# NSTB
National SCADA Test Bed

enhancing control systems security in the energy sector

SAND2007-6839C

Sandia National Laboratories

# Threat Analysis Framework

John T. Michalski
Sandia National Laboratories, USA
jtmicha@sandia.gov

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.

U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

# Why do we care about threat analysis?

## September 11 Attacks

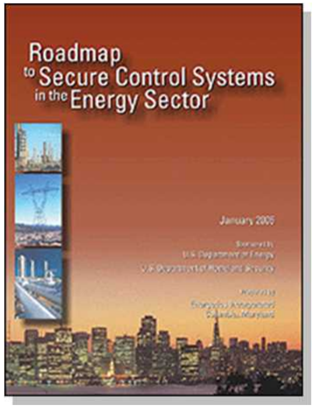
## Pearl Harbor

All images: Retrieved July 24, 2007 from Encyclopedia Britannica Online: http://www.britannica.com

# Why An Integrated Risk Analysis Approach is Needed for Control System 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**



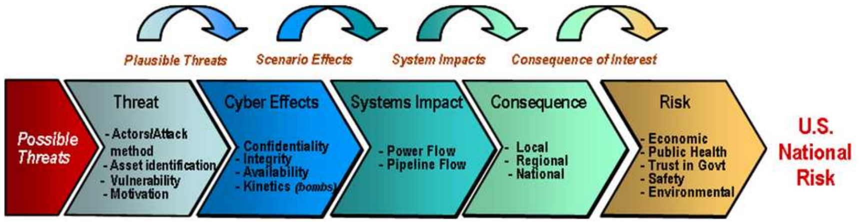

*“Assess Risk: Determine risk by combing potential… consequences of a terrorist attack...known vulnerabilities…and general or specific threat information.”*

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

Homeland Security

# How Can Integrated Risk Analysis Help the Energy Sector Reduce the Risk of Energy Disruptions

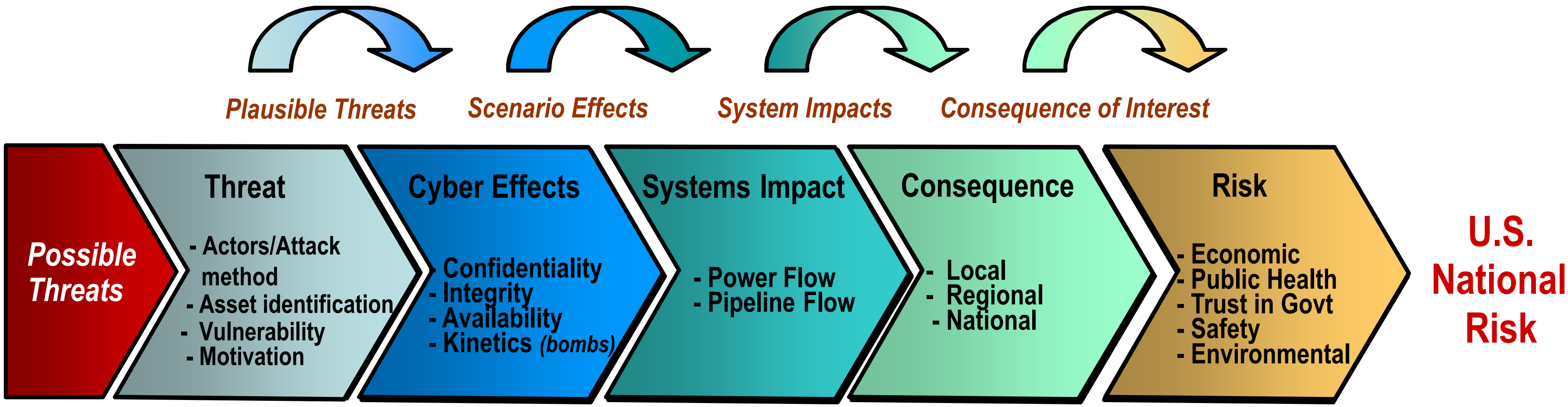
- **Understand**
  - Threats, vulnerabilities, and consequences at facility to national scale
- **Assess**
  - Risk exposure through an end-to-end, threat-vulnerability-consequence analysis capability
- **Mitigate**
  - Vulnerabilities through fundamental security practices and security technologies




