

# ENERGY ASSURANCE TECHNOLOGIES

## Project Fact Sheet

### CYBER SECURITY TRAINING AND AWARENESS FOR REAL TIME COMMUNICATION AND CONTROL (RTCC) SYSTEMS

#### BENEFITS

- More secure energy infrastructure operations
- Improved RTCC system security
- Improved RTCC design
- Greater understanding of RTCC vulnerabilities
- Better security information sharing with industry

#### APPLICATIONS

Today, there are over one thousand SCADA systems in operation in electric utilities and numerous vendors of SCADA and RTCC products. These systems currently include very little inherent security. Knowledge of system vulnerabilities and an understanding of how to better secure these systems will provide industry with guidance to develop more secure RTCC systems and security products.

This project supports DOE's Energy Infrastructure Training and Analysis Center (EITAC) which will be a facility where stakeholders can simulate and deal with upsets to the energy infrastructure grids.

#### PROVIDING ENERGY INFRASTRUCTURE STAKEHOLDERS WITH TOOLS TO HELP THEM SECURE CRITICAL RTCC SYSTEMS FROM CYBER ATTACK

This project will provide first responders, energy sector owners and operators, and academics with a better understanding of vulnerabilities, consequences, and best practices for RTCC cyber security. It will also assist energy sector standards bodies with efforts to incorporate security into the design of RTCC systems.

The consequences of an energy infrastructure disruption can be disastrous. Short, localized outages disrupt businesses, stress law enforcement, and can endanger lives. Larger scale blackouts – for any length of time – could impact everything from Wall Street markets to essential government services. Critical energy infrastructures – such as electric power, oil and gas production and distribution – rely on highly computerized and networked Real-Time Communication and Control (RTCC) Systems. These RTCC systems include Supervisory Control and Data Acquisition Systems (SCADA), Energy Management Systems (EMS) and other process control systems. RTCC systems, designed to handle automatically most problems arising from customary natural disasters such as weather overloads, must be protected from malicious cyber attacks. However, very little information is currently available to assist the energy sector in securing these systems.

#### Quality Up-to-Date Training



It is essential to provide stakeholders of the energy infrastructure with quality, up-to-date training



## Project Description

This project is divided into two main tasks. The first task focuses on developing education/training/awareness tools for the energy sector. This includes the development of training material that incorporates vulnerability demonstrations, case studies, and self-assessment methods for industry. The second task focuses on development of best practice guidelines for RTCC cyber security, and development of more secure RTCC systems through participation in key standards bodies.

## Progress and Milestones

- Vulnerability assessment course (1Q/04)
- Security design course (3Q/04)
- Cryptography course (3Q/04)
- Common vulnerabilities document (4Q/03)
- Common information frameworks document (1Q/04)
- Security best practice documents (2Q/04)
- Laboratory-based vulnerability demonstrations (3Q/04)
- Security advisement to key standards bodies:
  - American Gas Association (AGA) (1Q/04)
  - International Electromechanical Commission (IEC) (3Q/04)
  - Institute of Electrical and Electronics Engineers (IEEE) (2Q/04)
  - American Petroleum Institute (API) (2Q/04)

### PROJECT PARTNERS

Sandia National Laboratories  
Albuquerque, NM

National Energy Technology Laboratory  
Morgantown, WV

West Virginia University  
Morgantown, WV

### FOR PROJECT INFORMATION, CONTACT:

Juan J. Torres  
SCADA Security Program  
Manager  
Advanced Information and Control Systems  
Department  
Sandia National Laboratories  
P.O. Box 5800; MS 1351  
Albuquerque, NM 87185-1351  
Phone/Fax: (505) 844-0809 / 284-5104  
Email: [jjtorre@sandia.gov](mailto:jjtorre@sandia.gov)  
[www.sandia.gov/scada](http://www.sandia.gov/scada)

or

Donald Geiling  
Project Manager  
U.S. Department of Energy  
National Energy Technology Laboratory  
3610 Collins Ferry Road  
Morgantown, WV 26507-0880  
Phone: 304-285-4784  
Email: [dgeili@netl.doe.gov](mailto:dgeili@netl.doe.gov)

### FOR PROGRAM INFORMATION, CONTACT:

David Salem  
Technology Manager  
U.S. Department of Energy  
Office of Energy Assurance  
1000 Independence Ave, SW  
Washington, DC 20585  
Phone: 202-586-8710  
Email: [David.Salem@hq.doe.gov](mailto:David.Salem@hq.doe.gov)

or

Albert B. Yost II  
Business Area Coordinator  
U.S. Department of Energy  
National Energy Technology Laboratory  
3610 Collins Ferry Road  
Morgantown, WV 26507-0880  
Phone: 304-285-4479  
Email: [ayost@netl.doe.gov](mailto:ayost@netl.doe.gov)

### FOR ADDITIONAL INFORMATION:

Visit our home page at  
[www.ea.doe.gov](http://www.ea.doe.gov)

Office of Energy Assurance  
U.S. Department of Energy  
Washington, D.C. 20585

February 2004