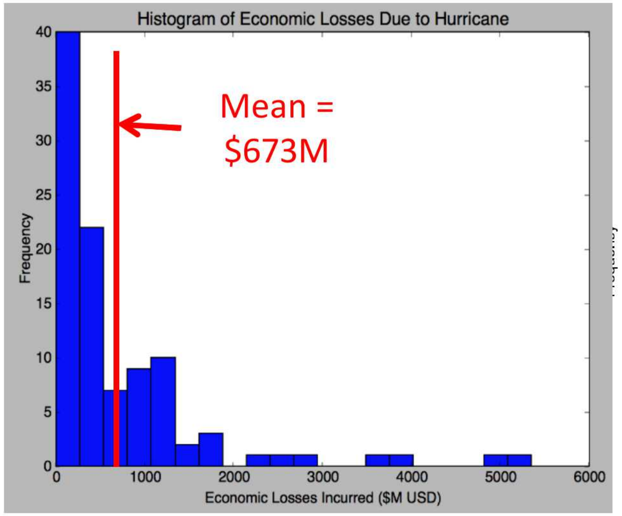

Baseline mean was $990M

Invest the same $100M in both flood walls and burying cables

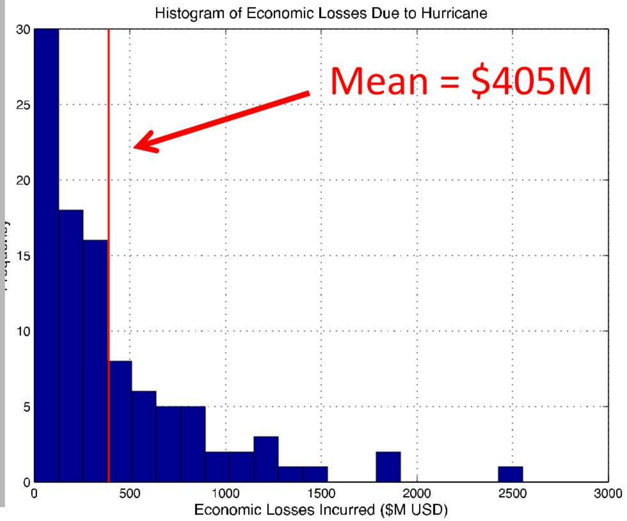
$100M of generator flood walls only




$100M of burying lines only

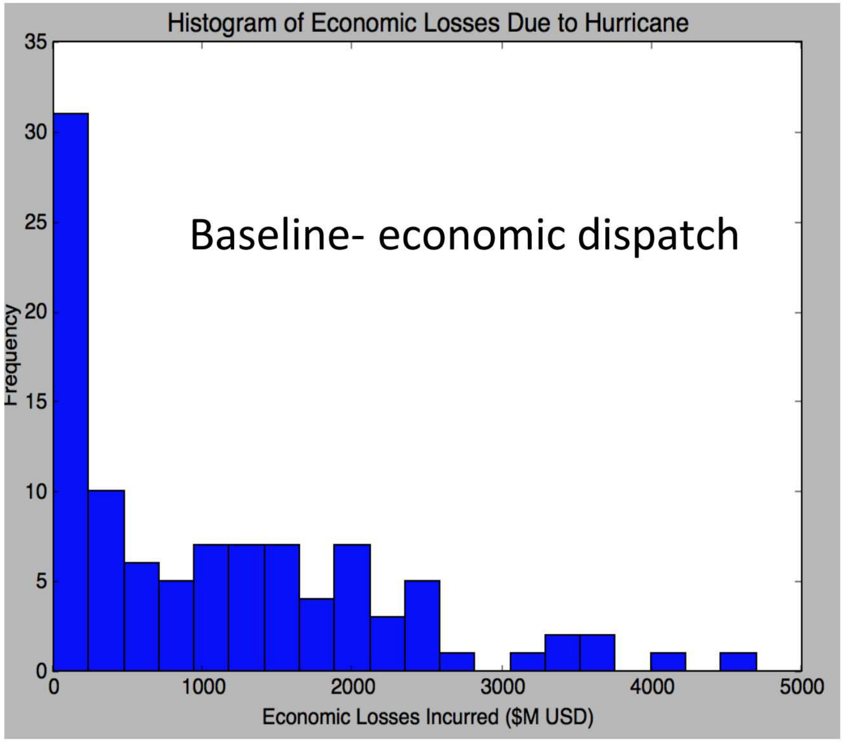



$100M of burying lines and generator flood walls

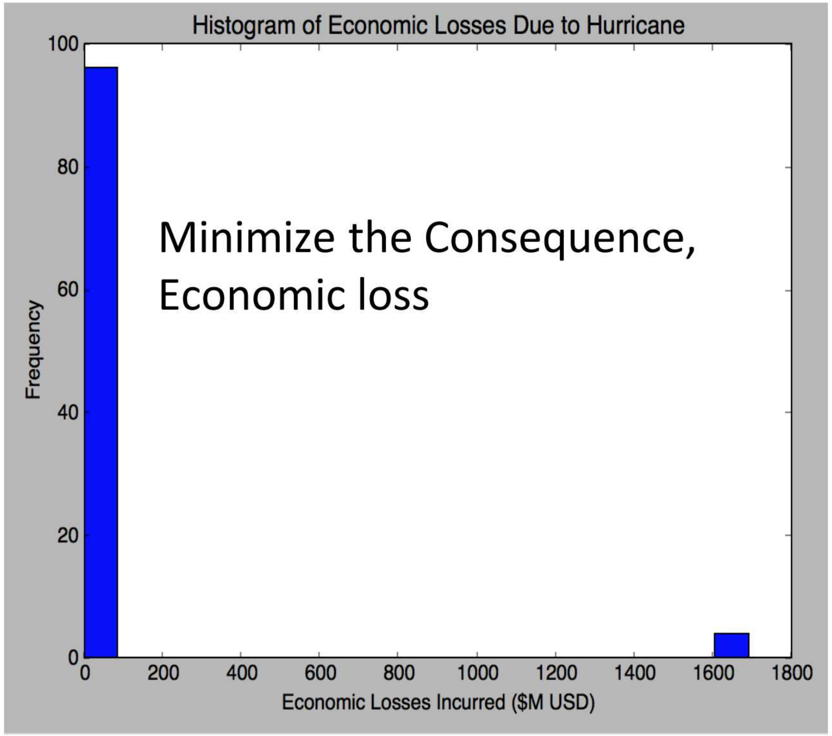



Simulations conducted as part of DOE's Quadrennial Energy Review, using IEEE 188-bus test case, to assess utility planning resilience to storms.

# What if we change the dispatch objective



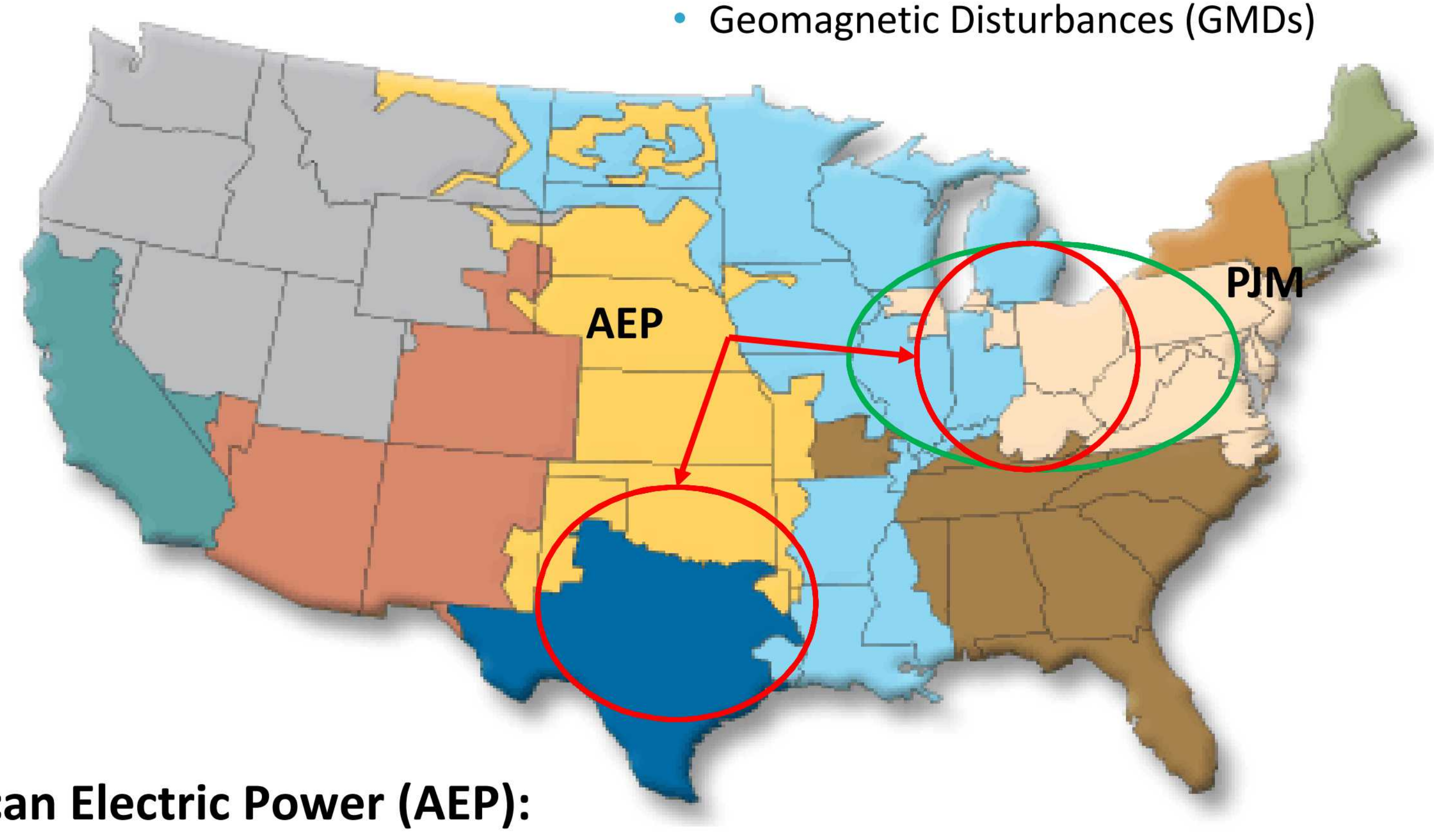

VS




In our IEEE 118 bus resiliency example, it is possible to mitigate nearly all economic consequences of the posited hurricane

