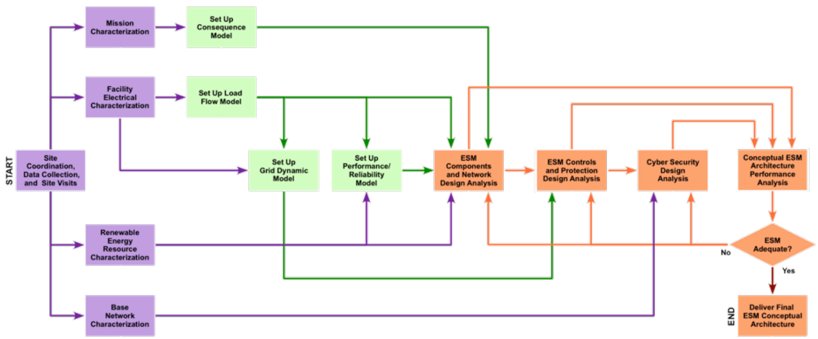
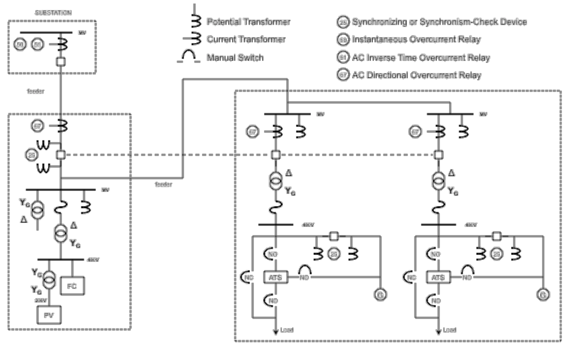
SAND2012-6725C

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

Energy Surety

Energy Surety Elements	
Safety	Safely supplies energy to end user
Security	Maintains power in a malevolent environment
Reliability	Maintains power when and where needed
Sustainability	It can be maintained for mission duration
Cost Effectiveness	Produces energy at lowest predictable cost

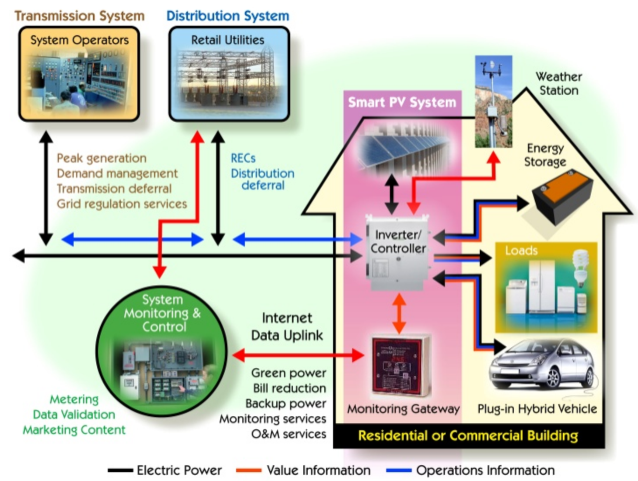
A framework for improving mission readiness

Renewable Systems Interconnection

Removing Barriers and Reducing Risk

Sandia National Laboratories

- The penetration of renewables is increasing
- The power grid was not designed for variable generation and bi-directional power flow
- 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



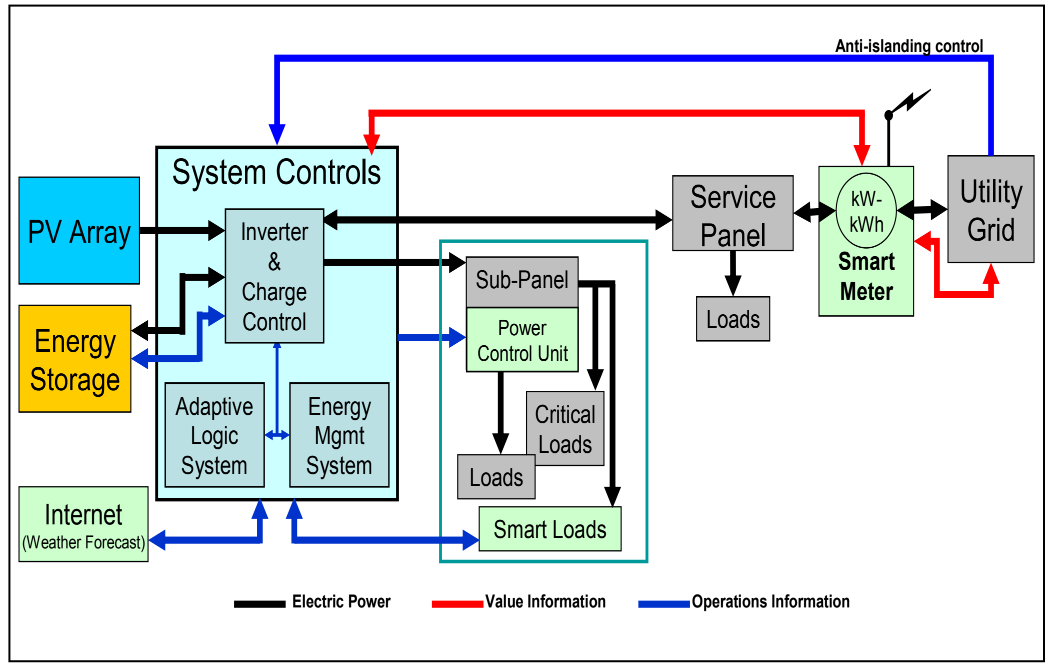
15 MW PV Installation, Nellis Air Force Base, NV

