

NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

Risk-Informed Evaluation of Security Technology Insertions and Next-Generation Control System Architectures via Modeling and Simulation

**HCSS:NEC4CPS Workshop
November 8-9, 2006**

Peter Sholander

Sandia National Laboratories

(505) 844-0646

peshola@sandia.gov



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND Report 2006-6562C. Unclassified, Unlimited Release.



Sandia National Laboratories

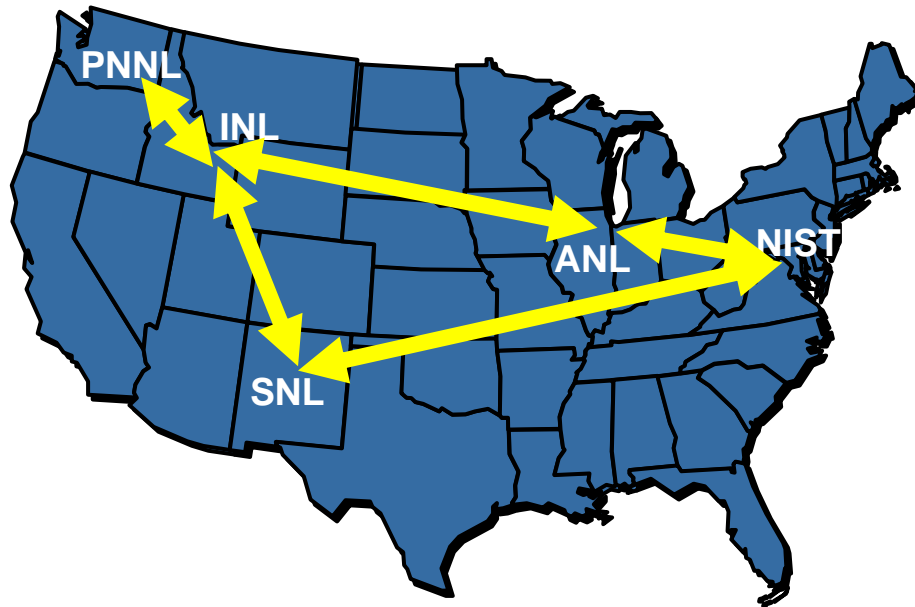
National SCADA Test Bed

OBJECTIVE

Support industry and government efforts to enhance control systems cyber security across the energy infrastructure

Scope

Department of Energy (DOE) multi-laboratory program jointly managed and executed by **Sandia National Laboratories** and Idaho National Laboratory.



Key program areas

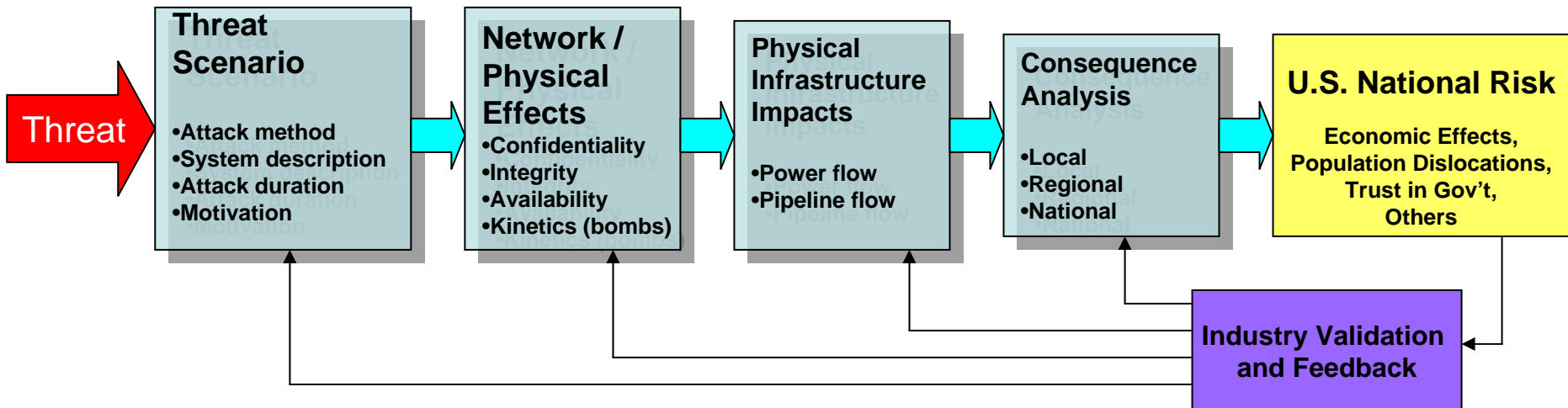
- Supervisory Control and Data Acquisition (SCADA) system vulnerability assessment/mitigation
- RDT&E of advanced secure control systems technology
- support development of security standards
- outreach and awareness

