# Detection and Analysis of Threats to the Energy Sector (DATES)


**Alfonso Valdes**

Senior Computer Scientist

**SRI International**



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.

# Securing Process Control Systems

- **Digital controls are essential to modern infrastructure systems**
- **Migration from proprietary systems to commodity platforms, TCP/IP and other common standards, connection to corporate IT**
  - Significant gains in productivity, inter-operability
  - Increasing exposure to cyber attack?
- **Best practice architectures call for perimeter defenses**
  - Increasingly diffuse electronic perimeter
- **Intrusion Detection provides a necessary complementary defense**

# DATES Vision

- Future control systems with PCS aware defense perimeter
- IDS systems fully tuned for control system protocols and highest threat attacks
- Realtime event correlation system for threat identification and response
- Developed in partnership with leading SIEM and PCS providers
- Demonstrated on realistic PCS implementations

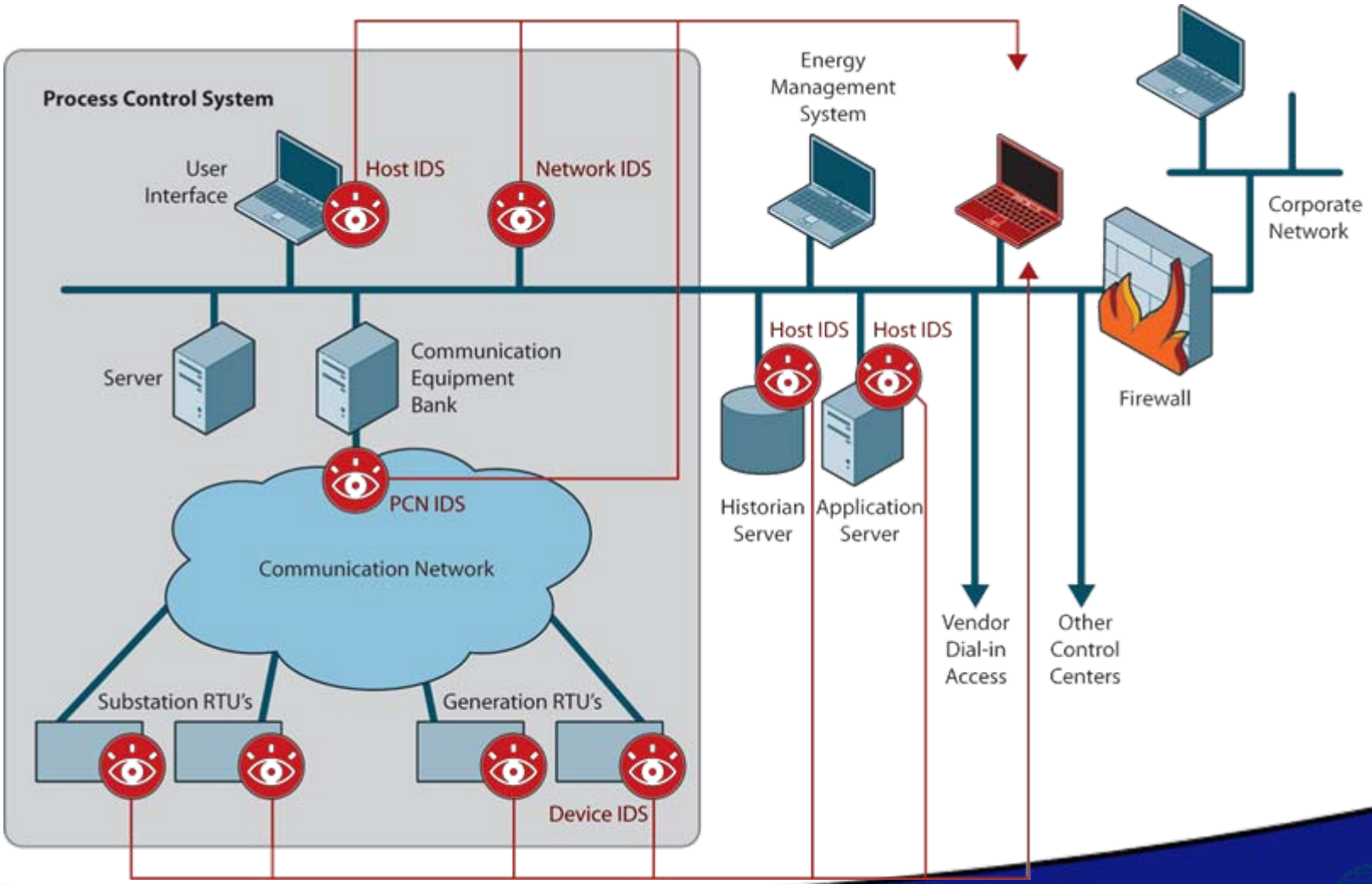
# Intrusion Monitoring as Part of Defense in Depth