Source: SunPower Corporation

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

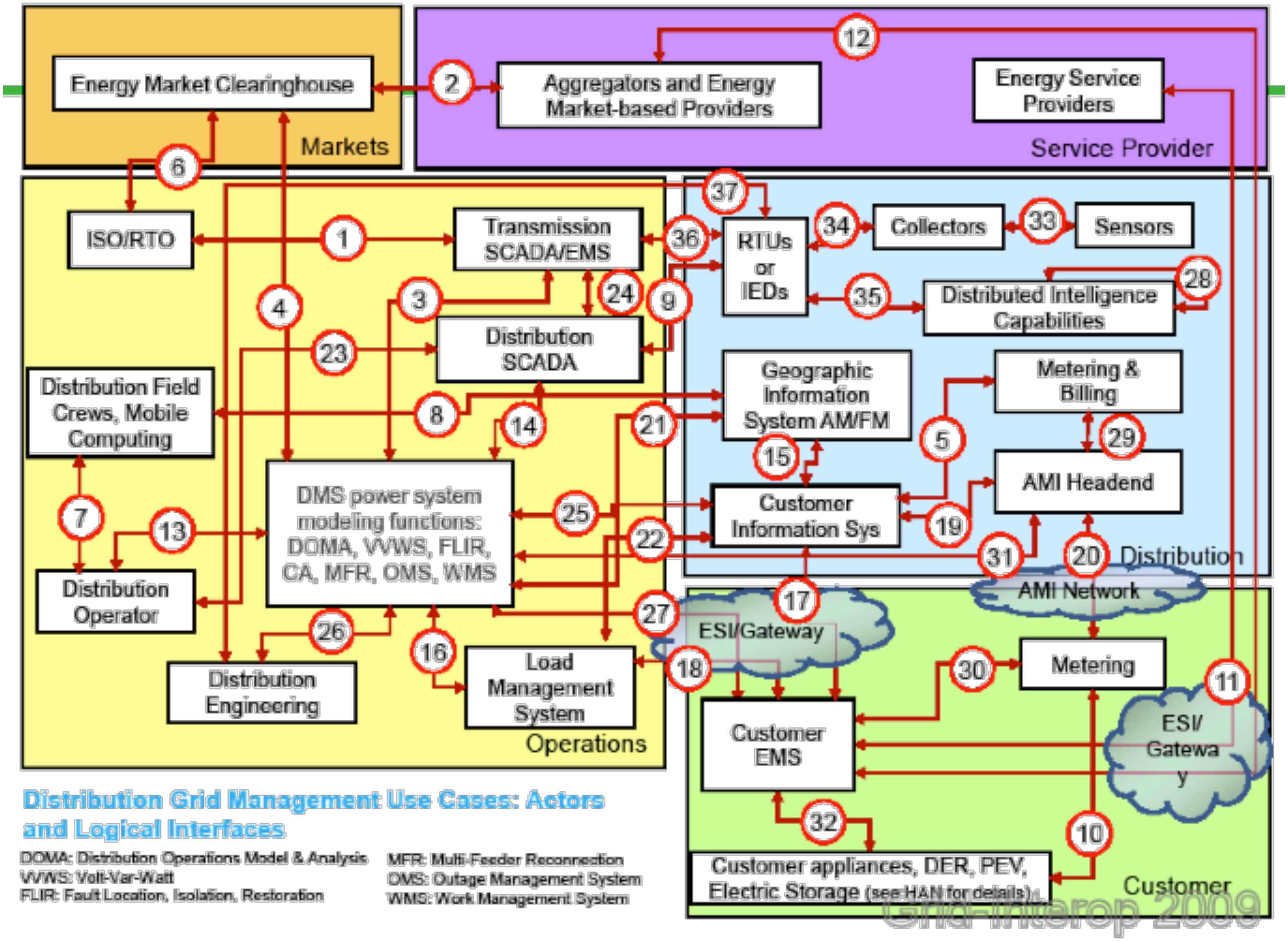
Information is Critically Important

- 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



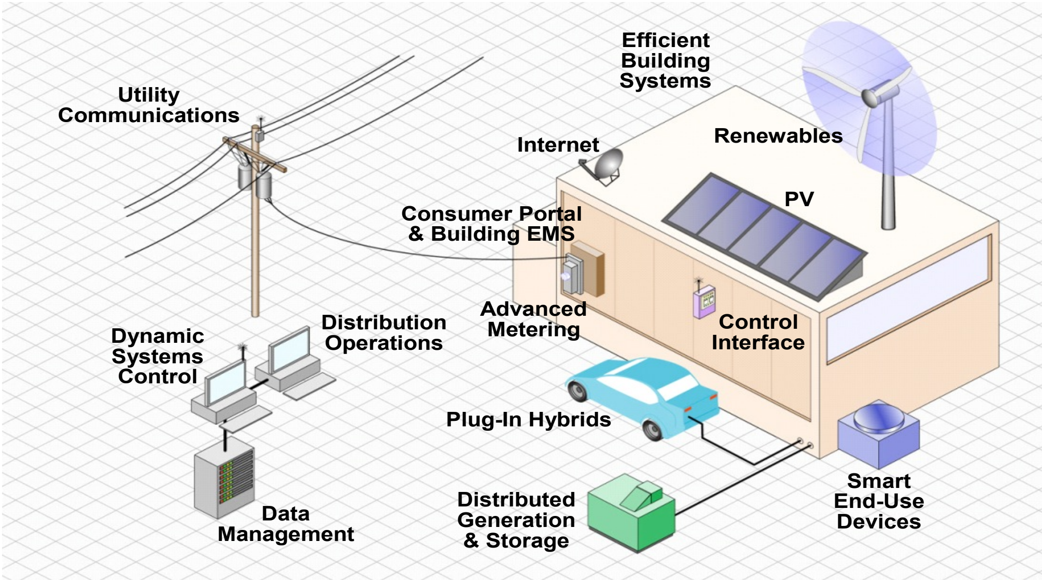
Smart Grid Includes Complex Information Flows

Sandia National Laboratories



Trends Causing Increased Risk

- Increasing interconnectedness at all levels
- Adoption of standardized technologies with known vulnerabilities
- Connectivity of control systems to other networks
- Insecure connections
- Widespread availability of technical information about control systems
- Increasing reliance on automation



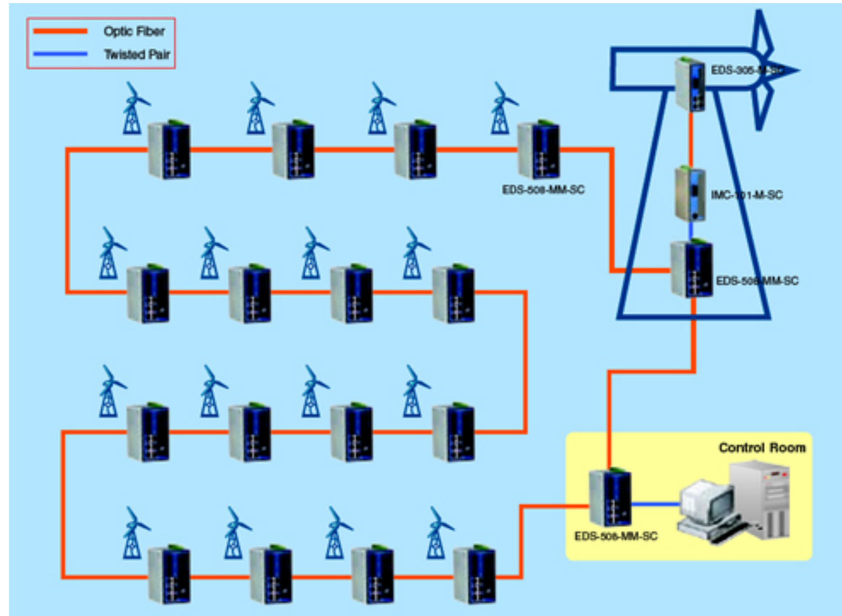
Cyber Security at the Component Level

- Each control with physical or cyber access presents an intrusion point.
- Access must be controlled and data integrity must be maintained at each accessible point.
- Examples of components might be:
  - Advanced meter
  - Photovoltaic inverter
  - Photovoltaic module
  - Home energy management system
  - Substation control system
  - Field sensor
  - Safety control system
  - Smart appliance

Cyber Security at the Generation Level

Sandia National Laboratories

