

# Intrusion Monitoring and Situational Awareness in Infrastructure Systems

Sponsored by the Department of Energy National SCADA Test Bed Program  
Managed by the National Energy Technology Laboratory  
The views herein are the responsibility of the authors and do not necessarily reflect those of the funding agency.

**Alfonso Valdes**  
Senior Computer Scientist

**SRI International**



# Outline



- **Challenge to Infrastructure Systems**
- **Monitoring as part of Defense in Depth**
- **DATES Project Summary and Vision**
- **Model Based Detection in Control Systems**
- **Approach**
  - Detection
  - Event Management for Situational Awareness
  - Sector View
  - Test and Evaluation
- **Summary**

# Trends in Process Control Systems



- **Ubiquitous connectivity**
  - Improvements in productivity
  - Near real time access to process parameters
  - Modern systems in oil and gas, electric generation/distribution, manufacturing, water, transportation, and other sectors now depend on digital controls
  - Perimeter is diffuse or non-existent
- **Formerly proprietary standards, isolated networks (Security through obscurity and isolation)**
- **Increasingly, open standards (TCP/IP), common platforms, interconnected to business systems**
  - Vulnerabilities of IT systems now apply to PCS
  - Patching, security awareness and security practice in PCS tend to lag
- **This has improved productivity and efficiency, but potentially made these systems less secure**
  - Of interest to hacktivists, terrorists

# Monitoring as Part of Defense in Depth



## ◆ Control Systems use perimeter defenses

- Firewalls, switches
- Network segmentation
- DMZ between control and business networks

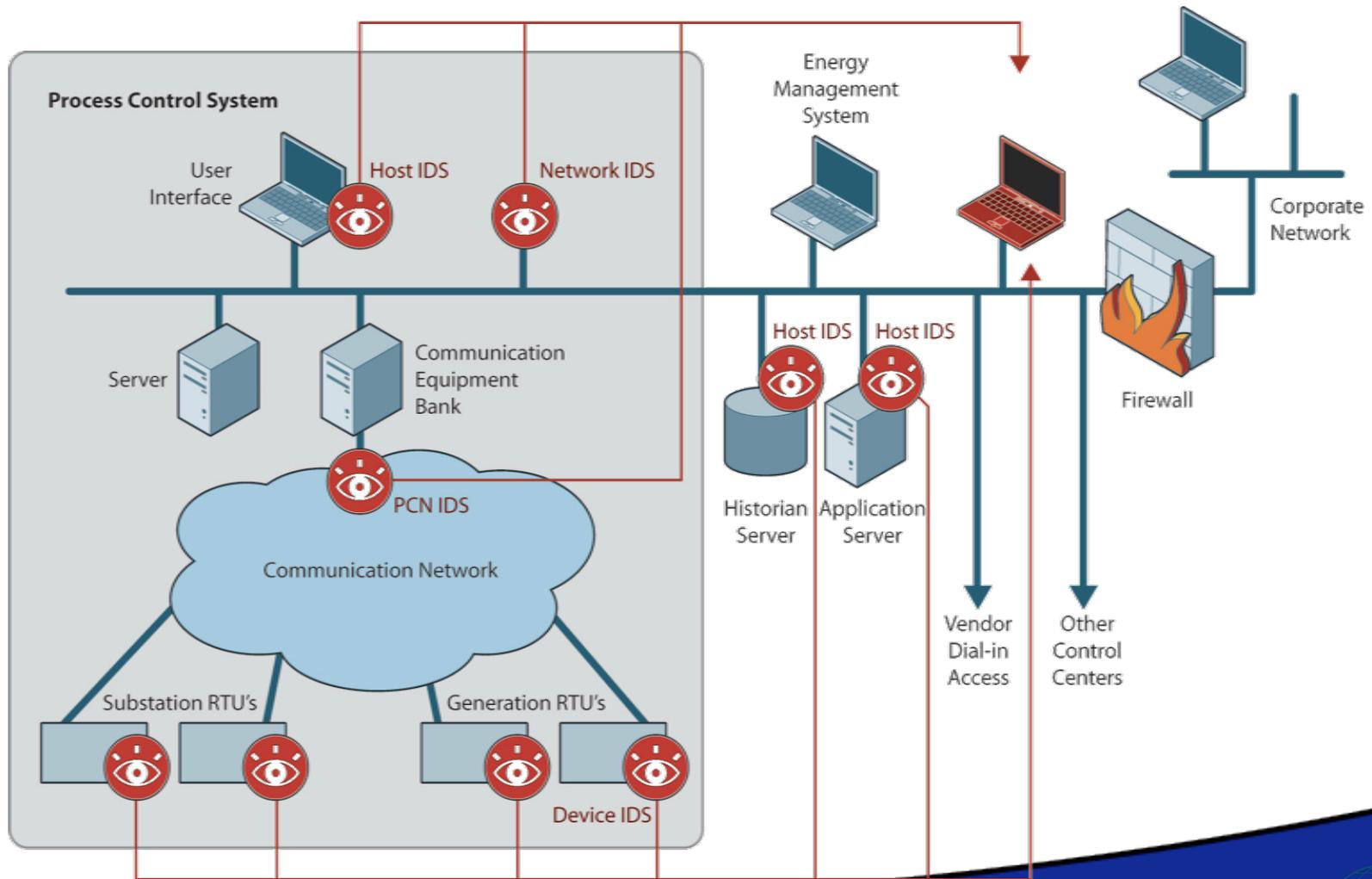
## ◆ Why monitor?

