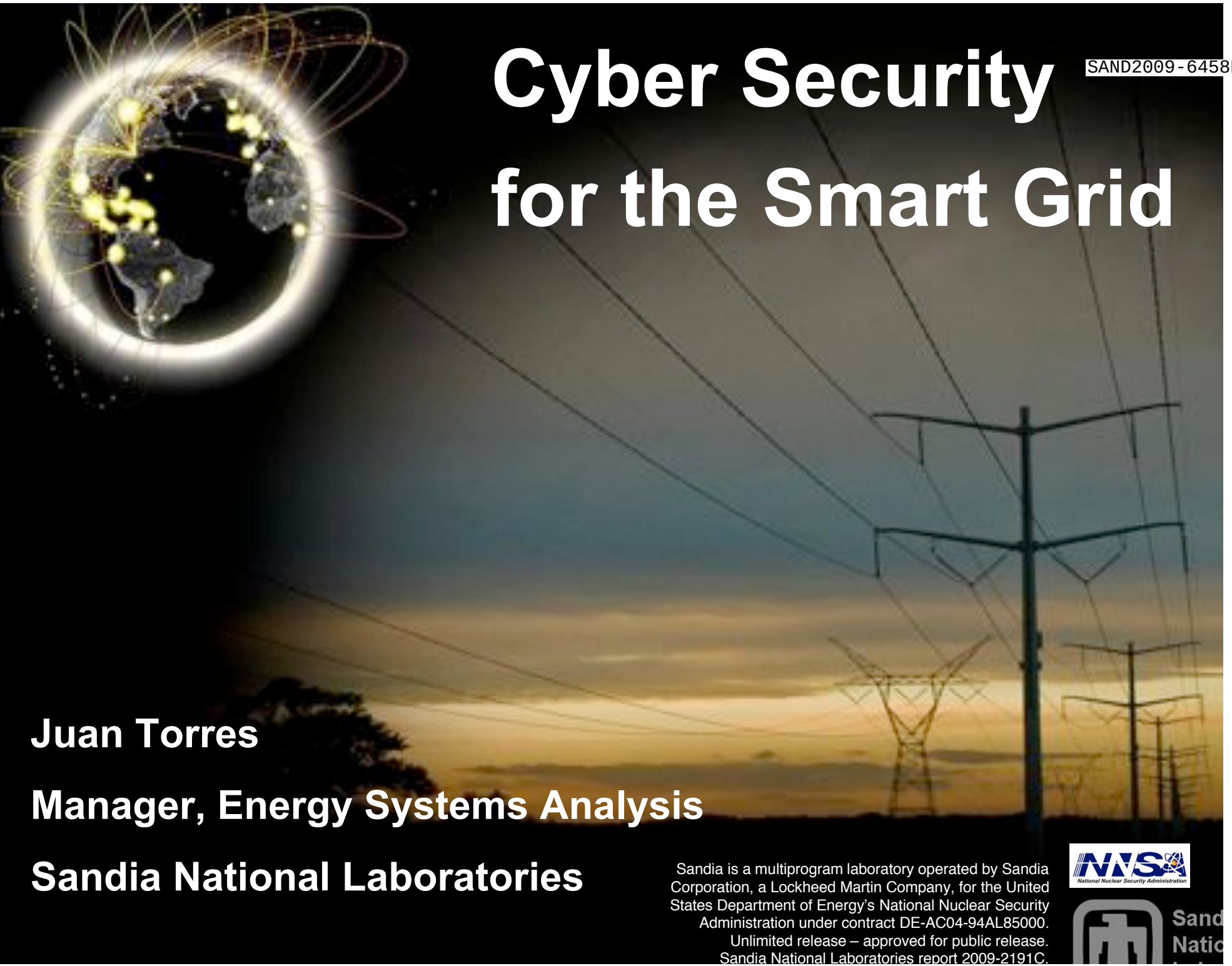


Cyber Security for the Smart Grid

SAND2009-6458P

Juan Torres

Manager, Energy Systems Analysis

Sandia National Laboratories

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.
Unlimited release – approved for public release.
Sandia National Laboratories report 2009-2191C.