# With Utility Partners, Testing the Value of Resilience Metrics and Analysis for Decision-Making

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

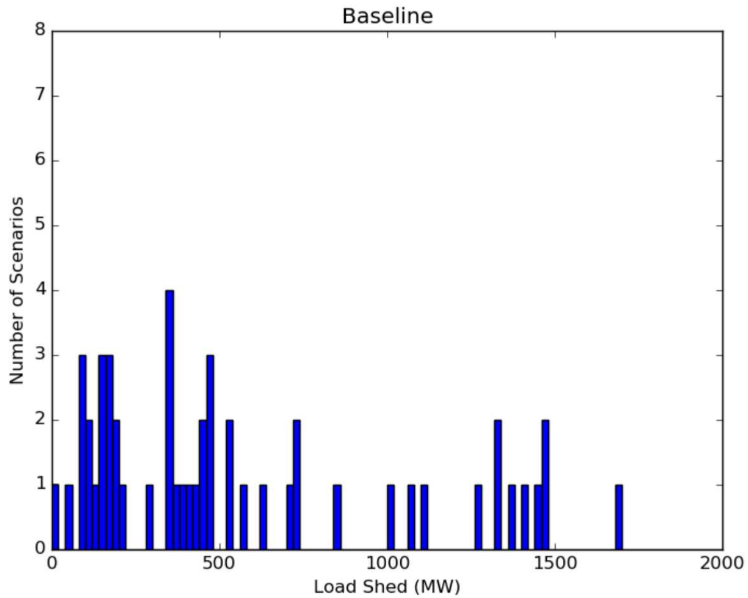


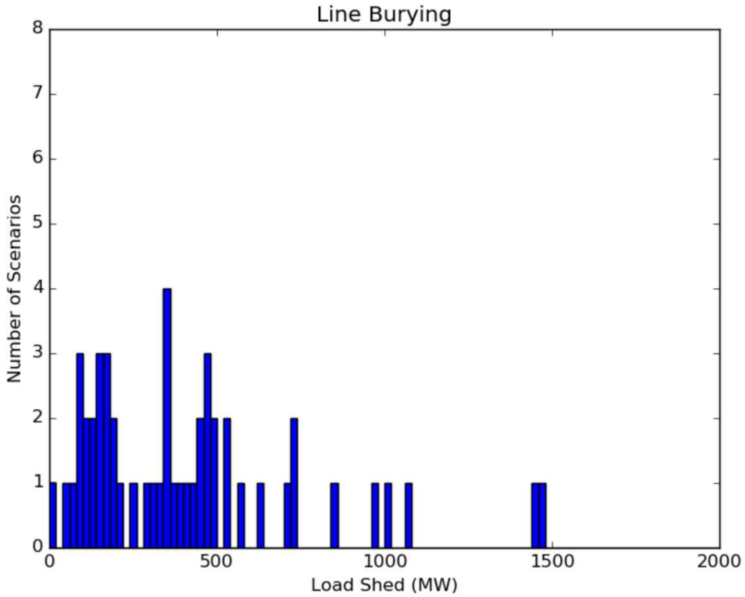

- **American Electric Power (AEP):**
  - Extreme weather (e.g., snow and ice storms)
  - Physical security threats (e.g., copper thieves and state actors)

# Extreme Weather Planning Preliminary Results

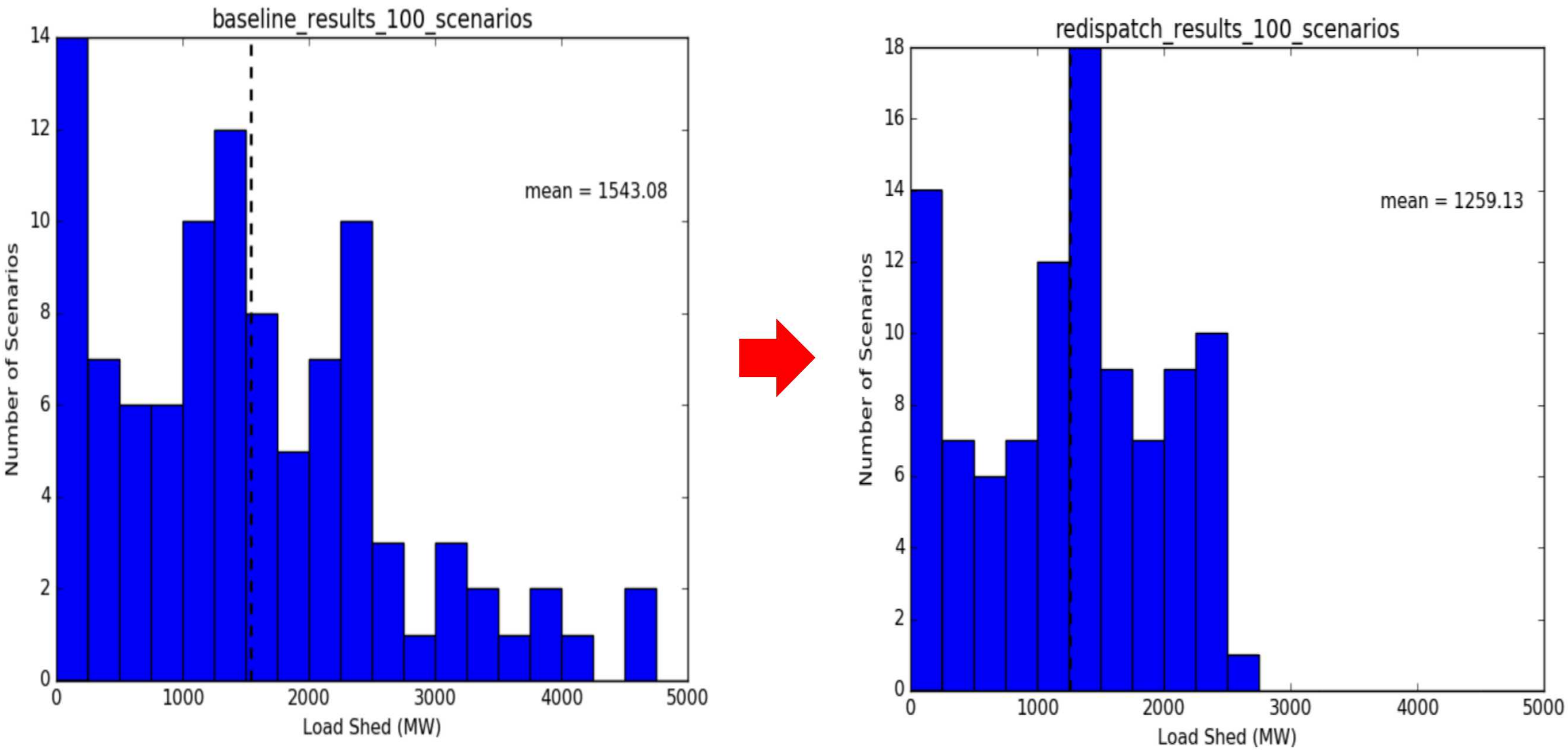
- **Objective**: Minimize load shedding when an outage due to a sudden loss of transmission lines (30 on average) occurs, represented by 50 scenarios
- **Constraints**: Generators ramping constraints, budget on number of lines buried
- **Decision Variables**: Lines to bury, generation dispatch before the contingencies occur

Load shedding decreased from 600 MW to 400 MW



# Resilience to Extreme Weather: Baseline versus Proactive Redispatch



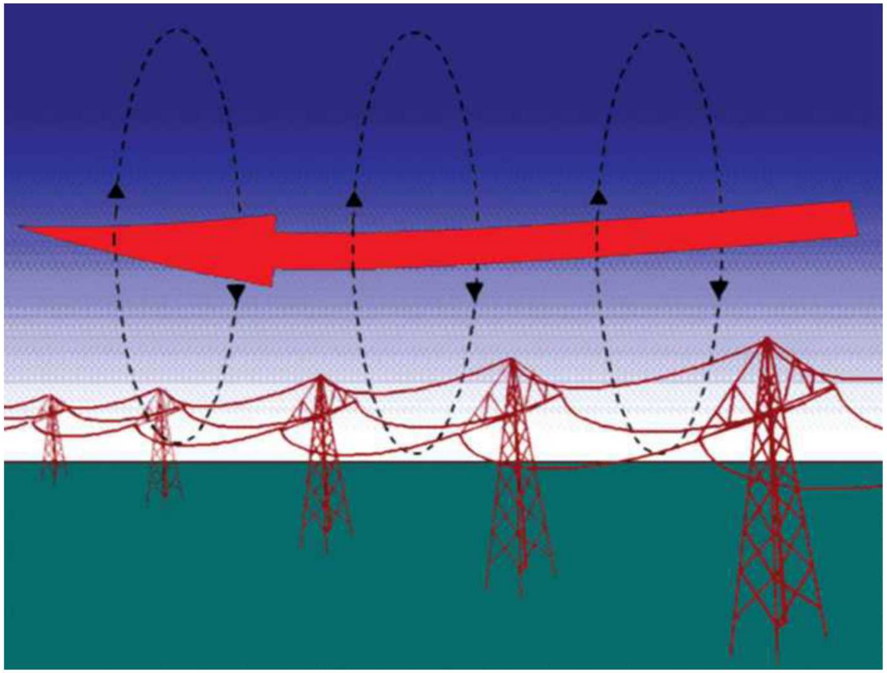

Simply re-dispatching generation in advance of a storm can significantly reduce consequences (as quantified by load shed)

*Note: conservative results did not use any a-priori knowledge of impending weather*

# GMD Effects on the Grid

- Electrojets perturb earth's geomagnetic field, inducing voltage potential at earth's surface and resulting in **geomagnetic induced currents (GICs)** in the grid

- Grid risks:
  - Damage to bulk power system assets, typically transformers
  - Loss of reactive power support which could lead to voltage instability and power system collapse