- Ensure perimeter defenses are still effective (Configuration Drift)
- Ensure perimeter defenses are not bypassed (Out of band connections, dual ported devices)
- Ensure perimeter defenses are not compromised (Attack on the firewall itself)
- Be aware of unsuccessful attempts to penetrate



# Detection and Analysis of Threats to the Energy Sector

# High Level Monitoring Architecture





# DATES Vision

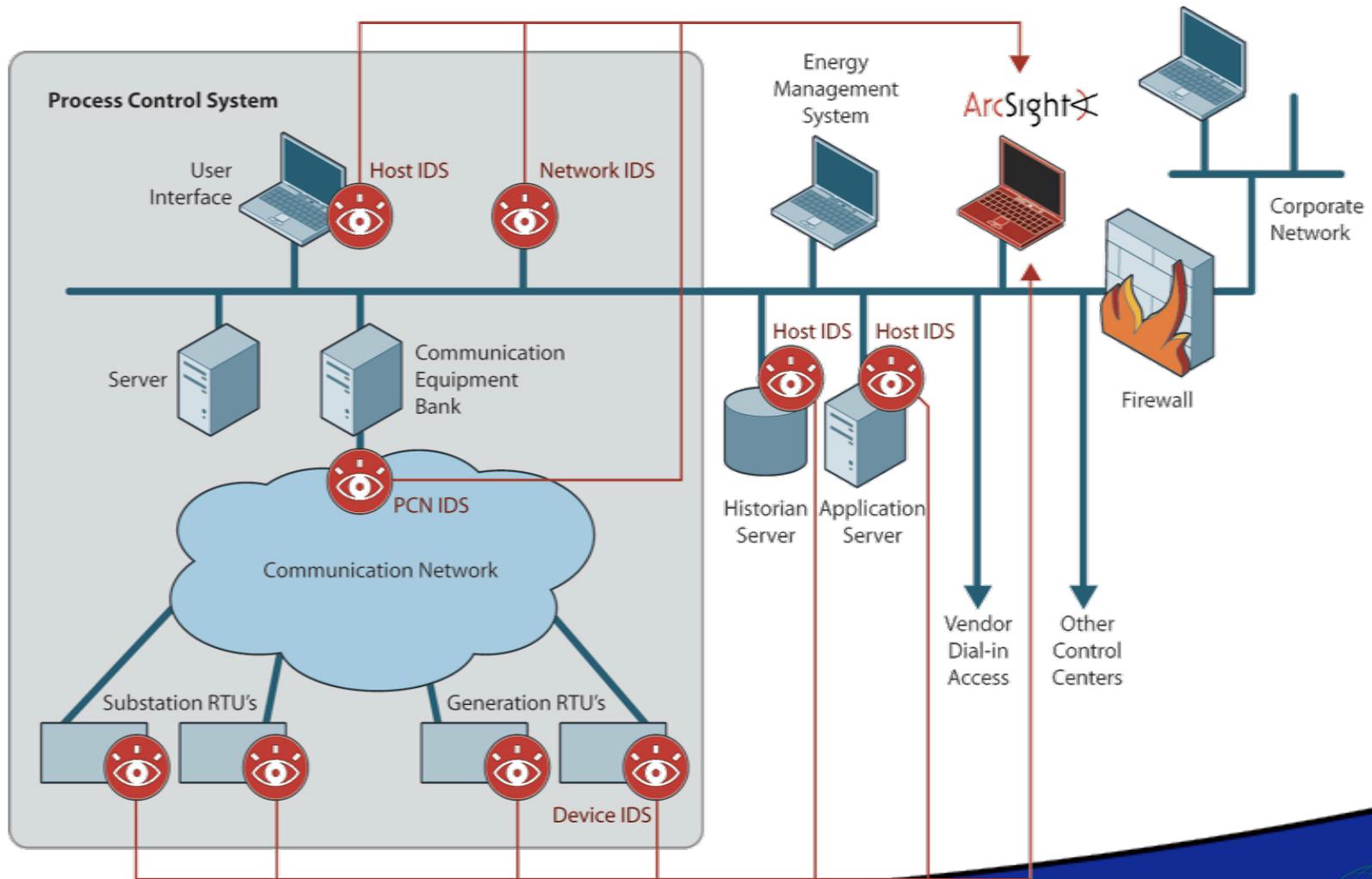
- ◆ **Future control systems with PCS aware defense perimeter with globally-linked cyber defense coordination...**
  - IDS systems fully tuned for control system protocols and highest threat TCP/IP attacks
  - Realtime event correlation system to support local operator identification and response
  - Specification-based policies enabling intrusion prevention without impacting availability
  - An anonymous and secure peer sharing framework that allows
    - Sector wide threat intelligence acquisition and rapid republication to emerging threats
