

ENERGY ASSURANCE TECHNOLOGIES

Project Fact Sheet

RISK ASSESSMENT METHODOLOGIES FOR ENERGY INFRASTRUCTURES

BENEFITS

- Provide a systematic, risk-based approach for evaluating and improving the security of energy infrastructure networks
- Applicable to electric power transmission lines and energy pipelines and their associated critical elements and facilities
- Provide security analyses based on specific system-level vulnerabilities, threats, and consequences of an attack
- Enable identification of critical system nodes and facilities and security risks
- Provide system owners and operators with cost-benefit analyses of possible security upgrades

APPLICATIONS

The proposed work will support energy infrastructure security and protection efforts by providing a systematic performance-based risk assessment approach that will enable energy customers to assess system-level risks and identify consequence mitigation strategies. This will provide customers and utilities with the ability to compare options for improvements in energy system security and reliability, including interdependencies, relative to their associated costs.

METHODS AND TOOLS TO IDENTIFY, EVALUATE, AND HELP REDUCE SYSTEM VULNERABILITIES

The security and protection of our energy infrastructure is extremely important to our nation's economy and social well-being. A major disruption to our energy infrastructure could significantly impact many segments of the population through impacts on basic human services, transportation, telecommunications, emergency services, banking, or manufacturing. Recently, intentional malevolent attacks, have become a realistic possibility that must now be considered. If carried out successfully, an attack could compromise the integrity and function of a facility or infrastructure, causing serious injuries or fatalities or leading to cascading outages and damage to other facilities or infrastructures, ultimately causing serious economic impacts. Malevolent attacks can be physical or cyber-based, coordinated and planned by either outside groups or insiders, and can include multiple, coordinated attacks against critical or important facilities. These low-probability, high-consequence events require performance-based approaches to insure facility or system security and protection. This is especially true for systems, like the U.S. energy infrastructure, that have critical elements that are highly distributed and widely dispersed.

The techniques developed to address intentional malevolent attacks and other high consequence events are often risk-based. This approach compares relative risks of an attack on the system based on the severity of the potential consequences of a given attack, the probability of the attack, the security effectiveness of the facility to the attack, and the ability to recover from the attack. These approaches have been developed and utilized in the electric power and natural gas transmission pipeline infrastructures, but have focused at the plant or company level.

Project Description

The focus of this project is to provide two major elements of the energy infrastructure – electric power generation/transmission systems and natural gas transmission pipeline systems – with improved performance-based methods and tools to identify, evaluate, and help reduce system vulnerabilities to a wide range of potential malevolent events or attacks. While there are differences between these two energy infrastructure sectors, they have many similarities including being highly dispersed systems with key facilities that are widely scattered, making them difficult to protect using only traditional physical security techniques. Additionally, these two sectors have become increasingly dependent on each other. For example, many electric utilities and independent power producers utilize natural gas for electric power generation and therefore interruption of the natural gas supply could significantly impact electricity generation. In other cases, natural gas transmission pipelines utilize electric powered compressors to supply natural gas to consumers and an interruption in electric power could impact natural gas supply.



This project integrates three energy infrastructure vulnerability and risk assessment methods developed at Sandia – one for electric power transmission, one for petrochemical facilities, and one for critical asset identification in dispersed networks – into one tool for analyzing these important elements of the energy infrastructure. This approach will provide customers and utilities with a comprehensive, cost-effective, performance-based approach to assess the vulnerabilities of these energy services. This integrated risk assessment approach will enable customers and utilities to 1) identify system-level critical nodes and facilities based on various event scenarios, 2) identify and compare the risks and consequences of these events, and 3) identify cost-effective approaches to mitigate these risks and consequences and improve system security and reliability. The integrated risk assessment approach will be demonstrated and validated in cooperation with energy industry partners to pilot test the developed tools in the second year of this project. After validation, the approach will be developed into an education and training program that will be provided to industry and regulatory agencies through a train-the-trainer program developed in cooperation with industry.

Progress and Milestones

This project includes the following milestones:

- Upgrade existing risk-based vulnerability assessment methods for the electric transmission and petrochemical industries (3Q/04)
- Integrate the risk assessment methods with critical system node evaluation tool (4Q/04)
- Assess one or two energy networks in cooperation with industry participants using the developed tools to evaluate ease of use and completeness (2Q/05)
- Coordinate training program and methodology commercialization (4Q/05)

Economic and Commercial Potential

The economic consequences of a major security breach at a refinery or attack on an electric power line can be significant. It can lead to a shutdown of the energy network resulting in a loss of its economic value for extended periods, with cascading impacts throughout the economy of the region and the nation. Use of the developed risk assessment approach can help reduce vulnerabilities of energy systems and help minimize the consequences of security breaches or malevolent attacks.

In addition, the use of these techniques can help identify the critical elements of an energy network and focus protection efforts and upgrades on those facilities or elements. This enables energy system owners and operators with the ability to identify the most cost-effective methods to improve overall system security and reliability.

PROJECT PARTNERS

Sandia National Laboratory

Gas Technology Institute

American Gas Association

Interstate Natural Gas Association
of America

Bonneville Power Authority

Tennessee Valley Authority

**INTERESTED IN JOINING THE PARTNERSHIP, BEING
INFORMED OF OUTCOMES, OR BEING A
DEMONSTRATION SITE? CONTACT:**

Mike Hightower
Sandia National Laboratories
P.O. Box 5800, MS0710
Albuquerque, NM 87185
Phone: 505-844-5499
Email: mmhight@sandia.gov

or

Swenam Lee
U.S. Department of Energy
National Energy Technology Laboratory
626 Cochran Mill Road
Pittsburgh, PA 15236-0940
Phone: 412-386-4664
Email: swenam.lee@netl.doe.gov

FOR PROGRAM INFORMATION, CONTACT:

Mr. James McGlone
Program Manager
U.S. Department of Energy
Office of Energy Assurance
1000 Independence Ave, SW
Washington, DC 20585
Phone: 202-586-8710
Email: James.McGlone@hq.doe.gov

or

Mr. 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

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

February 2004