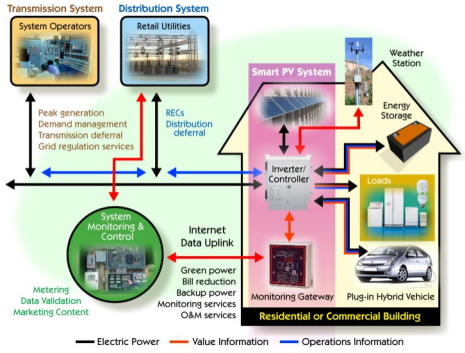
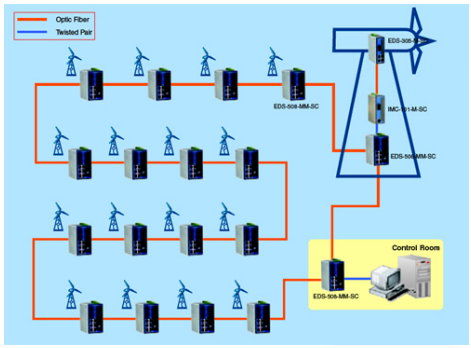
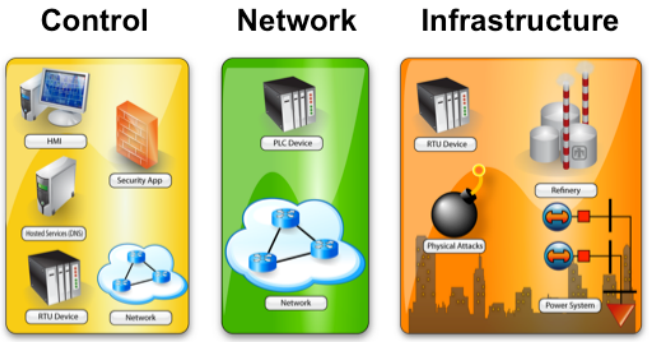
Exceptional service in the national interest

Sandia National Laboratories







Cyber Security for Renewable Energy

Jason Stamp, Ph.D.

Energy Surety Engineering and Analysis

U.S. DEPARTMENT OF ENERGY

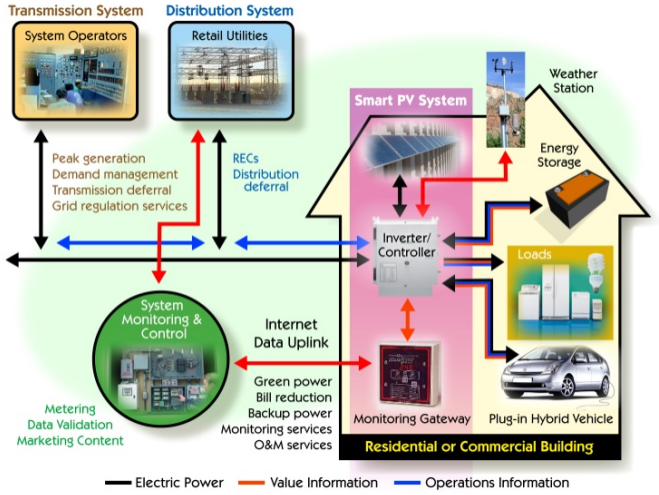
NNSA National Nuclear Security Administration

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

Renewable Systems Interconnection: Removing Barriers and Reducing Risk

Sandia National Laboratories

- The penetration of renewables is increasing
- We are addressing the challenges of engineering, integrating, operating, and maintaining power grid systems with high penetrations of renewables through:
  - Renewable energy and control system technology development
  - Advanced distribution systems
  - System level test and demonstration
  - Distributed renewable energy system analysis
  - System monitoring and assessment
  - Codes, standards, and regulatory advisement