- Unlike the origins of fossil energy generation of electricity, many renewable systems use advanced controls, digital sensors, network architectures near generation sources.
- Examples of generation level considerations:
  - Solar dish/trough/panel sensor
  - Wind control stations
  - Field weather and environmental data sensors
  - Networking architecture and routers



Cyber Security at Interconnected Levels

- 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 (encryption)
- 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?
  - Will standardized technology simply lead to a single target (i.e. common operating systems)

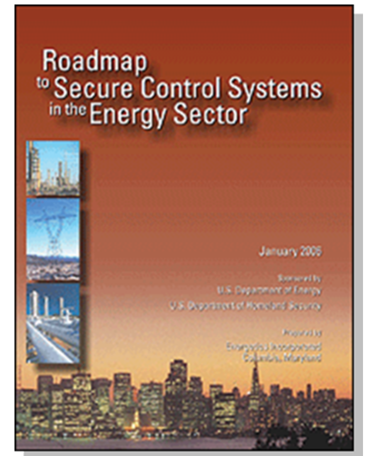
Cyber Security Elements Needing Attention in Renewable Energy Systems

- 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

An Integrated Risk Analysis Approach Is Important for Cyber Security

Sandia National Laboratories

- *"By systematically documenting and prioritizing known and suspected control system vulnerabilities [threats] and their potential consequences, energy sector asset owners and operators will be better prepared to anticipate and respond to existing and future threats."*
  - **Roadmap to Secure Control Systems in the Energy Sector, Identifying Strategic Risk (pg.A2)**
    - **January 2006**



