

# NSTB

**National SCADA Test Bed**

enhancing control systems security in the energy sector

## Threat Analysis

**Richard Colbaugh**

**John Michalski**

**Sandia National Laboratories**



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



**Sandia National Laboratories**

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

# Threat-to-Consequence Framework



## **Challenges/Needs**

Characterize threat from open and closed sources

Assess ease with which vulnerability information can be discovered

Discover active adversary intent

## **Results/Benefits**

Taxonomy for sharing threat profiles

Evidence that an adversary can learn “bad” things on the “open web”

Precursors to adversary’s intent

A means to measure threat for better allocation of mitigation resources

# Threat-to-Consequence Framework



What was the nature of the threat in the Rogue Software Scenario?

What credible adversaries were *interested* in conducting a Rogue Software Scenario on the energy infrastructure?

What control system vulnerabilities were available and *discovered* by the technically-savvy adversary?

What information was available that enabled the adversary to implement the Rogue Software Scenario?

How does threat information feed into the threat-to-consequence framework?

How can this analysis be used to prioritize risk reduction activities that address this rogue software attack?

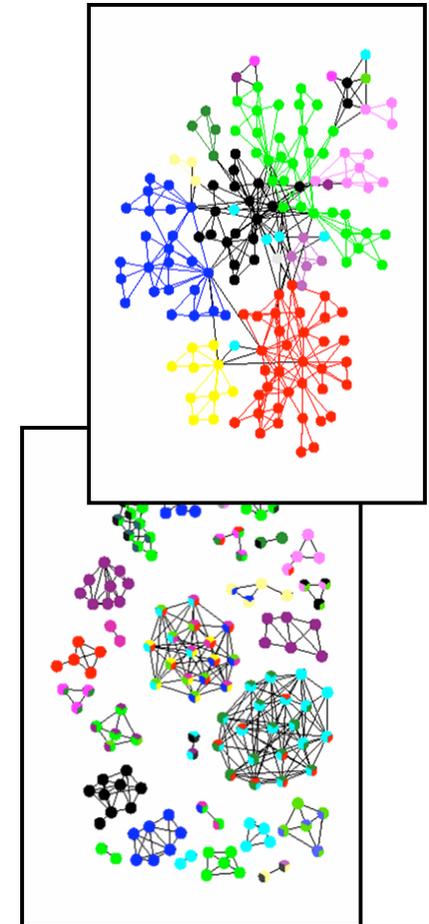
# Introduction

## Graph analysis?

- Model: represent objects of interest (e.g., people, information, system components) as nodes and relationships between objects as links.

[Example: social network.]

- Motivation:
  - usual things (scalable, expressive/quantitative, intuitive, ... ;
  - particularly well-suited for *discovery* – provides comprehensive, semantically rich description of system.



# Introduction

## Problem formulation

- Adversary interest:

Is there *interest* in a particular class of vulnerabilities on the part of any adversary which poses a credible threat?

Example: Can we find “chatter” regarding a class of SCADA vulnerabilities in “authoritative” sources?