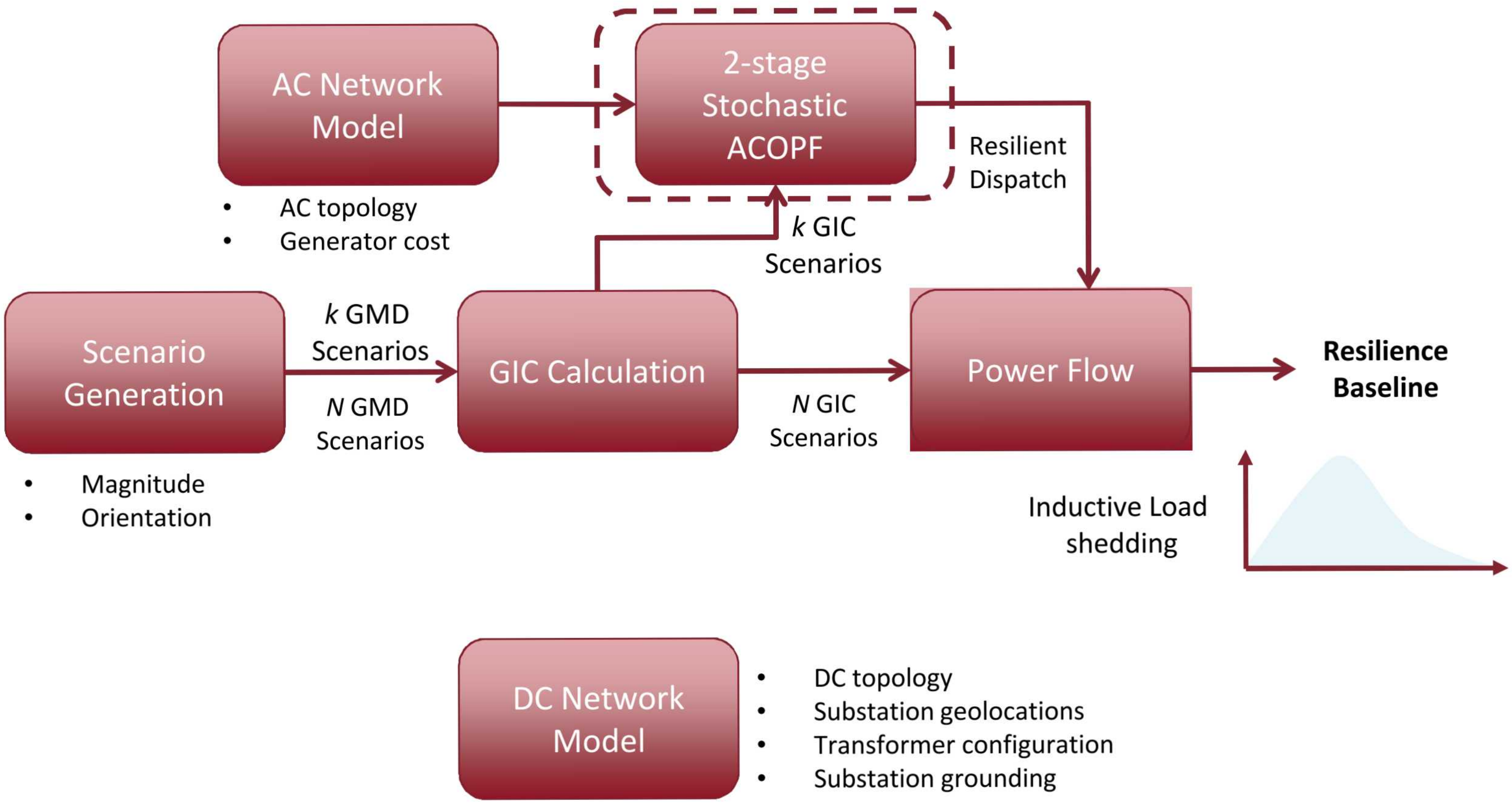


*Magnetic coupling between electrojet and power transmission line*

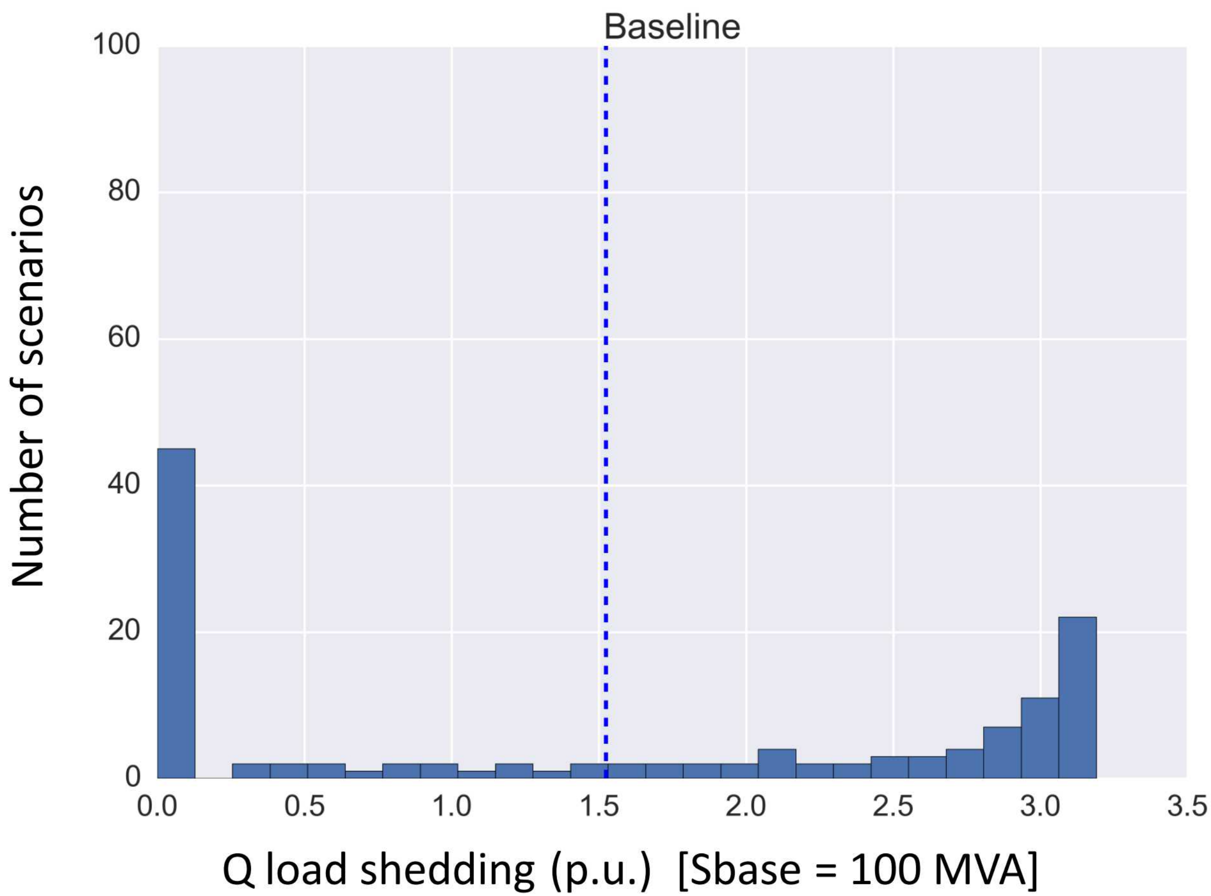
Source: D. Boteler, "Geomagnetic effects on power systems". IEEE Electrification magazine, pp. 4-7, Dec. 2015

# GMD Grid Resilient Performance

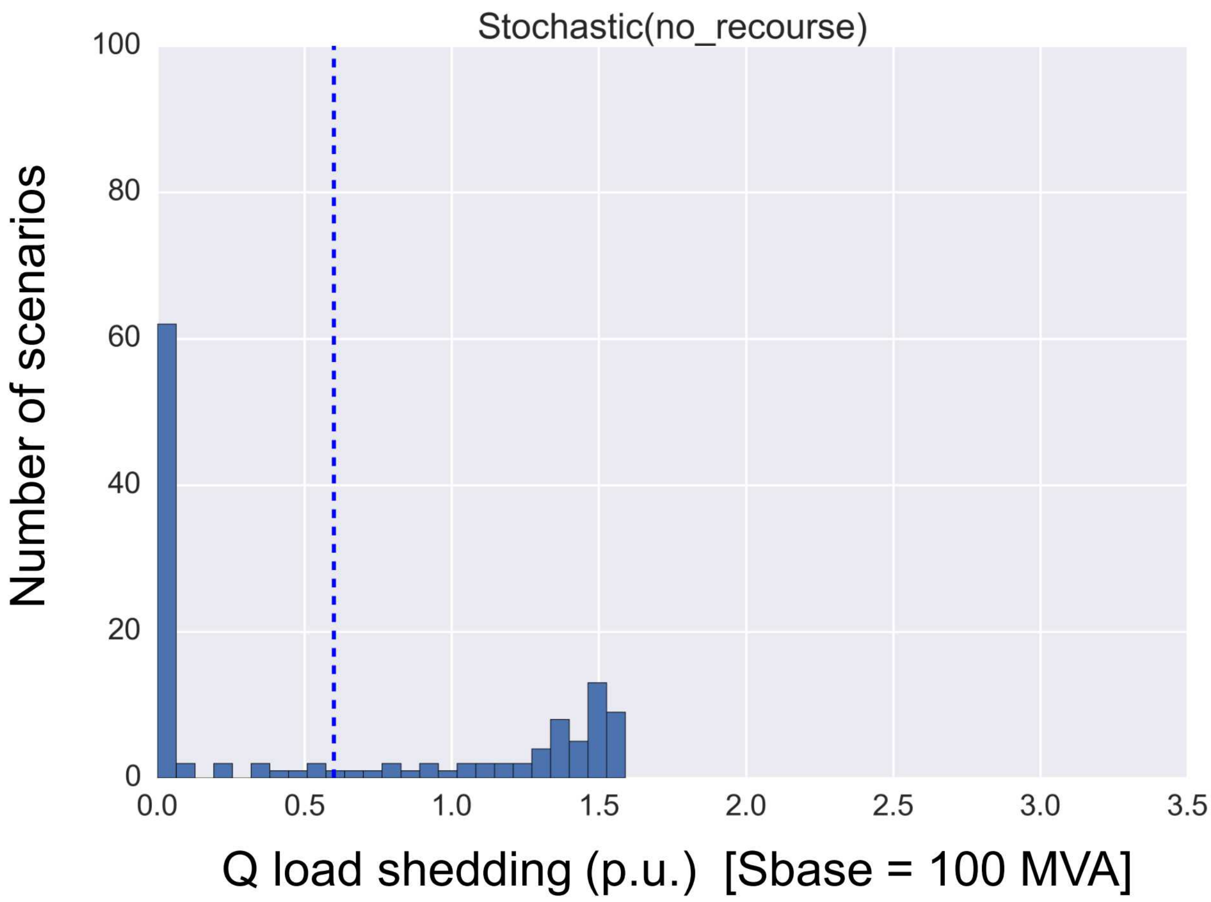
By switching from an economical operation to a resilience-based operation we are able to reduce the probability of system voltage collapse due to a GMD