**T** (resource) * **V** (weakness) * **C** (effects) = **R**

# Threat analysis is a subset of a higher model

## *Threat to Consequence Risk Model*




## *Threat to Consequence Risk Model*

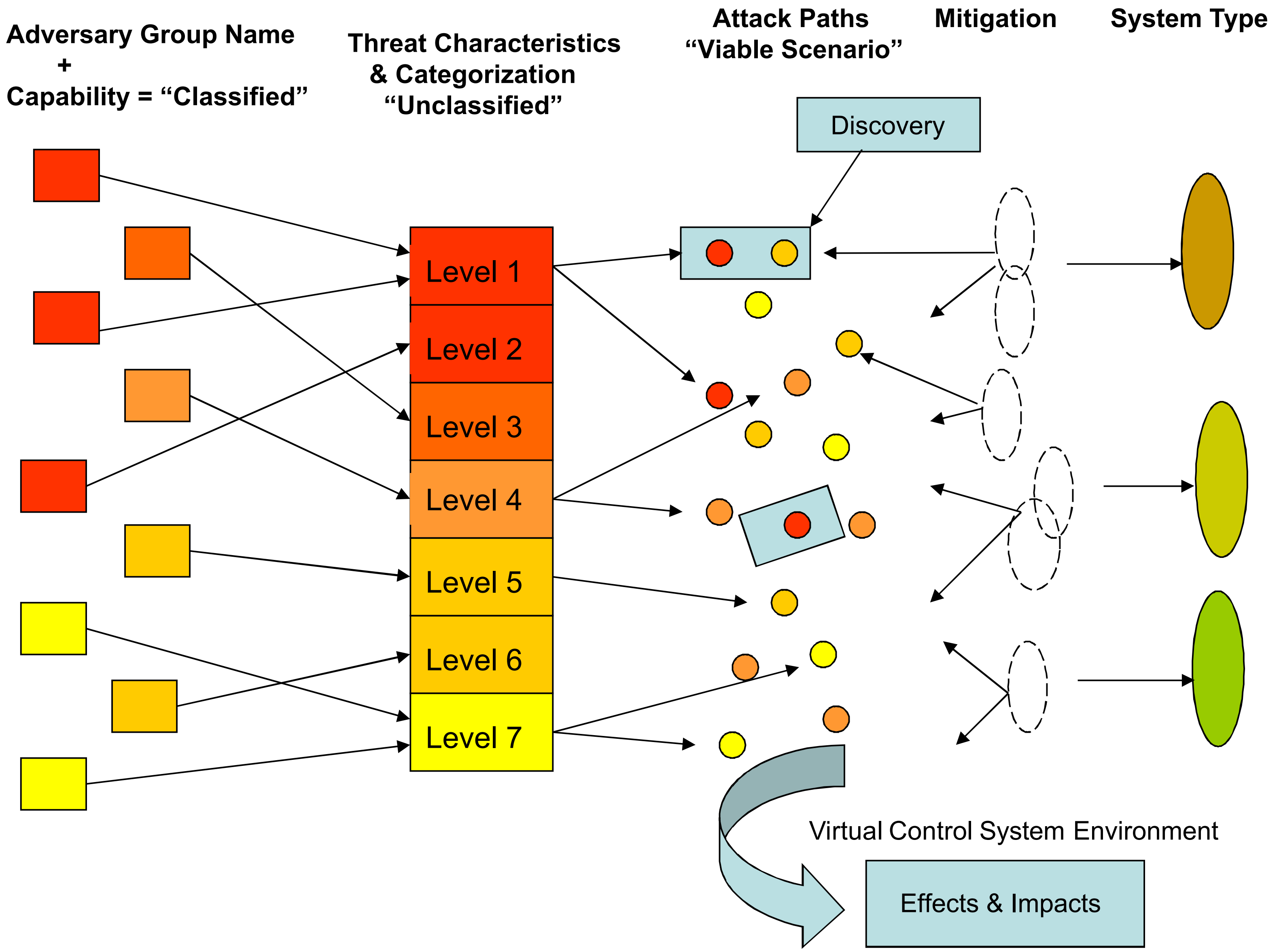
| | | | | |
|---|---|---|---|---|
| What Threats are we Concerned about? | Evaluate effects of cyber vulnerabil-ities | What are the physical impacts? | How do failures cascade into other CI? | Assess and quantify the Risk? |

