SAND2010-3881P

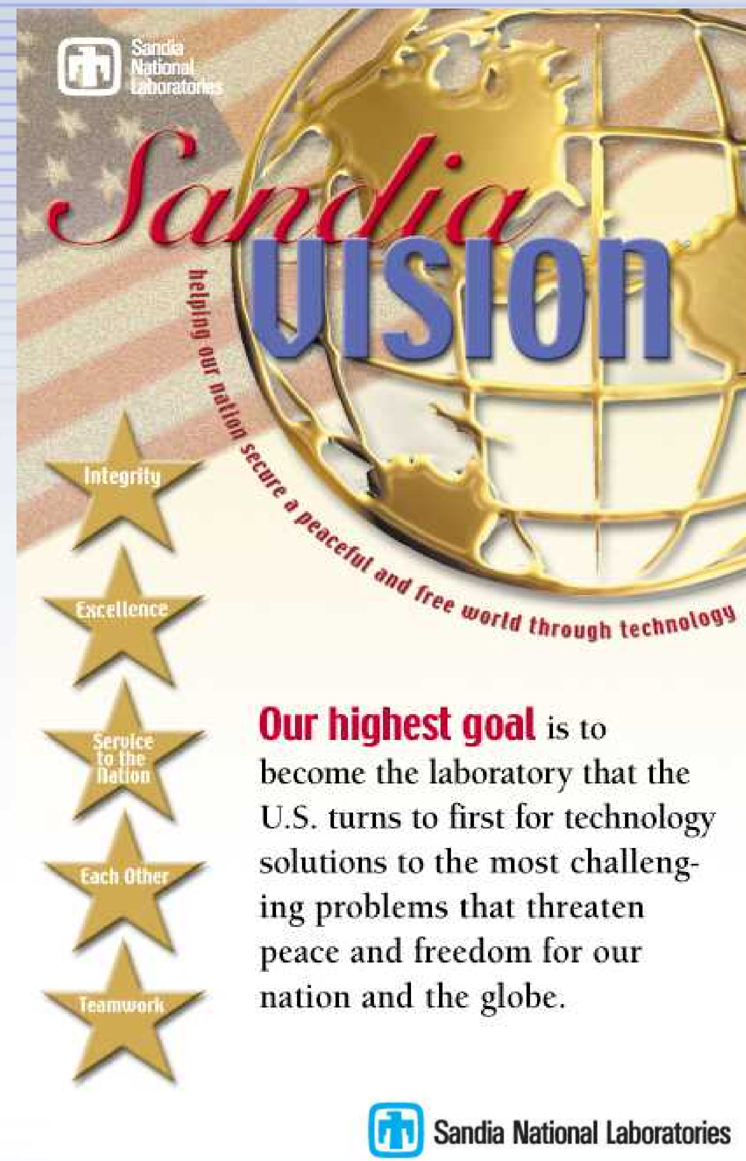
Cyber Threat Characterization: Electric Power Grid

Juan Torres
Manager, Energy Systems Analysis
(505) 844-0809
jjtorre@sandia.gov
www.sandia.gov/scada

Sandia National Laboratories is a multi program laboratory 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.

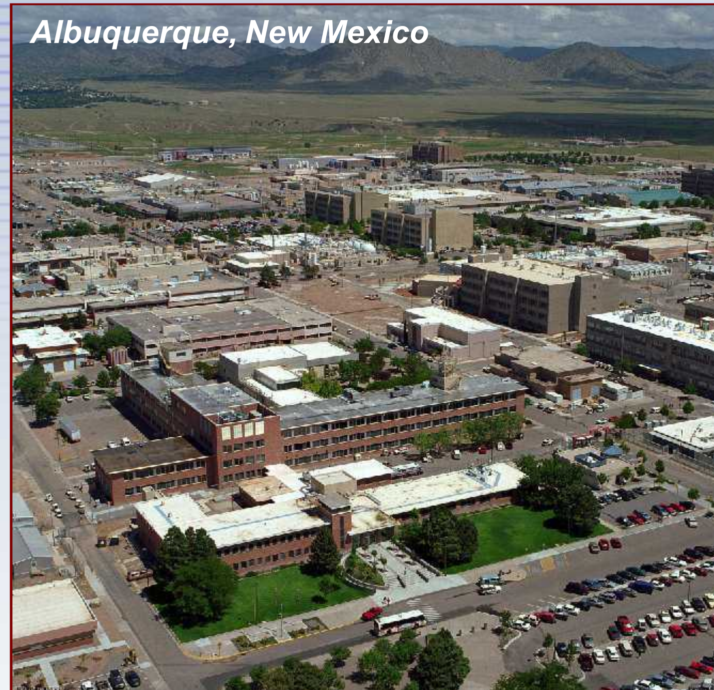
Sandia National Laboratories
"Exceptional Service in the National Interest"

- National Security Laboratory
- Broad mission in developing science and technology applications to meet our rapidly changing, complex national security challenges
- Safety, security and reliability of our nation's nuclear weapons stockpile



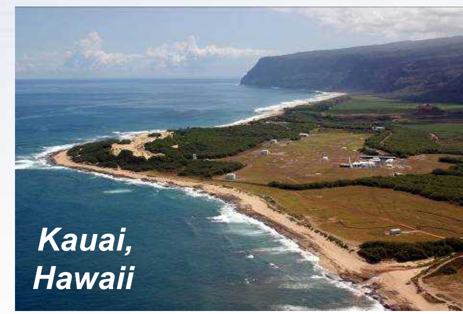
Sandia National Laboratories is Geographically Distributed

