
# Cybersecurity for Energy Delivery Systems

## 2010 Peer Review

**Alexandria, VA ♦ July 20-22, 2010**

**Co-PI: Jason Stamp, Ph.D.**

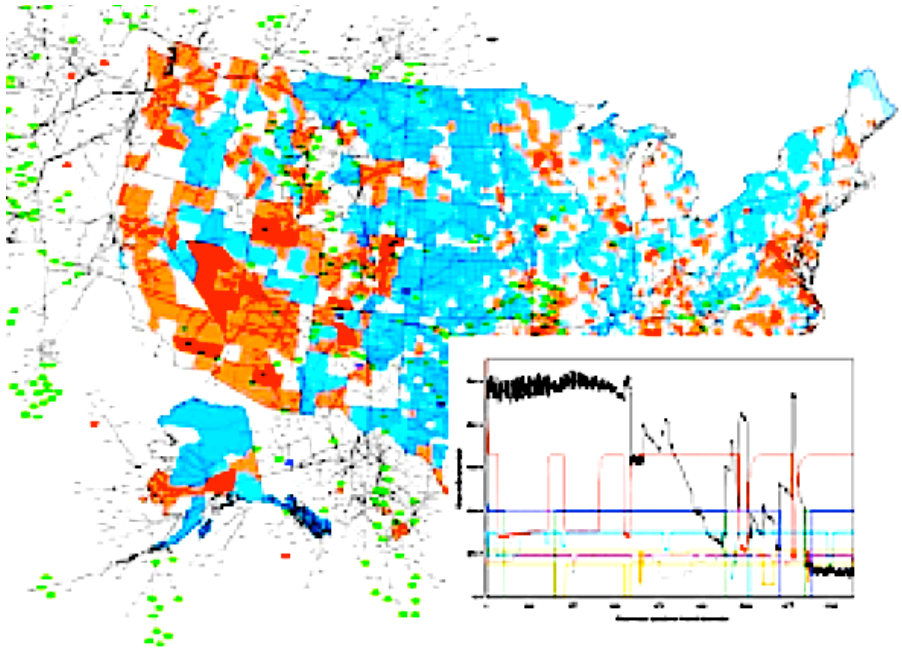
**Co-PI: Laurie Phillips**

**Sandia National Laboratories**

**Reliability Impacts for Cyber Attack (RICA)**

# Summary Slide: Reliability Impacts for Cyber Attack (RICA)

- **Outcomes:** Quantitative impact analysis of cyber attacks against power grid control systems (that affect grid topology and operations), including potential mitigation steps, using reliability metrics. Analyze large-scale cases using simulation software in a High-Performance Computing (HPC) environment.
- **Roadmap Challenges**: Develop evidence-based business case to increase and shape investment in control system security.
- **Major Successes:** Build environment is operational and in use, nearly all major software components are functioning, test cases run well.



- **Schedule:** Prototype tool July 2010; reliable HPC software September 2010; final report September 2010
- **Level of Effort:** $250k
- **Funds Remaining:** $35k
- **Performer:** SNL
- **Partners:** WECC (pending), Iowa State University (FY10)

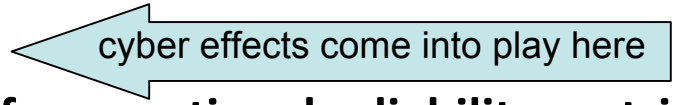
# Approach and Execution: Research Goals

- **Questions like these can be addressed using RICA:**
  - How are reliability impacts different for vulnerable relays or SCADA systems?
  - What's the relevant level of protection for smart meters?
  - What's the impact of cutting the number of successful cyber attacks in half? Is it the same as recovering twice as quickly?
  - What effect do vulnerable control systems for PV/wind have on grid reliability?
  - What is the potential impact of a new hypothetical vulnerability?
- **For certain classes of adversaries (example threat matrix shown):**

| Category | Funding | Goal Intensity | Stealth | Physical Access | Cyber Skills | Implementation Time | Organization Size |
|---|---|---|---|---|---|---|---|
| I | H | H | H | H | H | Decades or years | Hundreds |
| II | H | H | H | M | M | Years | Low hundreds |
| III | M | H | M | M | M | Months | Tens |
| IV | L | M | H | L | H | Months | Tens |
| V | L | M | M | L | M | Months | Up to ten |
| VI | L | L | L | L | L | Weeks | One |

} RICA

# Approach and Execution: Research Plan

- **RICA measures the impact of cyber attack by determining (via modeling) unserved load many times for different load* and grid conditions**
- **Performance is attributed to experiment parameters (constant over $10^5$-$10^7$ simulation runs):**
  - Initial grid topology (currently focused on the WECC area)
  - Failure parameters of grid components (MTTF/MTTR)
  - Attack parameters & targets (MTTA/MTTR) 