15 MW PV Installation, Nellis Air Force Base, NV

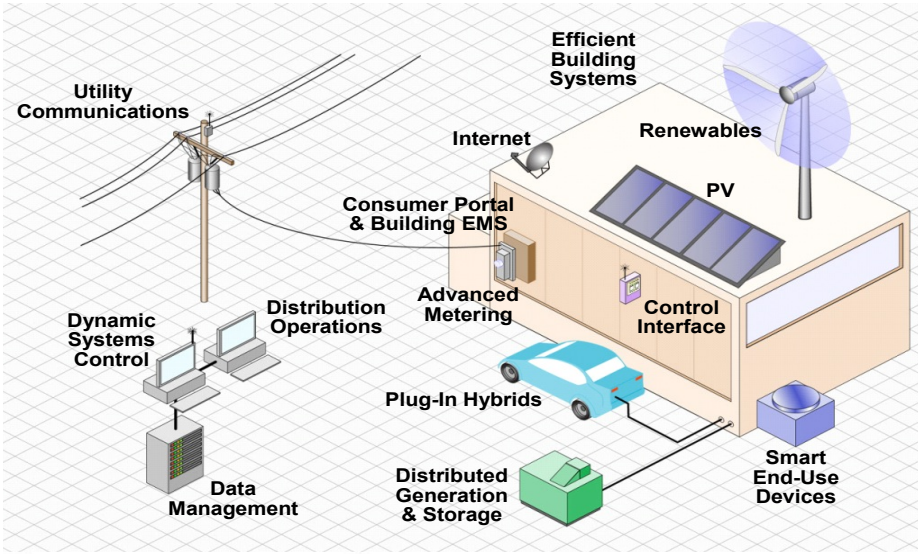
Source: SunPower Corporation

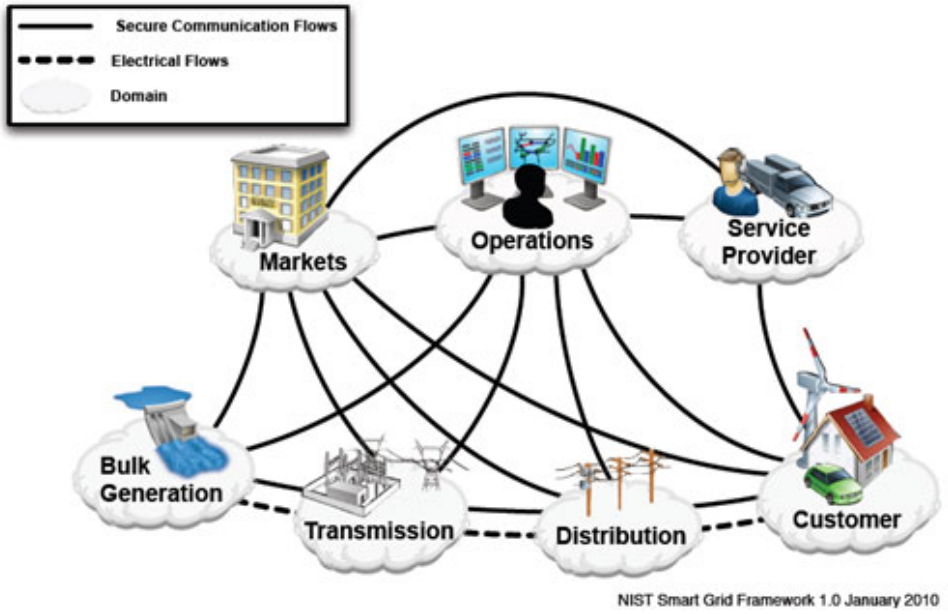
http://www1.eere.energy.gov/solar/rsi.html

Information is Critically Important

Sandia National Laboratories

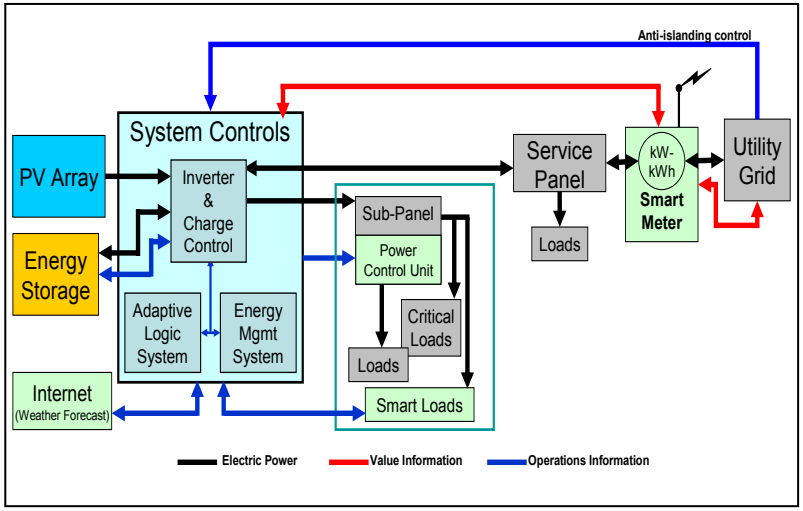
- New grid technology:
  - Distributed generation
  - Renewable generation
  - Energy storage
  - Advanced metering / control
- Necessitates decentralized management and control of the power system:
  - Ramp rate control
  - Voltage profile management
  - Fault identification and isolation
  - Controlled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