Sandia is Organized into Three Strategic Management Groups

Integrated Technologies and Systems
Three Management Units

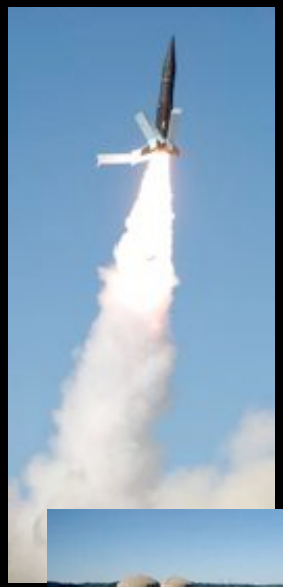
- *Energy, Resources, and Nonproliferation*
- *Homeland Security*
- *Defense Systems & Assessments*

Nuclear Weapons
One Management Unit

- *Nuclear Weapons*

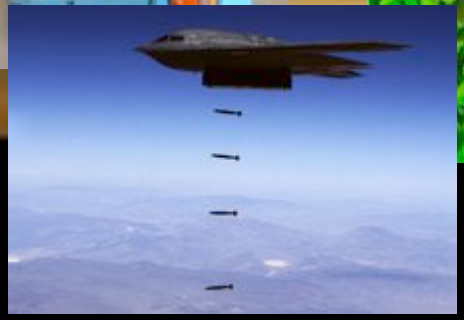
Laboratory Transformat
Two Management Units

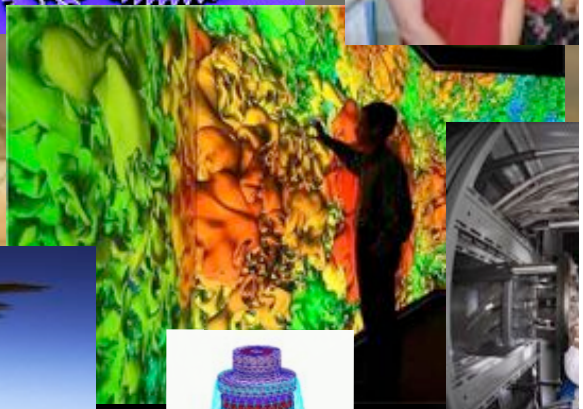
- *Integrated Enabling Services*
- *Science, Technology, and Engineering*









Information is Critically Important For the Smart Grid

- New grid technology:
  - Distributed generation
  - Renewable generation
  - Energy storage
  - Advanced metering / control
- Necessitates decentralized management and control of the power system:
  - Ramp rate control
  - Voltage profile management
  - Fault identification and isolation
  - Controlled islanding
- It all depends on shared information flow