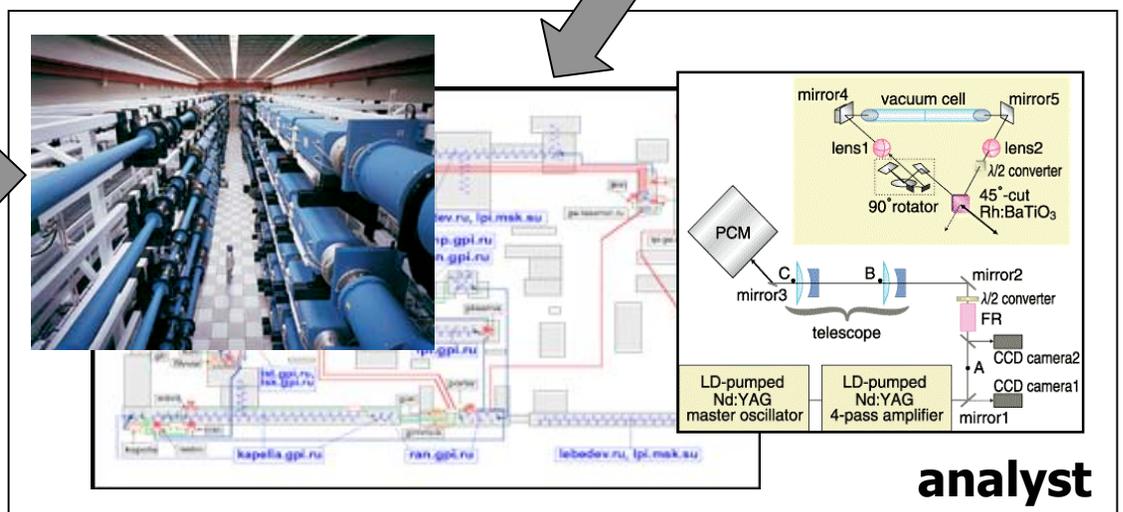
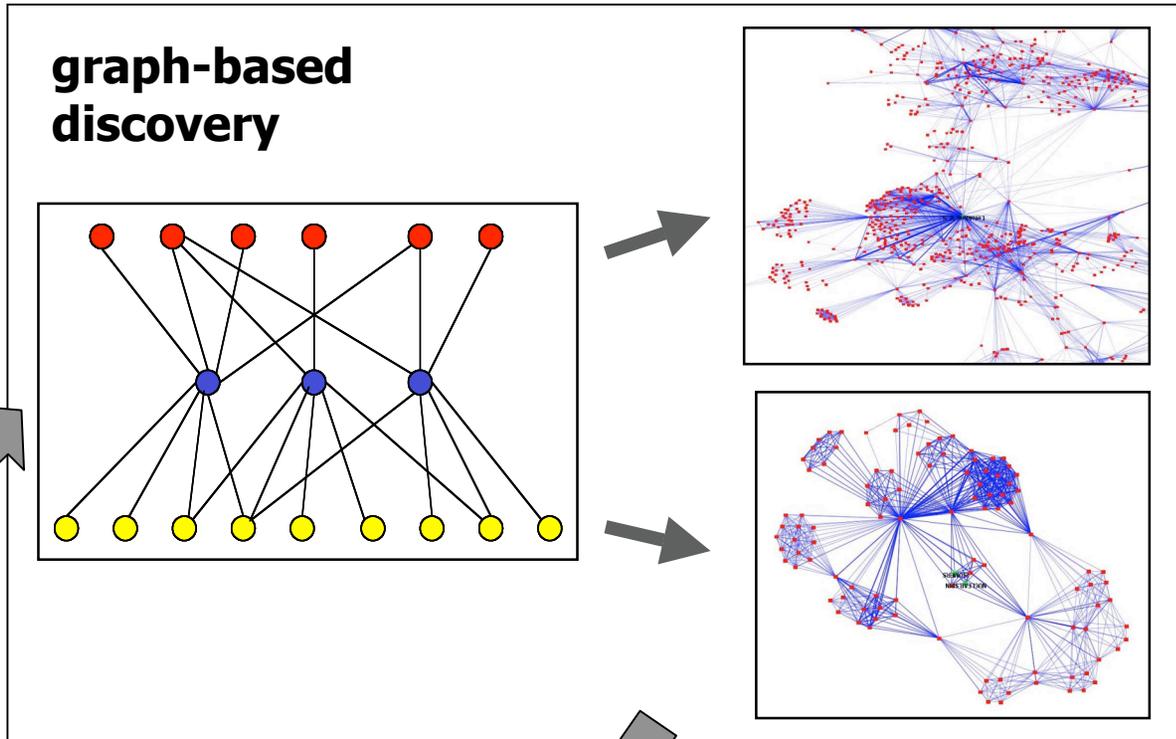
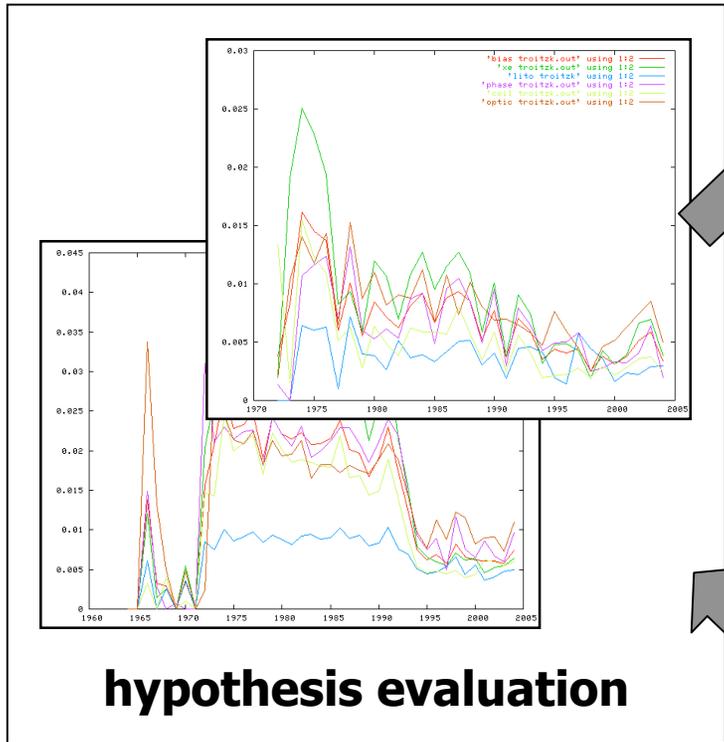
- Discoverable capability:

We focus on the *discoverability* of the information required to learn of, and exploit, system vulnerabilities.