NIST Smart Grid Framework 1.0 January 2010

Trends Causing Increased Risk

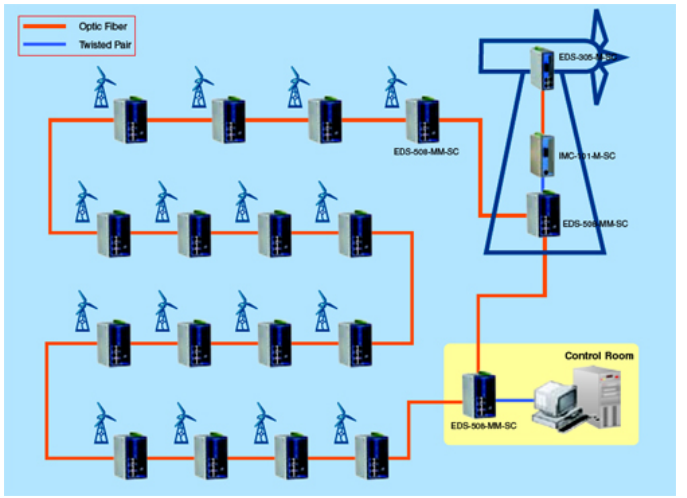


- Same issues as control systems in general:
  - Increasing interconnectedness
  - Standardized technologies / vulnerabilities
  - Connectivity of control systems to others
  - Insecure connections
  - Availability of technical information
  - Increasing reliance on automation
- Each control with physical or cyber access presents an intrusion point.
- Unlike the origins of fossil energy generation of electricity, many renewable systems use advanced controls, digital sensors, network architectures near generation sources
- Several issues should be considered regarding the interconnection of numerous renewable energy technologies
  - Diverse systems (hardware, software)
  - Numerous end nodes and access points at all locations across the grid
  - Number of data sources and sensors greatly increased
  - The need to protect data across widespread areas

Cyber Security for Renewable Energy

Sandia National Laboratories

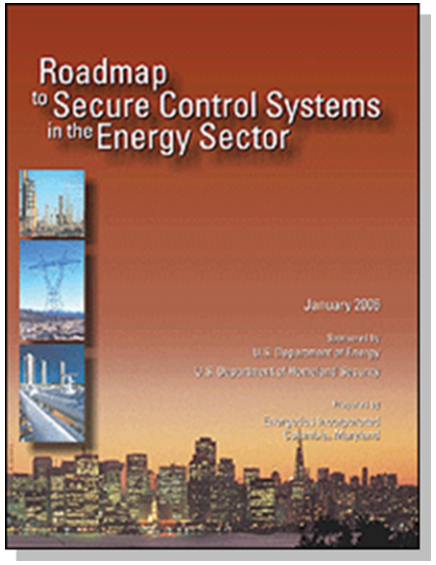
- Components:
  - Access must be controlled and data integrity must be maintained at each accessible point
  - Examples: advanced meter, photovoltaic inverter/ module, home energy management system, substation control system, field sensor, safety control system, smart appliance
- Renewable energy generation:
  - Depend on networking architecture and routers
  - Examples: solar dish/trough/panel array, wind aggregation stations, field weather and environmental data networks
- Interconnection scale key questions:
  - Should there be required/regulated protocols, physical and cyber security controls?
  - Who should be accountable for protecting the data and infrastructure at the many layers and end points?