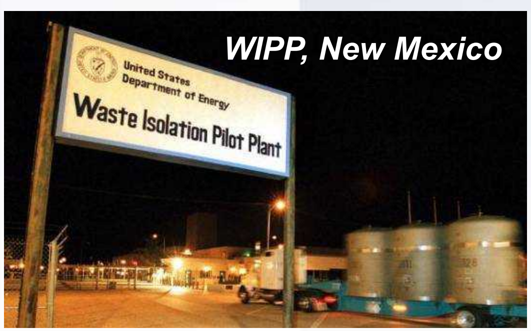

Tonopah, Nevada


Albuquerque, New Mexico

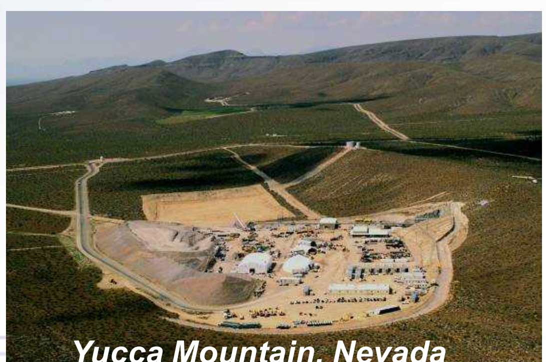

Kodiak, Alaska


Pantex, Texas


Kauai, Hawaii



WIPP, New Mexico

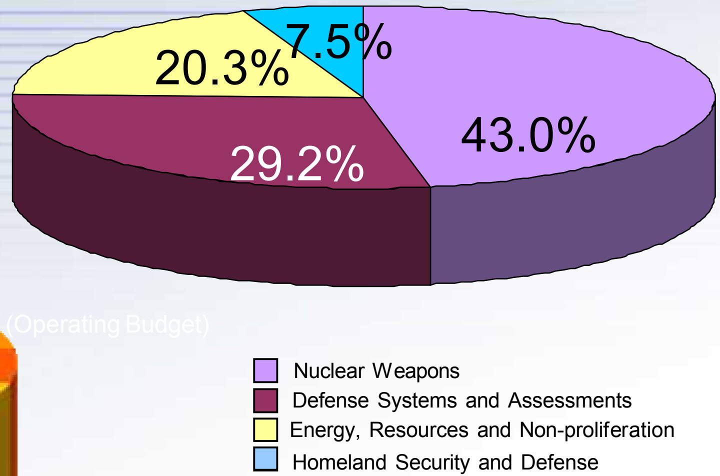

Yucca Mountain, Nevada


Livermore, California

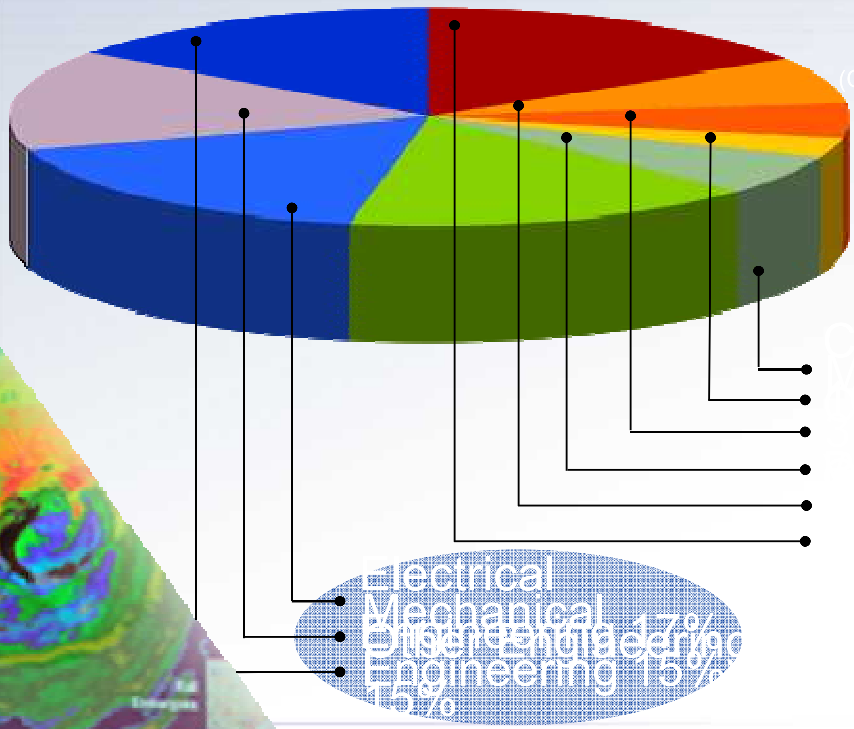
People and Budget

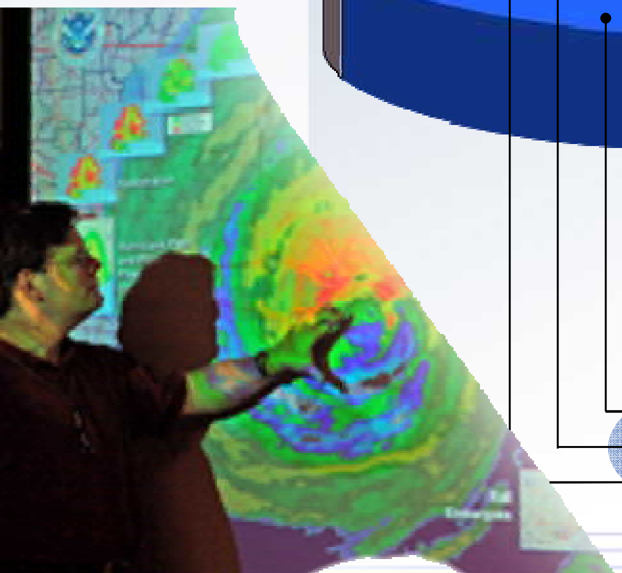
- FY07 permanent workforce: 8,478
- FY07 budget: $2.4B