Industry Needs

- From *Roadmap to Secure Control Systems*
 - Measure and assess security posture for facility providers. The goal is that by 2008, 50% of asset owners and operators can perform self-assessments of their control systems using consistent criteria.
 - Develop and integrate protective measures for Process Control Systems (PCS). The goal is to provide “security test harnesses” for evaluating next generation architectures and individual PCS components by 2014.
- North American Electric Reliability Council (NERC)
 - Risk informed evaluation of security solutions for NERC Top 10 Vulnerabilities
 - NERC Critical Infrastructure Protection (CIP) standard requires risk assessment of “critical cyber assets”

Threat to Consequence: End-to-End Process for SCADA

- Goal
 - Calculate risk to determine the business case for security technologies
- State-of-the-art
 - Existing tools for each piece
 - Need an integrated suite of tools that address the overall problem

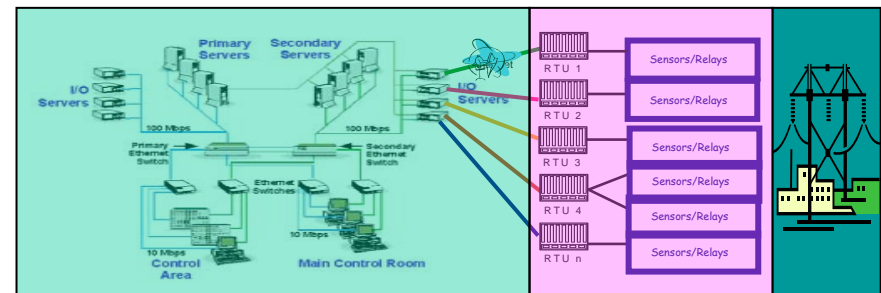


Existing Tools (a non-comprehensive list!)

- Threat
 - Difficult since Intelligence data can not be shared with Industry
 - Need better information sharing tools
- Effects/Impacts → Site- or Sector-Specific Consequences
 - Network: ns3, OPNET, QualNet, Emulab, DETER...
 - Power: PSS/E, PowerWorld, ...
 - Oil/Gas: Stoner Pipeline Simulator,...
 - Water: EPANET, ...
- Cross-Sector Consequences
 - National Infrastructure Simulation and Analysis Center (NISAC)
- Vulnerability and Risk
 - Attack Trees, Protection Trees, Red Teaming, ...
 - EASI, SAVI & ATLAS (vulnerability), JCATS (combat simulation)
 - Structured Expert Judgment (e.g., Analytic Hierarchy Process (AHP), Vital Issues Process (VIP), Evidence Theory)

Relevant Sandia (and other National Lab) Tools

- National Infrastructure Simulation and Analysis Center (NISAC)
 - Effects of infrastructures and their interdependencies on supply and demand under different conditions
 - time of day/year, unusual event, new regulations, incentives, market structures.
 - Large-scale microeconomic simulation
 - impacts of vulnerabilities and disruptions on national economic security.
 - Railroad Network Analysis System
 - commodity flow disruptions due to destruction of assets, and to study policy options concerning the movement of toxic chemicals by rail.
 - Interdependent Energy Infrastructure Simulation System
 - focused on electric power and natural gas
 - Urban Infrastructure Suite (UIS)
 - models for urban population mobility, epidemiology, telecommunications, transportation, and water.
- Virtual Control System Environment (VCSE)
 - “Emulab for PCS + Simulation”
 - Combined analysis of system availability, system performance, and cyber security posture.
 - Mix of real, simulated and emulated systems/software/hardware provides tradeoffs between cost, scalability, and accuracy.
 - Model effects/impacts in multiple coupled infrastructures
 - Leverage commercial tools (OPNET, MATLAB, High Level Architecture, ...)



Control Centers (LANs, HMIs, SCADA Servers) Wide Area Network (WAN) Process Control System Process