Cyber Security Elements Needing Attention in Renewable Energy Systems

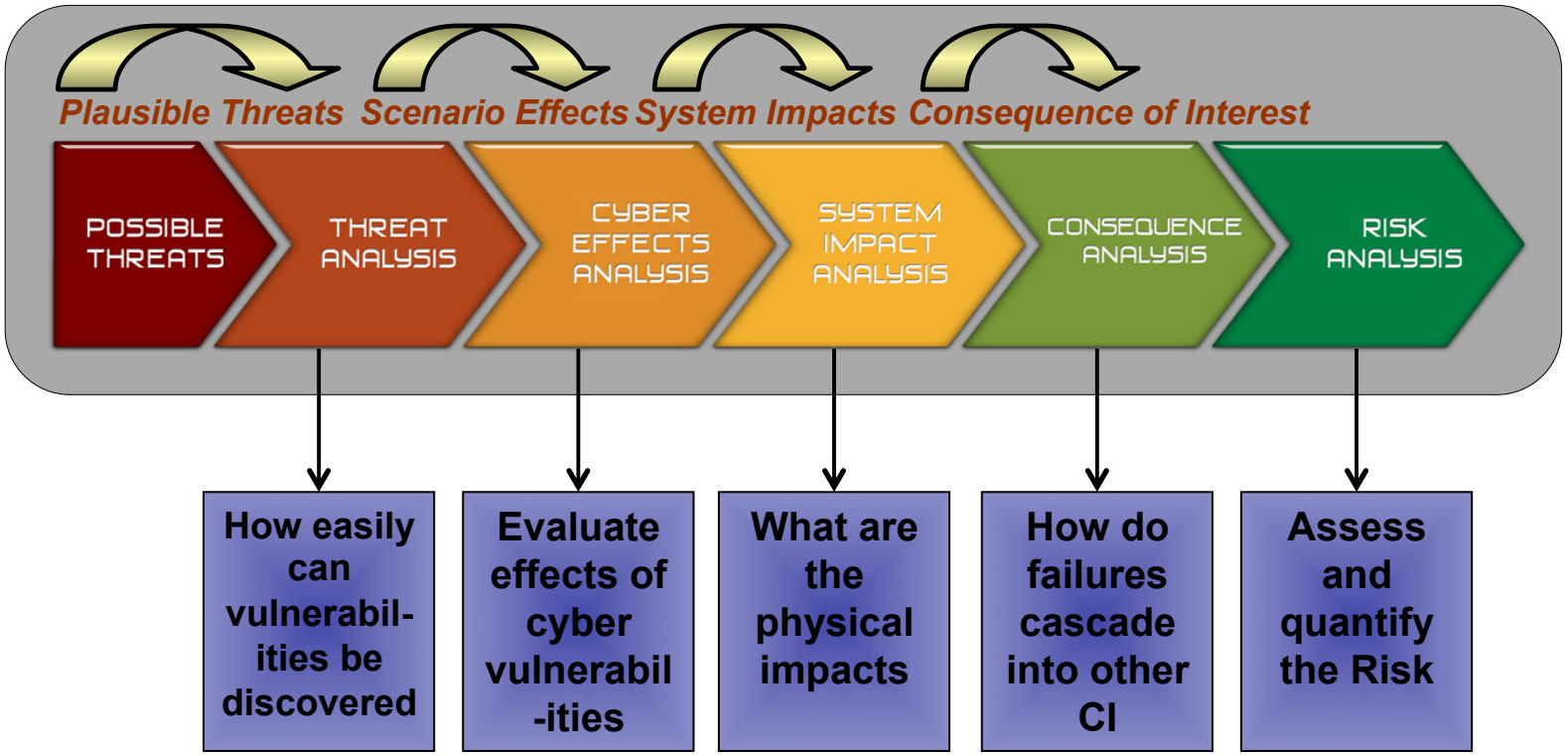
Sandia National Laboratories

- Cyber and Physical Access Control
- Authentication
- Intrusion Detection and Anomaly Detection
- Data Encryption
- Secure Protocols
- Secure Application Code
- Secure/Patched Operating Systems
- Life Cycle Maintenance and Scalability
- Operational policies and procedures that support human interaction with systems
- Emergency Response Plans
- Periodic Security Assessments