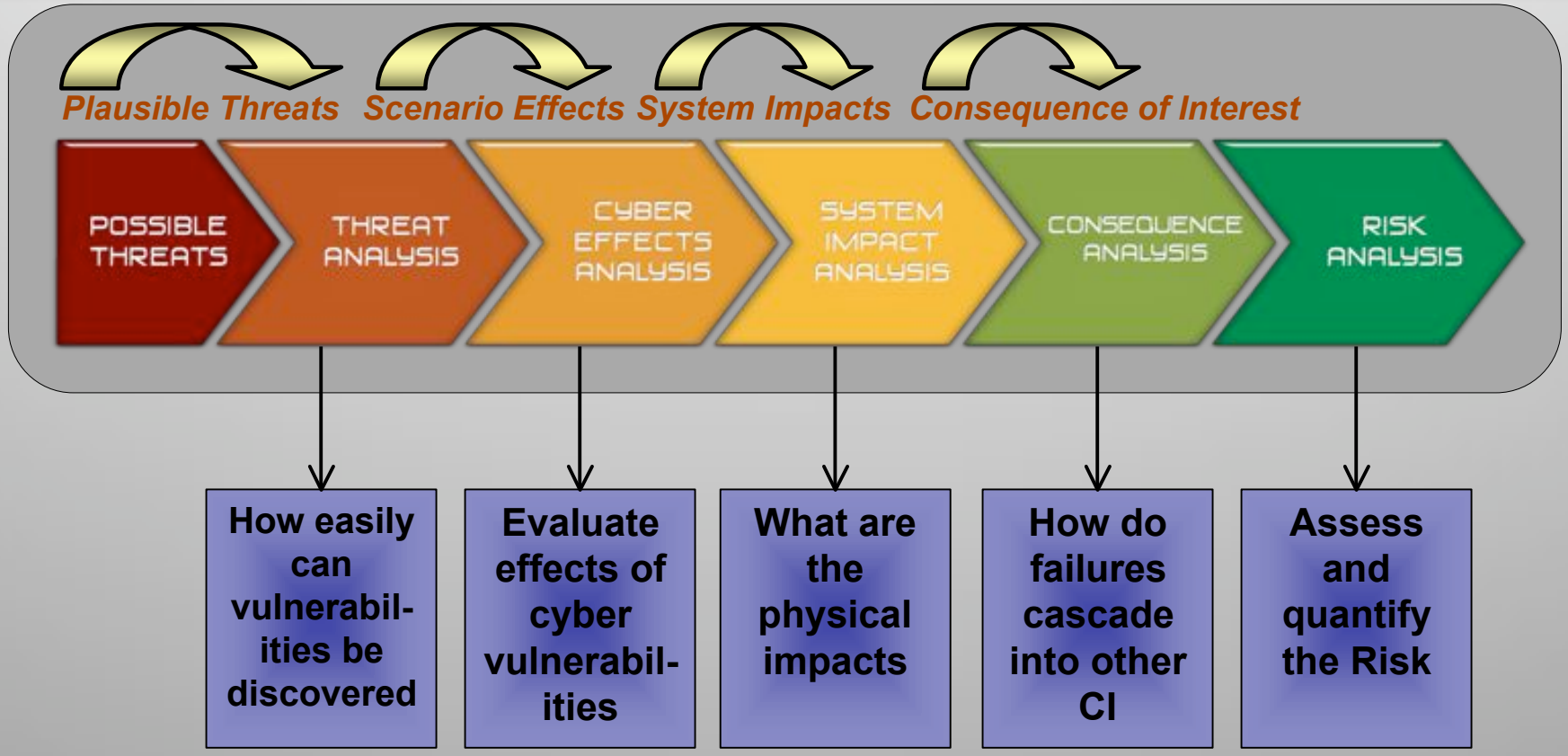
Information in the Smart Grid

- Information classes:
  - Voltage, current, frequency, etc.
  - Fault and reliability conditions
  - Pricing and market information
- Data shared between disparate stakeholders:
  - Regional reliability organizations
  - Markets
  - Transmission
  - Generation
  - Distribution
  - Consumers
- Smart Grid relies very much on information flow

Critical Components of Smart Grid Security

- Technology and systems risk assessment
  - Threats
  - Vulnerabilities
  - Impacts
  - Consequences
- Attack-tolerant information and control architectures
- Rapid forensics and recovery

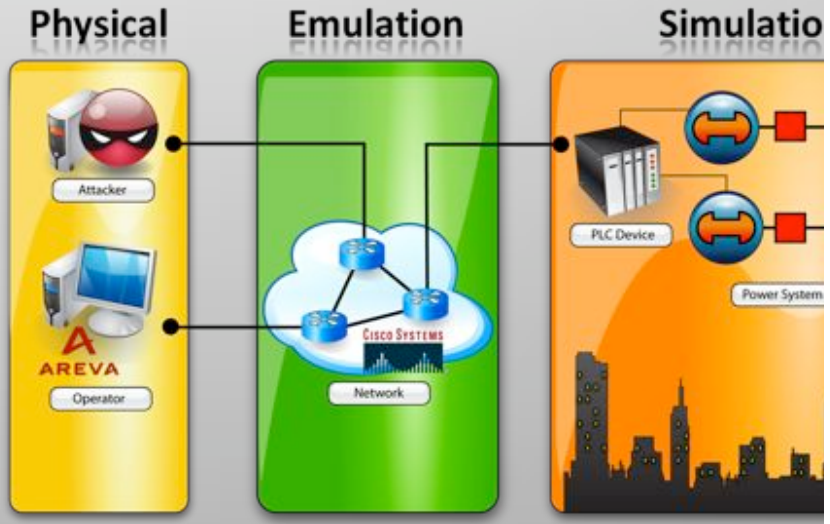
Risk Assessment Analysis



Provides a Framework for Conducting Smart Grid Risk Analysis

Vunerability and Scenario Analysis: Virtual Control System Environment (VCSE)

- High fidelity modeling environment
- Simulation and analysis of control system devices and network communications
- Execute cyber attacks and assess control system impacts – *cyber-to-physical bridge*
- Enables real-time, hardware/software-in-the-loop analysis
- Current capabilities:
  - SCADA communication protocols (Modbus, DNP3)
  - Real and virtual remote terminal units (RTUs)
  - Static and dynamic power system simulation



Possible Threats → Threat Analysis → Cyber Effect Analysis → System Impact Analysis → Consequence Analysis → Risk Analysis

VCSE Use Case Examples

- **Analyze Cyber Vulnerabilities in the Power Grid**
  - (OUO) Smart Grid Advanced Metering Infrastructure Attack (March 2009)
    - Leverage wireless mesh network to launch an attack on the grid
  - Known Vulnerability Analysis (April 2009)
    - US-CERT announced vulnerability in Domain Name System (DNS)
  - Life-cycle Rogue Software Attack (June 2008)
    - Rogue software planted during routine maintenance upgrade

