

ESTEP Sponsors Effort to Protect Critical Data Infrastructures

Framework Underway to Secure Supervisory Control & Data Acquisition Networks

MANY EXPERTS HAVE become increasingly concerned about the potential for cyber attacks to negatively impact and possibly disable our nation's critical infrastructures, including the power grid. A new project, sponsored by the Energy Systems Technology and Evaluation Program (ESTEP), is working towards a solution.

Sponsored by the Office of Naval Research, the ESTEP program focuses on energy technologies that reduce costs, increase energy security, and ultimately increase the reach and persistence of the warfighter.

Securing SCADA Networks

A Supervisory Control and Data Acquisition (SCADA) network allows digital input from computing components, which might be thousands of miles away, to control physical assets (like motors, actuators, and pumps). While this allows for efficient management of infrastructure systems, there is a threat inherent in the unprotected nature, interconnected paradigm, and global footprint of SCADA networks. Because these networks could be extremely

vulnerable to security threats and cyber attacks, there are a number of technologies being developed to improve SCADA security. The Cyber-SCADA Evaluation Capability (C-SEC) project was formed to evaluate these technologies and develop a framework with which others can do the same.



The most well-known example of a cyber threat to date happened in Iran in 2010. A virus known as Stuxnet disrupted centrifuges at a uranium enrichment plant, and subsequently infected other computers in the country. A handful of malicious files—the world's first digital weapon—was able to operate for close to a year before being discovered, and has subsequently spread to many other parts of the world. Because the malware was signed by a digital

certificate to make it appear as though it had come from a reliable company, it rendered automated-detection software useless. Sophisticated malware such as this prompted the research and development of anti-viral solutions.

The C-SEC project was formed to evaluate technologies for securing SCADA networks as they relate to energy systems and to integrate the best of these technologies into a new capability.

The main challenge facing the C-SEC team, headed by Jose Romero-Mariona of the Space and Naval Warfare Systems Center Pacific (SSC Pacific), is the fact that they are dealing with two opposing requirements—the necessity for SCADA networks to stay up all the time, and the security to ensure that there is no abnormal/malicious activity on them. Currently, there is no sure way to conduct an initial security scan of SCADA networks without the real possibility of system shut-down as a result of such scanning. This severely limits what we know today of our SCADA networks and what is in them.

The Cyber-SCADA Evaluation Capability project was formed to evaluate SCADA network security technologies and develop a framework with which others can do the same.

As the team began to evaluate SCADA security technologies, it became clear that they would need a laboratory environment where a sample baseline SCADA network (with real SCADA equipment and related hardware) could be utilized to explore current SCADA vulnerabilities. In this laboratory environment, the team tested various security technologies and assigned a numeric

score to each. The highest scoring technologies were incorporated into the C-SEC software tool to provide interested users with relevant information and results regarding security technologies available.

This software tool, which is now being perfected, allows for the streamlined evaluation of SCADA security technologies, including secu-

rity metrics, which can provide a detailed picture of how well current security technologies secure SCADA networks and their components. The software will identify any system shortcomings and provide recommendations on how to best secure it. This tool was developed using open-source software to enable wide use and reuse of the technology.

The Basics About the Energy Systems Technology & Evaluation Program

ESTEP FOCUSES ON energy technologies that reduce costs, increase energy security, and ultimately increase the reach and persistence of the warfighter. ESTEP seeks to identify viable emerging energy technologies, obtained for the most part from open-market sources and in-house government demonstrations. Technologies identified as promising by ESTEP will be demonstrated, and data will be collected to evaluate the performance and reliability of selected technologies under various environmental and operating conditions.

The entire program encompasses the following investment areas:

- Cyber and Energy Management for Information Systems
- Power and Energy Components
- Power and Energy Production/Efficiency