**Provide a Framework for Conducting CS Cyber-Security Analysis**

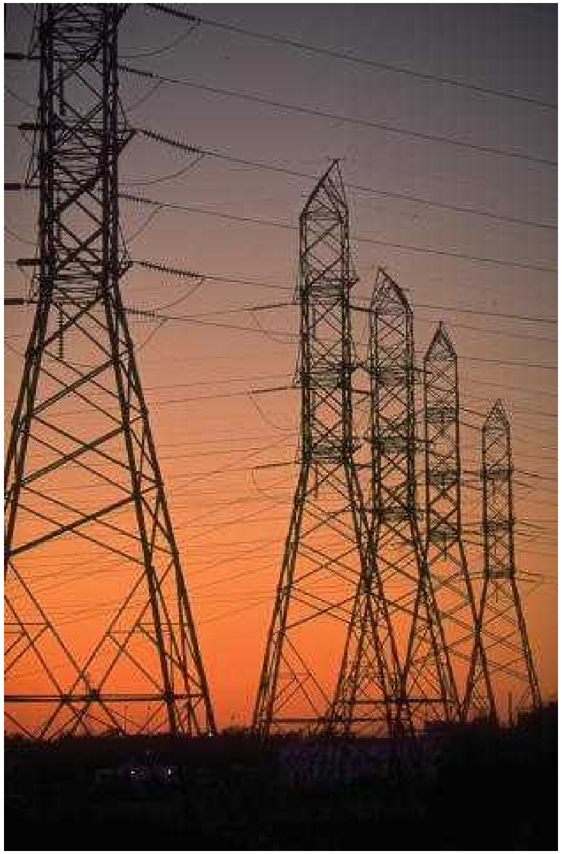
# What are the problems in threat analysis?

- Current high-level threat analysis methodologies do not provide a means for unclassified information sharing.
  - Compartmented information, Industry has a limited ability to view classified information concerning threat
- A common vocabulary and open communication path is needed to increase the security of assets and the reliability of critical infrastructure
- Critical infrastructure entities need actionable threat information to predict attack paths and develop mitigation strategies.
  - Adversary capability information
- Focused on "threat of the day"
  - Nation state, terrorist, hacker, organized crime
- Continuous nature of threat space
  - Infinite number of variations
- Lack of comprehensive approach to threat mitigation

# Threat Analysis Block



# What do the components accomplish?



*TVA transmission lines. Retrieved* July 24, 2007 from Budget of the United States Government, FY 2006: http://www.whitehouse.gov/omb/budget/fy2006/other.html

Builds a common vocabulary and tool that:

- Defines measurable capabilities
- Protects classified sources
- Identifies threat capabilities
- Simplifies threat space
- Enables design of generic protection mechanisms
- Enables open communication

# Defining Malevolent Threat

A malevolent threat is an organization or individual with

- a political, social, or personal goal, and
- some level of capability or intention to oppose.

A threat may employ methods that are

- cyber,
- kinetic, or
- hybrid cyber-kinetic.

# Threat Characterization & Categorization

- Define classes of threat
  - Decouple characteristics/capabilities from named groups
  - Ensure full-spectrum coverage
  - Unclassified
  - Validate from multiple sources
- Develop attribute characteristics for each class of threat
  - Include cyber and physical
  - Include tangibles and intangibles
  - Ensure linkage and relevance to all Threat-to-Consequence components