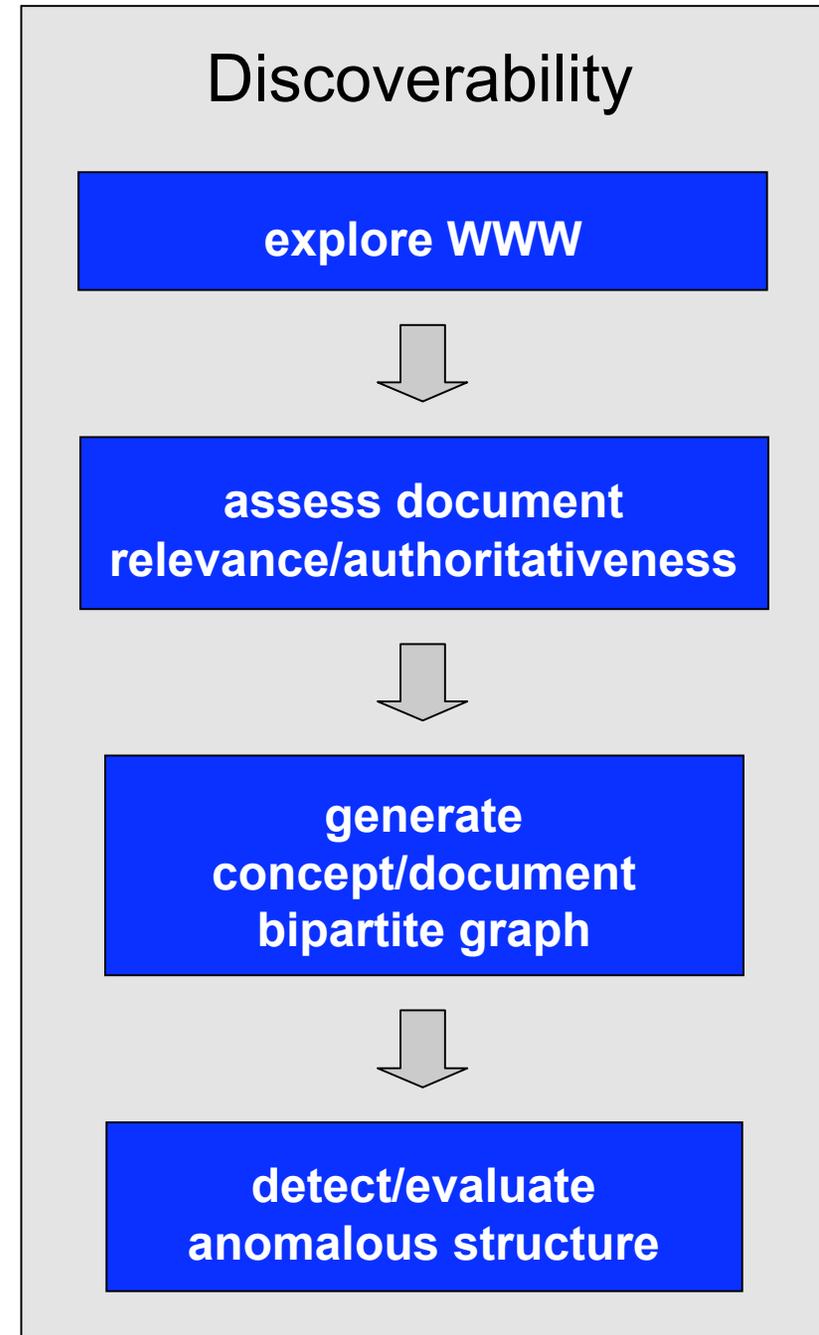
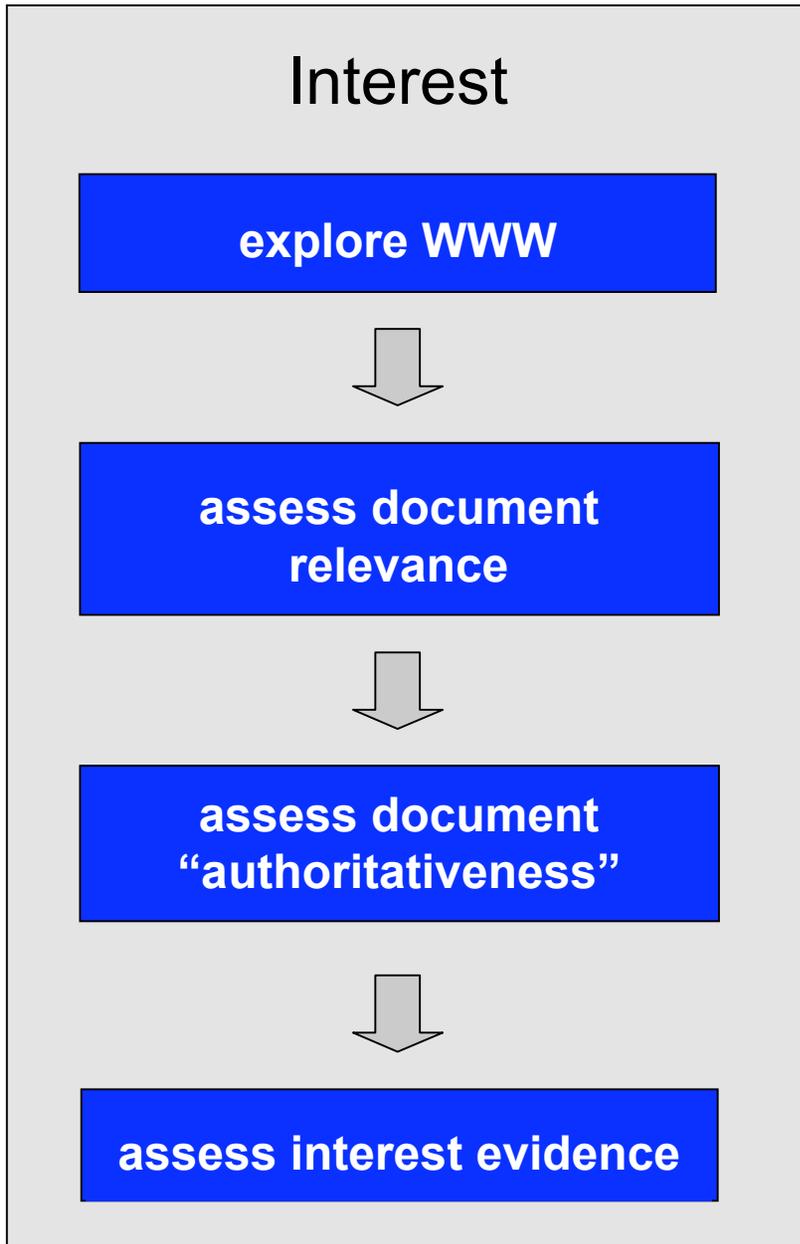
Example: Can a technically-savvy adversary discover a SCADA system vulnerability and acquire both the technical knowledge and system-specific data/information necessary exploit it?

# Approach

Basic idea



# Approach



# Illustrative example: NW threat discovery

## Observation

Materials exist which represent attractive alternatives to traditional elements used in nuclear weapons (NW) (for substate groups):

- weaponization-related properties are comparable to  $^{235}\text{U}$ ;
- possess advantages from perspective of material acquisition.

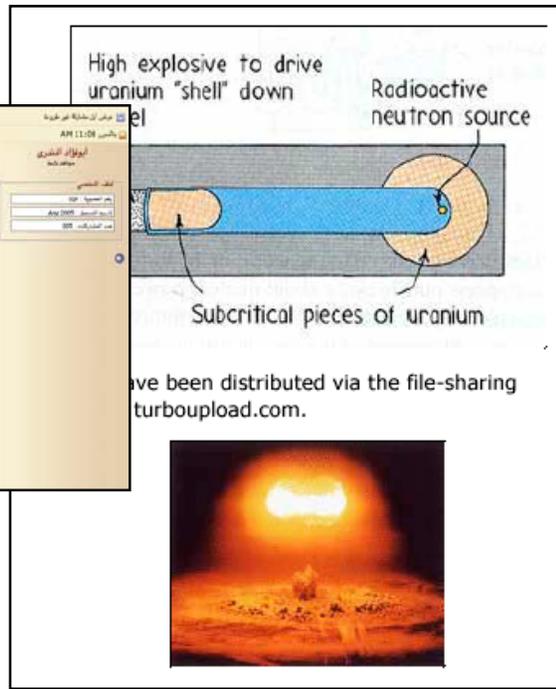
## Basic questions

- Are substate groups *interested* in nontraditional approaches to NW (NT-NW)?
- Can technically sound NT-NW approaches be *discovered* by a non-expert adversary?