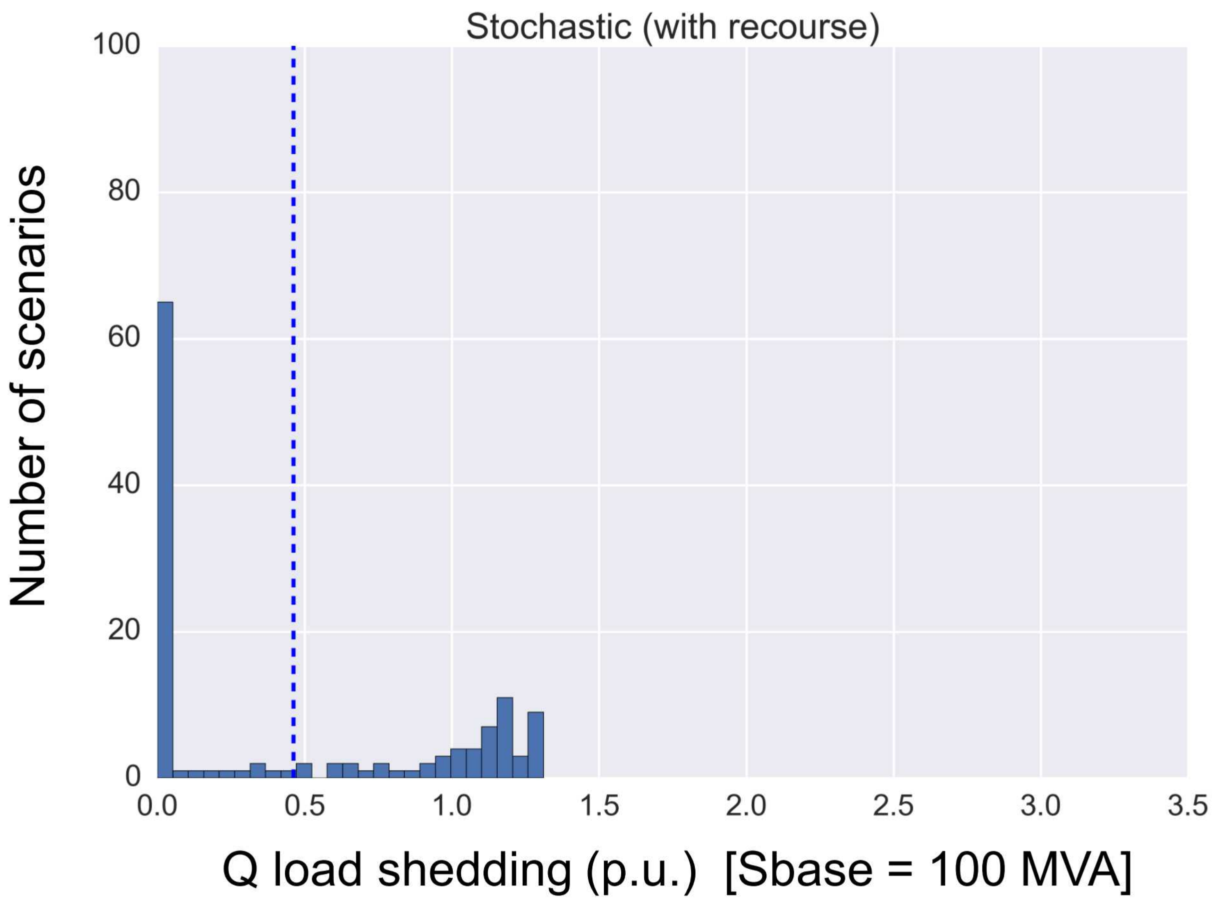
# 20-Bus Test Case – Baseline



# 20-Bus Test Case – Stochastic (no recourse)

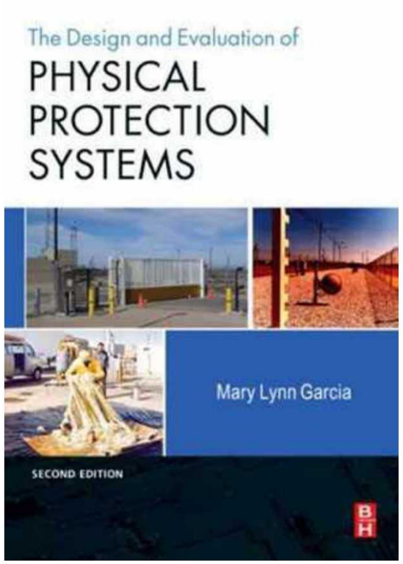


# 20-Bus Test Case – Stochastic with Recourse



# Goals for Physical Security Model

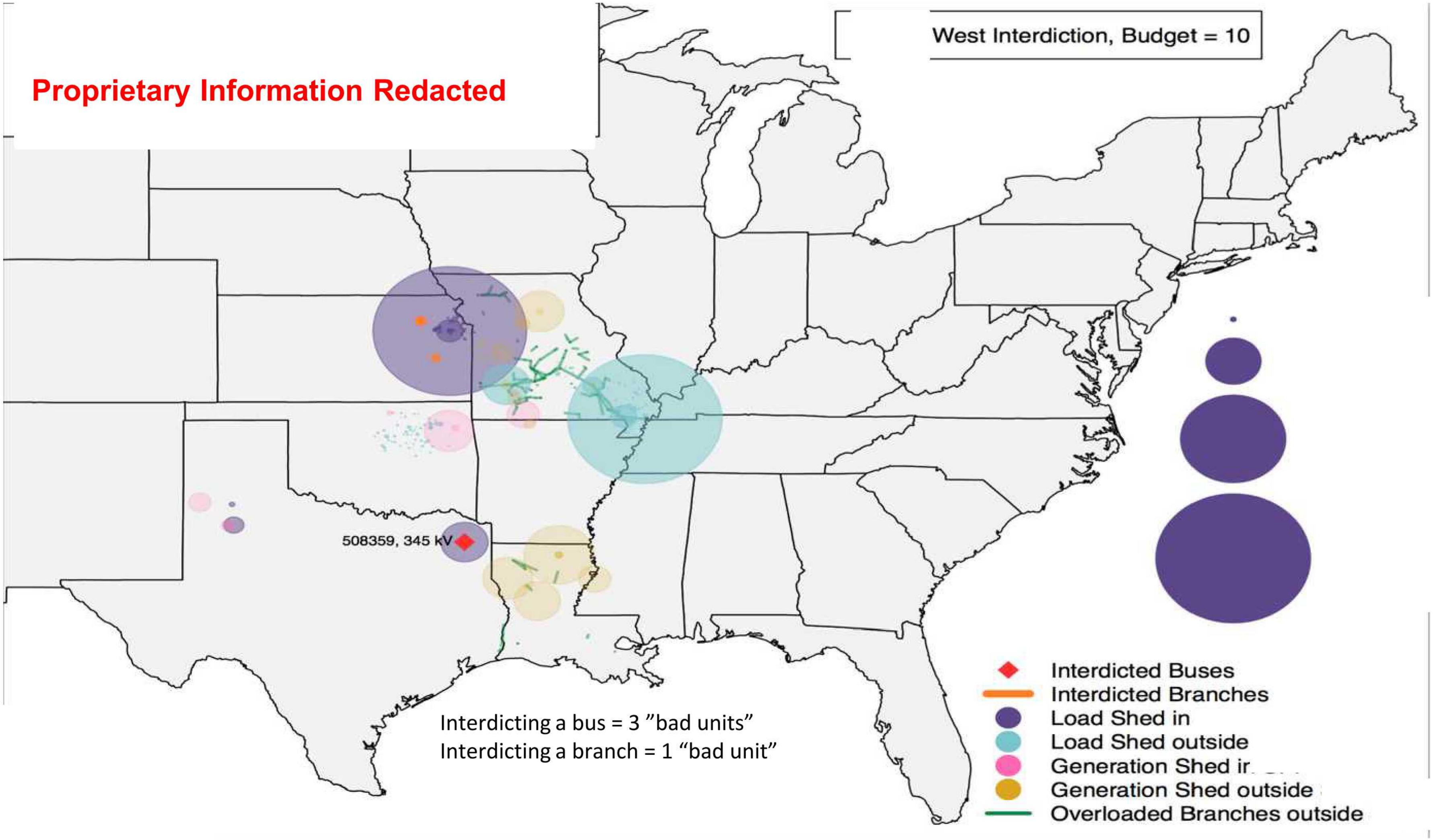
- Prioritization system-wide security investments
  - Consider investments across multiple sites
  - Consequence Metrics include **deterrence, detection,** and **delay**
  - Investments must impact one or more of those three categories




- Include lifecycle cost and address uncertainty around benefit
- Provide an optimal multi-year investment plan across sites given limited resources, focusing on performance for the highest priority locations (e.g. specific substations)

| Systems-level Analysis | Evaluation of Criticality | Design Recommendations |
|---|---|---|

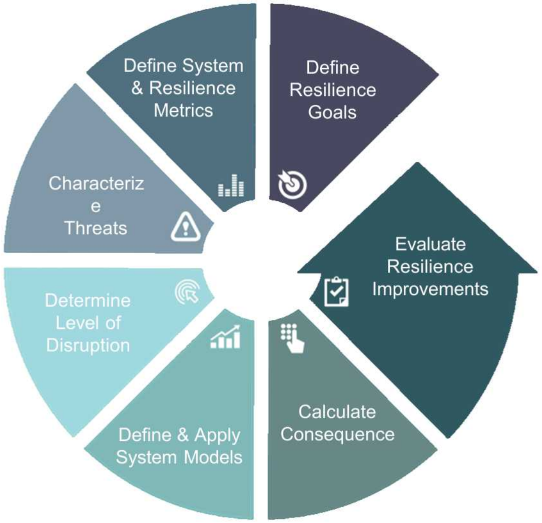
# Model Shows Optimized Impacts Based on Interdiction Budget – Preliminary Results

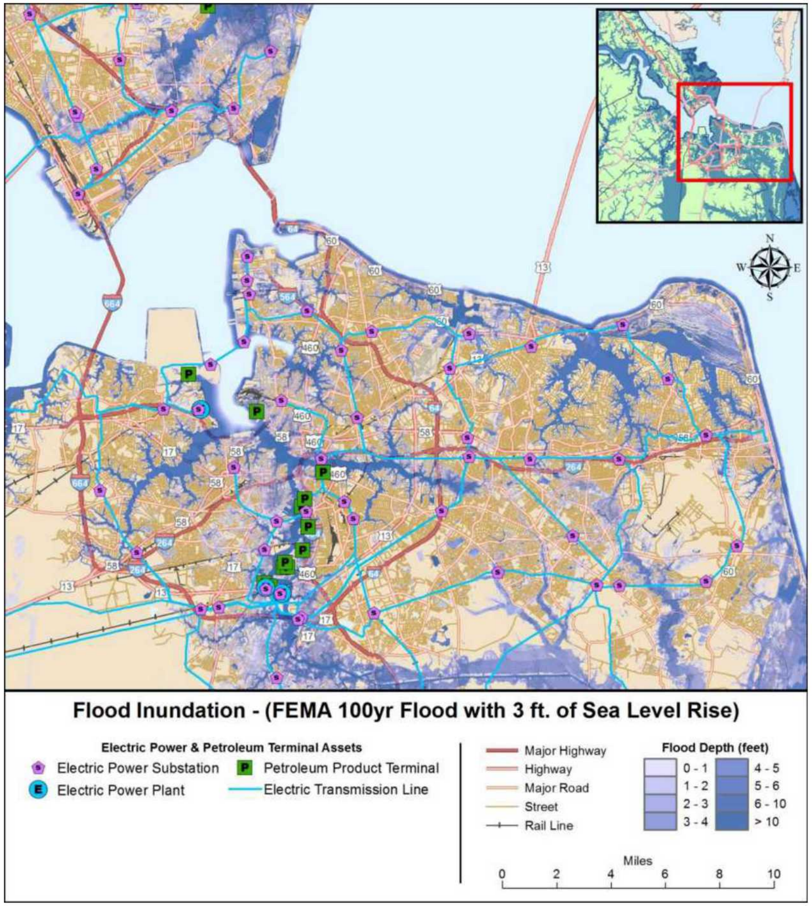



Interdicting a bus = 3 ”bad units”
Interdicting a branch = 1 “bad unit”

