



www.thei3p.org

Institute for  
Information  
Infrastructure  
Protection

# Status and accomplishments of the I3P's Process Control Systems Security Research Project

**John Cummings, Project Director**

*PCSF – Atlanta, GA*

*March 6, 2007*

This work was supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

# I3P Project Objective: Help O&G Sector Manage PCS Risks

## ■ Understand

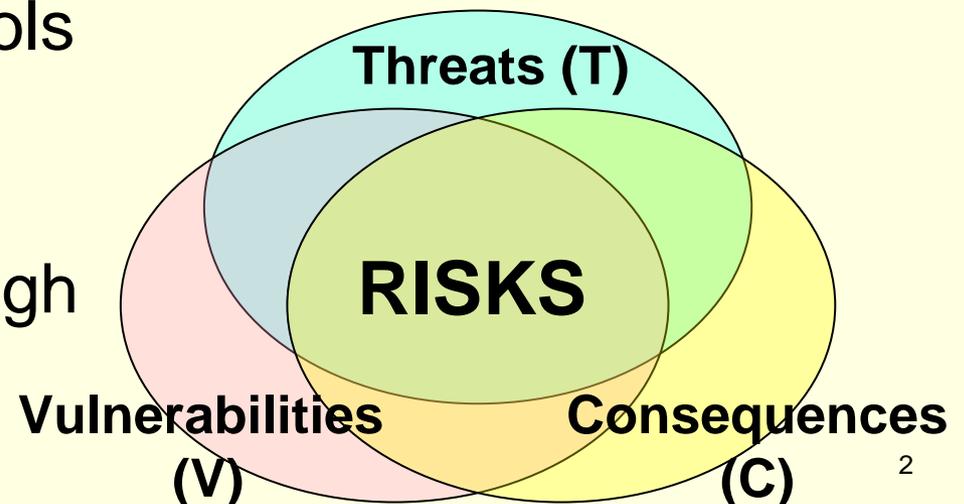
- Threats, vulnerabilities, consequences at facility to national scale

## ■ Assess

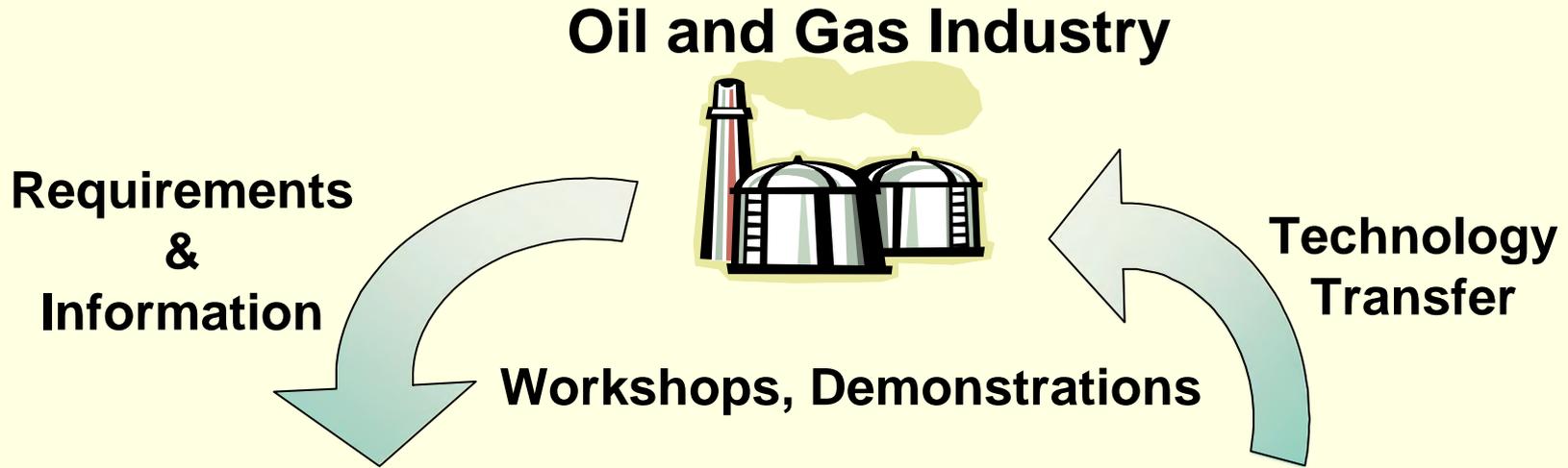
- Risk exposure through new assessment tools and metrics

## ■ Mitigate

- Vulnerabilities through novel security technologies

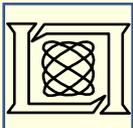


# Project Organization



- *Risk Characterization*
- *Interdependencies*
- *Metrics*

- *Security Tools*
- *Information Sharing*
- *Technology & Knowledge Transfer*



# Research Approach

---

Understand vulnerabilities, analyze the impacts of disruption, characterize the risks

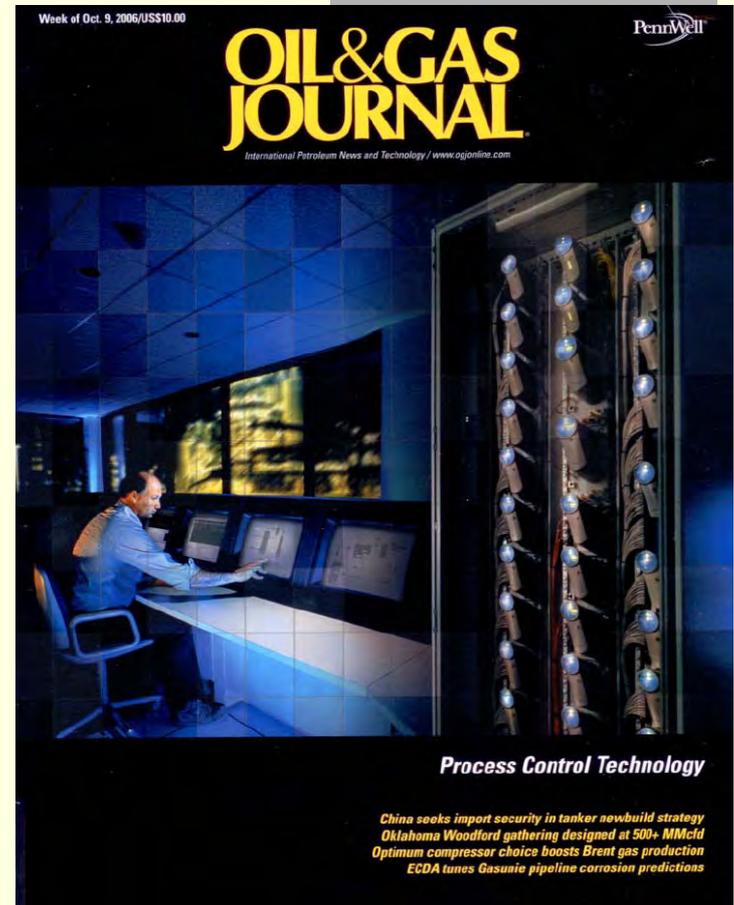
Understand and develop metrics that can be used to measure improvement

