

Idaho Super Computing Center (ISC)

The INEEL has a long history of doing test range activities. In the 1940s, the site began as a naval gunnery range and was designated a national reactor testing station. In 1974, we became the INEL and continued with nuclear materials research testing, adding an armor-manufacturing component in 1984. Our name changed again in 1997 to include an environmental component, and last year we were designated as the leading center in nuclear energy R&D for the Department of Energy. National Security Programs are building on this 60-year history. After September 11th, the INEEL realized that the site's expertise, combined with its infrastructure and 890 square miles of remote land, could be invaluable in helping the nation learn how to protect its most critical infrastructure. The INEEL External Review Board, Chaired by Vic Reis, independently came to the same conclusion. So, the Critical Infrastructure Protection Test Range concept was born. We refer to it as the CI Test Range.

Two of the major components of the CI Test Range that are located here at the ISC are the SCADA and Cyber Security Test Beds. The CI Test Range has received funding of approximately \$4M to date from the Department of Energy, Office of Energy Assurance. Other components of the CI Test Range reside at the INEEL site and include a Wireless Communications Test Bed, and a Physical Security Test Bed. Future plans include a Transportation Test Bed, a remote command and control center, and various other facilities that will be used for training and testing. Information about some of these programs has been posted on the website.

The first test bed that we want to talk about today is the **Supervisory Control and Data Acquisition or SCADA Test Bed**. It should be noted that SCADA systems are the nerve center, or "brains" if you will, of several different facets of critical infrastructure around the world including electric, gas and oil distribution systems, water and sewer systems, and numerous types of manufacturing plants.

Our current plans include spending ~\$2.5M on this part of the Test Range in FY04

- We plan to develop an "integrated" SCADA Test Bed – with links to cyber, wireless/communications and physical INEEL assets.
- We plan to test legacy and contemporary SCADA systems. In order to do this, we will be increasing hardware & software component diversity so that we can best emulate legacy and current industry environments.
- Plans also call for expansion and enhancement of the SCADA Test Bed to provide commercial, confidential and secure testing and evaluation areas as well as a SCADA Test Bed Control Center.
- We plan to develop a SCADA Outreach Program.
- As part of this program, we plan to establish a dedicated training facility to conduct classes for industry on intrusion detection, data analysis and advanced protection.

A major program that will utilize the assets of the SCADA Test Bed is the National SCADA Program.

- This Program is a collaboration between the INEEL and Sandia National Lab. It is sponsored by the DOE Office of Energy Assurance, and is slated to receive \$2M in funding this FY, split equally between the two labs.
- It will take the best skills and assets from the two national labs and combine them into a single test bed that will be linked via computers.
- It will be developed with input from the user and vendor communities.
- There will be a heavy emphasis on teaming with industry.

- The program will provide independent validation and verification of systems & components.

A very unique part of the Test Range is the INEEL Power Loop which is located at the site, west of Idaho Falls.

- The INEEL maintains an independent power grid which is 61 miles long, 50 mega watts, with a control center and seven isolatable substations.
- This grid allows for full scale testing of complete systems in a controlled environment.

Recent activity at the SCADA Test Bed includes the installation of an ABB Ranger SCADA system in January of this year. SCADA testing is planned for the April-May timeframe with results to be issued in June. These tests will be performed on the ABB system with interconnects to cyber, communications and physical security components.

Next we would like to talk to you about our **Cyber Security Test Bed**.

Current plans are for ~\$560K spending level on this part of the Test Range in FY04

- We will be enhancing existing workspace with dedicated network infrastructure and resources.
- The Cyber Security Test Bed will be integrated with the SCADA, the Wireless/Communications & the Physical Security Test Beds.
- The work to be performed here includes testing and evaluating the components, sub-systems and systems used to control, communicate with and protect energy-related assets.
- Actual construction is expected to begin in February. Planned construction activities include changing lights, replacing ceiling tiles, installing a dedicated HVAC system, and removing all unnecessary wiring and conduit.

Areas of Expertise at the INEEL Cyber Security Test Bed include:

- Intrusion detection
- Network traffic analysis
- Enterprise integrated war dialing
- Incident response and reporting
- Operating system vulnerability assessment
- System forensics
- New technology assessment
- Tool development

The Cyber Security Program is full lifecycle:

- They perform Research & Development;
- They design Information Technology, Communications, and Control Systems;
- Then they use it in operations. In other words, they use what they design on our own infrastructure here at the INEEL.

The last thing that I want to mention about our Cyber Security Program is that we have established University Research Alliances with the University of Idaho and Idaho State University, both of which are designated as National Security Administration, Centers of Excellence for Information Assurance.