FY07 Operating Revenue
$2.3 B



Technical Staff (3,921) by Degree
(Start of FY08)





Sandia National Laboratories

The DOE National SCADA Test Bed

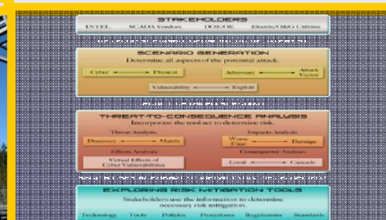
Reducing energy infrastructure security risk through asset-owners and solution providers

Reducing security weaknesses in today's SCADA technology:

- SCADA/EMS system Assessments
  - -- 9 Systems
- Completed: ABB, AREVA, GE, Siemens
  - -- 85% of vendors
- Cryptographic analysis of AGA-12 serial link encryption

Development of an Integrated Risk Analysis capability:

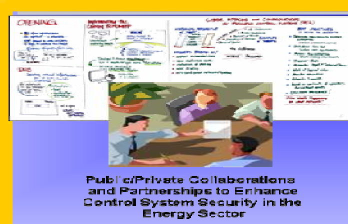
- Modeling/Simulation to evaluate end-to-end cyber security risk – answer the questions: So What?; Should we be concerned?



- Threat discovery
- Effects, Impacts M&S, & Consequence analysis
- Assessing newly found Vulnerabilities

Outreach and Awareness:

- CS security training courses:
  - -- Red Team/Blue Team
  - -- 450 attended over the past 12mnths
- Mitigation Techniques for NERC "Top-10" vulnerabilities
- Standard Catalog
- NERC CIP Assessment Guidelines
- Focus of Program to expand to Oil and Gas industry



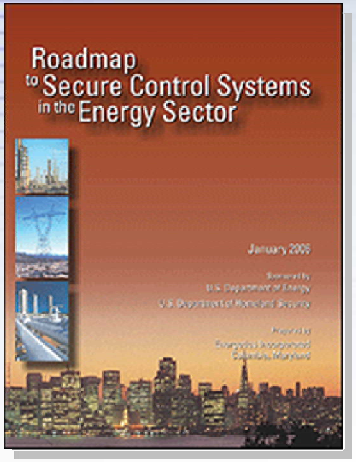
Development of next generation security solutions:

- Virtual Control Systems Environment
- Open PCS Security Architecture Interoperable Design (OPSAID)
- Network Mapping tool (ANTFARM)
- Trust-Anchor for Supply-Chain threat

Sandia National Laboratories

An Integrated Risk Analysis Approach is Important for Cyber Security

- ***"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

Sandia National Laboratories

Cyber Risk and the Role of Threat

Characterization of Risk to the Grid

- Risk in terms of threat, vulnerability, and consequence.