- **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—What's on YOUR Field LAN?)
  - Ensure perimeter defenses are not compromised (Attack on the firewall itself)
  - Be aware of unsuccessful attempts to penetrate

# Detection Strategies

- **Signature: Look for known misuse**
- **Model Based**
  - Note regularities in PCS traffic
  - From configuration to rules
  - Machine learning of comm patterns, master/slave, temporal dynamics
  - Encode a model of expected behavior
  - Alert on exceptions
- **Specification**
  - Based on formal analysis of a protocol, or a particular implementation of a protocol
- **Deep process awareness**

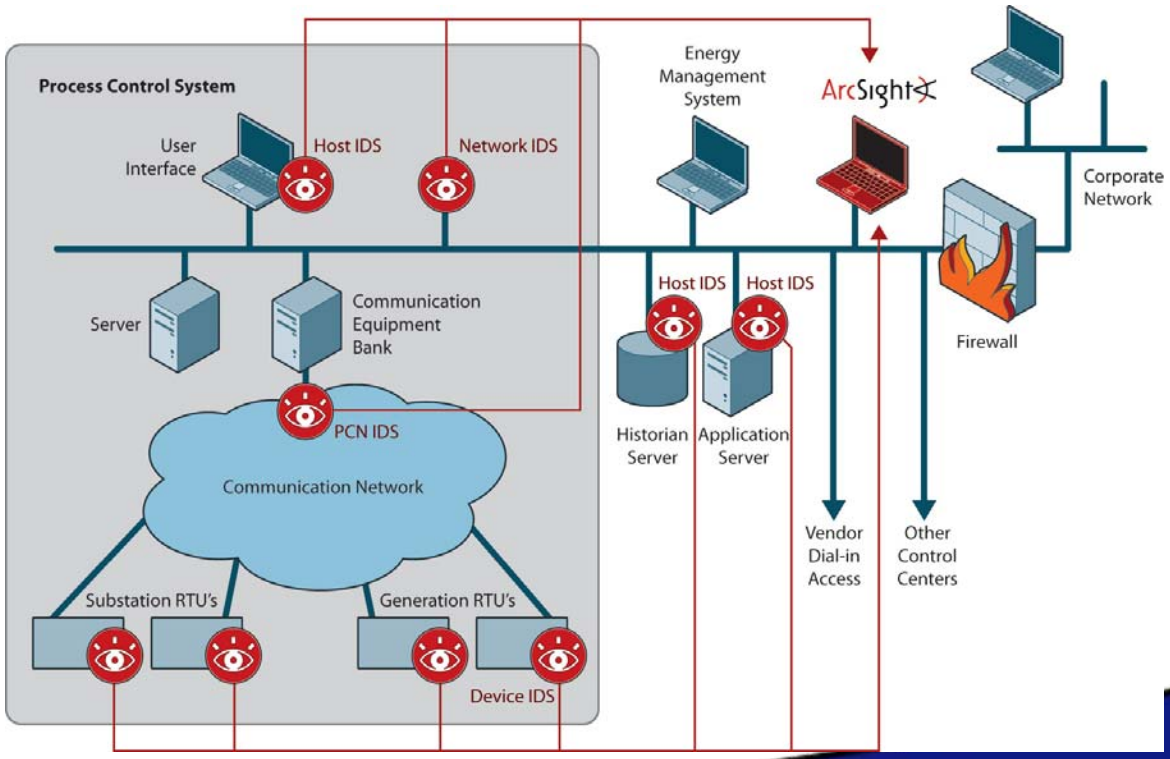
# High Level Monitoring Architecture



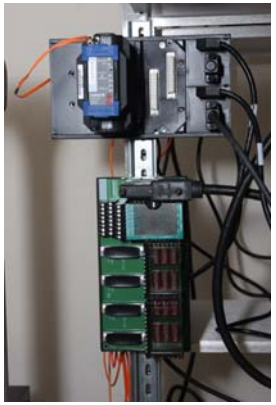
# Visualization of Comm Patterns (OPC)