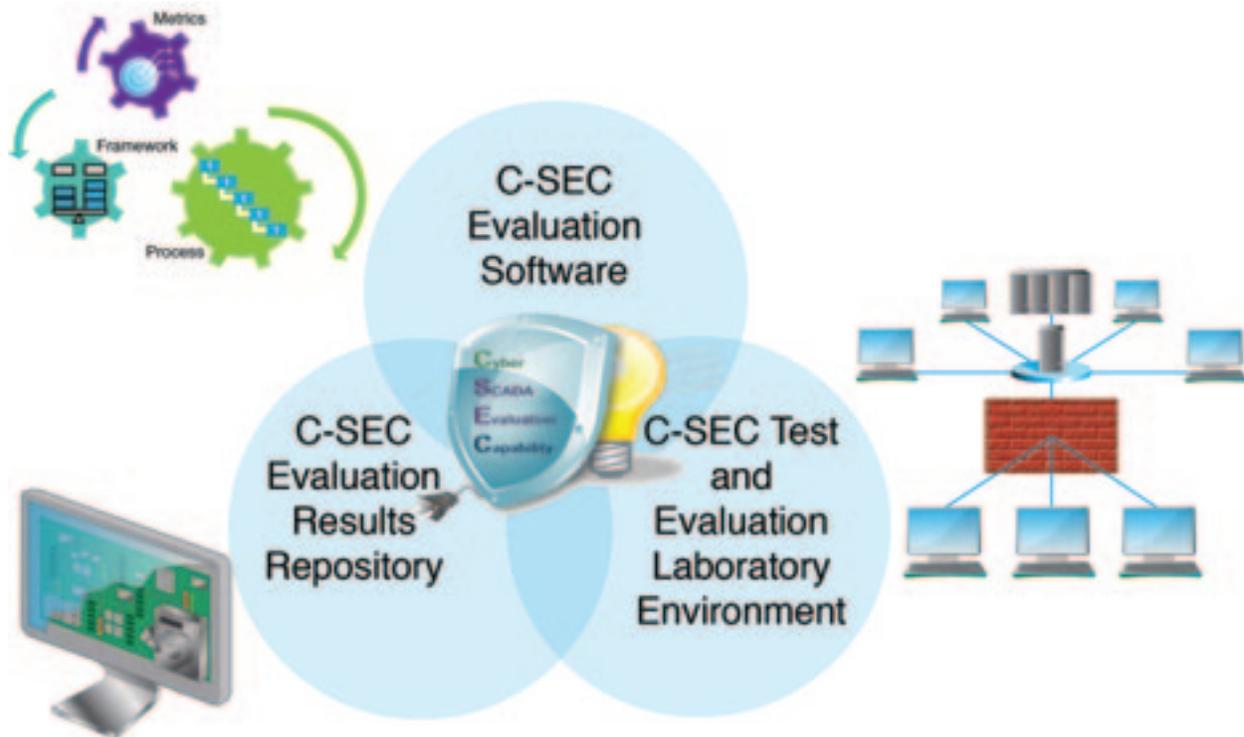


Established in fiscal year 2013, ESTEP casts a wide net across the Department of the Navy, academia, and private industry to investigate and test emerging energy technologies at Navy and Marine Corps installations. At present, ESTEP conducts nearly two dozen in-house government energy projects, ranging from energy management to alternative energy and storage technologies. Additionally, an ESTEP Broad Agency Announcement has awarded several contracts to industry in those same energy areas.

In addition to testing and evaluating performance and reliability of energy technologies, the ESTEP program provides mentoring (via on-the-job training and education of interns) and other workforce development opportunities by partnering with the Troops-to-Engineers program for veterans at San Diego State University and other universities. Workforce and professional development are key components of ESTEP and integral to the success of executing and transitioning energy technology projects at naval facilities.

ONR provides funding and oversight for ESTEP, and program management is being handled by SSC Pacific. The Naval Facilities Engineering and Expeditionary Warfare Center and the Naval Postgraduate School are executing selected research projects, and every project plans to involve at least one veteran intern utilizing an ESTEP grant to academic institutions.

For more information about ESTEP, contact Stacey Curtis at 619-553-5255 and stacey.curtis@navy.mil.



Another crucial part of this work involves the creation of a results database (or repository) where C-SEC evaluations can be shared among organizations within the Department of Defense. This sharing of results will provide information to bases and organizations that have similar systems, and will help standardize the way that these technologies are being evaluated. Information on costs and training technologies will also be included in this repository.

The team is currently building an app and lightweight environment, called “C-SEC On The Move,” to enable mobile devices such as smartphones and tablets to

leverage the C-SEC software and repository. This will enable any trained individual to utilize a light version of C-SEC software on the spot at any base or installation, thereby facilitating informed decision making.

The team is also conducting pilot training sessions to determine how best to deliver training on C-SEC and C-SEC On The Move. One session is tailored toward government scientists, and one is geared toward the warfighter. The warfighter training sessions are leveraging the Troops-to-Engineers program at San Diego State University.

Looking Ahead

Together, the C-SEC software and results repository will establish requirements and metrics for securing SCADA networks, which will benefit current and future security posture and will further integrate security considerations. C-SEC will also eliminate duplication of efforts in researching security technologies, thereby maximizing limited budgets, and increasing return on investment estimations.

Using C-SEC On The Move will enable the warfighter to select appropriate security technologies and conduct routine security scans bi-weekly or monthly, thereby achieving a level of cyber security not previously achievable. [↕](#)



An electric power dispatcher foreman operates the SCADA system at Commander Fleet Activities, Yokosuka, Japan. C-SEC software will enable such users to enhance the security of their SCADA systems.

Joe Schmitt

Jose Romero-Mariona
Space and Naval Warfare Systems Center Pacific
619-553-8119
DSN: 553-8119
jose.romeromariona@navy.mil