- **Training Simulator for Oil & Gas**
  - Interactive cyber training simulator for control system oper
  - Simulates a cyber attack on an oil refinery and leads the 's through a series of events before an explosion occurs
  - Adversary attack graph is automated and the shortest path target is constantly being calculated

Possible Threats → Threat Analysis → Cyber Effect Analysis → System Impact Analysis → Consequence Analysis → Risk Analysis

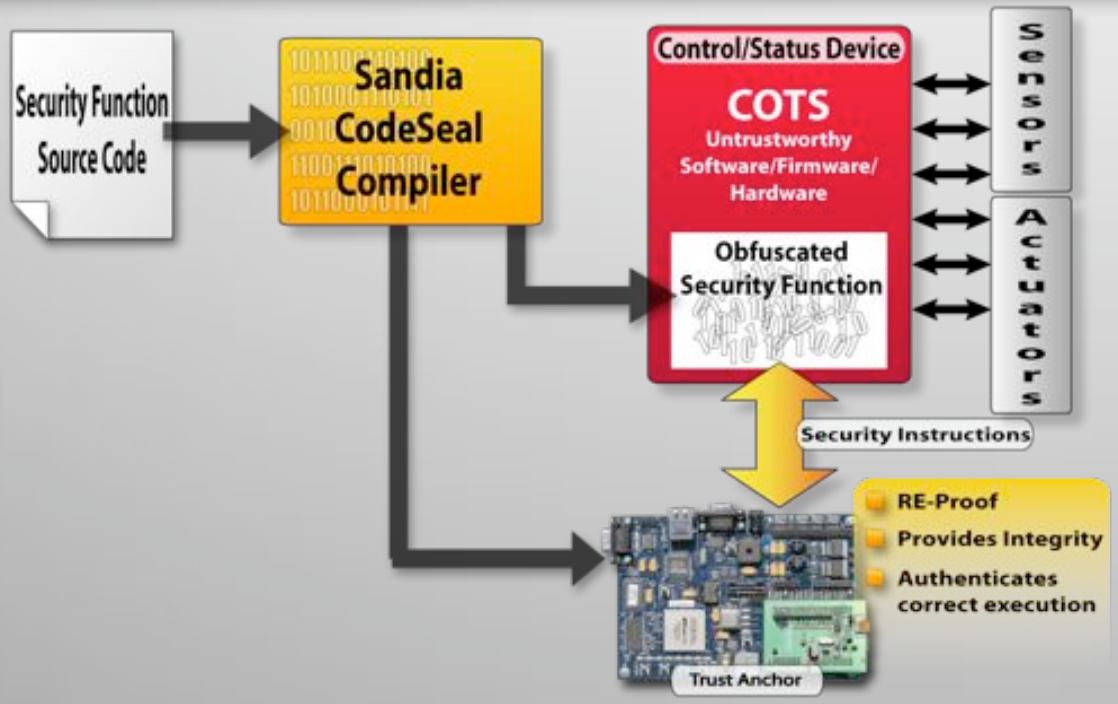
Impact Analysis

- **Develop complementary tools to estimate electrical outages that may result from cyber attack that will help prioritize attention and remediation**
  - Determine plausible scenarios that can cause significant impacts (discover previously unknown issues ahead of the adversary)
  - Evaluate the potential impacts of plausible attack scenarios
  - Analyze worst-case adversary impacts
  - Develop optimal security improvement investments
- **Help make Smart Grid management and control resilient, and facilitate rapid attack recovery**

Consequence Estimation

- **Stakeholders have a need to base consequence on metrics they care about**
  - Economics, public image, health and safety, etc. (Performance Measures)
- **Physical impacts must somehow be mapped to metrics**
  - Constructed Scales are the 'linkage' between an impact and the value tree analysis of that impact
- **Metrics will most likely not be equally important to all interested parties in every situation**
  - Can use pair-wise comparison techniques to weigh metrics
- **As impacts occur, metrics and specific system data can be used to calculate a numerical value (the performance index) for consequence**
- **Metrics can also highlight areas of concern within the system that mitigations could be applied to**