    - An ability to allow DOE/ISOCs/Corporate Alliances to isolate sector-specific attack patterns and to respond as a community

# Project Relevance



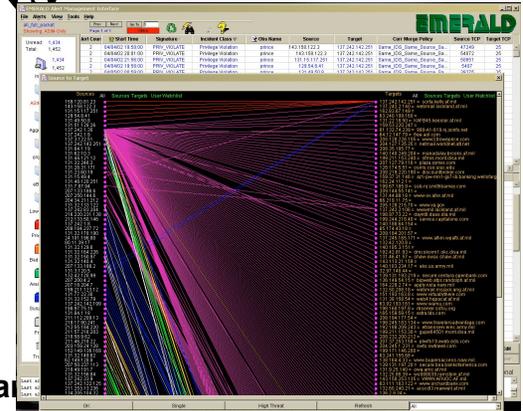
- **DOE's challenge to industry and the R&D community: to survive cyber attack on control systems with no loss of critical function**
- **DATES addresses this challenge by enabling the following capabilities**
  - Detection of attacks at various points in a PCS
  - Situational awareness across the assets of one utility
  - Identify and contain propagating attacks
  - Sector-coordinated response to sector-wide attacks
- **Control systems are critically important to the safe and efficient operation of infrastructure systems but are vulnerable to cyber attacks:**
  - Control systems security problems and remediation approaches are different from IT
  - Effects of cyber attacks on operations and interdependent infrastructures not well understood