Research technical solutions

Work with stakeholders to transfer the knowledge gained and the technology developed

# Engaging Industry to Understand Risks

- **Characterization of O&G control systems risks through workshops and numerous site visits and industry discussions**
  - Threat assessment
  - Vulnerability analysis and categorization
  - Effectiveness of mitigations
  - Recommendations on path forward
- **Development of representative test environment and vulnerability scenarios to direct technology development**



**I3P Risk Characterization Paper  
in Oil & Gas Journal**

# 2<sup>nd</sup> Industry Workshop

## June 8, 2006; La Jolla

- Focused on presentation and demonstration of research results in action-ready format

### *PROCESS CONTROL SYSTEMS SECURITY WORKSHOP*

**I3P** Institute for Information Infrastructure Protection  
*Demonstrations of Security Solutions and Research Findings for the Oil and Gas Industry*



**June 8, 2006 — La Jolla, California**

- We collected stakeholder feedback

**I3P Contact Information:**  
 45 Lyme Road  
 Hanover NH 03755  
 Tel: (603) 646 0692  
 Fax: (603) 646-0660  
 E-mail: [research@thei3p.org](mailto:research@thei3p.org)

For registration and more information, see [www.thei3p.org/scada/workshop2/](http://www.thei3p.org/scada/workshop2/)  
 Registration is **FREE** with registration for the June 6-7 PCSF Spring Meeting (see [www.pcsforum.org](http://www.pcsforum.org))  
 1-day registration for June 8 is \$100

# 3<sup>rd</sup> Industry Workshop

## February 15-16, 2007; Houston

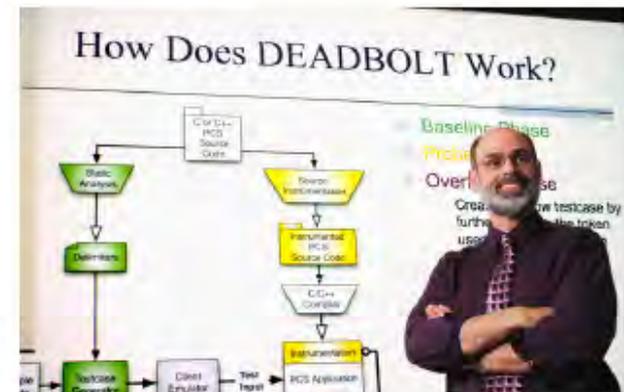
- Overview of recent cyber threats to PCS
- Demo of vulnerabilities
- Latest research findings
- Multi-disciplinary approach to PCS security
- Training in risk management, security tools, mitigation techniques

You are Invited to a

## Process Control Systems Security Workshop

Hosted by the Institute for Information Infrastructure Protection (I3P) to address security and technology needs in the oil and gas industry