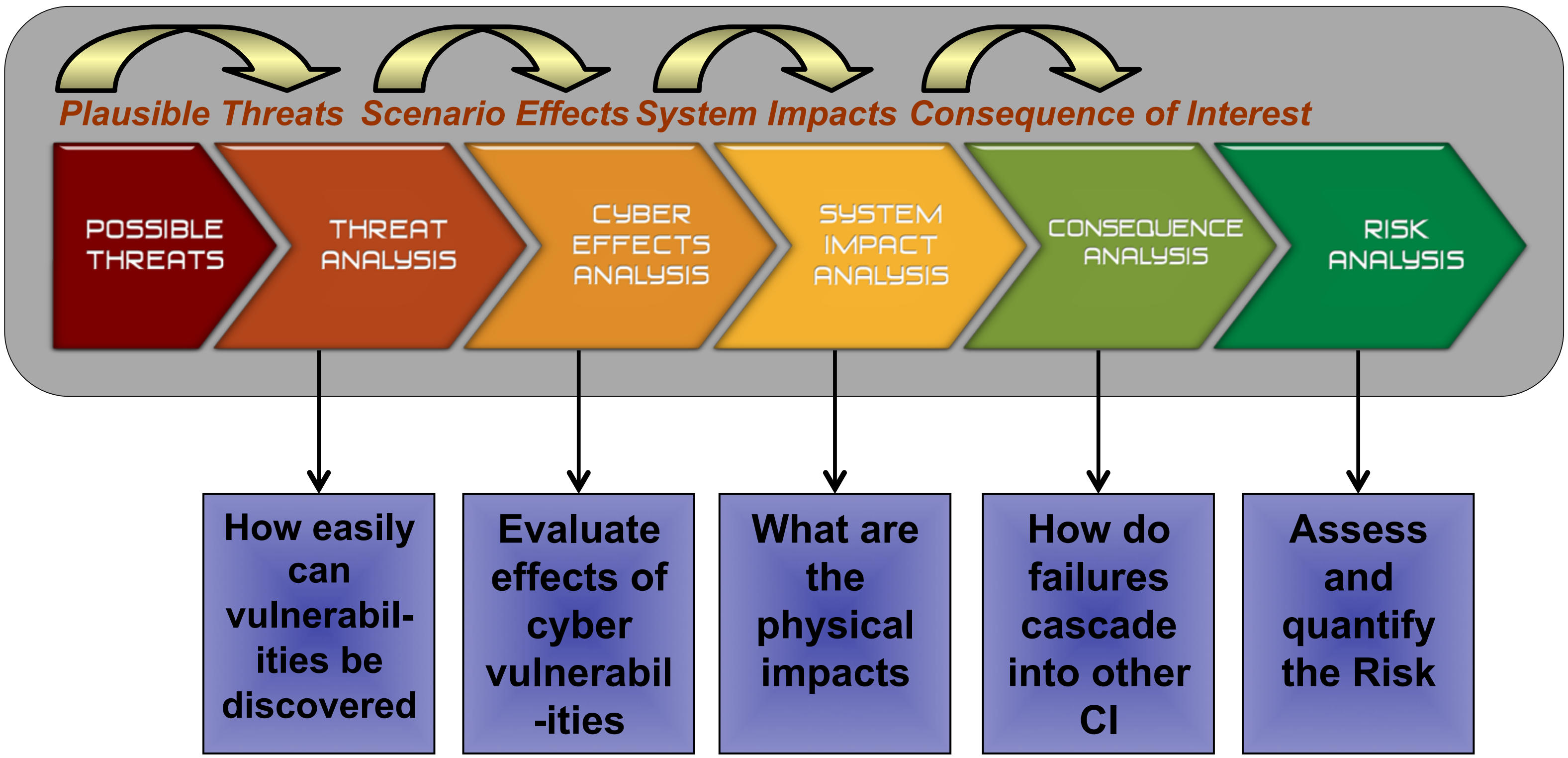
"Assess Risk: Determine risk by combing potential… consequences of a terrorist attack...known vulnerabilities…and general or specific threat information."

Homeland Security

National Infrastructure Protection Plan (NIPP), Risk Management Framework
Department of Homeland Security, 2005