# Capability Attributes of Generic Threat

Commitment Family

**Intensity**

**Stealth**

**Time**

Resource Family

**Technical Personnel**

**Knowledge**

**Cyber**

**Kinetic**

**Access**

# 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 |

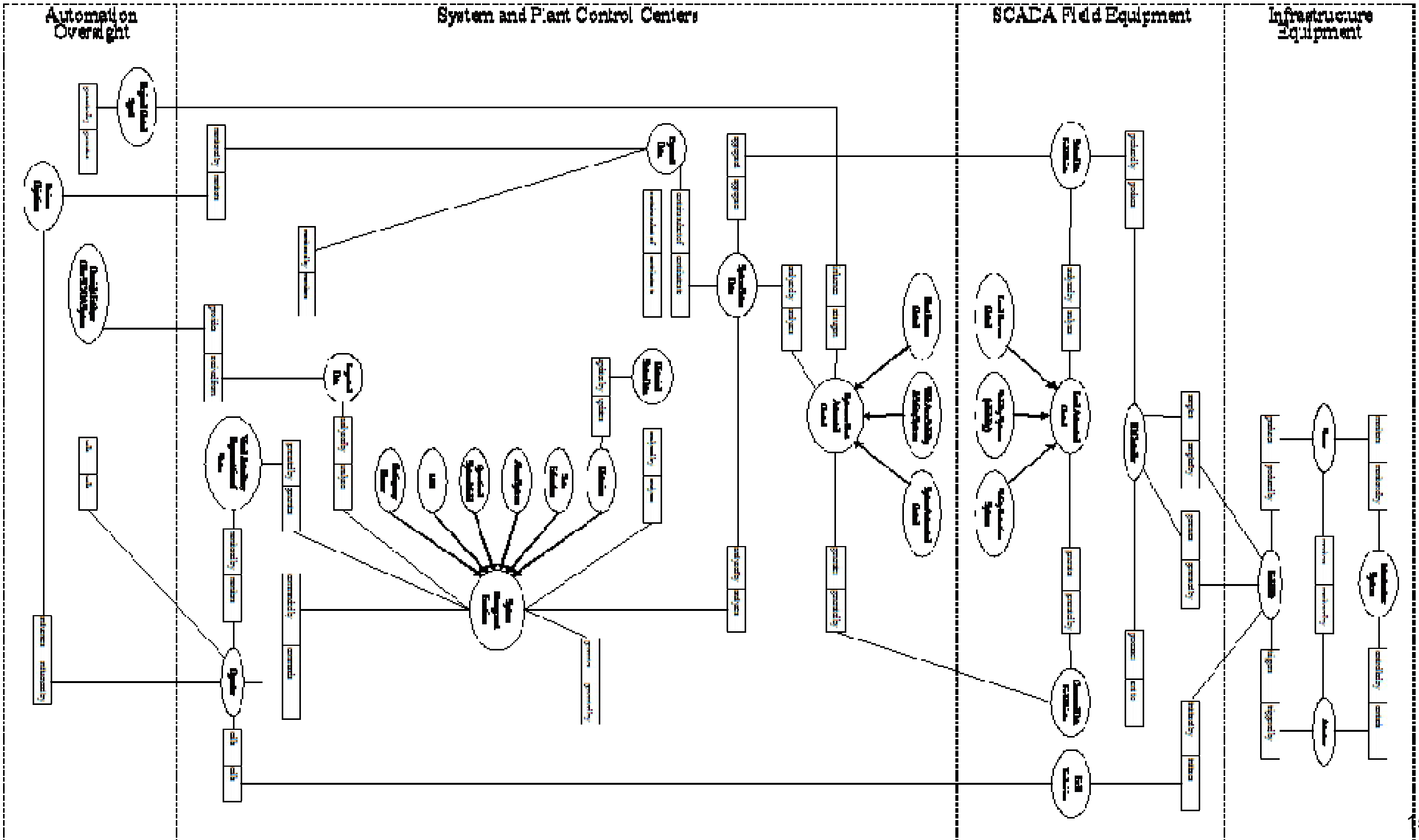
# Viable Scenario, Attack Paths

- Develop realistic scenario
  - Identify System Architecture
  - Develop adversary-level attack paths
  - Stay away from insider, if possible
  - Internally consistent and logically structured
  - Major consequence