THREAT X VULNERABILITY X CONSEQUENCE RISK

Resources *Weaknesses* *Effect* *Business Impact*

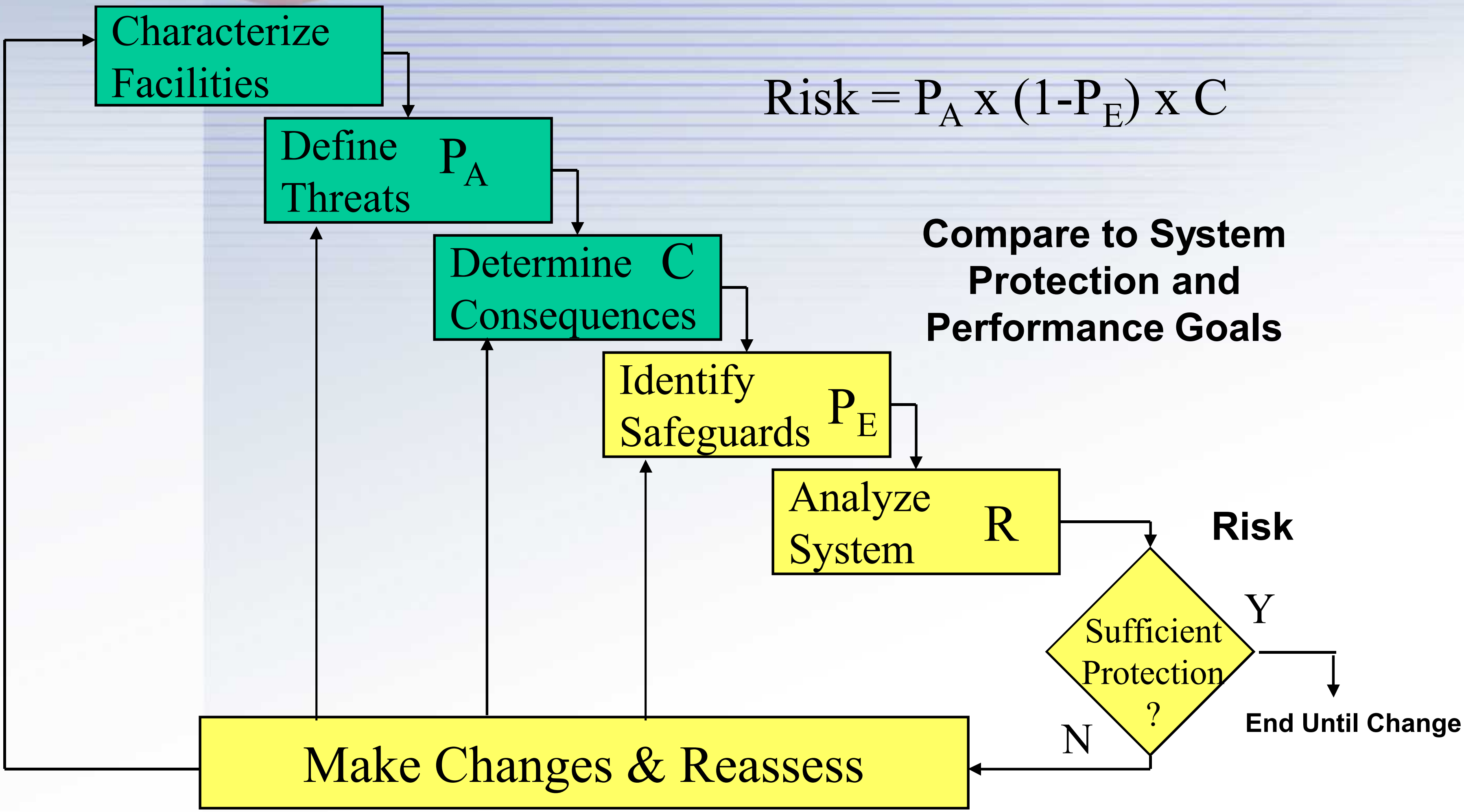
Physical Impact

- Threat is the entity able to do harm, intentionally or unintentionally. Can be a human, a weather event, a mechanical failure, etc.
- Vulnerability is a weakness in the system that can be exploited.
- Consequence is the resulting effect when a threat exploits a vulnerability.

Risk Analysis for Energy Systems

$$Risk = P_A \times (1-P_E) \times C$$

Compare to System Protection and Performance Goals



Threat Characterization

- 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 individuals 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

Application Designers

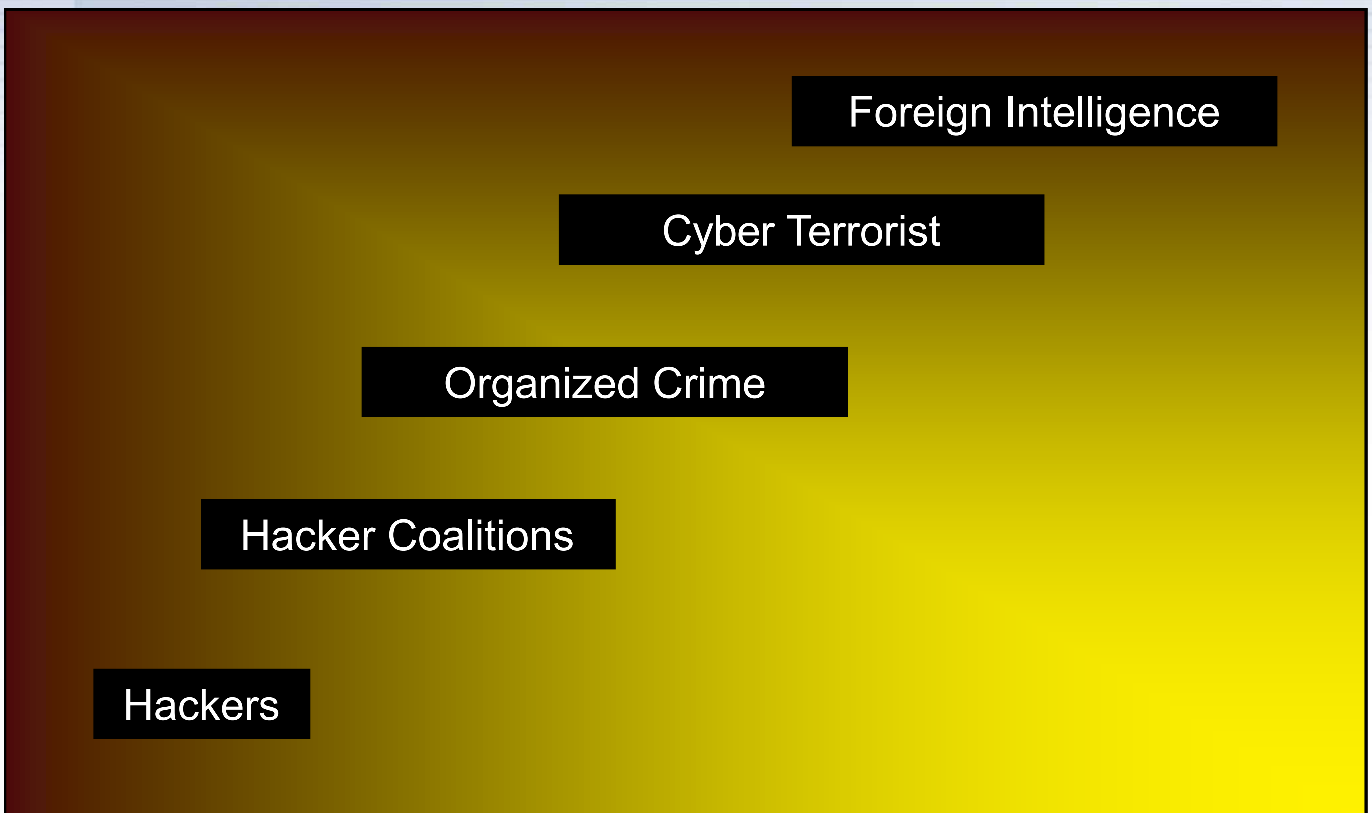
Network Administrators

System Administrators

Power Users

Limited Access/Privilege

Range of Threats: Outsider Adversaries



Example: Who is the Threat?