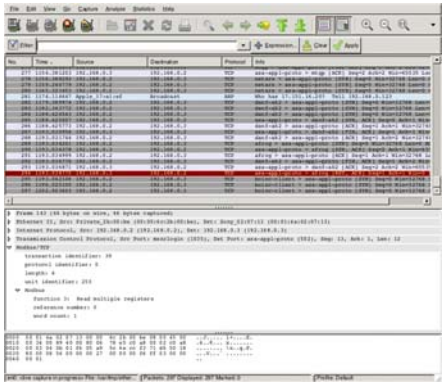
# Detection and Event Management

- **Control System aware IDS at the Device, Control LAN, and Host**
- **Event Correlation integrates new detection data sources into ArcSight**
- **Result:**
  - Correlate attack steps
  - Follow an attack across LAN segments



# Test System Diagram (SRI/Invensys)








Control LAN

Field LAN

# Partnership Between R&D and Industry

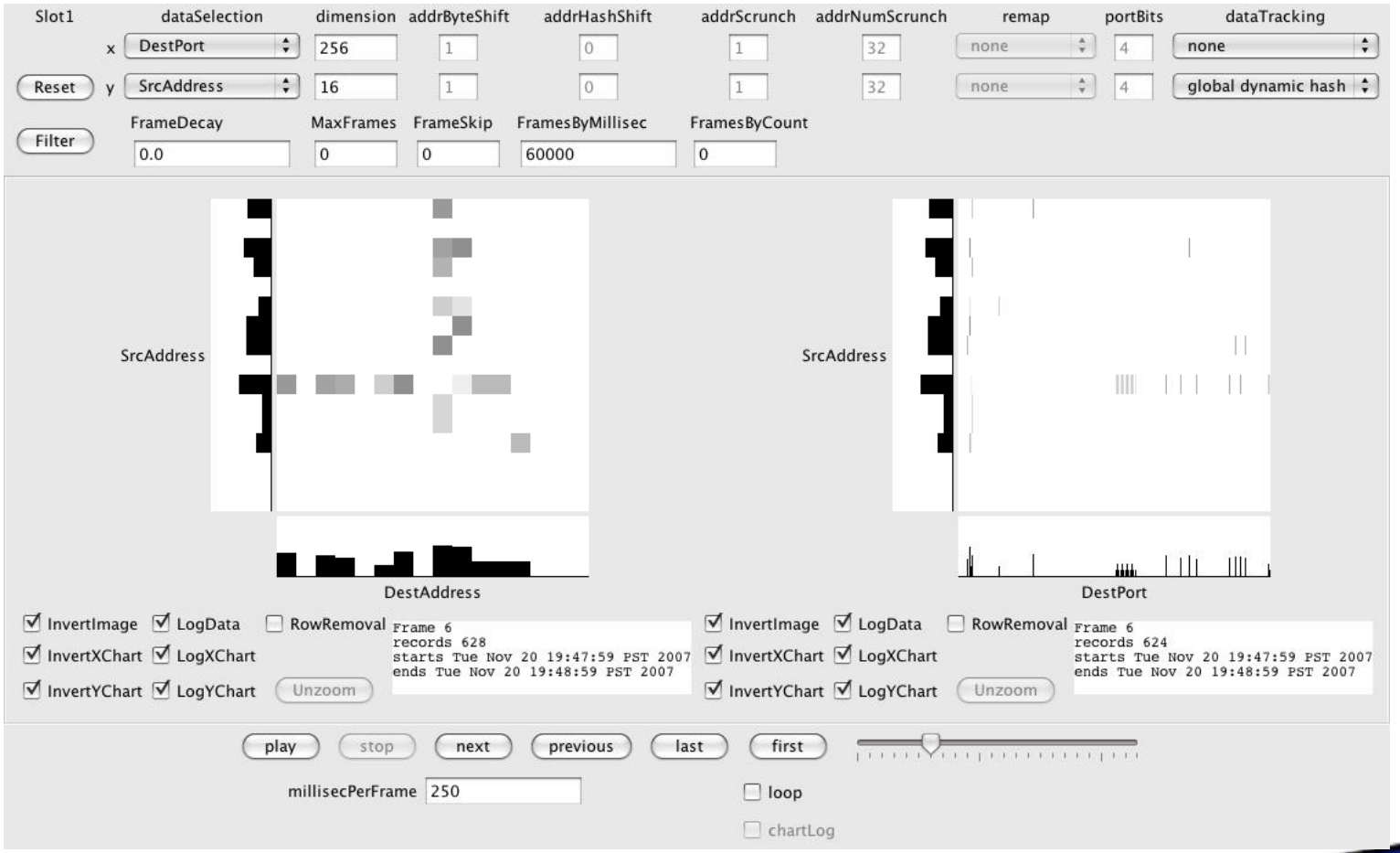
- **SRI (Overall Lead): Intrusion Detection, Protocol Analysis, Event Aggregation**
- **Sandia National Laboratories: Architectural Vulnerability Analysis, Attack Scenarios, Red Team**
- **ArcSight: Security Incident Event Management, Situational Awareness Dashboards**
- **Invensys: Demonstration System, real-world protocol implementations**