# Application of Sandia Resilience Methods to the City of Norfolk, VA

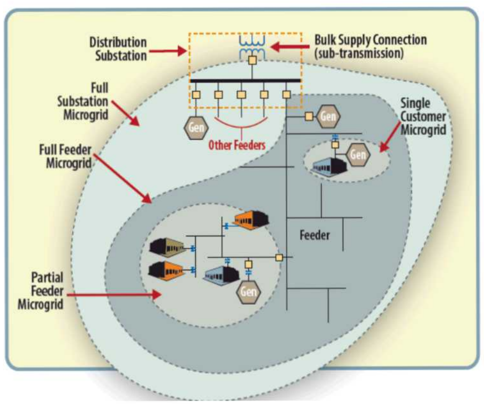
- Design Basis Threat (DBT): 100 Year Flood +0ft, +1.5ft, +3ft
- Scope: power, fuel, communications and transportation systems
- Applied analysis principles to identify and compare resilience enhancement options

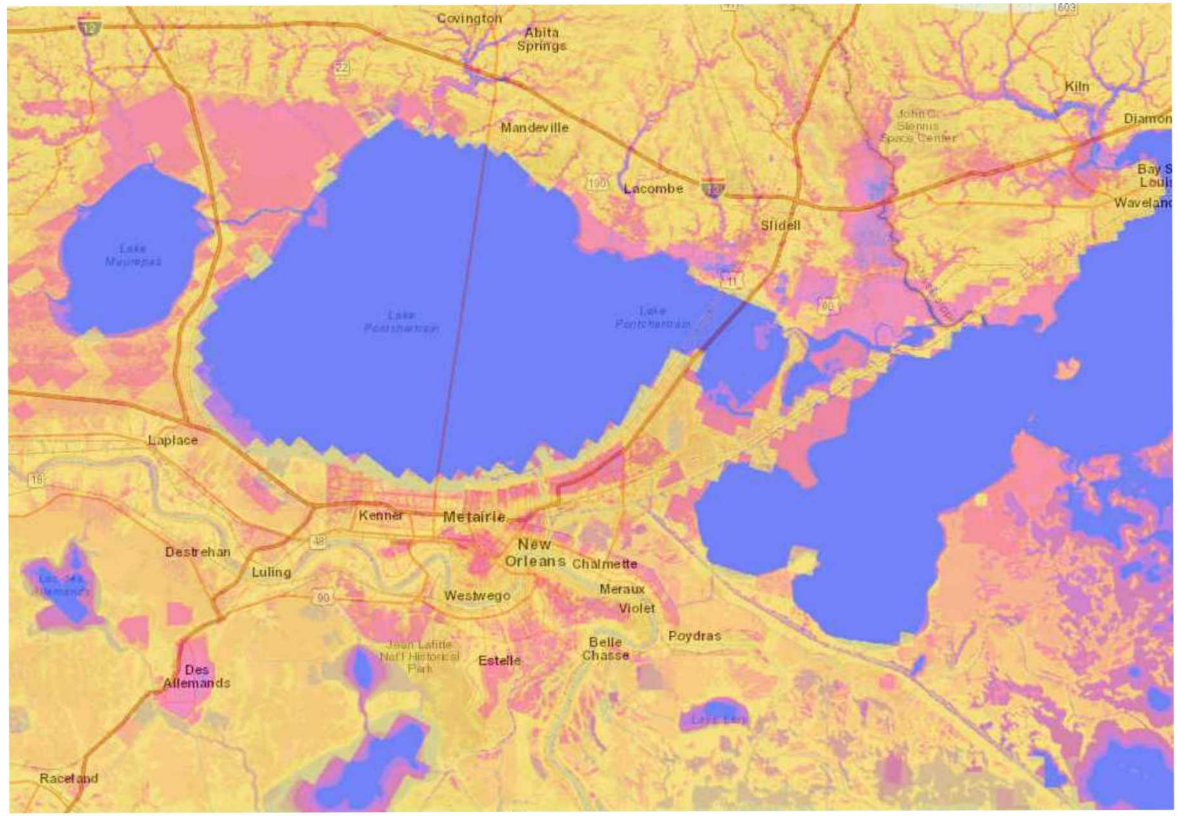


# Case Study: New Orleans, LA

GRID MODERNIZATION LAB CONSORTIUM

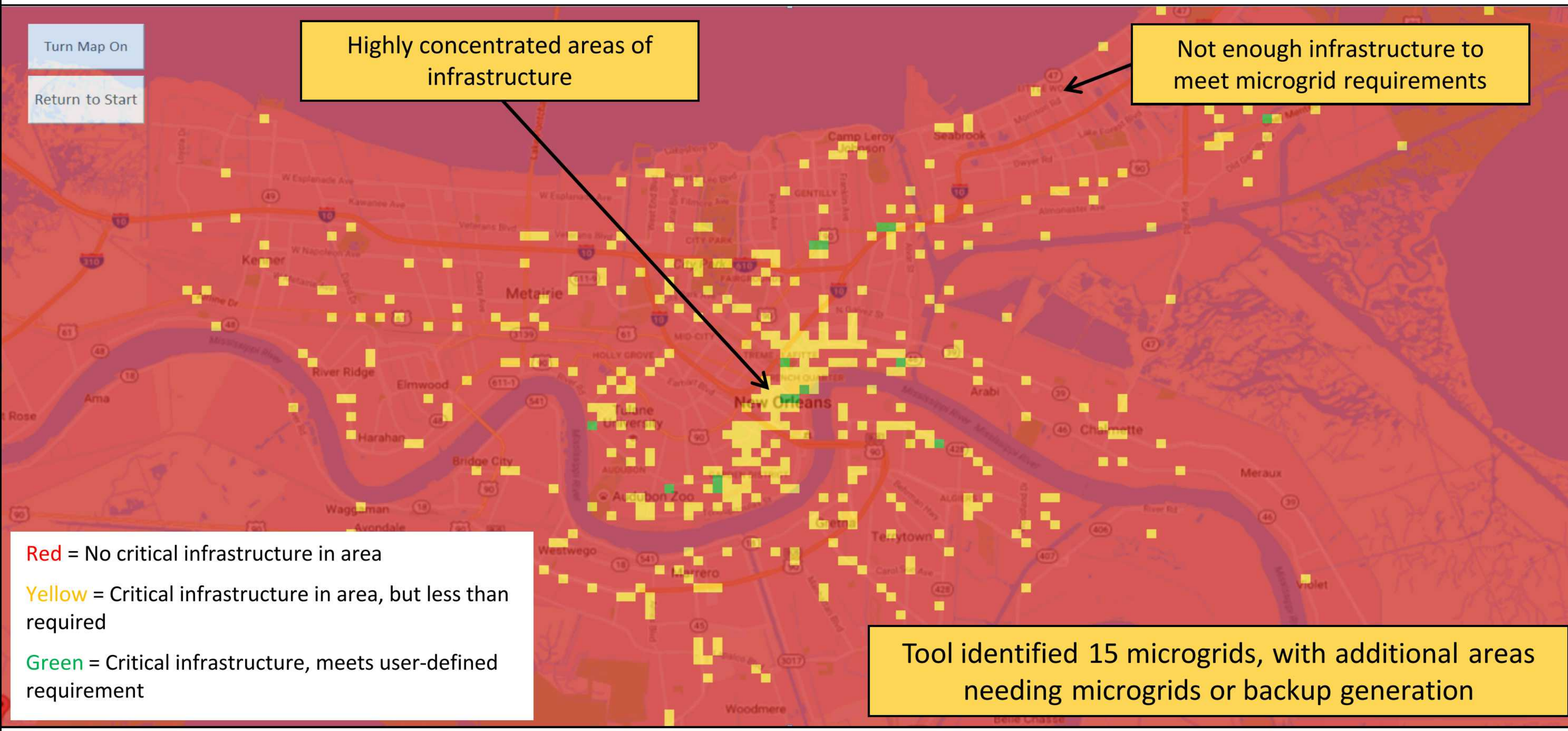



*Results of Hurricane Inundation Modeling for New Orleans and surrounding regions*

- **New Orleans:** 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.

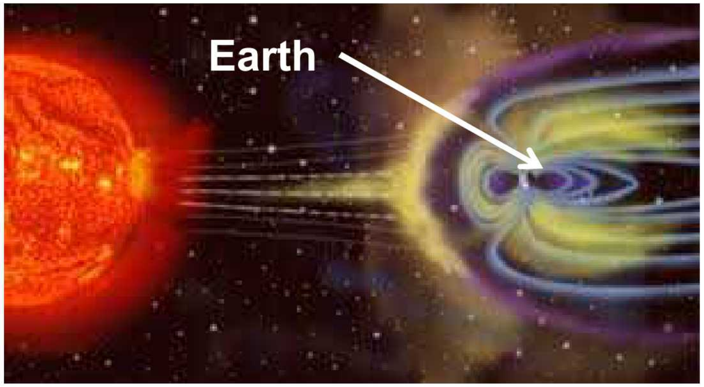
# New Orleans Microgrid Screening

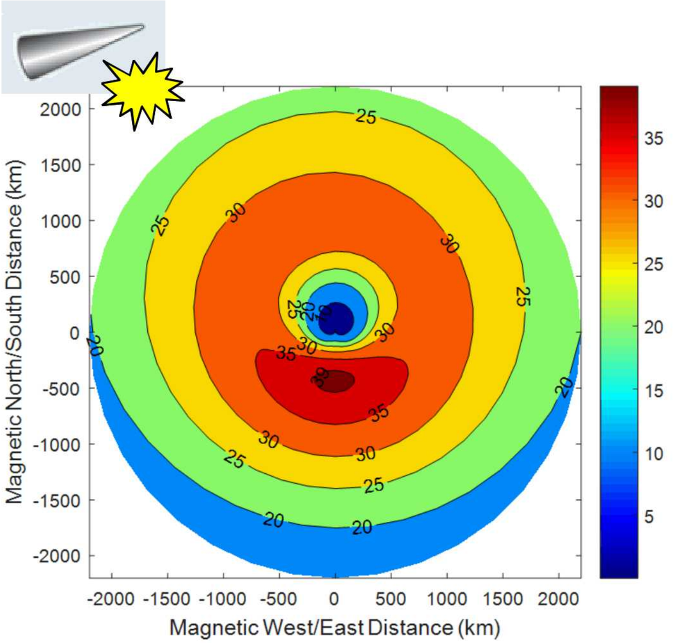



Area size of 1000 ft x 1000 ft | minimum of 4 buildings per microgrid

# EMP Threats

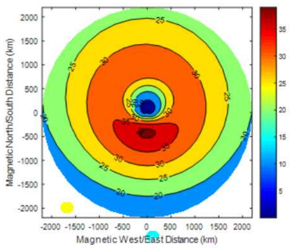
- **Geomagnetic disturbance**
  - Solar mass ejections generate variations in the Earth's magnetic field
  - **Induced power line currents can saturate and damage transformers**
- **Nuclear weapon detonation**
  - Ionizing radiation output *creates* a non-ionizing radiation environment at the Earth's surface
  - Large geographic coverage for a high altitude explosion
  - Electromagnetic fields have both space and time dependencies
- **Directed energy sources**
- **More…**



