Addressing Cyber-Threats to Industrial Control Systems

Industrial Control Systems Require Special Protection from Cyber-Attacks

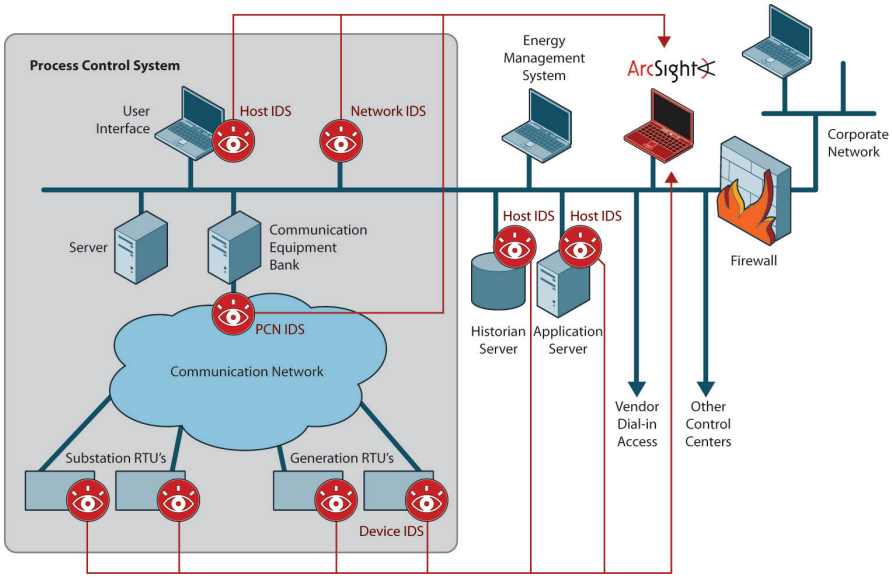
Industrial control systems (ICS) keep production and delivery systems in the manufacturing, energy, and water sectors running smoothly. However, security systems designed to protect corporate IT systems do not address the special needs of protecting ICS.

As ICS incorporate digital technology, adopt standard protocols and platforms, connect with conventional information technology (IT) systems and the Internet, and rely more on wireless networks, they are more vulnerable to cyber-threats.

SRI is Developing Cyber-Threat Solutions

SRI's Infrastructure Security program researches, develops, and supports activities to improve the security of infrastructures, including energy, financial systems, telecommunications, and the Internet. Recent energy projects include:

- *Bio-Inspired Technologies for Enhancing Cyber Security in the Energy Sector*
- *National Electric Sector Cybersecurity Organization Resource (NESCOR)*
- *Detection and Analysis of Threats to the Energy Sector (DATES)*
- *Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC)**



DATES architecture diagram

SRI works with organizations addressing cybersecurity concerns. For example, we

- *Provide technical, managerial, and administrative support for the Department of Homeland Security's Cyber Security Research and Development Center**
- *Are a member of the Industrial Control Systems Control Security Joint Working Group**
- *Contribute to cybersecurity roadmaps, including* Roadmap to Achieve Energy Delivery Systems Cybersecurity *(Energy Sector Control Systems Working Group);* Cross-Sector Roadmap for Cybersecurity of Control Systems *(Industrial Control Systems Joint Working Group), and* A Roadmap for Cybersecurity Research *(U.S. Department of Homeland Security)**
- *Host the Malware Threat Center and develop tools such as BotHunter® to detect malware*

Working with SRI

SRI conducts client-sponsored research and development for government agencies, businesses, foundations, and other organizations. SRI also brings its innovations to the marketplace by licensing its intellectual property and creating new ventures.

* SRI's participation funded by the U.S. Department of Homeland Security, Science and Technology Directorate.

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

SRI teamed with Sandia National Laboratories, ArcSight, and Invensys Process Systems to develop a breakthrough integrated capability in detection, security event monitoring, and large-scale threat analysis to defend against cyber-attacks against digital control systems in the energy sector. Features of the detection and security information/event management (SIEM) solution include:

- *Multiple detection algorithms, including an ICS-aware SNORT knowledge base and SRI's components for stateful packet inspection, probabilistic/ Bayesian analysis, and event threading*
- *A unique model-based detection capability and pattern anomaly detection to leverage the unique traffic characteristics of ICS and enable detection of novel attacks such as zero-day exploits*
- *Integration with the ArcSight SIEM Platform—and capable of integration with other types of event-consuming components*

The DATES solution can be flexibly deployed in an ICS, with multiple instances of the detection component monitoring different network segments in the field and in the control center itself, to communicate events to the SIEM console.

SRI can support a configuration of the detection component with multiple monitoring interfaces for simultaneous monitoring of multiple network segments. This provides an actionable view of potentially correlated and escalating attacks on different parts of the ICS environment.

Monitoring is a critical complementary defense to perimeter protection. DATES provides a security view not otherwise available in ICS control room and field networks. Its unique multi-algorithm capability identifies a variety of known attacks. DATES also has the highly valuable potential to detect previously unknown attacks, known as zero-day exploits.

SRI seeks industry partners for collaboration to extend and deploy detection and SIEM capabilities developed under DATES.

Contact Us

Barbara Heydorn
Director, Center of Excellence in Energy
barbara.heydorn@sri.com

Ulf Lindqvist
Program Director, Infrastructure Security
ulf.lindqvist@sri.com
650.859.2351

About SRI International

Silicon Valley-based SRI International, a nonprofit research and development organization, performs sponsored R&D for governments, businesses, and foundations. SRI brings its innovations to the marketplace through technology licensing, new products, and spin-off ventures. SRI is known for world-changing innovations in computing, health and pharmaceuticals, chemistry and materials, sensing, energy, education, national defense, and more.

Headquarters
SRI International
333 Ravenswood Avenue
Menlo Park, California 94025-3493
650.859.2000

Additional U.S. and international locations
www.sri.com

Stay Connected

facebook.com/sri.intl
twitter.com/SRI_Intl
youtube.com/user/innovationSRI
linkedin.com/company/sri-international
http://goo.gl/rv3iX

The DATES project was supported by the United States Department of Energy under Award Number DE-FC26-07NT43314. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.