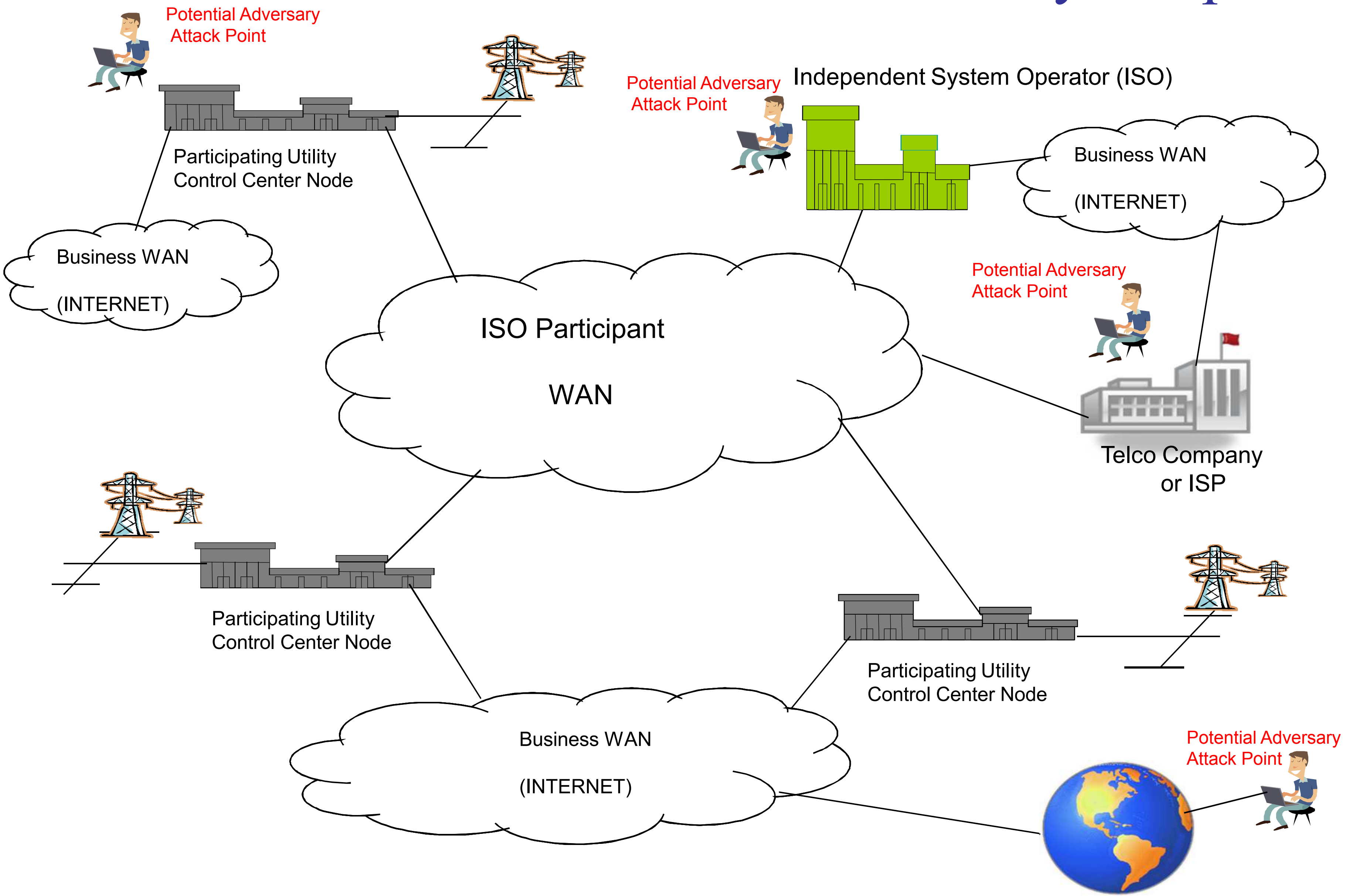
# Generic System Architecture

- Use Control System Reference Model when actual architecture is not available
  - Reference Model Breaks Control system down into Four primary levels for analysis, identifies boundaries and interfaces
    - Infrastructure equipment
    - Scada Field equipment
    - System and Plant Control Center
    - Automation Oversight
- Identify adversary attack paths
  - Use scenario information validated by dynamic discovery tool to determine how threat will be actualize within the control system architecture
- Pursue scenarios that result in major consequence not nuisance's
  - Use VCSE tool to help validate subsequent effect and impact

