SAND2016-4875C

Exceptional service in the national interest

Sandia National Laboratories

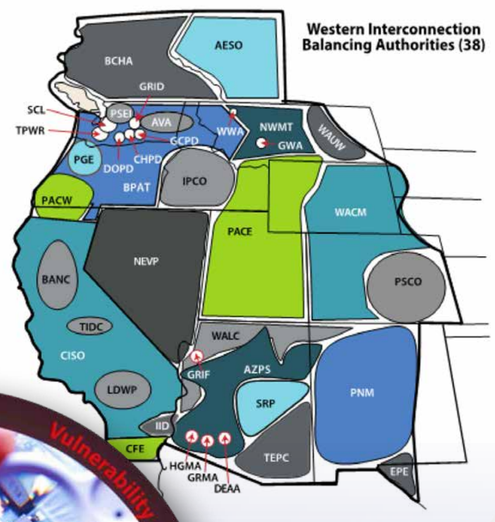
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2016-?????

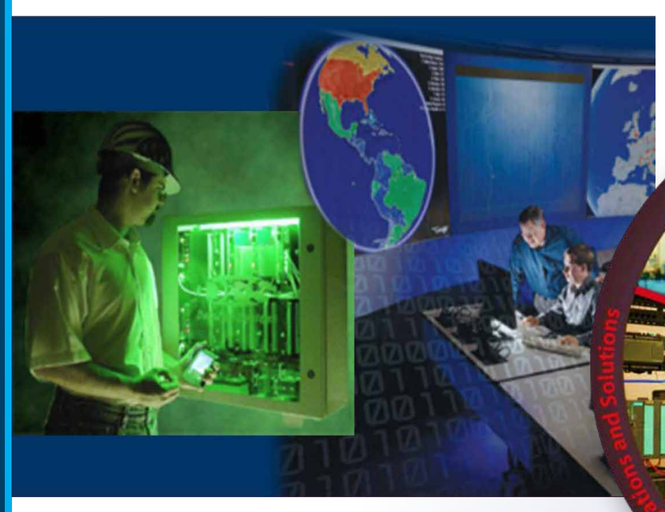
Cyber Physical Analysis of the Electric Grid

PROJECT OVERVIEW

- Critical infrastructure, including the electrical grid, is highly dependent on advanced control systems which are integrated with information and communications systems
- Protecting these systems is difficult
- New cyber vulnerabilities emerge frequently
- Sandia created the Integrated Cyber Physical Impact Analysis (ICPIA) Framework to address this problem
- Analysis was not limited to California and looked at the U.S. WECC (or Western Interconnection).

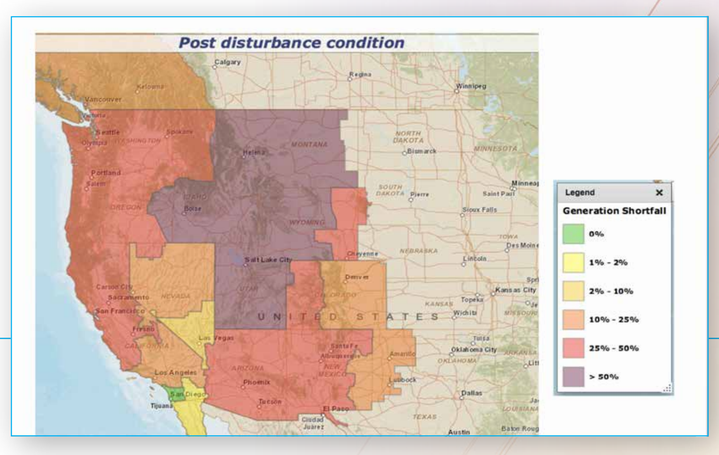
WECC Base Case - Heavy Summer 2014
- **Load: 170,000 MW**
- **Area: nearly 1.8M sq mi**
- **Generators: 3,850**
- **Buses: 19,500**