Risk Assessment Analysis

Sandia National Laboratories



Provides a Framework for Conducting Smart Grid Risk Analysis

Cyber Security for Control Systems

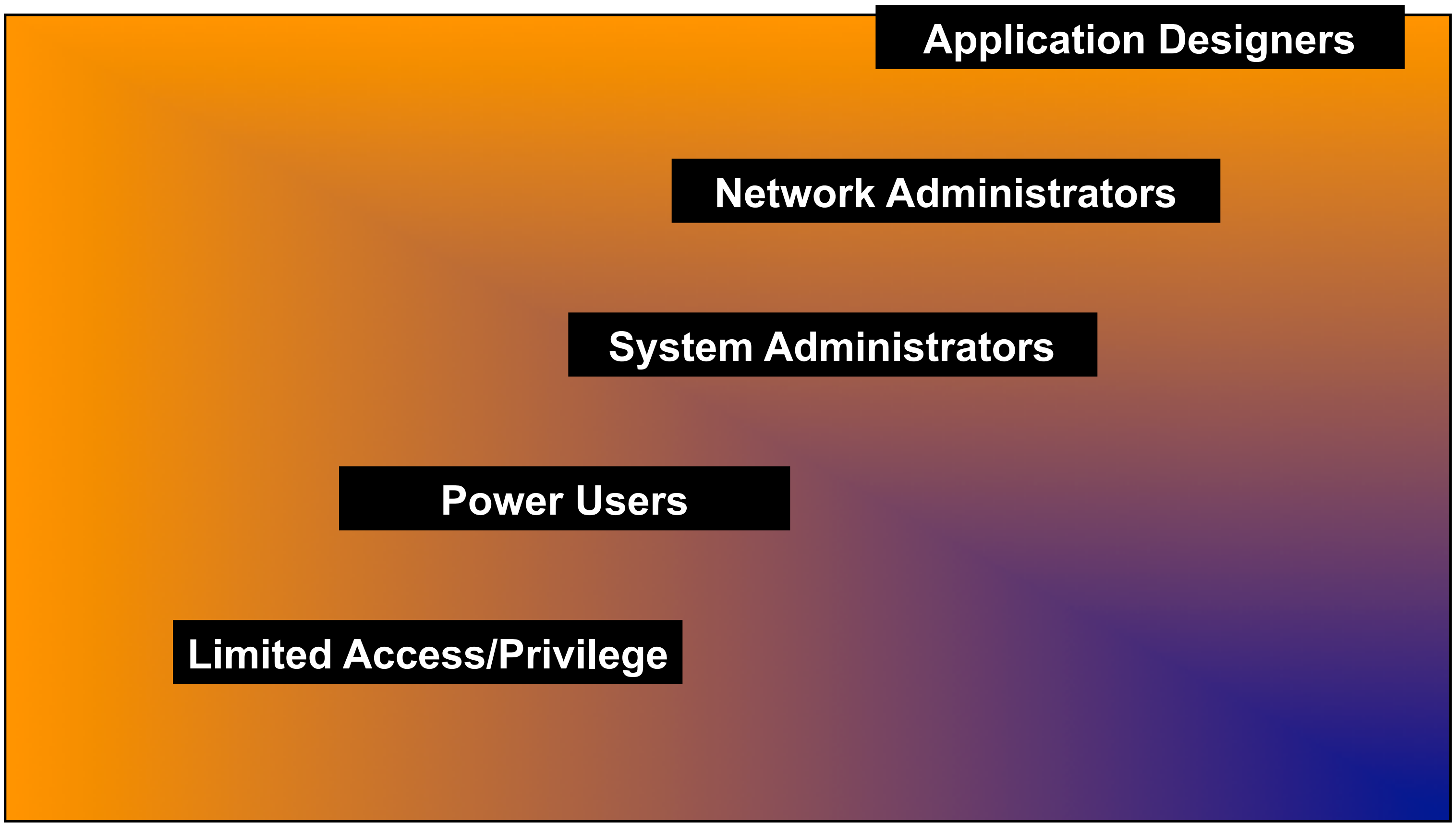
- Controls use cases:
  - Automated grid management and control – frequency, voltage, load management, etc (anything automated, second-to-second requirements)
  - Supervisory control – human-in-the-loop grid management (i.e. base command decides to energize priority load)
  - Protective relaying – specific channels dedicated to coordination between relays (also automated, time sensitivity on the order of cycles)
  - Configuration management – remote device (re)configuration, downloading fault data, engineering configuration and management, etc.
  - Connections to other systems: with utility systems for ancillary services, and with building systems for efficiency / load management
- Controls design must ensure expected microgrid performance meets standards for power quality, voltage, frequency, protection, etc.
- Must protect the DATA and the FUNCTIONALITY associated with these