- UK citizen accused of crashing systems at the Port of Houston by DoS attack and hacking on its computer systems on 20 Sep 2001
  - Attack froze web service, containing vital data for shipping, mooring companies and support firms responsible for helping ships navigate in and out of the harbor
  - Attack traced to a computer at Caffrey's UK home by US police
  - Allegedly aimed at taking a South African chatroom user offline whose comments were attacking the US. Caffrey allegedly took offense at the comments because his girlfriend was American
- Specific lessons
  - IT systems vital in overall control system
  - Distance is not a factor
  - Damage may be a collateral effect of other hostile acts

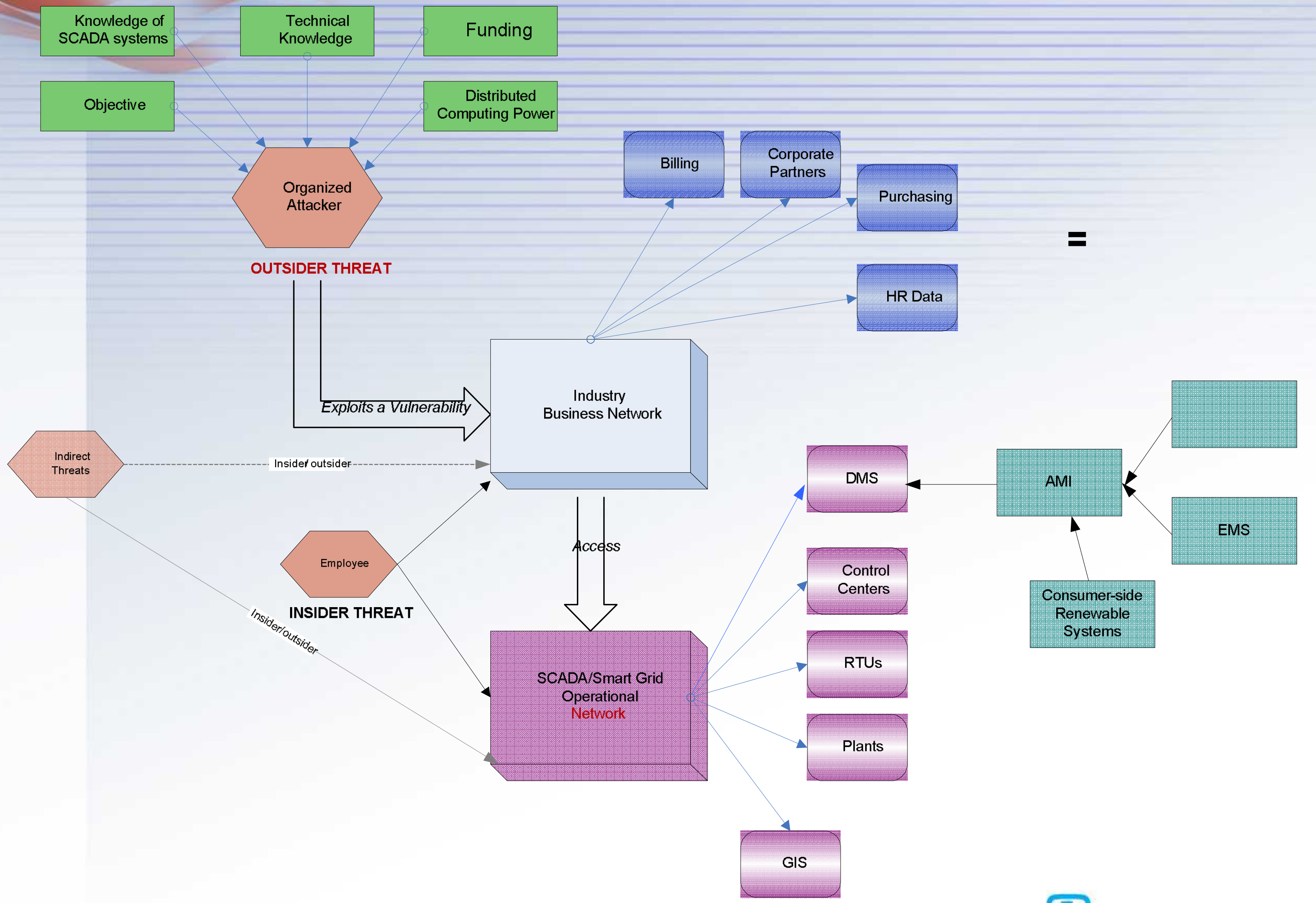
Port of Houston: 8th largest in world w/ $10.9B revenue

Threat Capability and Characterization

How does the Threat Work?

- Worms, viruses, trojans, backdoors, spear phishing, botnets,
- Openly available tools
  - Exploits within hours of public release of patches
  - Attack functions combined into multi-tools
  - Simpler tools are very mature
  - Open-source control protocol tools
- Openly available information
  - Open protocols
  - Openly available components

Anatomy of Threat Activity



Sandia National Laboratories

Generic Threat Matrix

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

- **"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.

Sandia National Laboratories

Threat

- Threat can be characterized as one of three types:
  - Normal Threat: An event or condition that affects the reliability of the day-to-day operations
  - Abnormal Threat: A natural disaster, such as hurricane-force winds or earthquakes.
  - Malevolent Threat: A manmade event or condition