# Illustrative example: NW threat discovery

Sample result: interest

Computational exploration of www uncovers “authoritative” pages expressing such interest, including an Al Qaeda site encouraging search for nuclear bomb materials which are “effective alternative to uranium and available on the market”.

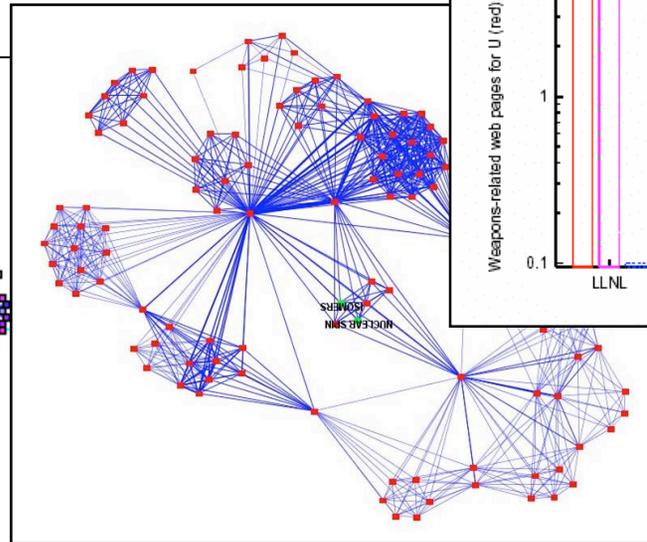
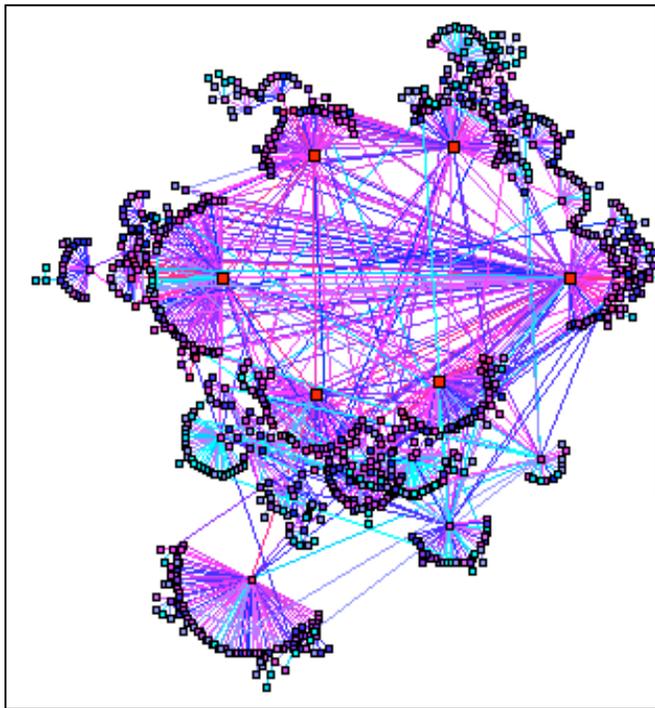


# Illustrative example: NW threat discovery

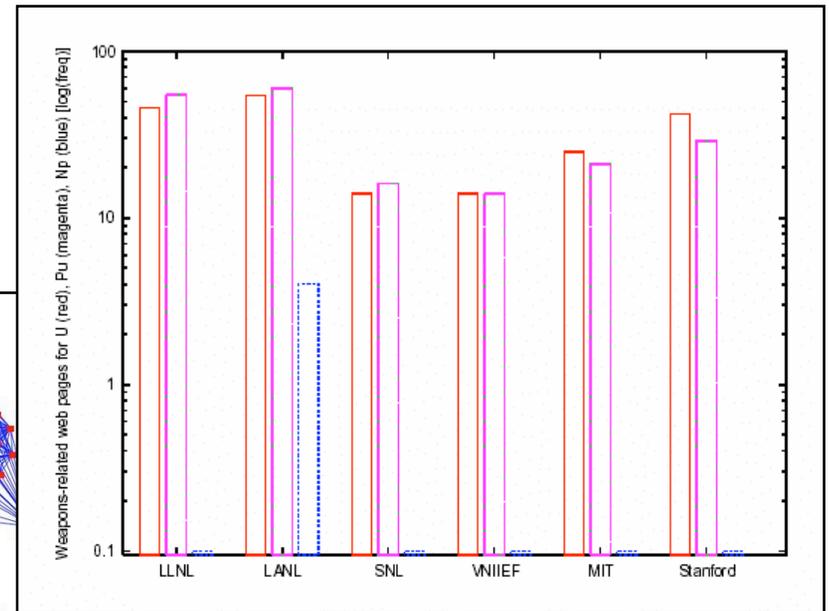
Sample result: discoverability

Analysis demonstrates discoverability of (technically sound) NT-NW ideas.

WWW exploration



analysis of concepts/  
relations



anomaly detection

# Rogue Software Scenario

Basic questions:

Part 1:

- Can vulnerabilities be discovered on the WWW that fit an hypothesis/scenario?
- Is information available that can provide an adversary with the details to develop an exploit or an approach?
  - “If an adversary wanted to know how to do ‘bad thing X’, could they learn how to do it from the Open Web?”