ELECTRICAL POWER TRANSMISSION LEVEL SCENARIO

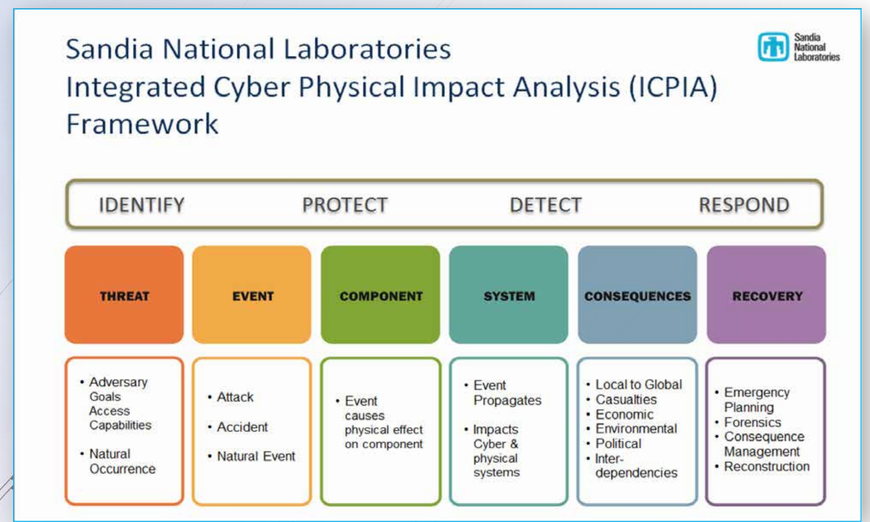
- Created linked models/simulations to demonstrate a complex, multi-stage attack on the grid involving systems at various levels exploring short-term and long-term consequences
  - Demonstrated stage attack and cyber-physical impacts in a live, virtual, and constructed environment.
- Combines Sandia's cyber, power system, and critical infrastructure modeling and simulation capabilities
- This capability provides:
  - Consideration of (potential) cascading impacts across systems
  - Opportunities for training at the control system level

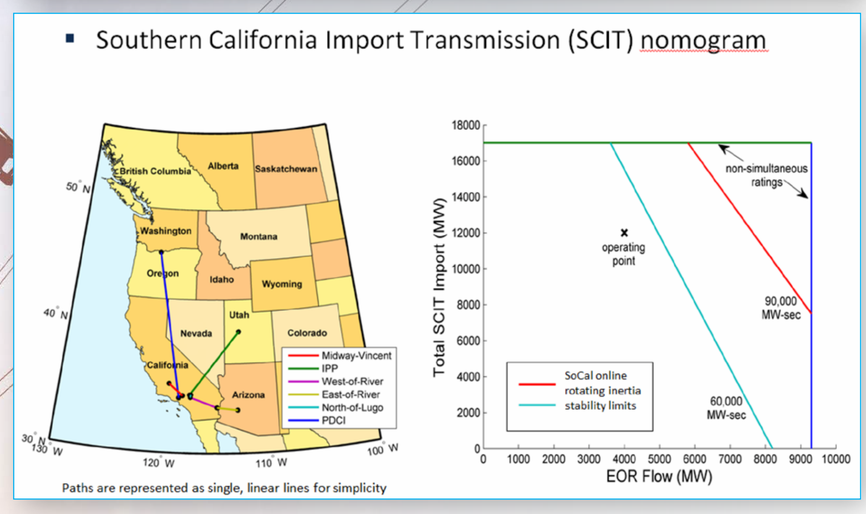


Elements of Cyber Attack and Cascading Consequenses

INTEGRATED CYBER PHYSICAL IMPACT ANALYSIS (ICPIA) FRAMEWORK

- Performs modeling and simulation at various levels in order to understand the potential impacts of a cyber attack on the electric grid.
- Identifies an energy system's:
  - Key components and their interfaces
  - Vulnerabilities and risks
  - Areas where technology or systems can be added or augmented to reduce the probability or consequences of an event, and use that information to:
    - Identify gaps in technical basis of regulation
    - Relevant capabilities, including across the DOE complex
- These modeling and simulation capabilities can be integrated to deliver a differentiating defense approach. The result can be used to:
  - Design secure architectures
  - Provide test beds for integrating systems
  - Explore the impact of previously unidentified threats and vulnerabilities
  - Act as a training tool, and perform other valuable lifecycle functions.





SANDIA'S UNIQUE CAPABILITIES

- Our relationships with intelligence agencies and our responsibility to defend nuclear weapons have provided Sandia with a deep understanding of the Nation-State adversary.
- The cyber attack surface is nearly infinite and complex. Solving the problem requires coordination and collaboration among various government and private entities.
- Sandia's breadth of expertise is key – we have expertise in power systems, control systems, integrated infrastructure impacts and cybersecurity.