- **The outcome of each experiment is a set of conventional reliability metrics, e.g., Loss of Load Expectation (LOLE) and Frequency of Interruption (FOI)**

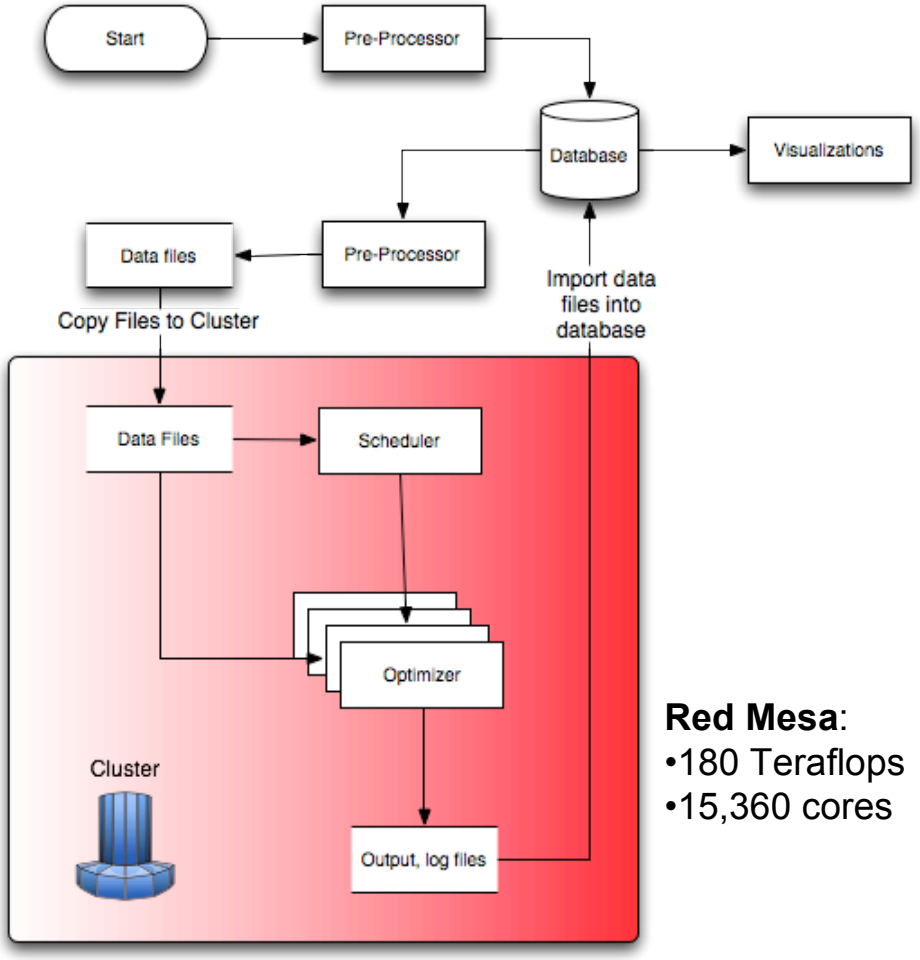
*note: time of day & year are represented by 365x24 hourly load profiles

# Approach and Execution: Research Plan

- **Technical barriers:**
  - RICA could not simulate large power grid models (Solution: FY10 focus on HPC simulation of WECC with parametric analysis for risk given different attack and recovery rates)
  - Optimal power flow software module is not performing adequately (Solution: conversion to interior-point method leveraging network distribution factors)
- **Acceptance barriers:**
  - Quantitative analysis is unfamiliar for industry (Solution: use accepted reliability calculation techniques and metrics)
  - Cyber models/scenarios can be made more realistic (Solution: FY11 plans to improve modeling, perhaps using Hidden Markov Models, Petri nets, etc.)
  - RICA is considered as a transmission-only tool (Solution: FY11 plans to analyze cyber attack against AMI/renewables for distribution and microgrids)
- **Complementary follow-on work: develop complementary quantitative approach for high-resource adversaries**

# Technical Accomplishments, Quality, and Productivity

- **FY10 Technical Milestones Met:**
  - Build environment
  - Code module test harness
  - Preprocessor module runs
  - Simulation scheduler
  - Load flow module
  - Database & prototype visualization
- **FY10 Milestones Remaining:**
  - Optimal power flow
  - Functional federated software
  - WECC simulation and parametric analysis