Threat

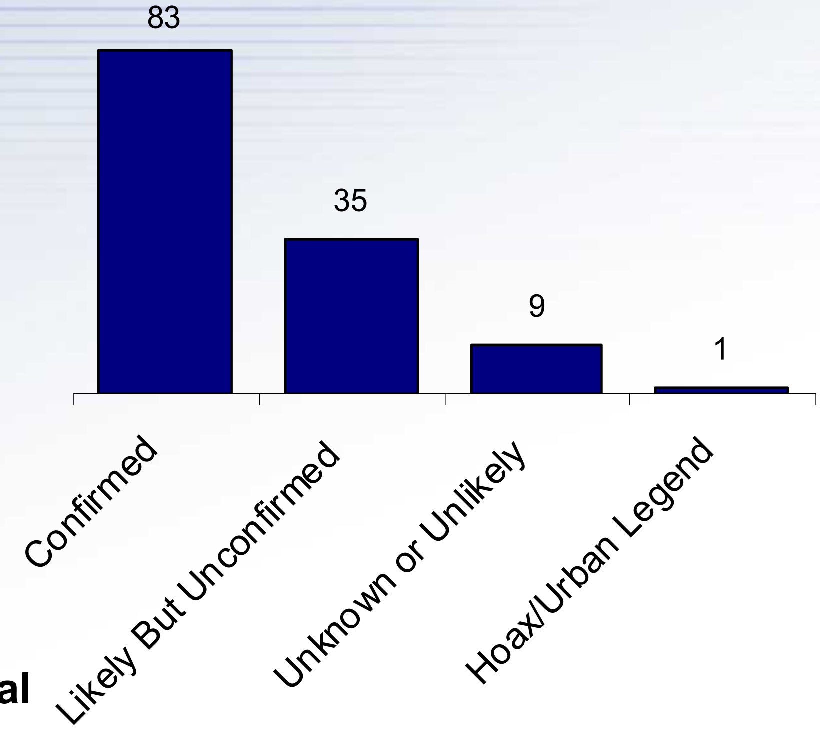
- Threat Attributes
- Commitment Attribute Family
  - Three attributes in the commitment family: Intensity, Stealth, and Time.
- Resource Attribute Family
  - Three attributes in the resource family: Personnel, Knowledge, and Access.

Threat Analysis

What Has Been Documented?

Insights from the Industrial Security Incident Database (ISID)

- **Spring 2006 ISID Status**
  - **135 Incidents (7 Pending)**
  - **22 Contributor companies from:**
    - USA, Canada, UK, France, and Australia
    - Oil/Gas, Chemical, Power, Food, Water…



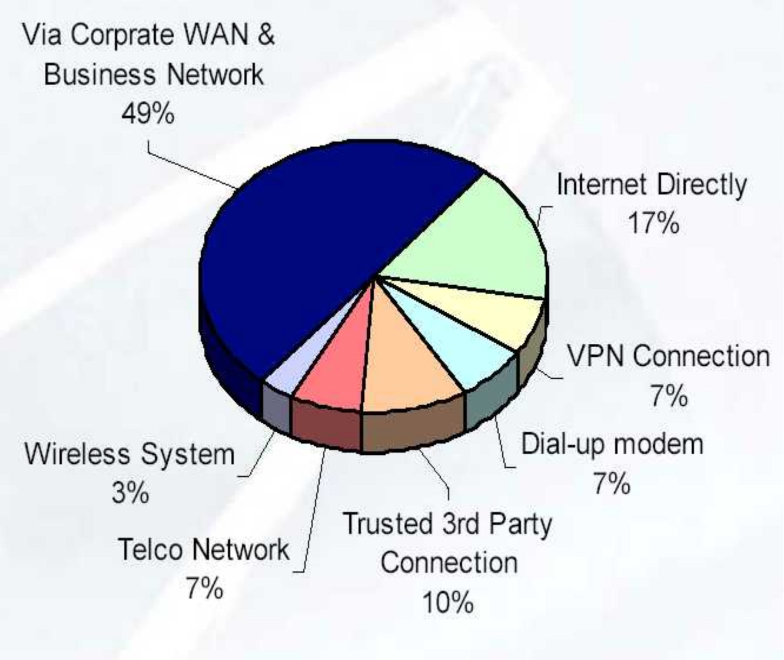
Source: Eric Byres and David Leversage, Industrial Security Incident Database

What Has Been Documented?

Insights from the Industrial Security Incident Database (ISID)

- **Major shift in point of entry**
  - **38% remote entry through 2001**
  - **56% remote entry after 2001**
- **Drivers include**
  - **Adoption of COTS**
  - **Network convergence**

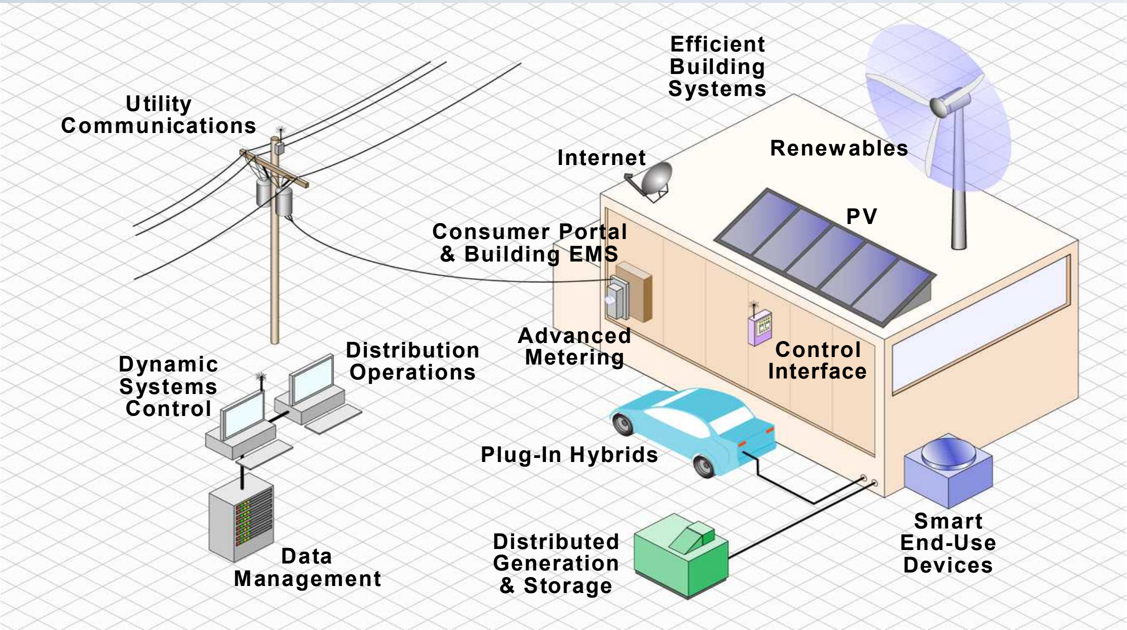
Source: Eric Byres and David Leversage, Industrial Security Incident Database



