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

A security monitoring capability featuring multiple detection algorithms and cross-domain event correlation for defense against cyberattacks on energy control systems

*A cost-shared effort between industry and*

U.S. DEPARTMENT OF ENERGY | Cybersecurity, Energy Security, and Emergency Response

Cyber Security for Energy Delivery Systems

## DATES

**Project Lead:**
SRI International

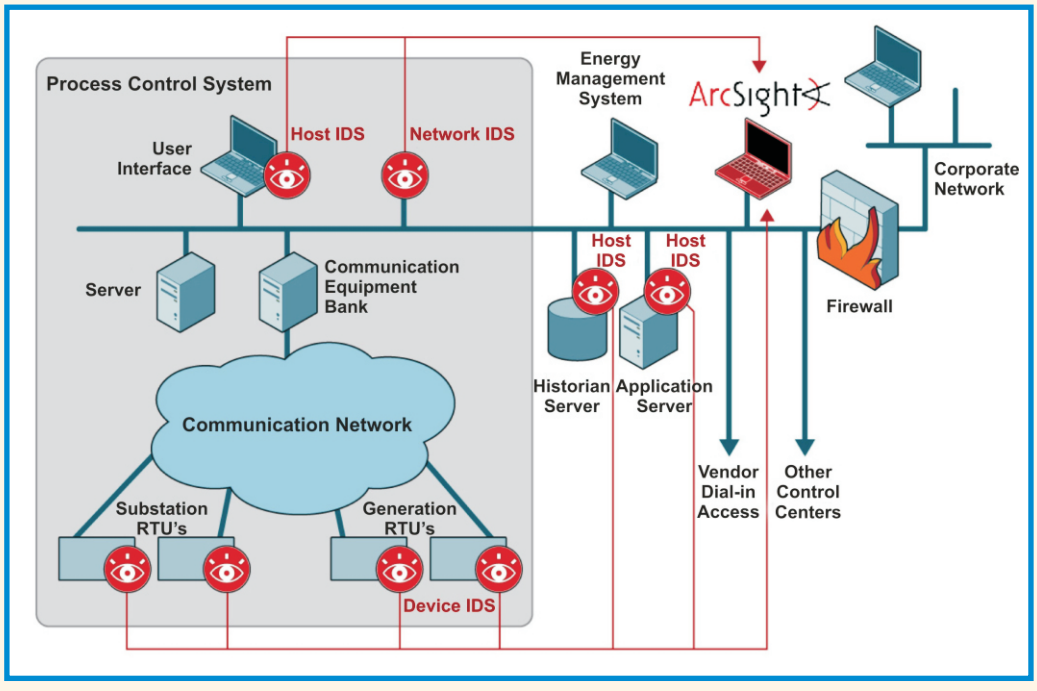
**Partners:**
ArcSight
Sandia National Laboratories
Invensys

## The Concept

DATES is a detection and security information/event management (SIEM) solution enabling asset owners to protect their energy control systems at the network, host, and device level from cyber attacks. DATES complements traditional, signature-based detection with multiple detection algorithms, including model-based and flow anomaly detection and cross-site attack correlation. The DATES detection and SIEM solution gives operators succinct and intuitive attack visualization, with attacks prioritized as to their impact on critical cyber assets and network zone crossing. This enhances an asset owner's situational awareness capability beyond simple event detection and log management.

The DATES monitoring platform uses multiple algorithms to examine packet headers, including a Snort sensor enhanced with a SCADA-aware rule set, stateful protocol analysis, and a Bayes component. Such a combination of model-based detection with anomaly detection leverages the unique traffic characteristics of energy control systems to detect zero-day attacks that violate these characteristics. The model-based capability lets the user configure the detection system for valid connection patterns. DATES will detect patterns violating the model-generated specification, such as attacks that alter the connectivity and traffic flows in the users' control systems. DATES also supports multiple monitoring interfaces, providing the security operator with an actionable view of potentially correlated and escalating attacks throughout different parts of the control system environment

## Diagram of the DATES Architecture



## The Approach

DATES was developed as an intrusion detection system—which alerts operators but does not perform intrusion prevention—because of the critical nature of energy control systems and the potential for attackers to harness automated responses to inflict denial of service attacks. As a detection system, DATES provides the security administrator with root cause information to allow a quick and adequate human reaction to detected events.

The project team developed the multi-algorithm detection capability, including the model-based and flow anomaly detection capability and SIEM correlation scripts. The correlation scripts comprehend asset criticality, network zones, and alert incident class, enabling correlation and prioritization of an attack that escalates and crosses to higher criticality zones. The scripts are currently specific to the ArcSight SIEM platform; however, they can be tailored for other SIEM solutions or event-consuming components. To test and validate DATES, the team developed testing environments both at SRI and Sandia, and conducted demonstrations of the visualization of critical and escalating attacks.

## Next Steps

In 2010, the project team will explore commercialization opportunities identified by ArcSight and engage utilities and interested system vendors to further apply and evaluate DATES.

For more information on the features, benefits, and application of DATES, visit www.csl.sri.com/projects/dates/.

## Benefits

- Enhances attack detection using protocol analysis and probabilistic (Bayes) detection capabilities
- Provides model-based and anomaly detection for identifying new, zero-day attacks
- Prioritizes and visualizes attacks, particularly attacks that escalate in criticality and/or cross control systems network zone boundaries
- Enhances situational awareness levels compared to simple event detection and log management
- Interfaces passively to the monitored network, minimizing interference to the critical functions of the control systems

**Cybersecurity for Energy Delivery Systems (CEDS)**

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

**For more information:** https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

**Initial Leads**

Carol Hawk
Program Manager

Alfonso Valdes
SRI International
650-859-4976
alfonso.valdes@sri.com

**Current Contact as of Aug. 2020**

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov