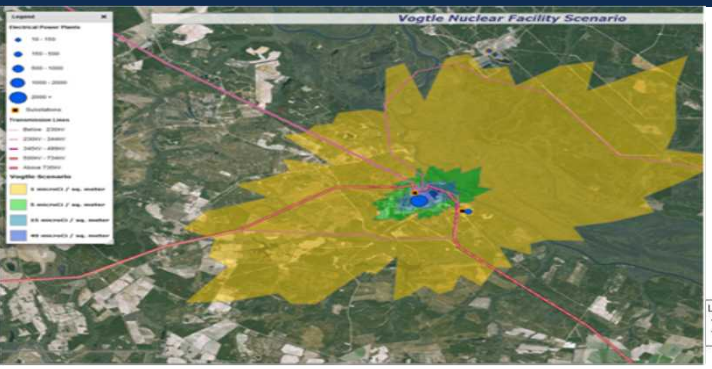
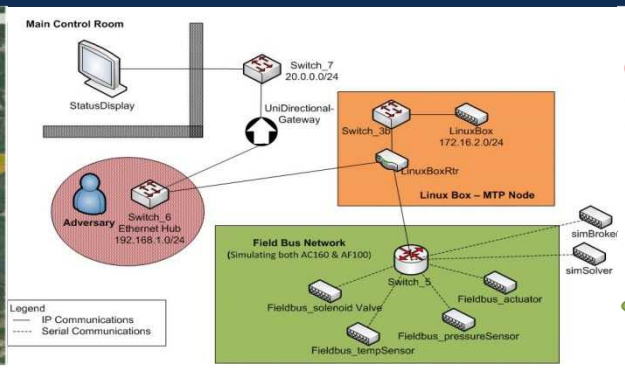
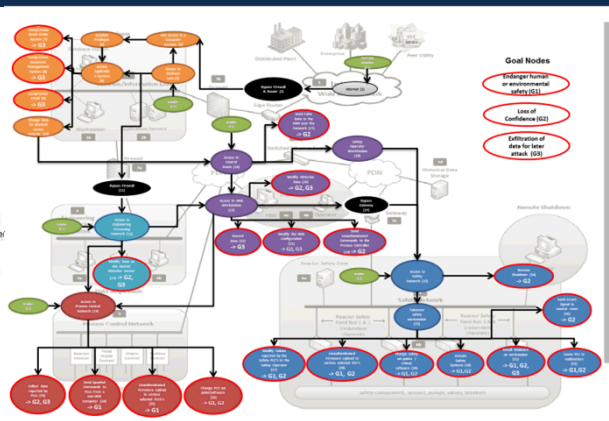
SAND2016-4802PE

Exceptional service in the national interest

Sandia National Laboratories







Integrated Cyber Physical Impact Analysis

For *Technology, Training and Demonstration Area*

Center for Global Security and Cooperation

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

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. SAND NO. 2011-XXXXP

Integrated Cyber Physical Impact Analysis Overview

Sandia National Laboratories

Opportunity - National infrastructure is increasingly reliant on advanced control systems. The systems are complex and increasingly connected to the open internet. Protection is difficult and must consider new vulnerabilities and potential attacks. Sandia has developed an array of modeling and simulation capabilities, which can be integrated to secure our control systems.

- Leverages capabilities:
  - Threat modeling
  - Adversary-based vulnerability assessment
  - Network and control system emulation, simulation and analysis
  - Physical system modeling and simulation
  - Critical infrastructure modeling

Integrated Cyber Physical Impact Analysis (ICPIA) Framework

IDENTIFY PROTECT DETECT RESPOND

THREAT	EVENT	COMPONENT	SYSTEM	CONSEQUENCES	RECOVERY
• Adversary Goals Access Capabilities • Natural Occurrence	• Attack • Accident • Natural Event	• Event causes physical effect on component	• Event Propagates • Impacts Cyber & physical systems	• Local to Global • Casualties • Economic • Environmental • Political • Inter-dependencies	• Emergency Planning • Forensics • Consequence Management • Reconstruction

Scenarios Exercise ICPIA Framework

Sandia National Laboratories

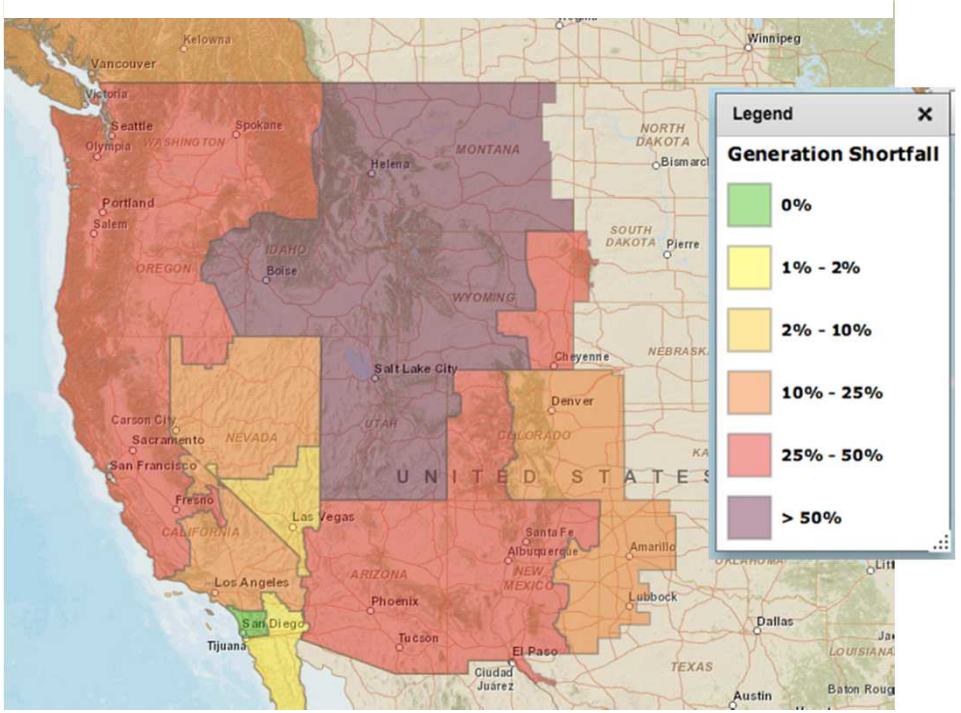
3 scenarios explore cyber attacks focus on different aspects of power systems:

1. electric power transmission
2. a nuclear power plant digital safety system
3. renewable energy distribution control

Transmission Scenario

The attack caused electric power import stability limits for Southern California TO BE EXCEEDED causing a widespread outage. We demonstrated attacker actions and resulting impacts to control systems and power transmission in an environment combining emulated, simulated, and hardware devices

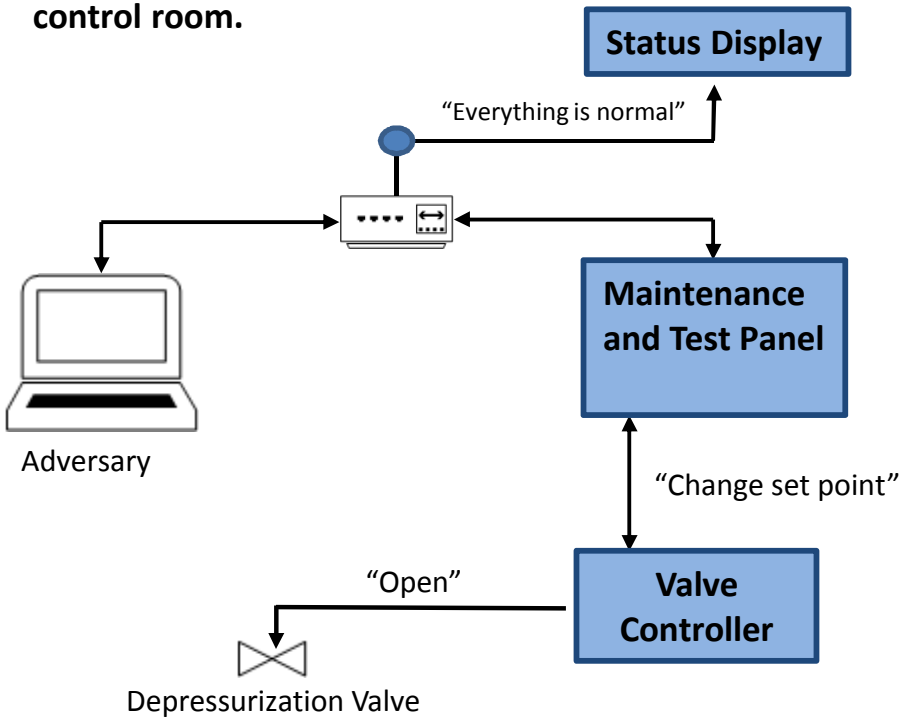
Generation Shortfall

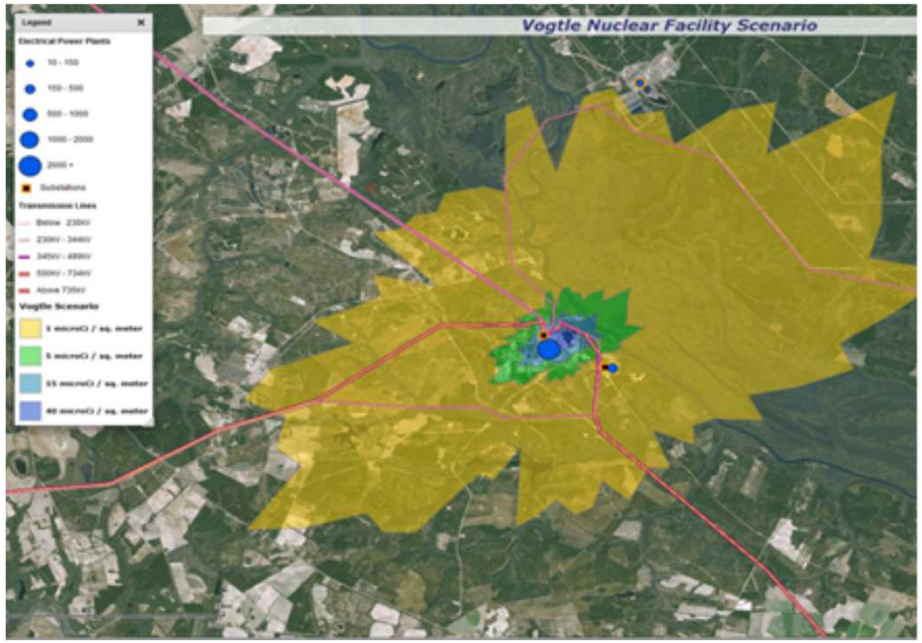


Nuclear Scenario

Attack targets the digital safety system causing loss of coolant and depressurization to containment. Failure of coolant makeup and heat removal leads to core melt.

Adversary installs a network hub and changes set points to actuate valve while sending normal plant status to the control room.

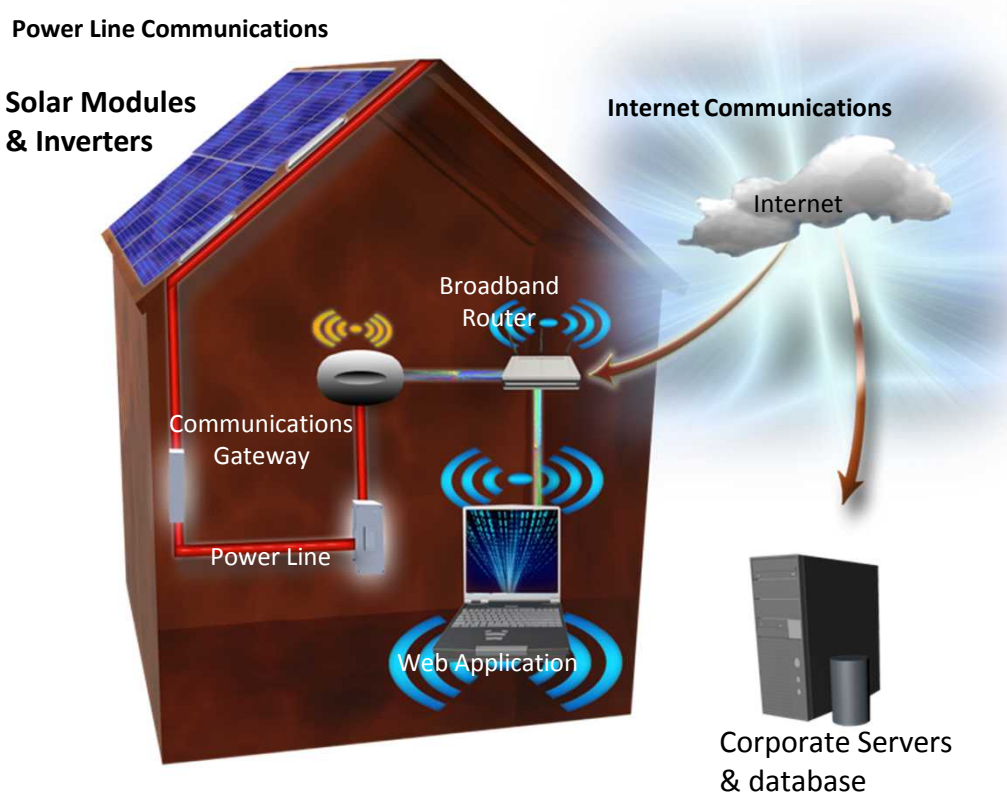




Radioactive plume and land contamination model

Distribution Control Scenario

- Remote communications to solar panels is enabled by smart meters and inverters
- We identified vulnerabilities and demonstrated an attack
- Our results and mitigation recommendations were provided to the manufacturer!



Next Steps

Sandia National Laboratories

- We continue to expand our modeling capabilities and use them to help defend national infrastructure and important control systems.
- Areas of focused capability development:
  - evaluate **emerging attack technologies**,
  - **integrate analysis** from different domains across the framework,
  - methodologies to identify **resilient systems,** and
  - **automate analysis** to support multiple scenarios.