# Control System Reference Model



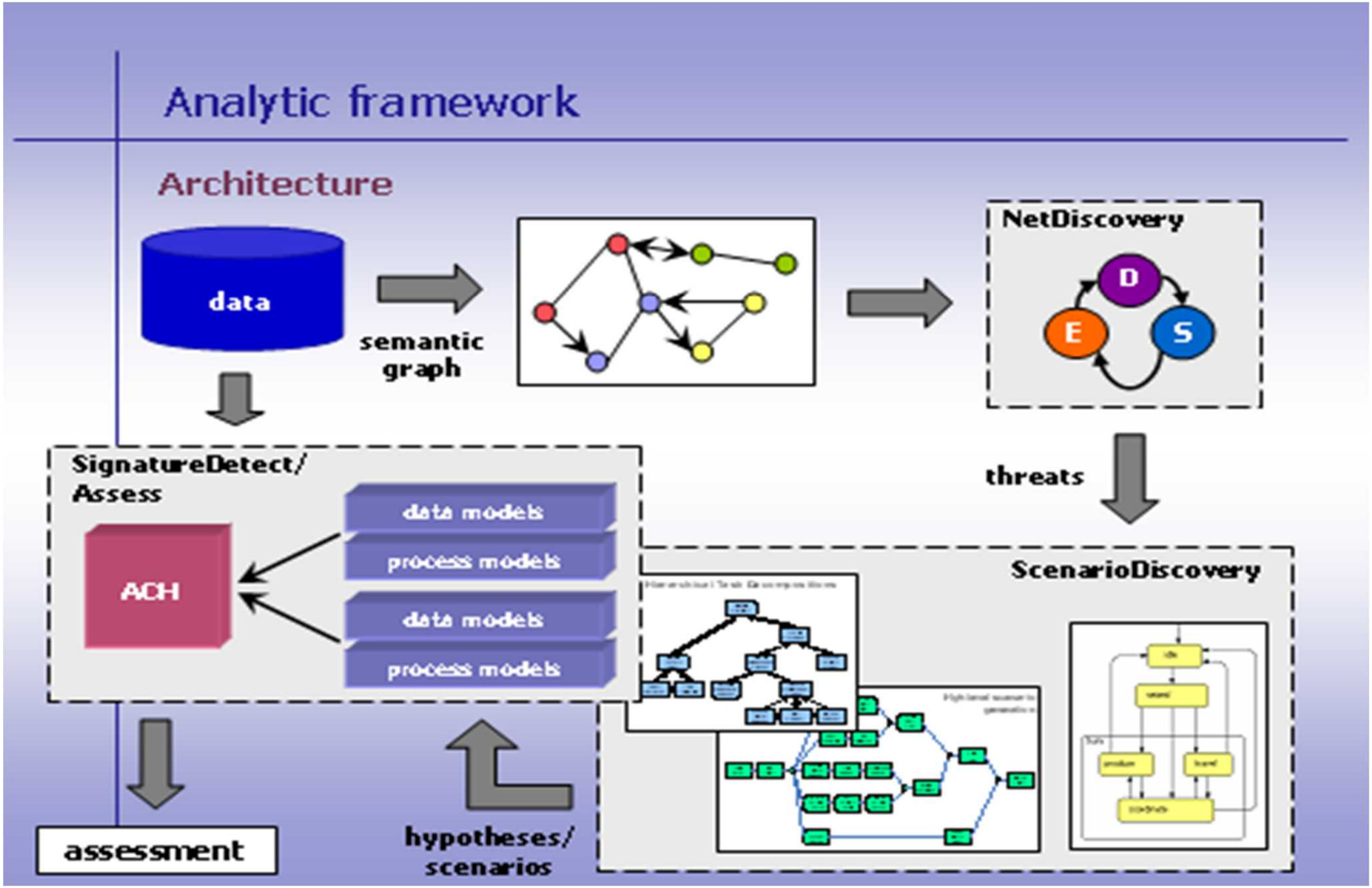
# ISO Scenario Architecture with Adversary Endpoints



# Discovery

- Develop Real-Time Vulnerability Analysis
  - how likely the vulnerability has been identified by an adversary and the adversary is discussing an exploitation
- Use Graph based analysis to discover relationships in data
  - Use semantics to identify relationships
  - Vertex or node is equivalent to a data source (Not all sources are created equal, authoritative vs. non authoritative)
  - An edge is an association with multiple data sources
- Analyze and evaluate Data, from plausible data associations
- Review viable scenarios, search on derived approach
- Signature Detection
  - Assessment, analyze competing scenario hypothesis

# Discovery


Analytic framework
Architecture
data
semantic
graph
NetDiscovery
D
E
S
threats
SignatureDetect/
Assess
ACH
data models
process models
data models
process models
ScenarioDiscovery
assessment
hypotheses/
scenarios

# Mitigation

Based on Generic Control System type (Control System Reference Model)