Risk Assessment Analysis

Sandia National Laboratories



Provides a Framework for Conducting Smart Grid Risk Analysis

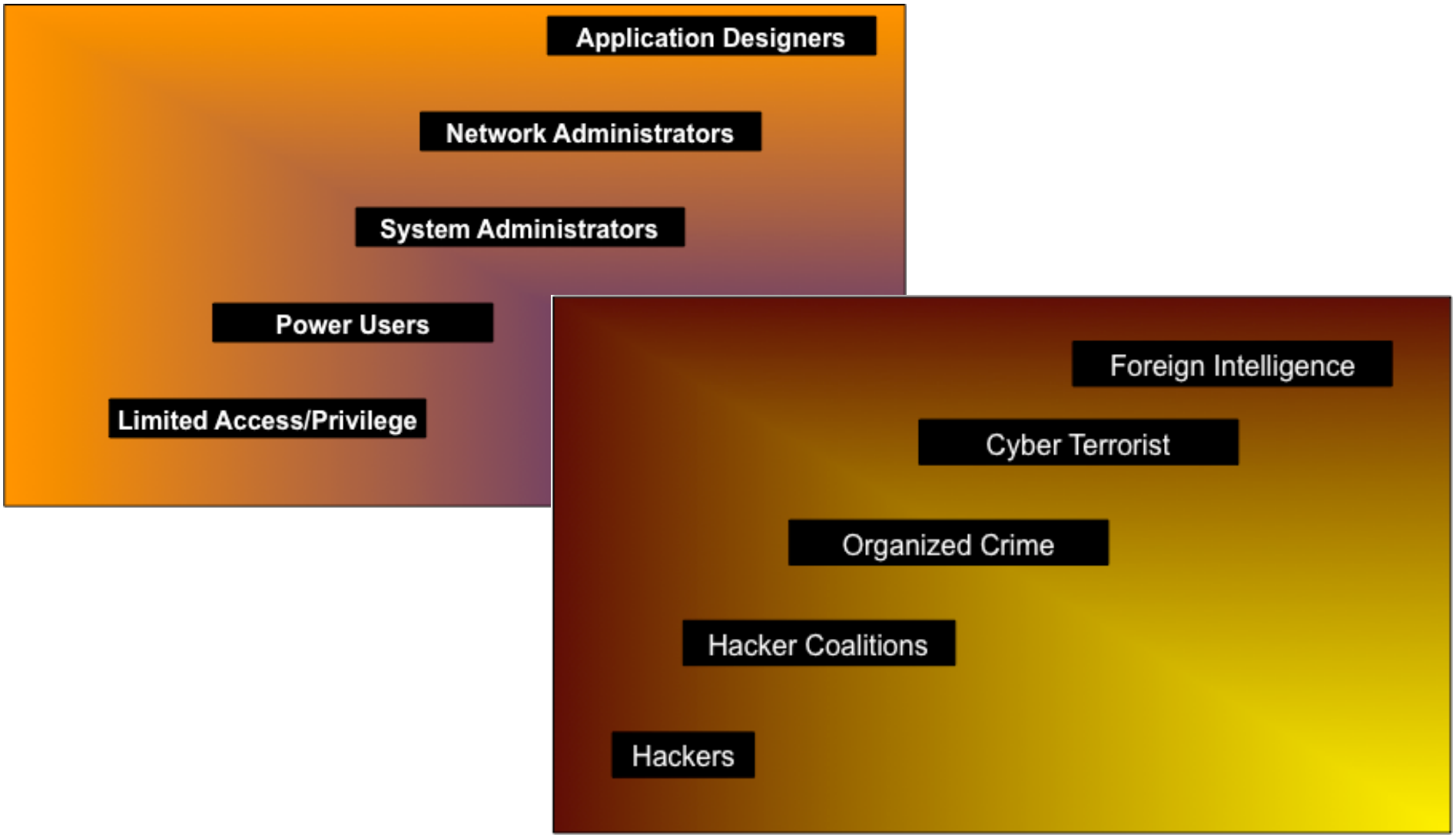
Threat Characterization

Sandia National Laboratories

- Characterizing security threats to process control systems on the electric grid should consider:
  - Implication of impending danger (i.e., what may an attacker do?)
  - Source of that danger (i.e., who is the attacker?)
- Threats are individual or groups with the potential to cause harm can be characterized by their level of access, motivations, and capabilities.
- Threats can be insiders, hackers or crackers, terrorists, organized crime, and nation states. Because of the intimate knowledge of assets and ready access to these assets, insider attacks can do substantial damage.