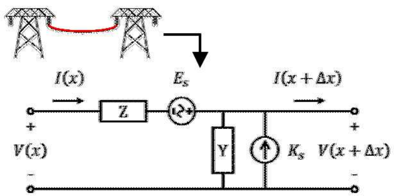



# Sandia’s Lab-Directed R&D Approach: Three Integrated Thrusts

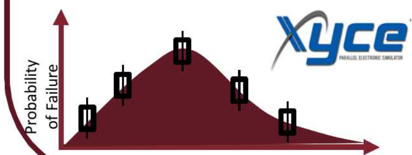
## Thrust 1
## Vulnerability Assessment




Environments

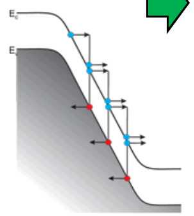



Coupling



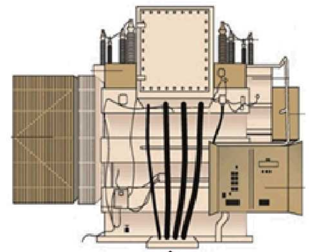

Failure Analysis

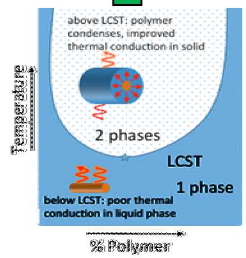
## Thrust 2
## Material & Device Innovation



Avalanche Breakdown in a Wide Band-Gap diode

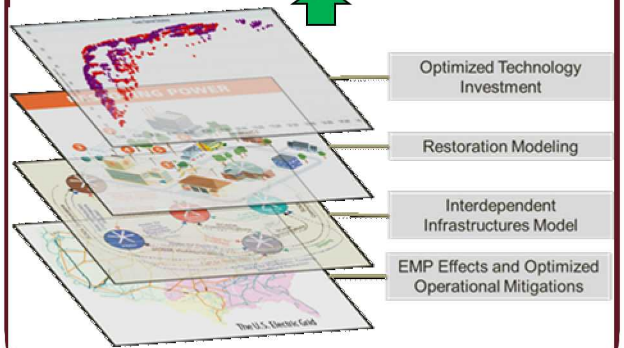
EMP hardened assets






Design New Component Materials to Withstand EMP Effects

## Thrust 3
## Optimal Resilience Strategies


Modular Multi-Layered Modeling Approach

### R&D

- Large scale coupling modeling with significant number of unknowns
- Component response and failure estimation to EMP waveforms

### R&D

- Develop Wide Band-Gap EMP arrestor
- LCST Polymers for thermal management during E3/GMD

### R&D

- Baseline assessment of EMP Effects w/ Large Scale Stochastic, AC Dynamic Optimization
- Risk mitigation by Tech Deployment, Operational Mitigation & Optimal Restoration

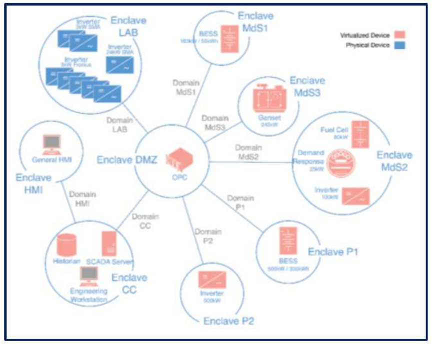
Georgia Tech — Research at Purdue — EPRI — Los Alamos National Laboratory EST. 1943

# Sandia's R&D on Cybersecurity for the Electric Grid

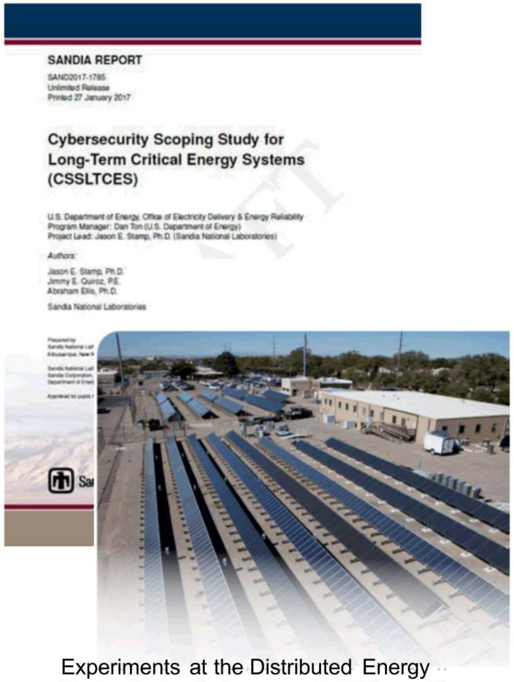
*Energy enables our way of life. Digitization of energy generation and distribution is growing and must be protected from cyberattack.*

Sandia's grid cyber and resilience efforts address all aspects of the NIST Cybersecurity Framework:

- ***Identify:*** Situational awareness, risk management and consequence analysis
- ***Protect:*** Supply chain integrity
- ***Detect:*** Firmware intrusion detection
- ***Respond, Recover:*** Adaptive system architectures; moving-target defense
- Tools: Emulytics™, SCEPTRE™, Weaselboard

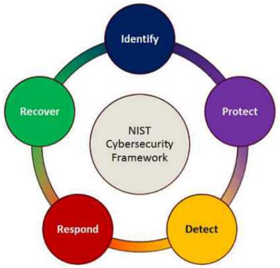



Sandia's Cyber Reference Architecture enclaves distributed energy devices to minimize vulnerabilities.



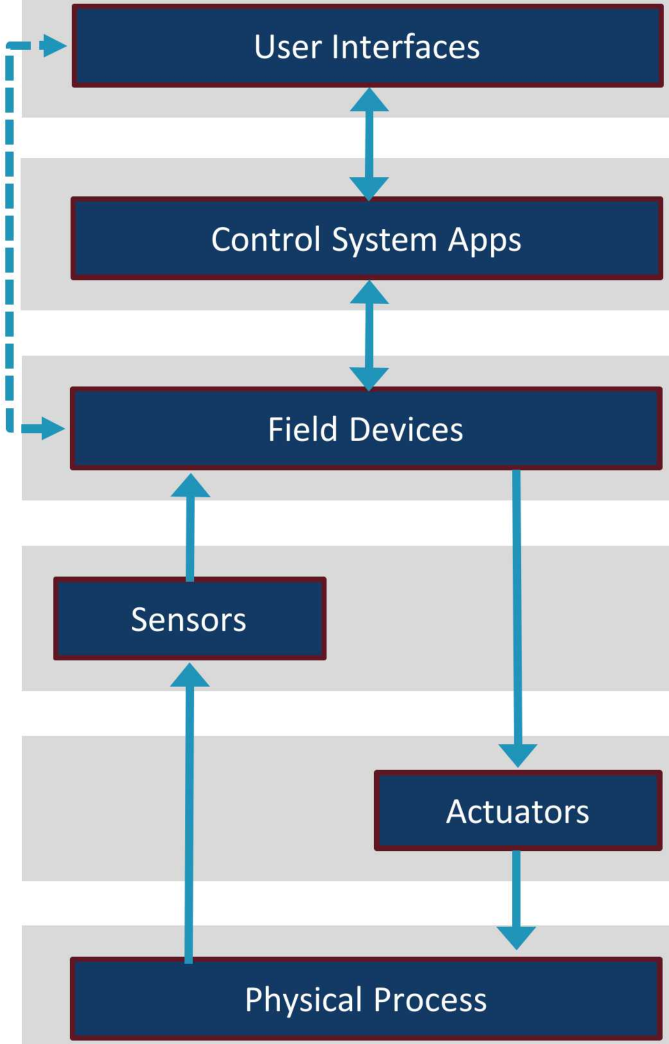

Experiments at the Distributed Energy Technologies Laboratory (DETL) provide new technologies and inform the community.

As Sandia engineers develop new grid communications and control technologies, cybersecurity is built in from the start




**We combine deep expertise in cyber defense with technology leadership in the evolving grid to address the toughest national cybersecurity issues.**

# 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

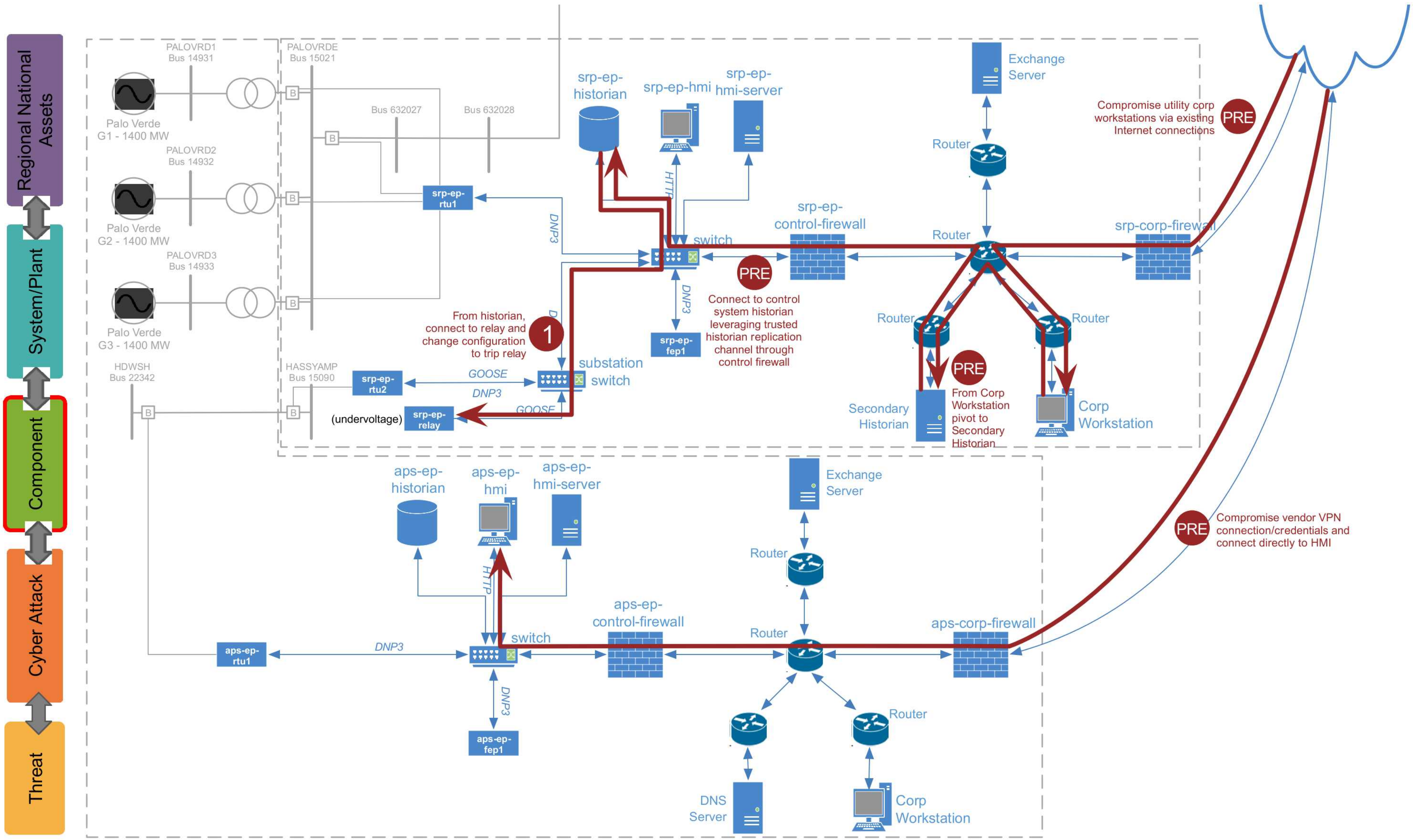
Thermocouples
Accelerometers
Photoresistors

