ENERGY ASSURANCE TECHNOLOGIES

Project Fact Sheet

Critical Infrastructure Test Range

Benefits

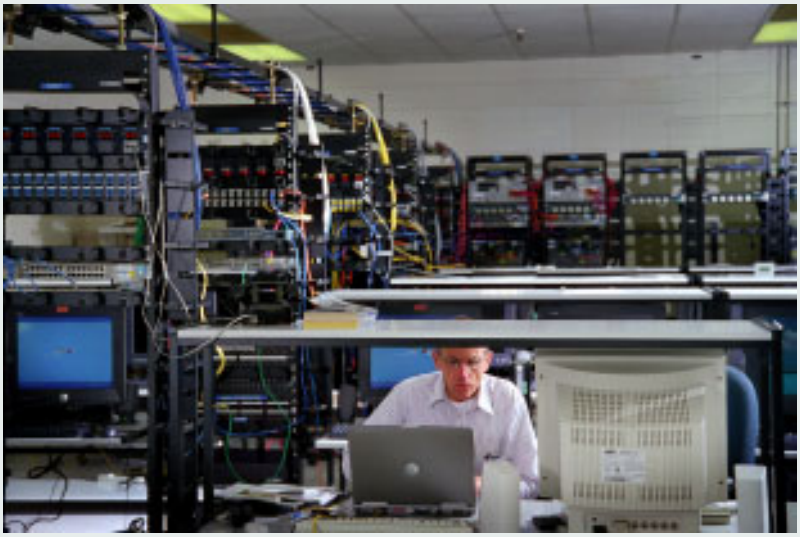
- Helps identify vulnerabilities in critical energy infrastructure
- Provides "quick fixes" as well as improved designs for more secure and robust systems and components
- Leads to developing and implementing protective measures
- Leads to development of better systems standards and certification
- Used for vulnerability awareness education for industry and other stakeholders

Applications

The Test Range is used to independently identify energy assurance system and component vulnerabilities, assess these vulnerabilities and then develop, verify and validate solutions. PCS vendors and end-users can then use these solutions for their systems. We can then apply the knowledge gained to the development of national and commercial standards and certification procedures for energy assurance-related systems and components. This will ensure that new systems and components integrated into the existing infrastructures do not introduce new vulnerabilities.

Helping protect the nation's energy infrastructure by providing component and system-level testing

The Idaho National Engineering and Environmental Laboratory (INEEL) Critical Infrastructure Test Range consists of specialized and integrated test beds and test control centers. The test range is located on the 890-square-mile U.S. Department of Energy reservation, located in southeastern Idaho. The INEEL Critical Infrastructure Test Range includes capabilities to test a variety of process control systems (PCS) – including those using supervisory control and data acquisition (SCADA[1]), distributed control systems (DCS) and programmable logic controllers (PLC) – cyber security, communications and electrical power grid in an integrated manner and at full scale. Oil and gas delivery systems can be tested in cooperation with DOE's Rocky Mountain Oilfield Testing Center (RMOTC).



An engineer monitors one of many ongoing tests at the Cyber Security/SCADA Test bed. These Test beds are two elements of the INEEL Critical Infrastructure Test Range, which provides system-level testing capability to test the nation's critical infrastructure systems and protective measures at near full scale.

[1] Supports the National SCADA Test Bed Program, jointly run by INEEL and Sandia National Laboratory

Project Description

The Test Range provides a component and system-level testing capability to test the nation's critical infrastructure systems and protective measures at near full scale. This approach will allow our nation to fix the vulnerabilities facing us today, use that information to develop defensive procedures for today's infrastructures, and develop tomorrow's smart infrastructures that will be much more attack resistant by design and construction.

The CI Test Range consists of specialized critical infrastructure test beds and test control centers. These individual test beds can also be integrated to test interdependencies. The principal programmatic components are as follows:

- SCADA
- Cyber Security
- Communications
- Power Grid
- Physical Security

Progress and Milestones

- Established two industry agreements established with SCADA manufacturers. (1Q/04)
- Installed one commercial SCADA system for testing. (1Q/04)
- Commercial SCADA system testing. (3Q/04)
- Install new Land Mobile Radio (LMR) components to support emergency responder communications. (3Q/04)
- International SCADA Conference. (4Q/04)
- Facility modifications to expand SCADA and Cyber Test Beds capabilities. (3Q/04)

Economics and Commercial Potential

A disruption in the energy infrastructure can impact the security of the nation and well being of our citizens. As a result of the August 14, 2003 power outage in the northeast United States and Canada, 50 million people were impacted and an estimated $4.5-$12B in economic activity was lost. Improvements in the robustness of the energy infrastructure can substantially mitigate such losses.

The Government, private sector (e.g., energy utilities) and general public are demanding a more robust and secure energy infrastructure. Such demands will, by necessity, provide significant commercial opportunities.

Project Partners

Bechtel Telecommunications

AT&T Wireless

Siemens

ABB Inc. – Network Management

U.S. Department of Energy

U.S. Department of Homeland Security

U.S. Department of Defense

Interested in joining the partnership, being informed of outcomes, or being a demonstration site? Contact:

Alan Snyder
Program Manager
Idaho National Engineering and
Environmental Laboratory
P.O. Box 1625
Idaho Falls, ID 83415-3840
Phone: 208-526-1725
Email: amq@inel.gov

or

Jacqueline Gernant
Project Manager
Idaho Operations Office
Idaho Falls, ID 83415-3840
Phone: 208-526-1742
Email: gernanja@id.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

For Additional Information:

Visit our home page at
www.ea.doe.gov

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

March 2004