How the bad guys got in…

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



Trends Impacting Security

- Open Protocols
  - Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- Common Operating Systems
  - Standardized computer platforms increasingly used to support control system applications
- Interconnected to Other Systems
  - Connections with enterprise networks to obtain productivity improvements and information sharing
- Reliance on External Communications
  - Increasing use of public telecommunication systems, the Internet, and wireless for control system communications
- Increased Capability of Field Equipment
  - "Smart" sensors and controls with enhanced capability and functionality

Pressures Against Effective Security

- Pressure against recognizing security as critical for automation system development, deployment, and management
- Limited security management policies and procedures for PCS and automation systems
- Wide availability of conventional information technology (IT) hardware and software/operating systems
- Desire for improved operational and process efficiency
- Lack of business case for PCS security investment
  - Little concrete data on automation system attacks
  - Legal precedent not well-established
  - Automation products that have limited intrinsic security capabilities
  - No contractual requirements for security
- Security is 5-10 years behind typical IT systems

Integrated Risk Analysis

Plausible Threats → *Scenario Effects* → *System Impacts* → *Consequence of Interest*

Possible Threats

Threat
- Actors/Attack method
- Asset identification
- Vulnerability
- Motivation

Cyber Effects
- Confidentiality
- Integrity
- Availability
- Kinetics

Systems Impact
- Power Flow
- Pipeline Flow

Consequence
- Local
- Regional
- National

Risk
- Economic
- Public Health
- Trust in Govt
- Safety
- Environment

Threat-to-Consequence Risk Model

What threats are we concerned about?	Evaluate effects of cyber vulnerabili-ties	What are the physical impacts?	How do failures cascade into other CI?	Assess and quantify the Risk?

Provides a Framework for Conducting Control Systems Risk Analysis

Anecdotes

- A common misconception is the separation of control system and business networks
  - One facility thought they had two separate networks and pointed to their pair of Cisco routers at the external connection as proof. Upon examination, the routers were configured as primary and backup for both the incoming business and control networks
  - Another facility thought they had done a good job of separation - until the assessment team discovered that their safety systems resided on the control network (not all that good an idea in the first place) and the safety engineers programmed the safety systems from their corporate desktops

Anecdotes

- You may believe your business and control networks are well-separated, but -
  - A facility used PLCs in addition to their DCS, run by different departments in the organization and the PLC engineers worked on their systems from their corporate desktops
  - Another activity that seems to breach the separation is advanced optimization - sometimes the control engineers do much of their data gathering, planning and setup on their corporate systems and directly transfer their settings to the control network for step testing

Reported Data

- Collecting data reported optionally by industry and utilities is a difficult process.
- Analysis often includes extrapolated data.
- BCIT/ISID, HSIN, and CERT are groups collecting incident data. These are focused on identifying vulnerabilities, reducing risk, and assessing threat.
- SANS Internet Storm Center offers
  - Top 10 ports targeted
  - Top 10 source IPs
  - Data/Reports
  - Trends

Reported Data

- Incident data for critical infrastructure that is meaningful includes
  - 2000-3000 estimated incidents to Fortune 500 companies each year (ISID, Symantec)
  - 100 incidents per year or more occur to industry (BCIT Indus Sec)
  - In 2004, BCIT investigated 41 industrial security incidents, with 11 pending, and 7 classed as hoaxes.

Report Address Cyber-to-Physical Impacts

Reliability Impacts from Cyber Attack on Electric Power Systems

Jason Stamp, *Member, IEEE*, Annie McIntyre, *non-member*, and Bryan Ricardson, *non-member*

Abstract—**The level of risk from cyber attack against control systems used in the electrical grid is uncertain. At various times, the likelihood of attack, the availability of opportunity in the form of cyber vulnerabilities, the impact to the power system, and the consequences have all been debated at length. This research addresses the issue of grid impacts from cyber attack. (The remaining issues are not considered; as such, intent and opportunity are assumed.) One significant part of the analysis is the development of a Cyber-to-Physical (C2P) bridge, which links cyber attack vectors to resulting events in the Electric Power Grid (EPG); for example, a successful cyber penetration of a protective relay in a substation may result in an unplanned breaker trip. The analysis approach calculates an estimate of the grid performance degradation of cyber attacks, as they affect system reliability. The work models cyber attack in terms of unexpected outages to grid equipment; this way, for a given probability of cyber attack, the additional degradation to system reliability that results may be quantitatively determined. After simulation, the difference in reliability (with or without cyber attack) is the average grid impact for a given attack probability. This report includes tests for the algorithm to show its efficacy and versatility for analysis of various cyber impacts. With refinement, the proposed approach could be used as an important tool for control system risk analysis.**

Index Terms—**Power system reliability, computer network security, power system protection, SCADA systems.**

This work was supported by the National SCADA Test Bed (NSTB) program at the United States Department of Energy's Office of Electricity Delivery and Energy Reliability.

J. Stamp and A. McIntyre are with the Energy Systems Analysis department of Sandia National Laboratories, Albuquerque, New Mexico, 87185 USA.

B. Richardson is with the Critical Infrastructure Systems department at Sandia National Laboratories.

Sandia National Laboratories report 2008-7074C.
Manuscript received October 24, 2008.