Range of Threats: Insider / Outsider Adversaries

Sandia National Laboratories



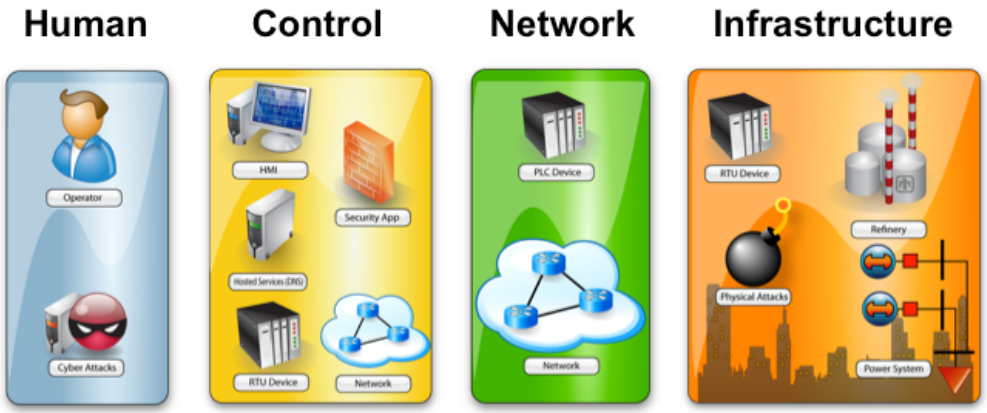
Generic Threat Matrix

Sandia National Laboratories

"Categorizing Threat: Building and Using a Generic Threat Matrix," by David Duggan, Sherry Thomas, Cindy Veitch, Laura Woodard; Sandia National Laboratories Technical Report SAND2007-5791.

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	KNOWLEDGE CYBER	KNOWLEDGE KINETIC	ACCESS
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

Cyber Security Design and Testing

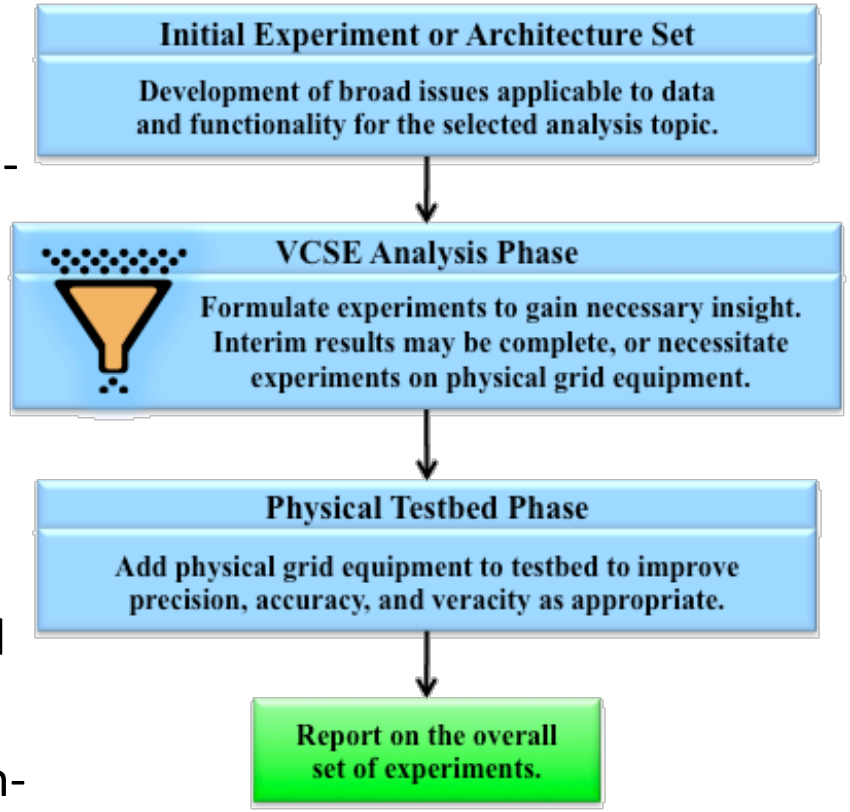


- Use cases:
  - Automated grid control
  - Supervisory control
  - Protective relaying
  - Configuration management
  - Connections to other systems
- Controls design must ensure expected performance meets standards for power quality, voltage, frequency, protection, etc.
- Must protect the DATA and the FUNCTIONALITY associated with these
- Test cases for cyber security:
  - Usability: how difficult is it to install, maintain, and use the cyber security architecture? Does it function reasonably (i.e. it can't take 20 minutes to log into a system)?
  - Functionality: how well does the cyber security architecture function against possible attacks?
  - Transparency: does the cyber security architecture interfere with normal operations (i.e. it can't introduce latency on a protective relaying channel)?