# Architecture (Tasks 1 and 2)



# Detection Strategy: Control LANs

- **EMERALD IDS/MCorr appliance**
  - Pattern Anomaly
  - Bayes analysis of TCP headers
  - Stateful protocol eXperts
  - Complemented by custom ruleset SNORT
- **Alerts (potentially from multiple IDS appliances) forwarded to correlation framework**
- **PCS Enhancements**
  - Digital Bond PCS rule set
  - Model Based Detection
  - Expand KB to comprehend additional protocols, e.g., OPC



EMERALD Alert Management Interface

Alert Gan	Time	Alert Count	Start Time	Signature	Incident Class	Obs Name	Source	Target
011707	18 51 00	35457	011707 15 05 48	DYN_UNAUTHORIZED_T...	Connection Violation	snort_ipv4	10.0.0.10... [2]	10.0.0.101... [2]
011707	18 44 21	25	011707 15 49 32	DYN_BLEEDING-EDGE...	Privilege Violation	AlertMgr	192.168.0.100	10.0.0.11
011707	18 44 21	9	011707 15 49 32	DYN_BLEEDING-EDGE...	Privilege Violation	snort_ipv4	192.168.0.100	10.0.0.11
011707	18 26 43	4	011707 15 58 59	DYN_BLEEDING-EDGE...	Privilege Violation	snort_ipv4	10.0.0.11	10.0.0.10
011707	18 26 30	162	011707 15 05 48	SUSPICIOUS	Suspicious Usage	AlertMgr	10.0.0.7... [3]	10.0.0.100... [2]
011707	18 26 30	324	011707 15 53 36	DYN_UNAUTHORIZED_T...	Connection Violation	snort_ipv4	10.0.0.1... [3]	10.0.0.1... [4]
011707	18 26 30	349	011707 15 22 47	DYN_UNAUTHORIZED_T...	Connection Violation	snort_ipv4	10.0.0.7... [3]	10.0.0.7... [3]
011707	18 26 30	9	011707 18 24 25	DYN_MODBUS_TCP_RE...	Action Logged	snort_ipv4	10.0.0.11	10.0.0.100
011707	18 24 30	18	011707 18 23 04	DYN_MODBUS_TCP...	Access Violation	snort_ipv4	10.0.0.11	10.0.0.100
011707	18 23 41	9	011707 18 23 08	BAD_ACCESS	Access Violation	snort_ipv4	10.0.0.11	10.0.0.100
011707	18 22 04	1	011707 18 22 04	DYN_UNAUTHORIZED...	Connection Violation	snort_ipv4	10.0.0.10	10.0.0.100
011707	18 14 48	277	011707 15 43 59	PORT_SCAN	Probe	eBayes-TCP	192.168.0.100	10.0.0.11
011707	18 09 50	29	011707 15 49 32	DYN_BLEEDING-EDGE...	Privilege Violation	AlertMgr	192.168.0.100	10.0.0.11
011707	18 09 50	7	011707 15 49 32	DYN_BLEEDING-EDGE...	Privilege Violation	snort_ipv4	192.168.0.100	10.0.0.11
011707	15 58 01	1	011707 15 58 01	NEW_SVC	Suspicious Usage	eBayes-TCP-host	192.168.0.100	10.0.0.11
011707	15 51 48	4818	011707 15 43 59	DYN_UNAUTHORIZED...	Connection Violation	AlertMgr	192.168.0.100	10.0.0.11
011707	15 51 48	4821	011707 15 50 21	DYN_UNAUTHORIZED...	Connection Violation	AlertMgr	10.0.0.11	192.168.0.100
011707	15 51 48	4819	011707 15 43 59	DYN_UNAUTHORIZED...	Connection Violation	snort_ipv4	192.168.0.100	10.0.0.11
011707	15 27 50	8	011707 15 22 47	DYN_MODBUS_TCP_W...	Suspicious Usage	snort_ipv4	10.0.0.7	10.0.0.100
011707	15 22 47	7	011707 15 05 48	SUSPICIOUS	Suspicious Usage	AlertMgr	10.0.0.7... [2]	10.0.0.100... [2]
011707	15 07 00	2	011707 15 05 48	NEW_MB_UNIT	Suspicious Usage	emodbus	10.0.0.10	10.0.0.100... [2]