Threat Characterization

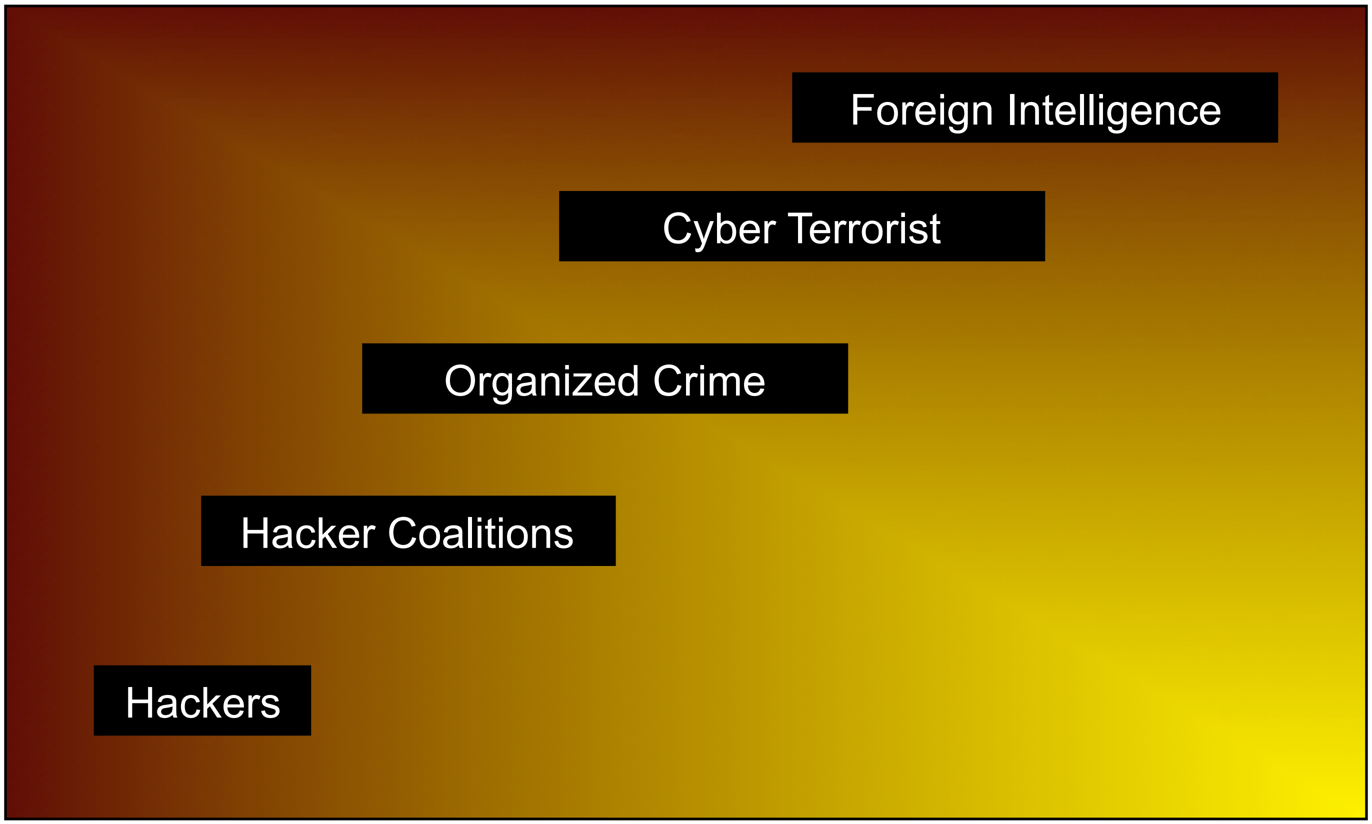
Sandia National Laboratories

- 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 Adversaries



Range of Threats: Outsider Adversaries



Generic Threat Matrix

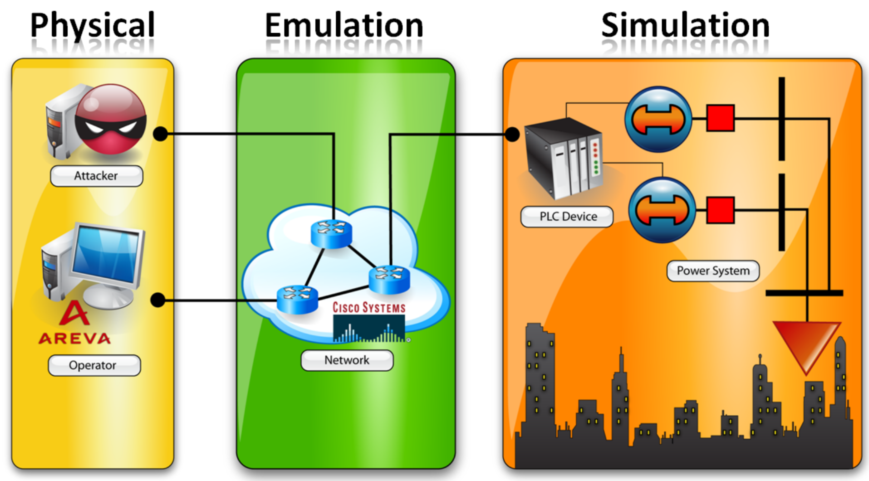
"Categorizing threat : building and using a generic threat matrix." by *Sandia National Laboratories, Albuquerque, NM, Duggan, David Patrick, Thomas, Sherry Reede, Veitch, Cynthia K., Woodard, Laura*. Sandia Technical Report SAND2007-5791.

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
					KNOWLEDGE		
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	CYBER	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