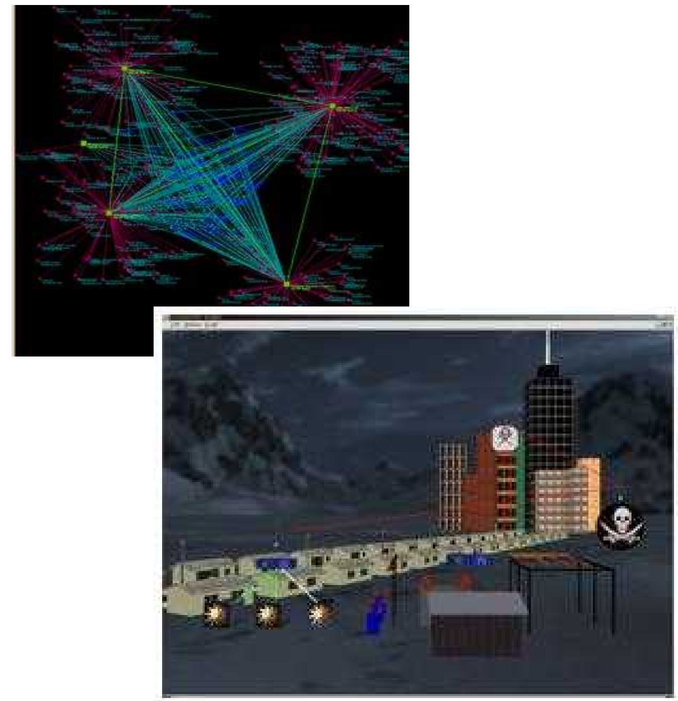
- Develop protection strategies (Fy08 activity)
  - Develop generic protection models for each level of adversary
  - Identify Residual Risks
- Use Virtual Control System Environment (Defense analysis)
  - Simulate exploit
  - Identify effect analyze impact
  - Integrate mitigation

# Virtual Control System Environment (VCSE)

- *Provide a Security Evaluation Tool for Analysis of Cyber Vulnerabilities on Control Systems*
- ***DOE/OE OMG Planning Guide***

- Tool will answer - **Given a plausible threat/vulnerability - What effects can be achieved on control systems?**
- A modeling and simulation tool will be developed to analyze and assess threats and cyber vulnerabilities on control systems (CS) without risking disruptions to critical operations.

- **VCSE will permit the end-user to configure a simulation environment of control system devices and network communication protocols and enable real-time, hardware-in-the-loop interfaces**



- VCSE will reduce the risk of energy disruption by:
  - **Providing a realistic setting designed to replicate portions of a vulnerable infrastructure;**
  - **Launch cyber attacks in a controlled setting; and**
  - **Evaluate effective mitigation tactics**

# Threat Framework Analysis Summary

- Leverage open and closed source data to better quantify the level of threat in terms that are meaningful to the energy asset owners.
  - **The generic threat profile framework will provide a path for classified information to be declassified and used in an unclassified setting**
- Identify Scenarios that leverage viable attack paths that can be realized by the level of capability of the threat.
- Develop a discovery tool that takes as input a set of cyber-vulnerabilities and attempts to discover and assess evidence that an adversary is interested in exploiting them.
- Provide mitigation techniques that can thwart or reduce impact of realized threats.

# Deliverables

- Unclassified “Threat Analysis Framework” document (2007)
- Unclassified “Categorizing Threat” document that define threat classes with defined characteristics (Generic Threat Profile, 2007)
- Generic unclassified adversary level attack paths (2008)
- Detailed, relevant scenarios (2008-2009)
- Real-time vulnerability analysis (2007-2009)
- Generic protection models for each level of adversary (2008-2009)
- Threat usage process for each component in the Threat-to-Consequence model (Output of Scenario development (2008-2009)

# Threat Analysis Reports

**SANDIA REPORT**
SAND2007-5791
Unlimited Release
Printed September 2007
**Categorizing Threat**
**Building and Using a Generic Threat Matrix**
David P. Duggan, Sherry R. Thomas, Cynthia K. K. Veitch, and Laura Woodard
Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
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.
Approved for public release; further dissemination unlimited.

**SANDIA REPORT**
SAND2007-5792
Unlimited Release
September 2007
**Threat Analysis Framework**
David P. Duggan and John T. Michalski
Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
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.
Approved for public release; further dissemination unlimited.

http://infoserve.sandia.gov/

# Questions?

Threat Analysis Framework
John T. Michalski
jtmicha@sandia.gov