Enabling Distributed Trust for Smart Grid with CodeSeal



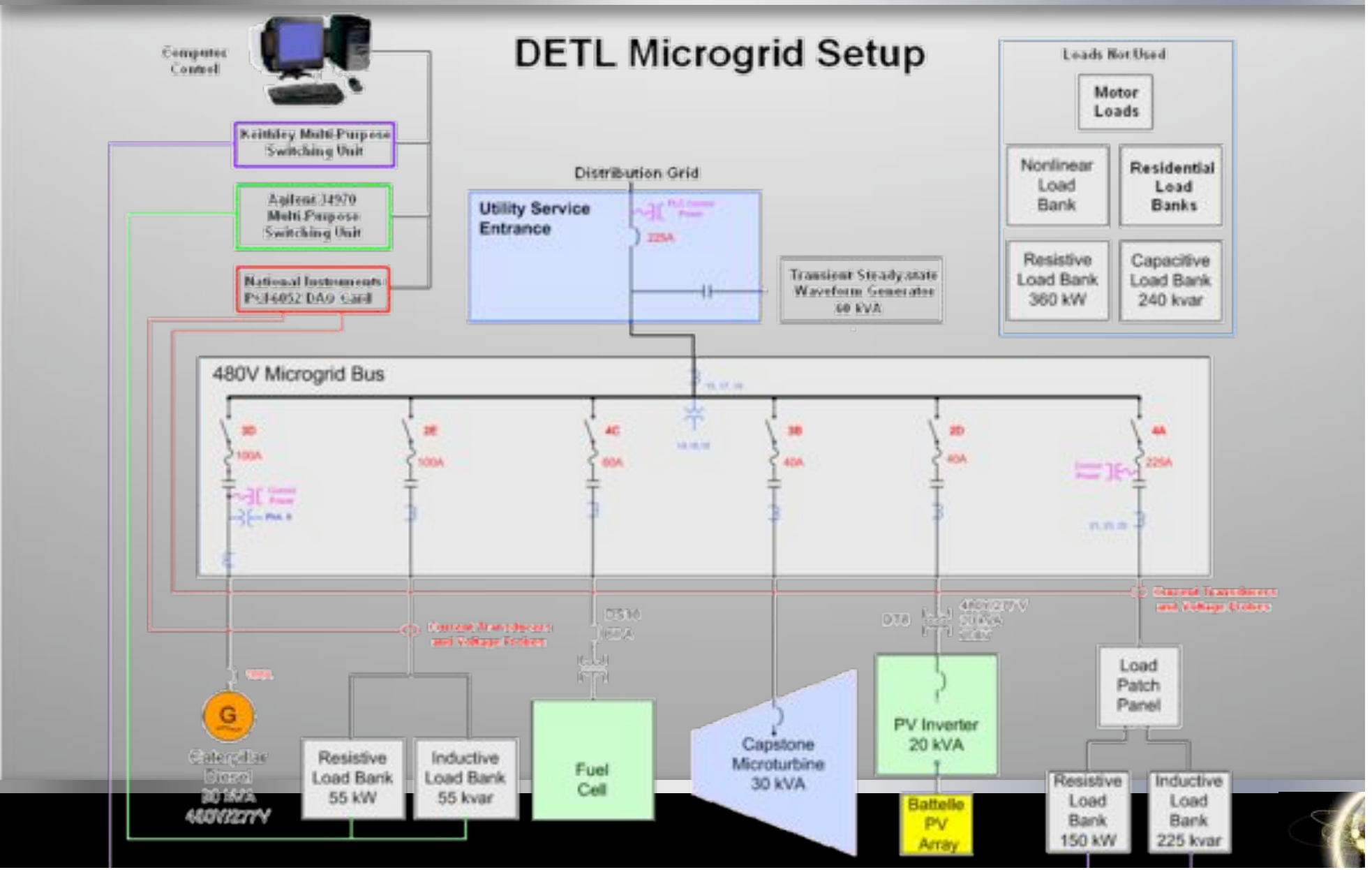
Threats addressed:

- The adversary controls commercial hardware and software supply chains
- The adversary has ongoing access to our systems through administration, configuration, and update

Properties of CodeSeal:

- Built and managed in a lifecycle apart from the COTS that they are designed to protect but cannot be influenced by that system
- Interfaced to the system you are attempting to protect
- Sufficiently low complexity to allow for meaningful and effective security analysis

Testing Cyber Security In a Physical Testbed



Contact Information

Juan Torres
Manager
Energy Systems Analysis
Sandia National Laboratories
jjtorre@sandia.gov
(505) 844-0809

Jennifer DePoy
Manager
Critical Infrastructure Syste
Sandia National Laboratori
jdepoy@sandia.gov
(505) 844-0891

CCSS Online - http://www.sandia.gov/scada