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

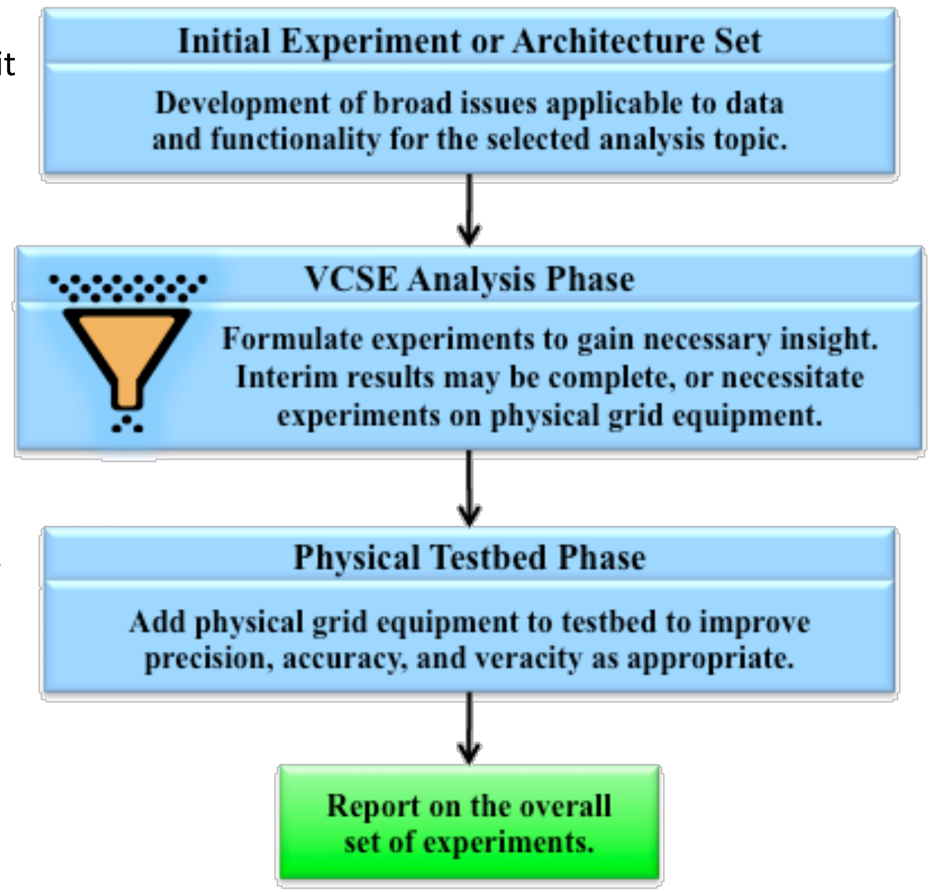
Sandia National Laboratories

- 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



Cyber Security Analysis Process

- Test cases for cyber
  - 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)?
- Design is supported by testbed environments (perhaps of the simulated-emulated-physical sort) over microgrid design domains of controls, communications / networking, and the electrical energy system
- Test system assets can be retained to support red team/auditing practice