Detail	Value
Sensor Description	Digital_Bond_Inc_modbus_tcp_rules_v_1_0-1111000: Modbus TCP - Unauthorized Read Request to a PLC
Observer Type	0
Observer ID	2084
Observer Stream	19
Observer Name	snort_ipv4
Observer Start Time	0
Observer Version	011707 15 05 48
Observer Location	minime-andia
Outcome Generic	Outcome Unknown
Source IP	10.0.0.11

at 1/17/07 3:13 PM  
Last alerts update at 1/17/07 3:13 PM  
Last alerts update at 1/17/07 3:14 PM



# Model Based Detection in PCS

# Approaches Provide Complementary Protection



Approach	Basis	Attacks Detected	Generalization
Misuse	Signature, Protocol reconstruction	Known	No
Anomaly	Learned models of normal	Must appear anomalous (not all do, FP)	Yes
Probabilistic	Model learning	Match patterns of misuse	Some
Spec based	Analysis of protocol spec	Attacks must violate spec (not all do)	Yes

## **Drawbacks of specification-based models:**



- ◆ **For general enterprise systems, constructing models is expensive and difficult**
  - system complexity,
  - complexity of user activity
- ◆ **Inaccurate models can lead to false alarms and/or missed detections**



# Aspects of Model-Based Detection

## ◆ Values in specific fields in protocol

- Must be valid according to the protocol
- Must be valid for the specific implementation (learned)

## ◆ Dependent values

- A value in one field restricts the value or range of values in other fields

## ◆ Communication Patterns

- Master/Slave relations
- Allowed protocols between nodes
- Message frequency



## Detecting Unusual Communication Patterns (2)

- ◆ Learn Patterns via monitoring
- ◆ Similar patterns are potentially merged
- ◆ New pattern generates alerts when observation of new patterns becomes unusual
  - Aspects of annealing
- ◆ Rarely seen patterns are pruned out
- ◆ Ability to whitelist rare patterns or blacklist not so rare patterns



# Visualization of Comm Patterns (OPC)



## Security Incident Event Management



- ◆ **Implement an event correlation framework to integrate new detection data sources into the ArcSight security event management framework**
- ◆ **Provide a groundbreaking Security Incident/Event Management (SIEM) capability in infrastructure systems.**