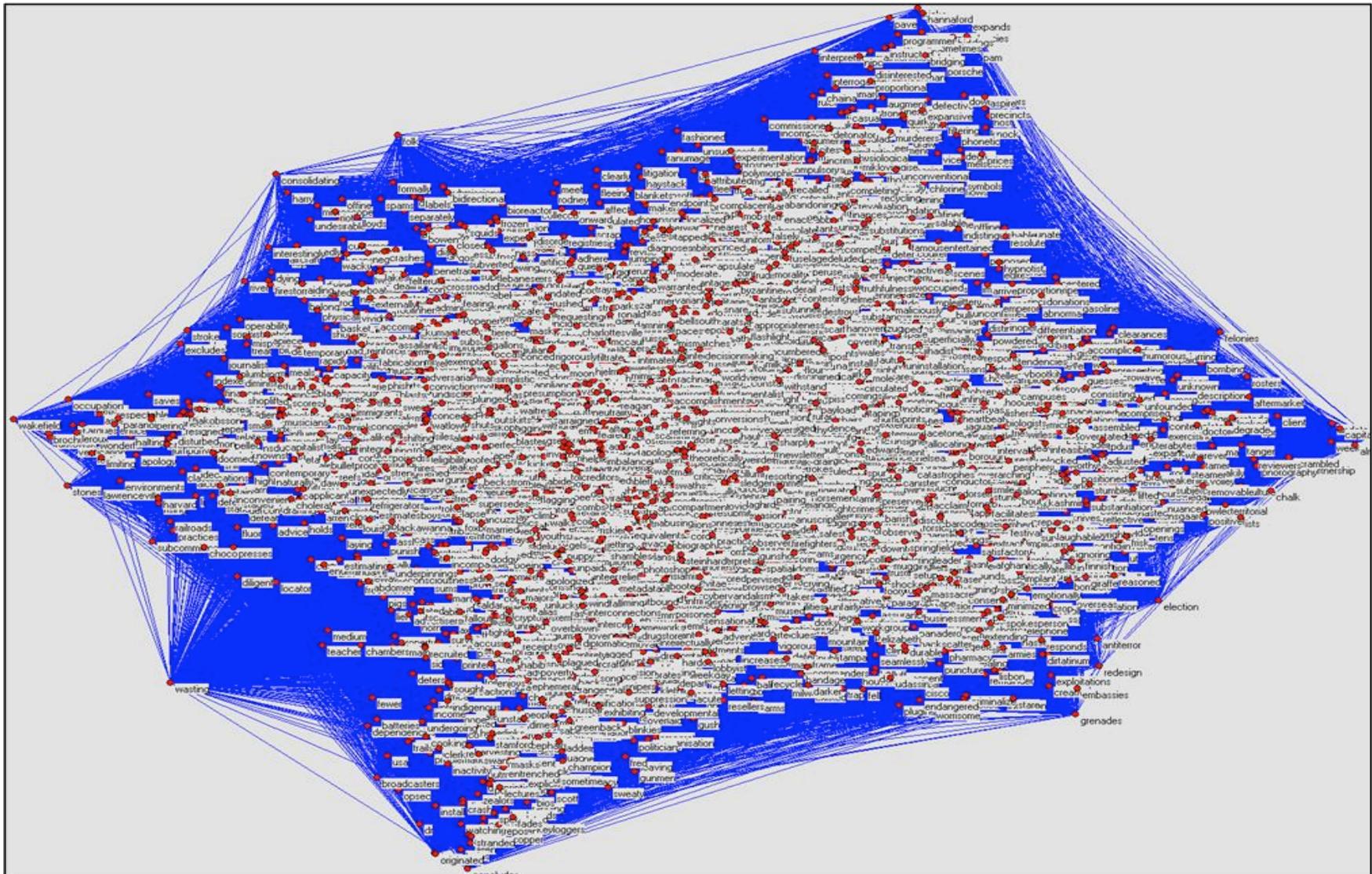
Part 2:

- Is there a plausible threat (adversary) interested in this information?
  - Any chatter?
- Is the adversary capable of exploiting the vulnerability
  - Threat matrix consultation

# Discovery, process development

- 1) Domain of interest, SCADA vulnerability and exploits.
- 2) Develop Seed List of relevant concepts
- 3) Use filtering techniques such as “part-of-speech” and “singular value decomposition” to group the web pages into meaningful clusters.
- 4) Develop a concept-concept graph for each cluster of documents, and use concept co-occurrence distance and proximity filtering to reduce edge density;
- 5) Identify highly related “communities” of concept terms within each resulting graph component.
- 6) Manually assess each graph “community” and review the sets of related web pages for information of interest.

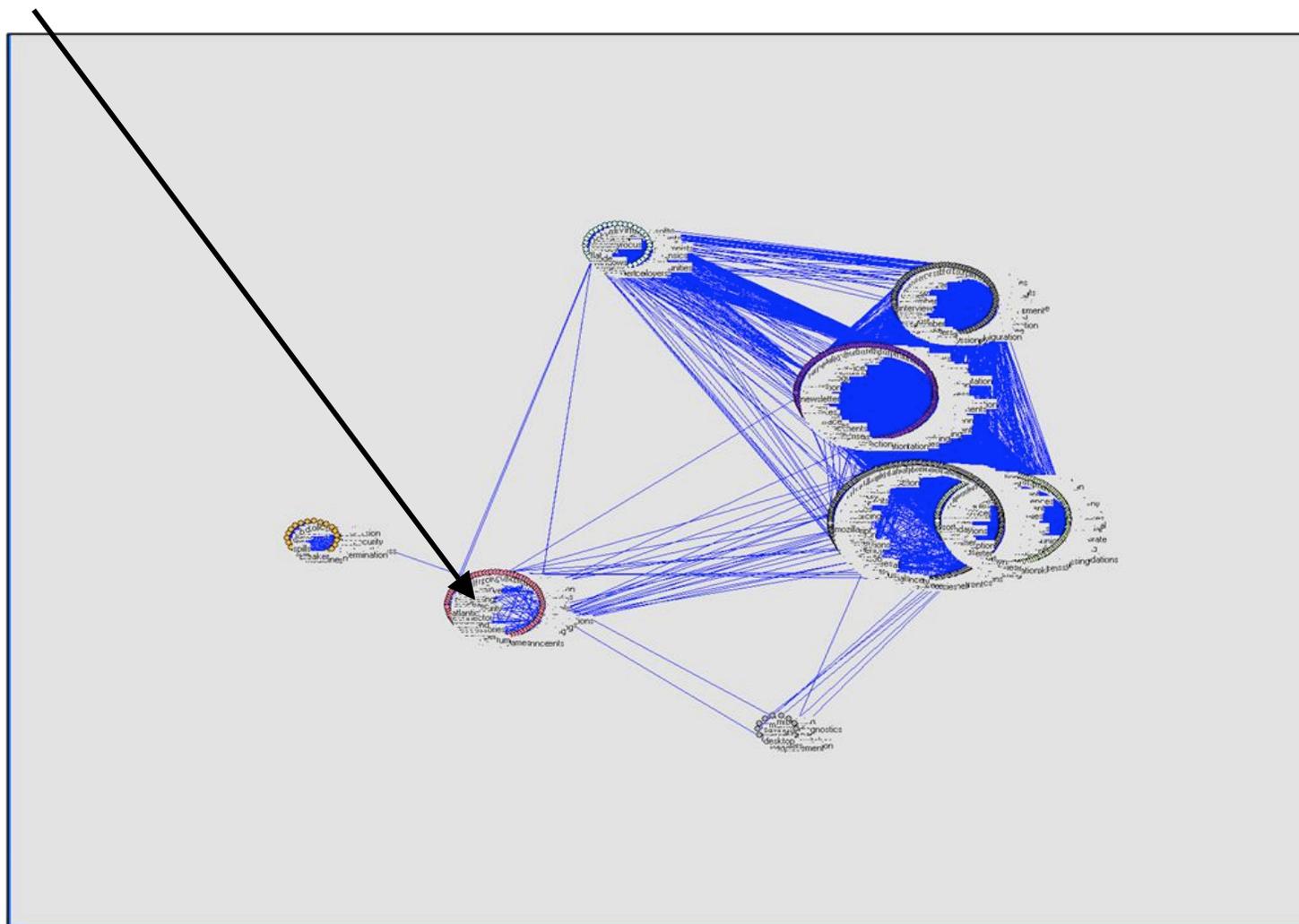
# Data Collection Using Seed Terms





# A Community Graph

*A community of Interests, terms and their co-occurrence relationships*



# Threat analysis results

It's within these communities interesting web pages can be Discovered!

- 1) Open linker/embedder for process control (OPC) server vulnerability
- 2) Front End Processor (FEP) using OPC server interface
- 3) How power grids fail
- 4) Operational parameters & settings

# Web Page of Interest: OPC vulnerability

## Multiple vulnerabilities in Takebishi Electric DeviceXplorer MODBUS OPC server

---

OPC servers provide a standard way to interoperate automation and control systems, bridging data from several industrial protocols such as DNP3, MODBUS, etc. to a more standard data access interface. They are often used in SCADA systems to consolidate network device information in a singlepoint; as such OPC servers are usually considered critical applications.

Takebishi Electric commercialises an OPC Server ("Takebishi.MODBUS.1"), more information is available at <http://www.takebishi.co.jp/>.

The product presents various security vulnerabilities, allowing an attacker with access to the OPC interface to arbitrarily read and write the process memory, leading to the execution of attacker-provided code.

The vulnerabilities reside in the server implementation of the following OPC Data Access interface methods:

- \* IOPCServer::RemoveGroup

By providing specially crafted OPC handles the attacker can force the server to access arbitrary memory in read/write operations which can be leveraged to execute arbitrary code in the OPC server.

# Web Page of Interest: FEP with OPC Server

## Front-End Processor

Bow Networks' eLAN product family addresses a wide range of communications and data integration issues from the substation to the control center, and into the enterprise. Each product is focused on a specific application within the utility's communication infrastructure. The eLAN Front-End Processor is packaged to address the utility's need to manage communications from remote sites, over a range of communications media.

### *Benefits*

- **Offload EMS communication processor**
- **Economical port expansion**
- **DNP Poll Accelerator**
- **Management of complex communication infrastructure**
- **Wide range of security options**
- **Supports redundant masters and control centers**
- **Optional enterprise access**

### **eLAN Front-End Processor Overview**

- The eLAN FEP is based on our field-proven TIE (Telemetry Integration Environment) module, which was originally developed as the telemetry front end for a major EMS vendor and is currently installed in over 50 utilities worldwide. The eLAN FEP provides protocol mediation capability in a vendor-neutral configuration, allowing users of a wide range of EMS systems to offload many of the tasks of managing communications with their field devices. eLAN FEPs are frequently deployed to provide capabilities not available in native front ends, such as IP network support, security, or simply as a cost effective way to add additional ports.
- The eLAN FEP may be easily upgraded to provide full enterprise application integration through the addition of open interfaces such as OLE for Process Control (OPC) and ODBC. These interfaces allow other applications, such as historians or enterprise databases, to access data from field devices without requiring an interface directly to the EMS.

# Web Page of Interest: Load shedding events

## Load-Shedding Scheme Protects Utility from Voltage Collapse

The complexity of operating a transmission system has increased over the years. **The failure of a single critical element, if not managed correctly, can result in cascading outages and distribution of the entire transmission system.** Intervention by system operators is often not possible because voltage collapse can take place in fractions of a second. Maintaining reliability sometimes requires automatic load-shedding schemes. The Public Service Company of New Mexico's (PNM) **undervoltage load-shedding (UVLS)** scheme is one design that prevents either a fast or slow voltage collapse for low probability events involving the loss of multiple transmission elements.

## TYPES OF POWER SYSTEM INSTABILITIES DURING SYSTEM DISTURBANCES

### A. Basics – Voltage vs. Frequency Stability

In a power system, **frequency is a measure of the balance of MW generation and MW load.** When MW generation and MW load are exactly in balance, the frequency is at the normal level of 60 Hz. **When load exceeds generation, the frequency goes down.** The rate of decline depends on the inertia of the generators within the system. Under normal conditions, there are slight changes of frequency when load suddenly increases or generation trips off-line which results in a slight (hundreds of a hertz) reduction in frequency until the aggregate generation in the system can be increased to meet the new load condition. **If there is a large negative imbalance between MW load and MW generation, the frequency is reduced.** UFLS schemes on the utility system are designed to restore the balance by shedding load.

**Steady-state instability** - The ability to transfer real (MW) power is described by the power transfer equation and is plotted graphically. From the power transfer equation in Fig. 5, it can be seen that the maximum power ( $P_{max}$ ) that can be transmitted is when (SEE PDF)  $= 90^\circ$ , i.e.  $\sin 90^\circ = 1$ . **When the voltage phase angle between local and remote generation increases beyond  $90^\circ$ , the power that can be transmitted is reduced and the system becomes unstable and usually splits apart into islands.** If enough lines are tripped between the load center and the remote generation supplying the load center, the reactance ( $X$ ) between these two sources increases, thereby reducing the maximum power ( $P_{max}$ ) which can be transferred.