978-1-4244-3811-2/09/$25.00 ©2009 IEEE

I. Introduction

THE Roadmap to Secure Control Systems in the Energy Sector identifies a critical need to better understand the possible impacts of attacks on electric power systems in order to better prioritize mitigation investment to control risk. The roadmap also points out that "asset owners are hard-pressed to justify control system security" because they are unable to "quantify and demonstrate the potential impacts of cyber attacks on energy sector control systems." [1]

There are significant technical challenges. The existing infrastructure is large and complex, the problem is inherently uncertain (e.g., the behavior of both the attackers and the infrastructure is probabilistic), and quantitative, scientifically rigorous impact assessments are needed.

In today's infrastructures, most effects achievable by control system — opening a breaker, shutting down a generator — can be achieved by cyber attack, with the effort required dependent on cyber security measures in place [2]. The primary effect of including cyber attack in an impact analysis is that it increases both the size of the system under study (not just considering the physical components, but also the cyber components) and the number of ways it can be attacked (by adding cyber vulnerabilities). A cyber-capable adversary can exploit a larger set of vulnerabilities against a system that now must be considered as a physical network and a cyber-based control system operating together [3]. Adding "cyber" makes finding plausible scenarios harder by increasing the number of possible scenarios by several orders of magnitude.

Previous approaches to analyzing the system-wide impact of attacks and perturbations to infrastructures have included:

1) *Ad hoc analysis:* e.g., subject matter experts performing reductive analysis via hierarchical risk decomposition.
2) *Static analysis:* e.g., based on studies of system equilibria.
3) *"Brute force" methods:* requiring extensive and expensive computer simulations of outage permutations.

These techniques are useful and do provide insight into infrastructure failure mechanisms but ultimately none provides an efficient way to study cyber threat impact.

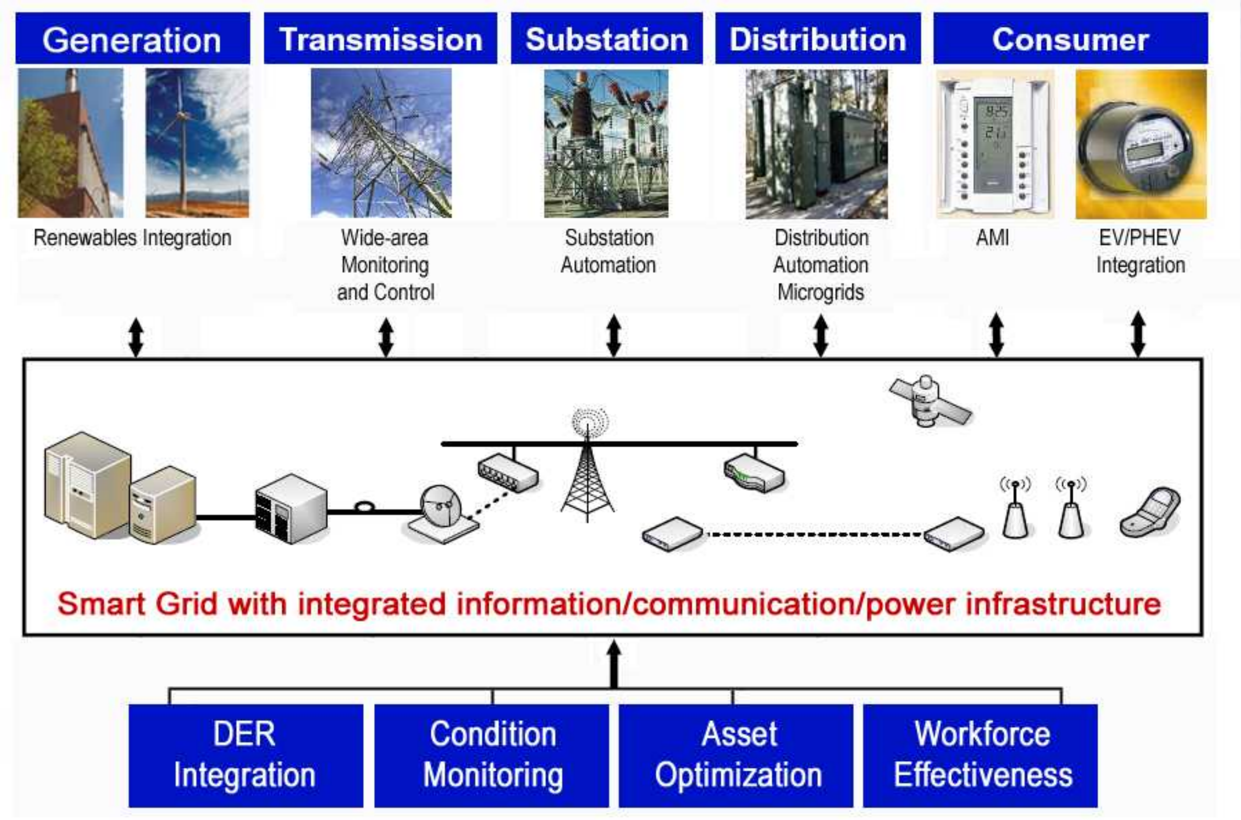
This Impacts Analysis (IA) research is intended to provide a means to quantitatively estimate electric supply interruptions that can be caused by cyber attack. An approach like this can be used to help answer two critical questions for control systems cyber security:

- What attack scenarios are plausible to achieve a significant electric supply interruption?

- Conclusions on Data Reporting:
  - Reported numbers are by choice
  - Understanding incident trends can be beneficial
  - Categorizing incidents by threat aids analysis
  - Extrapolated data can reduce overall risk
  - Useful in business continuity planning and ROI

Path Forward – Addressing Smart Grid Risk

Smart Grid Enables Dynamic Optimization of Grid Resources and Operations



Summary & Questions

- Risk characterization and mitigation requires an understanding of threat.
- Threat can be defined by motivations, commitment, and resources.
- Threat analysis can assist in preparedness and risk reduction.
- Catalogued incident data can be useful, but….*the threat is constantly changing*!