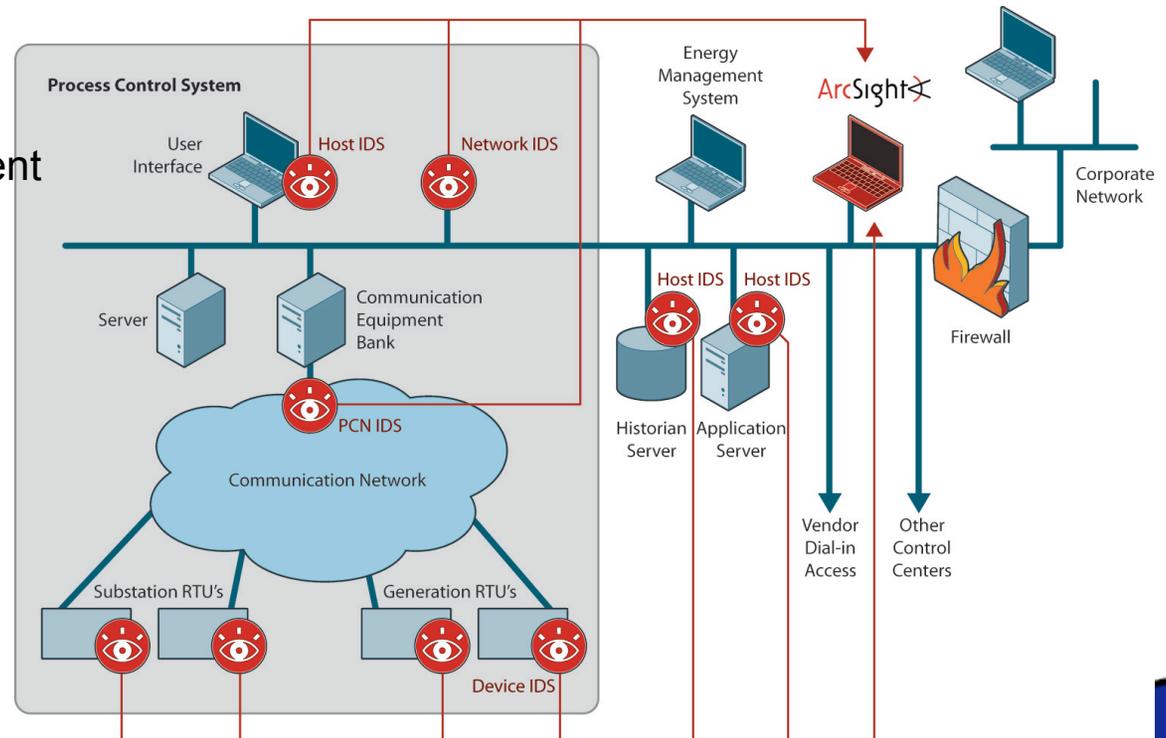
# Detection and Event Management



- Control System aware IDS at the Device, Control LAN, and Host
- Event Correlation integrates new detection data sources into ArcSight

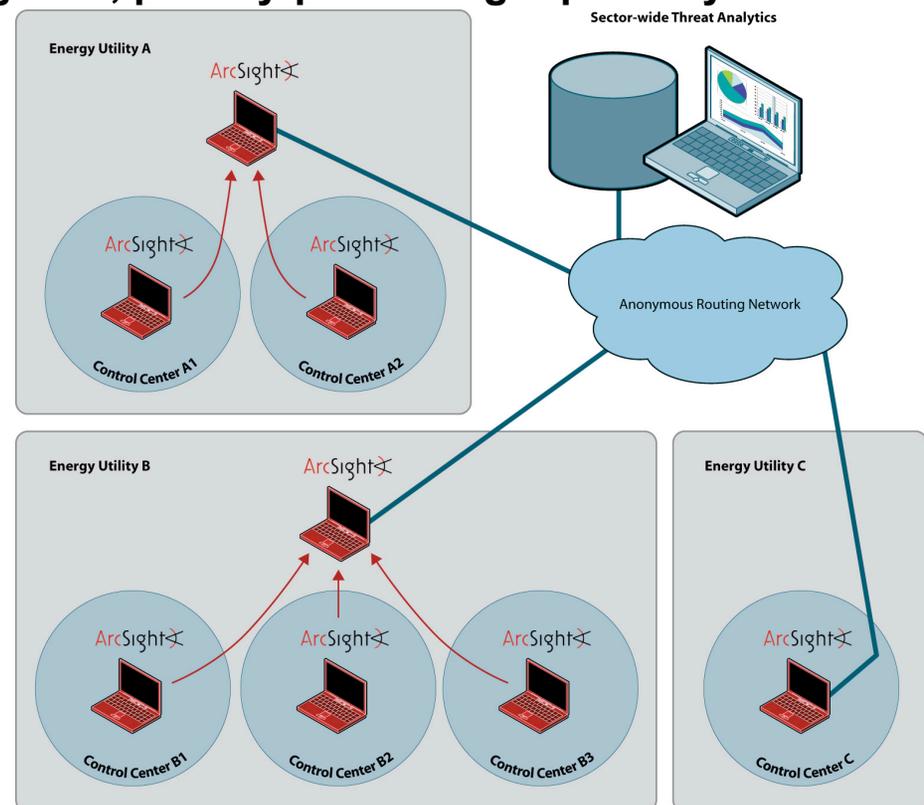
- Result:

- Breakthrough Detection and Security Incident/Event Management (SIEM) in infrastructure systems.
- High fidelity situational awareness



# Sector Level Threat Detection and Analysis

- Develop a sector-wide, distributed, global, privacy-preserving repository of security events
- Enable participants to automatically
  - Contribute event data without attribution
  - Query databases for emerging threats
  - Conduct analyses to assess their security posture relative to that of other participants.

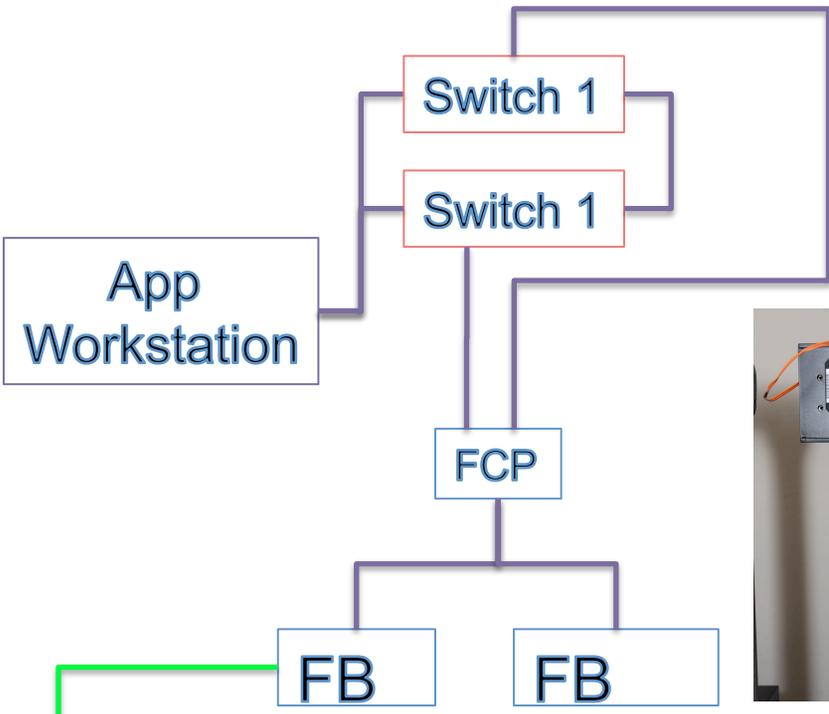
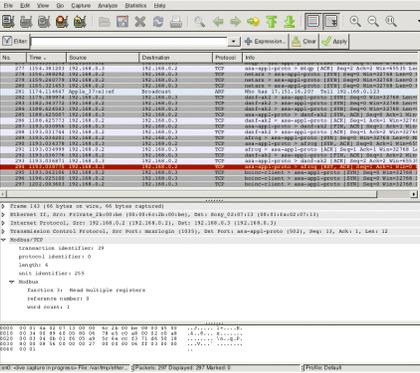
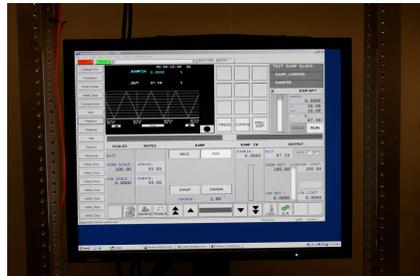




## Test and Evaluation

- ◆ **Implement a development environment in cooperation with a control systems vendor**
- ◆ **Sandia will provide a red team assessment of this defense-enabled control system architecture.**
- ◆ **As solutions mature, Sandia will conduct an extensive red team test and evaluation on the actual system.**

