

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



An increasingly critical need

As Industrial Control Systems (ICS) rely more and more on digital technology and networking, they become increasingly vulnerable to cyber attack. The digital workstations used in control centers inherit many of the vulnerabilities of conventional IT systems, but lag in security best practices for a variety of reasons specific to ICS. Field devices are increasingly sophisticated, connected via TCP/IP networking technology and featuring real time operating systems and in some cases web-based configuration.

While displays in control centers provide extensive diagnostic and control capability of remote field assets from a process point of view, they may be effectively blind to

security issues in field networks. Moreover, the control center workstations may themselves be attacked, either from inadequately secured connections to business networks or via portable devices that enter the ICS environment.

Perimeter defense complemented by high-fidelity monitoring are essential components of a defense-in-depth strategy. Correctly configured switches and firewalls, along with careful network segmentation, can provide valuable perimeter defense for ICS, including DCS and SCADA. Even with a strong perimeter defense, security monitoring is required to make the system owner aware of attack attempts, penetration or circumvention of the defenses, and insider misuse. The DATES monitoring solution

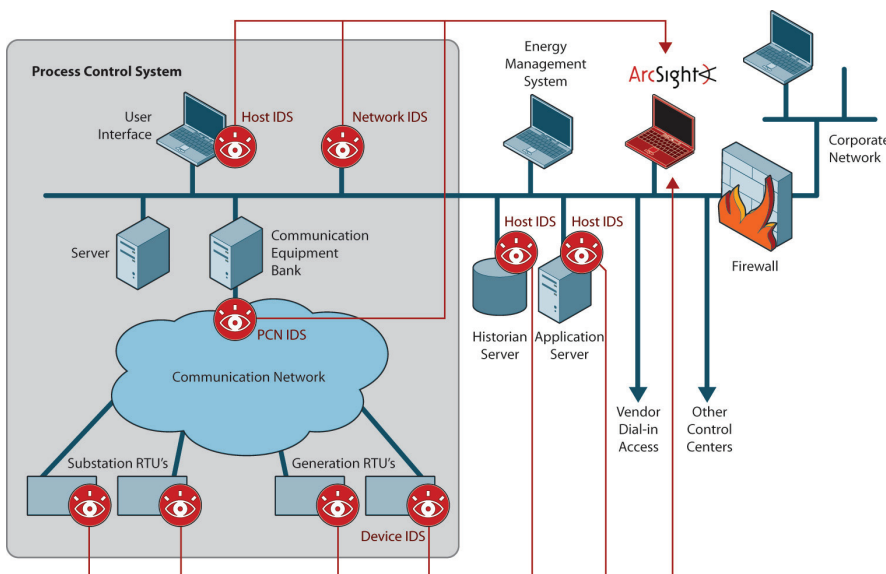
complements perimeter defenses and provides the ICS security operator a significantly improved level of situational awareness.

The DATES monitoring solution complements perimeter defenses and provides the ICS security operator with a significantly improved level of situational awareness.

Detection and analysis of threats to the energy sector (DATES)

DATES is a detection and security information/event management (SIEM) solution specifically tailored to protect ICS used in the energy sector. Features of the DATES monitoring platform include:

- Multiple detection algorithms, including an ICS-aware SNORT knowledge base, as well as SRI's components for stateful packet inspection, probabilistic/Bayesian analysis, and event threading.
- A unique model-based detection capability as well as pattern anomaly detection, which leverage the unique traffic characteristics



DATES architecture diagram



of ICS to enable detection of novel attacks such as zero-day exploits.

- DATES is currently well integrated with the advanced market-leading ArcSight SIEM Platform, and can easily be extended to communicate with other types of event-consuming components.
- A passive interface to the monitored network, using a mirror or span port to each monitored network segment. This makes the monitoring appliance invisible to conventional network scans, and guarantees that the critical function of the ICS is not affected at all.

DATES may be flexibly deployed in an ICS, with multiple instances of the detection component monitoring different network segments in the field as well as in the control center itself, communicating events to the SIEM console.

We also support a configuration of the detection component that has multiple monitoring interfaces, and is thus able to monitor multiple network segments simultaneously. This provides the security operator an actionable view of potentially correlated and escalating attacks on different parts of the ICS environment.

Benefits to the asset owner

Monitoring is a critical complementary defense to perimeter protection. DATES provides a security

view not otherwise available in ICS control room and field networks. The unique multi-algorithm capability in DATES identifies a variety of known attacks, and also has the highly valuable potential to detect previously unknown attacks known as zero-day exploits.

DATES is not in itself an Intrusion Prevention System (IPS), a function that must be approached with caution in ICS environments as attackers often can harness automated responses to inflict denial-of-service. Instead, DATES provides the security administrator with root cause information whenever possible to allow quick and adequate human reaction to incidents.

More information

DATES is developed under sponsorship from the United States Department of Energy, National SCADA Test Bed (DOE-NTSB). SRI's partners are Sandia National Laboratories, ArcSight, and Invensys Process Systems. We are interested in collaboration with asset owners in the energy sector for guidance, information exchange, or pilot deployment.

For more information, contact:

Alfonso Valdes
SRI International
alfonso.valdes@sri.com
650.859.4976

www.csl.sri.com/projects/dates/

About SRI International

Silicon Valley-based SRI International is one of the world's leading independent research and technology development organizations. SRI, which was founded by Stanford University as Stanford Research Institute in 1946 and became independent in 1970, has been meeting the strategic needs of clients and partners for more than 60 years. The nonprofit institute performs sponsored research and development for government agencies, businesses, and foundations. SRI also licenses its technologies, forms strategic alliances, and creates spin-off companies. In 2008, SRI's consolidated revenues, including its wholly owned for-profit subsidiary, Sarnoff Corporation, were approximately \$490 million.

Menlo Park Headquarters

SRI International

333 Ravenswood Avenue
Menlo Park, CA 94025-3493
650.859.2000

Washington, D.C.

SRI International

1100 Wilson Blvd., Suite 2800
Arlington, VA 22209-3915
703.524.2053

Additional U.S. and international locations

www.sri.com

SRI International is a registered trademark. All other trademarks are the property of their respective owners.

Copyright 2009 SRI International. All rights reserved. 9/09