Sheraton Houston Brookhollow Hotel  
Houston, Texas  
February 15 - 16, 2007

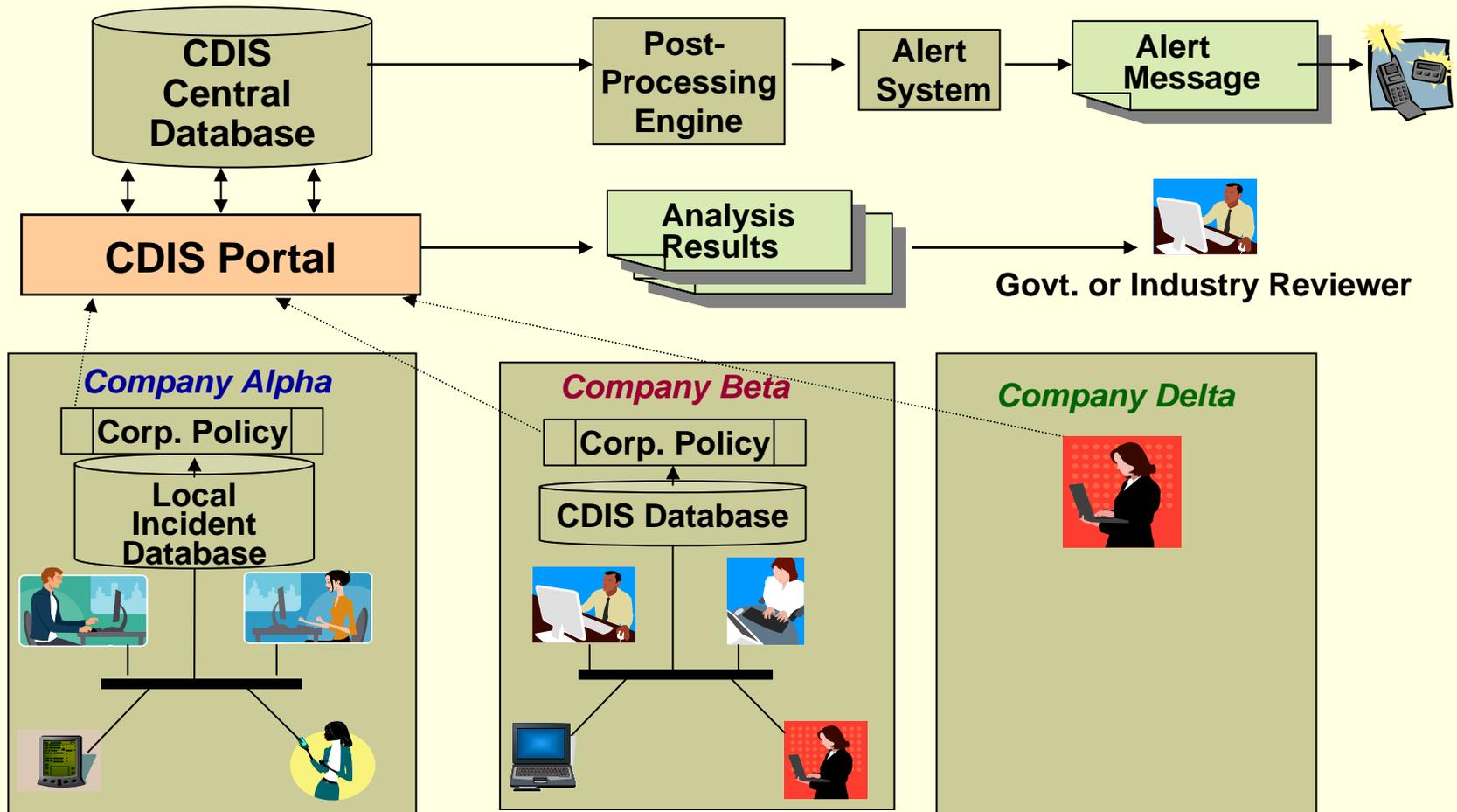


# Risk management insights and methodologies

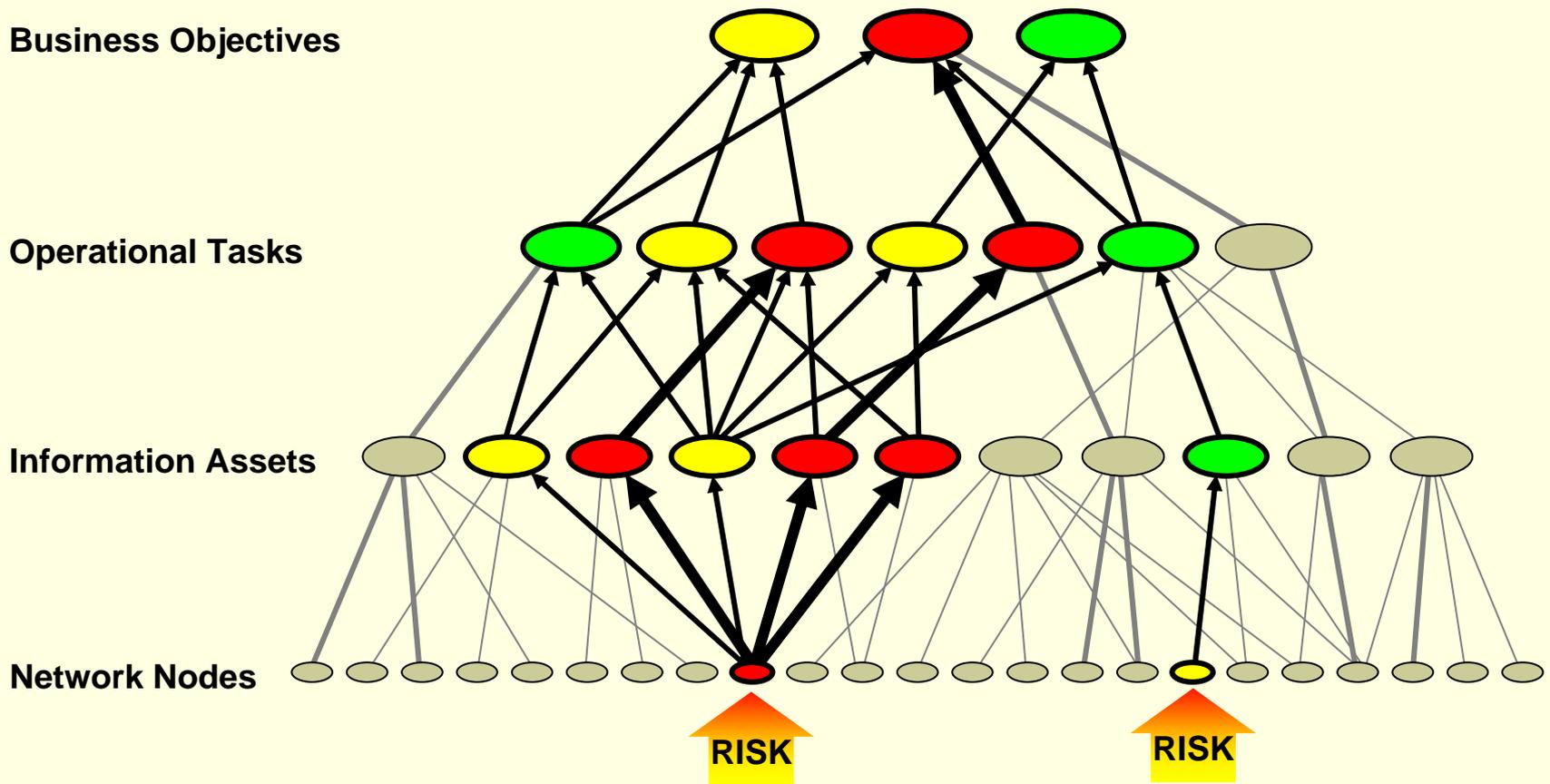
---

- **Raising the alarm: industry information sharing following an attack**
- **Identifying corporate risks with RiskMAP**
- **Understanding and applying security metrics**
- **Cascading impacts of PCS attacks**
- **Failures in oil and gas infrastructure: trends, causes and consequences**