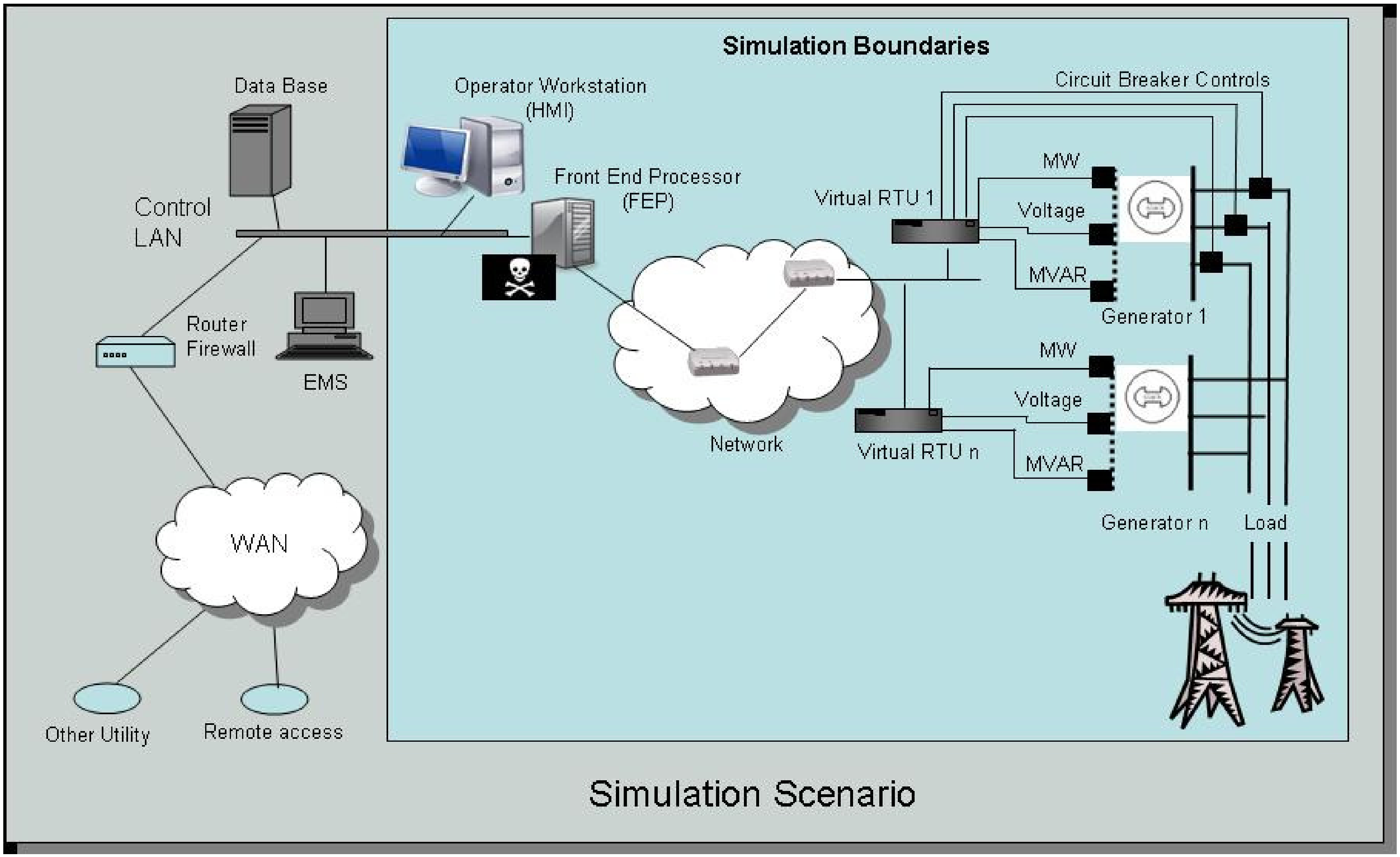


VCSE Heterogeneous Simulation Technologies

Domain	Physical	Emulated	Simulated
Control	PLC, SCADA, relays, historian…	Virtual SCADA server; Soft PLC; VMWare ESXi, virtual historian…	RTU model, relay model, simulated ladder logic…
Network	Cables, firewalls, routers, NIDS…	DynaMIPS (CISCO router); QEMU…	OPNET (SITL), routing model, wireless channel model…
Power Grid	(1)	N/A	Solar/wind models, SimPowerSystems, load flow software…

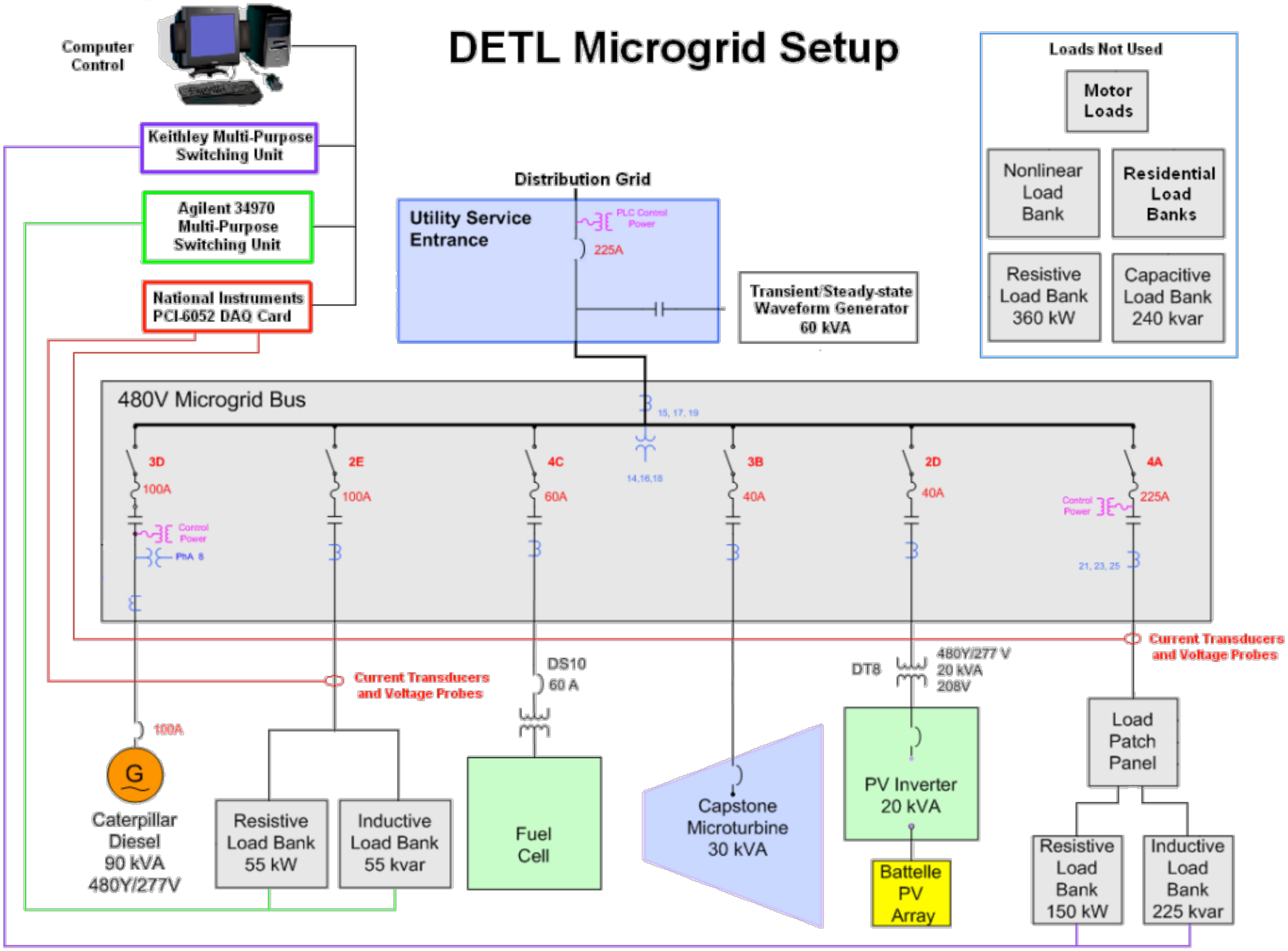
(1) Not yet integrated with VCSE, may include diesel generators, PV system, breakers, batteries…

VCSE Power Grid Model



Testing Cyber Security 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