**At this point, the power system is in deep trouble**

## Web Page of Interest, Frequency parameters

Although discrete value detection can be employed, the strategy that is currently adopted is that only a sustained frequency decrease, lasting for at least 100 ms, and resulting in a fall of at least 0.25 Hz, is deemed to constitute a sufficient frequency deviation to merit load disconnection.

The frequency of a power system will change when the load-generation equilibrium is disturbed. If the unbalance is caused by a deficiency of generation, the system frequency will decay to a value at which load-generation equilibrium is reestablished. If equilibrium cannot be established, system collapse will occur.

### NERC Standards Workshop

- Frequency decline shall be arrested at no less than 58.0 Hz.
- Frequency shall not remain below:
  - 58.5 Hz for greater than 10 seconds, cumulatively, and
  - 59.5 Hz for greater than 30 seconds, cumulatively

# Results Summary: What does it mean?

- Discoverable capability:
  - Can a technically savvy adversary discover a SCADA system vulnerability and acquire both the technical knowledge and system-specific data/information necessary exploit it? **[yes]**
    - **Found a protocol vulnerability**
    - **Found a product using this protocol**
    - **Found critical operational/design information about power grid**
- Adversary interest: Can we find “chatter” regarding a class of SCADA vulnerabilities in “authoritative” sources? **[Work in Progress]**
- IC Analysis provided NO information indicating adversary interest

Red = Low capability

Orange = Moderate capability

Green = High capability

Threat Capability Requirements	
\$ needed	L
Cyber (knowledge & access)	H
Physical infrastructure (knowledge)	L
Stealth	H
Must be willing to risk	M
Length of time needed	H
Organization size	M

# Questions?

# Backup Slides



Query

Threat Discovery Tool



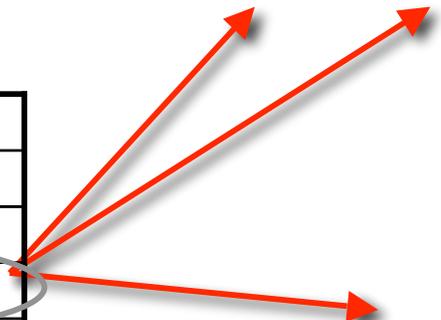
Response

Threat Vectors  
(Derive Scenarios)

Threat Information

- Vulnerability discover
- "chatter"

Intensity	Stealth	Cyber	Kinetic
1			
2			
3			
4			
5			



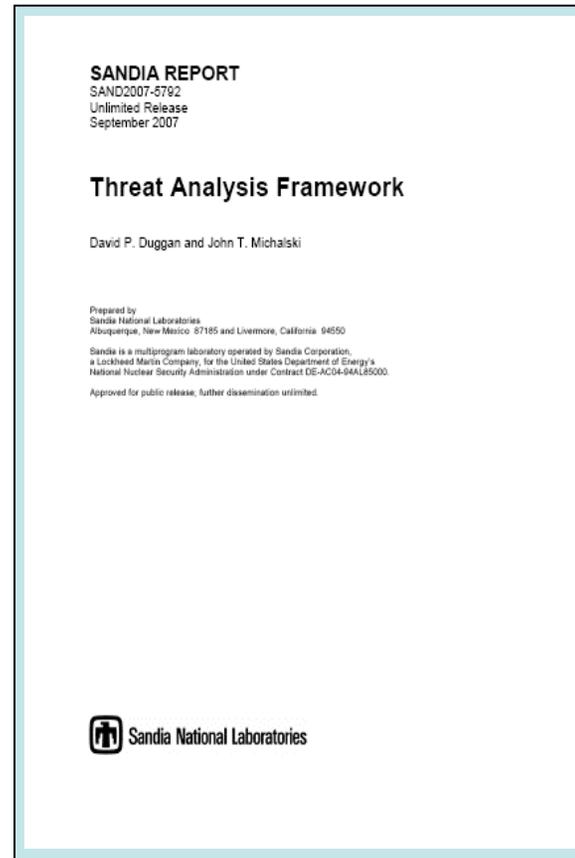
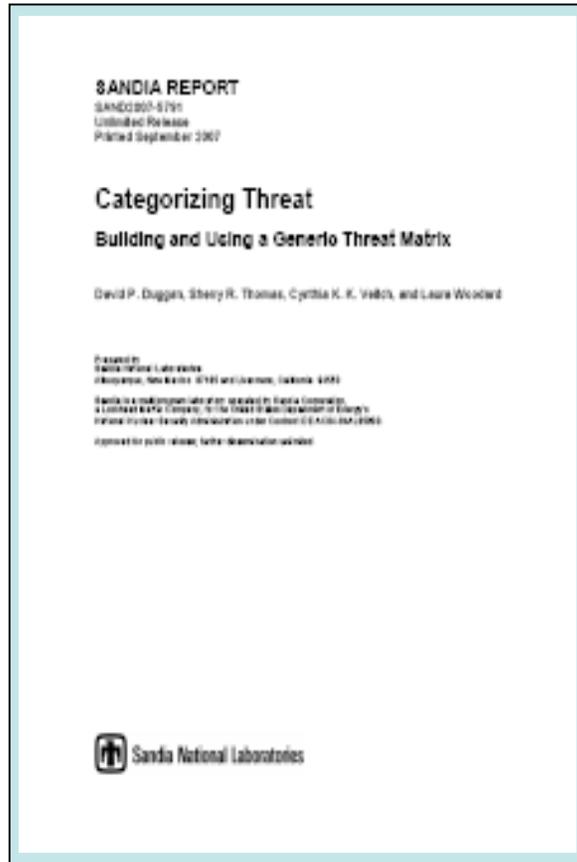
Matrix Attributes

Threat Capability Matrix



IC Analysts

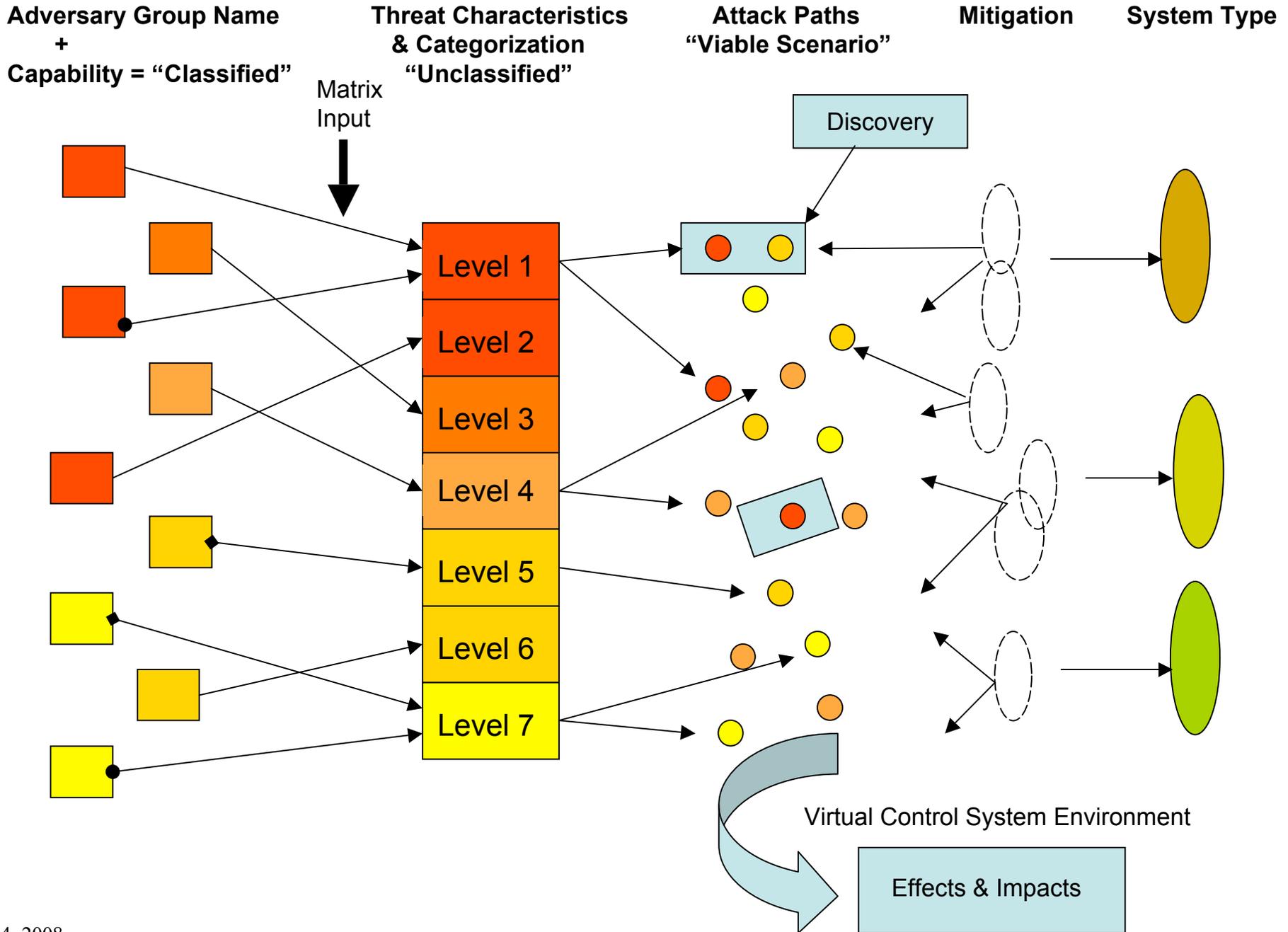
# NSTB Threat Analysis Reports



# Seed lists

- Distributed-Control-System
- OLE
- OPC
- Process Control System
- Front End Processor
- RTU
- FEP
- Automation
- Matrikon
- Energy Management system
- EMS
- OPC server
- load-shedding
- Electricity-generation
- Electricity-transmission
- High-voltage-circuit-breaker
- Cascade
- Grid

# Threat Analysis Framework



# Adversary attributes slide 1 of 2

## **Commitment of Adversary:**

- Intensity – Measure of how far a threat is willing to go and what a threat is willing to risk to accomplish its goal. Because the group needs a large and sustained presence, the intensity with which they can pursue the end goal would need to be high.
- Stealth – The stealth required to inject exploits into a supply chain and have those exploits remain invisible during dormancy points to a High level of stealth. It would be catastrophic for the organization and their goals to have this discovered prior to triggering.
- Time – A fairly long period of time is necessary for attacks implemented through the life cycle, especially in the area of Process Control Systems. It could take years to ensure there is enough adoption of compromised systems to make the attack successful.

# Adversary attributes slide 2 of 2

## Resources of Adversary:

- Size of Technical Organization – The threat attribute quantifies the number of group members that a threat is capable of dedicating to the building and deployment of the technical capability in pursuit of its goal.
- Knowledge – Since this attack setup deals mostly with cyber knowledge, we can identify the necessary cyber knowledge to perform the exploit generation, testing, and implementation. It requires a Medium-to-High level of knowledge to perform the necessary work.
- Access – To gain the access necessary to affect the life cycle of the intended targets will require an organization with Medium-to-High capabilities in this area. They will need to place an individual at the appropriate level into a position whereby they could implant the exploit. It will have to be done at least one time, if into a “master” copy, or multiple times if inserted after the equipment has been built.

## Level of adversary

- Taking all the levels of capability from the above analysis, the adversary groups most capable of performing the described scenario would be in threat levels 2 or 3. An adversary group in the threat levels of 4 or 5 could possibly perform the described scenario, but the time factor is an important consideration that cannot be rushed using the implantation method described in the scenario and groups from threat levels 4 and 5 don't have the ability to run operations for the length of time needed in this scenario. With the adversary group most likely from levels 2 or 3, the Intensity attribute would need to be High, while Kinetic knowledge could be either Medium or High.