# I3P Vision For Reporting and Analysis



# RiskMAP: Finding Corporate Risks



**On the path to commercialization...**

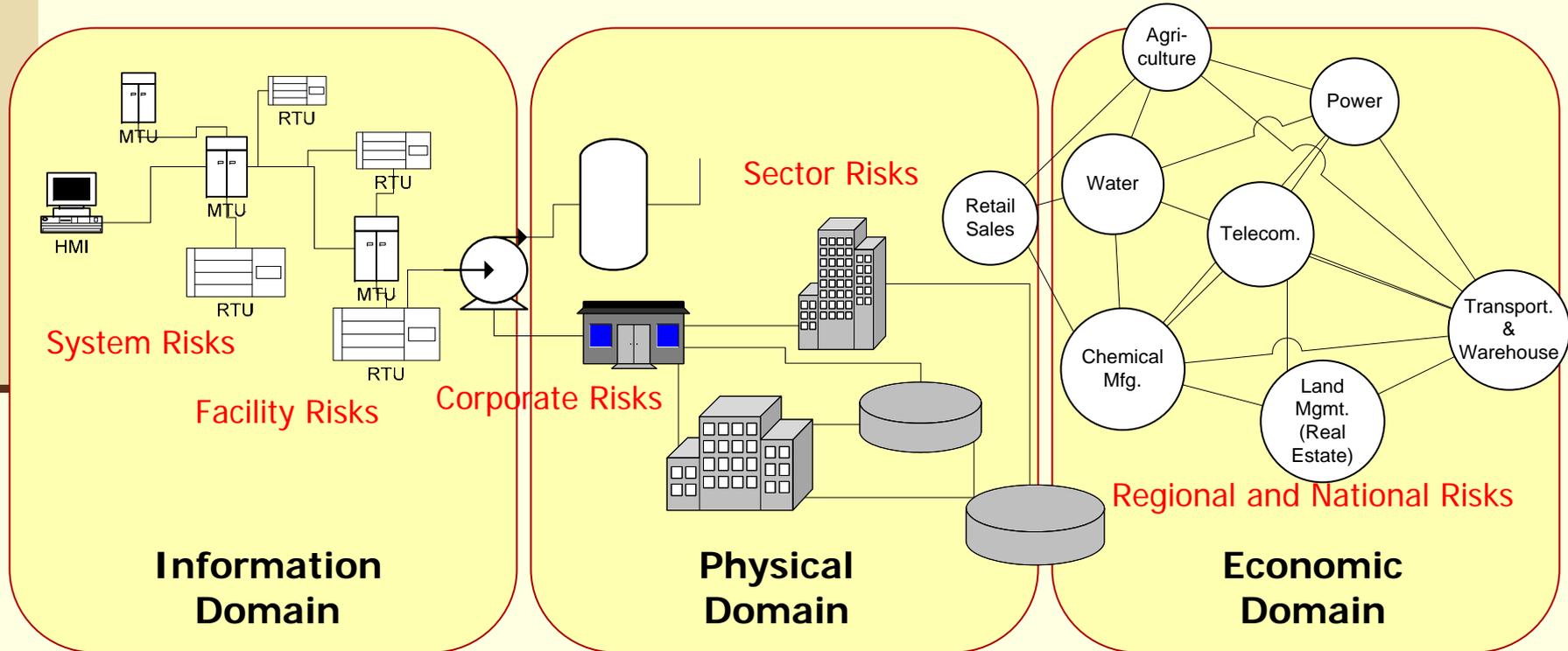
# Understanding and Applying Security Metrics

- Well-designed security metrics are needed to help the enterprise manage the security component of its business risks
- Reports: State of Practice, Metrics Requirements, and Metrics Tools reports
- Tools: 21 Steps Metric Tool & P-STET

# Understanding Cascading Impacts of Attacks on PCS

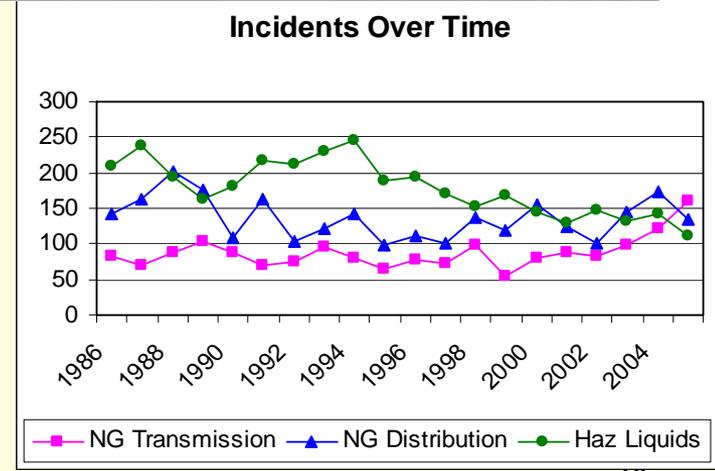
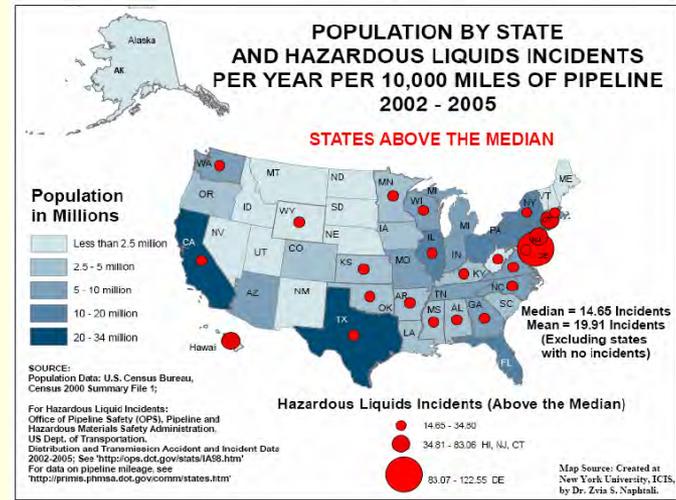
Quantifying cascading impacts requires:

- modeling and analysis at multiple scales
- supports decision making at multiple levels



# Understanding Trends, Causes and Consequences of Failures

- Looked at data on:
  - international terrorist attacks on pipeline infrastructures
  - domestic accidents and failures (from the Office of Pipeline Safety)
- Modeled trends to identify those causes that pose the greatest consequences
- Looked at correlations between the type of failure event and cost (i.e., product loss, property damage, clean-up & recovery)

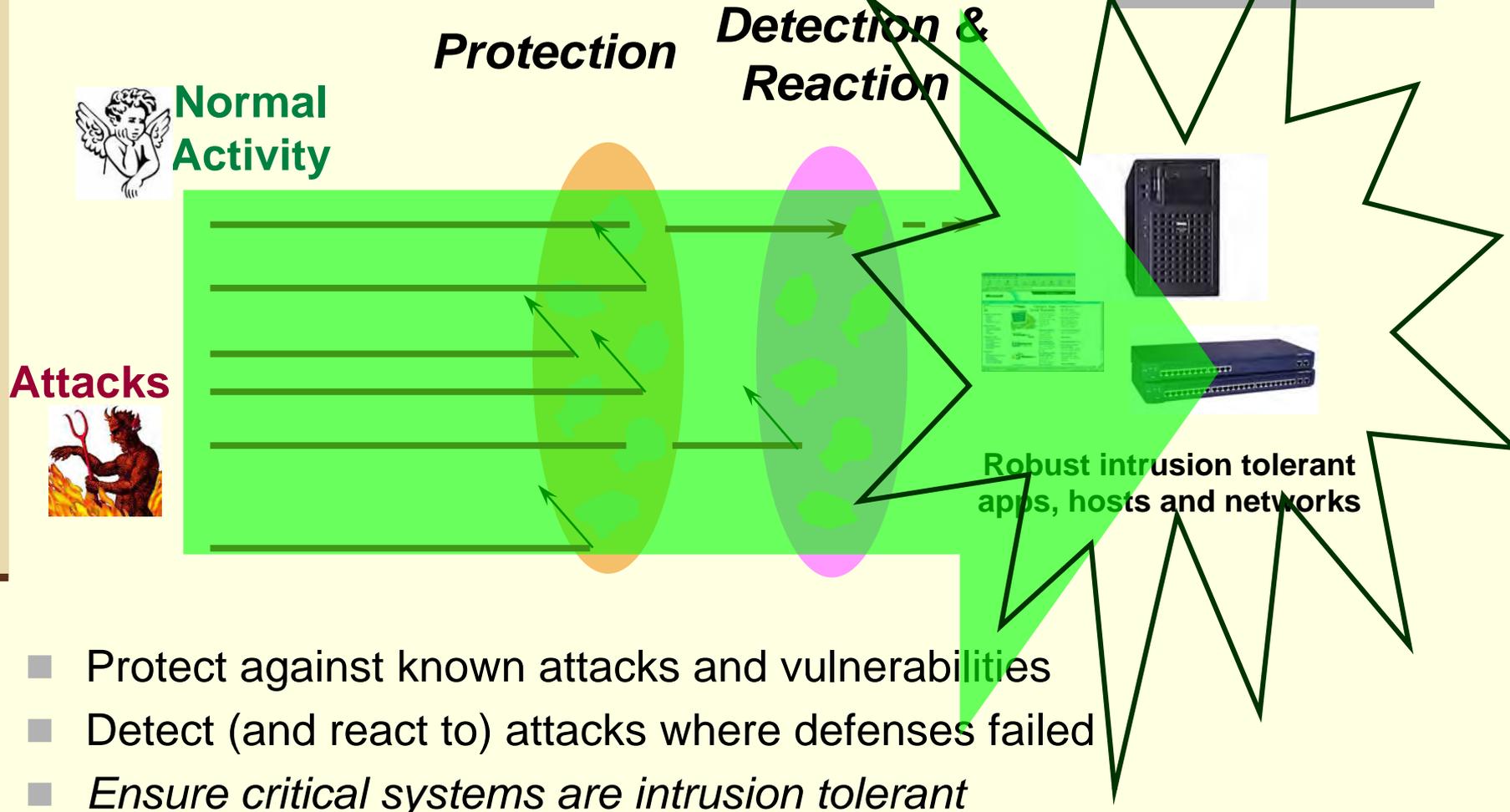


# Security tools and technologies

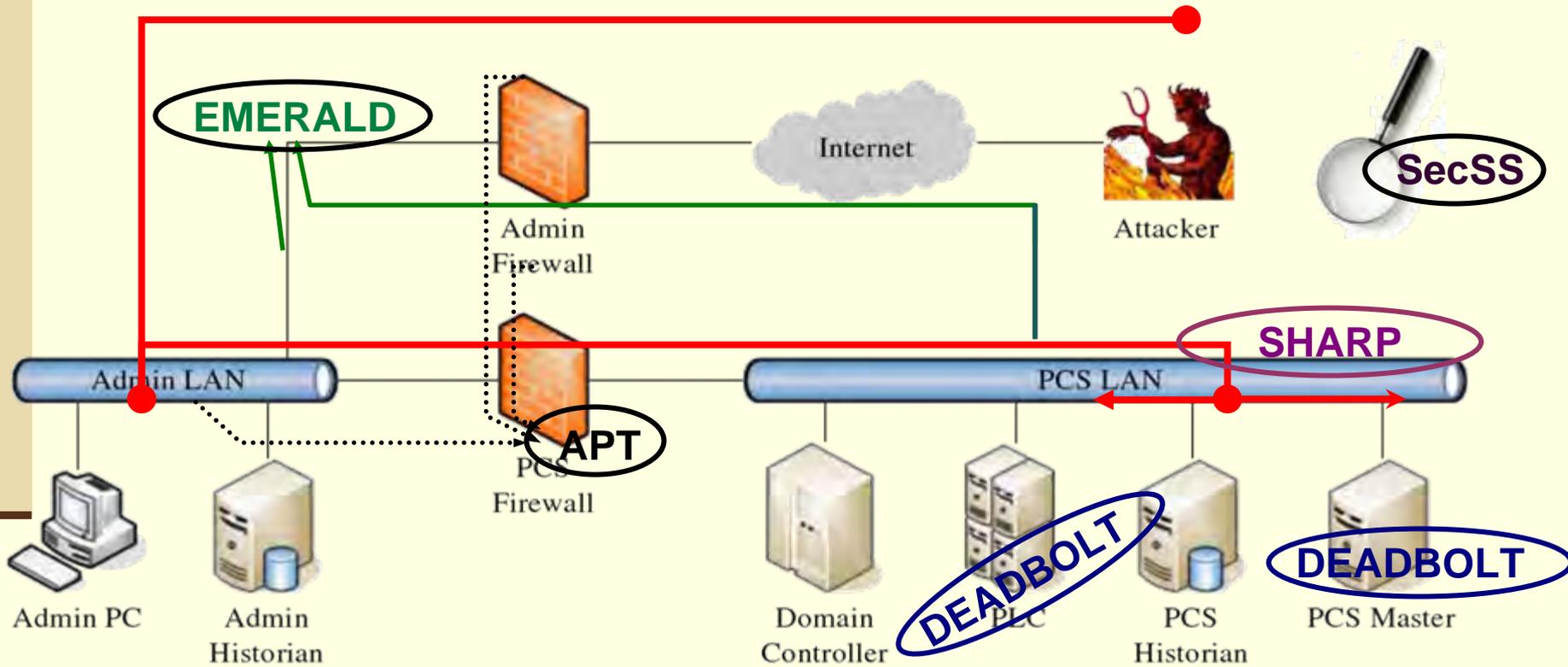
---

- Securing software with DEADBOLT
- Creating a secure platform with SHARP
- Implementing sound access policy with APT
- Addressing protocol vulnerabilities with SecSS
- Extending EMERALD for monitoring and situational awareness in Process Control Networks

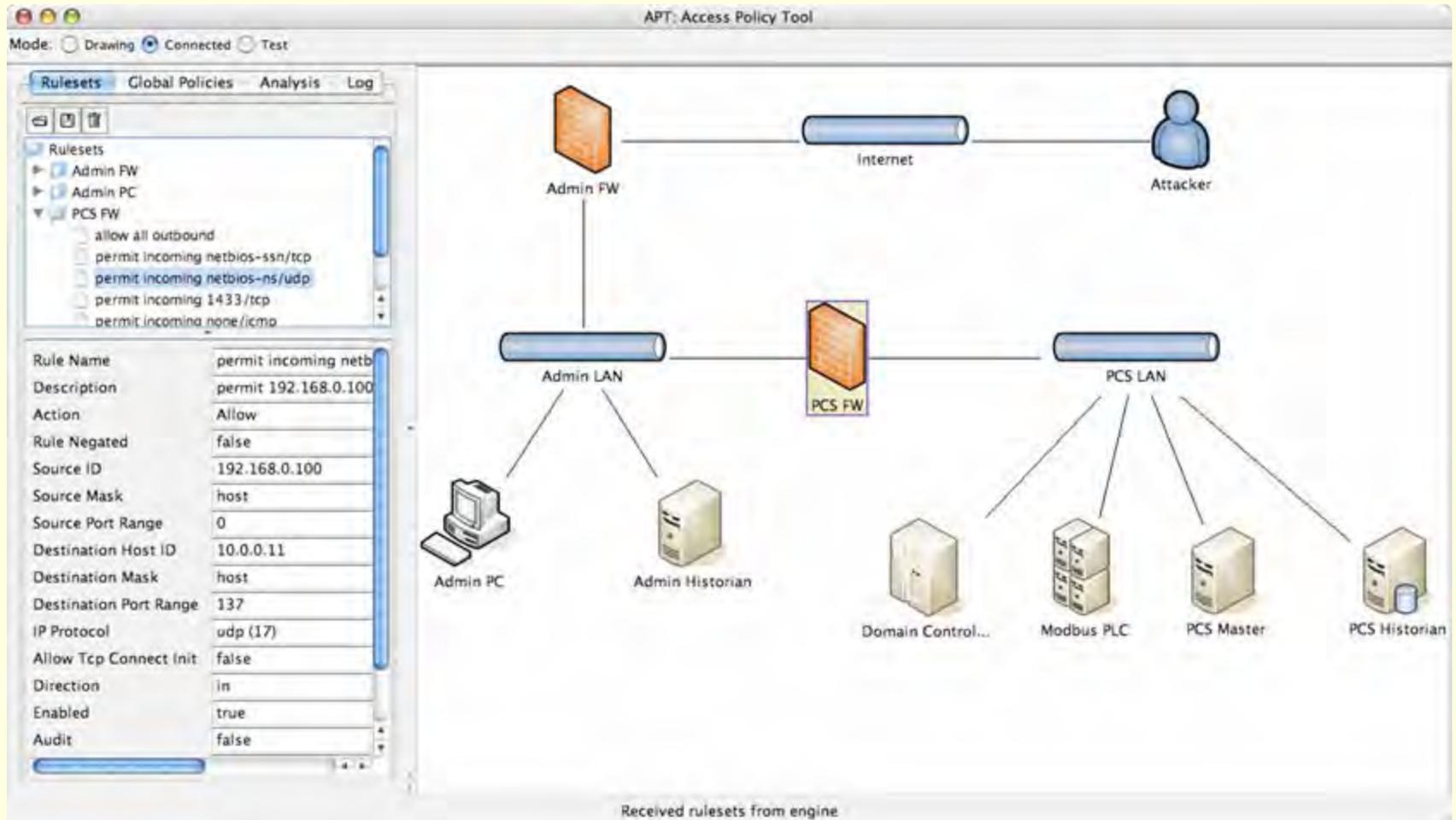
# Defense in Depth



# Tools



# Verifying Proper Policy Implementation with APT



# Detecting an Improper Configuration with the SecSS

PLC Information (Slave)

Master Information

Requested Operations

Operation Details

```

|||||MODBUS DEVICE|||||
-----Device ID-----
Unit ID:      1
Unit address: MAC=00:90:C2:C0:1F:FB IP=10.0.0.100
-----Master ID-----
1.-master:   MAC=00:0C:29:10:54:F9 IP=10.0.0.10
2.-master:   MAC=00:0C:29:93:34:17 IP=10.0.0.11
-----Function Codes-----
FC 3: READ HOLDING REGISTERS (OK), from: 1
FC 4: READ INPUT REGISTERS (OK), from: 1
FC 16: WRITE MULTIPLE REGISTERS (OK), from: 2
-----Addressed Memories (MB references)-----
Address:      200   Type:      INPUT REGISTERS (read only)
Master IP:    10.0.0.10      Status:    accomplished
---Memory Read---
Offset 0:    10011100  01111111
Offset 2:    01000100  10111011
...
Offset 22:   01000010  10010010
-----
Address:      244   Type:      HOLDING REGISTERS (read/write)
Master IP:    10.0.0.10      Status:    accomplished
---Memory Read---
Offset 0:    10000000  00000000
Offset 2:    01000100  10111011
-----
Address:      244   Type:      HOLDING REGISTERS (read/write)
Master IP:    10.0.0.11      Status:    accomplished
--Memory Written--
Offset 0:    11000000  00000000
Offset 2:    01000100  10011110
|||||-----|

```

# Detecting PCN Misuse with EMERALD

The screenshot shows the EMERALD Alert Management Interface. The main window displays a table of alerts with columns for Alert Gen Time, Alert Count, Start Time, Signature, Incident Class, Obs Name, Source, and Target. A sidebar on the left shows navigation options like Inbox, EMERALD, UIUC, UTILSA, and Trash. A detail view at the bottom shows the signature and value for a selected alert.