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

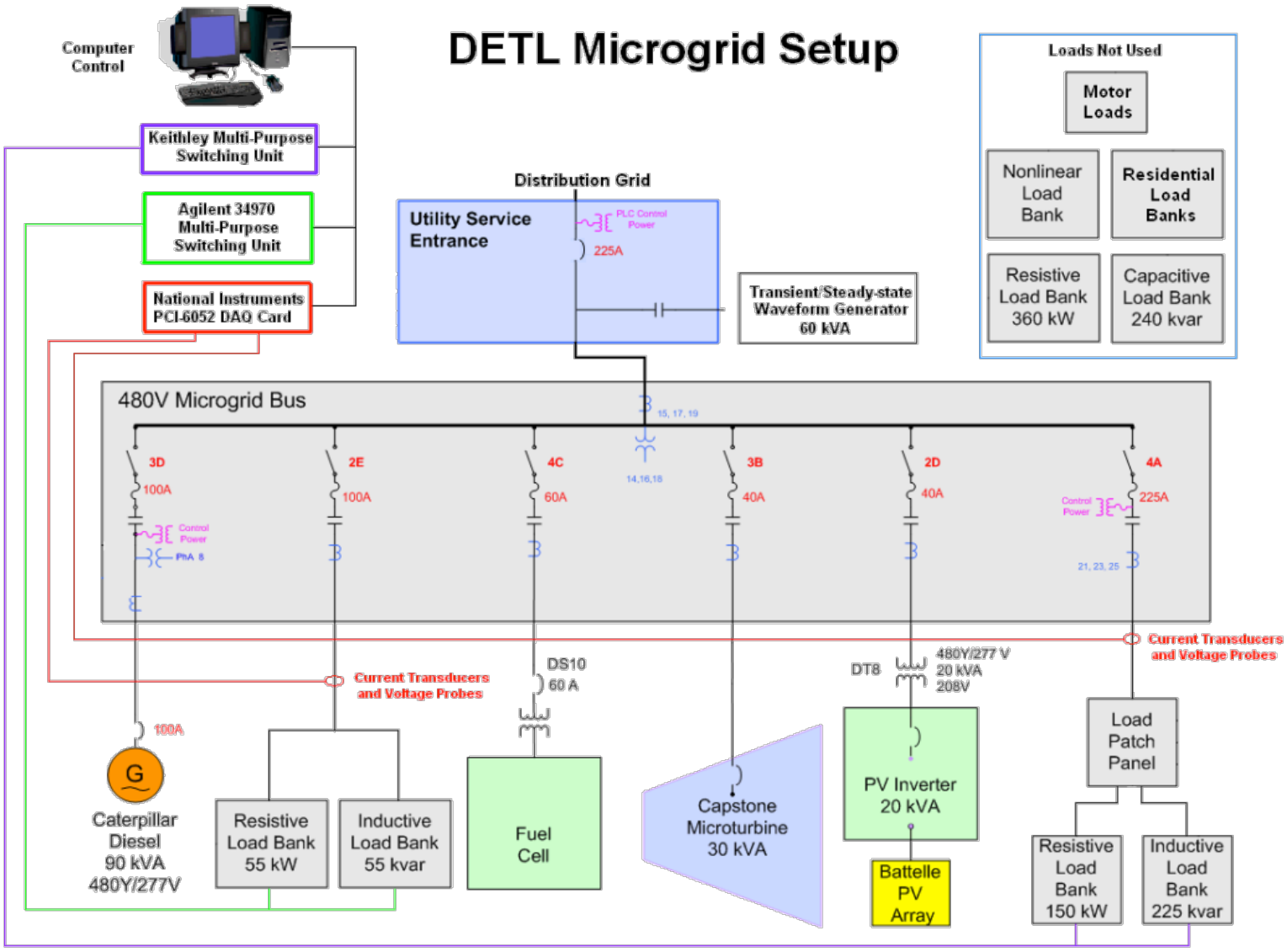
Sandia National Laboratories

- Variable fidelity modeling environment
- LVC (Live-Virtual-Constructive)
- Design is supported by testbed environments (perhaps of the simulated-emulated-physical sort) over design domains of controls, communications / networking, and the electrical energy system
- Test system assets can be retained to support red team/auditing practice
- Execute cyber attacks and assess control system impacts
- Enables real-time, hardware/software-in-the-loop analysis



Testing Cyber In a Physical Testbed

Sandia National Laboratories



Discussion

Jason E. Stamp, Ph.D.
Distinguished Member of the Technical Staff
Sandia National Laboratories
PO Box 5800, Albuquerque, New Mexico 87185-1108
505-284-6797, jestamp@sandia.gov

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