# DATES Summary

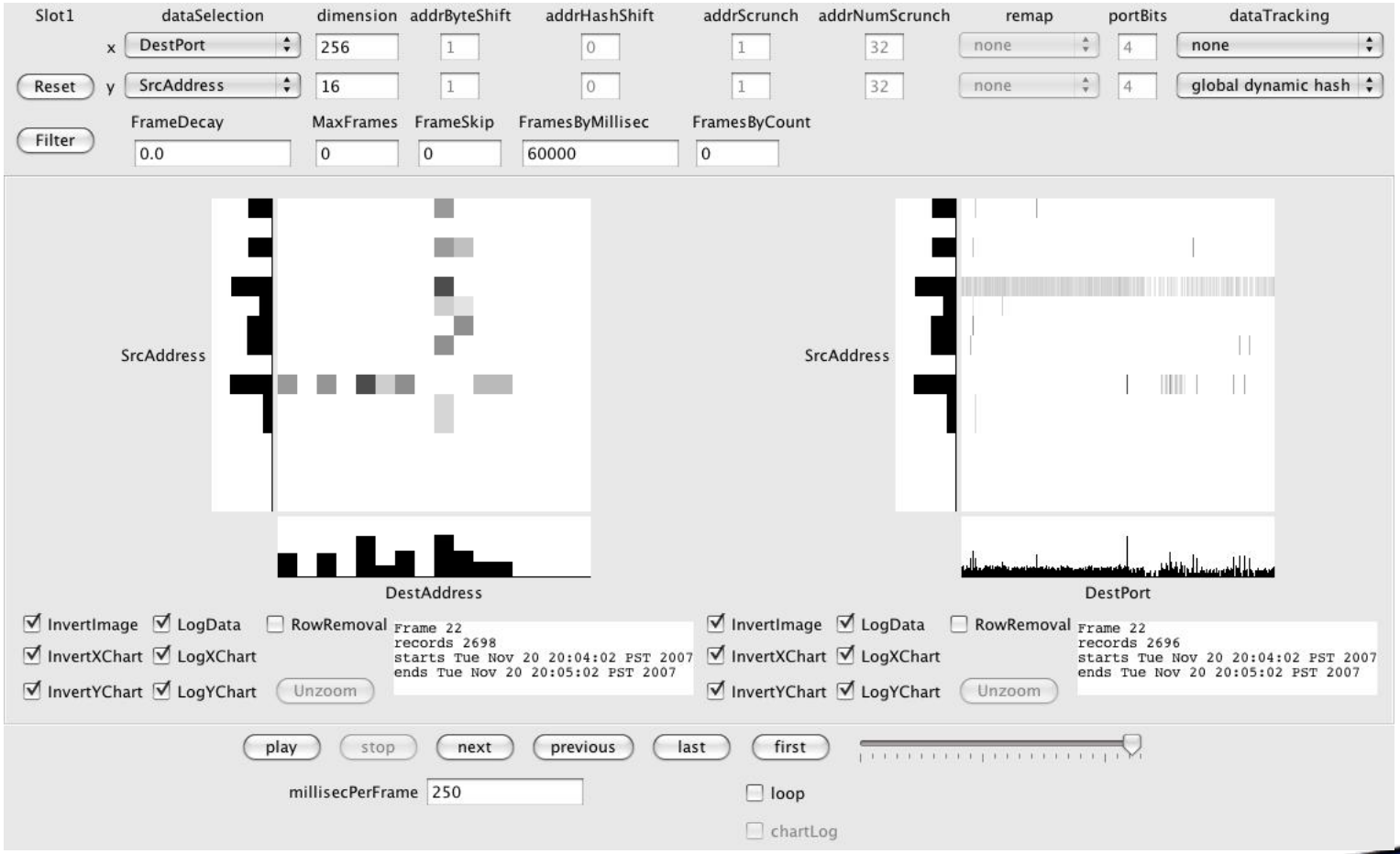
- IDS is a necessary complement to perimeter in PCS
- DATES is developing novel approaches beyond signature detection
- Industry partnerships ensure real world relevance

# Backup

# OPC Trace (Normal)



# OPC Trace (Port Scan)



# 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**