Alert Gen Time	Alert Count	Start Time	Signature	Incident Class	Obs Name	Source	Target
01/18/07 10:27:36	8	01/18/07 10:26:02	DYN_MODBUS_TCP_RE	Action Logged	snort_ipv4	10.0.0.11	10.0.0.100
01/18/07 10:28:39	53	01/18/07 10:25:02	DYN_MODBUS_TCP_RE	Access Violation	snort_ipv4	10.0.0.11	10.0.0.100
01/18/07 10:29:36	1883	01/18/07 10:25:00	DYN_UNAUTHORIZED_T	Connection Violation	snort_ipv4	10.0.0.11... [2]	10.0.0.11... [2]
01/18/07 10:18:18	1	01/18/07 10:18:18	DYN_BLEEDING-EDGE_	Privilege Violation	snort_ipv4	10.0.0.11	10.0.0.10
01/18/07 10:17:36	4503	01/18/07 10:15:57	DYN_UNAUTHORIZED_	Connection Violation	AlertMgr	102.168.0.100	10.0.0.11
01/18/07 10:17:36	4501	01/18/07 10:15:57	DYN_UNAUTHORIZED_	Connection Violation	AlertMgr	102.168.0.100	10.0.0.11
01/18/07 10:17:36	4502	01/18/07 10:15:57	DYN_UNAUTHORIZED_	Connection Violation	AlertMgr	10.0.0.11	102.168.0.100
01/18/07 10:17:36	4507	01/18/07 10:15:57	DYN_UNAUTHORIZED_	Connection Violation	snort_ipv4	10.0.0.11	102.168.0.100
01/18/07 10:15:41	1	01/18/07 10:15:41	DYN_BLEEDING-EDGE_	Privilege Violation	snort_ipv4	102.168.0.100	10.0.0.11
01/18/07 10:15:13	1	01/18/07 10:15:13	EXTERN_SQL	Access Violation	snort_ipv4	102.168.0.100	10.0.0.11
01/18/07 10:23:56	13	01/18/07 10:15:02	PROBE	Probe	AlertMgr	102.168.0.100	10.0.0.11
01/18/07 10:16:38	314	01/18/07 10:07:26	DYN_UNAUTHORIZED_T	Connection Violation	snort_ipv4	10.0.0.11... [2]	10.0.0.11... [2]
01/18/07 10:09:14	2	01/18/07 10:07:26	NEW_MB_UNIT	Suspicious Usage	emodbus	10.0.0.10	10.0.0.100... [2]
01/18/07 10:29:38	184	01/18/07 10:07:26	SUSPICIOUS_USAGE	Suspicious Usage	AlertMgr	10.0.0.10... [2]	10.0.0.100... [2]
01/18/07 09:31:27	1	01/18/07 09:31:27	APT_FW	Access Violation	AlertMgr	102.168.0.100	10.0.0.11
01/18/07 09:31:27	1	01/18/07 09:31:27	APT_FW	Access Violation	APT	172.16.0.0	102.168.0.0
01/18/07 10:26:08	45	01/18/07 09:24:17	probIncident	Probe	secs-ids	10.0.0.11	10.0.0.100
01/18/07 10:26:08	21	01/18/07 09:24:13	mbWriteViolation	Integrity Violation	secs-ids	10.0.0.11	10.0.0.100
01/18/07 10:26:08	84	01/18/07 09:24:13	newEntryLog	Action Logged	secs-passive-scanner	10.0.0.11	10.0.0.100
01/18/07 10:27:30	128	01/18/07 09:24:13	IncompleteMBTransaction	Suspicious Usage	secs-passive-scanner	10.0.0.11	10.0.0.100
01/18/07 10:26:08	217	01/18/07 09:24:12	illegalMBFunction	Suspicious Usage	secs-ids	10.0.0.11	10.0.0.100
01/18/07 10:26:01	228	01/18/07 09:24:12	mbReadViolation	Access Violation	secs-ids	10.0.0.11	10.0.0.100
01/18/07 10:26:08	2	01/18/07 09:24:12	RogueDeviceViolation	Connection Violation	secs-ids	10.0.0.11	10.0.0.100
01/18/07 10:07:26	5	01/18/07 09:08:37	newEntryLog	Action Logged	secs-passive-scanner	10.0.0.10	10.0.0.100... [2]

Annotations in the image point to specific rows in the table:

- "Multiple sensors" points to the 'AlertMgr' and 'snort\_ipv4' entries in the 'Obs Name' column for several rows.
- "Correlation" points to the 'AlertMgr' and 'secs-ids' entries in the 'Obs Name' column for several rows.

Detail view for the selected alert:

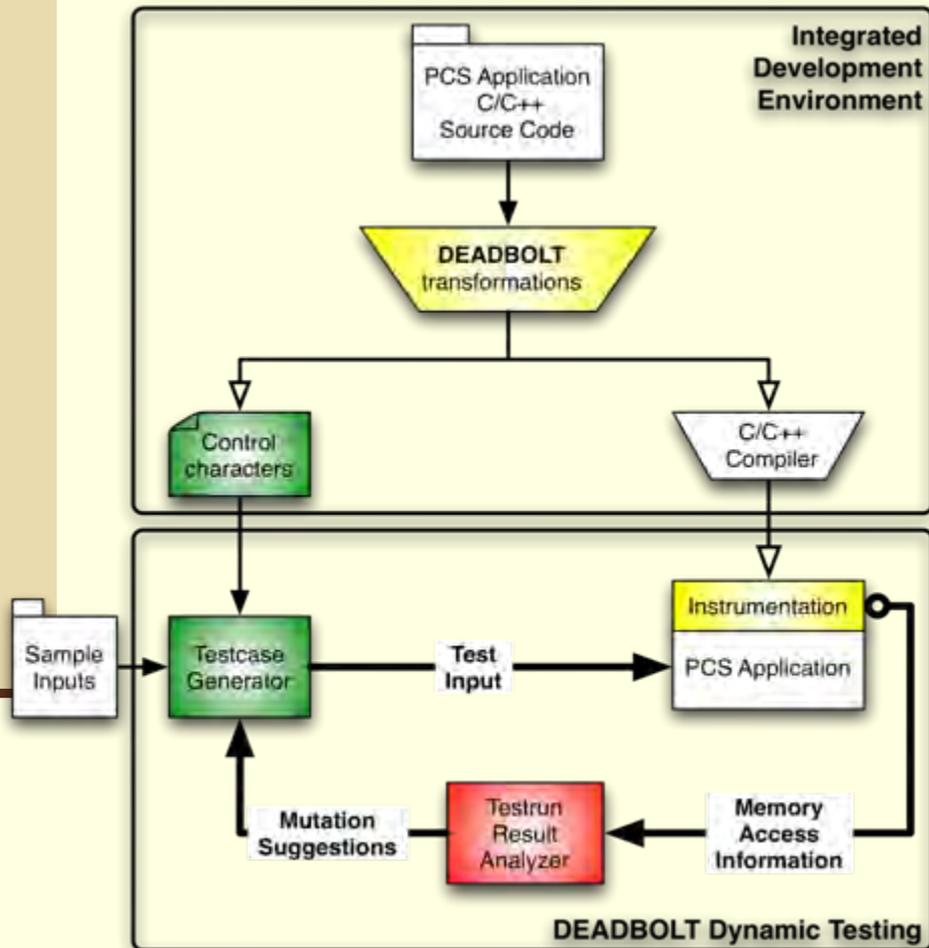
Detail	Value
Signature	DYN_UNAUTHORIZED_UDP_COMMUNICATION_BETWEEN_PCS_HISTORIAN_AND_NON-LOCAL_HOST
Local Description	DYN_UNAUTHORIZED_UDP_COMMUNICATION_BETWEEN_PCS_HISTORIAN_AND_NON-LOCAL_HOST
Sensor Description	CONNECTION_PATTERN:3008006: Unauthorized udp communication between PCS_HISTORIAN and non-local host
Observer Type	0
Observer ID	2084
Observer Stream	19
Observer Name	snort_ipv4

Multiple sensors

Correlation

Last alerts update at 1/18/07 9:32 AM  
Last alerts update at 1/18/07 9:33 AM  
Last alerts update at 1/18/07 9:34 AM

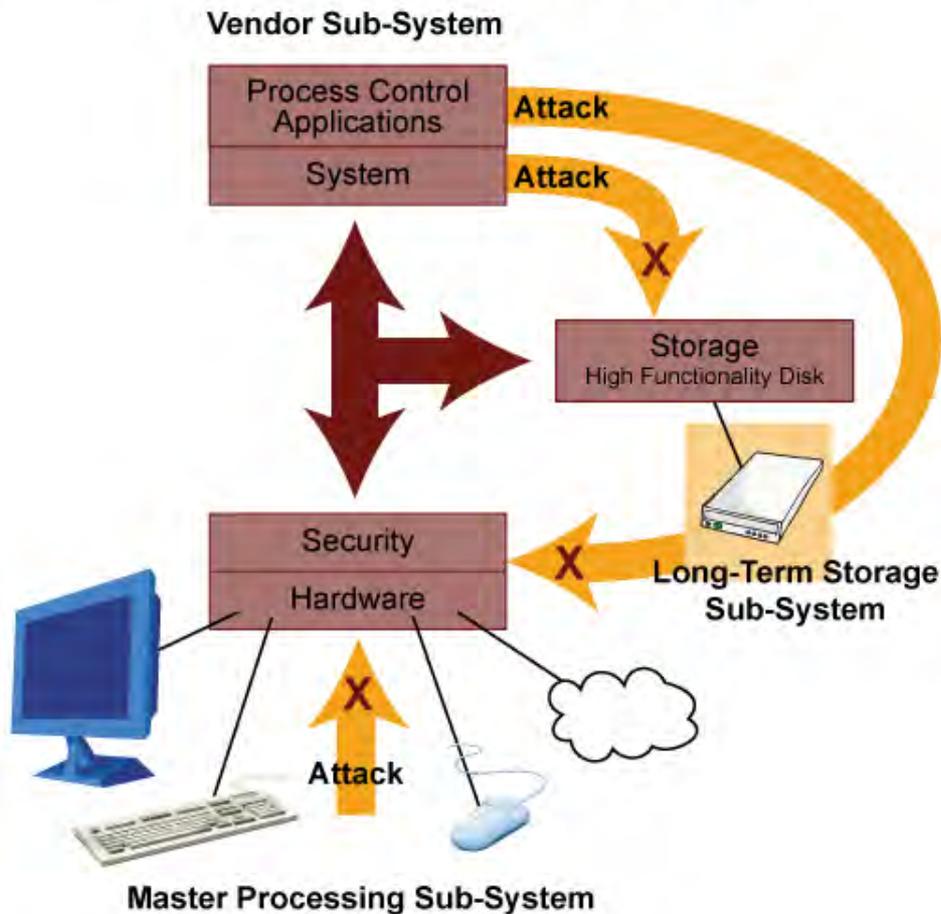
# Detecting Security Vulnerabilities with DEADBOLT



- Instruments C/C++ software for memory access errors
- Generates test inputs from a small collection of sample inputs
- Identifies the exact line of the software vulnerability

# Hardening the Platform with SHARP

## Security-Hardened Attack Resistant Platform



- Reduces possibility of privilege escalation
- Detects tampering and takes evasive action where possible
- Controls and protects local fixed and removable storage media from insider threats

# For More Information

- More project information is available on the I3P website: [www.thei3p.org/projects/pcs.html](http://www.thei3p.org/projects/pcs.html)
- There are several I3P talks at the Conference and a booth
- For general information about the I3P and its research agenda, contact:

Eric Goetz, I3P  
research@thei3p.org  
(603) 646-0692



*The PCS security research team gratefully acknowledges the support of the I3P, the oversight of DHS, and the guidance of all our industry partners*