Breakers/Switches
Motors
Valves

Oil & Gas Refining
Electrical Distribution and Transmission
Manufacturing

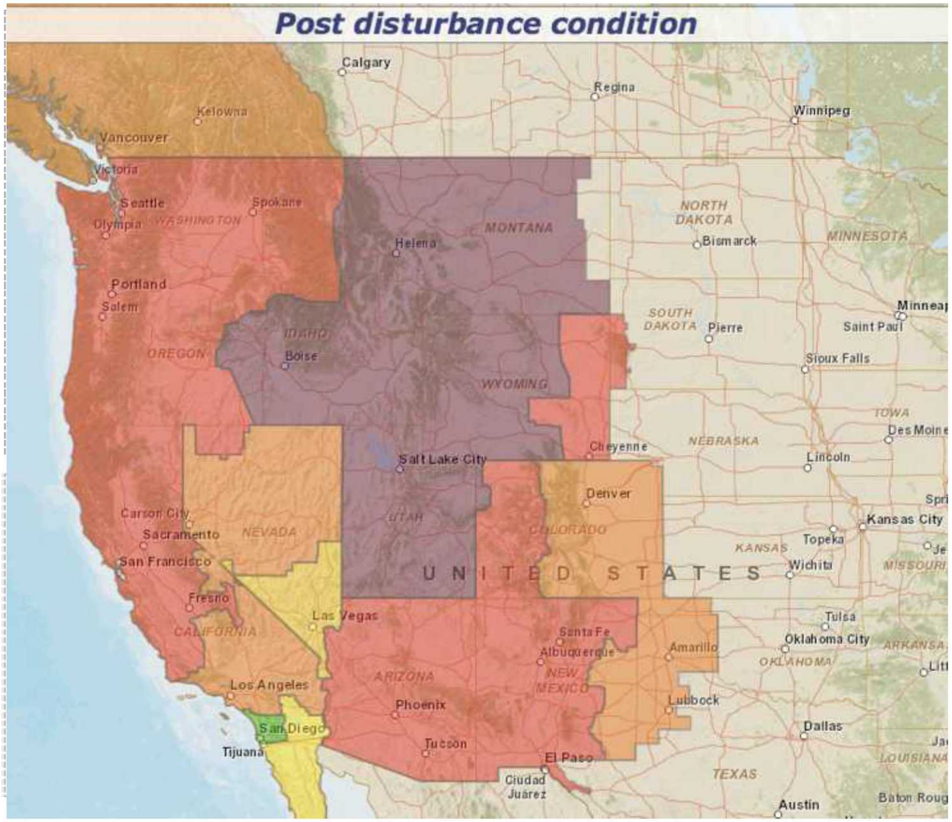
# Integrated Cyber Physical Grid Model

## *Attack Execution (Step 1) – Transmission Scenario*



# We Explored a Full-scale Simulation of a Cyber Attack on the Western US Grid






- Assets of 4 major power providers
- Extensive prepositioning (3 insiders)
- Multiple steps in execution (6 coordinated steps)

Consequence models employed Sandia's FASTMAP tool and expertise in DHS' National Infrastructure Simulation and Analysis Center (NISAC)

# Recommendations for Critical Energy Systems Cybersecurity

Sandia National Laboratories

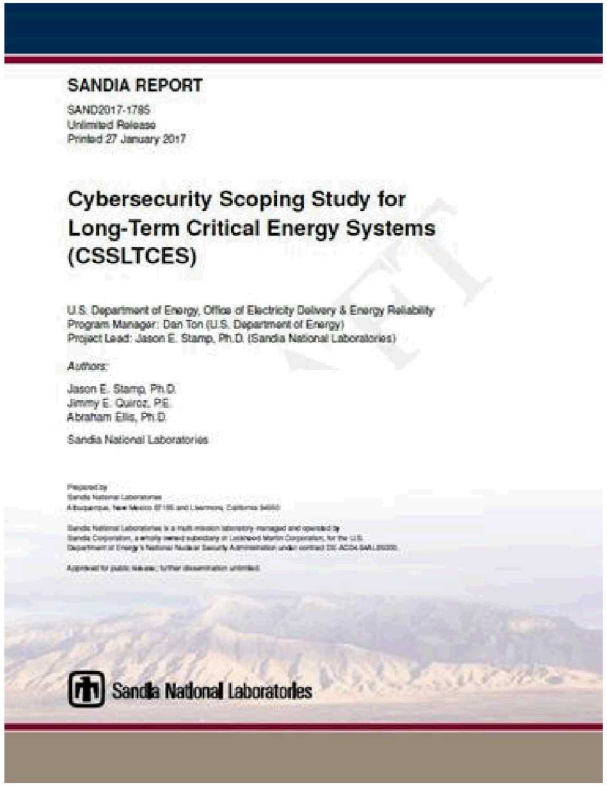
- Study conducted for DOE/OE Smart Grid R&D Program
  - Networked and remote microgrids, distribution-connected systems
- Employing "Defense-in-Depth" approach: Multiple security layers addressing *People*, *Technology* & *Operations* vulnerabilities

<u>Short-term gaps</u>

1) Reliability Mgmt. Framework difficult & ad hoc to apply (NIST-derived)
2) Great gains to be made through improved hygiene
3) Many stakeholders not attuned to cyber needs (e.g., some DOD)
4) Unclear authorities/ responsibilities


Long-term R&D <u>Recommendations</u>

1) Trusted Monitors
2) Virtualization
3) Field Device Security
4) Security Analytics



SANDIA REPORT
SAND2017-1785
Unlimited Release
Printed 27 January 2017

**Cybersecurity Scoping Study for Long-Term Critical Energy Systems (CSSLTCES)**

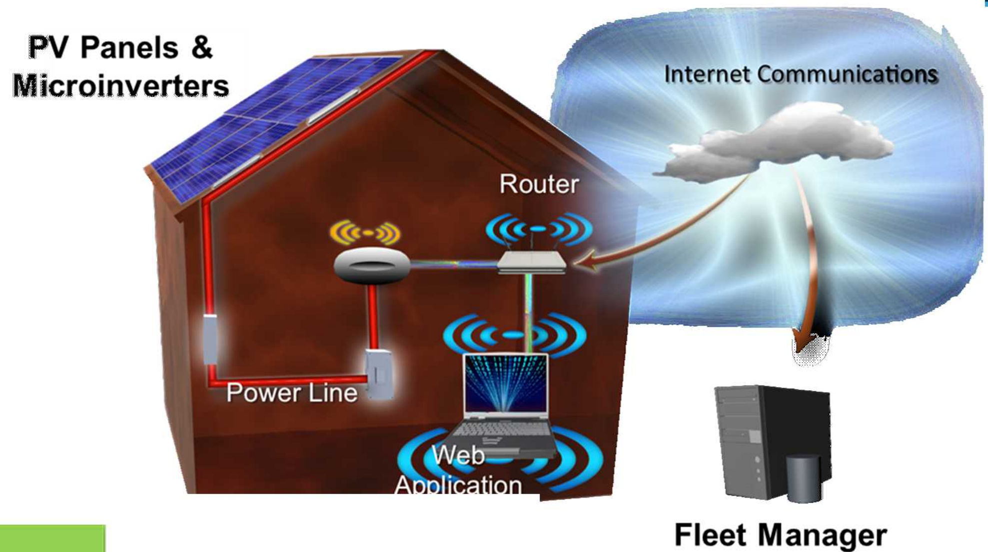
U.S. Department of Energy, Office of Electricity Delivery & Energy Reliability
Program Manager: Dan Ton (U.S. Department of Energy)
Project Lead: Jason E. Stamp, Ph.D. (Sandia National Laboratories)

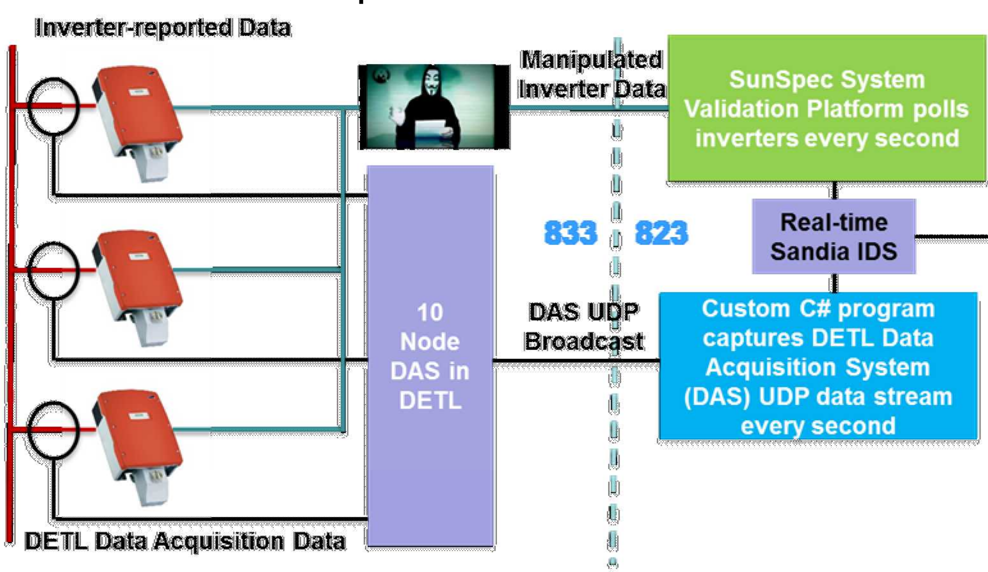
Authors:
Jason E. Stamp, Ph.D.
Jimmy E. Quiroz, P.E.
Abraham Ellis, Ph.D.
Sandia National Laboratories

Sandia National Laboratories

# Cyber Defense Against DER Data Manipulation

- Scenario: modify inverter performance data to cause billing problems and adjust control set points to impact grid stability
- Analysis at Sandia combines SNL's cyber, power system, and critical infrastructure modeling and simulation capabilities



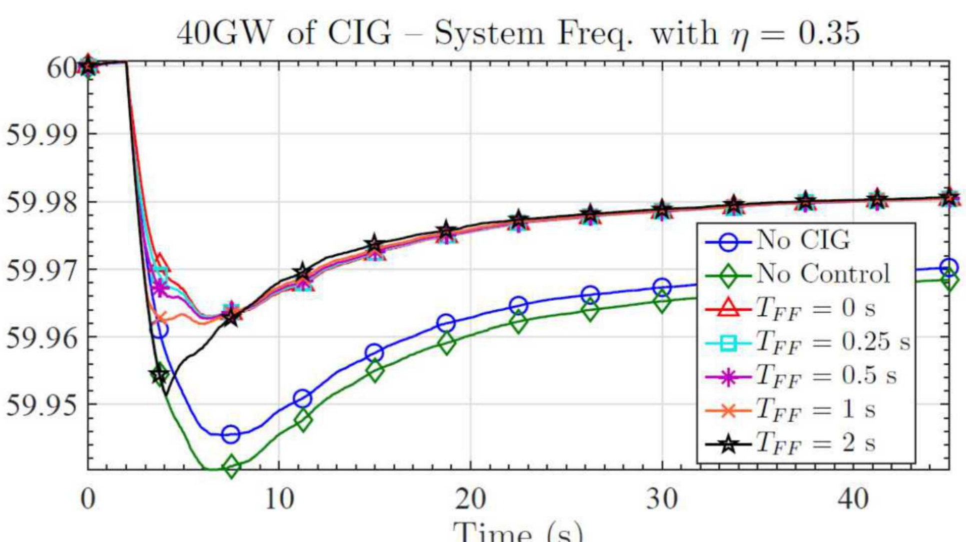




- Sandia is creating Intrusion Detection Systems to alarm when DER data is manipulated.