**Red Mesa**:
•180 Teraflops
•15,360 cores

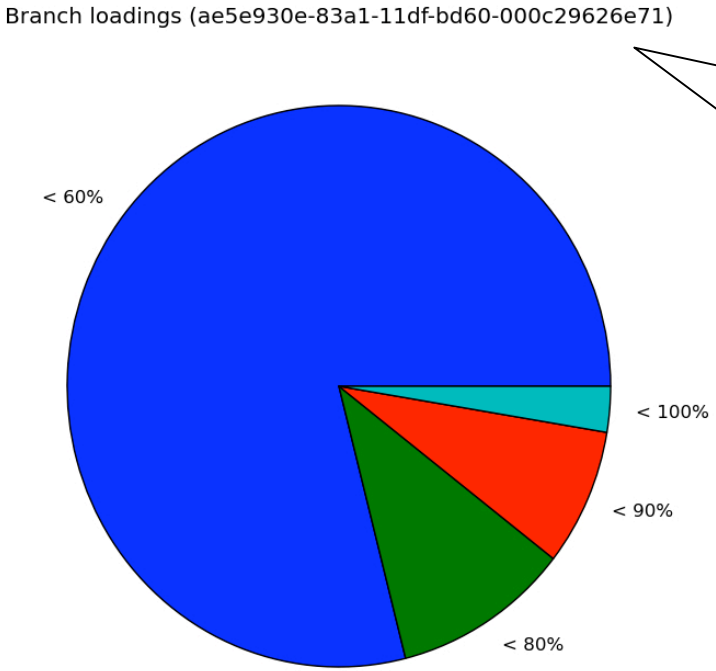
- **Project Success: use of RICA for impacts analysis by stakeholders to develop "evidence-based business cases to increase and shape investment in control system security"**

# Collaboration/Technology Transfer

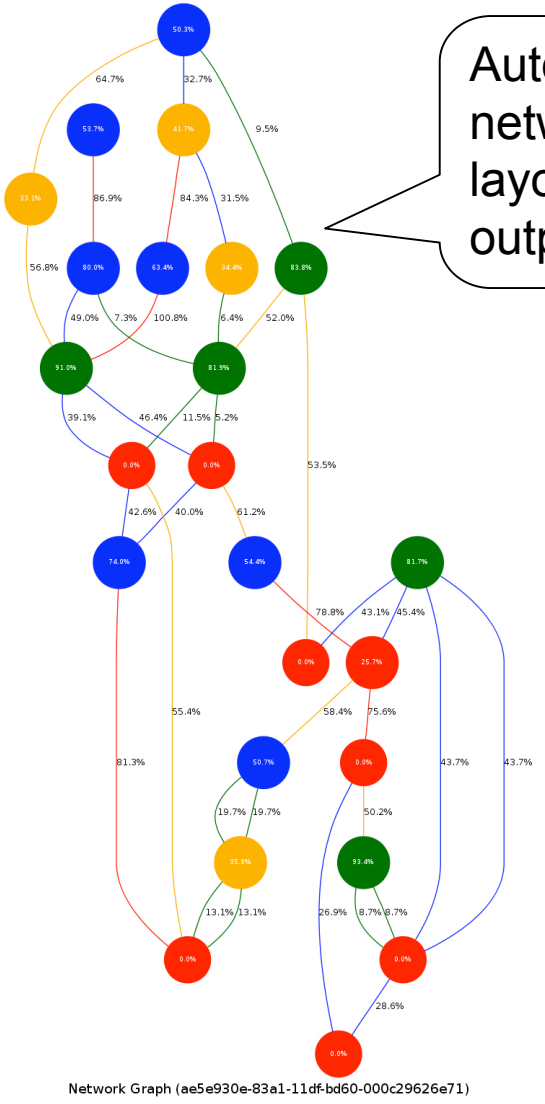
- **Leveraging additional Sandia HPC funding opportunity**
- **Plans to gain industry input:**
  - Still getting feedback from published article last year
  - Writing a journal article this FY
  - Developing WECC relationship
  - Project has existing relationships with universities
  - Participation on relevant technical committees
- **Plans to transfer technology/knowledge to end user:**
  - Intended for use by:
    - Government/research: understand risk given new vulnerabilities or mitigation
    - Industry: maintain system reliability given known organizational attack rates
  - Interact with WECC to:
    - Broaden industry interaction
    - Gain acceptance through power flow validation (possibly using WECC load profiles)
    - Understand WECC decision-making process to determine key RICA uses

# Questions?

**RICA: Quantitative impact analysis of cyber attacks against power grid control systems (that affect grid topology and operations), including potential mitigation steps, using reliability metrics**




Serial # of simulation set




Automatic network layout tool output