# System Diagram



— Control LAN  
— Field LAN



## The Team

- ◆ **SRI (Overall Lead): Intrusion Detection, Protocol Analysis, Event Aggregation, Privacy Preserving Sector-wide Repository**
- ◆ **Sandia National Laboratories: Architectural Vulnerability Analysis, Attack Scenarios, Red Team**
- ◆ **ArcSight: Security Incident Event Management**



# Summary

- **DATES provides essential monitoring capability in support of DOE Roadmap objectives**
  - PCS specific monitoring at device, network, host levels
  - Applicable to O&G and electric sectors
  - Breakthrough capabilities in PCS SEM
  - Sector-wide view
- **Solution will be validated on a realistic DCS testbed through rigorous experimentation**
- **Complementary to best practices**
- **Synergies with industry and the research community**



Backup

# Security Monitoring of Control Systems



- **Barrier defenses (switches, firewalls, network segmentation) are essential, but**
- **An orthogonal view is essential to detect when these have been bypassed or penetrated**
- **One detection approach may not alert on a critical exploit**
- **Project Objectives in Detection:**
  - Develop, adapt, enhance, and implement required intrusion detection technologies
  - Provide timely and accurate alerting in the case of attempted cyber attacks against control systems
  - Provide customized attack detection capabilities at each of the network, host, and device levels
- **Correlation of related events is essential to provide the operator coherent situational awareness**

# Intrusion Detection Approaches



- **Signature: Match traffic to a known pattern of misuse**
  - Stateless: String matching, single packet
  - Stateful: Varying degrees of protocol and session reconstruction
  - Good systems are very specific and accurate
  - Typically does not generalize to new attacks
- **Anomaly: Alert when something “extremely unusual” is observed**
  - Learning based, sometimes statistical profiling
  - In practice, not used much because of false alarms
  - Learning systems are also subject to concept drift



## Intrusion Detection Approaches (2)

- ◆ **Probabilistic (Statistical, Bayes): A middle ground, with probabilistically encoded models of misuse**
  - Some potential to generalize
- ◆ **Specification based (some group this with anomaly detection): Alert when observed behavior is outside of a specification**
  - High potential for generalization and leverage against new attacks

# Our Hypothesis



- **By comparison to enterprise systems, control systems exhibit comparatively constrained behavior:**
  - Fixed topology
  - Regular communication patterns
  - Limited number of protocols
  - Simpler protocols
- **As such, specification- and model-based IDS approaches may be more feasible**
- **Such an approach nicely complements a signature system**
- **Benefits are a compact, inherently generalized knowledge base and potential to detect zero day attacks**



## Protocol Model: Individual fields

- ◆ **MODBUS function codes are one byte**
  - 256 possible values, but
  - MSB is used by servers to indicate exception
  - 0 is not valid, so valid range in 1-127
- ◆ **Range is partitioned into public, user-defined, and reserved**
  - With no further knowledge, can construct a “weak specification”
- ◆ **Many actual devices support a much more limited set of codes**
  - Permits definition of a stronger, more tailored specification



## Protocol Model: Dependent Fields

- ◆ **Encode acceptable values of a field given the value of another field**
  - Example dependent fields include length, subfunction codes, and arguments
  - For example, “read coils” function implies the length field is 6
  - For other function codes, length varies but a range can be specified
- ◆ **Specifications for multiple ADUs: future work**

# Detecting Unusual Communication Patterns



- **Specification of network access policies**
  - Comms between CZ and DMZ are restricted to corporate historian client and DMZ historian server
  - Comms between DMZ and PCZ are restricted to PCZ SCADA historian and DMZ historian server
  - SCADA server may communicate with the flow computer and the PLC using MODBUS
  - SCADA server may communicate to SCADA historian
  - SCADA HMI may communicate with SCADA server and engineering station
- **Detection of exceptions is via SNORT rules**
- **More complex networks (more devices) can be accommodated via IP address assignment with appropriate subnet masks**