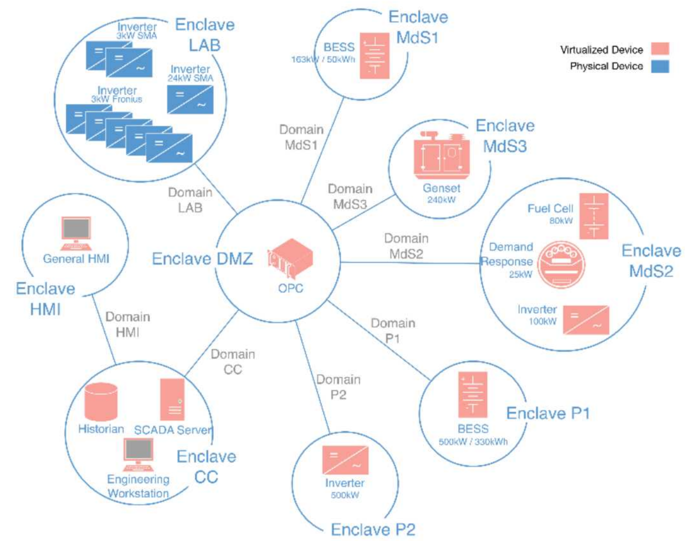
# GMLC: System Performance vs Latency/Security

- 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).**

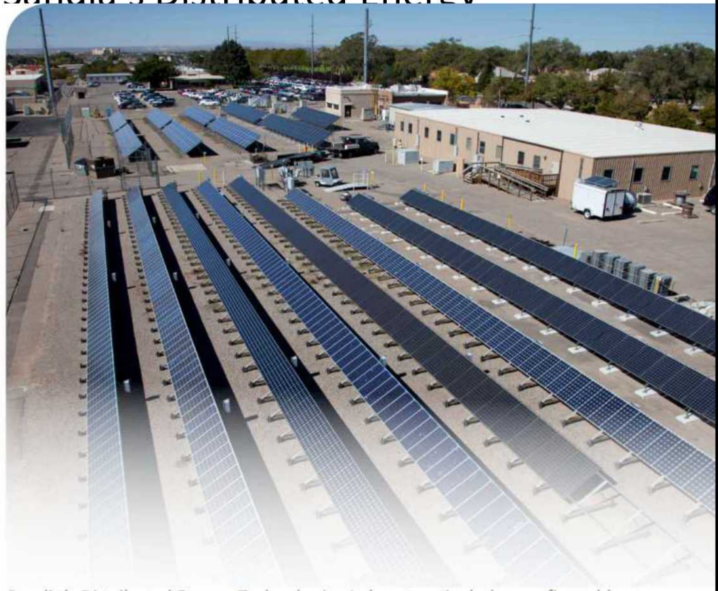



**Cyber Reference Architecture which enclaves DER devices to minimize common-mode vulnerabilities.**

# GMLC: 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)



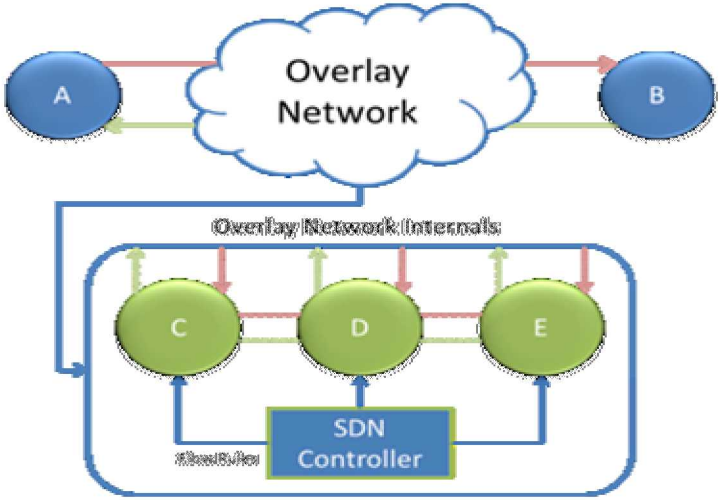
- Currently Implementing NESCOR scenarios within DETL environment
  - WAMPAC.11 – Compromised communication between substations
  - DER.6 - Compromised DER sequence of commands cause power outage
  - DER.16 – DER SCADA system issues invalid command

- Next steps: Configure and complete NESCOR scenario implementation
  - Analyze machine learning features and classification of cyber/physical events

Lawrence Livermore National Laboratory | Sandia National Laboratories | Pacific Northwest NATIONAL LABORATORY | INL Idaho National Laboratory | BERKELEY LAB Lawrence Berkeley National Laboratory | OAK RIDGE National Laboratory

# 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

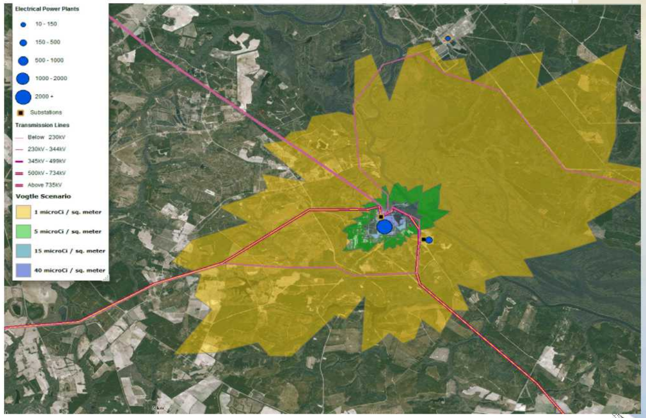


# SNL Nuclear Cyber R&D Research Thrusts

Sandia National Laboratories

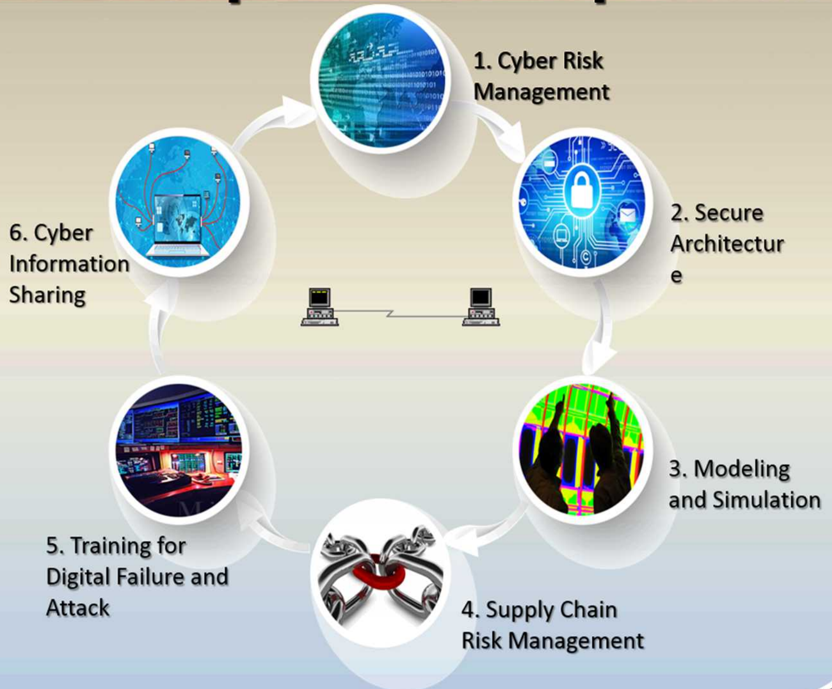

Threat to Consequence Modeling

Fallout From Hypothetical Cyber Attack

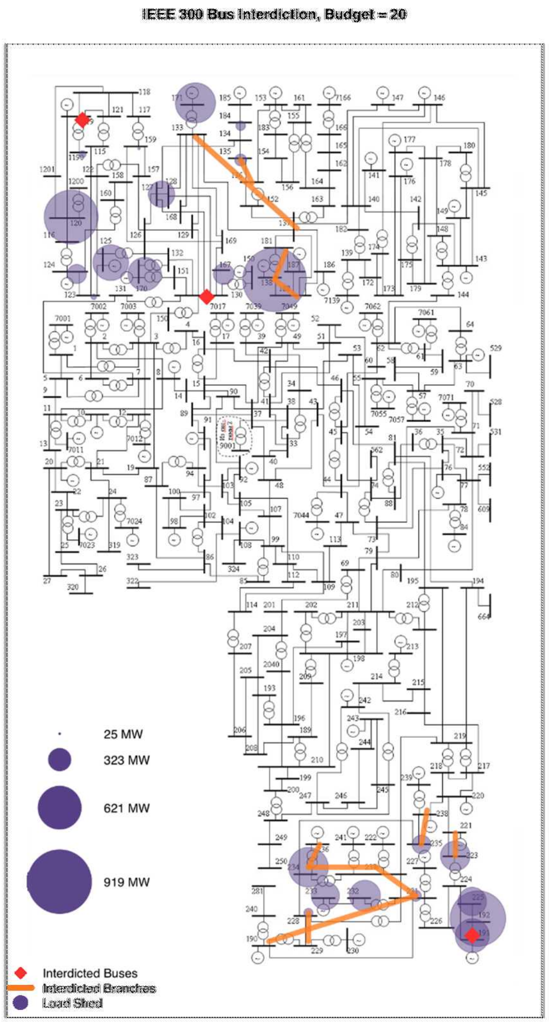


## Research and Development Roadmap Thrusts

- The lifecycle analysis results in a list of requirements and needs. These requirements and needs are categorized into 6 initial research thrust areas:



# Learning From Our Energy 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
- 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

# Thank you!

Charles Hanley

Sr. Manager, Grid Modernization and Military Energy Systems

Sandia National Laboratories

(505)844-4435

cjhanle@sandia.gov