INEEL NATIONAL SECURITY

Increasing Capabilities and Security for Automation

SCADA Test Bed

Mitigate impacts to critical infrastructure, and aggressively recover from attacks involving cyber or physical threats.

Idaho National Engineering and Environmental Laboratory

INEEL

Home of Science and Engineering Solutions

Vulnerability

The risks to U.S. energy infrastructures from cyber attacks are real. One vulnerability is the communication and control systems used for planning, operation, and maintenance of infrastructure grids. These systems include Supervisory Control and Data Acquisition (SCADA) systems, many of which are designed and built by foreign-owned companies. The high cost of SCADA systems discourages backup inventories. It could take several months to replace the loss of a large SCADA system.

Risks exist and action guidelines are required to prepare for attack and to mitigate any impacts on our grids. U.S. industry does not have national guidance on improving the robustness of the systems. Further, the new trend is away from older hierarchical SCADA systems to the use of open standard operations systems and distributed network-based control systems. The nation needs to address the issues associated with these new systems.

Increasing Security

INEEL – in partnership with Sandia National Laboratories – is establishing a comprehensive program called the National SCADA Test Bed that combines efforts in security administration and governance, standards, industry alliances, education and awareness, modeling, vulnerability assessments of U.S. utilities,

and research and development. The SCADA Test Bed will also align with Homeland Security activities in physical security, certification and system reliability of the energy infrastructure.

The earliest tasks will focus on vulnerability assessments of SCADA systems and performing demonstrations of vulnerable systems to raise the awareness of equipment suppliers and utilities. The early tasks will also concentrate on providing near-term solutions to the identified vulnerabilities. Long-term solutions requiring new technologies and methods will be provided in the later phases of the program.

The SCADA Test Bed is an integral component of the Critical Infrastructure Test Range.

The INEEL Critical Infrastructure Test Range provides field-scale testing for numerous federal agencies and is available for commercial customers as well. The 890-square-mile INEEL site is a high-tech model of much of our nation's critical infrastructure. This laboratory site – almost 75 percent the size of Rhode Island – has historically been a state-of-the-art test site. From its beginnings as a test bed for commercial and Naval reactors to newer test bed missions of establishing the safety basis for commercial nuclear power and waste treatment technologies, the INEEL is unique in its existing critical infrastructure and its engineering approach to testing complex systems. Test networks may be used to simulate transportation nodes or support special operations. The INEEL also has computer networks, cyber security and intrusion detection labs, as well as high performance and cluster computing labs that complement National Infrastructure Simulation and Analysis Center (NISAC) simulations supporting SCADA field tests. INEEL systems are field-size in scale, applicable to traditional grid systems, and can test interdependencies efficiently.

SCADA Test Bed

INEEL has established an initial SCADA Test Bed capability that combines deployed field-scale SCADA components with traditional INEEL strengths of integrated system design, testing and demonstration. INEEL has extensive experience in the design, development, integration, systemization, testing and demonstration of SCADA systems within its 890-square-mile site. The multitude of SCADA systems in real-time use at the INEEL includes the top two classic systems:

- The Electrical Power Transmission and Distribution System SCADA – includes PC workstations with a real-time control operating system and a fiber optic wide area network (WAN), enabling remote control and monitoring of all of the Laboratory's T&D loop substations and eliminating the need to staff each substation. Each substation has a programmable logic controller performing distributed monitoring and control. The software, both at the PLC and workstation level, was developed at the INEEL and is representative of the SCADA systems in older, established installations of commercial utilities that constitute much of the existing grid.
- The Utility Control System is a SCADA controlling the Idaho Nuclear Technology and Engineering Center's electrical distribution system. It provides control and monitoring of the EDS at INTEC during all power states and transitions. The UCS monitors and controls devices from the 138 kV substation level to the load center feeder breaker level. It automates many reconfigurations and includes multiple protections that provide testing flexibility.

For more information:

Ken Watts
(208)526-9628
kdw@inel.gov

Gary Seifert
(208) 526-9522
sei@inel.gov